Средство администрирования устройств аутентификации

Единый Клиент JaCarta

Руководство пользователя для ОС Linux

Статус	Публичный
Листов	75

Оглавление

1. О документе 4
   - 1.1 Назначение документа 4
   - 1.2 На кого ориентирован данный документ 4
   - 1.3 Организация документа 4
   - 1.4 Рекомендации по использованию документа 4
   - 1.5 Соглашения по оформлению 4
   - 1.6 Авторские права, товарные знаки, ограничения 6
   - 1.7 Лицензионное соглашение 6
2. Основные понятия 8
   - 2.1 Назначение 8
   - 2.2 Термины и определения 8
   - 2.3 Режимы работы средства 8
   - 2.4 Принципы безопасной работы средства 8
   - 2.5 Функции и интерфейсы функций средства, доступные каждой роли пользователей 8
   - 2.6 Параметры (настроек) безопасности средства, связанные с доступными пользователю функциями средства 9
   - 2.7 Типы событий безопасности, связанные с доступными пользователю функциями средства 9
   - 2.8 Действия после сбоев и ошибок эксплуатации средства 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 Информация о PIN-коде пользователя 13
4. Обзор пользовательского интерфейса 14
   - 4.1 Запуск Единого Клиента JaCarta 14
   - 4.2 Меню быстрого запуска 15
   - 4.3 Режимы работы программы 15
     - 4.3.1 Переключение между режимами 15
     - 4.3.2 Основное окно в стандартном режиме 16
     - 4.3.3 Основное окно в расширенном режиме 17
   - 4.4 Зарегистрировать виртуальный токен 18
   - 4.5 Просмотр сведений о программе 22
   - 4.6 Завершение работы программы 22
5. Работа в программе в стандартном режиме 23
   - 5.1 Просмотр информации об электронном ключе 23
   - 5.2 Изменение имени электронного ключа 24
   - 5.3 Изменение PIN-кода пользователя 25
   - 5.4 Разблокирование PIN-кода пользователя 29
     - 5.4.1 Приложение PKI и PKI/BIO 29
     - 5.4.2 Приложение ГОСТ 30
   - 5.5 Установка PIN-кода подписи 32
   - 5.6 Изменение PIN-кода подписи 34
   - 5.7 Разблокирование PIN-кода подписи 35
6. Работа в программе в расширенном режиме 40
   - 6.1 Просмотр информации о приложениях на электронном ключе 40
   - 6.2 Диагностика целостности приложения 42
   - 6.3 Операции с сертификатами в приложении электронного ключа 42
     - 6.3.1 Создание запроса на сертификат 43
     - 6.3.2 Импорт сертификата 46
     - 6.3.3 Экспорт сертификата 50
     - 6.3.4 Просмотр сертификата 53

6.4 Операции с объектами в приложении электронного ключа ... 53
6.4.1 Просмотр списка объектов ... 54
6.4.2 Удаление объектов ... 55

7. JaCarta WebPass: описание, работа и основные методы использования ... 57

7.1 Начало работы ... 58
7.2 Сценарий использования ... 59
7.2.1 Смена PIN-кода ... 59
7.2.2 Управление слотами ... 60

Приложение А. Обозначения электронных ключей ... 73

Контакты ... 74

Офис (общие вопросы) ... 74
Техподдержка ... 74

1. О документе

1.1 Назначение документа

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

1.2 На кого ориентирован данный документ

Документ предназначен пользователей ПО "Единый Клиент JaCarta", владельцев электронных ключей JaCarta.

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 указаны параметры электронных ключей при поставке;
- в разделе 4 "Обзор пользовательского интерфейса" содержится информация об основных приемах работы с ПО "Единый Клиент JaCarta";
- в разделе 5 "Работа в программе в стандартном режиме" приведены операции, совершаемые в ПО "Единый Клиент JaCarta" в стандартном режиме;
- в разделе 6 "Работа в программе в расширенном режиме" приведены операции, совершаемые в ПО "Единый Клиент JaCarta" в расширенном режиме без ввода PIN-кода администратора электронного ключа;
- в разделе 7 "JaCarta WebPass: описание, работа и основные методы использования" приведена информация о том, как работает электронный ключ, его режимы работы и основные процедуры использования.

1.4 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве ознакомительного материала (подробного руководства по 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 (см. Таблица 1).

Таблица 1 — Элементы оформления

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

Ссылка [стр. 4]	Используется для выделения перекрестных ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме
	Ссылка, примечание, заметка
	Совет
	Загрузка (адрес для загрузки ПО, документа)
	Вопрос

1.6 Авторские права, товарные знаки, ограничения

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

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

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

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

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

1.7 Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

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

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

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

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

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

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

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в

данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;

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

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

2. Основные понятия

2.1 Назначение

ПО "Единый Клиент JaCarta" — программное обеспечение, предназначенное 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[1] – последовательность символов, позволяющая разблокировать PIN-код пользователя после его блокировки.

Апплет – программное обеспечение, реализующее функциональность приложения электронного ключа.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

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

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

2.3 Режимы работы средства

Режимы работы ПО "Единый Клиент JaCarta"", переключение между режимами, вид основного окна программы и описание областей графического интерфейса подробно описаны в подразделе "4.3 Режимы работы программы".

2.4 Принципы безопасной работы средства

Основной принцип безопасной работы программы – наличие двух режимов работы программы, рассчитанных на взаимодействие с программой либо пользователя программного средства, либо администратора.

Действия, совершаемые администратором программы, доступны только после предоставления PIN-кода администратора в интерфейсе программы.

Действия, совершаемые пользователем программы, доступны только после предоставления PIN-кода пользователя в интерфейсе программы.

2.5 Функции и интерфейсы функций средства, доступные каждой роли пользователей

Можно выделить две основные роли пользователей программы: администратор и пользователь.

Функции и интерфейсы функций программы, доступные пользователю, представлены в разделе "5 Работа в программе в стандартном режиме".

Функции и интерфейсы функций программы, доступные администратору, представлены в разделе "6 Работа в программе в расширенном режиме".

---

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

Интерфейсы функций описаны для каждой отдельной операции, совершаемой программой.

2.6 Параметры (настроек) безопасности средства, связанные с доступными пользователю функциями средства

Пользователю доступны функции средства, описанные выше (см. подраздел 2.5). Связанные с этими функциями настройки безопасности программы включают в себя операции с PIN-кодом администратора, PIN-кодом пользователя и PIN-кодом подписи.

Проверяемые характеристики параметров безопасности:

- знание PIN-кода;
- владение электронным ключом.

2.7 Типы событий безопасности, связанные с доступными пользователю функциями средства

Функции программы могут возвращать пользователю программы ошибки, связанные с неверно указанным PIN-кодом администратора, PIN-кодом пользователя, либо PIN-кодом подписи.

В случае многократного неверного предъявления PIN-кода и блокирования устройства, графический интерфейс программы отобразит соответствующие кнопки для разблокирования устройства.

2.8 Действия после сбоев и ошибок эксплуатации средства

Виды сбоев и ошибок эксплуатации средства и совершаемые в случае сбоя действия представлены в таблице (см. Таблица 2).

Таблица 2 – Виды сбоя эксплуатации и действия в случае сбоя

Виды сбоя эксплуатации	Действие в случае сбоя
Выход электронного ключа из строя	Необходимо сообщить администратору о выходе электронного ключа из строя и следовать его дальнейшим указаниям
Введён неправильный PIN-код	Повтор ввода PIN-кода
PIN-код заблокирован	Попытаться разблокировать PIN-код; обратиться к администратору

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 стандартном режиме (см. раздел 5 "Работа в программе в стандартном режиме").*

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

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

Пример. *В моделях электронных ключей JaCarta PKI и JaCarta PRO установлено приложение PKI, но в модели JaCarta PKI данное приложение реализовано апплетом/приложением Laser, а в модели JaCarta PRO – апплетом PRO. Название апплета конкретного приложения отображается в интерфейсе Единого Клиента JaCarta в расширенном режиме (см. раздел 6 "Работа в программе в расширенном режиме").*

Соответствие приложений, апплетов и моделей электронных ключей, работа с которыми поддерживается в операционных системах семейства Linux, приведено в таблице (см. Таблица 3).

Таблица 3 – Соответствие приложений, апплетов и моделей электронных ключей

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

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

3.2 Параметры электронных ключей при поставке

При поставке электронные ключи имеют параметры, приведенные в таблице (см. Таблица 4).

Таблица 4 – Параметры электронных ключей при поставке

Приложение и апплет / Параметр, операция	Приложение PKI		Приложение ГОСТ		Приложение STORAGE апплет Datastore	Приложение OTP апплет AladdinOTP
	апплет PRO	апплет Laser	версия 2.5.3 – 2.5.9	версия 2.5.13 и выше		
PIN-код пользователя по умолчанию[2]	1234567890	11111111	1234567890	1234567890	1234567890	1234567890
PUK-код для разблокирования	не предусмотрен	не предусмотрен	0987654321	не предусмотрен	не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	не установлен	00000000	не предусмотрен	0987654321	не установлен	не предусмотрен
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	возможно	невозможно	невозможно	невозможно	операция не предусмотрена
Форматирование без назначения PIN-кода администратора	возможно	невозможно	невозможно	невозможно	невозможно	операция не предусмотрена
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом …	… PIN-код пользователя задается заново	… PIN-код пользователя задается заново	… PIN-код пользователя остается прежним	… PIN-код пользователя остается прежним	… PIN-код пользователя остается прежним	операция не предусмотрена
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	возможно	возможно[3]	возможно[4]	невозможно	невозможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно	невозможно	возможно (настраивается политикой)	невозможно	невозможно

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

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

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

3.3 Информация о PIN-коде пользователя

Основные операции, которые выполняет пользователь в процессе эксплуатации электронного ключа выполняются с предъявлением PIN-кода пользователя.

PIN-код пользователя сообщает администратор при передаче пользователю электронного ключа. Значение PIN-кода может отличаться от типового значения, перечень которых представлен в таблице (см. Таблица 4).

Если в памяти электронного ключа записано несколько приложений, например, PKI и ГОСТ, то для каждого приложения предусмотрен свой PIN-код пользователя.

При получении электронного ключа на руки настоятельно рекомендуется сменить PIN-код пользователя (см. подраздел 5.3 "Изменение PIN-кода пользователя").

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

В случае ввода неверного значения PIN-кода пользователя в количестве раз, превышающее указанное в настройках, PIN-код пользователя будет заблокирован. При заблокированном PIN-коде пользователя невозможно выполнение операций с электронным ключом, которые требуют предъявления PIN-кода пользователя.

Для заблокированных приложений доступна операция разблокирования PIN-кода пользователя. Данная операция выполняется администратором, описание ее выполнения приведено в документе " MFA JC EK. Руководство администратора для операционных систем семейства Linux".

4. Обзор пользовательского интерфейса

4.1 Запуск Единого Клиента JaCarta

Для запуска Единого Клиента JaCarta необходимо:

1. Нажать кнопку  и выбрать "Утилиты" → "JaCartaUC" (см. Рисунок 1);

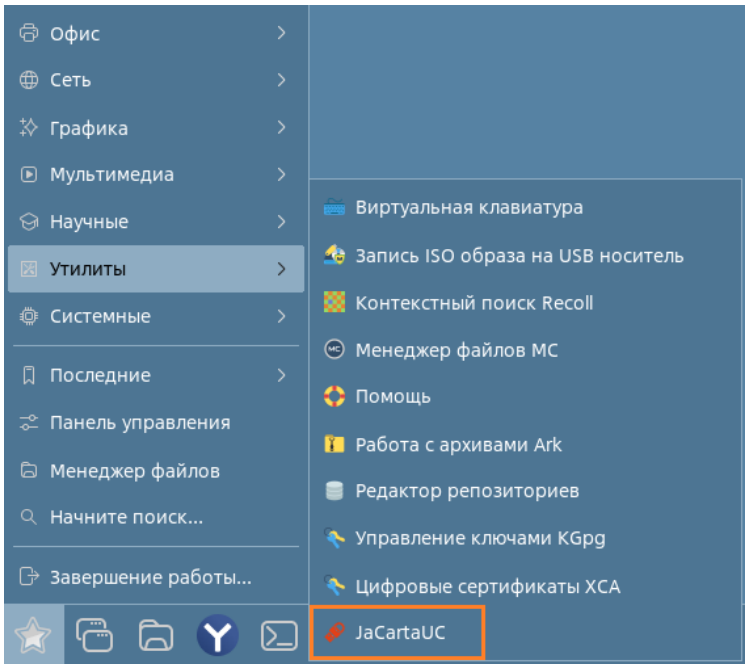


Рисунок 1 – Запуск Единого Клиента JaCarta

2. Откроется основное окно Единого Клиента JaCarta (см. Рисунок 2), при этом в панели управления в нижней части экрана появится значок вызова меню быстрого запуска программы . По умолчанию основное окно Единого Клиента JaCarta открывается в стандартном режиме;

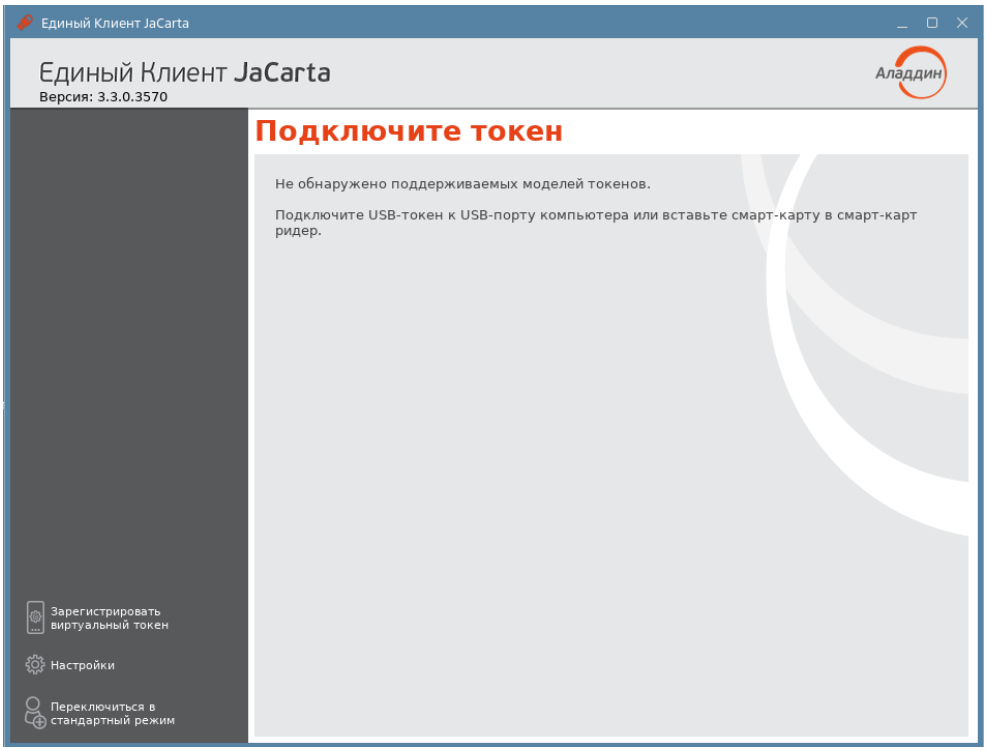


Рисунок 2 – Основное окно Единого Клиента JaCarta и меню быстрого запуска в панели управления

3. Для закрытия основного окна Единого Клиента JaCarta нажать кнопку "Закрыть" в правом верхнем углу. Значок вызова меню быстрого запуска продолжит отображаться в панели управления.

4.2 Меню быстрого запуска

Значок вызова меню быстрого запуска отображается в панели упроавления (в нижней части экрана) даже при закрытом окне ПО "Единый Клиент JaCarta" и предоставляет доступ к меню быстрого запуска.

Для вызова меню быстрого запуска необходимо открыть контекстное меню значка в панели управления (см. Рисунок 3).

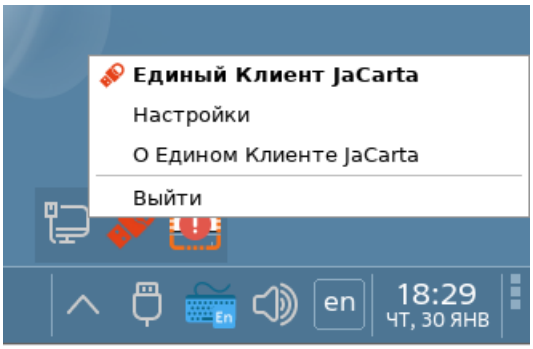


Рисунок 3 –Меню быстрого запуска Единого Клиента JaCarta

Меню быстрого запуска содержит следующие команды:

- ПО "Единый Клиент JaCarta" – открывает окно основного интерфейса ПО "Единый Клиент JaCarta";
- "Настройки" – открывает окно настроек программы;
- "О Едином Клиенте JaCarta" – открывает окно со сведениями о программе (см. подраздел 4.5);
- "Выйти" – позволяет выйти из программы, при этом значок перестает отображаться в панели управления.

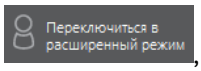
4.3 Режимы работы программы

ПО "Единый Клиент JaCarta" поддерживает следующие режимы работы:

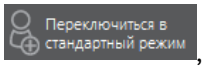
1. **Стандартный режим** – позволяет просматривать краткие сведения о подсоединённых электронных ключах, сменить PIN-код пользователя, назначить или изменить PIN-код подписи, изменить метку электронного ключа.
2. **Расширенный режим** – позволяет просматривать подробные сведения о подсоединённых электронных ключах и предоставляет доступ к операциям над приложениями электронного ключа и объектами каждого приложения.

4.3.1 Переключение между режимами

Чтобы определить в каком режиме открыто окно ПО "Единый Клиент JaCarta", необходимо обратить внимание на название кнопки "Переключиться в режим ..." в основном окне программы (см. рисунок 2). Если кнопка имеет вид:



, то вход осуществлен в стандартном режиме;



, то вход осуществлен в расширенном режиме.

Для переключения между стандартным и расширенным режимом:

1. Для переключения Единого Клиента JaCarta из стандартного режима в расширенный режим нажать кнопку "Переключиться в расширенный режим". При первом нажатии кнопки будет отображено

сообщение о переключении в расширенный режим. Установить отметку "Не отображать это сообщение в дальнейшем", чтобы не предупреждение в дальнейшем не отображалось:

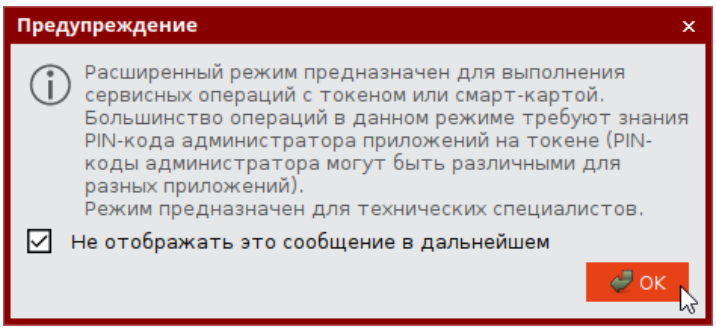


Рисунок 4 – Сообщение при переключении в расширенный режим

2. Для переключения Единого Клиента JaCarta из расширенного режима в стандартный режим нажать кнопку "Переключиться в стандартный режим".

4.3.2 Основное окно в стандартном режиме

По умолчанию основное окно Единого Клиента JaCarta открывается в стандартном режиме. На рисунке (см. Рисунок 5) приведен вид основного окна в стандартном режиме с подключенным к компьютеру пользователя электронным ключом.

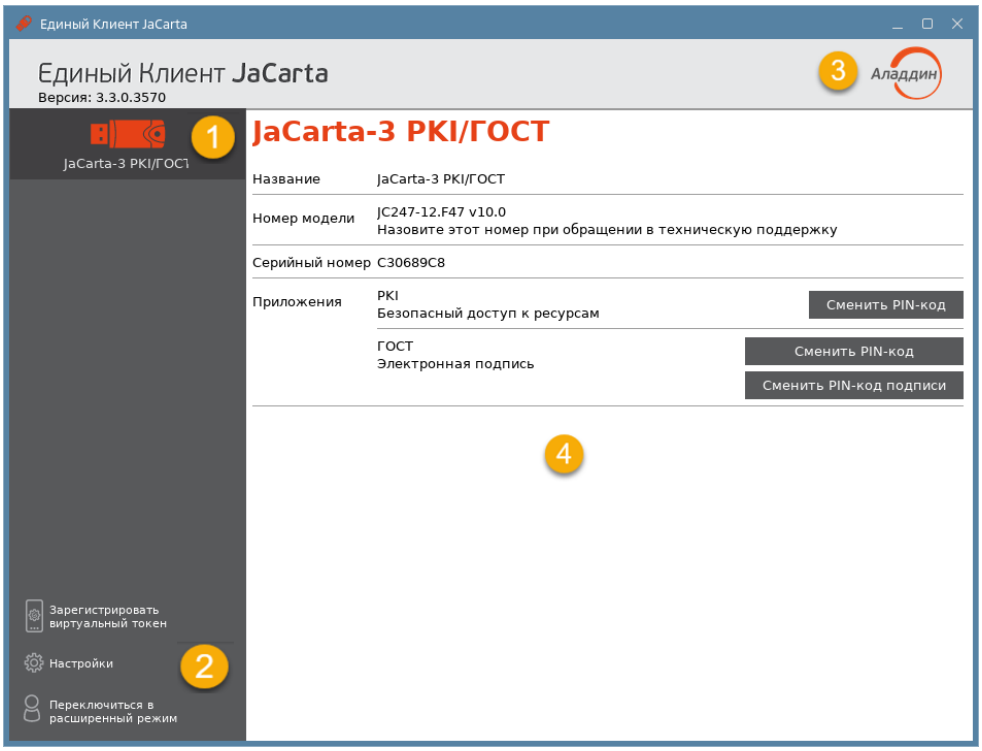


Рисунок 5 – Основное окно Единого Клиента JaCarta в стандартном режиме

Основное окно в стандартном режиме содержит следующие области:

1	Область для отображения подсоединенных к компьютеру электронных ключей. Если к компьютеру пользователя Единого Клиента JaCarta не подсоединен ни один электронный ключ, то данная область пуста. Если подсоединено несколько электронных ключей, то для работы с конкретным ключом щелкнуть значок нужного ключа, после чего в области 4 будут отображены его основные свойства. Вид значка, обозначающий подключенный электронный ключ различается в зависимости от типа ключа. Перечень значков приведен в приложении А на стр. 60
2	Область содержит кнопки: • "Зарегистрировать виртуальный токен" – кнопка для регистрации виртуального токена. Подробное описание приведено в подразделе 4.4; • "Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе " MFA JC EK. Руководство администратора для Linux"; • "Переключиться в расширенный режим" – кнопка для переключения Единого Клиента JaCarta в расширенный режим
3	Открывает окно со сведениями о программе ПО "Единый Клиент JaCarta"
4	Область для отображения информации о выбранном электронном ключе и кнопок управления PIN-кодами пользователя и PIN-кодами подписи приложений электронного ключа.

4.3.3 Основное окно в расширенном режиме

На рисунке (см. Рисунок 6) приведен вид основного окна в расширенном режиме с подключенным к компьютеру пользователя электронным ключом.

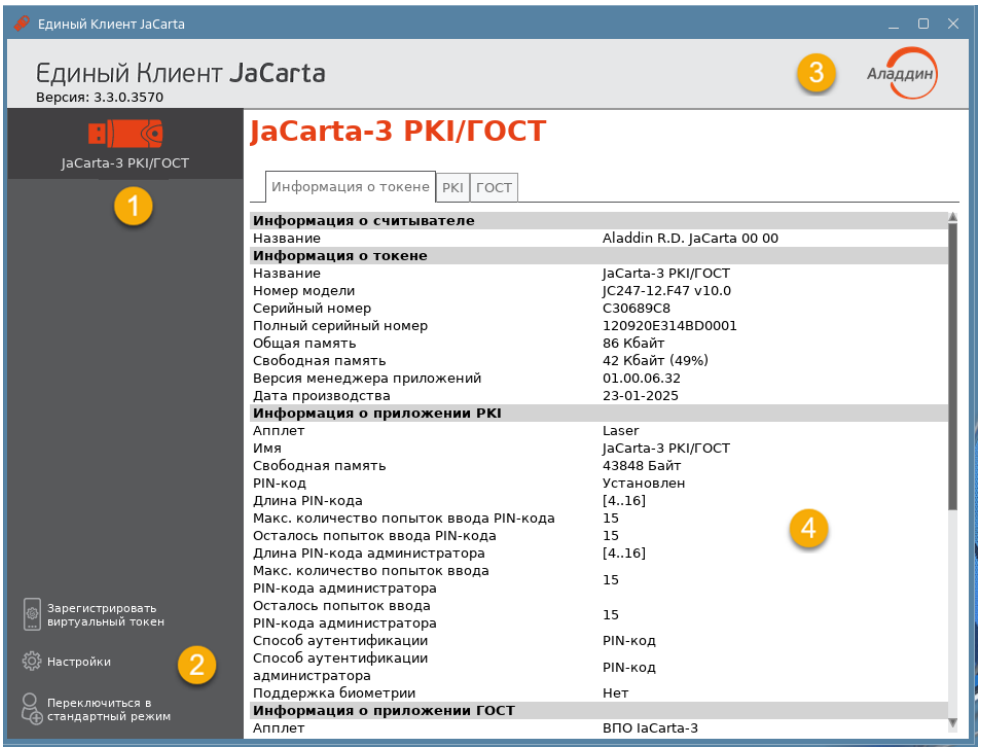


Рисунок 6 – Основное окно Единого Клиента JaCarta в расширенном режиме

Основное окно в расширенном режиме содержит следующие области:

1	Область для отображения подсоединенных к компьютеру электронных ключей. Если к компьютеру пользователя Единого Клиента JaCarta не подсоединен ни один электронный ключ, то данная область пуста. Если подсоединено несколько электронных ключей, то для работы с конкретным ключом щелкнуть значок нужного ключа, после чего в области 4 будет отображен полный список его свойств. Вид значка, обозначающий подключенный электронный ключ различается в зависимости от типа ключа. Перечень значков приведен в приложении А на стр. 60
2	Область содержит кнопки: • "Зарегистрировать виртуальный токен" – кнопка для регистрации виртуального токена. Подробное описание приведено в подразделе 4.4; • "Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе " MFA JC EK. Руководство пользователя для Linux"; • "Переключиться в стандартный режим" – кнопка для переключения Единого Клиента JaCarta в стандартный режим
3	Открывает окно со сведениями о программе ПО "Единый Клиент JaCarta" (см. п. 4.4 "Переключение между режимами")
4	Область управления электронным ключом, выбранным в области 1. В расширенном режиме данная область представлена в виде нескольких вкладок: • на вкладке "Информация о токене" отображается информация о считывателе, информация об электронном ключе и приложениях на электронном ключе (см. рисунок 6): • на вкладке с наименованием приложения доступны операции с данным приложением и объектами, хранящимися в памяти электронного ключа. Для каждого приложения предусмотрена отдельная вкладка. На рисунке (см. Рисунок 6) электронный ключ содержит приложение PKI и приложение ГОСТ, поэтому данная область содержит вкладку "Информация о токене", вкладку "PKI" и вкладку "ГОСТ" для управления приложением PKI, приложением ГОСТ и объектами в этих приложениях.

4.4 Зарегистрировать виртуальный токен

Виртуальный токен – электронная версия аппаратного USB-токена или смарт-карты.

Для работы с виртуальным токеном необходимо ПО JaCarta Virtual Token, которое позволяет использовать мобильное устройство в качестве средства доступа к защищённым информационным ресурсам предприятия, так же как аппаратный USB-токен или смарт-карту.

Перед началом работы должны быть установлены:

- Мобильное приложение JaCarta Virtual Token, доступное для скачивания из магазина приложений, соответствующее операционной системе устройства (приложение реализовано для ОС iOS и Android);
- Клиент JaCarta Virtual Token. Подробно про процесс установки см. в документе "JaCarta Virtual Token. Руководство пользователя", раздел "Клиент JaCarta Virtual Token. Установка и настройка".

После установки Клиента JaCarta Virtual Token и перезагрузки Единого Клиента JaCarta появится новый элемент управления – кнопка "Зарегистрировать виртуальный токен" (см. Рисунок 7).

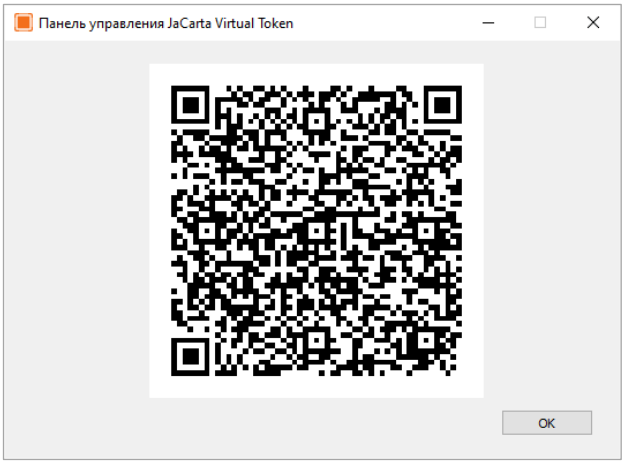


Рисунок 7 – Основное окно Единого Клиента JaCarta. Сгенерированный QR-код

Далее необходимо нажать кнопку "Зарегистрировать виртуальный токен" будет открыто окно [Панель управления JaCarta Virtual Token], содержащее сгенерированный QR-код для регистрации.

На мобильном устройстве открыть установленное мобильное приложение JaCarta Virtual Token. На главном экране нажать кнопку "Добавить" или  (см. Рисунок 8). Будет открыто окно считывания QR-кода (см. Рисунок 9). Отсканировать QR-код, сгенерированный в Панели управления JaCarta Virtual Token.



Рисунок 8 - Мобильное приложение JaCarta Virtual Token. Добавление нового устройства



Рисунок 9 - Мобильное приложение JaCarta Virtual Token. Сканирование QR-кода

В Панели управления JaCarta Virtual Token подтвердить регистрацию мобильного устройства с помощью кнопки "Подтвердить" (см. Рисунок 10).

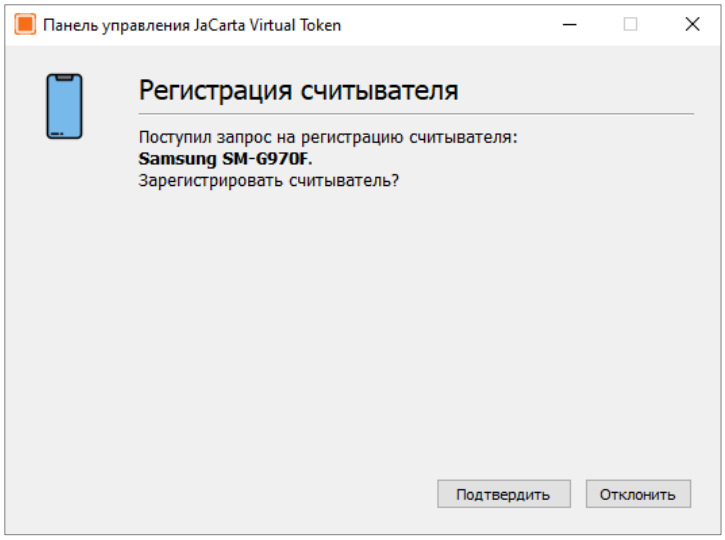


Рисунок 10 – Панель управления JaCarta Virtual Token. Подтверждение регистрации на мобильном устройстве

В случае подтверждения регистрации, отобразится информационное сообщение (см. Рисунок 11).

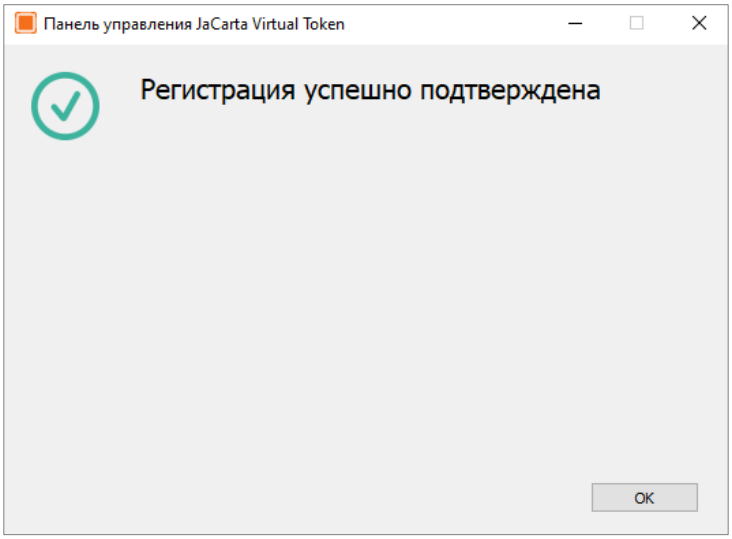


Рисунок 11 - Панель управления JaCarta Virtual Token. Сообщение об успешной регистрации

После регистрации виртуальный токен будет отображаться в окне Единого Клиента точно также, как и аппаратный USB-токен (см. Рисунок 12), операции также аналогичны: переименование токена, смена PIN-кода пользователя, просмотр информации о токене.

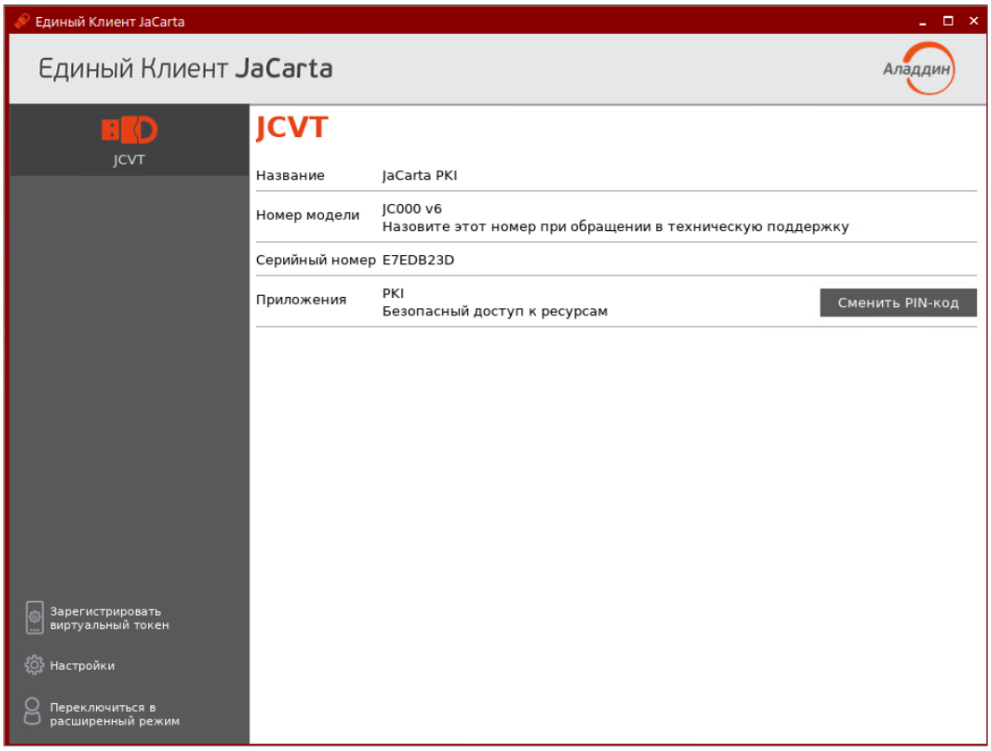


Рисунок 12 - Отображение зарегистрированного виртуального токена

> *Описание работы виртуального токена и Мобильного приложения JaCarta Virtual Token приведено в документе «JaCarta Virtual Token. Руководство пользователя»*

> *Для работы с виртуальным токеном необходимо поменять PIN-код пользователя.*
>
> *По умолчанию заданы следующие настройки:*
>
> *PIN-код пользователя – 11111111;*
>
> *PIN-код администратора - 00000000*

4.5 Просмотр сведений о программе

Для просмотра сведений о программе ПО "Единый Клиент JaCarta" необходимо:

1. В основном окне программы нажать кнопку с логотипом компании в верхнем правом углу 

. Будет отображено окно со сведениями о версии программы и контактами техподдержки (см. Рисунок 13);

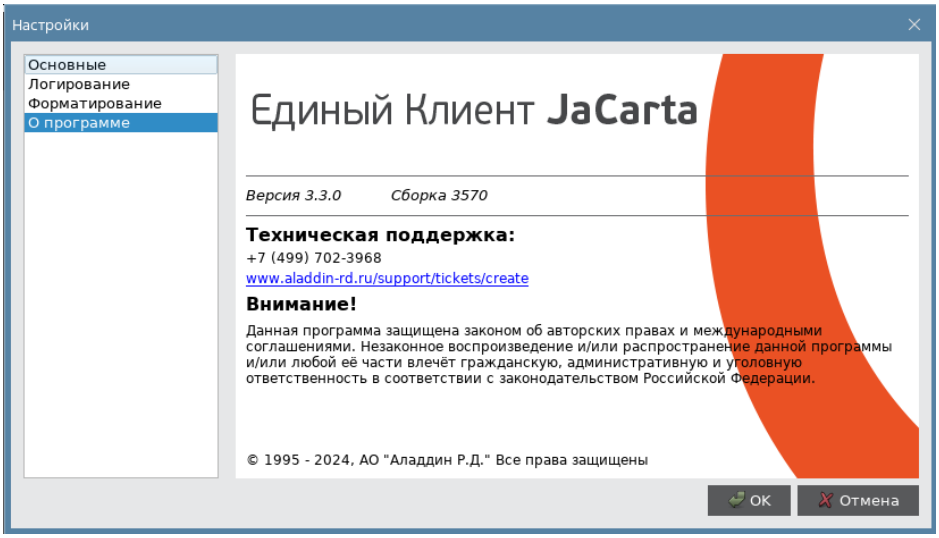


Рисунок 13 – Пункт меню настроек «О программе»

2. Нажать кнопку "ОК" либо кнопку "ОК" в правом нижнем углу для закрытия окна.

4.6 Завершение работы программы

Для завершения работы программы необходимо:

1. Активировать команду "Выйти" в меню быстрого запуска Единого Клиента JaCarta (см. рисунок 3). Работа Единого Клиента JaCarta будет завершена. Значок  перестанет отображаться в панели управления.

5. Работа в программе в стандартном режиме

В стандартном режиме Единого Клиента JaCarta доступны следующие операции с электронными ключами для незаблокированных приложений:

- просмотр информации об электронном ключе;
- изменение имени электронного ключа;
- изменение PIN-кода пользователя;
- установка, изменение, разблокирование PIN-кода подписи (для электронных ключей с приложением ГОСТ).

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

5.1 Просмотр информации об электронном ключе

Для просмотра информации об электронном ключе с помощью Единого Клиента JaCarta не требуется авторизация на электронном ключе.

Для просмотра информации об электронном ключе:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева (см. Рисунок 14);

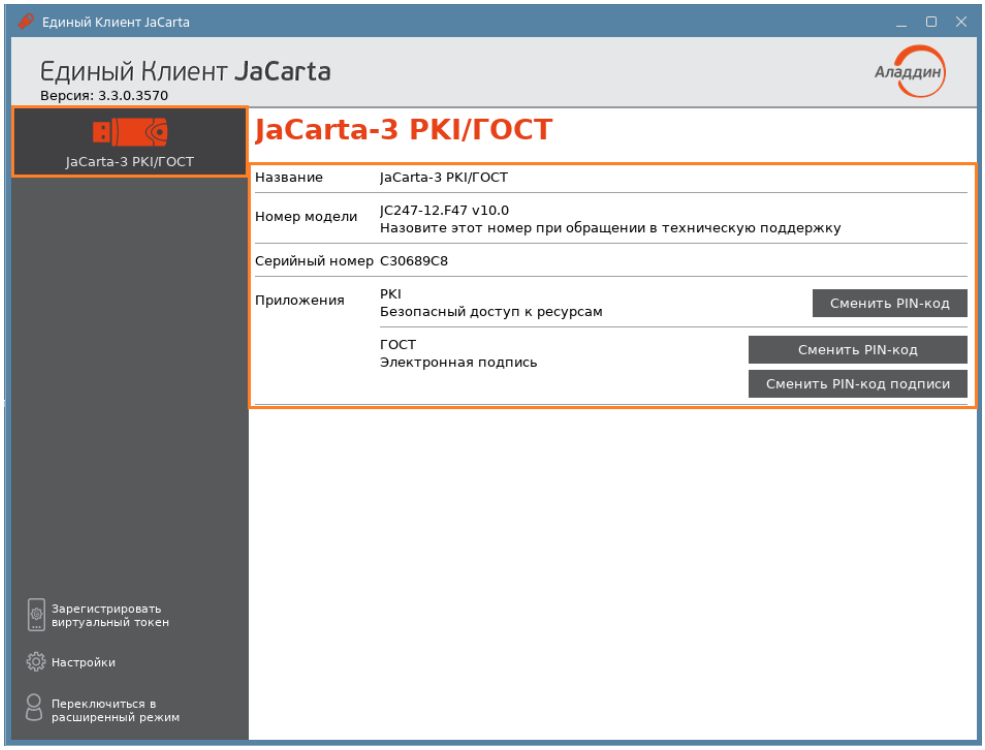


Рисунок 14 – Информация о выбранном электронном ключе в стандартном режиме

Для выбранного ключа в стандартном режиме отображается следующая информация:

– "Название" – название модели электронного ключа;

– "Номер модели" – номер модели выбранного ключа. В случае возникновения проблем при использовании пользователь должен сообщить этот номер в службу технической поддержки;

- "Серийный номер" – серийный номер электронного ключа;
- "Приложения" – перечень приложений, установленных в памяти электронного ключа. Первым в списке отображается приоритетное на данном ключе приложение.

3. Закрыть основное окно Единого Клиента JaCarta нажатием кнопки "Закрыть" в левом верхнем углу.

5.2 Изменение имени электронного ключа

Для изменения метки электронного ключа с помощью Единого Клиента JaCarta требуется авторизация на электронном ключе с предъявлением PIN-кода пользователя.

Для изменения метки электронного ключа:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Активируйте команду "Переименовать токен" в контекстном меню выбранного значка (см. Рисунок 15);

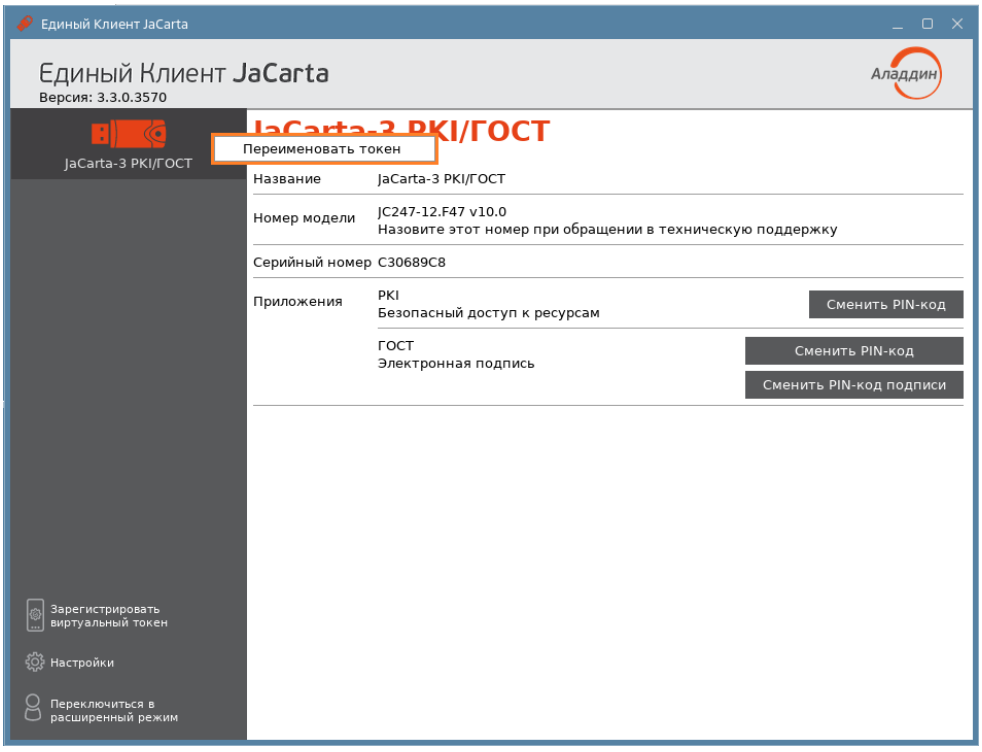


Рисунок 15 – Вызов окна "Переименовать токен" в стандартном режиме

4. Будет отображено одноименное окно (см. Рисунок 16);

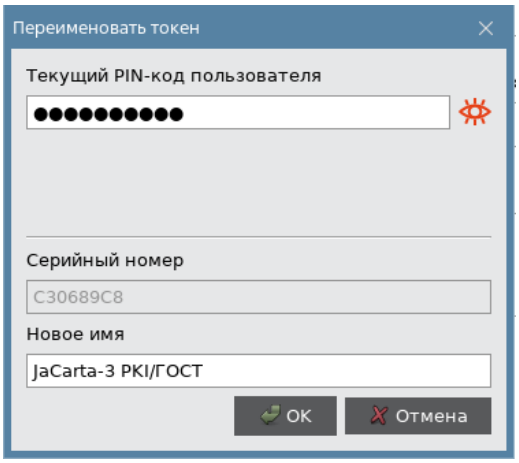


Рисунок 16 – Окно "Переименовать токен" в стандартном режиме

5. В окне "Переименовать токен" заполнить следующие поля:
   - в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя. Если на электронном ключе установлено несколько приложений, то ввести PIN-код приложения, которое является приоритетным – это приложение отображается первым в списке установленных приложений в основном окне;
   - в поле "Новое имя" ввести новое имя электронного ключа.
6. Нажать кнопку "OK". В случае успешной авторизации на электронном ключе его имя будет изменено (см. Рисунок 17).

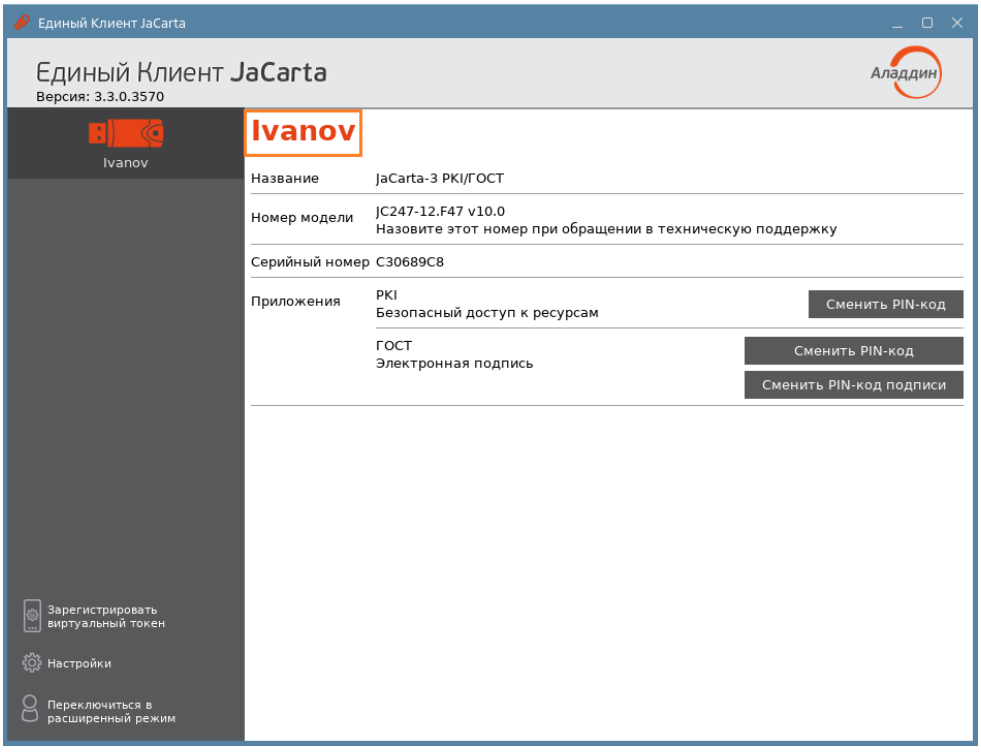


Рисунок 17 – Основное окно в стандартном режиме. Имя ключа изменено

5.3 Изменение PIN-кода пользователя

В случае отображения в окне Единого Клиента JaCarta сообщения о том, что установлен PIN-код по умолчанию (см. Рисунок 18), рекомендуется сменить PIN-код пользователя.

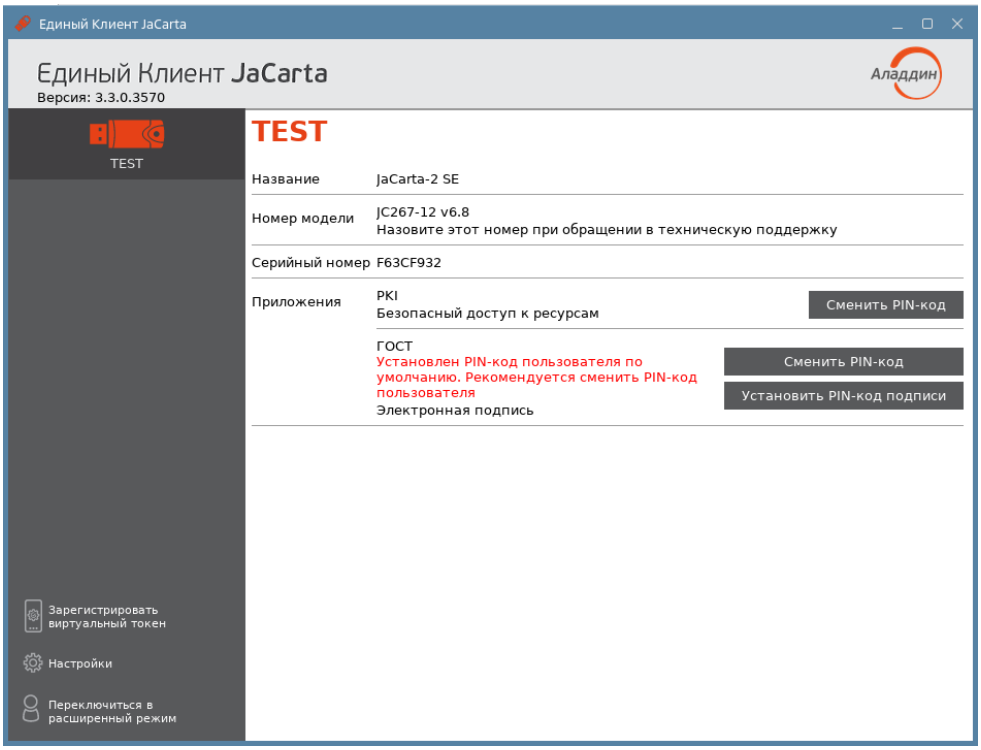


Рисунок 18 — Окно Единого Клиента JaCarta

Операция изменения PIN-кода пользователя выполняется отдельно для каждого приложения, установленного на электронном ключе и доступна только для незаблокированного приложения с установленным PIN-кодом пользователя. Для выполнения операции требуется предъявление текущего PIN-кода пользователя данного приложения.

Для изменения PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;

3. В основном окне Единого Клиента JaCarta в стандартном режиме нажать кнопку "Сменить PIN-код" для выбранного приложения. На рисунке (см. Рисунок 19) приведен пример смены PIN-кода приложения PKI;

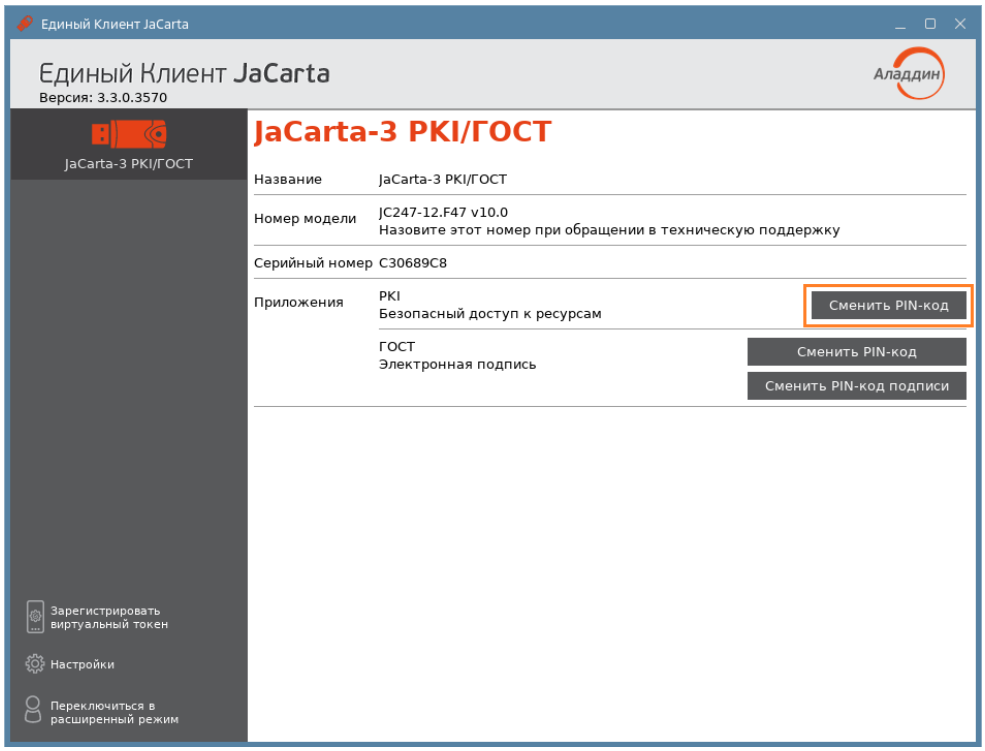


Рисунок 19 – Вызов окна "Сменить PIN-код" в стандартном режиме

4. В окне "Сменить PIN-код" заполнить следующие поля (см. Рисунок 20):
   - в поле "Текущий PIN-код" ввести PIN-код пользователя выбранного приложения (в данном примере приложения PKI);
   - в поле "Новый PIN-код" ввести значение нового PIN-кода пользователя

     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.
   - в поле "Подтвердить PIN-код пользователя" ввести значение нового PIN-кода пользователя повторно.

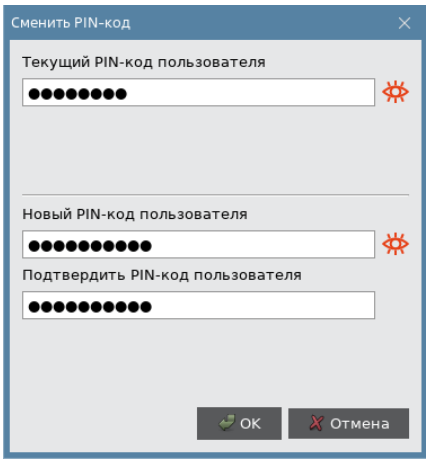


Рисунок 20 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода введены верно

Новое значение PIN-кода пользователя не должно совпадать с его текущим значением. Если значения совпадают, то будет отображено сообщение об этом и операция не будет продолжена (кнопка "OK" неактивна) до тех пор, пока не будет введено другое значение PIN-кода (см. Рисунок 21).

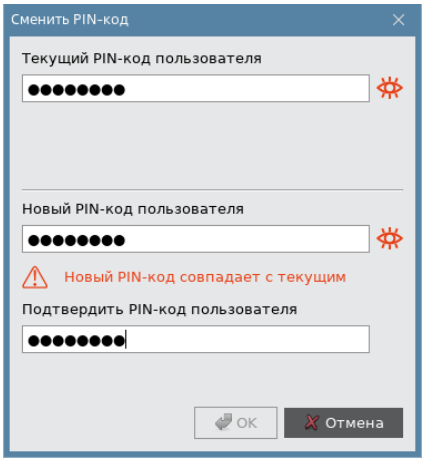


Рисунок 21 – Окно изменения PIN-кода пользователя. Значение нового PIN-кода совпадает с текущим

Значения, введенные в поля "Новый PIN-код" и "Подтвердить PIN-код пользователя" должны совпадать. Если значения не совпадают, то будет отображено сообщение об этом и операция не будет продолжена до тех пор (кнопка "OK" неактивна) до тех пор, пока не будет введено другое значение PIN-кода (см. Рисунок 22).

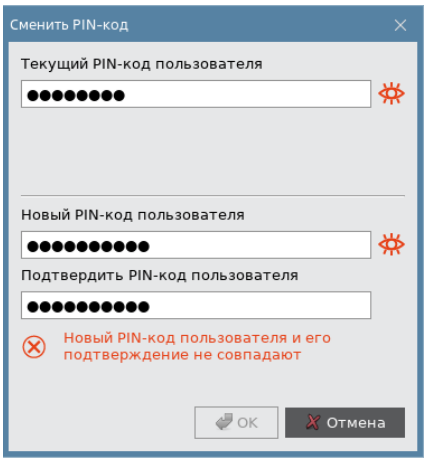


Рисунок 22 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода не совпадают

По умолчанию введенные значения PIN-кода показаны в скрытом виде. Чтобы показать их в явном виде нажать кнопку . Для возвращения к отображению в скрытом виде нажать кнопку  (см. Рисунок 23).

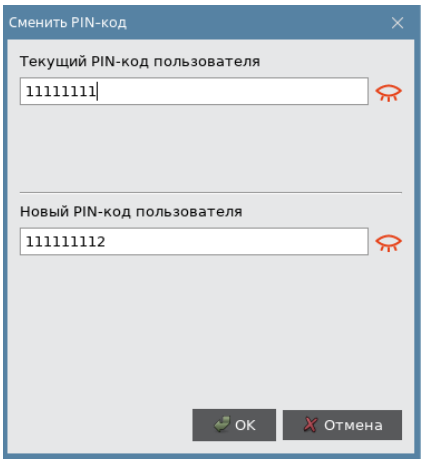


Рисунок 23 – Окно изменения PIN-кода пользователя. Отображение значений полей в явном виде

5. Нажать кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-кода пользователя будет изменен (см. Рисунок 24);

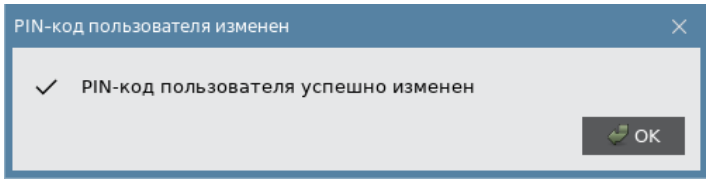


Рисунок 24 – Сообщение об успешном изменении PIN-кода пользователя

6. Нажать кнопку "OK" в окне сообщения для его закрытия.

5.4 Разблокирование PIN-кода пользователя

Если пользователь превысил максимальное допустимое число последовательных неверных попыток ввода PIN-кода, то он блокируется.

5.4.1 Приложение PKI и PKI/BIO

Для разблокирования PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. 25). Иначе кнопка заблокирована;



Рисунок 25 - Элемент управления "Разблокировать PIN-код"

4. Далее будет открыто окно "Разблокировать PIN-код" (см. Рисунок 26);
5. В поле "PIN-код администратора" ввести текущий PIN-код администратора;
6. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новый PIN-код пользователя и нажать кнопку "OK";

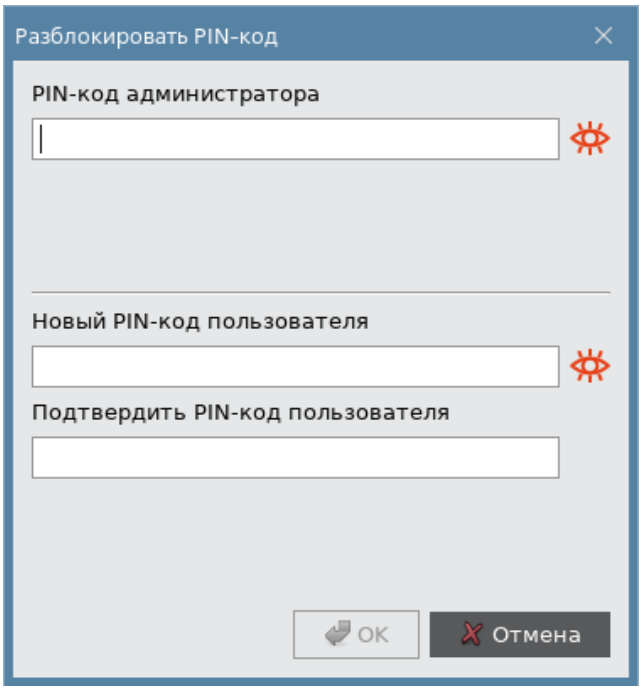


Рисунок 26 - Разблокировка PIN-кода пользователя

7. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение – нажать кнопку "OK", чтобы закрыть его (см. Рисунок 27).

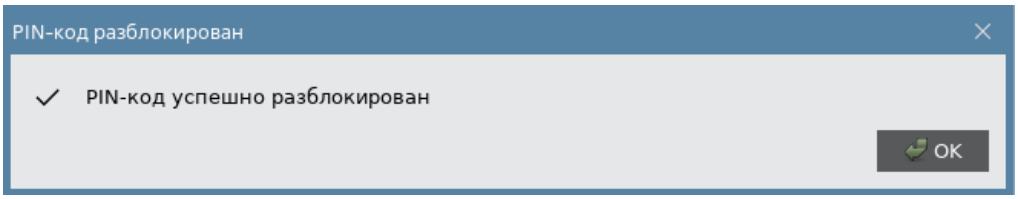


Рисунок 27 - Сообщение об успешной разблокировке PIN-кода пользователя

5.4.2 Приложение ГОСТ

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

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

Для разблокирования PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. Рисунок 28);

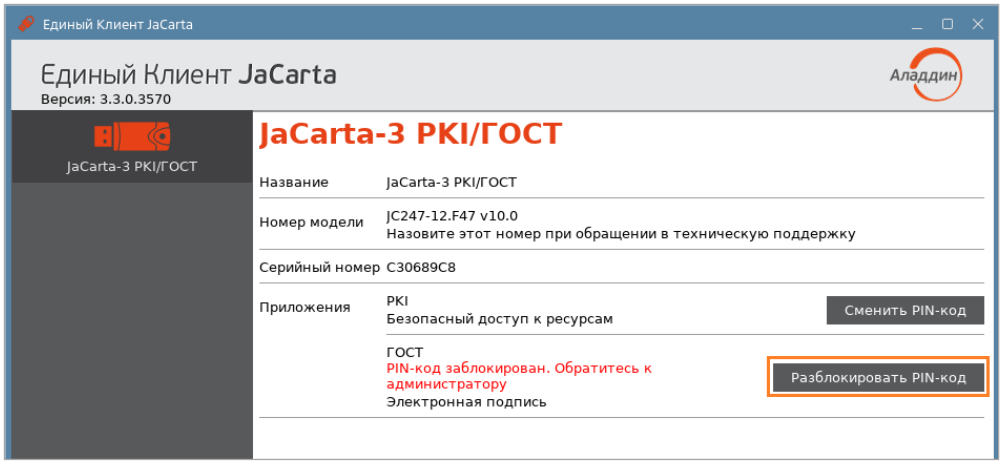


Рисунок 28 - Элемент управления "Разблокировать PIN-код"

4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода" (см. Рисунок 29);

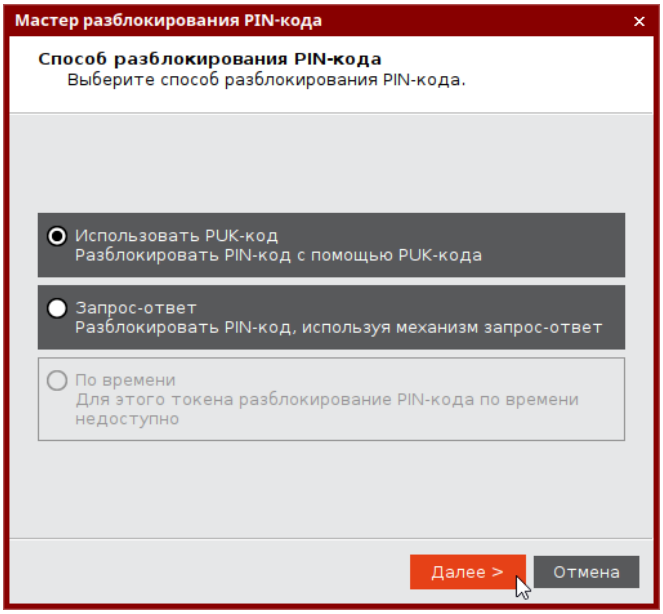


Рисунок 29 - Окно "Разблокировка PIN-кода пользователя"

5. Выбрать пункт "Использовать PUK-код" и нажать кнопку "Далее";
6. В поле "PUK-код" ввести текущий PUK-код[5], после чего нажать кнопку "Далее";
7. При успешной разблокировке отобразится соответствующее сообщение. Для его закрытия нажать кнопку "Завершить" (см. Рисунок 30).

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

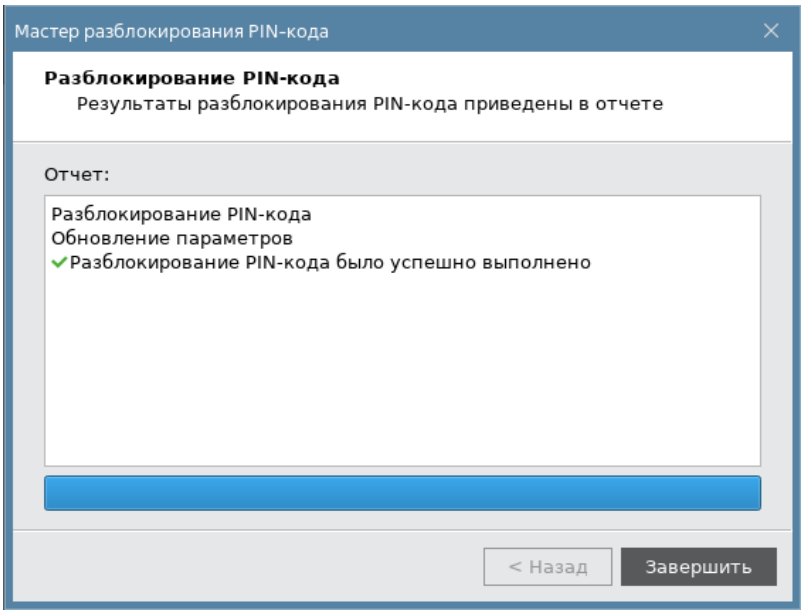


Рисунок 30 - Информационное сообщение об успешной разблокировке PIN-кода пользователя

5.5 Установка PIN-кода подписи

Операция установки PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ при получении электронного ключа. PIN-код подписи необходим для выполнения операций электронной подписи.

Операция доступна только для незаблокированного приложения. Для выполнения операции требуется предъявление текущего PIN-кода пользователя данного приложения.

После установки PIN-кода подписи доступна операция изменения PIN-кода подписи (см. п. 5.6 "Изменение PIN-кода подписи").

PIN-код подписи блокируется после ввода неправильного PIN-кода подписи в количестве раз, превышающее указанное в настройках. Для заблокированного PIN-кода подписи доступна операция его разблокирования (см. подраздел 5.7 "Разблокирование PIN-кода подписи").

Для установки PIN-кода подписи необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;

3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Установить PIN-код подписи" для приложения ГОСТ (см. Рисунок 31);

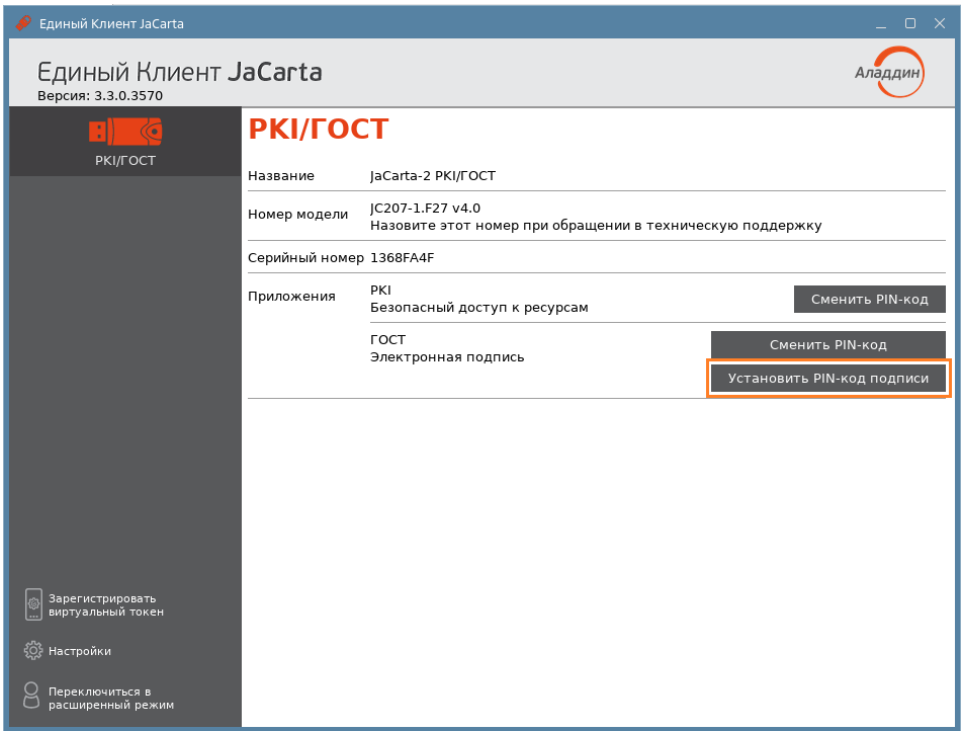


Рисунок 31 – ПО "Единый Клиент JaCarta". Главное окно

4. В окне "Установить PIN-код подписи" заполнить следующие поля (см. Рисунок 32):
   - в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя выбранного приложения (в данном примере приложения ГОСТ);
   - в поле "Установить PIN-код подписи" ввести значение нового PIN-кода подписи;

     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.
   - в поле "Подтвердить PIN-код подписи" ввести значение нового PIN-кода подписи повторно. При этом значения, введенные в поля " Установить PIN-код подписи" и "Подтвердить PIN-код подписи" должны совпадать. Если значения не совпадают, то будет отображено сообщение об этом и операция не будет продолжена до тех пор, пока не будет введено другое значение PIN-кода.

   По умолчанию введенные значения PIN-кода показаны в скрытом виде. Чтобы показать их в явном виде нажать кнопку . Для возвращения к отображению в скрытом виде нажать кнопку .

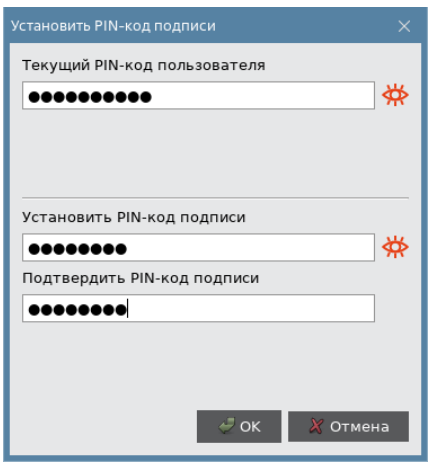


Рисунок 32 - Окно установки PIN-кода подписи. Значения PIN-кода введены верно

5. Нажать кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-код подписи будет установлен. На экране появится сообщение об этом (см. Рисунок 33);

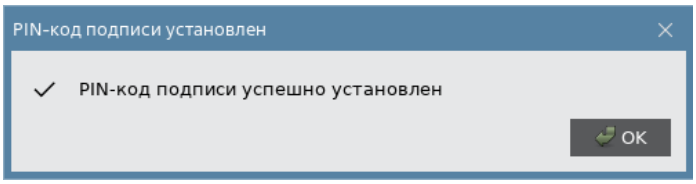


Рисунок 33 – Сообщение об успешной инициализации PIN-кода подписи

6. Нажать кнопку "OK" в окне сообщения.

5.6 Изменение PIN-кода подписи

Операция изменения PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ с установленным PIN-кода подписи. Операция доступна только для незаблокированного приложения. Для выполнения операции изменения PIN-кода подписи требуется предъявление текущего PIN-кода пользователя данного приложения.

Для изменения PIN-кода подписи необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Сменить PIN-код подписи" для приложения ГОСТ (см. Рисунок 34);

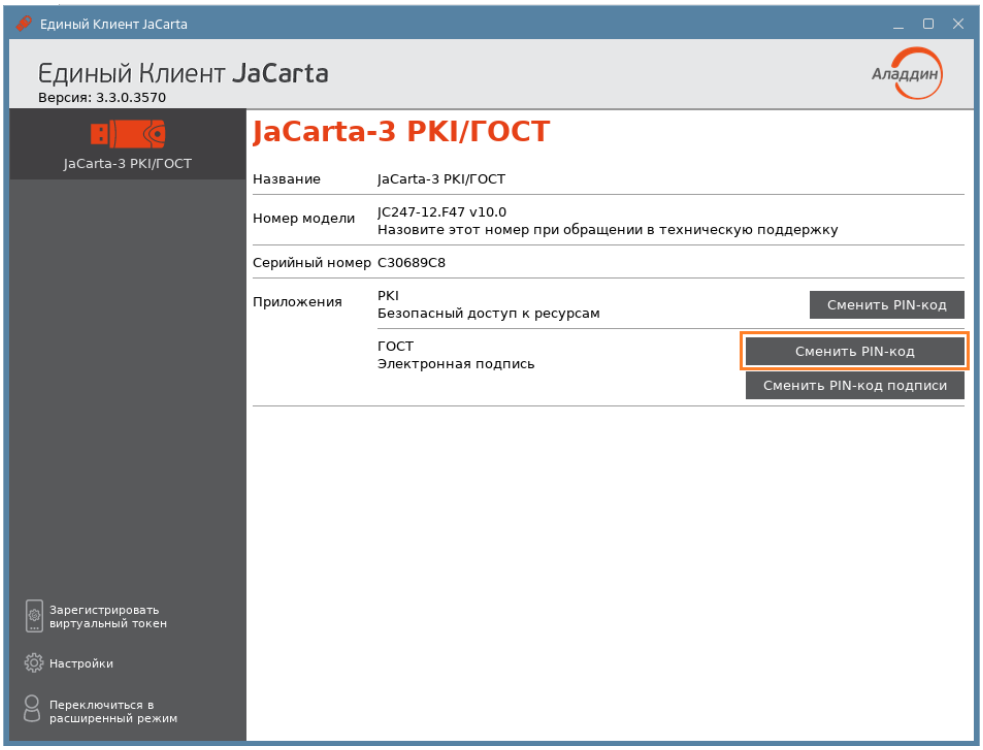


Рисунок 34 - ПО "Единый Клиент JaCarta". Главное окно

4. В окне "Сменить PIN-код подписи" заполнить следующие поля (см. Рисунок 35):
   - в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя выбранного приложения (в данном примере приложения ГОСТ);
   - в поле "Текущий PIN-код подписи" ввести PIN-код подписи;

– в поле "Новый PIN-код подписи" ввести значение нового PIN-кода подписи. При этом новое значение PIN-кода подписи не должно совпадать с его текущим значением. Если значения совпадают, то будет отображено сообщение об этом и операция не будет продолжена до тех пор, пока не будет введено другое значение PIN-кода.

> *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.*

– в поле "Подтвердить PIN-код подписи" ввести значение нового PIN-кода подписи повторно. При этом значения, введенные в поля " Новый PIN-код подписи" и "Подтвердить PIN-код подписи" должны совпадать. Если значения не совпадают, то будет отображено сообщение об этом и операция не будет продолжена до тех пор, пока не будет введено другое значение PIN-кода.

По умолчанию введенные значения PIN-кода показаны в скрытом виде. Чтобы показать их в явном виде нажать кнопку . Для возвращения к отображению в скрытом виде нажать кнопку .

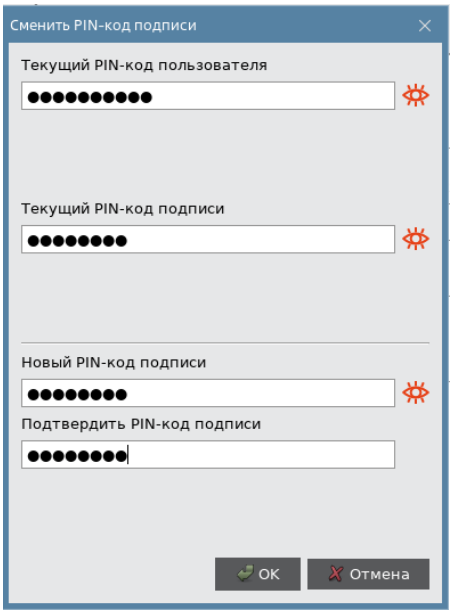


Рисунок 35 - Окно изменения PIN-кода подписи. Значения PIN-кода введены верно

5. Нажать кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-код подписи будет установлен. На экране появится сообщение об этом (см. Рисунок 36);

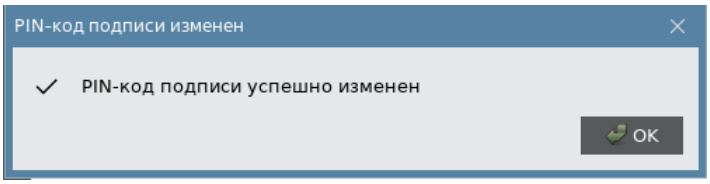


Рисунок 36 – Сообщение об успешном изменении PIN-кода подписи

6. Нажать кнопку "OK" в окне сообщения для его закрытия.

5.7 Разблокирование PIN-кода подписи

Операция разблокирования PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ и заблокированным PIN-кодом подписи. Операция доступна только для незаблокированного приложения.

> *В результате разблокирования PIN-кода подписи происходит сброс счетчика неверных попыток ввода PIN-кода, значение PIN-кода подписи при этом не изменяется.*

Для выполнения операции разблокирования PIN-кода подписи требуется предъявление PUK-кода[6] данного приложения электронного ключа. Информация об установке PUK-кода отображается в основном окне Единого Клиента JaCarta в расширенном режиме (см. п. 6 "Работа в программе в расширенном режиме").

> *Если PUK-код не установлен, то возможен вариант разблокирования PIN-кода подписи с использованием механизма "запрос-ответ". В этом случае потребуется участие в процедуре администратора безопасности.*

После разблокирования PIN-кода подписи доступна операция изменения PIN-кода подписи (см. п. 5.6 "Изменение PIN-кода подписи").

Для разблокирования PIN-кода подписи с предъявлением PUK-кода необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Разблокировать PIN-код подписи" для приложения ГОСТ (см. Рисунок 37);

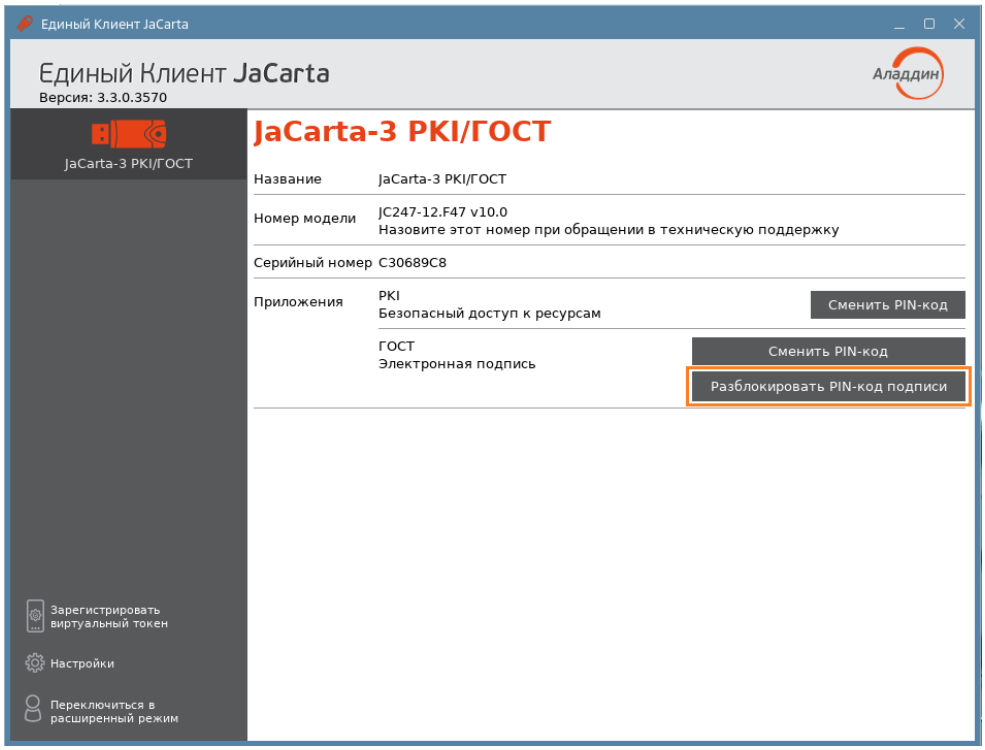


Рисунок 37 - ПО "Единый Клиент JaCarta". Главное окно

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

4. Будет отображено стартовое окно мастера разблокирования PIN-кода подписи. Выбрать способ разблокирования "Использовать PUK-код" (см. Рисунок 38);

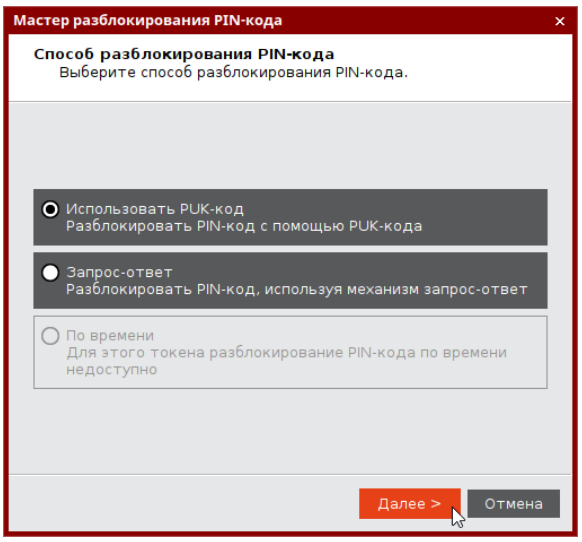


Рисунок 38 – Мастер разблокирования PIN-кода подписи. Выбор способа разблокирования "Использовать PUK-код"

5. Нажать кнопку "Далее". Будет отображено окно мастера разблокирования PIN-кода подписи для ввода PUK-кода приложения[7]. В поле "PUK-код" ввести значение PUK-кода;

При превышении допустимого количества неверных попыток ввода PUK-код блокируется. Разблокирование PUK-кода средствами Единого клиента JaCarta не предусмотрено. Для разблокирования PUK-кода необходимо обратиться к администратору безопасности.

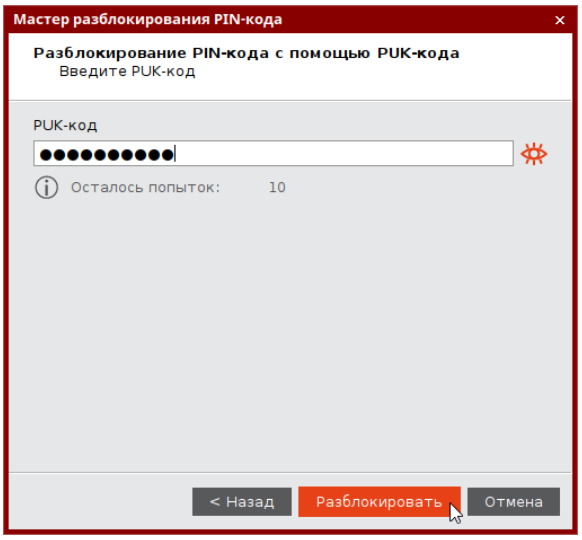


Рисунок 39 – Мастер разблокирования PIN-кода подписи. Ввод PUK-кода

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

6. Нажать кнопку "Разблокировать". В случае ввода верного PUK-кода будет выполнено разблокирование PIN-кода подписи. Информация об этом будет отображена в заключительном окне мастера разблокирования (см. Рисунок 40);

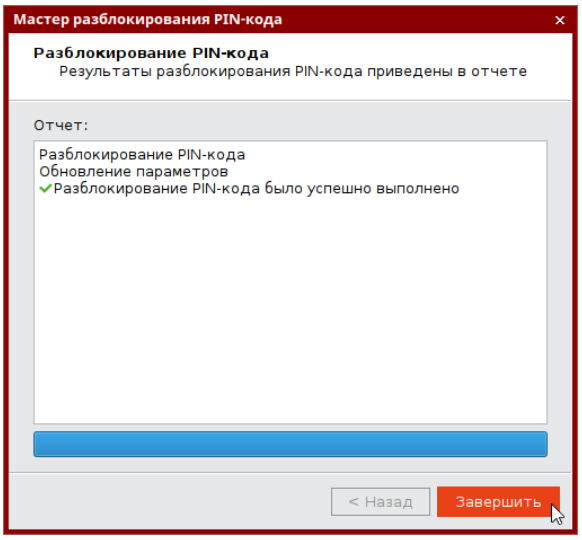


Рисунок 40 – Мастер разблокирования PIN-кода подписи. Информация об успешном разблокировании

7. Нажать кнопку "Завершить", чтобы закрыть окно мастера разблокирования.

Для разблокирования PIN-кода подписи с использованием механизма "запрос-ответ" необходимо:

1. Выполните шаги 1–2 процедуры разблокирования PIN-кода подписи с предъявлением PUK-кода (см. выше).
2. В стартовом окне мастера разблокирования PIN-кода подписи выбрать способ разблокирования "Запрос-ответ" (см. Рисунок 41);

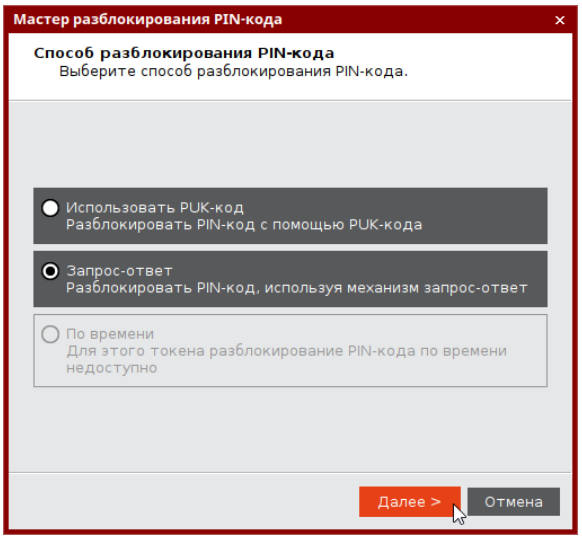


Рисунок 41 – Мастер разблокирования PIN-кода подписи. Выбор способа разблокирования "Запрос-ответ"

3. Нажать кнопку "Далее". Будет отображено окно мастера разблокирования PIN-кода подписи с автоматически сгенерированным значением в поле "Запрос" (см. рисунок 42). Передать это значение администратору безопасности любым удобным способом, например, по e-mail. Дождаться ответа. В процессе ожидания можно закрыть окно мастера разблокирования PIN-кода подписи;

4. Получить от администратора безопасности значение для разблокирования PIN-кода подписи и ввести его в поле "Ответ" (см. Рисунок 42);

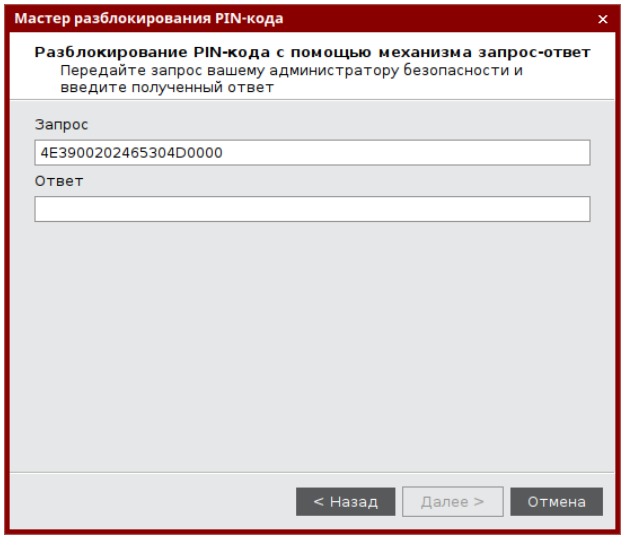


Рисунок 42 – Мастер разблокирования PIN-кода подписи. Получение запроса и ввода ответа

5. Нажать кнопку "Далее". Будет выполнено разблокирование PIN-кода подписи. Информация об этом будет отображена в заключительном окне мастера разблокирования (см. Рисунок 43);

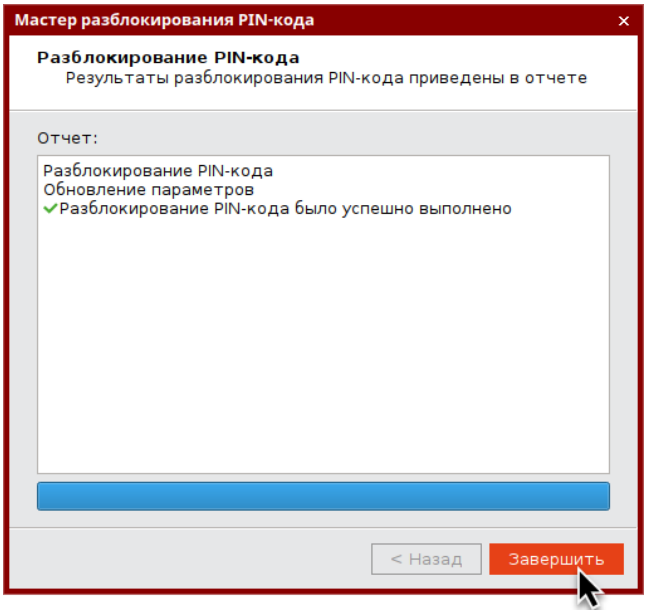


Рисунок 43 – Мастер разблокирования PIN-кода подписи. Информация о успешном разблокировании

6. Нажать кнопку "Завершить", чтобы закрыть окно мастера разблокирования.

6. Работа в программе в расширенном режиме

В расширенном режиме Единого Клиента JaCarta доступны следующие операции с электронными ключами для незаблокированных приложений:

- просмотр информации об электронном ключе и приложениях на электронном ключе;
- проверка целостности приложения (для электронных ключей с приложением ГОСТ);
- операции с сертификатами: создание запроса на сертификат и сохранение его в файл по указанному пути, импорт сертификата в память электронного ключа, экспорт сертификата из памяти электронного ключа, просмотр сертификата, хранящегося в памяти электронного ключа;
- операции с объектами в памяти электронного ключа: просмотр списка объектов, хранящихся в памяти электронного ключа, удаление объектов из памяти электронного ключа.

В данном документе описаны операции, которые не требуют авторизации на электронном ключе с предъявлением PIN-кода администратора. Операции, требующие ввода PIN-кода администратора описаны в документе "MFA JC EK. Руководство администратора для ОС Linux".

6.1 Просмотр информации о приложениях на электронном ключе

Для просмотра информации о приложениях на электронном ключе с помощью Единого Клиента JaCarta не требуется авторизация на электронном ключе.

Для просмотра информации о приложениях на электронном ключе необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Нажать кнопку "Переключиться в расширенный режим" и на вкладке "Информация о токене" будет отображена подробная информация о токене (см. Рисунок 44);

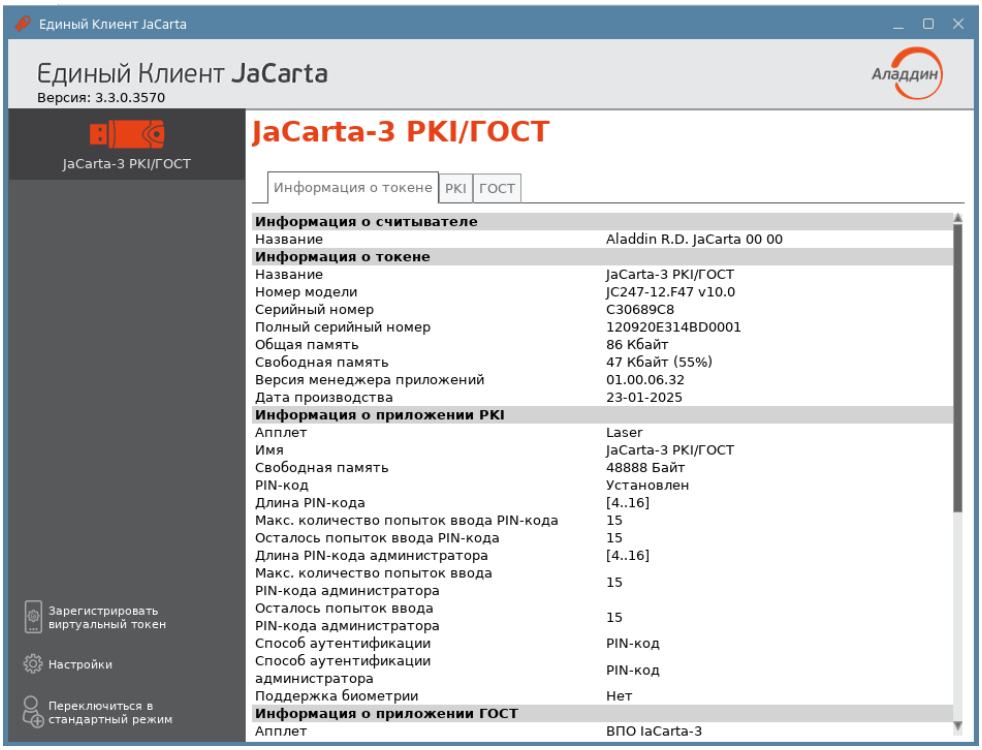


Рисунок 44 – Информация о приложениях на электронном ключе в расширенном режиме

Для выбранного ключа в расширенном режиме по умолчанию отображается вкладка "Информация о токене", в которой содержится информация о считывателе, информация об электронном ключе и информация о каждом приложении на электронном ключе.

Для каждого приложения, установленного в памяти электронного ключа, отображается следующая информация:

- "Апплет" – название апплета, который реализует функциональность данного приложения.
- "Имя" – название электронного ключа.
- "Длина PIN-кода" – количество символов PIN-кода пользователя приложения.
- "PIN-код" – статус PIN-кода пользователя приложения: установлен/не установлен.
- "Макс. количество попыток PIN-кода" – максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя.
- "Осталось попыток ввода PIN-кода" – количество неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода пользователя.
- "Длина PIN-кода администратора" – длина PIN-кода администратора выбранного приложения (только для приложений PKI, STORAGE).
- "Макс. попыток ввода PIN-кода администратора" – максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора (только для приложений PKI, PRO, STORAGE).
- "Осталось попыток ввода PIN-кода администратора" – количество неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода администратора (только для приложений PKI, PRO, STORAGE).
- "Способ аутентификации" – установленный способ аутентификации пользователя.
- "Способ аутентификации администратора" – установленный способ аутентификации администратора.
- "PIN-код подписи" – статус PIN-кода подписи приложения: установлен/не установлен
- "Макс. количество попыток ввода PIN-кода подписи" – максимально допустимое число неверных последовательных попыток ввода PIN-кода подписи.
- "Осталось попыток ввода PIN-кода подписи" - количество неверных попыток ввода PIN-кода подписи до блокировки возможности использования PIN-кода подписи.
- "PUK-код" – признак наличия установленного PUK-кода (только для приложения ГОСТ).
- "Макс. попыток ввода PUK-код" – максимально допустимое количество неверных последовательных попыток ввода PUK-кода (только для приложения ГОСТ).
- "Осталось попыток ввода PUK-кода" – количество оставшихся попыток ввода PUK-кода.
- "Версия токена" – номер версии электронного ключа (только для приложения ГОСТ).
- "Версия приложения" – номер версии установленного апплета (только для приложения ГОСТ).
- "Количество ключевых пар" – количество ключевых пар, хранящихся на токене на текущий момент (только для приложения ГОСТ).
- "Количество секретных ключей" – количество секретных ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ).
- "Количество открытых ключей" – количество открытых ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ).
- "Режим предъявления ключа администратора" – установленный режим предъявления ключа администратора (только для приложения ГОСТ)
- "Количество разблокировок" – количество успешно выполненных разблокирований PIN-кода пользователя (только для приложения ГОСТ)

6.2 Диагностика целостности приложения

В ходе операции диагностики целостности выполняется проверка контрольной суммы приложения. Операция диагностики целостности предусмотрена для приложения ГОСТ. Для выполнения операции не требуется авторизация в приложении.

Для диагностики приложения ГОСТ необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти во вкладку "ГОСТ" для доступа к операциям приложения ГОСТ и нажать кнопку "Диагностика" (см. Рисунок 45);

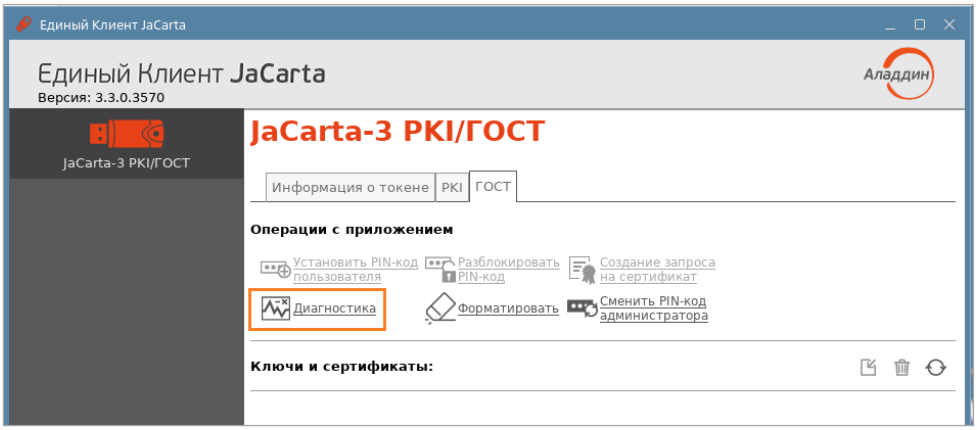


Рисунок 45 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Диагностика..." активна

4. Подтвердить выполнение диагностики. Будет выполняться диагностика целостности приложения ГОСТ (см. Рисунок 46);

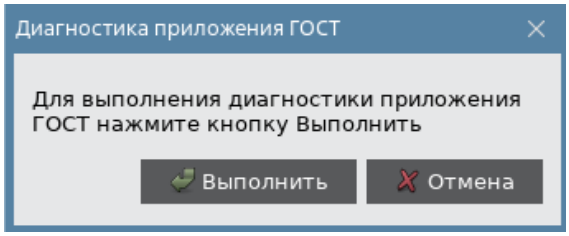


Рисунок 46 – Окно подтверждения диагностики

5. В случае успешного завершения операции будет отображена информация об этом. Нажать кнопку "ОК" для закрытия окна (см. Рисунок 46).

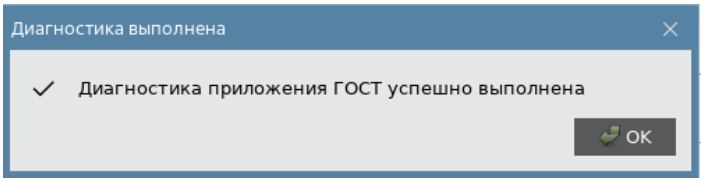


Рисунок 47 – Сообщение об успешном выполнении диагностики

6.3 Операции с сертификатами в приложении электронного ключа

Для выполнения операций с сертификатами, хранящимися в памяти электронного ключа, требуется авторизация на электронном ключе с предъявлением PIN-кода пользователя.

6.3.1 Создание запроса на сертификат

Для создания запроса на сертификат необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку с наименованием приложения, для которого необходимо создать запрос на сертификат (в данном примере выбрано приложение PKI) и нажать кнопку "Создание запроса на сертификат". Кнопка активна при вводе PIN-кода пользователя (см. Рисунок 48);

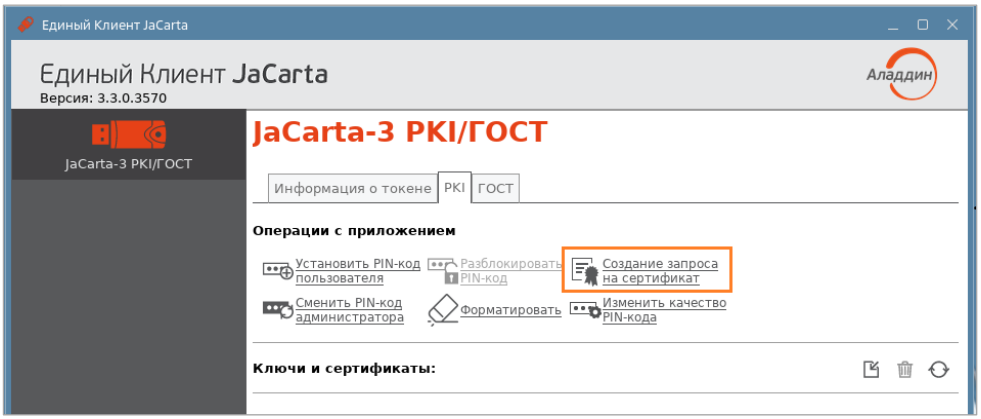


Рисунок 48 - Авторизация с помощью PIN-кода пользователя на электронном ключе в приложении PKI

4. В окне "Мастер создания запроса на сертификат" заполнить следующие поля (см. Рисунок 49):
   - в поле "Имя" ввести наименование создаваемого сертификата. Поле является обязательным для заполнения;
   - в раскрывающемся списке "Тип ключевой пары" выбрать алгоритм шифрования "RSA" (задан по умолчанию) либо "ECC";
   - в раскрывающемся списке "Размер ключа" выбрать размер открытого ключа. По умолчанию выбрано значение "1024".

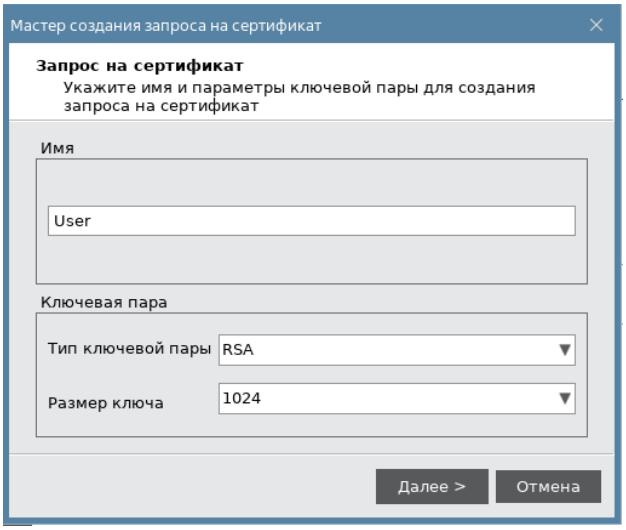


Рисунок 49 - Мастер создания запроса на сертификат. Ввод имени и параметров ключевой пары

5. Нажать кнопку "Далее". Будет открыто следующее окно мастера создания запроса на сертификат для ввода параметров сохранения файла создания запроса на сертификат (см. Рисунок 50). Заполнить следующие поля:

- в поле "Имя файла" указать путь сохранения файла запроса на сертификат. Для этого нажать кнопку "Обзор" и выбрать нужную папку. По умолчанию запрос на сертификат будет сохранен в файле с именем, совпадающем с именем сертификата, которое было ведено в предыдущем окне и с расширением "p10". Поле является обязательным для заполнения;
- в поле "Выберите формат запроса" выбрать формат файла запроса на сертификат: "Файлы X.509 в кодировке DER" либо "Файлы X.509 Base-64";
- установить отметку "Копировать в буфер обмена", если нужно скопировать запрос на сертификат в буфер обмена. Запрос копируется в одну строку без тегов.

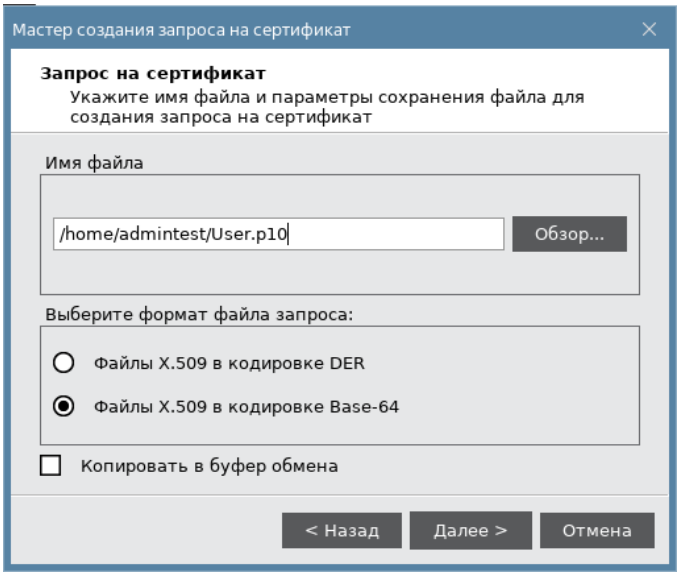


Рисунок 50 - Мастер создания запроса на сертификат. Ввод параметров файла запроса на сертификат

6. Нажать кнопку "Далее". Будет открыто следующее окно мастера создания запроса на сертификат для выбора опций использования для создания запроса на сертификат (см. Рисунок 51). Установить отметку в нужных полях:
   - Электронная подпись (выбрано по умолчанию);
   - Неотказуемость (выбрано по умолчанию);
   - Шифрование ключей (выбрано по умолчанию);
   - Шифрование данных (выбрано по умолчанию);
   - Согласование ключей;
   - Подписывание сертификата с помощью ключа;
   - Подписывание списка отзыва сертификатов;
   - Только шифрование;
   - Только расшифрование;

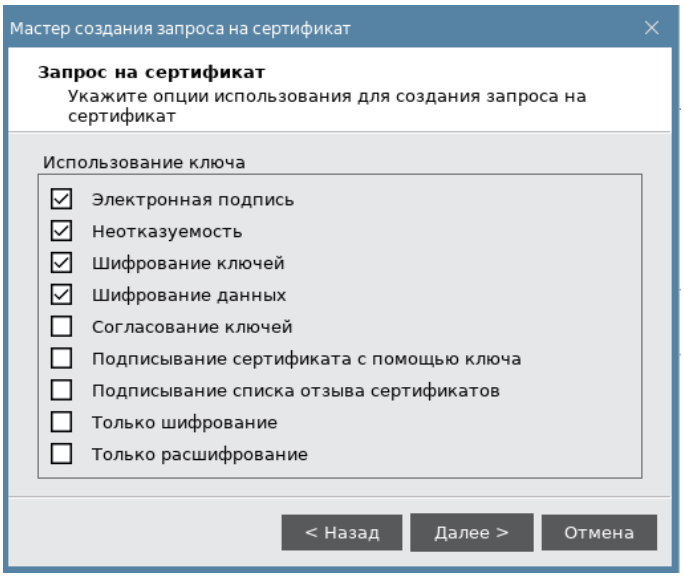


Рисунок 51 - Мастер создания запроса на сертификат. Опции использования ключа

7. Нажать кнопку "Далее". Будет открыто следующее окно мастера создания запроса на сертификат для указания опций предназначения для создания запроса на сертификат (см. Рисунок 52). Установить отметку в нужных полях:
   - Проверка подлинности клиента (выбрано по умолчанию);
   - Защищенная электронная почта (выбрано по умолчанию);
   - Проверка подлинности сервера;
   - Подпись кода;
   - Доверенное время.

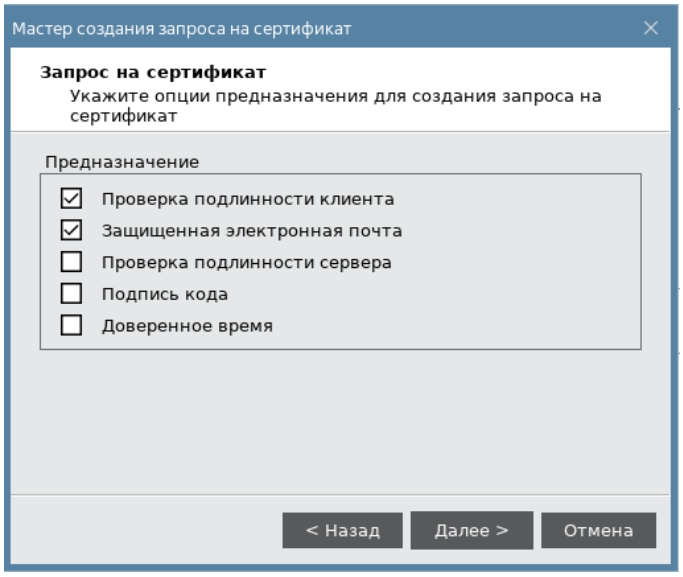


Рисунок 52 –Мастер создания запроса на сертификат. Опции предназначения

8. Нажать кнопку "Далее". Будет открыто следующее окно мастера создания запроса на сертификат для просмотра всех введенных параметров создаваемого запроса на сертификат. Для изменения параметров нажать кнопку "Назад", вернуться к нужному окну и отредактировать параметры (см. Рисунок 53);

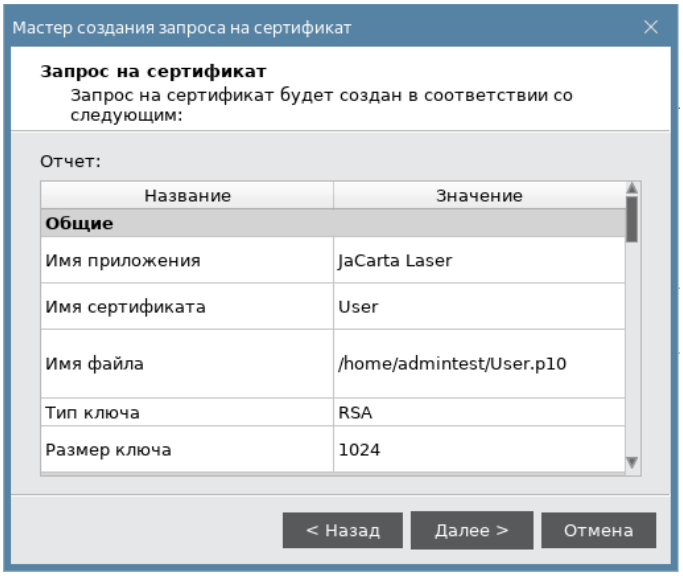


Рисунок 53 –Мастер создания запроса на сертификат. Параметры запроса на сертификат

9. Нажать кнопку "Далее". Будет выполняться создание запроса на сертификат. Ход выполнения операции и ее результат будет отображен в заключительном окне мастера создания запроса на сертификат. Файл запроса на сертификат будет сохранен по указанному пути (см. Рисунок 54);

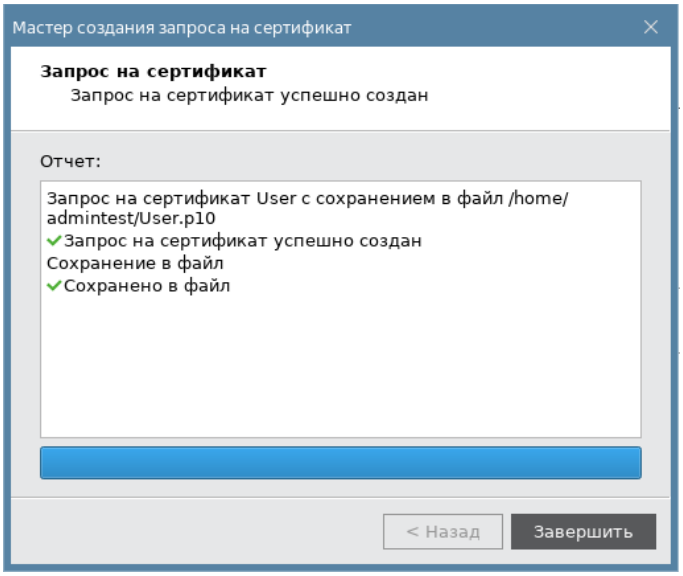


Рисунок 54 –Мастер создания запроса на сертификат. Результат создания запроса на сертификат

10. Нажать кнопку "Завершить" для выхода из мастера создания запроса на сертификат.

6.3.2 Импорт сертификата

Сертификат, устанавливаемый на электронном ключе, имеет срок действия. За 14 дней до окончания срока действия сертификата пользователь получит уведомление об истечении срока действия сертификата. Информационные сообщения будут приходить каждый день до окончания срока действия сертификата, пока он не будет заменен.

Для импорта сертификата необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Выбрать вкладку с наименованием приложения, в которое следует импортировать сертификат (в данном примере выбрано приложение PKI) и нажать кнопку "Ввести PIN-код" (см. Рисунок 55);

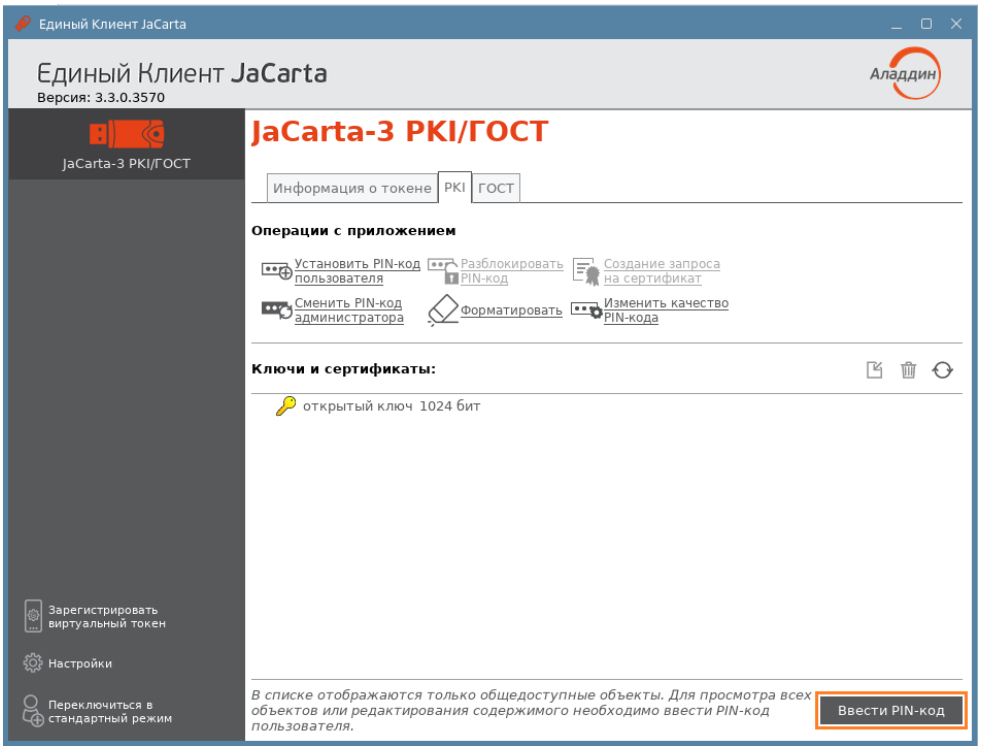


Рисунок 55 – Авторизация в приложении PKI

4. В появившемся окне с наименованием приложения ввести PIN-код пользователя данного приложения (см. Рисунок 56). Нажать кнопку "ОК";

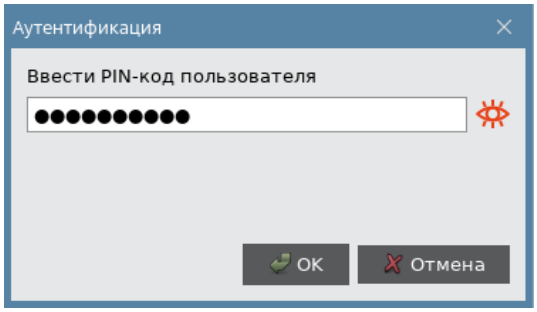


Рисунок 56 – Окно "Аутентификация"

5. В случае успешной авторизации в приложении в поле "Ключи и сертификаты" будет отображен полный список объектов данного приложения и станут доступны кнопки для выполнения операций над объектами (см. Рисунок 57);

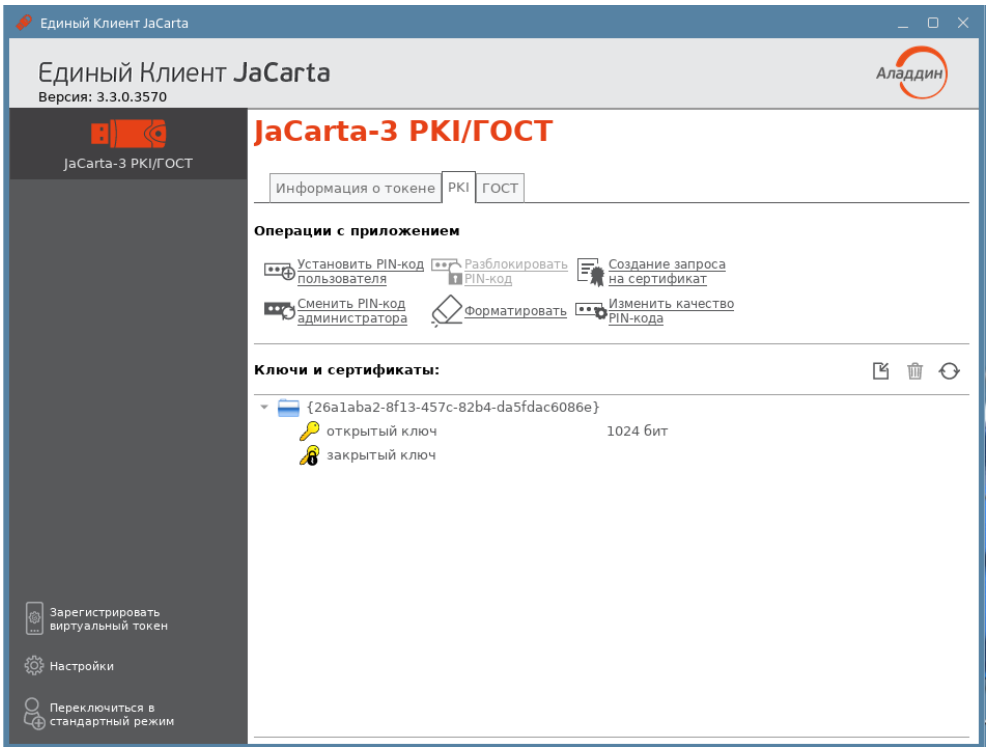


Рисунок 57 – Полный список объектов приложения и команда "Импорт"

6. Нажать кнопку  или вызвать контекстное меню в поле "Ключи и сертификаты "и выбрать команду "Импорт";
7. В окне "Мастер импорта сертификата" заполнить следующие поля (см. Рисунок 58):
   - в поле "Путь к файлу импортируемых данных" указать путь к импортируемому сертификату. Для этого нажать кнопку "Обзор" и в появившемся окне проводника выбрать файл сертификата;
   - в поле "Импортировать в контейнер" установить отметку, чтобы вручную задать имя контейнера, в который будет импортирован сертификат. В поле "Имя контейнера" ввести название контейнера. Если отметка не установлена, то имя контейнера будет сгенерировано автоматически;

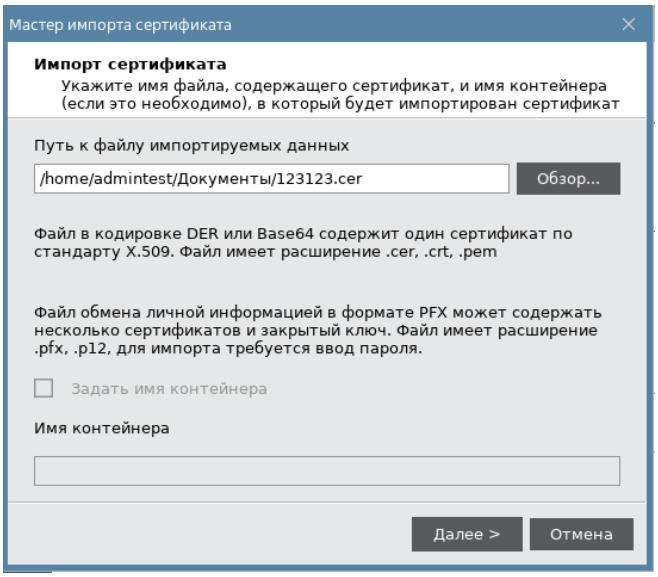


Рисунок 58 - Мастер импорта сертификата. Путь к импортируемым данным

8. Нажать кнопку "Далее". Будет отображено окно введенных настроек импорта. Для изменения параметров нажать кнопку "Назад", вернуться к нужному окну и отредактируйте параметры (см. Рисунок 59);

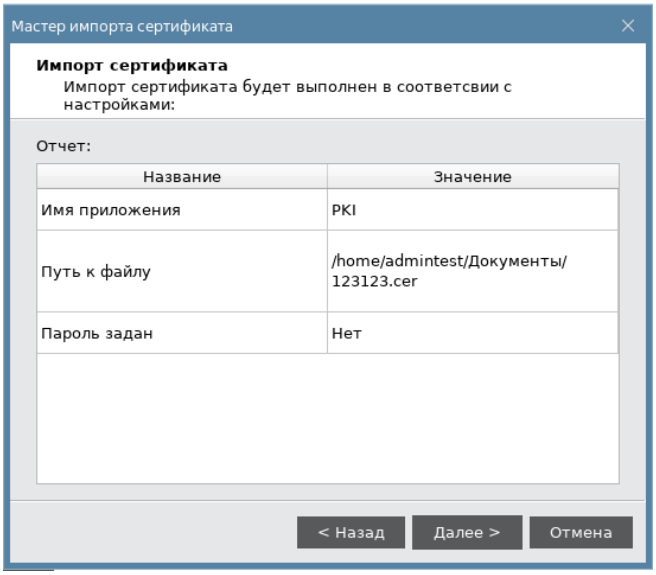


Рисунок 59 - Мастер импорта сертификата. Сообщение об успешном импорте сертификата

9. Нажать кнопку "Далее". Будет выполняться импорт объектов. Ход и результат выполнения операции будут отображены в завершающем окне мастера импорта сертификата (см. Рисунок 60);

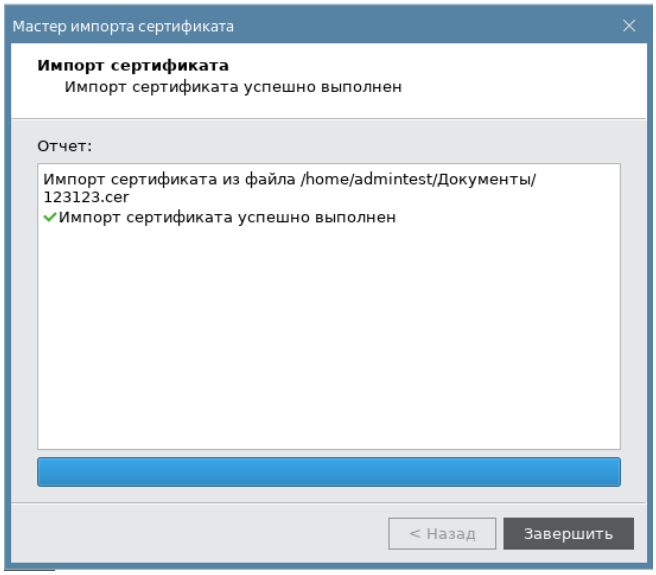


Рисунок 60 - Мастер импорта сертификата. Сообщение об успешном импорте сертификата

10. Нажать кнопку "Завершить" для завершения работы мастера импорта сертификата и закрытия окна. Импортированные объекты будут отображены в поле "Ключи и сертификаты" (см. Рисунок 61).

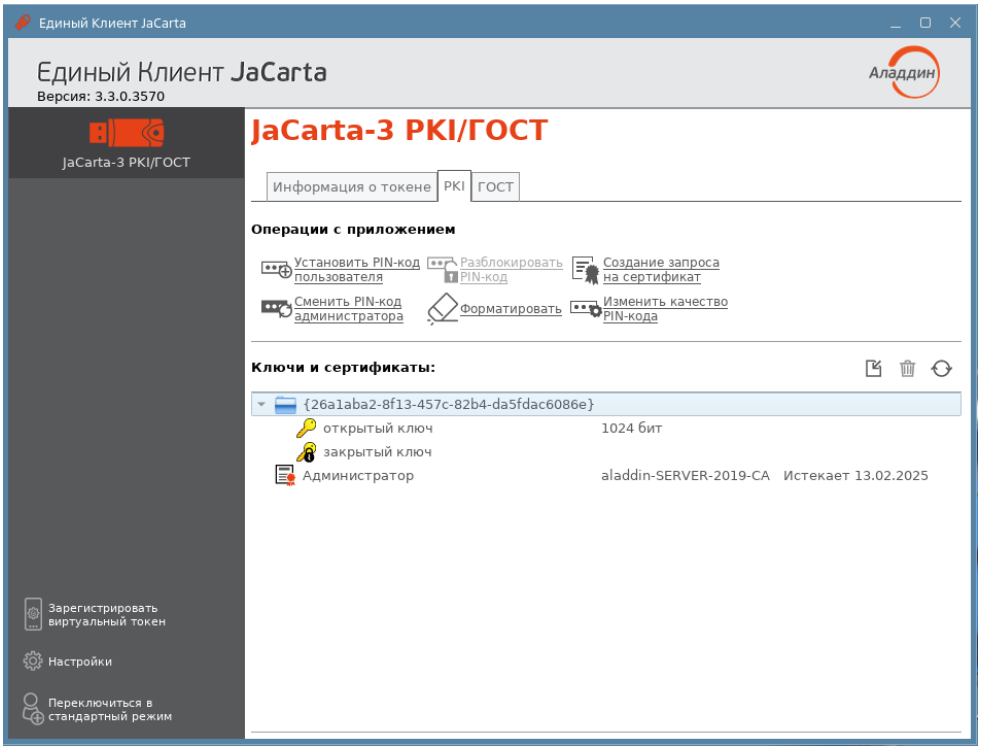


Рисунок 61 - Отображение импортированных объектов

6.3.3 Экспорт сертификата

Для экспорта сертификата необходимо:

1. Авторизоваться в приложении электронного ключа, из которого необходимо экспортировать сертификат (см. п.п. 1-3 процедуры импорта сертификата в п. 6.3.2). В поле "Ключи и сертификаты" выбрать экспортируемый объект и нажать кнопку  или активировать команду "Экспорт в файл" контекстного меню объекта (см. Рисунок 62);

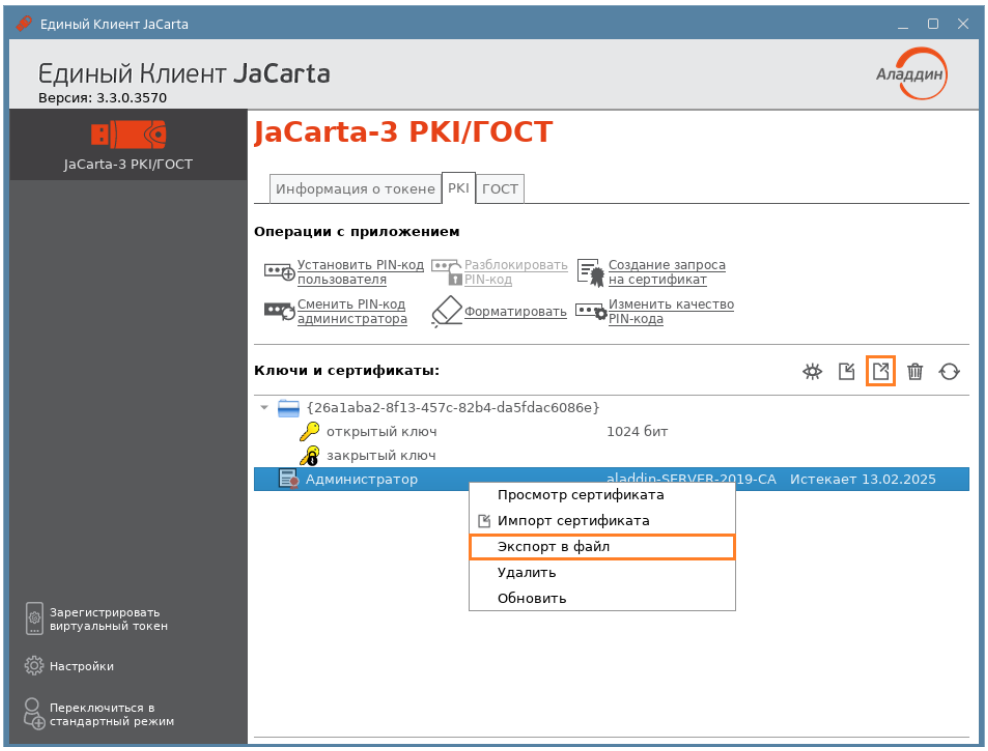


Рисунок 62 - ПО "Единый Клиент JaCarta". Кнопки перехода к экспорту данных

2. В окне "Мастер экспорта сертификата" заполнить следующие поля (см. Рисунок 63):
   - в поле "Путь к файлу для экспорта" указать путь для экспорта файла. Для этого нажать кнопку "Обзор" и в появившемся окне проводника выбрать нужную папку;
   - выбрать тип экспортируемого файла – "Файл в формате DER" или "Файл в формате Base64";

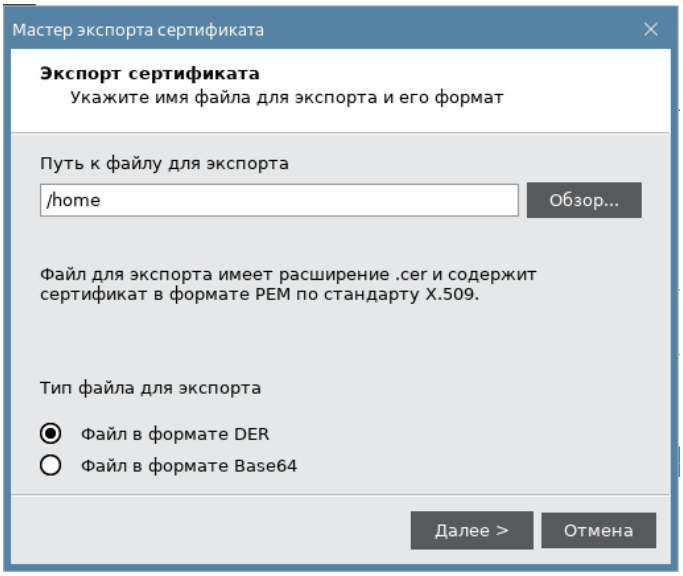


Рисунок 63 - Мастер экспорта сертификата. Ввод параметров экспортируемого файла

3. Нажать кнопку "Далее". Будет открыто следующее окно мастера экспорта сертификата для просмотра всех введенных параметров. Для изменения параметров нажать кнопку "Назад", вернуться к нужному окну и отредактировать параметры (см. Рисунок 64);

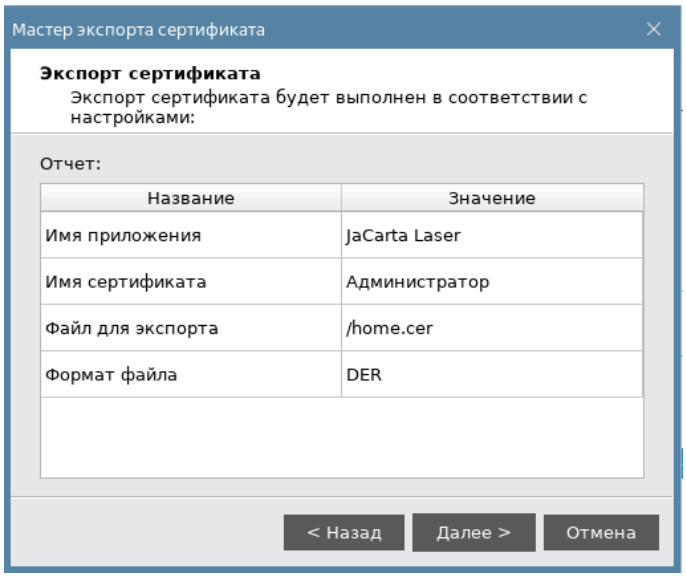


Рисунок 64 - Мастер экспорта сертификата. Результат экспорта

4. Нажать кнопку "Далее". Будет выполняться экспорт выбранного объекта. Ход и результат выполнения операции будут отображены в завершающем окне мастера экспорта сертификата (см. Рисунок 65).

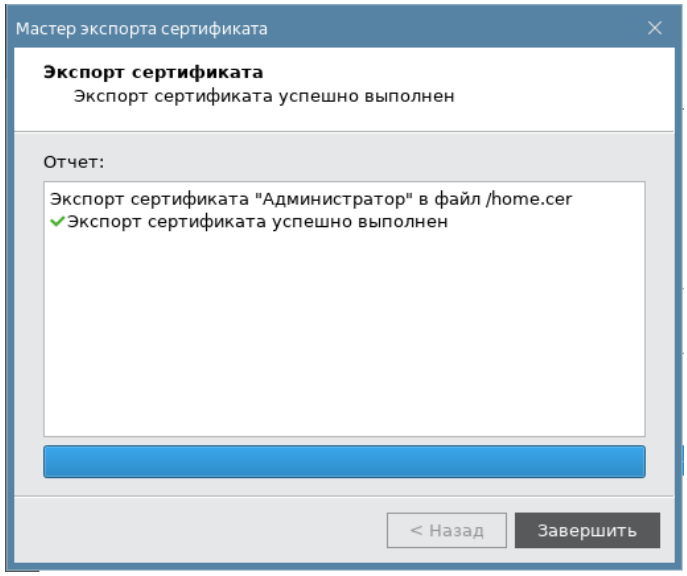


Рисунок 65 - Мастер экспорта сертификата. Результат экспорта

5. Нажать кнопку "Завершить" для выхода из мастера экспорта сертификата.

6.3.4 Просмотр сертификата

Для просмотра сертификата необходимо:

1. Авторизоваться в приложении электронного ключа, из которого необходимо экспортировать сертификат (см. п.п. 1-3 процедуры импорта сертификата в п. 6.3.2). В поле "Ключи и сертификаты" выбрать объект и нажать кнопку или активировать команду "Просмотр сертификата" контекстного меню объекта (см. Рисунок 66);

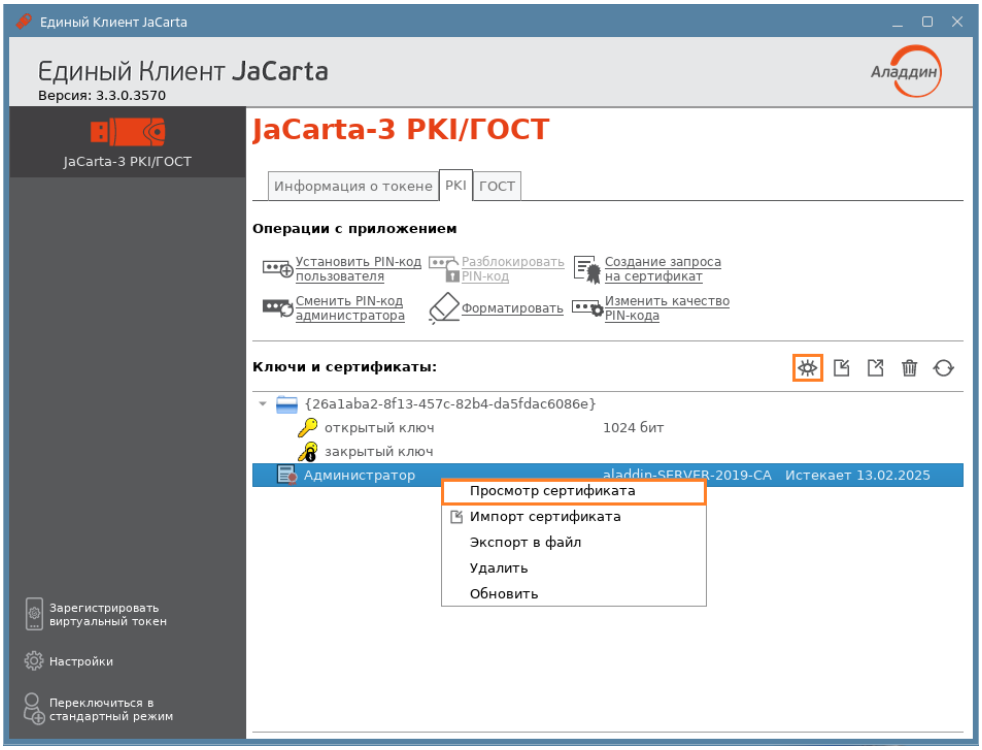


Рисунок 66 - Кнопки перехода к просмотру сертификата

2. Будет открыто окно, содержащее сведения о выбранном сертификате (см. Рисунок 67);

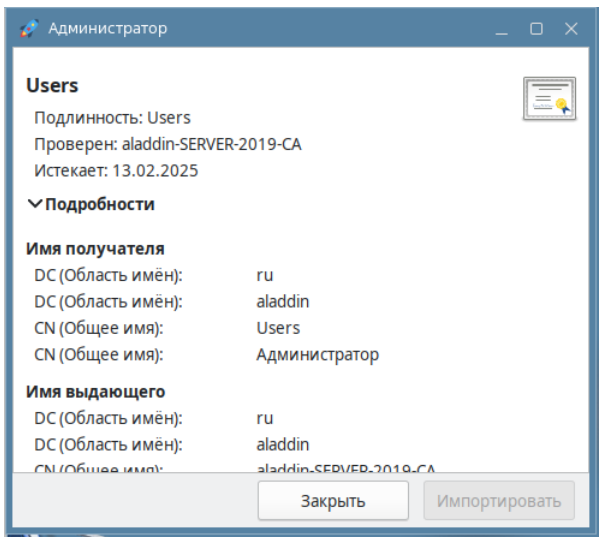


Рисунок 67 – Окно просмотра сертификата

3. Для выхода из окна просмотра нажать кнопку "Закрыть".

6.4 Операции с объектами в приложении электронного ключа

Для выполнения операций с объектами, хранящимися в памяти электронного ключа, требуется авторизация на электронном ключе с предъявлением PIN-кода пользователя.

Операции с объектами в памяти электронных ключей рекомендуется выполнять по указанию администратора.

В данном разделе операции с объектами описаны на примере сертификатов в приложении PKI.

6.4.1 Просмотр списка объектов

Для просмотра списка объектов:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Выбрать вкладку с наименованием нужного приложения. В поле "Ключи и сертификаты" будет отображен список общедоступных объектов, хранящихся в памяти электронного ключа (см. Рисунок 68);

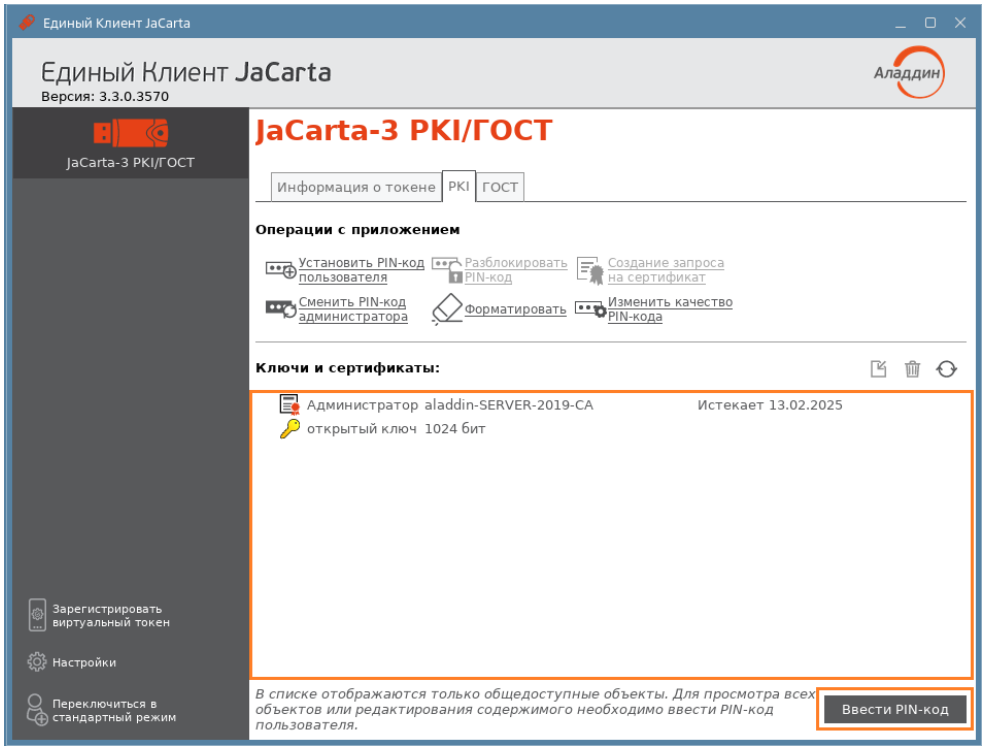


Рисунок 68 - Список общедоступных объектов в памяти электронного ключа

4. Нажать кнопку "Ввести PIN-код", в появившемся окне "Авторизация" ввести PIN-код пользователя для выбранного приложения (см. Рисунок 69);

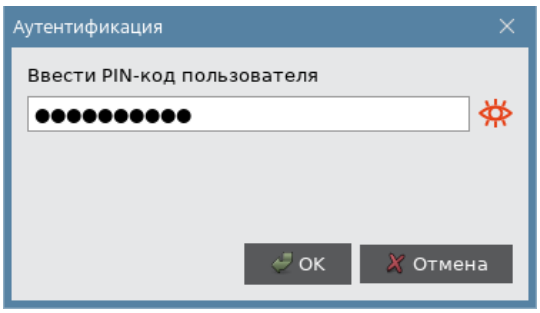


Рисунок 69 – Окно аутентификации в приложении электронного ключа

5. После успешной авторизации будет доступен для просмотра полный список объектов, а также появятся кнопки для управления объектами (см. Рисунок 70).

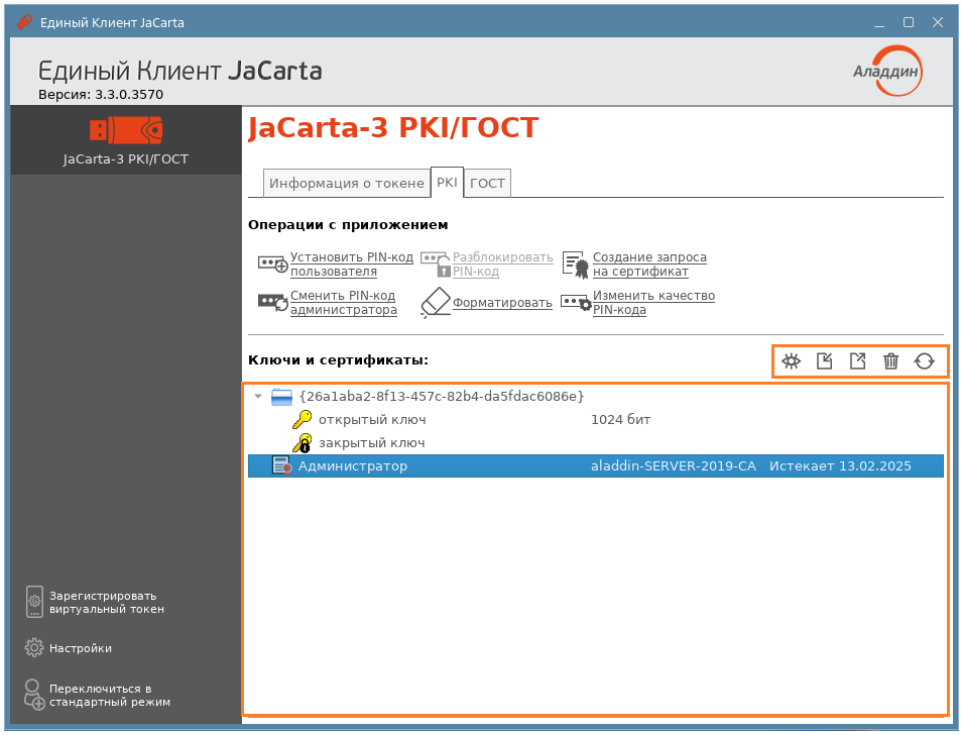


Рисунок 70 – Полный список объектов в памяти электронного ключа

6.4.2 Удаление объектов

Для удаления объекта необходимо:

1. Авторизоваться в приложении электронного ключа, из которого необходимо удалить объект. В поле "Ключи и сертификаты" выбрать удаляемый объект и нажать кнопку или активировать команду "Удалить" контекстного меню объекта (см. Рисунок 71);

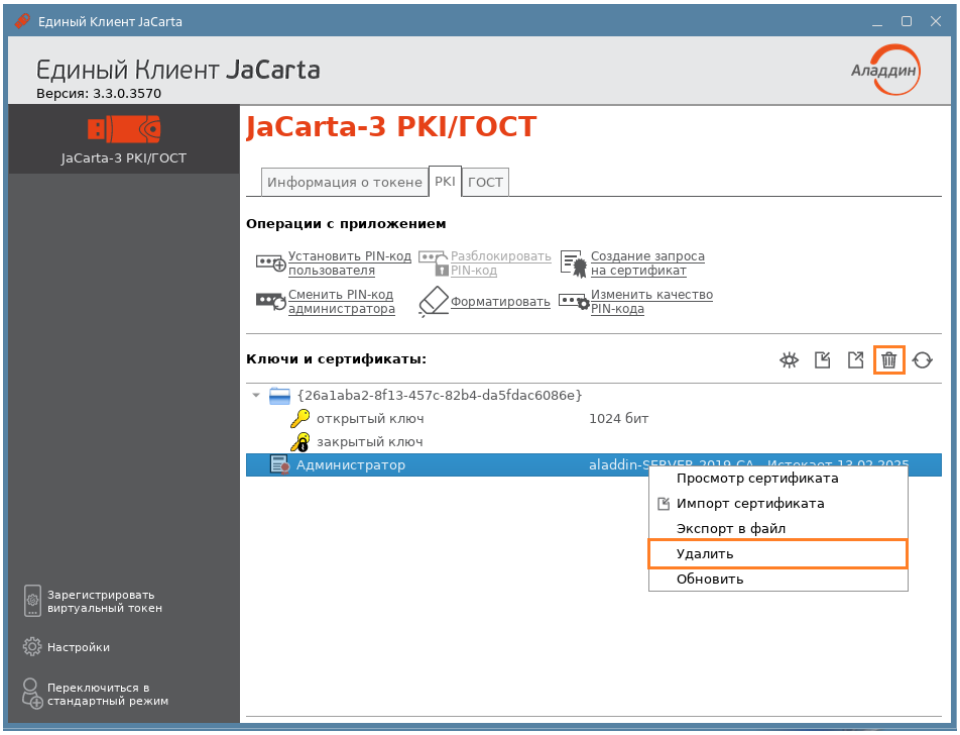


Рисунок 71 - Кнопки удаления данных

2. Будет открыто окно для подтверждения удаления (см. Рисунок 72);

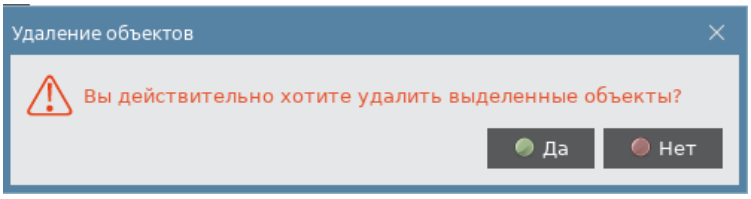


Рисунок 72 - Окно "Удаление объектов"

3. Нажать кнопку "Да" для подтверждения. Выбранный объект будет удален из памяти электронного ключа.

7. JaCarta WebPass: описание, работа и основные методы использования

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.

Внешний вид электронного ключа JaCarta WebPass приведен на рисунке (см. Рисунок 73).

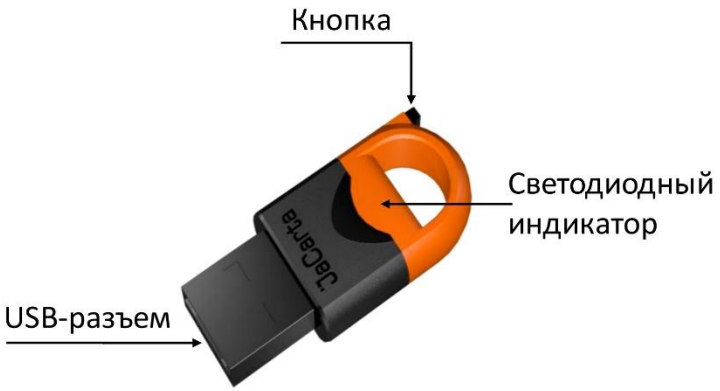


Рисунок 73 - Внешний вид электронного ключа JaCarta WebPass

Корпус электронного ключа JaCarta WebPass выполнен в форм-факторе с разъёмом USB Type A Male и состоит из двух частей разных цветов.

Внутри корпуса электронного ключа расположен светодиодный индикатор, отражающий различные режимы работы (см. Рисунок 73).

На корпусе электронного ключа расположена кнопка, используемая либо для генерации пароля, либо для запуска браузера. Поддерживается три варианта нажатий:

- одинарное нажатие (кратковременное нажатие не более 1 секунды) – используется для получения данных из слота №1;
- двойное нажатие (аналогично двойному щелчку мыши) – используется для получения данных из слота №2;
- длительное нажатие (нажатие и удержание в нажатом состоянии в течение 2-3 секунд) – используется для получения данных из слота №3.

Для того, чтобы пользоваться электронным ключом JaCarta WebPass необходимо знать какой тип слота имеет каждый из трех слотов и какой способ нажатия используется для каждого номера слота. Таким образом, необходимо знать соответствие: **№слота – Тип слота – Способ нажатия**.

Слот – набор данных и параметров, хранящихся на электронном ключе и необходимых для генерации пароля или перехода по адресу Web-ресурса (в зависимости от типа слота).

В каждом из слотов может храниться один из следующих видов информации:

- одноразовый пароль, генерируемый по заданному при инициализации алгоритму (тип слота «Одноразовый пароль»);
- многоразовый пароль, генерируемый в соответствии с заданными при инициализации критериями качества (тип слота «Пароль»);
- URL-адрес защищённого ресурса (тип слота «Интернет-адрес url»).

Слоты полностью независимы: инициализируются (конфигурируются), управляются и используются независимо друг от друга.

Количество активных слотов и конфигурация каждого из них задаётся при инициализации слотов.

Инициализация – установка основных параметров работы электронного ключа (подготовка к работе).

> *В процессе инициализации слота предыдущие значения параметров слота (если они ранее были записаны в слот)* ***УДАЛЯЮТСЯ****!*

PIN-код по умолчанию (заводские настройки): **1234567890**

> *Инициализация слота невозможна, если значение* ***PIN-кода по умолчанию*** *не было изменено на другое значение!*

PIN-код, отличный от PIN-кода по умолчанию, может быть установлен при производстве, либо пользователем в процессе эксплуатации электронного ключа. При смене PIN-кода необходимо указать текущий PIN-код и новый PIN-код.

В электронных ключах JaCarta WebPass для хранения информации используются три независимых слота. При использовании утилиты JaCarta WebPass Tool для защиты слотов от несанкционированной записи и удаления хранящихся в них данных используется PIN-код, общий (одинаковый) для всех трех слотов.

PIN-код используется при выполнении следующих операций:

- смена PIN-кода;
- инициализация слота (запись в слот одноразового или многоразового пароля либо URL-адреса защищенного ресурса);
- очистка слота.

7.1 Начало работы

Для начала работы необходимо подключить электронный ключ JaCarta WebPass или JaCarta U2F/WebPass к USB-порту.

При первом подключении электронного ключа JC-WebPass к компьютеру будет выполнен поиск и установка драйверов, необходимых для работы с электронным ключом. Все драйверы будут установлены автоматически без подключения к сайту Microsoft Windows Update. Действие будет произведено один раз и при последующих подключениях этого электронного ключа JaCarta WebPass к компьютеру повторяться не будет. При подключении к данному компьютеру другого электронного ключа той же модели диалог будет отображен повторно.

Окно Единого Клиента JaCarta с подключенным электронным ключом JaCarta WebPass будет выглядеть, как на рисунке (см. Рисунок 74).

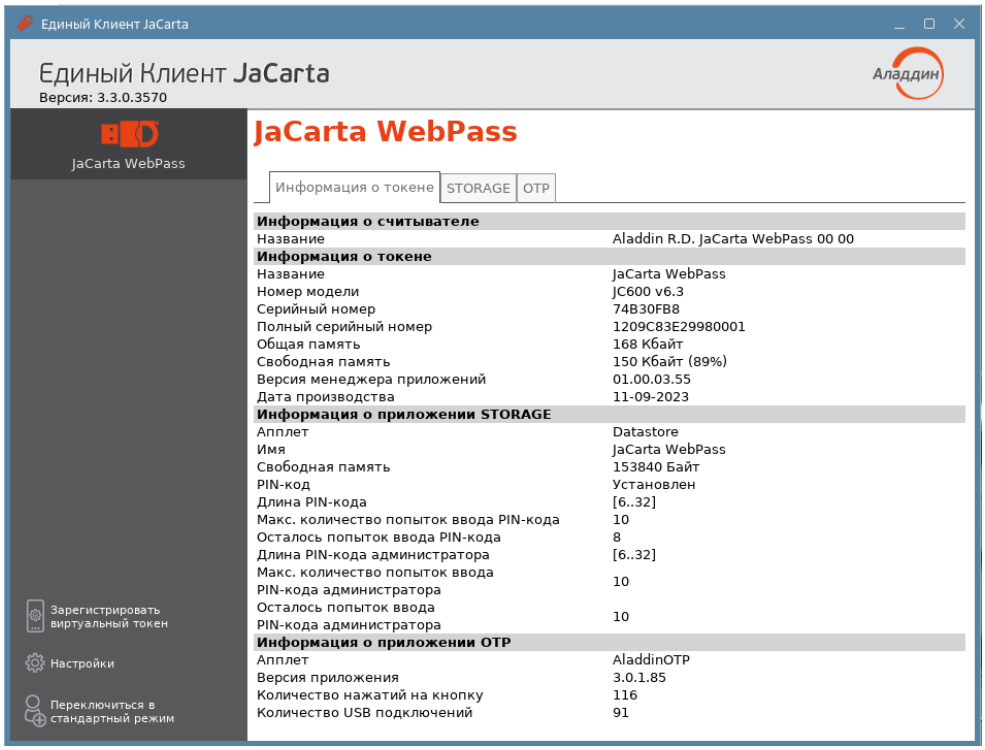


Рисунок 74 – Единый Клиента JaCarta с подключенным электронным ключом JaCarta WebPass

На вкладках в главном окне Единого Клиента JaCarta отображается следующая информация:

- "Информация о токене" - предназначена для просмотра подробных сведений о подсоединенном электронном ключе (модель ключа, установленные приложения, объем памяти, апплеты, записанные на электронный ключ и др.). Вкладка является активной по умолчанию;
- "STORAGE" – предоставляет возможность для выполнения операций с ключами и сертификатами, хранящимися в памяти электронного ключа;
- "OTP" – предоставляет доступ к операциям смены PIN-кода электронного ключа, операциям управления слотами: записи в них одноразового или многоразового пароля, записи URL-адреса защищенного ресурса, а также очистки слотов.

7.2 Сценарий использования

7.2.1 Смена PIN-кода

Смена PIN-кода электронного ключа может быть выполнена в любой момент работы с электронным ключом. Количество изменений PIN-кода не ограничено.

Кроме того, необходимо изменить PIN-код, заданный по умолчанию, перед началом использования электронного ключа.

Для смены PIN-кода электронного ключа необходимо:

1. Подключить электронный ключ к USB-порту. В основном окне утилиты перейти к вкладке "OTP" и нажать кнопку "Сменить PIN-код". Будет отображено одноименное окно (см. Рисунок 75);

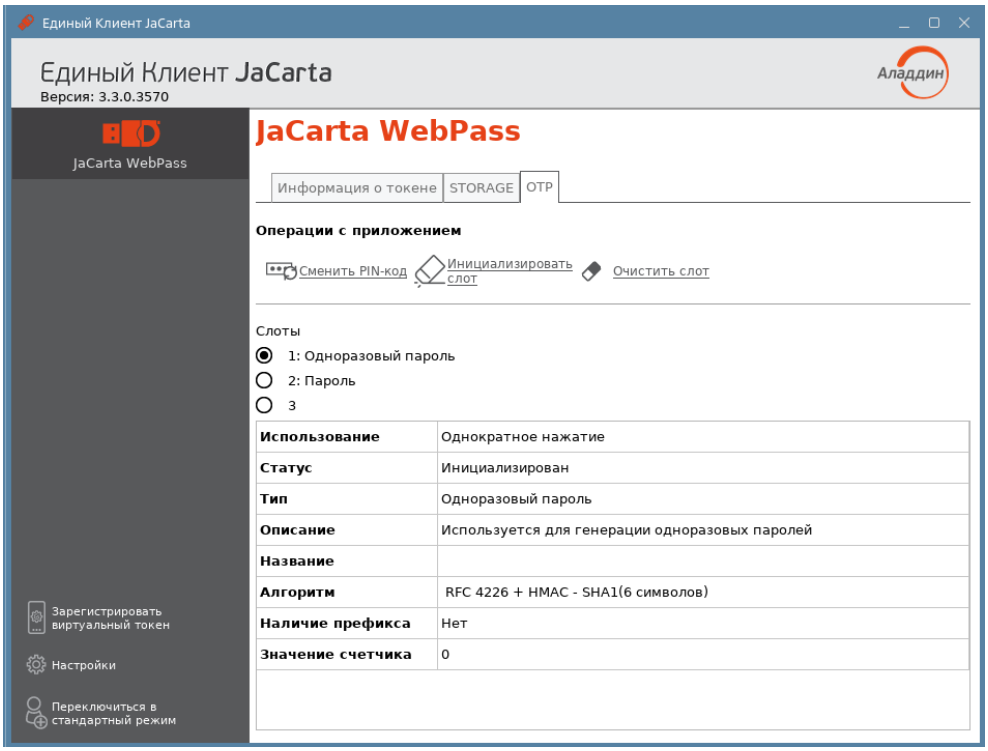


Рисунок 75 - Вызов окна "Смена PIN-кода"

2. Будет отображено одноименное окно (см. Рисунок 76);

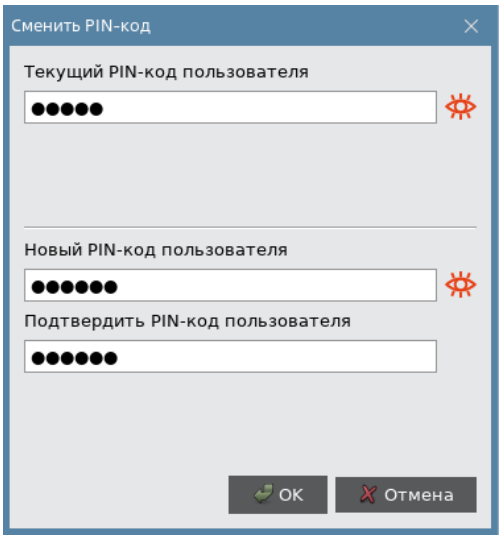


Рисунок 76 - Окно "Сменить PIN-код"

3. В окне "Сменить PIN-код" ввести текущий PIN-код, после ввести новый PIN-код и подтвердить его, затем нажать кнопку "OK". PIN-код электронного ключа будет изменен. На экране будет отображено окно с информацией об этом (см. Рисунок 77);

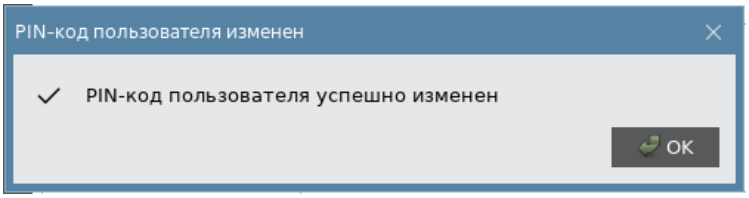


Рисунок 77 - Сообщение об успешной смене PIN-кода

4. Нажать кнопку "OK" для закрытия окна сообщения.

7.2.2 Управление слотами

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. 7.2.2.5) 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. пп. 7.2.2.2);
- многоразовый пароль, соответствующий указанным критериям качества (см. п. 7.2.2.3);
- URL-адрес защищенного ресурса (см. п. 7.2.2.4).

7.2.2.1 Просмотр информации о слотах

Для просмотра информации о слоте необходимо:

1. Подключить электронный ключ к USB-порту. В основном окне перейти к вкладке "OTP" и выбрать нужный слот. В нижней части окна будет отображена информация о параметрах инициализации и способе использования слота.

   На рисунке (см. Рисунок 78) приведен вид вкладки "OTP" по умолчанию (т.е. ни один из слотов не инициализирован) с выбранным слотом 1.

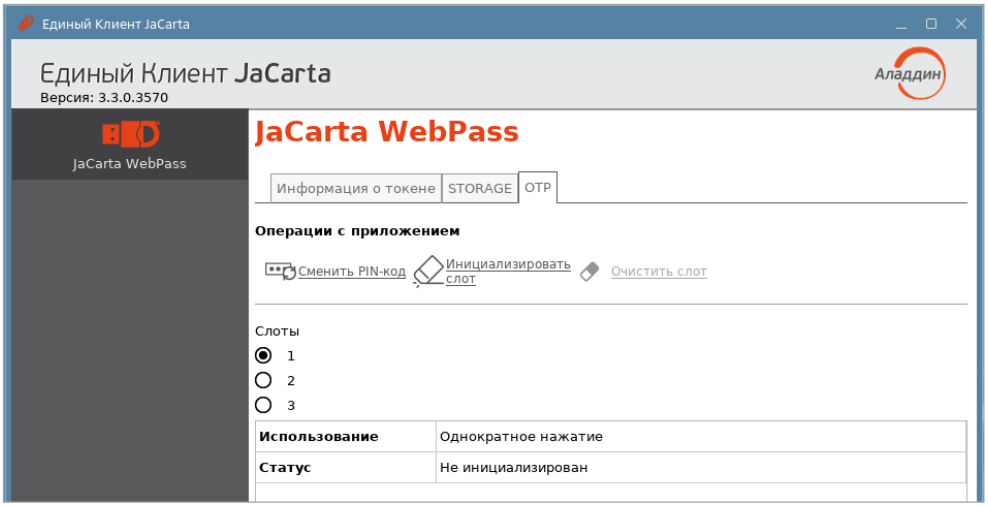


Рисунок 78 – Вкладка "OTP", просмотр информации о слоте 1 (ни один из слотов не инициализирован)

На рисунке (79) приведен вид вкладки "OTP" с инициализированными слотами 1, 2, 3 с выбранным слотом 3.

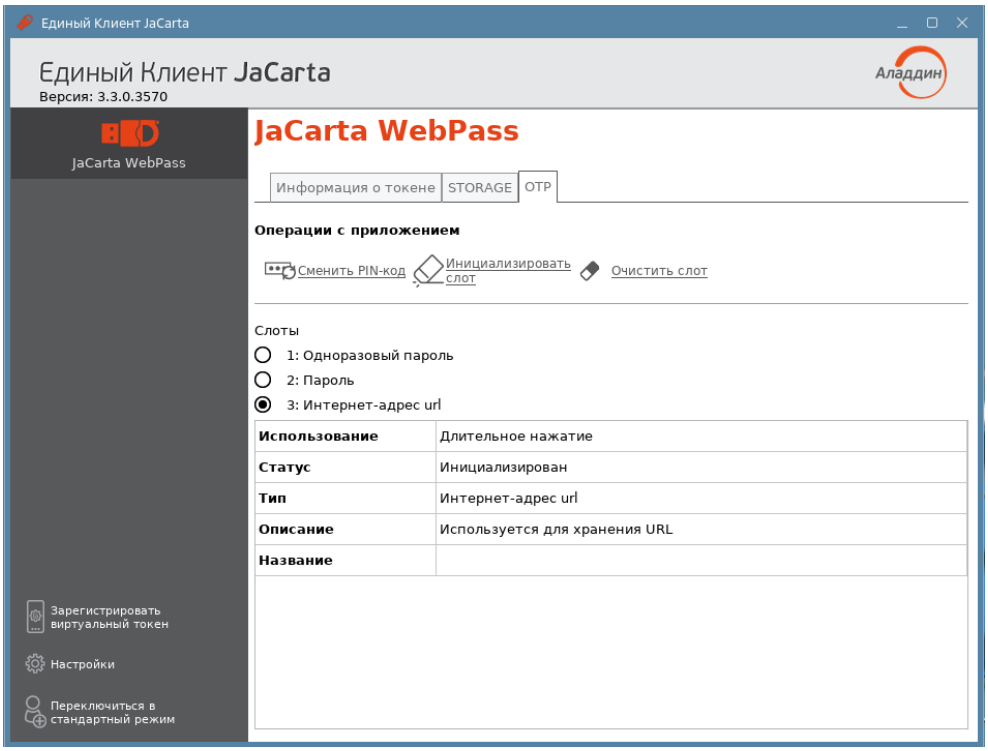
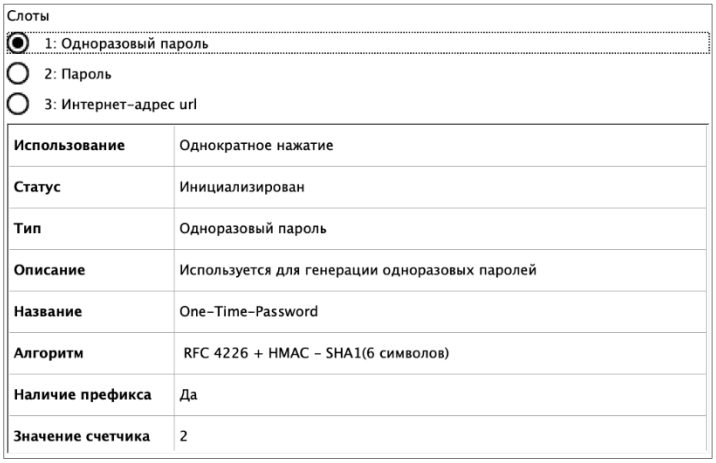
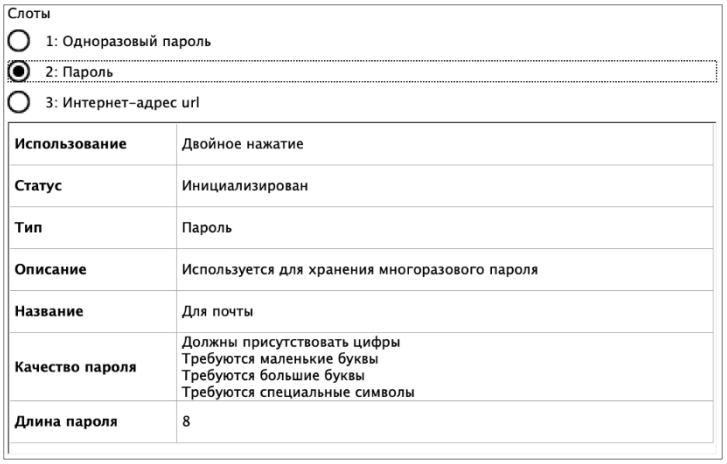


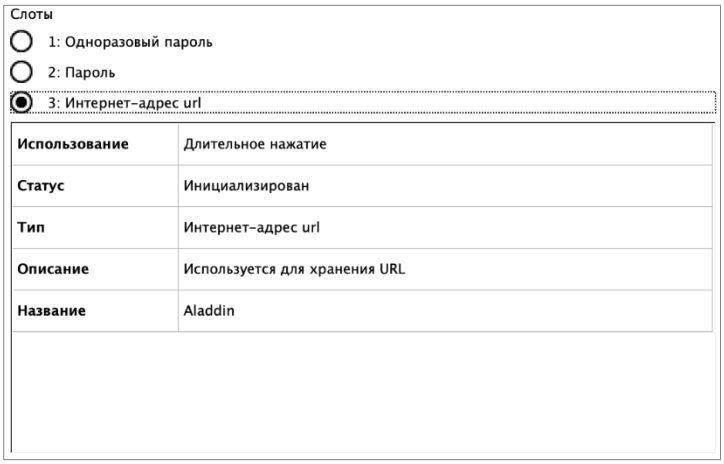
Рисунок 79 – Вкладка "OTP", просмотр информации о слоте 3 (все слоты инициализированы)

В таблице (см. Таблица 5) приведено описание полей, в которых отображается информация о слотах.

Таблица 5 – 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"

Элемент интерфейса	Описание
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
Поля для слота с типом "Пароль"	 Поле "Качество пароля" – содержит параметры качества пароля, заданные при инициализации слота: • длина пароля (количество символов от 4 до 160);

Элемент интерфейса	Описание
	• 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

7.2.2.2 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" необходимо:

1. На вкладке "OTP" выбрать тот слот, в который необходимо записать одноразовый пароль и нажать кнопку "Инициализировать слот";

   Примечание. *На рисунке (см. Рисунок 80) 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.*

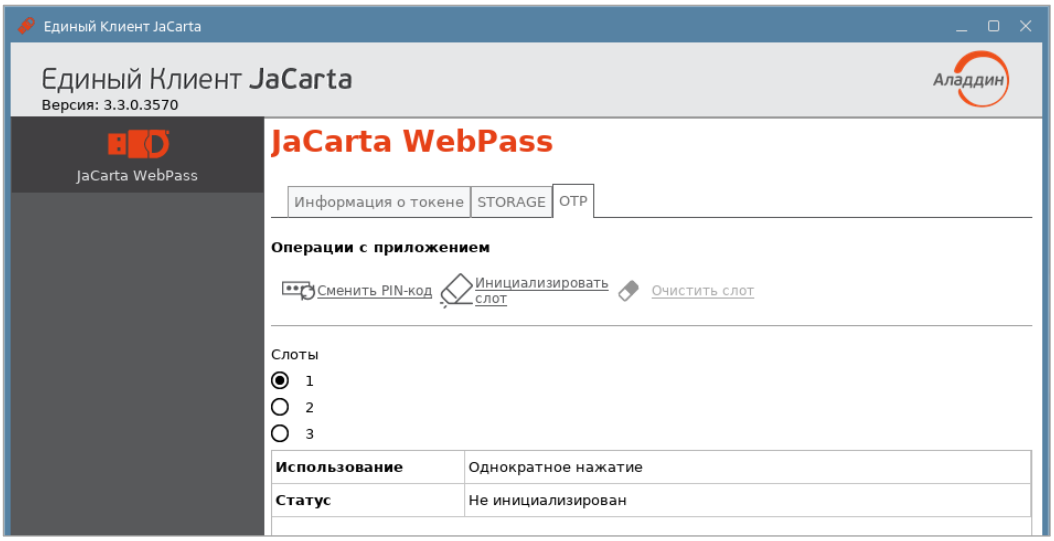


Рисунок 80 – Вкладка "OTP", выбора слота 1 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации". Заполнить поля мастера следующим образом (см. Рисунок 81):
   - в поле "Тип слота" выбрать в раскрывающемся списке значение "Одноразовый пароль";
   - в поле "Название слота" ввести название слота. Длина поля не должна превышать 32 символа;
   - в поле "Алгоритм" из раскрывающегося списка выбрать 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:
     - ввести нужное значение с клавиатуры (не более 32-х символов);
     - нажать кнопку S/N для автоматической вставки серийного номера электронного ключа в качестве префикса;
   - выбрать опцию "Автоматическая генерация вектора инициализации" или введите последовательность из 20 символов для RFC 4226 + HMAC-SHA-1 и 32 символа для RFC 4226 + HMAC-SHA-256 в поле "Вектор инициализации";
   - в поле "Значение счетчика" ввести значение счетчика генераций;
   - Выбрать опцию "Сохранить параметры инициализации", для сохранения введенных настроек инициализации для последующих инициализаций текущего слота.

   Нажать кнопку "Далее".

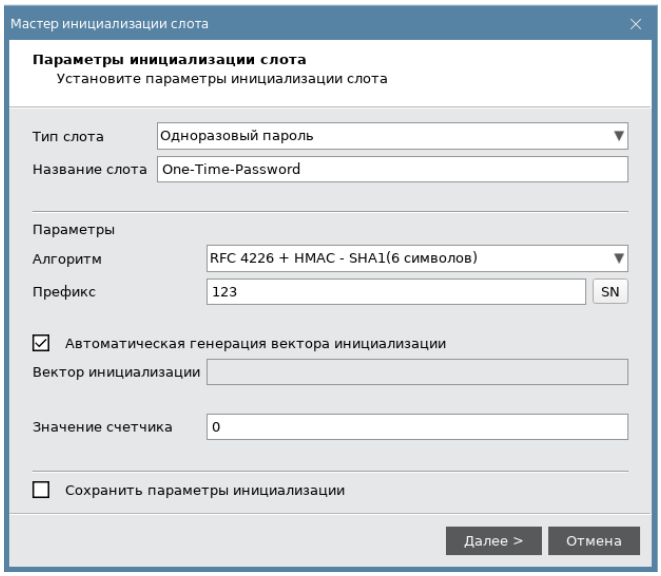


Рисунок 81 - Инициализация слота типом "Одноразовый пароль". Выбор параметров инициализации

3. В появившемся окне "Сохранение файла конфигурации" (см. Рисунок 82) при необходимости указать формат и имя файла, в который будут сохранены результаты инициализации слота:

Примечание. *Для регистрации электронного ключа JaCarta WebPass в системах SAM/JMS/JAS 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/JMS/JAS.*

– в поле "Выбрать формат файла" выбрать в раскрывающемся списке формат конфигурационного файла из предлагаемых значений: SAM/JMS, JAS;

– в поле "Имя файла" указать путь для сохранения конфигурационного файла. Для этого нажать кнопку "Обзор" и выбрать место сохранения конфигурационного файла. Если файл не существует и его требуется создать, то ввести его имя и нажать"Сохранить".

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

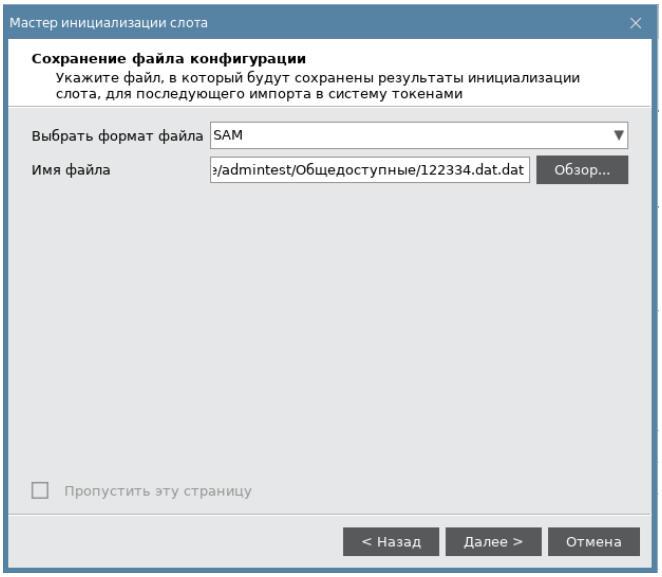


Рисунок 82 - Инициализация слота типом "Одноразовый пароль". Сохранение файла конфигурации

4. Далее ввести PIN-код электронного ключа в одноименное поле, после чего нажать кнопку "Далее" для запуска инициализации (см. Рисунок 83).

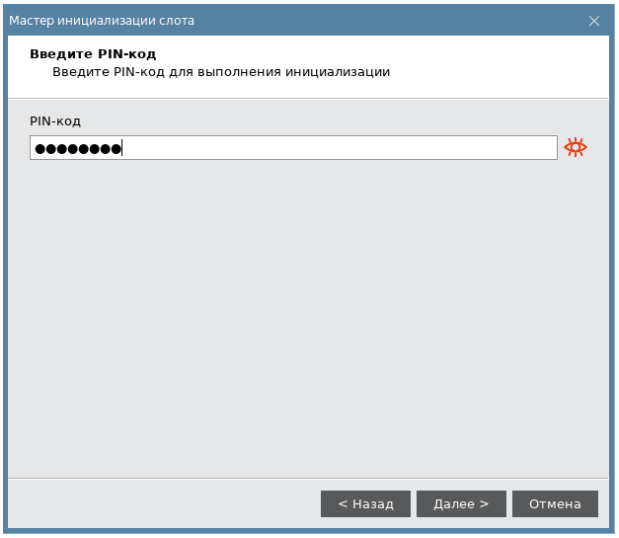


Рисунок 83 – Инициализация слота типом "Одноразовый пароль". Ввод PIN-кода

5. Далее будет отображаться настройки, установленные на предыдущих шагах, с которыми будет проходить процесс инициализации (см. Рисунок 84). Если все настройки указаны верно, нажать кнопку "Выполнить" для запуска инициализации.

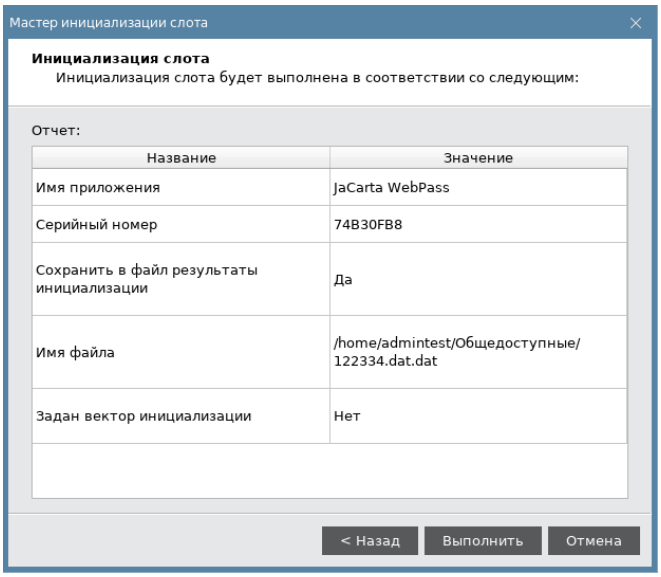


Рисунок 84 - Инициализация слота типом "Одноразовый пароль". Заданные настройки

6. В окне "Мастер инициализации слота" подтвердить инициализацию, нажав кнопку "Да" (см. Рисунок 85);

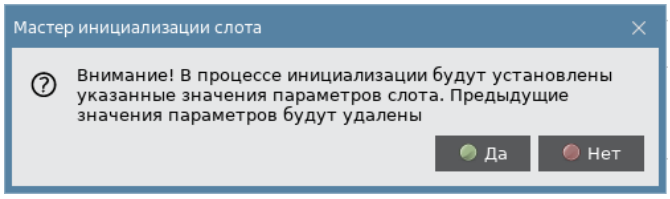


Рисунок 85 – Окно подтверждения заданных настроек

7. Будет отображен отчет по выполненной инициализации (см. Рисунок 86). Для закрытия окна нажать кнопку "Завершить";

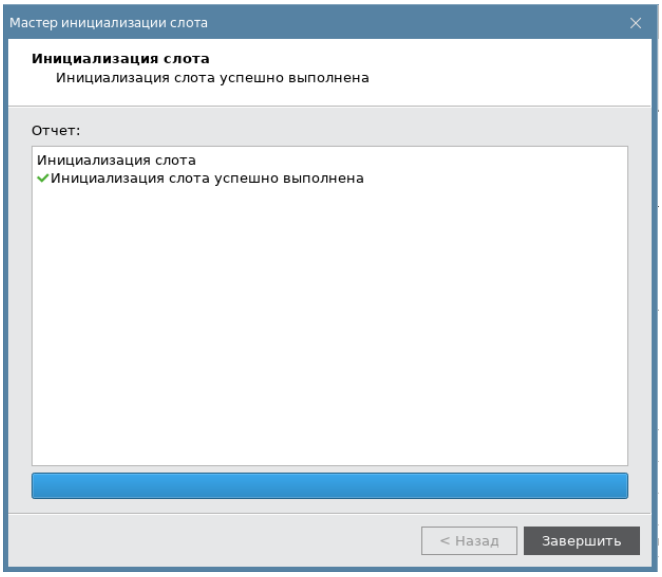


Рисунок 86 - Завершение инициализации слота

8. Окно Мастера инициализации слота будет закрыто. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Одноразовый пароль" (см. Рисунок 87).

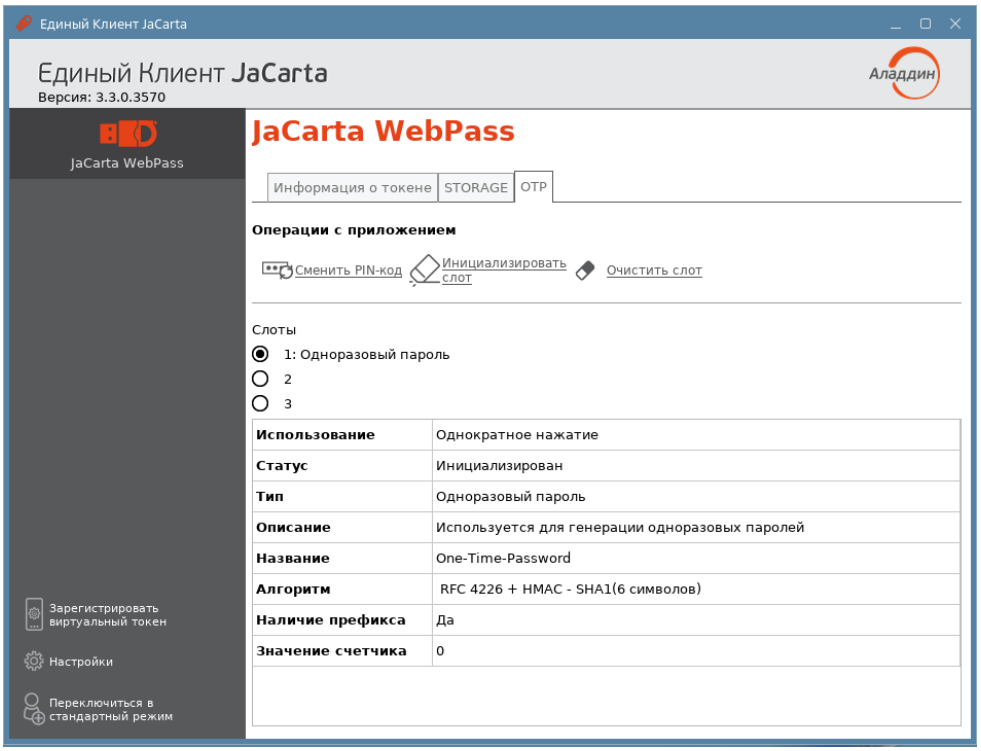


Рисунок 87 - Слот 1 инициализирован типом "Одноразовый пароль"

7.2.2.3 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" необходимо:

1. На вкладке "OTP" выбрать тот слот, в который необходимо записать многоразовый пароль и нажать кнопку "Инициализировать слот".

   Примечание. *На рисунке (см. Рисунок 88) 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.*

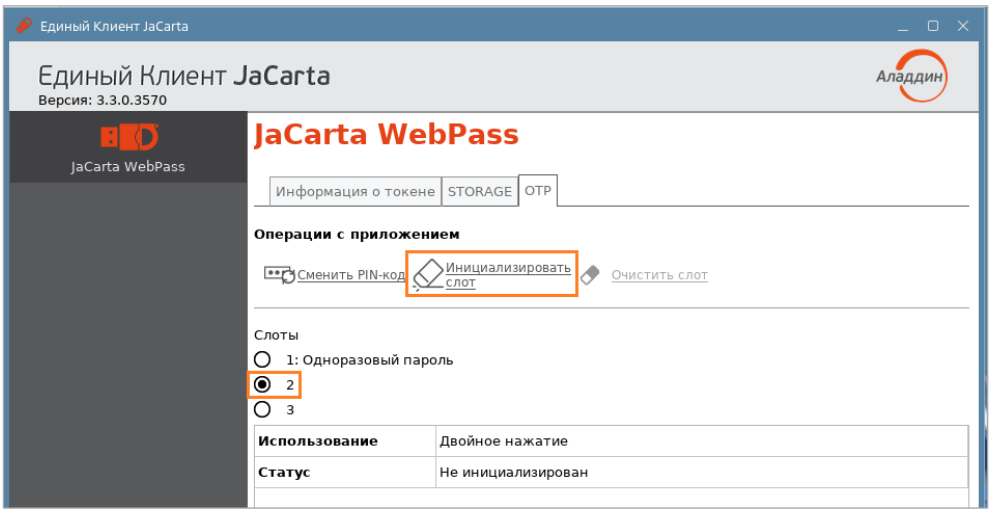


Рисунок 88 – Вкладка "OTP", выбора слота 2 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота". Заполнить поля мастера следующим образом (см. Рисунок 89):

   – в поле "Тип слота" выбрать значение "Пароль";

– в поле "Название слота" ввести название, например, "Для почты". Длина поля не должна превышать 32 символа;
– указать параметры качества, которым должен соответствовать многоразовый пароль:
  - в поле "Длина пароля" установить необходимую длину пароля (по умолчанию длина пароля составляет 4 символа);
  - выбрать опцию "Использовать маленькие буквы", если в состав пароля должны входить маленькие буквы;
  - выбрать опцию "Использовать большие буквы" если в состав пароля должны входить большие буквы;
  - выбрать опцию "Использовать цифры" если в состав пароля должны входить цифры;
  - выбрать опцию "Использовать специальные символы", если в состав пароля должны входить специальные символы;
  - выбрать опцию "Добавить код клавиши Enter к паролю при нажатии при необходимости.
– выбрать опцию "Сохранить параметры инициализации", если необходимо сохранить настройки инициализации для последующих инициализаций других слотов;

Нажать кнопку "Далее".

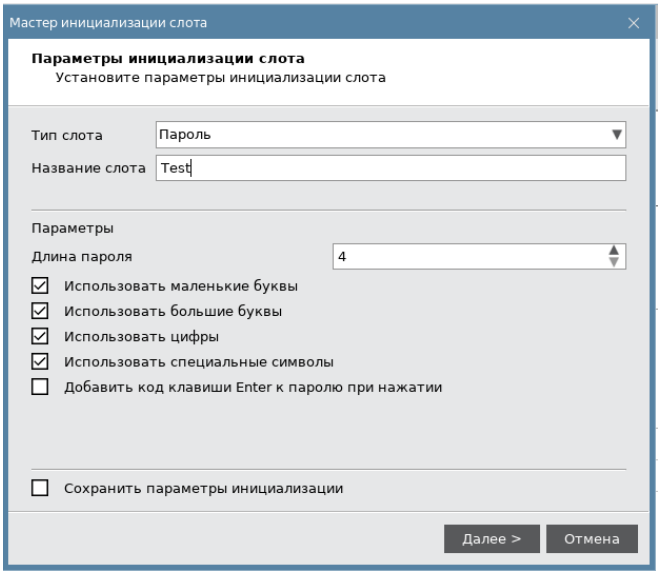


Рисунок 89 – Инициализация слота типом "Пароль". Выбор параметров инициализации

3. Далее прохождение Мастера аналогично шагам 4-6 п. 7.2.2.2.
4. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Пароль" (см. Рисунок 90).

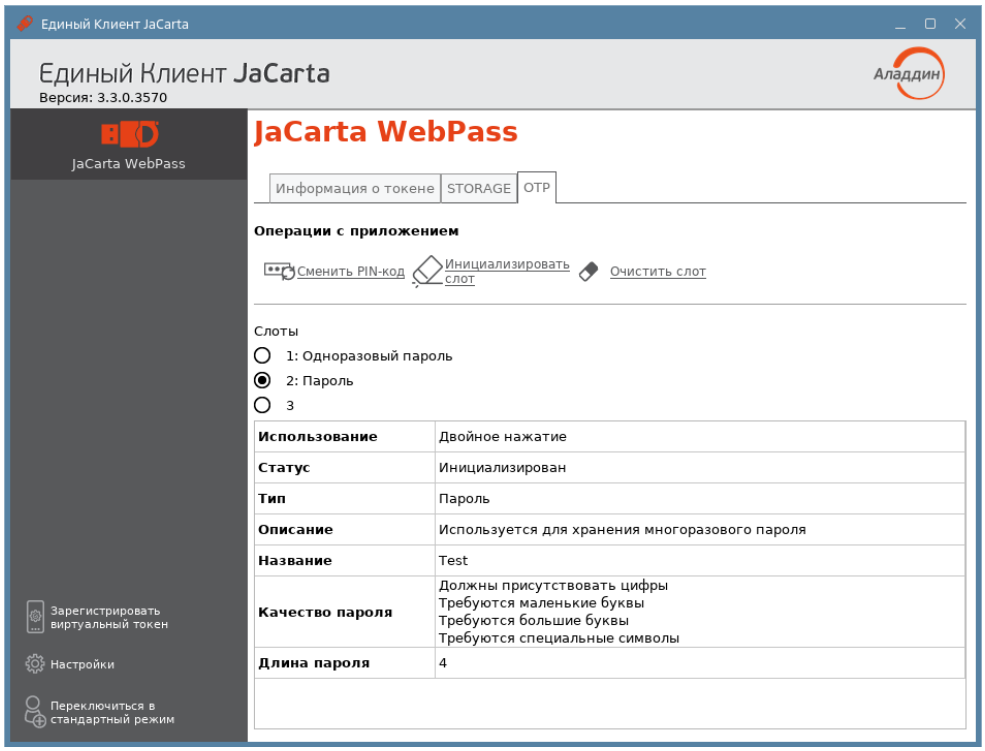


Рисунок 90 - Слот 2 инициализирован типом "Пароль"

7.2.2.4 Инициализация слота типом "Интернет адрес"

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

1. На вкладке "OTP" выбрать тот слот, в который необходимо записать адрес интернет-ресурса, на который будет осуществлен переход при нажатии на кнопку электронного ключа, и нажать кнопку "Инициализировать слот".

   Примечание. *На рисунке (см. Рисунок 91) 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.*

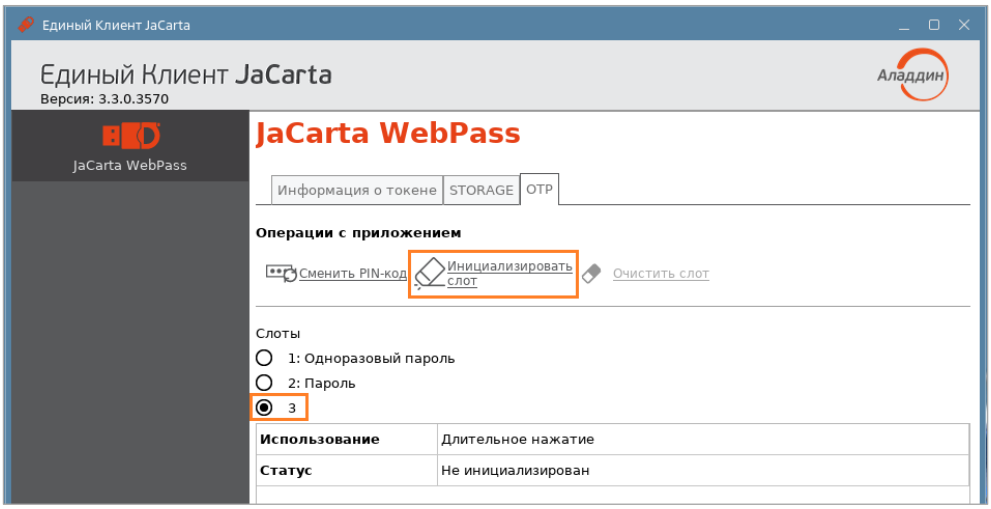


Рисунок 91 – Вкладка "OTP", выбора слота 3 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота". Заполнить поля мастера следующим образом (см. Рисунок 92):

   – в поле "Тип слота" выбрать значение "Интернет адрес url";

– в поле "Название слота" ввести название, например, "Aladdin". Длина поля не должна превышать 32 символа;
– в поле "Операционная система" выбрать тип операционной системы: Linux;
– в поле "Интернет адрес" ввести 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".*

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

Нажать кнопку "Далее".

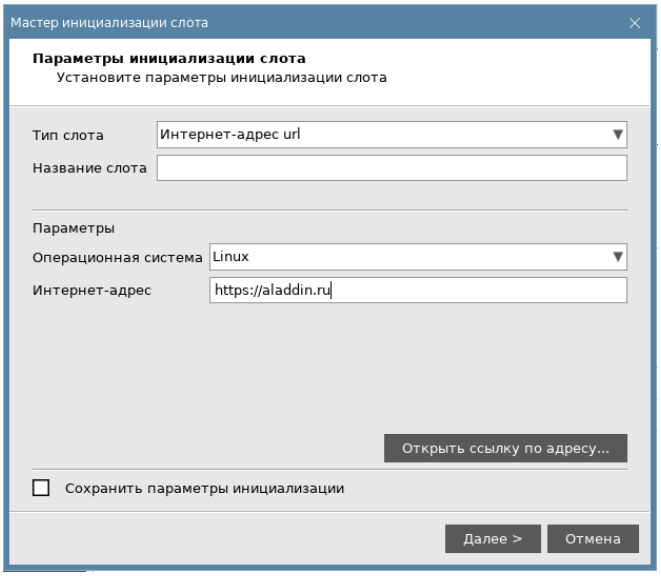


Рисунок 92 – Инициализация слота типом "Интернет-адрес"

3. Далее прохождение Мастера аналогично шагам 4-6 п. 7.2.2.2.
4. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Интернет-адрес url" (см. Рисунок 93).

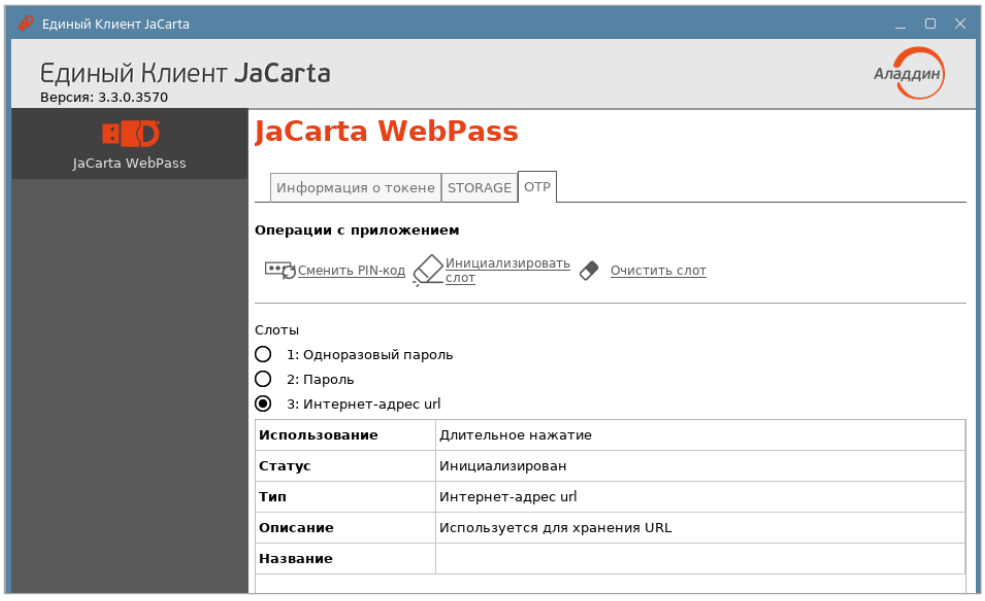


Рисунок 93 - Слот 3 инициализирован типом "Интернет-адрес url"

7.2.2.5 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.

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

Для очистки слота необходимо:

5. На вкладке "OTP" выбрать тот слот, который необходимо очистить. Нажать кнопку "Очистить слот" (см. Рисунок 94);

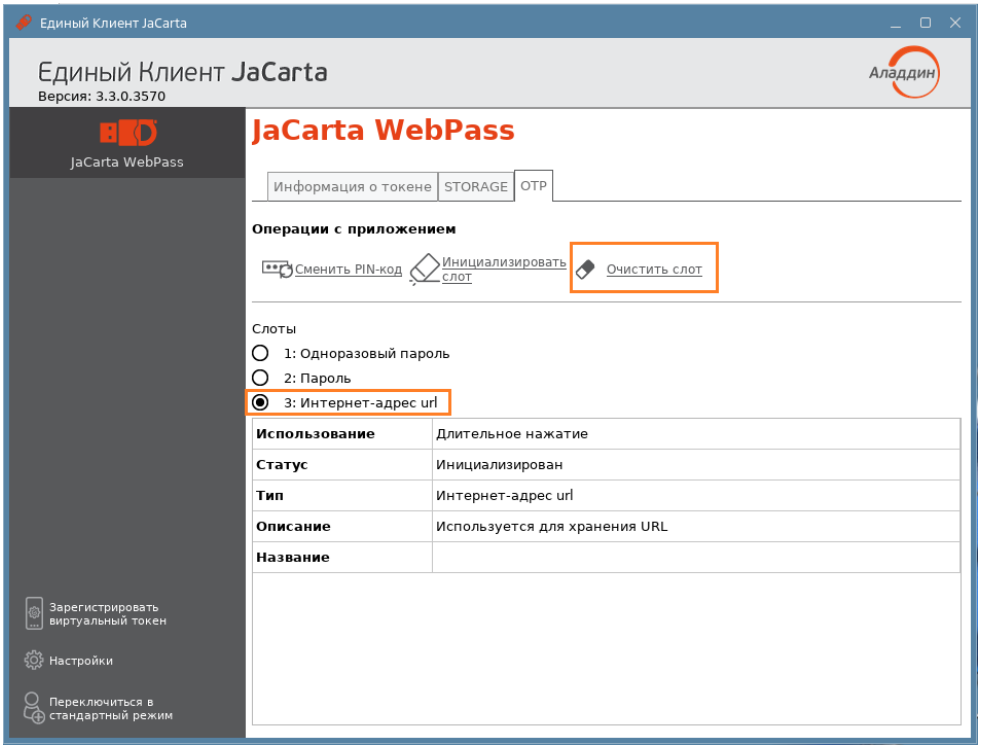


Рисунок 94 – Очистка слота

6. Будет открыто окно "Очистить слот" (см. Рисунок 95);
7. В поле "PIN-код" в окне "Очистить слот" ввести PIN-код электронного ключа и нажать кнопку "ОК";

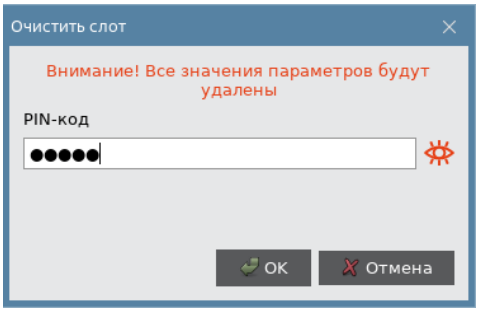


Рисунок 95 – Окно "Очистить слот"

8. Будет выполняться очистка слота. По ее завершении данные, хранящиеся в слоте, будут удалены. На экране будет отображена информация об этом (см. Рисунок 96).

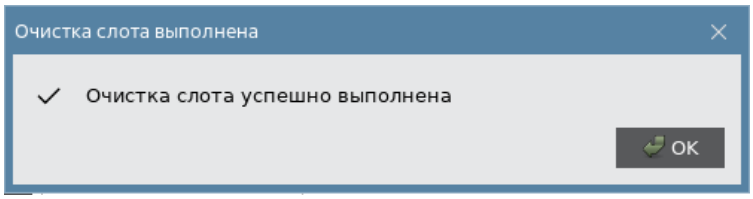


Рисунок 96 – Сообщение о завершении очистки слота

7.2.2.6 Блокирование слота

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

Приложение А. Обозначения электронных ключей

Обозначение	Описание
	MicroUSB-токен
	USB-токен JaCarta в корпусе nano
	USB-токен JaCarta в корпусе nano с кнопкой
	USB-токен JaCarta в корпусе mini
	USB-токен JaCarta в корпусе XL
	Смарт-карта
	Электронный ключ в форм-факторе Secure MicroSD
	USB-токен в металлическом корпусе
	Type C-токен в металлическом корпусе
	Тип электронного ключа не определён
	Электронный ключ находится на стадии определения

Контакты

Офис (общие вопросы)

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

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

E-mail: aladdin@aladdin.ru (общий)

Web: https://www.aladdin.ru

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

Техподдержка

Контакты службы техподдержки:

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

Коротко о компании

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

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

Основные направления

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

Лицензии

- Компания имеет все необходимые лицензии ФСТЭК России, ФСБ России для проектирования, производства и поддержки СЗИ и СКЗИ.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.

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

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