Единый Клиент JaCarta

Руководство пользователя для Windows

Обозначение документа	АЛДЕ.467669.015РЭ6
Статус	Публичный
Листов	74

Оглавление

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 для пользователей ПО Единый Клиент JaCarta, владельцев электронных ключей JaCarta и eToken.

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

Таблица 1 — Элементы оформления

Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ
Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
Гиперссылка	Используется для выделения внешних ссылок
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, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО "Аладдин Р.Д." без предварительного уведомления.

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

1.7 Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

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

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

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

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

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

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

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;

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

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

2. Основные понятия

2.1 Назначение

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. Версия для Microsoft Windows включает в себя компонент JaCarta SecurLogon.

2.2 Термины и определения

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

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

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

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

Апплет – программное обеспечение, реализующее функциональность приложения электронного ключа.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

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

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

3. Общие сведения об электронных ключах

3.1 Приложения, апплеты и модели электронных ключей

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

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

Примечание. *Наименование приложения не всегда содержится в названии модели электронного ключа. Например, в модели ключей JaCarta PKI установлено приложение PKI, но в модели JaCarta LT установлено приложение STORAGE. Название модели и приложения электронного ключа отображается в интерфейсе Единого Клиента JaCarta в стандартном режиме (см. п. 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. п. 6 "Работа в программе в расширенном режиме").*

Соответствие приложений, апплетов и моделей электронных ключей, работа с которыми поддерживается в Microsoft Windows, приведено в таблице 2.

Таблица 2 – Соответствие приложений, апплетов и моделей электронных ключей

Апплет или приложение	Модели электронных ключей
Приложение PKI, реализованное апплетом Laser	JaCarta Remote Access; JaCarta PKI; JaCarta PKI/Flash; JaCarta PKI/BIO; JaCarta PKI/WebPass; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 SE; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SF; Aladdin LiveOffice; Aladdin LiveOffice Common Edition Виртуальный токен

Апплет или приложение	Модели электронных ключей
Приложение PKI, реализованное апплетом PRO	JaCarta PRO; eToken PRO Anywhere; eToken NG-OTP (Java); JaCarta-2 PRO/ГОСТ
Приложение STORAGE, реализованное апплетом Datastore	JaCarta LT; JaCarta WebPass; JaCarta U2F
Приложение ГОСТ, реализованное апплетом Криптотокен 2 ЭП	JaCarta Remote Access; JaCarta SF/ГОСТ; JaCarta-2 ГОСТ; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 PRO/ГОСТ; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SE; JaCarta-2 SF; Aladdin LiveOffice; Aladdin LiveOffice Common Edition
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass; JaCarta U2F/WebPass; JaCarta PKI/WebPass

3.2 Параметры электронных ключей при поставке

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

Таблица 3 – Параметры электронных ключей при поставке

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

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

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

3.3 Информация о PIN-коде пользователя

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

PIN-кода пользователя сообщает администратор при передаче пользователю электронного ключа. Значение PIN-кода может отличаться от типового значения, перечень которых представлен в таблице 3.

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. п. 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-кода 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. Эта операции выполняются администратором, описание ее выполнения приведено в документе "Единый Клиент JaCarta. Руководство администратора для Windows".

4. Обзор пользовательского интерфейса

4.1 Запуск Единого Клиента JaCarta

Для запуска Единого Клиента JaCarta:

1. В меню "Пуск" активируйте команду "Аладдин Р.Д." → "Единый Клиент JaCarta":
2. Откроется основное окно Единого Клиента JaCarta, при этом в панели управления в нижней части экрана появится значок вызова меню быстрого запуска программы :

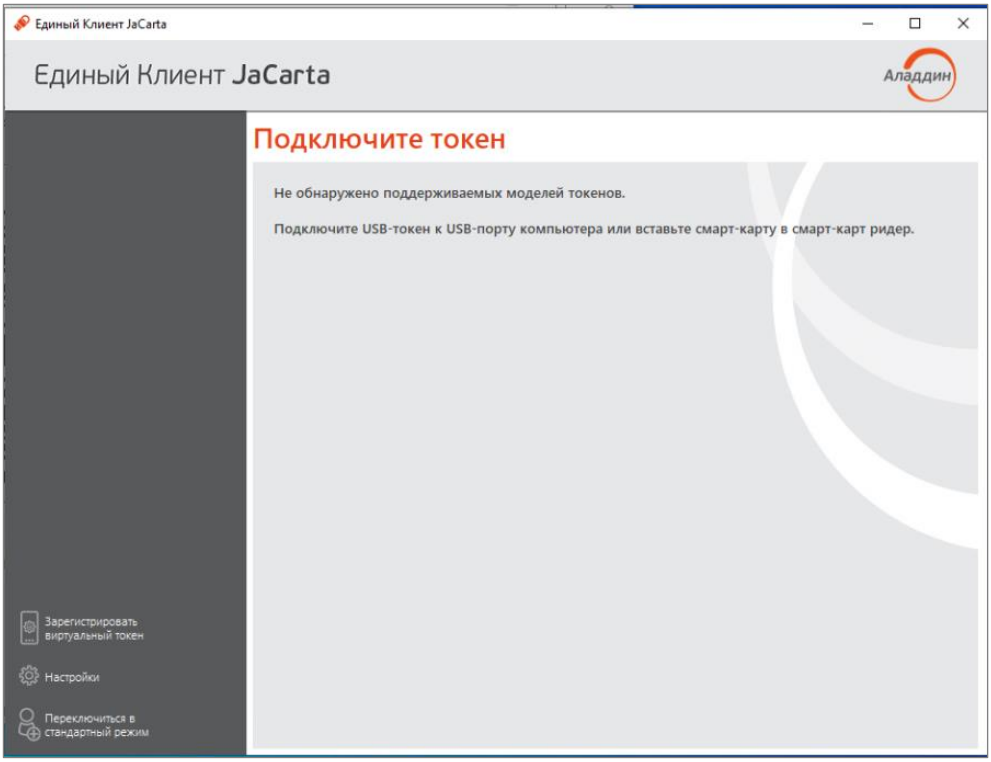


Рисунок 1 – Основное окно Единого Клиента JaCarta

По умолчанию основное окно Единого Клиента JaCarta открывается в стандартном режиме.

3. Чтобы закрыть основное окно Единого Клиента JaCarta щелкните 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 управления (в нижней части экрана) даже при закрытом окне Единого Клиента JaCarta и предоставляет доступ к меню быстрого запуска.

Для вызова меню быстрого запуска вызовите контекстное меню значка в панели управления:

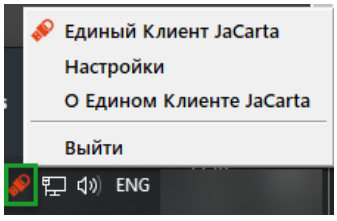


Рисунок 2 –Меню быстрого запуска Единого Клиента JaCarta

Меню быстрого запуска содержит следующие команды:

- "Единый Клиент JaCarta" – открывает окно основного интерфейса Единый Клиент JaCarta.
- "Настройки" – открывает окно настроек программы.

- "О Едином Клиенте JaCarta" – открывает окно со сведениями о программе (см. 4.4).
- "Выйти" – позволяет выйти из программы, при этом значок перестает отображаться в панели управления.

4.3 Режимы работы программы

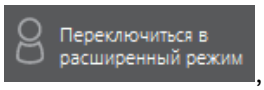
Единый Клиент JaCarta поддерживает следующие режимы работы:

Стандартный режим – позволяет просматривать краткие сведения о подсоединённых электронных ключах, сменить PIN-код пользователя, назначить или изменить PIN-код подписи, изменить метку электронного ключа.

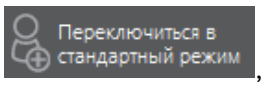
Расширенный режим – позволяет просматривать подробные сведения о подсоединённых электронных ключах и предоставляет доступ к операциям над приложениями электронного ключа и объектами каждого приложения.

4.3.1 Переключение между режимами

Чтобы определить в каком режиме открыто окно Единый Клиент JaCarta, необходимо обратить внимание на название кнопки "Переключиться в режим ..." в основном окне программы (см. рисунок 1). 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 нажмите кнопку "Переключиться в расширенный режим".
2. Для переключения Единого Клиента JaCarta из расширенного режима в стандартный режим нажмите 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 ниже приведен вид основного окна в стандартном режиме с подключенным к компьютеру пользователя электронным ключом:

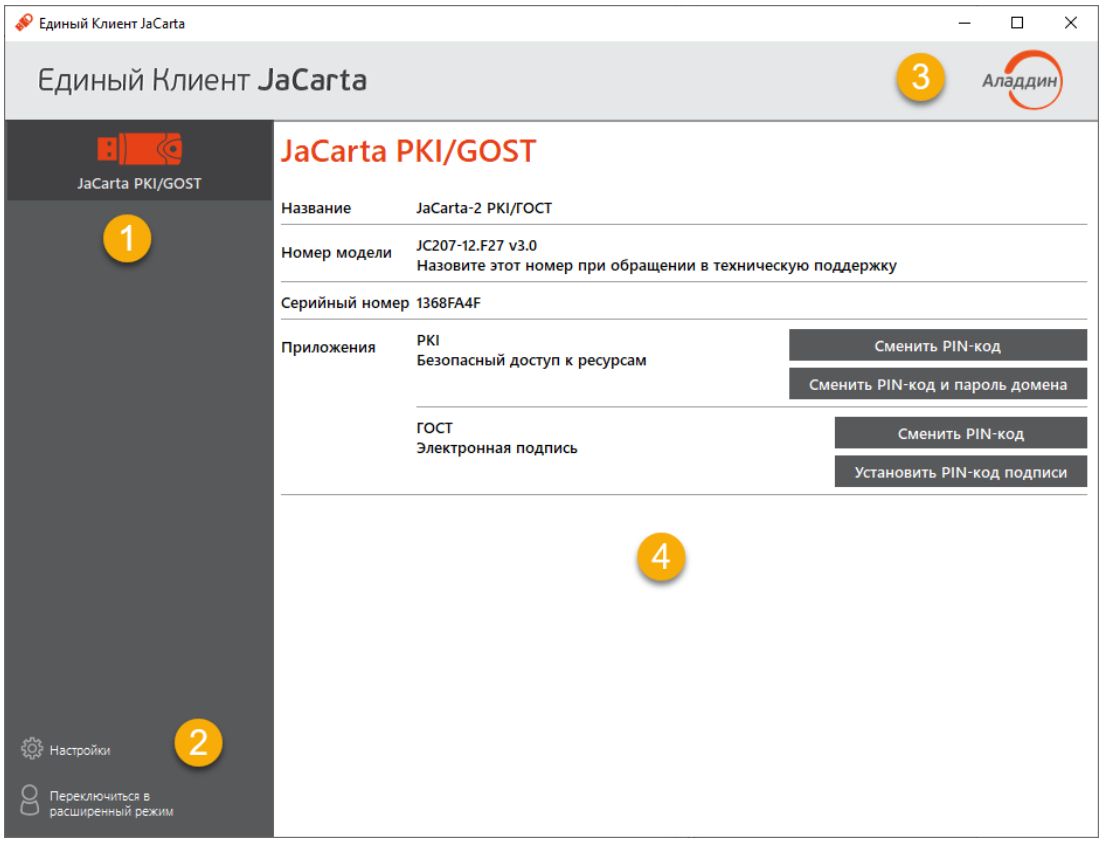


Рисунок 3 – Основное окно Единого Клиента JaCarta в стандартном режиме

Основное окно 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 щелкните 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. 70

2 Область содержит кнопки:

"Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе "Единый Клиент JaCarta. Руководство администратора для Microsoft Windows";

"Переключиться в расширенный режим" – кнопка для переключения Единого Клиента JaCarta в расширенный режим

3 Открывает окно со сведениями о программе 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

Вид основного окна в расширенном режиме приведен на рисунке ниже:

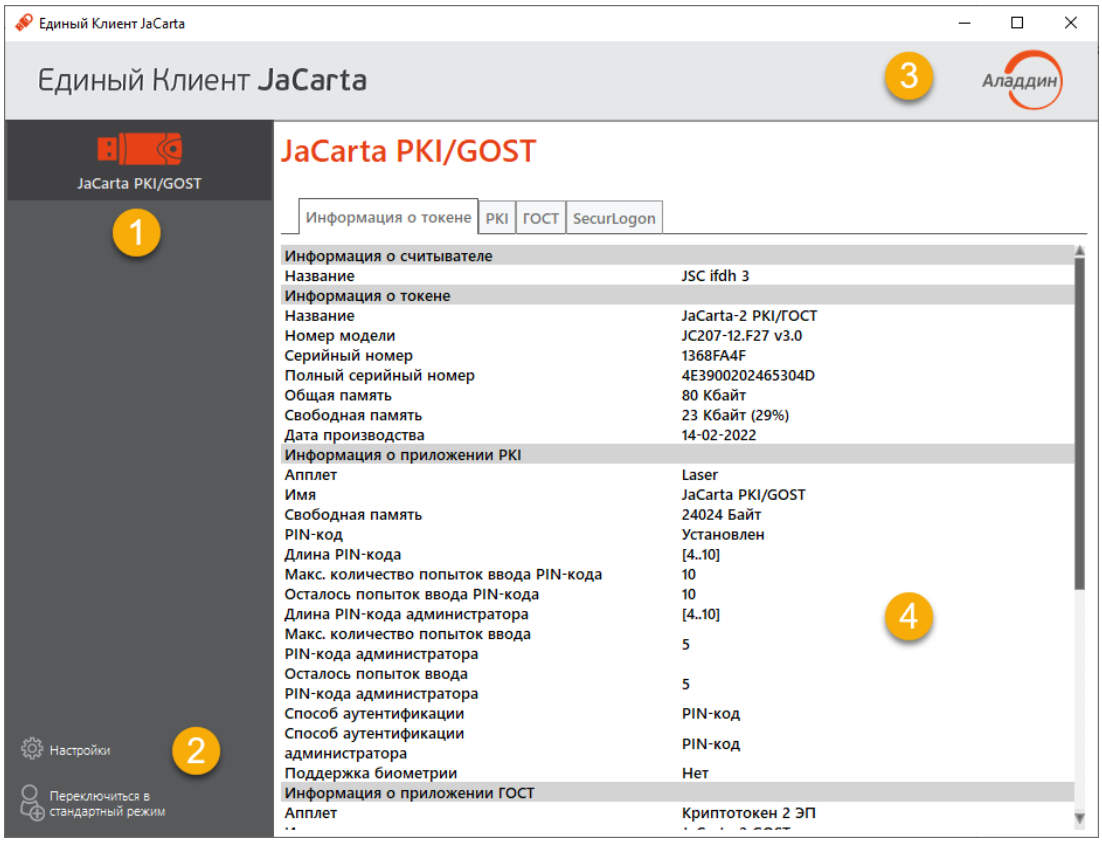


Рисунок 4 – Основное окно Единого Клиента JaCarta в расширенном режиме

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 щелкните 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. 70

2 Область содержит кнопки:

"Настройки" – кнопка для вызова окна настроек программы.

"Переключиться в стандартный режим" – кнопка для переключения Единого Клиента JaCarta в стандартный режим

3 Открывает окно со сведениями о программе 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 вкладок:

– на вкладке "Информация о токене" отображается информация об электронном ключе (см. рисунок 4);

– 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 4 электронный ключ содержит приложение PKI и приложение ГОСТ, поэтому данная область содержит вкладку "Информация о токене" и вкладку "PKI" для управления приложением PKI и объектами в этом приложении и вкладку "ГОСТ" для управления приложением ГОСТ и объектами в этом приложении.

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 Клиент JaCarta Virtual Token и перезагрузки Единого Клиента JaCarta появится новый элемент управления – кнопка "Зарегистрировать виртуальный токен" (см. Рисунок 5).

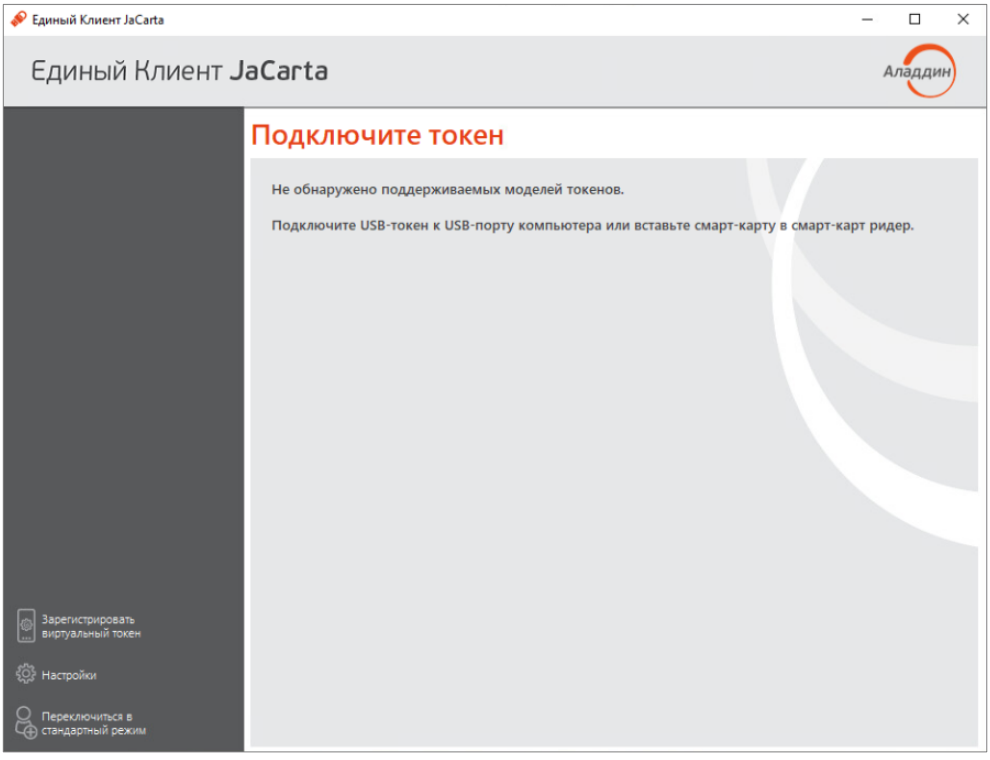


Рисунок 5 – Основное окно Единого Клиента JaCarta. Кнопка "Зарегистрировать виртуальный токен"

Нажать кнопку "Зарегистрировать виртуальный токен" будет открыто окно [Панель управления JaCarta Virtual Token], содержащее сгенерированный QR-код для регистрации (см. Рисунок 6).

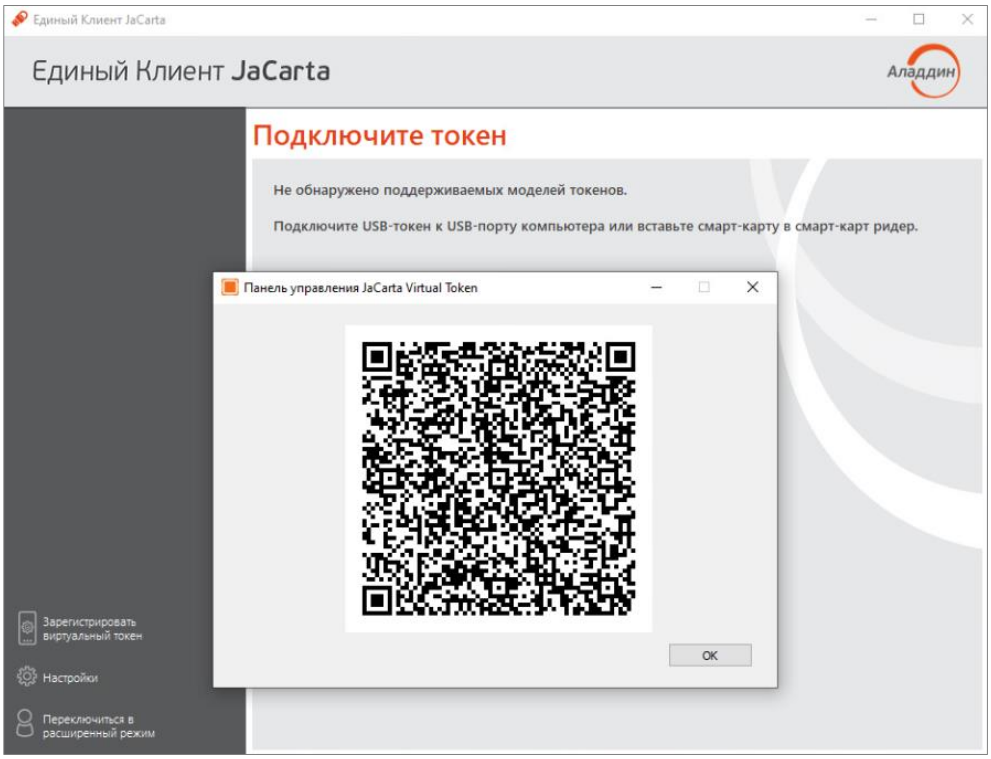


Рисунок 6 – Основное окно Единого Клиента JaCarta. Сгенерированный QR-код

На мобильном устройстве открыть установленное мобильное приложение JaCarta Virtual Token. На главном экране нажать кнопку "Добавить" или  (см. Рисунок 7). Будет открыто окно считывания QR-кода (см. Рисунок 8). Отсканировать QR-код, сгенерированный в Панели управления JaCarta Virtual Token.

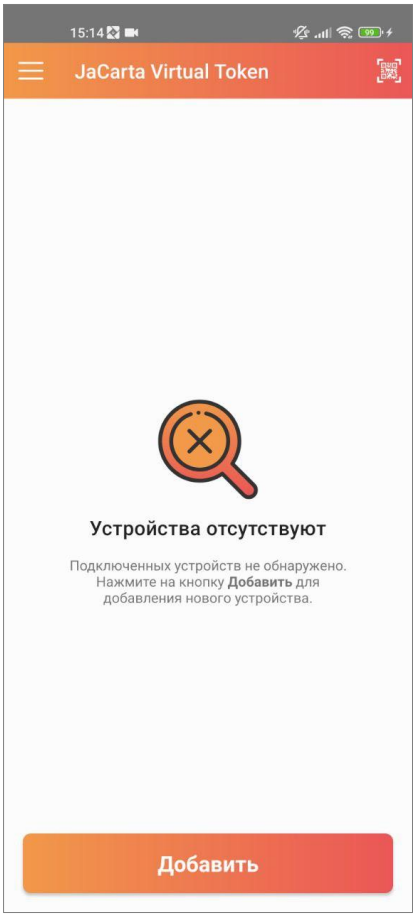


Рисунок 7 - Мобильное приложение JaCarta Virtual Token. Добавление нового устройства

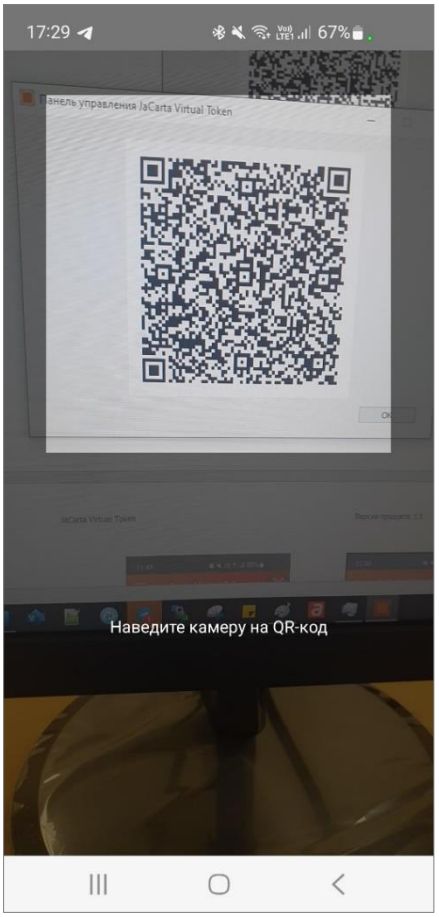


Рисунок 8 - Мобильное приложение JaCarta Virtual Token. Сканирование QR-кода

В Панели управления JaCarta Virtual Token подтвердить регистрацию мобильного устройства с помощью кнопки "Подтвердить" (см. Рисунок 9).

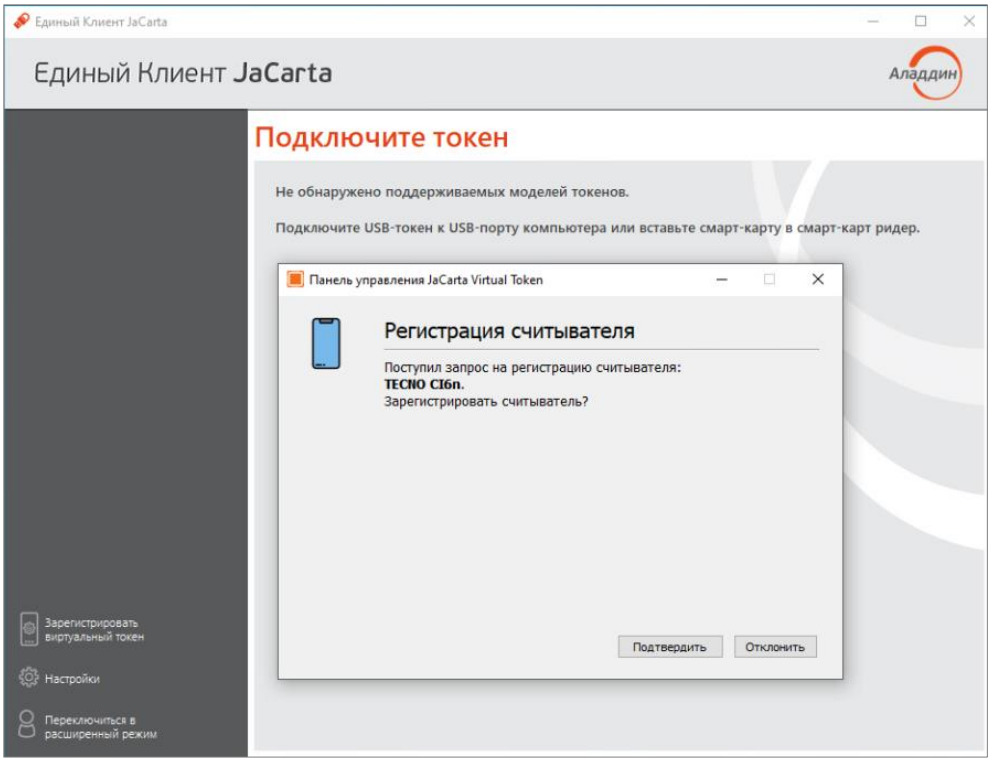


Рисунок 9 – Панель управления JaCarta Virtual Token. Подтверждение регистрации на мобильном устройстве

В случае подтверждения регистрации, отобразится информационное сообщение (см. Рисунок 10).

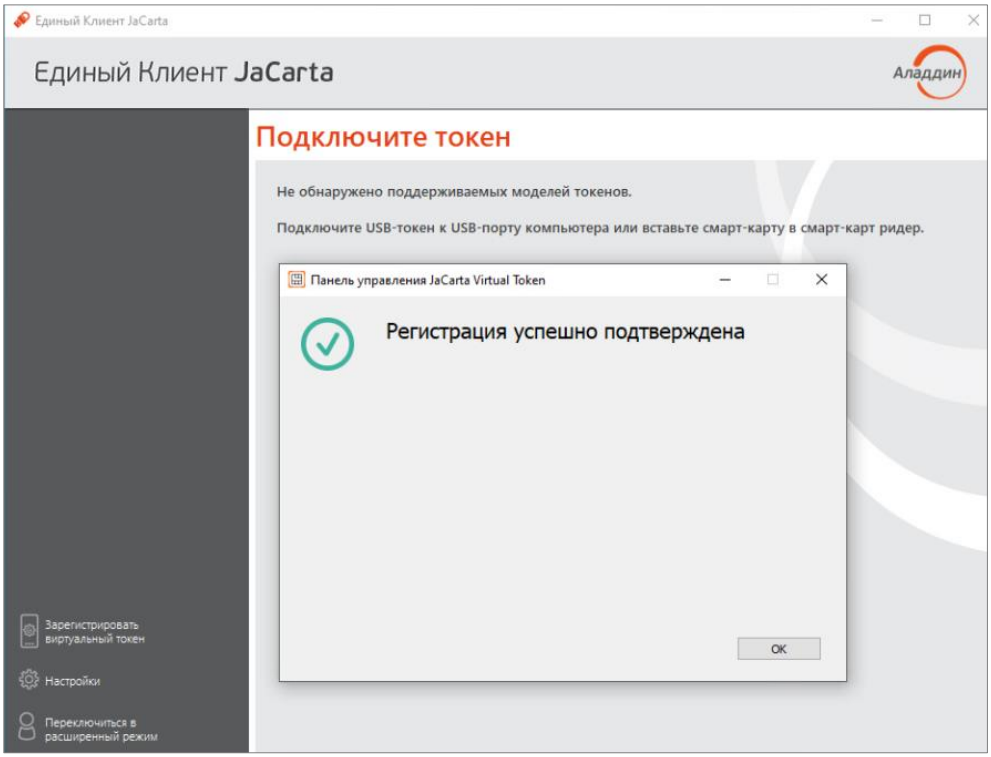


Рисунок 10 - Панель управления JaCarta Virtual Token. Сообщение об успешной регистрации

После регистрации виртуальный токен будет отображаться в окне Единого Клиента точно также, как и аппаратный USB-токен (см. Рисунок 11), операции также аналогичны: переименование токена, смена PIN-кода пользователя, просмотр информации о токене.

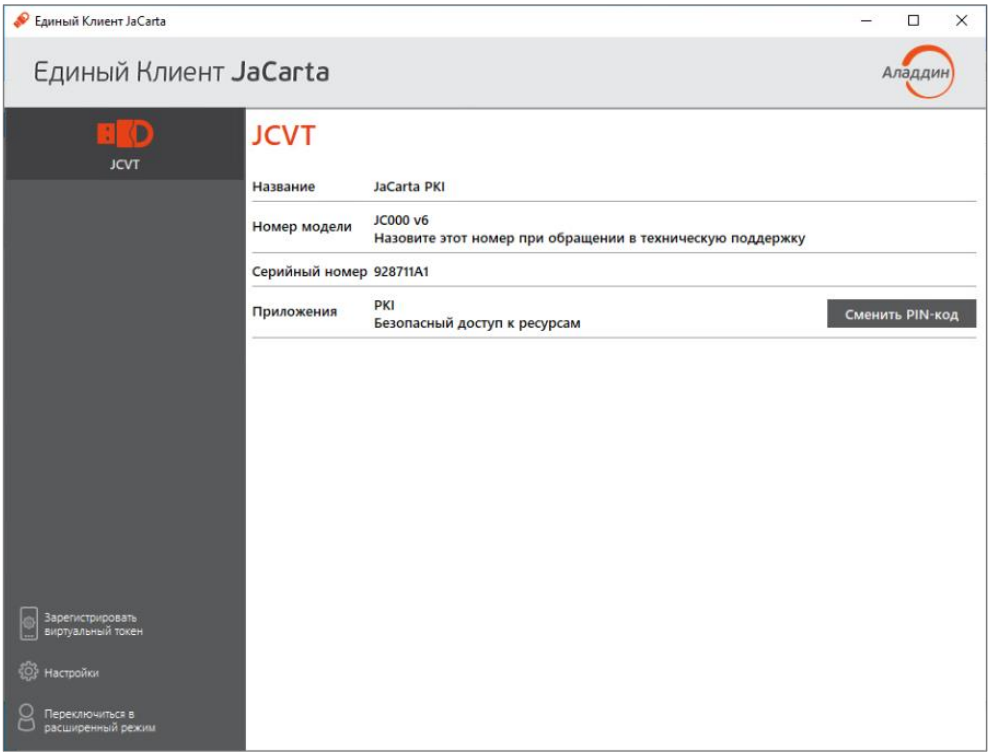


Рисунок 11 – Отображение зарегистрированного виртуального токена

> *Подробнее про работу с виртуальным токеном и Мобильным приложением JaCarta Virtual Token см. документ «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 Единый Клиент JaCarta:

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

либо активируйте команду "О Едином Клиенте JaCarta" в меню быстрого запуска Единого

Клиента JaCarta (см. рисунок 2). Будет отображено окно со сведениями о версии программы и контактами техподдержки:

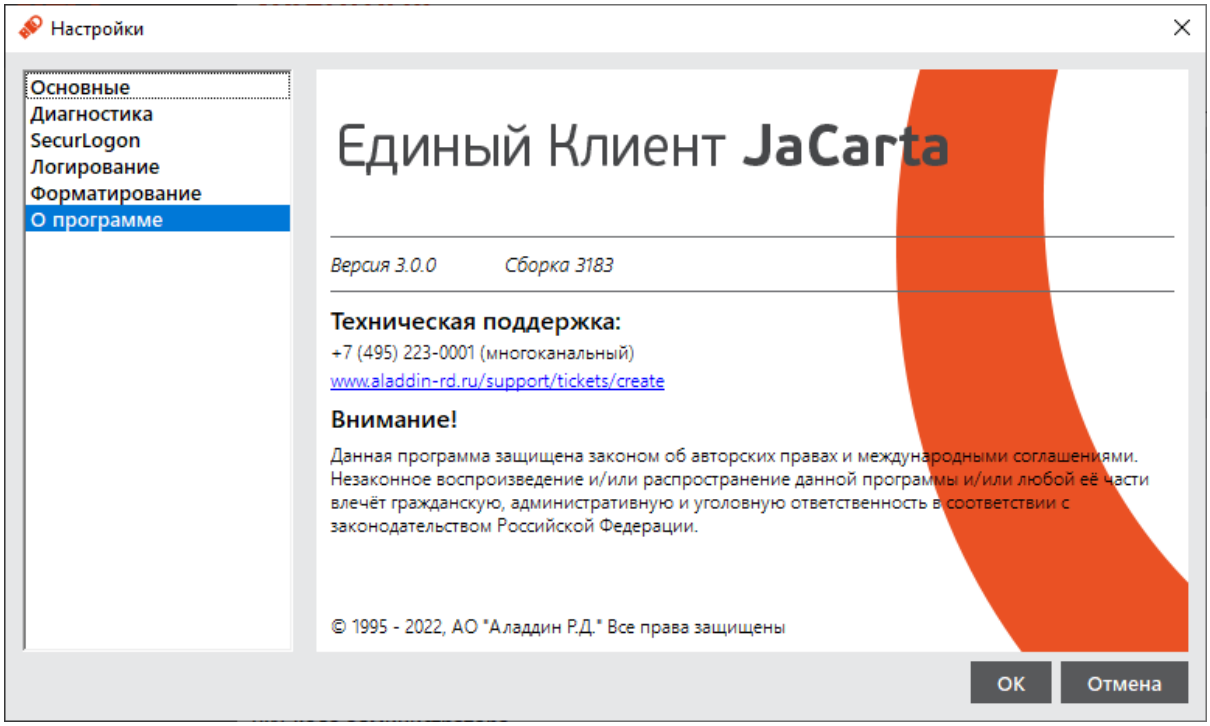


Рисунок 12 - Окно "О программе"

2. Нажмите кнопку "Закрыть" в правом верхнем углу для закрытия окна.

4.6 Завершение работы программы

Для завершения работы программы:

- Активируйте команду "Выйти" в меню быстрого запуска Единого Клиента JaCarta (см. рисунок 2). 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 названия (переименование) электронного ключа;
- изменение PIN-кода пользователя;
- установка, изменение, разблокирование PIN-кода подписи (для электронных ключей с приложением ГОСТ с апплетом Криптотокен 2 ЭП).

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. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера.
2. Информация об электронном ключе будет отображена в основном окне немедленно, выполнения дополнительных действий не требуется. Если подключено несколько электронным ключей, то выберите значок нужного ключа в области слева:

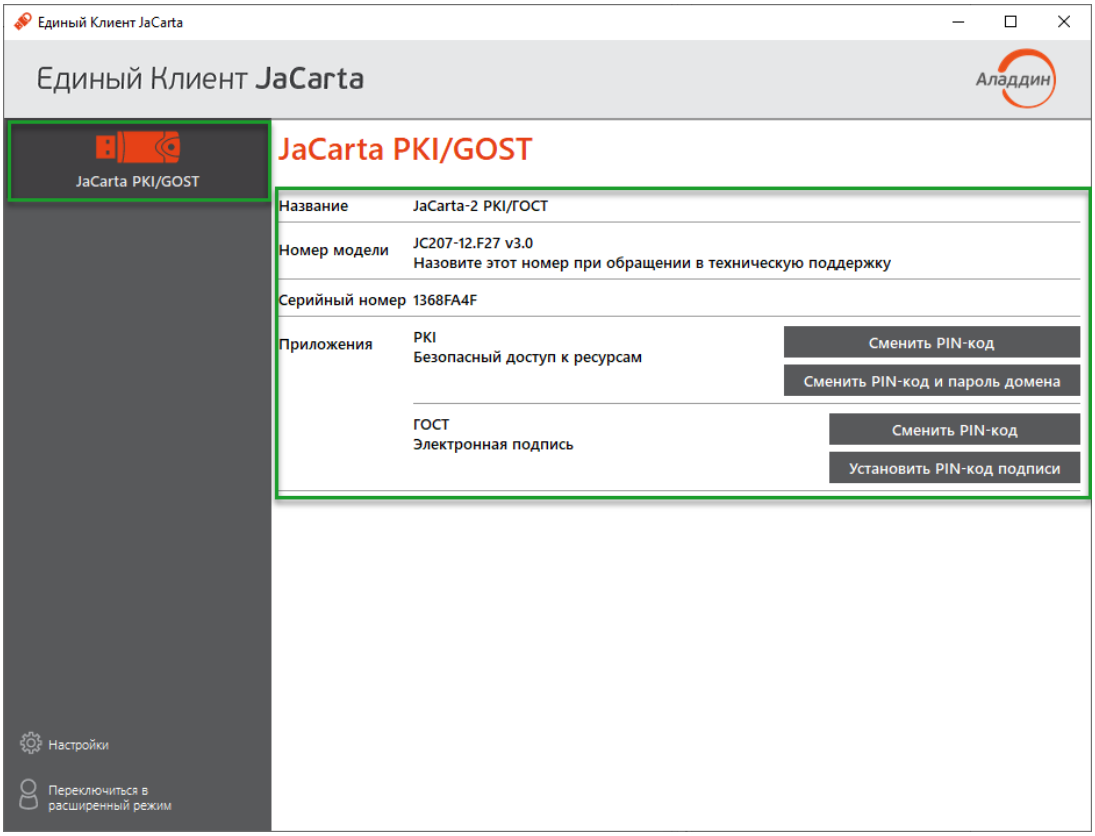


Рисунок 13 – Информация о выбранном электронном ключе в стандартном режиме

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" – уникальный номер электронного ключа;
- "Приложения" – перечень приложений, установленных в памяти электронного ключа. Первым в списке отображается приоритетное на данном ключе приложение. На примере, приведенном на рисунке 13 приоритетным приложением является приложение PKI.

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

5.2 Изменение названия (переименование) электронного ключа

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

Для изменения метки электронного ключа:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. Активируйте команду "Переименовать токен" в контекстном меню (нажатием правой кнопки мыши) выбранного значка. Будет отображено одноименное окно:

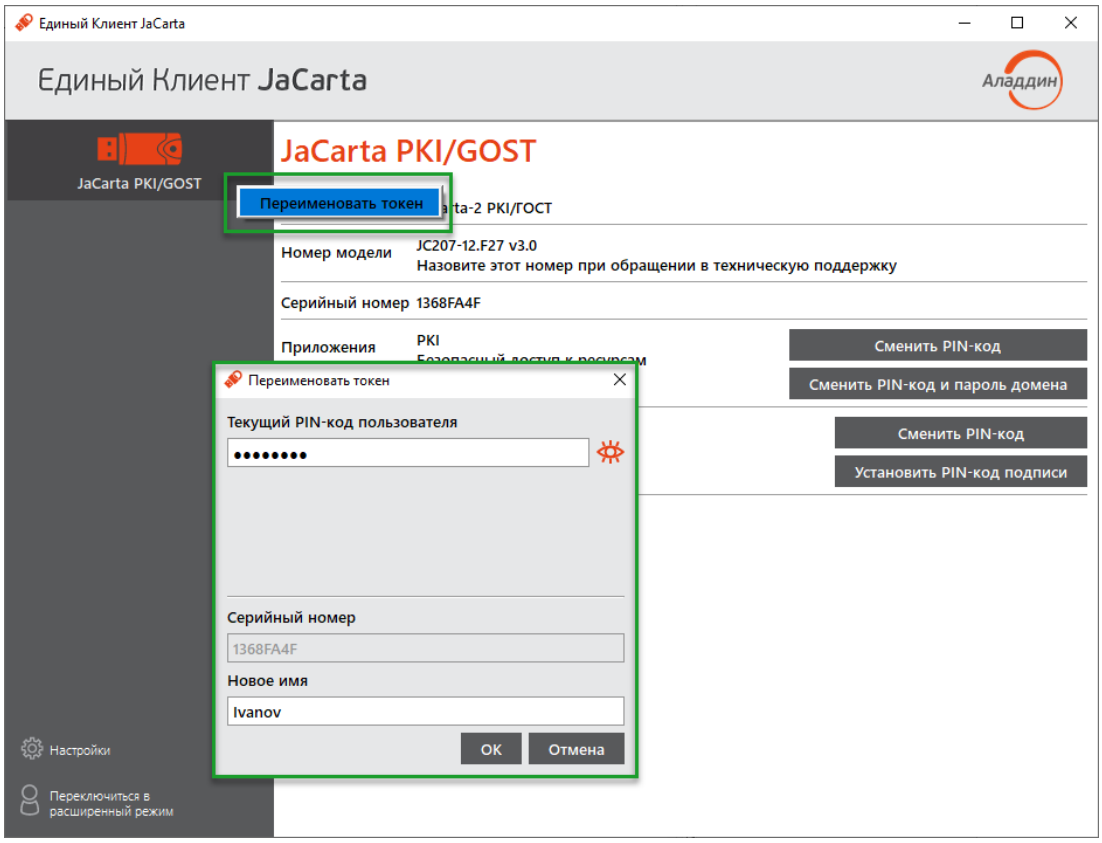


Рисунок 14 – Вызов окна "Переименовать токен" в стандартном режиме

3. В окне "Переименовать токен" заполните поля:
   - в поле "Текущий PIN-код пользователя" введите PIN-код пользователя. Если на электронном ключе установлено несколько приложений, то введите PIN-код приложения, которое является приоритетным – это приложение отображается первым в списке установленных приложений в основном окне;
   - в поле "Новое имя" введите новое имя электронного ключа.

4. Нажмите кнопку "ОК". В случае успешной авторизации на электронном ключе его имя будет изменено:

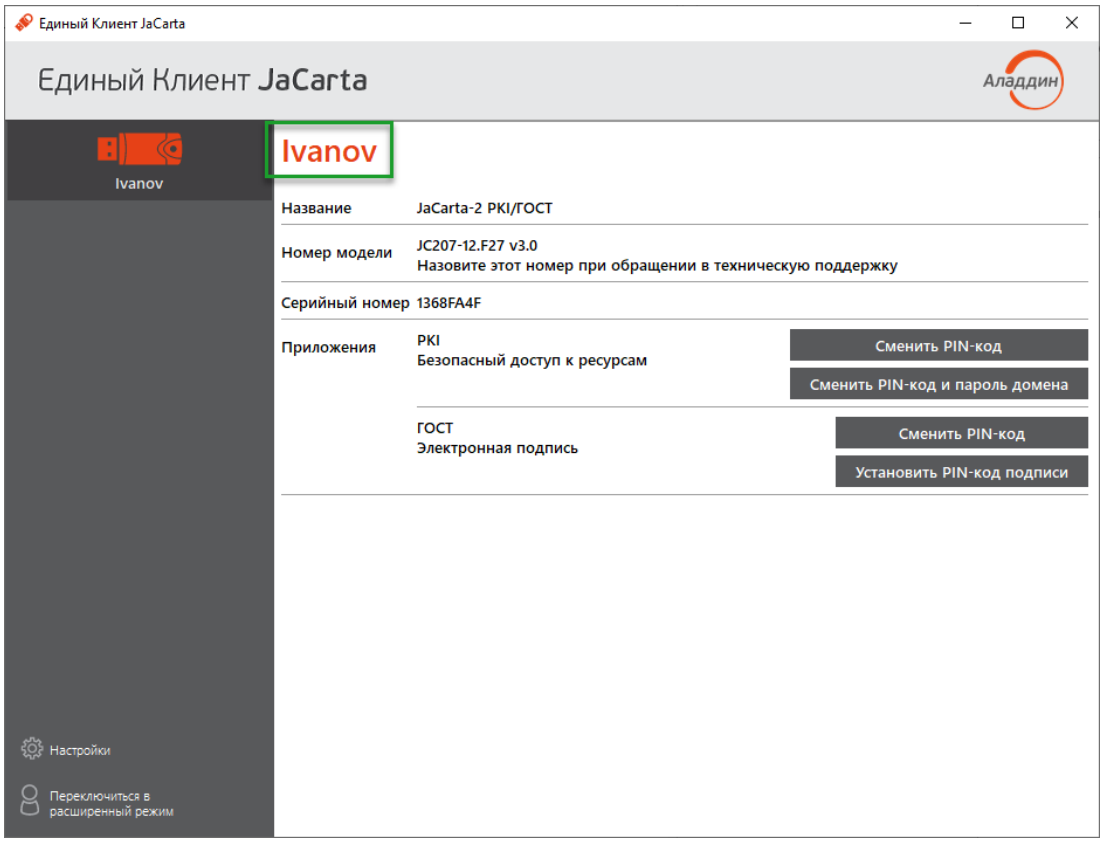


Рисунок 15 – Основное окно в стандартном режиме. Имя ключа изменено

5.3 Изменение PIN-кода пользователя

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:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

2. В основном окне Единого клиента JaCarta в стандартном режиме нажмите кнопку "Сменить PIN-код" для выбранного приложения (на скриншотах ниже приведен пример смены PIN-кода приложения PKI):

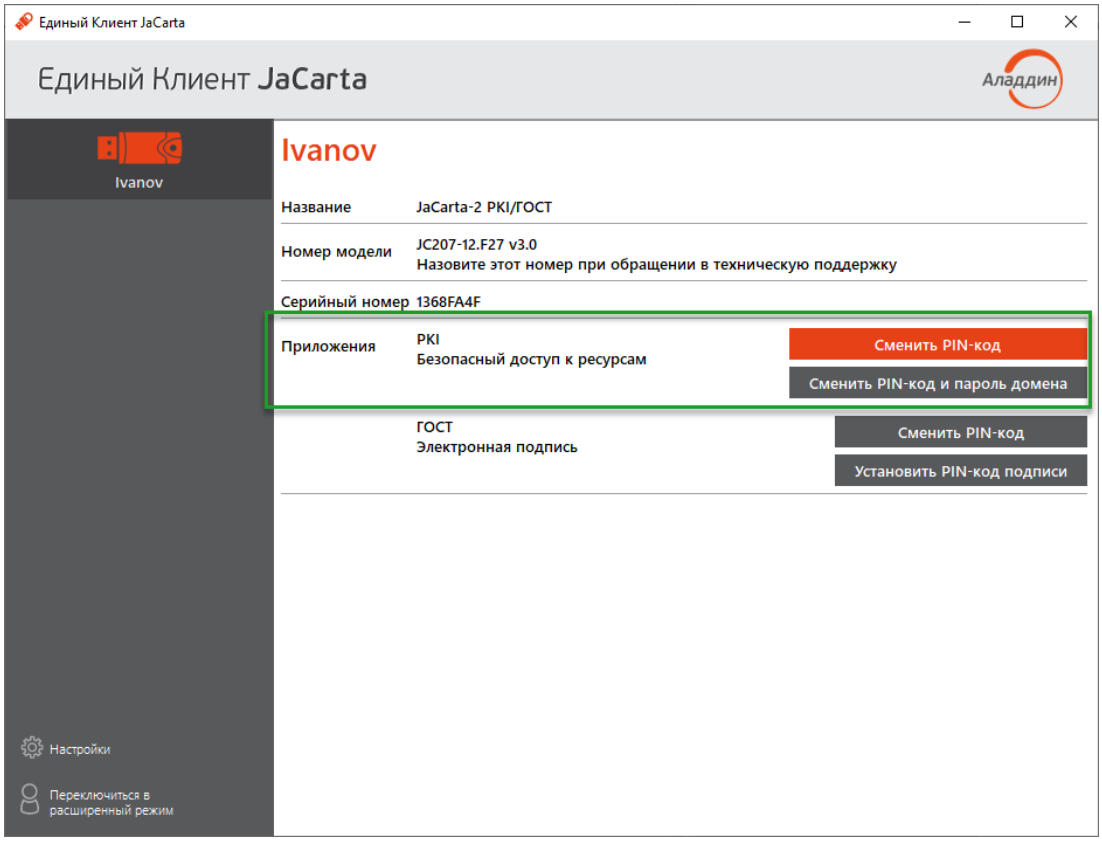


Рисунок 16 – Вызов окна "Переименовать токен" в стандартном режиме

3. Будет отображено окно для смены PIN-кода. Заполните поля в окне следующим образом (см. рисунок 17):
   - в поле "Текущий PIN-код пользователя" введите PIN-код пользователя выбранного приложения (в данном примере приложения PKI);
   - в поле "Новый PIN-код пользователя" введите 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 4 символа.*

– в поле "Подтвердить PIN-код пользователя" введите значение нового PIN-кода пользователя повторно:

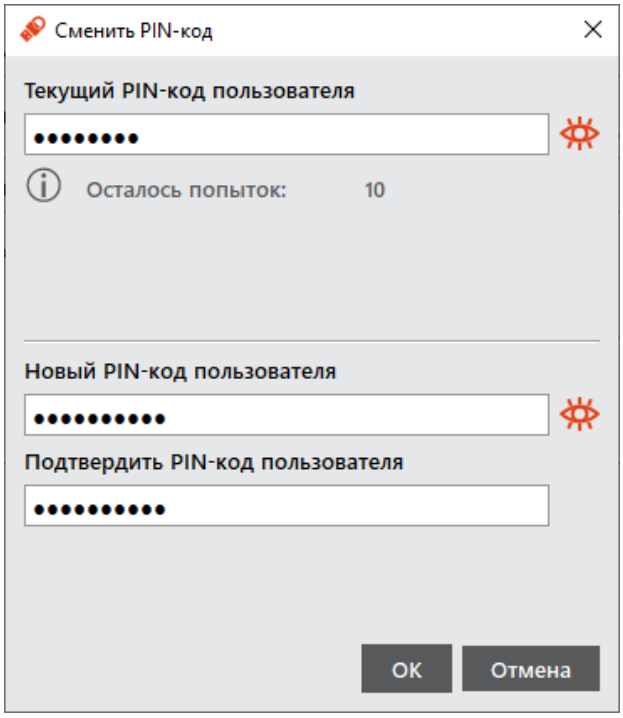


Рисунок 17 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода введены верно

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 (кнопка "Выполнить" неактивна) до тех пор, пока не будет введено другое значение PIN-кода:

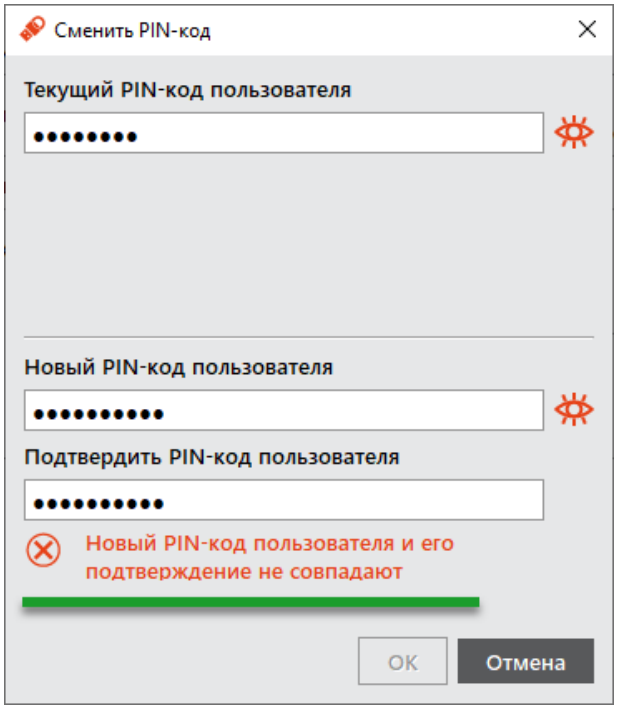


Рисунок 18 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода не совпадают

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

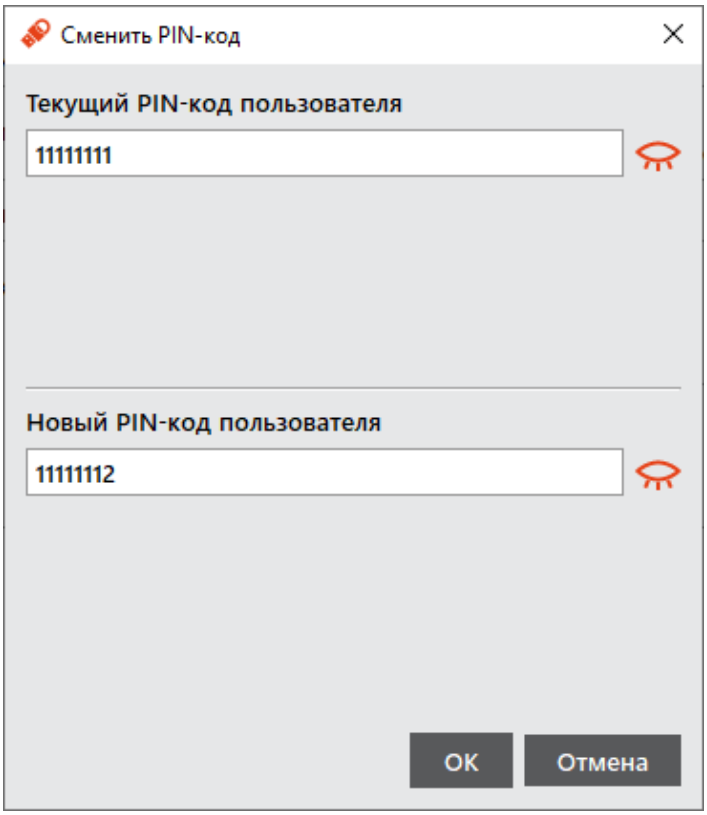


Рисунок 19 – Окно изменения PIN-кода пользователя. Отображение значений полей в явном виде

4. Нажмите кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-кода пользователя будет изменен:

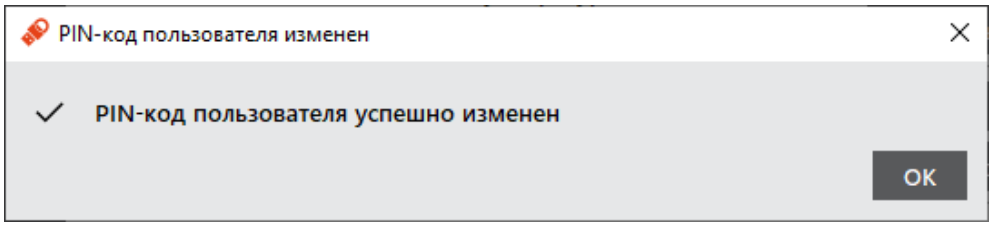


Рисунок 20 – Окно "PIN-кода пользователя изменен"

5. Нажмите кнопку "OK" в окне сообщения для его закрытия.

5.4 Установка PIN-кода подписи

Операция установки PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ и аппле-том Криптотокен 2 ЭП 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. 5.5 "Изменение PIN-кода подписи").

PIN-код подписи блокируется после ввода неправильного PIN-кода подписи в количестве раз, превышающем указанное в настройках. Для заблокированного PIN-кода подписи доступна операция его разблокирования (см. п. 5.6 "Разблокирование PIN-кода подписи").

Для установки PIN-кода подписи:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ с приложением ГОСТ с апплетом Криптотокен 2 ЭП к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. В основном окне Единого клиента JaCarta в стандартном режиме нажмите кнопку "Установить PIN-код подписи" для приложения ГОСТ:

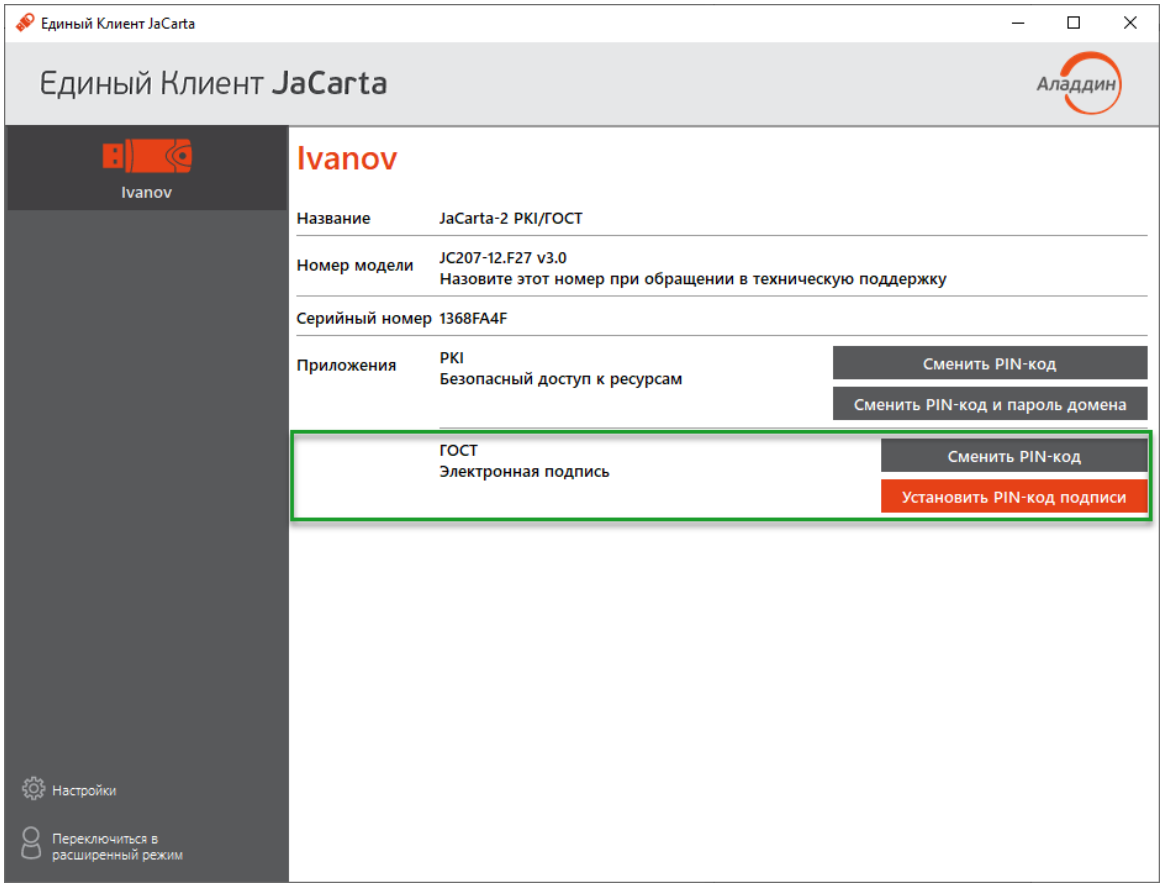


Рисунок 21 – Главное окно Единого Клиента JaCarta. Кнопка "Установить PIN-код подписи" активна

3. Будет отображено окно для установки PIN-кода подписи. Заполните поля в окне следующим образом (см. рисунок 22):
   - в поле "Текущий PIN-код" введите PIN-код пользователя приложения ГОСТ;
   - в поле "Установить PIN-код подписи" введите 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" введите 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 нажмите кнопку . Для возвращения к отображению в скрытом виде нажмите кнопку .

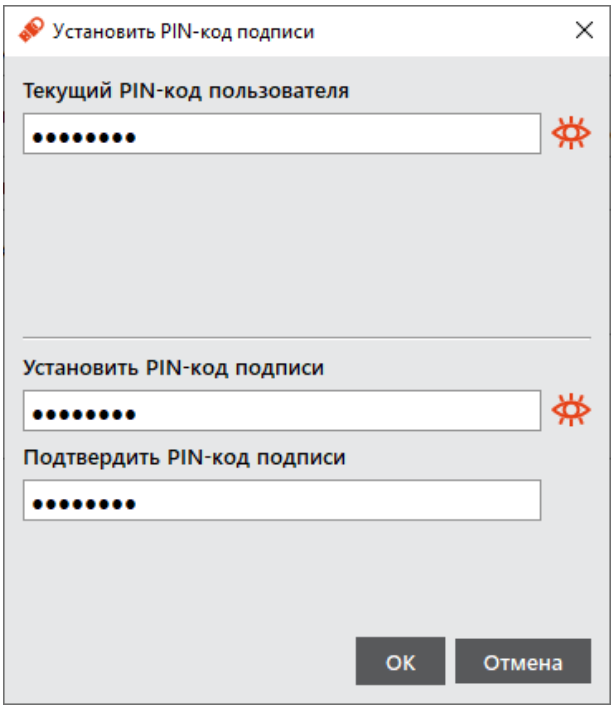


Рисунок 22 - Окно установки PIN-кода подписи. Значения PIN-кода введены верно

4. Нажмите кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-код подписи будет установлен. На экране появится сообщение об этом:

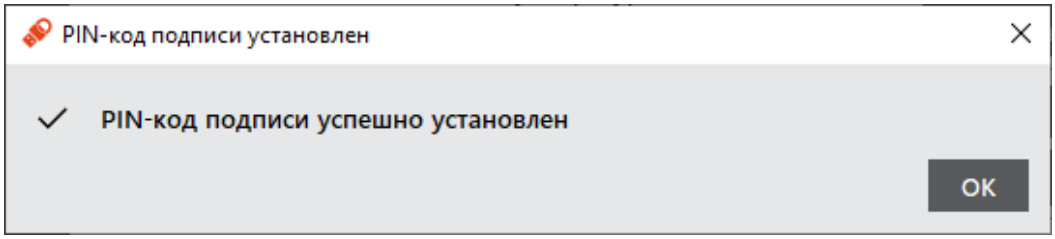


Рисунок 23 - Сообщение об успешной инициализации PIN-кода подписи

5. Нажмите кнопку "OK" в окне сообщения.

5.5 Изменение PIN-кода подписи

Операция изменения PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ и апплетом Криптотокен 2 ЭП 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:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ с приложением ГОСТ с апплетом Криптотокен 2 ЭП к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

2. В основном окне Единого клиента JaCarta в стандартном режиме нажмите кнопку "Сменить PIN-код подписи" для приложения ГОСТ:

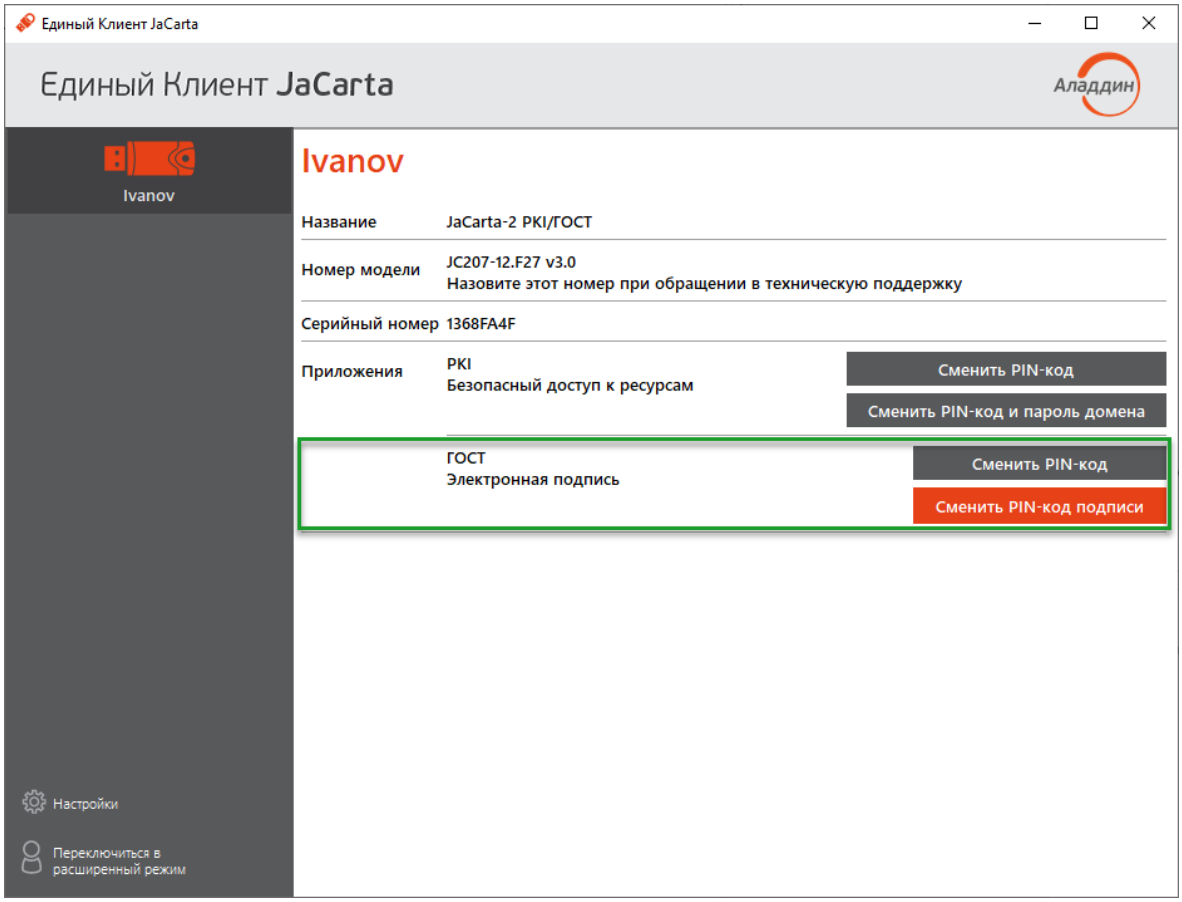


Рисунок 24 - Единый Клиент JaCarta. Главное окно

3. Будет отображено окно для изменения PIN-кода подписи. Заполните поля в окне следующим образом (см. рисунок 25):
   - в поле "Текущий PIN-код" введите PIN-код пользователя выбранного приложения (в данном примере приложения ГОСТ);
   - в поле "Текущий PIN-код подписи" введите PIN-кода подписи;
   - в поле "Новый PIN-код подписи" введите 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" введите 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 нажмите кнопку  . Для возвращения к отображению в скрытом виде нажмите кнопку  .

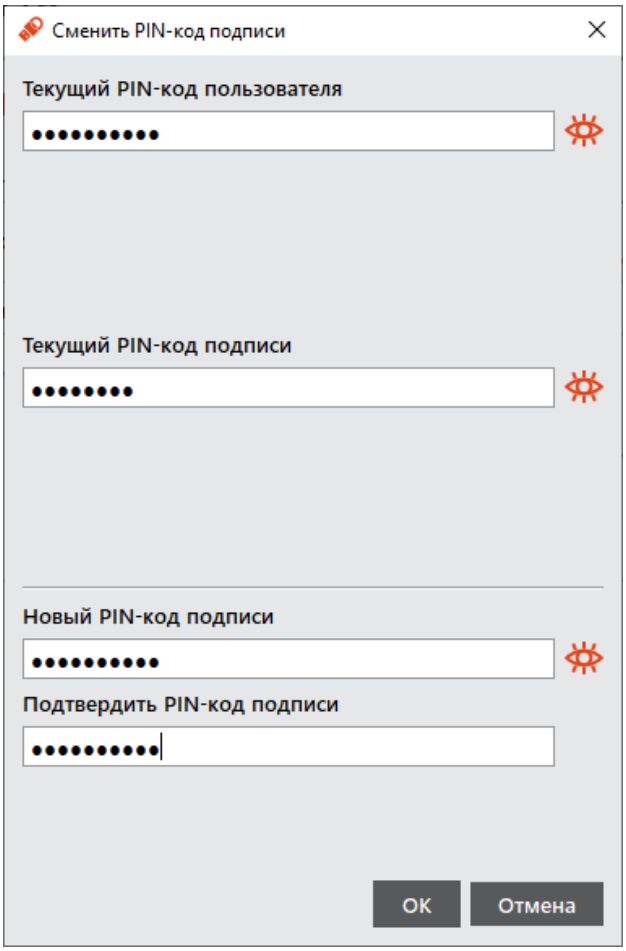


Рисунок 25 - Окно изменения PIN-кода подписи. Значения PIN-кода введены верно

4. Нажмите кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-кода подписи будет установлен. На экране появится сообщение об этом:

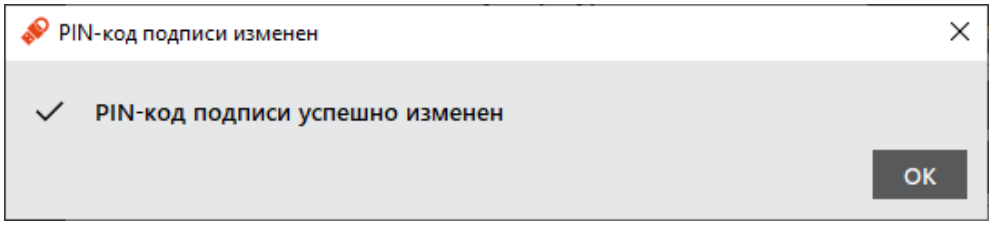


Рисунок 26 – Сообщение об успешном изменении PIN-кода подписи

5. Нажмите кнопку "OK" в окне сообщения для его закрытия.

5.6 Разблокирование PIN-кода подписи

Операция разблокирования PIN-кода подписи выполняется на электронных ключах с приложением ГОСТ с апплетом Криптотокен 2 ЭП 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 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 обратитесь к администратору для разблокирования PIN-кода подписи.

После разблокирования PIN-кода подписи доступна операция изменения PIN-кода подписи (см. п. 5.5 "Изменение PIN-кода подписи").

Для разблокирования PIN-кода подписи:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ с приложением ГОСТ с апплетом Криптотокен 2 ЭП к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. В основном окне Единого клиента JaCarta в стандартном режиме нажмите кнопку "Разблокировать PIN-код подписи" для приложения ГОСТ:

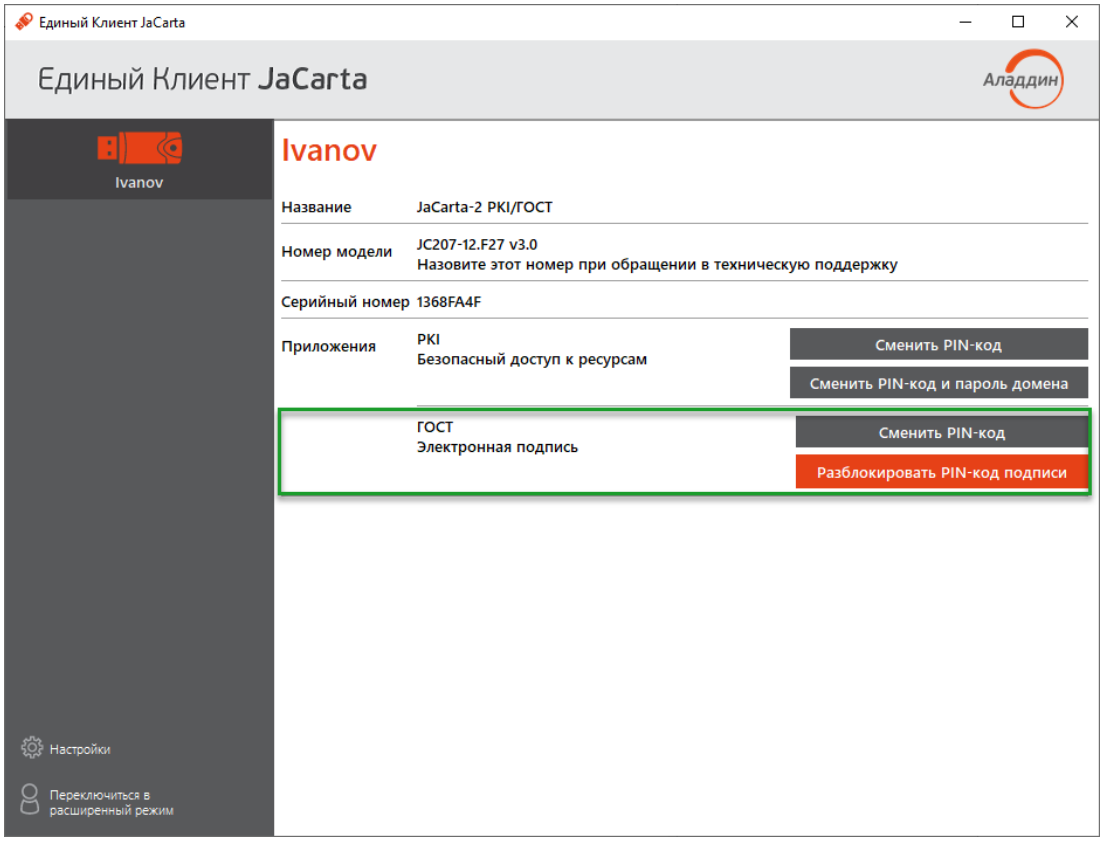


Рисунок 27 - PIN-код подписи заблокирован

3. Будет отображено окно с выбором способа разблокирования PIN-кода:

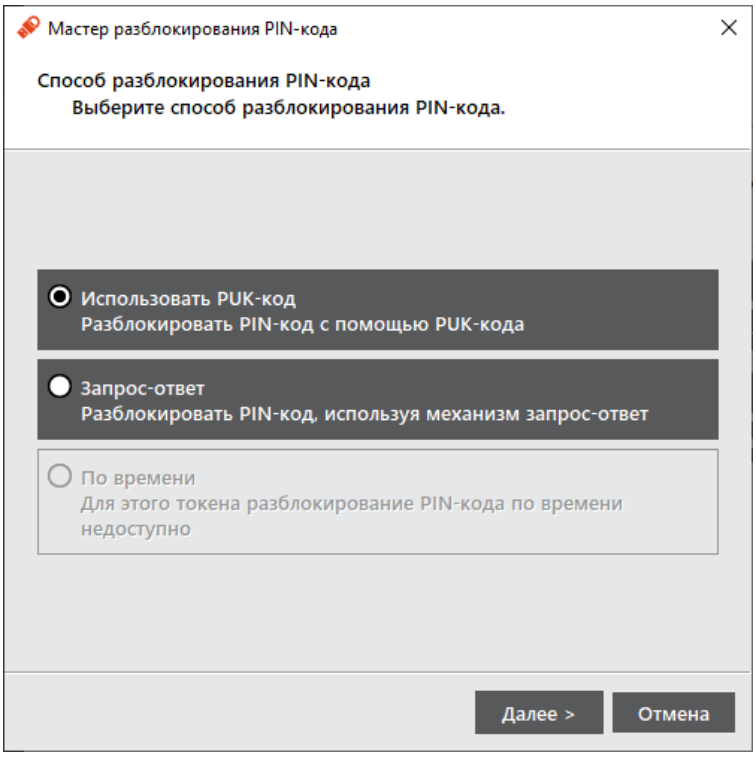


Рисунок 28 – Окно для ввода PUK-кода при разблокировании PIN-кода подписи

4. В окне выбора способа разблокирования PIN-кода необходимо выбрать желаемый способ разблокирования.
5. Если был выбран способ разблокирования PIN-кода с использованием PUK-кода, будет отображено окно для ввода PUK-кода. В поле "PUK-код" введите текущее 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 обратитесь к администратору безопасности.*

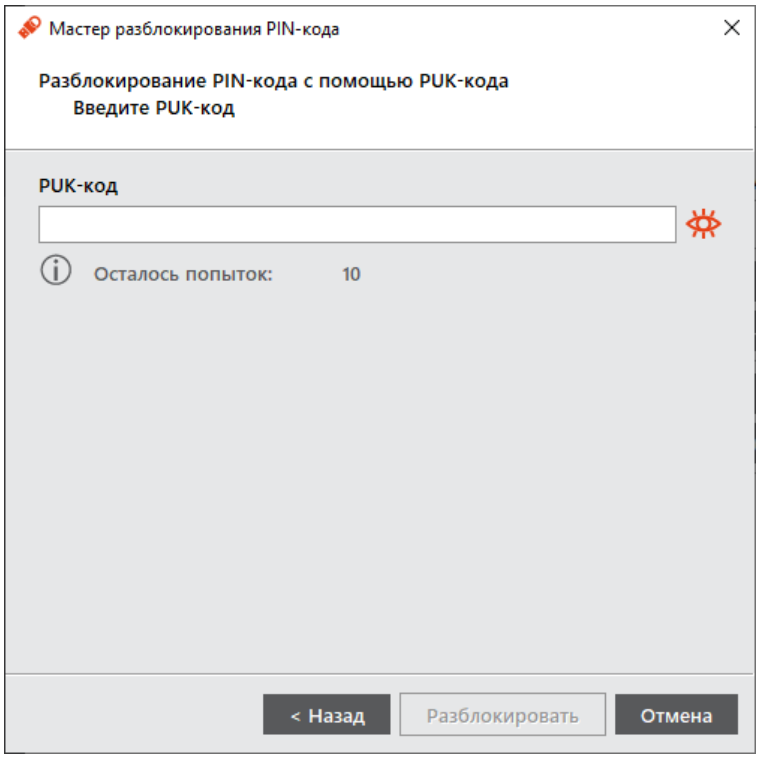


Рисунок 29 – Окно для ввода PUK-кода при разблокировании PIN-кода подписи

6. Нажмите кнопку "Разблокировать". В случае ввода верного PUK-кода будет выполнено разблокирование PIN-кода подписи. Для закрытия окна нажмите кнопку "Завершить".
7. Если был выбран способ разблокирования PIN-кода подписи с использованием механизма запрос-ответ будет открыто окна с запросом.

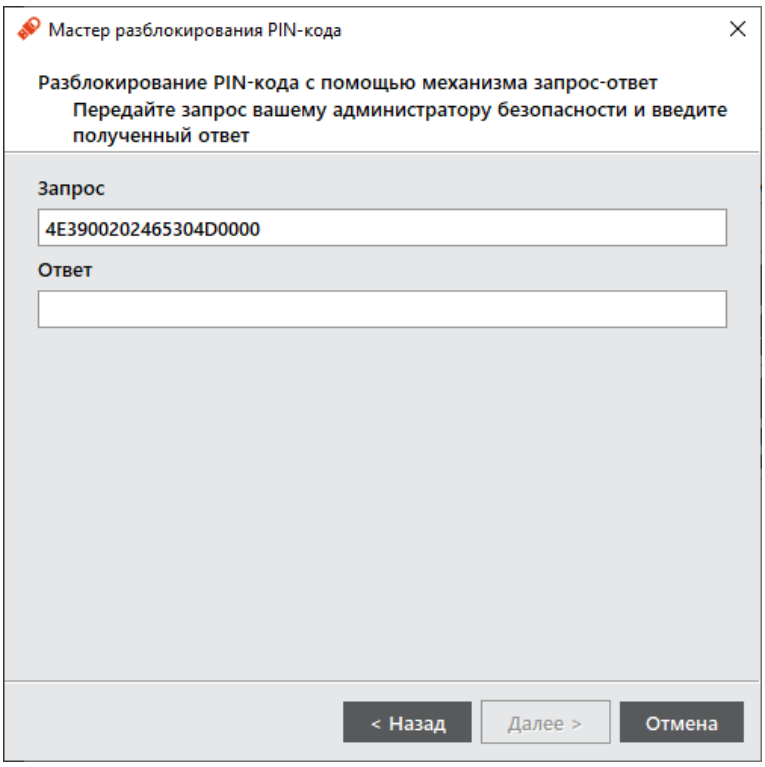


Рисунок 30 – Сообщение об успешном разблокировании PIN-кода подписи

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 с апплетом Крипто-токен 2 ЭП);
- 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"Единый Клиент JaCarta. Руководство администратора для Windows".

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:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера.
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронным ключей, то выберите значок нужного ключа в области слева.

3. Нажмите кнопку "Переключиться в расширенный режим" и на вкладке "Информация о токене" будет отображена подробная информация о токене:

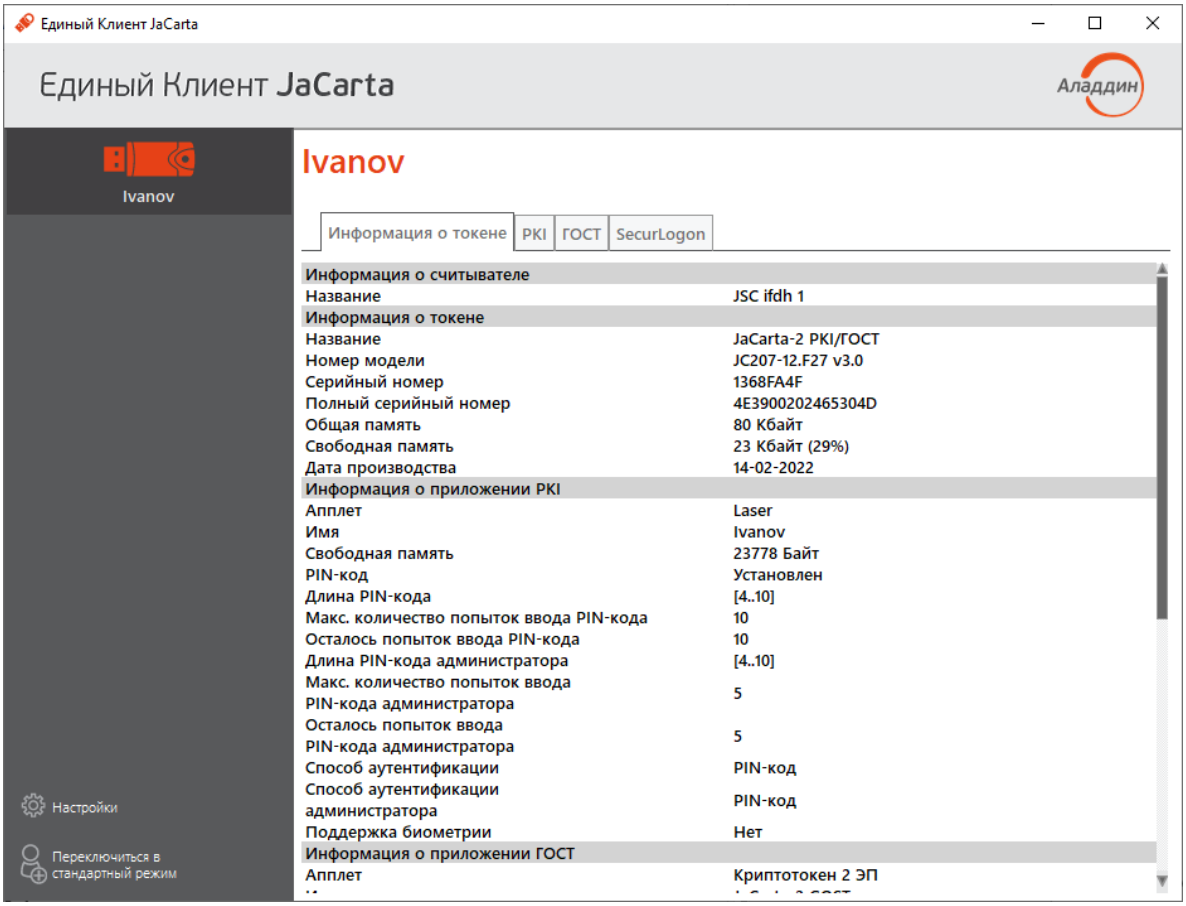


Рисунок 31 – Окно "Подробная информация о токене"

Вкладка "Информация о токене" содержит информацию:

- о считывателе электронного ключа в составе:
  - "Название" – наименование считывателя;
- информацию о токене в составе:
  - "Название" – название электронного ключа;
  - "Номер модели" – номер модели электронного ключа;
  - "Серийный номер" – серийный номер электронного ключа, который может быть нанесён на корпус;
  - "Полный серийный номер" – уникальный серийный номер электронного ключа;
  - "Общая память" – полный объём памяти электронного ключа;
  - "Свободная память" – объём свободной памяти электронного ключа;
  - "Дата производства" – дата производства электронного ключа.
- для каждого приложения, установленного в памяти электронного ключа, отображается следующая информация:
  - Заголовок "Информация о приложении *<наименование приложения>*";
  - "Апплет" – название апплета, который реализует функциональность данного приложения;
  - "Метка" – название электронного ключа;
  - "Свободная память" – объём свободной памяти электронного ключа;
  - "Длина PIN-кода пользователя" – количество символов PIN-кода пользователя приложения;

- "PIN-код пользователя" – статус PIN-кода пользователя приложения: установлен/не установлен;
- "Максимальное число попыток ввода PIN-кода пользователя" – максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя;
- "Число оставшихся попыток ввода PIN-кода пользователя" – 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);
- "Максимальное число попыток ввода PIN-кода администратора" – максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора (только для приложений PKI, PRO, STORAGE);
- "Число оставшихся 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 пользователя" – установленный способ аутентификации пользователя;
- "Способ аутентификации администратора" – установленный способ аутентификации администратора;
- "Поддержка биометрии" – статус поддержки использования биометрии: да/нет;
- "PUK-код" – признак наличия установленного PUK-кода (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Макс. попыток ввода PUK-код" – максимально допустимое количество неверных последовательных попыток ввода PUK-кода (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Осталось попыток ввода PUK-кода" – количество оставшихся попыток ввода PUK-кода;
- "Версия приложения" – номер версии установленного апплета Криптотокен 2 ЭП (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Количество ключевых пар" – количество ключевых пар, хранящихся на токене на текущий момент (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Количество секретных ключей" – количество секретных ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Количество открытых ключей" – количество открытых ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП);
- "Режим предъявления ключа администратора" – установленный режим предъявления ключа администратора (только для приложения ГОСТ);
- "Число разблокировок" – количество успешно выполненных разблокирований PIN-кода пользователя (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП).

6.2 Диагностика целостности приложения

В ходе операции диагностики целостности выполняется проверка контрольной суммы приложения. Операция диагностики целостности предусмотрена для приложения ГОСТ с апплетом Криптотокен 2 ЭП. Для выполнения операции не требуется авторизация в приложении.

Для диагностики приложения ГОСТ:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ с приложением ГОСТ с апплетом Криптотокен 2 ЭП к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

2. Нажмите кнопку "Переключиться в расширенный режим". Будет отображено основное окно Единого Клиента JaCarta в расширенном режиме. Выберите вкладку "ГОСТ" для доступа к операциям приложения ГОСТ с апплетом Криптотокен 2 ЭП.

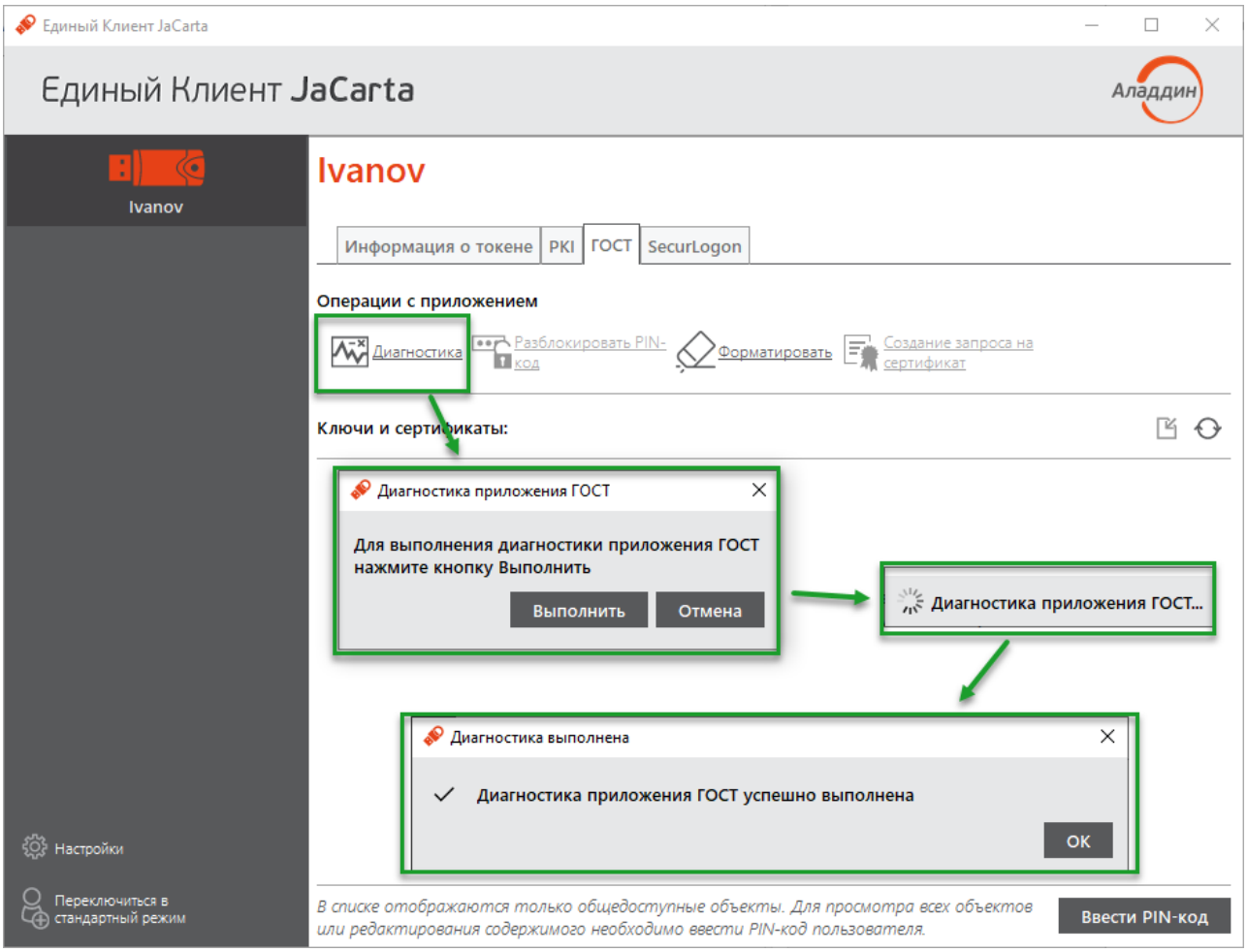


Рисунок 32 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Диагностика..." активна

3. Нажмите кнопку "Диагностика" и подтвердите выполнение диагностики. Будет выполняться диагностика целостности приложения ГОСТ. В случае успешного завершения операции будет отображена информация об этом. Нажмите кнопку "ОК" для закрытия окна.

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:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. Нажмите кнопку "Переключиться в расширенный режим". Будет отображено основное окно Единого Клиента JaCarta в расширенном режиме. Выберите вкладку с наименованием приложения, для которого необходимо создать запрос на сертификат (в данном примере выбрано приложение PKI) и

нажмите кнопку "Создание запроса на сертификат". Кнопка активна при вводе PIN-кода пользователя в данном окне.

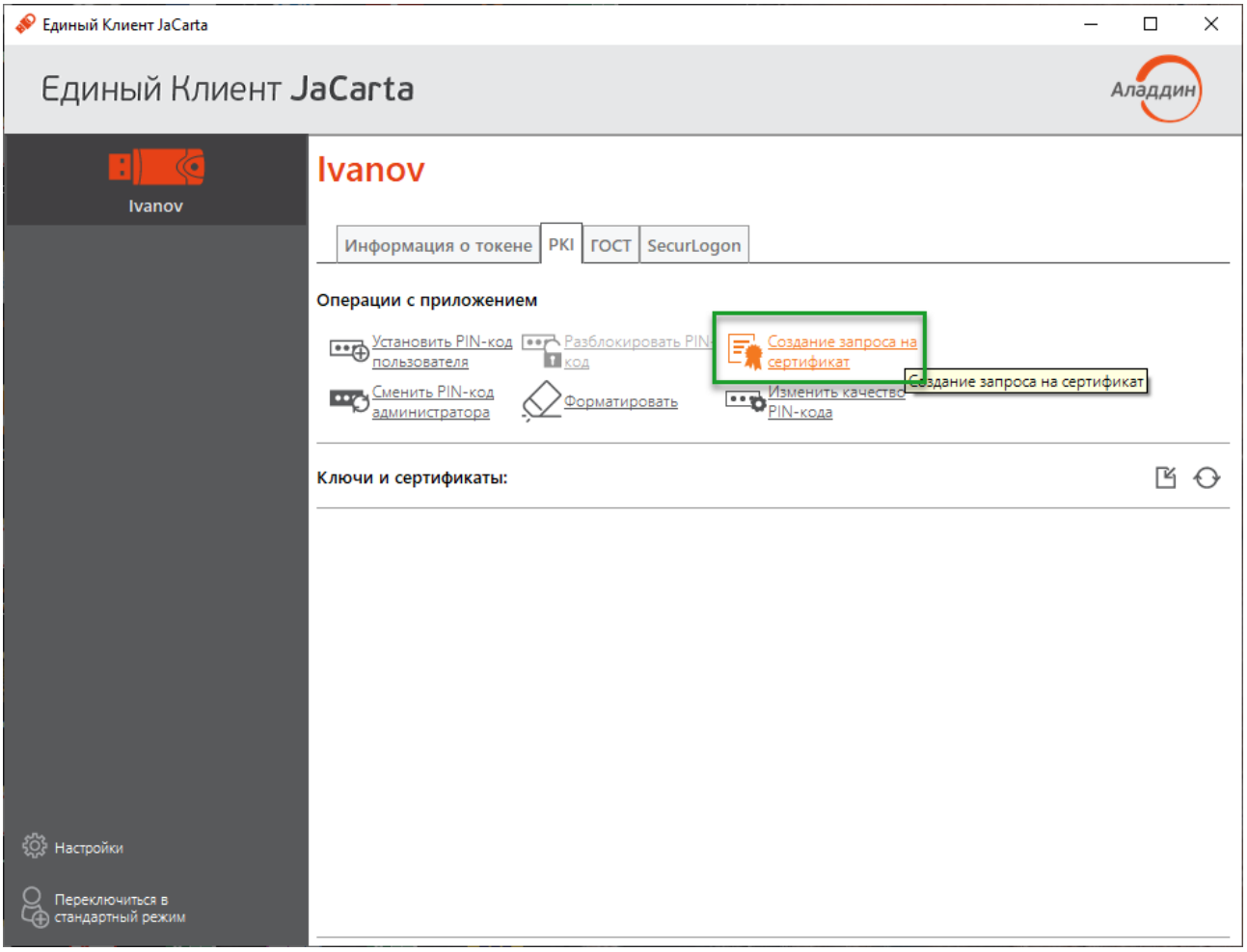


Рисунок 33 – Кнопка "Создание запроса на сертификат"

3. Будет отображено окно "Мастер создания запроса на сертификат" (Рисунок 34). Заполните поля следующим образом:
   - в поле "Имя" введите наименования создаваемого сертификата. Поле является обязательным для заполнения;
   - в раскрывающемся списке "Тип ключевой пары" выберите алгоритм шифрования "RSA" (задан по умолчанию) либо "EC";

– в раскрывающемся списке "Размер ключа" выберите размер открытого ключа. По умолчанию выбрано значение "1024".

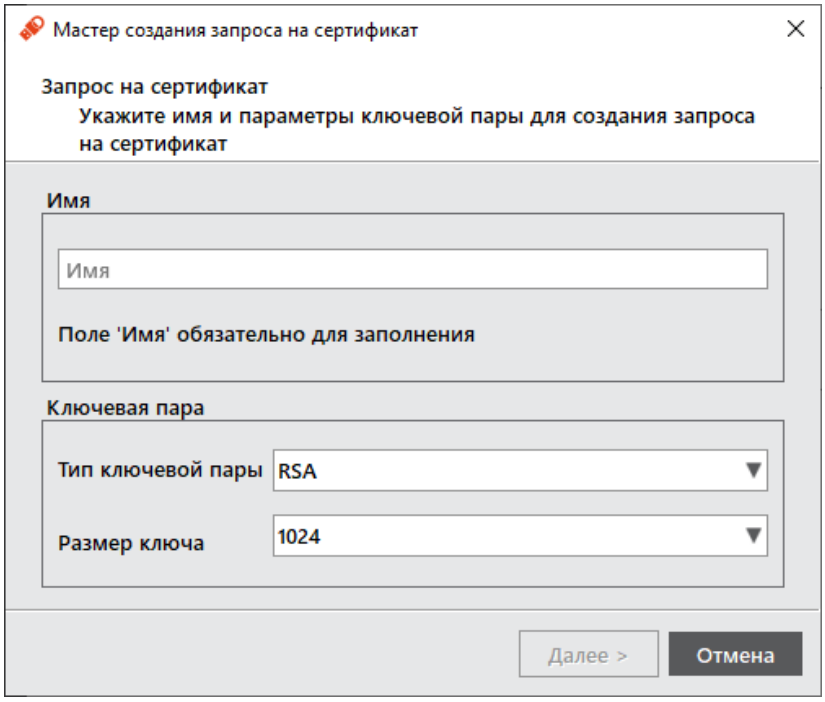


Рисунок 34 – Окно "Мастер создания запроса на сертификат"

4. Нажмите кнопку "Далее". Будет открыто окно для выбора пути сохранения файла запроса на сертификат. При нажатии кнопки "Обзор..." будет открыто окно Проводника Windows для выбора папки сохранения запроса на сертификат. Выберите нужную папку и при желании выберите имя файла, в котором следует сохранить запрос на сертификат. Выберите формат файла для запроса из предложенных (Рисунок 35).

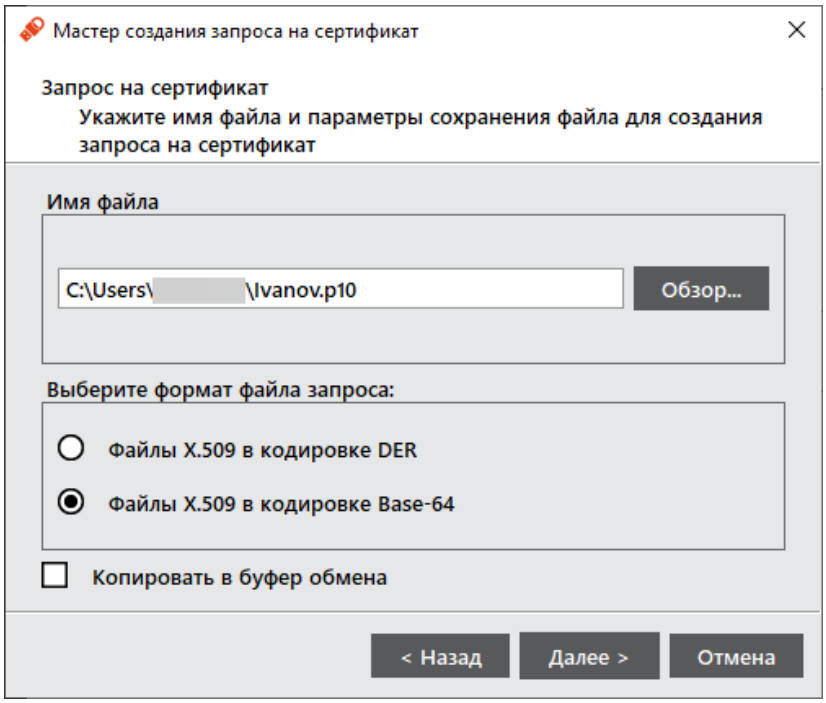


Рисунок 35 – Окно "Мастер создания запроса на сертификат"

5. Нажмите кнопку "Далее". Будет открыто окно выбора опций при создании запроса на сертификат (Рисунок 36). Выберите желаемые опции из списка.

– в поле "Использование ключа" установите 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".

– В поле "Предназначение" установите отметку в нужных полях:

- "Проверка подлинности клиента" (выбрано по умолчанию);
- "Защищённая электронная почта" (выбрано по умолчанию);
- "Проверка подлинности сервера";
- "Подпись кода";
- "Доверенное время".

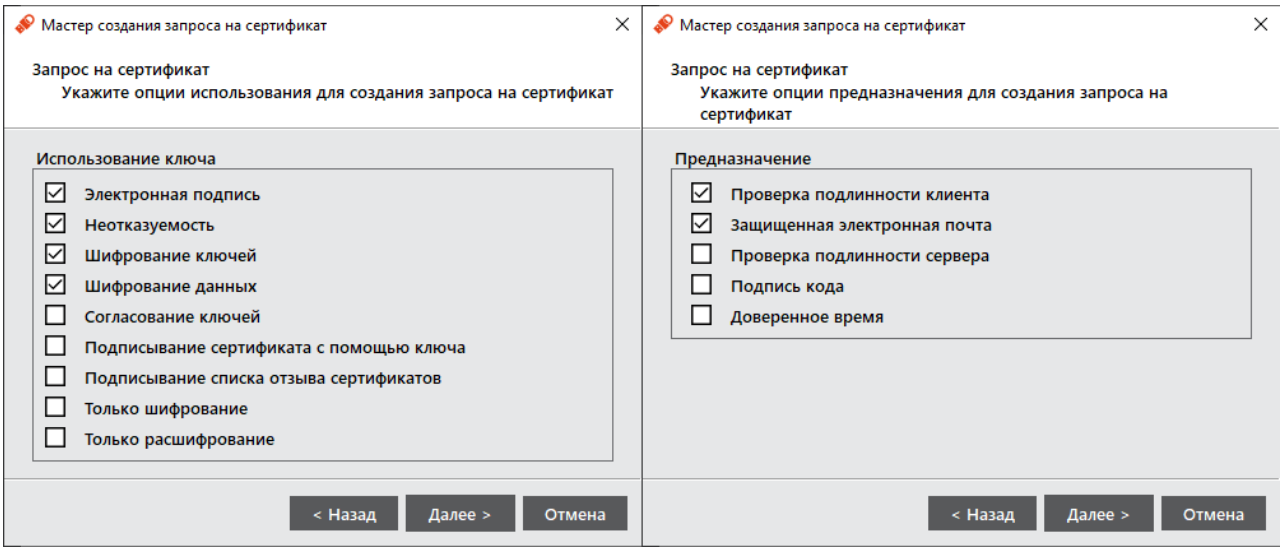


Рисунок 36 – Окна "Мастер создания запроса на сертификат", выбор опций при создании запроса на сертификат

6. Нажмите кнопку "Далее". Будет открыто окно подтверждения выбранных параметров создания запроса на сертификат.

7. Если все заполнено верно, нажмите кнопку "Далее". На экране будет отображаться информация о процессе создания запроса на сертификат. По окончании процесса будет отображено окно с информацией о пути сохранения запроса на сертификат (Рисунок 37).

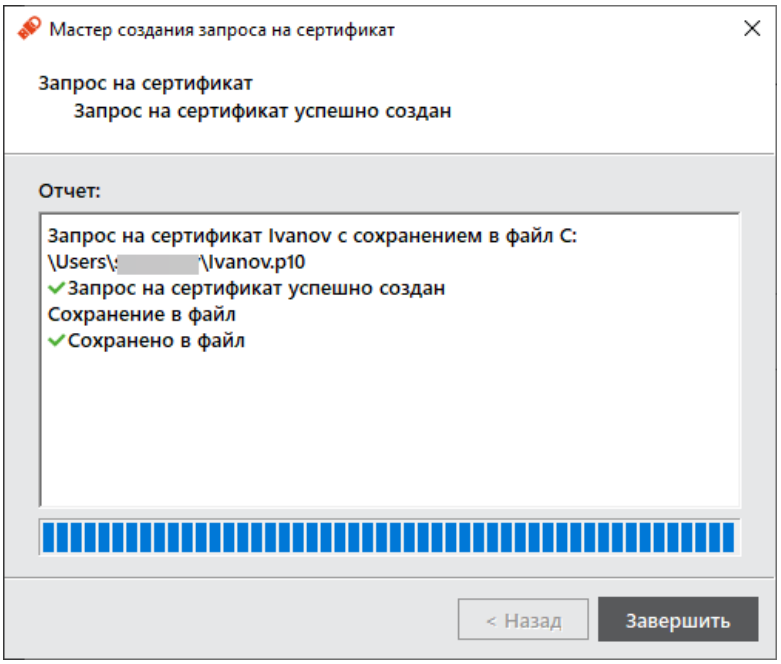


Рисунок 37 – Информация о завершении создания запроса на сертификат

8. Нажмите кнопку "Завершить" для закрытия окна "Мастер 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:

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. Нажмите кнопку "Переключиться в расширенный режим". Будет отображено основное окно Единого Клиента JaCarta в расширенном режиме. Выберите вкладку с наименованием приложения, в которое следует импортировать сертификат (в данном примере выбрано приложение PKI) и нажмите кнопку

"Ввести PIN-код". В появившемся окне с наименованием приложения введите PIN-код пользователя данного приложения:

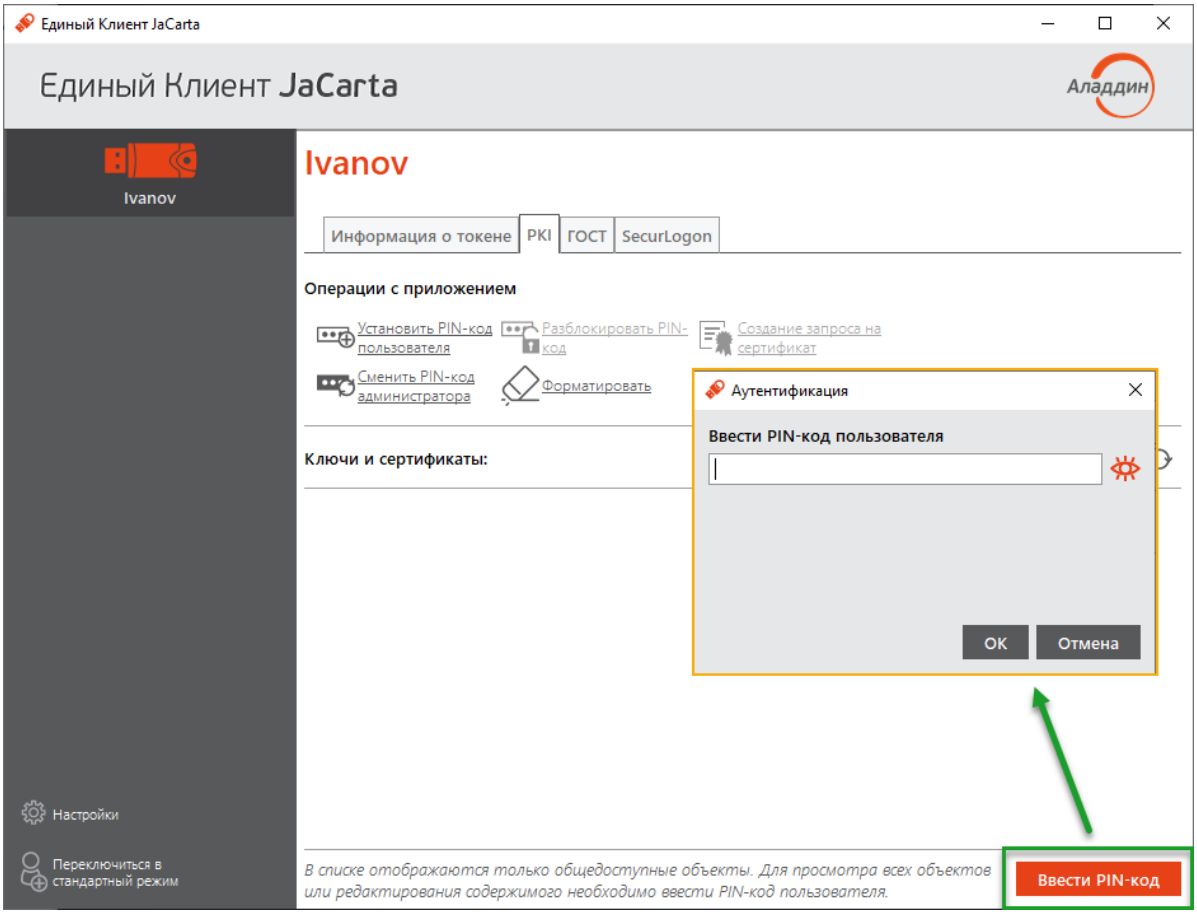


Рисунок 38 – Авторизация в приложении PKI

3. Нажмите кнопку "ОК". 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:

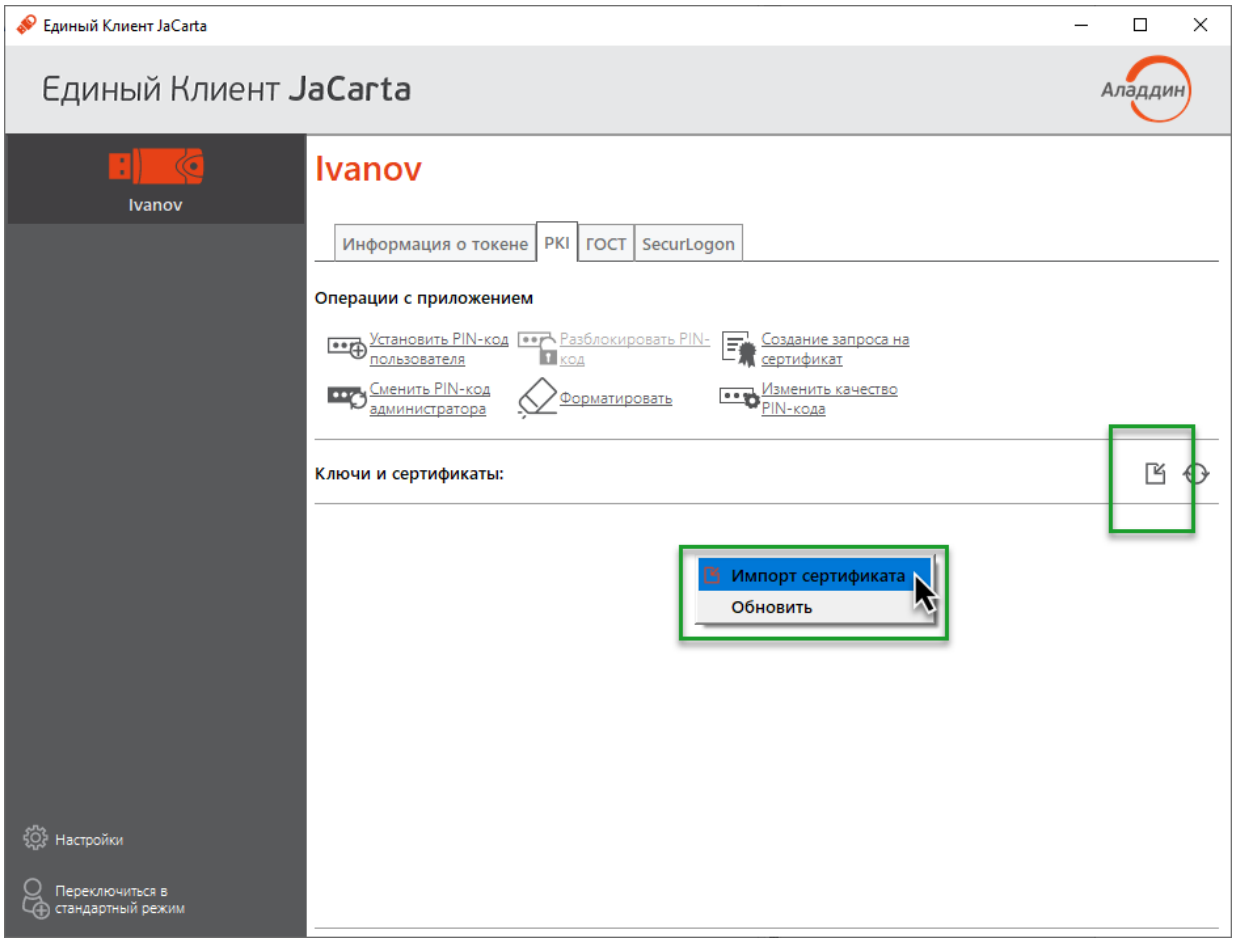


Рисунок 39 – Полный список объектов приложения и команда "Импорт"

4. Нажмите кнопку или вызовите контекстное меню в поле "Ключи и сертификаты "и выберите команду "Импорт". Будет отображено окно для импорта сертификата. Заполните поля следующим образом:
   – в поле "Путь к файлу импортируемых данных" укажите путь к импортируемому сертификату. Для этого нажмите кнопку "Обзор..." и в появившемся окне Проводника Windows выберите файл сертификата;

– в поле "Имя контейнера " установите отметку, чтобы вручную задать имя контейнера, в который будет импортирован сертификат. В поле ниже введите имя контейнера. Если отметка не установлена, то имя контейнера будет сгенерировано автоматически.

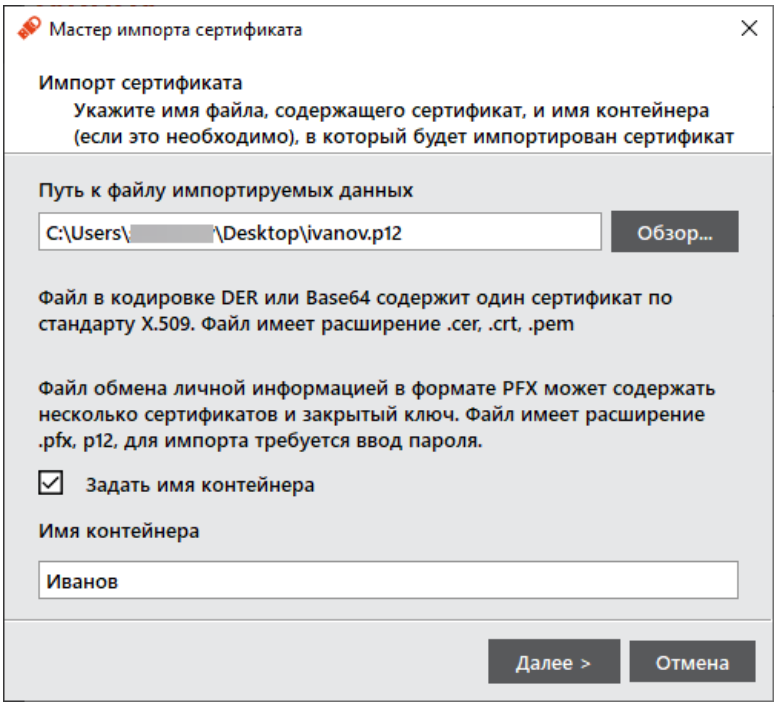


Рисунок 40 – Окно "Импорт сертификата или контейнера"

5. Нажмите кнопку "Далее". Если импортируемый сертификат содержит защищённый паролем закрытый ключ, то введите его в открывшемся окне;
6. При нажатии кнопки "Далее" Будет выполняться импорт сертификата в память приложения электронного ключа. По окончанию операции на экране появится сообщение об этом:

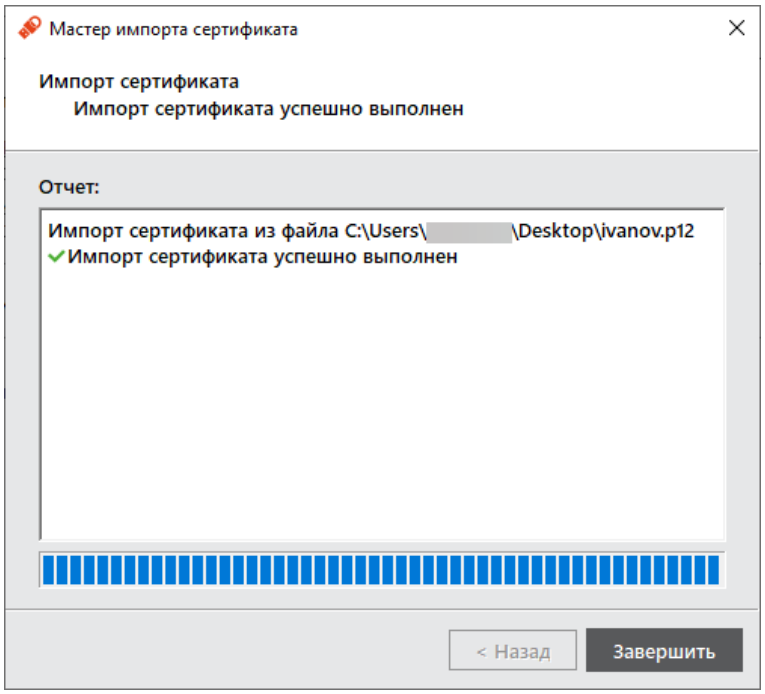


Рисунок 41 – Окно "Импорт сертификата или контейнера"

7. Нажмите кнопку "ОК" для закрытия окна сообщения. Импортированные объекты будут отображены в поле "Ключи и сертификаты", а также станут доступны кнопки для выполнения операций над объектом:

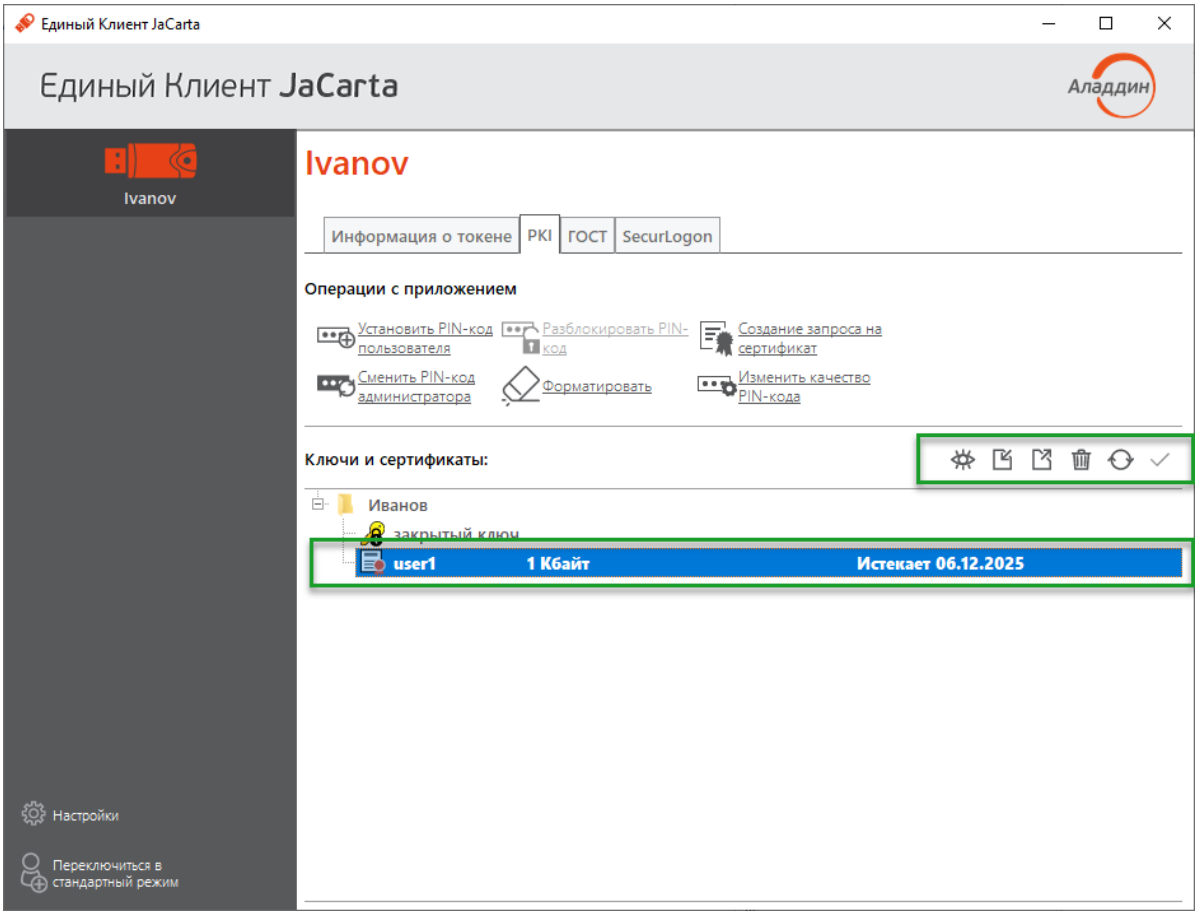


Рисунок 42 - Отображение импортированных объектов

6.3.3 Экспорт сертификата

Для экспорта сертификата в файл:

1. Авторизуйтесь 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" выберите экспортируемый объект и нажмите кнопку  или активируйте команду "Экспорт в файл" контекстного меню объекта:

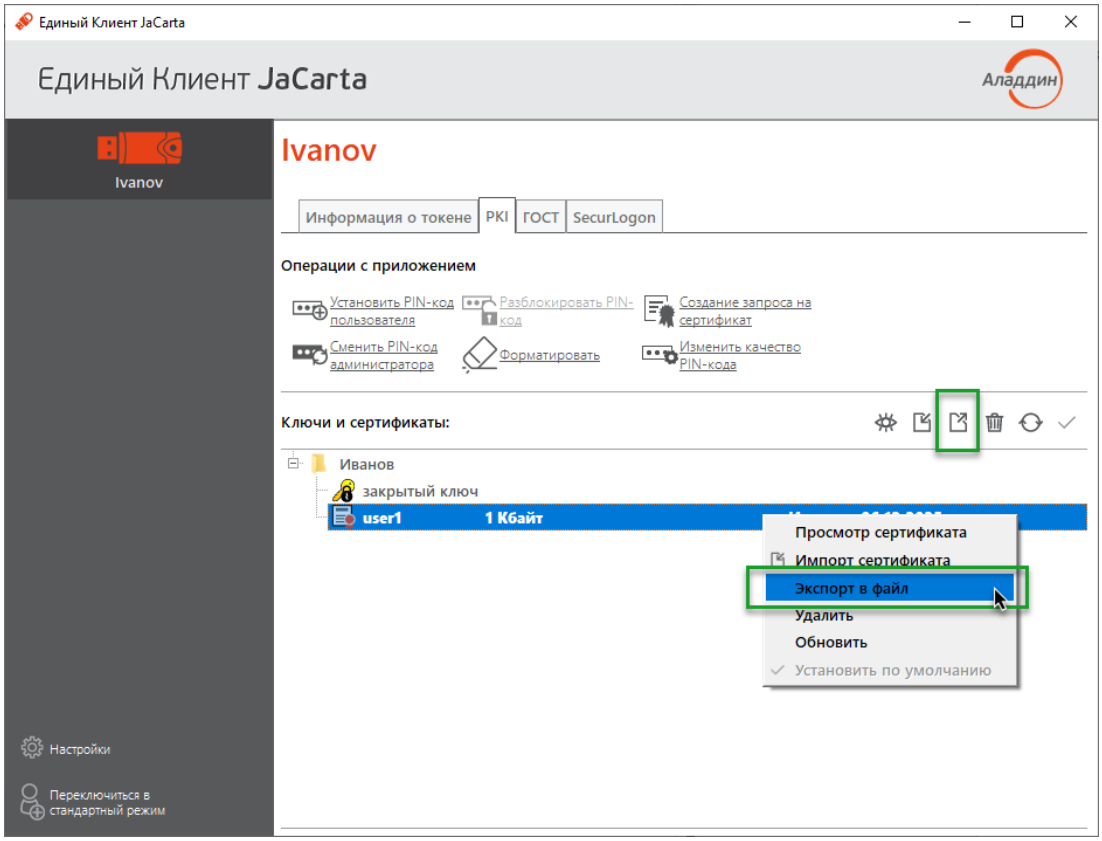


Рисунок 43 – Экспорт данных Единый Клиент JaCarta. Кнопки перехода к экспорту данных

2. Будет открыто окно для указания параметров экспорта сертификата (см. рисунок 44). Заполните поля следующим образом:
   - в поле "Путь к файлу для экспорта" укажите путь и имя файла для экспорта файла. Для этого нажмите кнопку "Обзор..." и в появившемся окне Проводника Windows выберите нужную папку.

Выберите необходимый тип файла для экспорта (по умолчанию выбран тип "Файл в формате Base64").

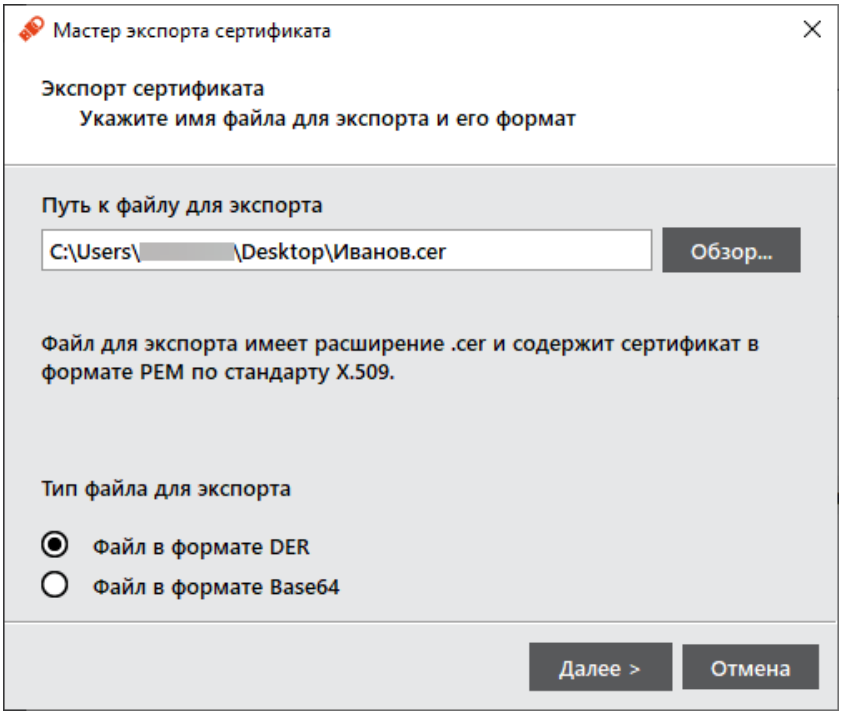


Рисунок 44 – Окно "Экспорт сертификата"

3. Нажмите кнопку "Далее". Будет выполняться экспорт выбранного объекта. Будет отображен результат выполнения операции. Нажмите кнопку "Завершить" для выхода из мастера экспорта сертификата.

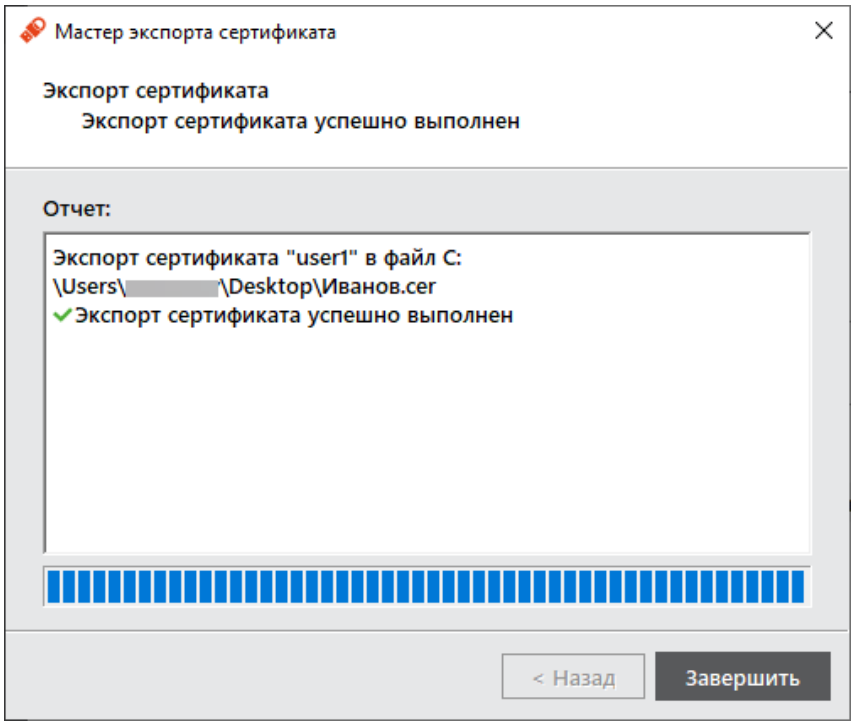


Рисунок 45 – Окно результатов экспорта

6.3.4 Просмотр сертификата

Для просмотра сертификата:

1. Авторизуйтесь в приложении электронного ключа, в котором необходимо просмотреть сертификат (см. п.п. 1-3 процедуры импорта сертификата в п. 6.3.2). В поле "Ключи и сертификаты" выберите сертификат и нажмите кнопку  или активируйте команду "Просмотр сертификата" в контекстном меню выбранного сертификата:

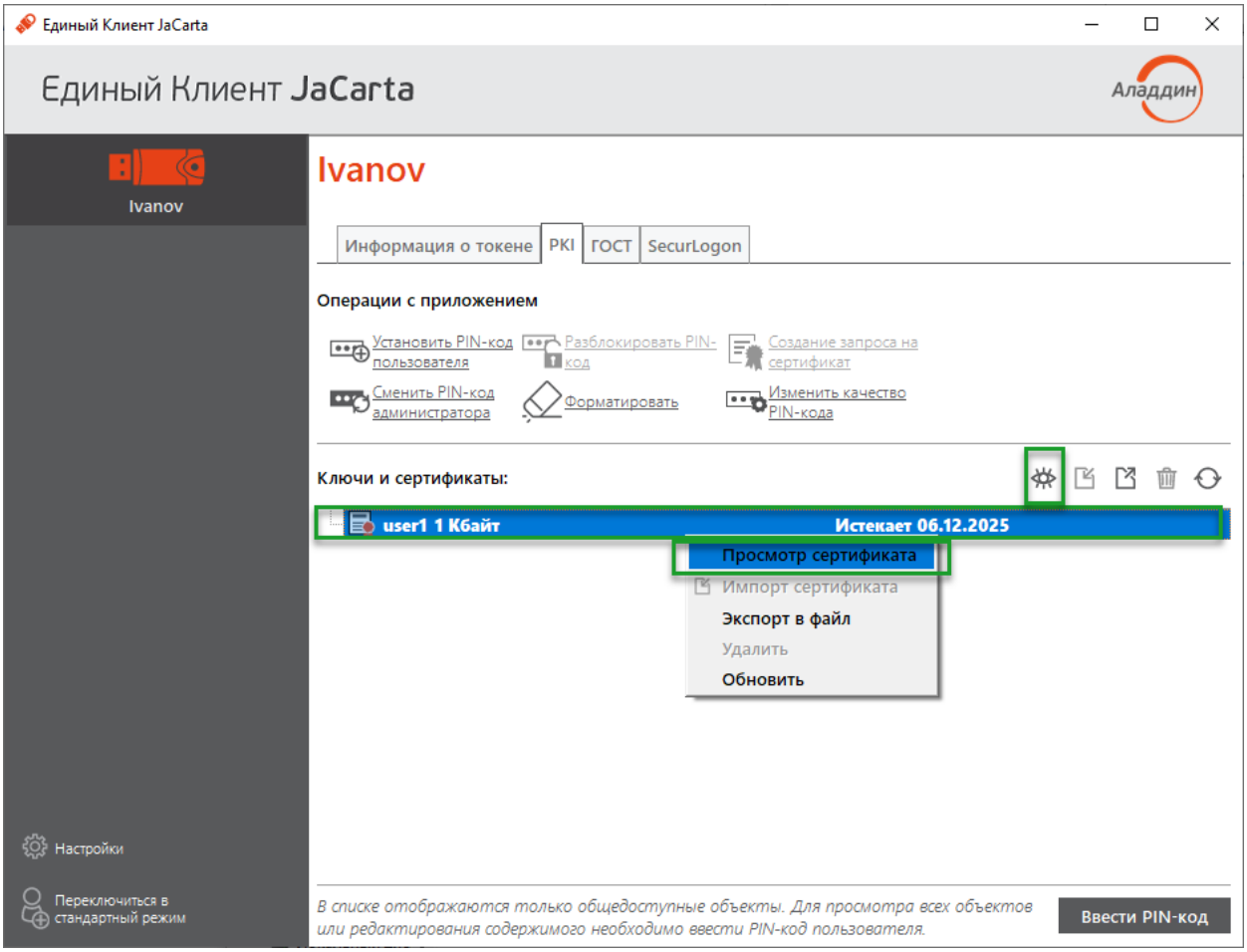


Рисунок 46 - Кнопки перехода к просмотру сертификата

2. Будет открыто окно, содержащее сведения о выбранном сертификате:

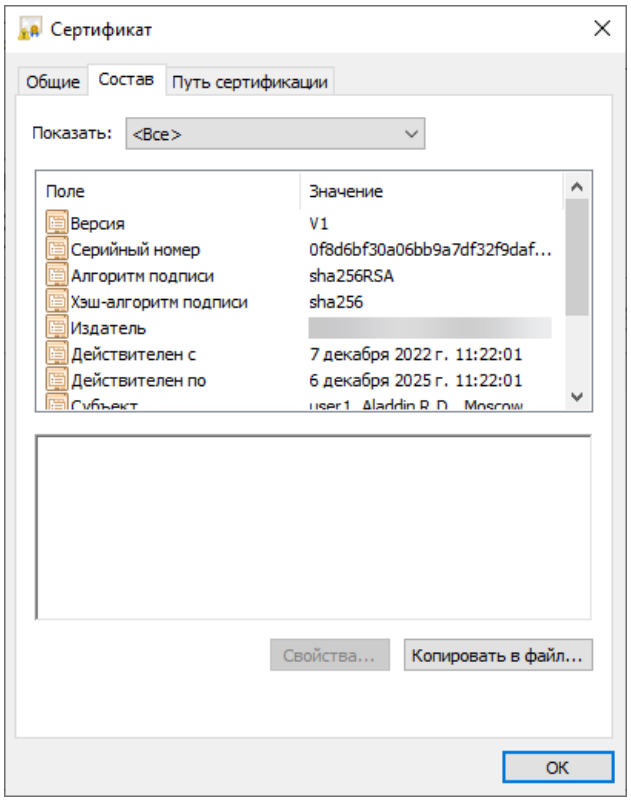


Рисунок 47 – Окно просмотра сертификата

3. Для выхода из окна просмотра нажмите кнопку "OK".

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. Запустите Единый Клиент JaCarta и подключите электронный ключ к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

2. Нажмите кнопку "Переключиться в расширенный режим" и выберите вкладку с наименованием нужного приложения. В поле "Ключи и сертификаты" будет отображен список общедоступных объектов, хранящихся в памяти электронного ключа (см. рисунок 48).

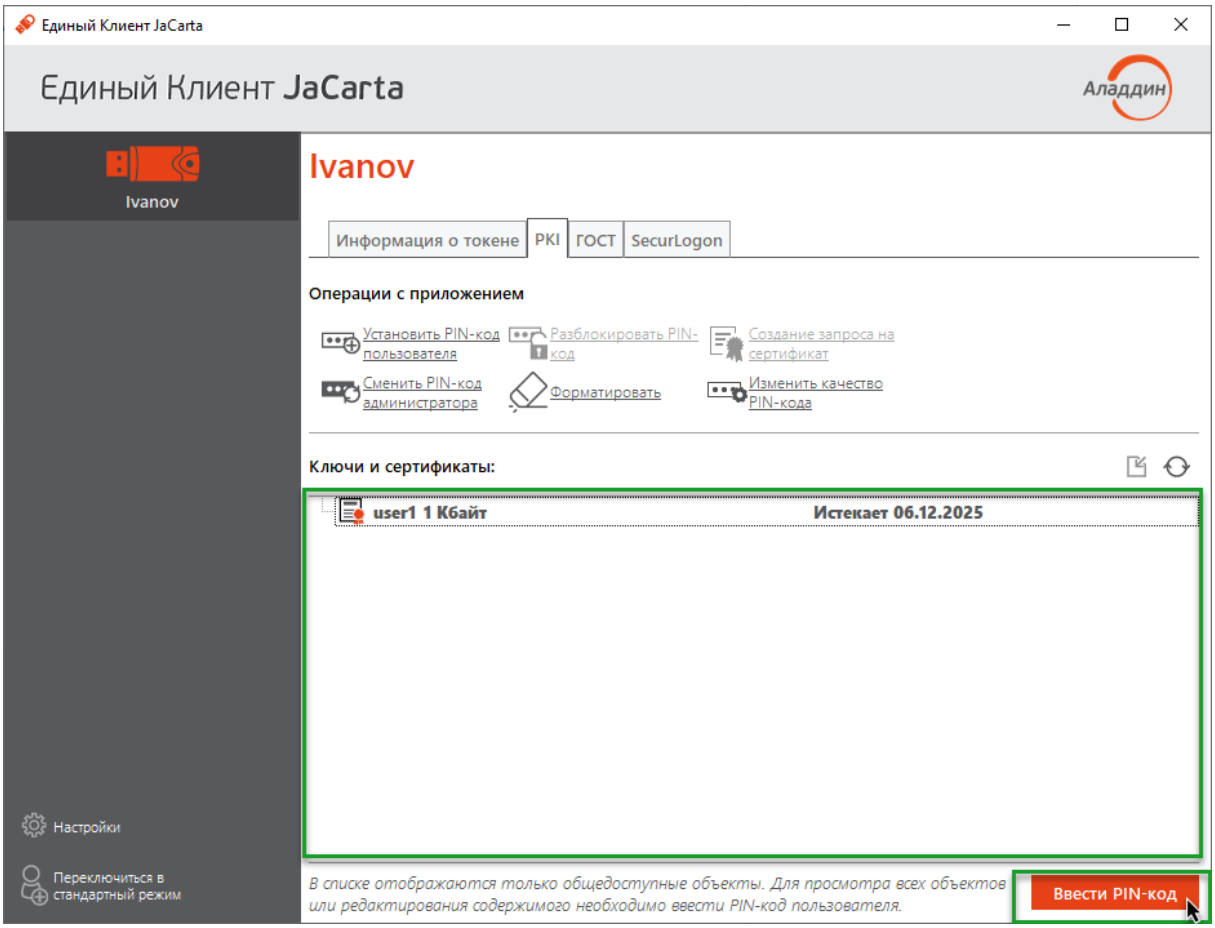


Рисунок 48 - Список общедоступных объектов в памяти электронного ключа

3. Нажмите кнопку "Ввести PIN-код", в появившемся окне "Авторизация" введите PIN-код пользователя для выбранного приложения:

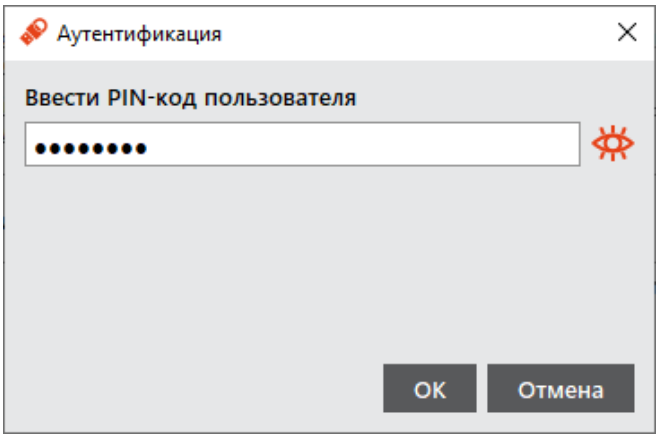


Рисунок 49 – Окно аутентификации в приложении электронного ключа

4. После успешной авторизации будет доступен для просмотра полный список объектов, а также появятся кнопки для управления объектами:

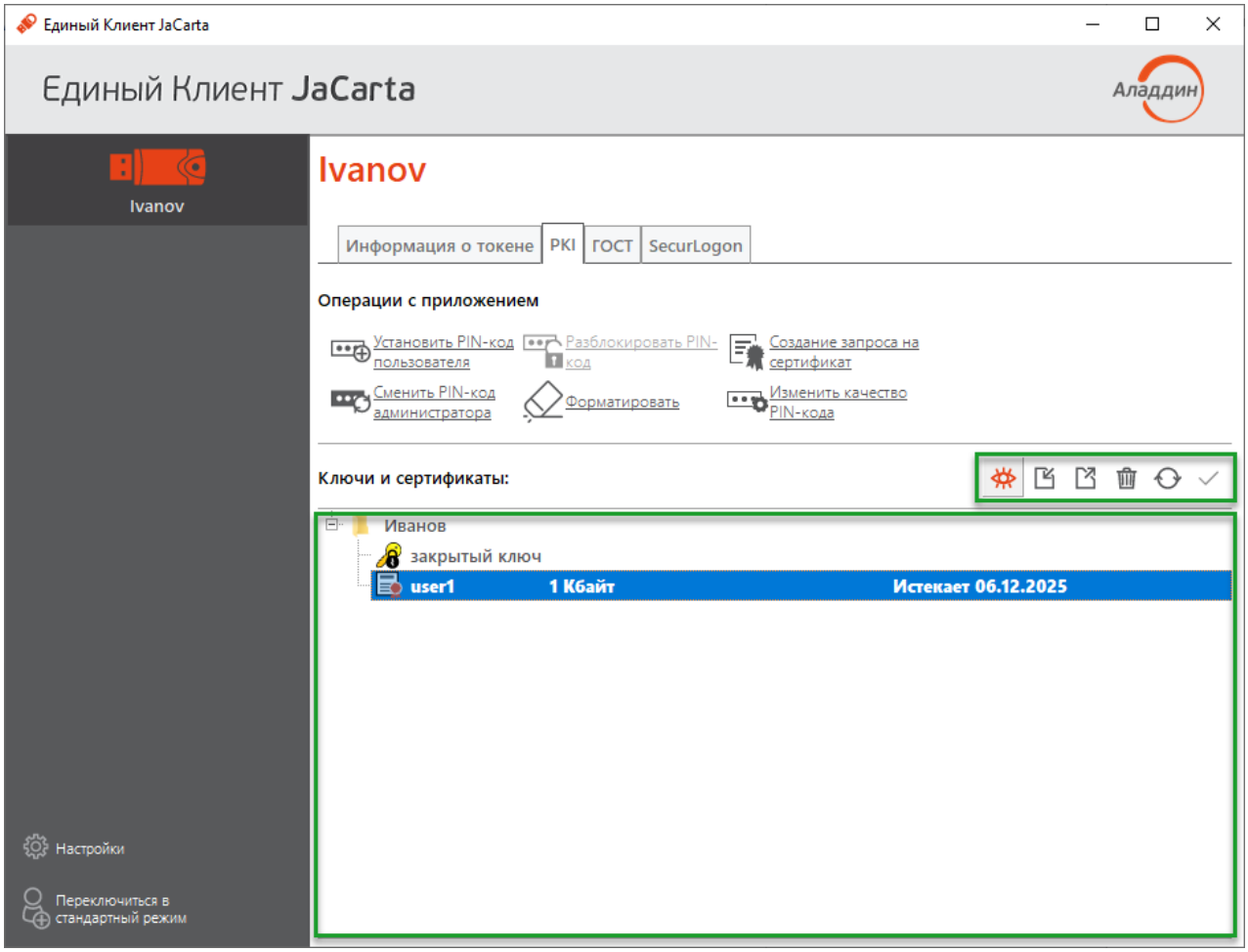


Рисунок 50 – Полный список объектов в памяти электронного ключа

6.4.2 Удаление объектов

Для удаления объекта:

1. Авторизуйтесь в приложении электронного ключа, из которого необходимо удалить объект. В поле "Ключи и сертификаты" выберите удаляемый объект и нажмите кнопку или активируйте команду "Удалить" контекстного меню объекта:

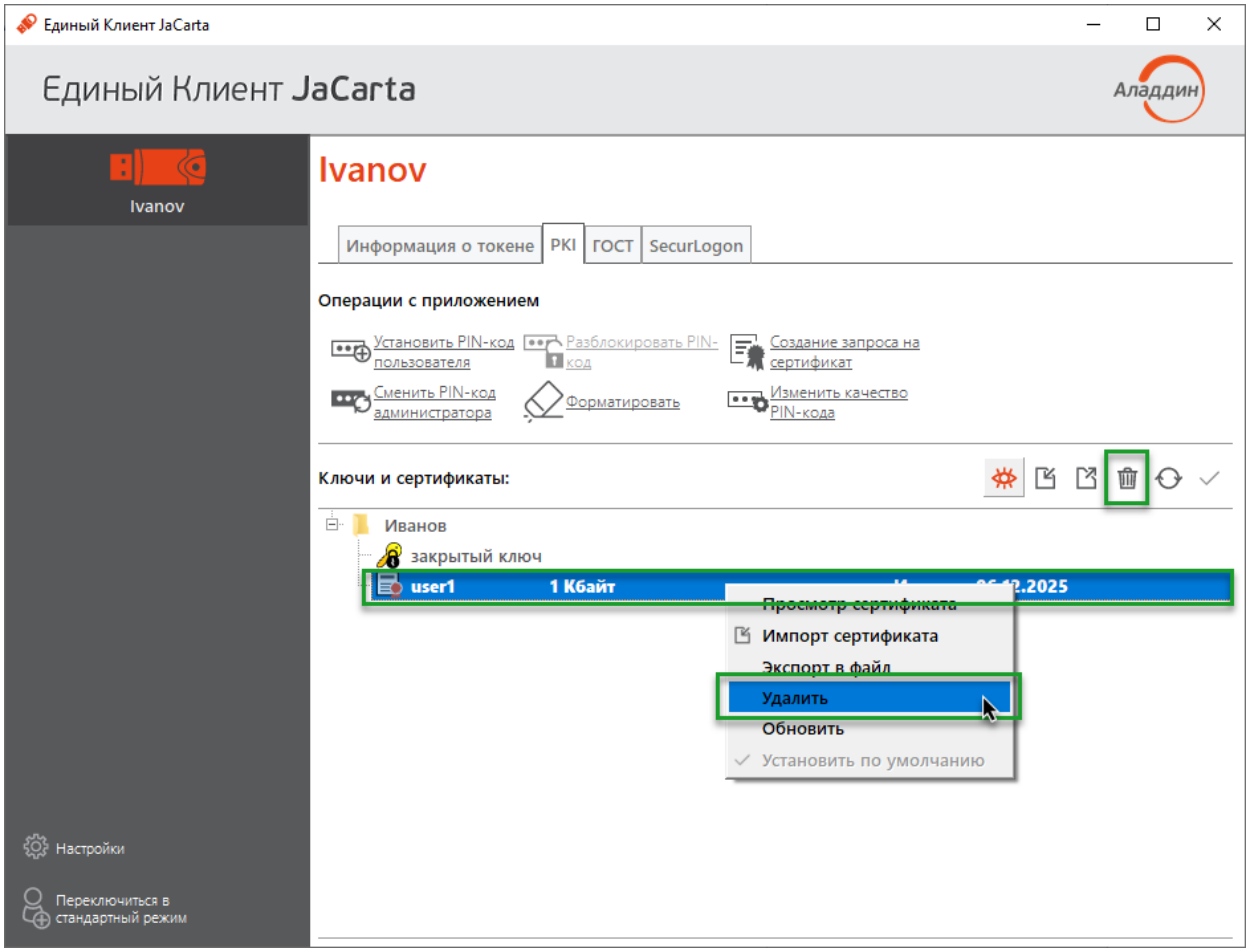


Рисунок 51 - Кнопки перехода к удалению данных

2. Будет открыто окно для подтверждения удаления:

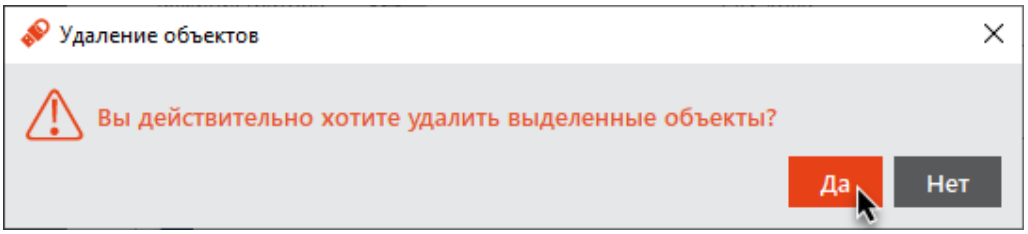


Рисунок 52 - Окно "Удаление объектов"

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

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

Внешний вид электронного ключа JaCarta WebPass приведен ниже (см. Рисунок 53).

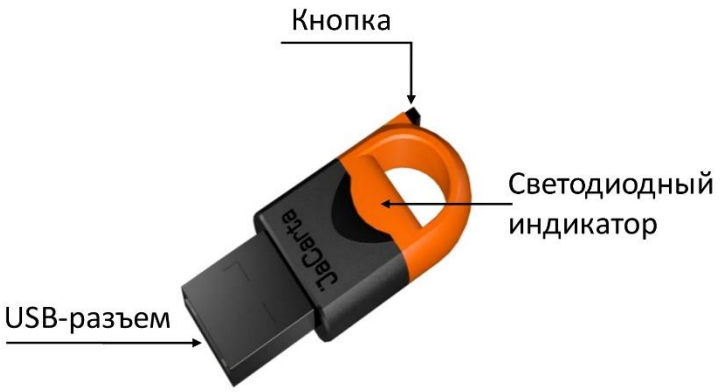


Рисунок 53 - Внешний вид электронного ключа JaCarta WebPass

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 53).

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 обра- зом, необходимо знать соответствие: **№слота – Тип слота – Способ нажатия**.

Слот – набор данных и параметров, хранящихся на электронном ключе и необходимых для генерации па- роля 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 пользовате- лем 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 защищен- ного ресурса);
- Очистка слота.

7.1 Начало работы

Для начала работы подключите 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 ниже (см. Рисунок 54).

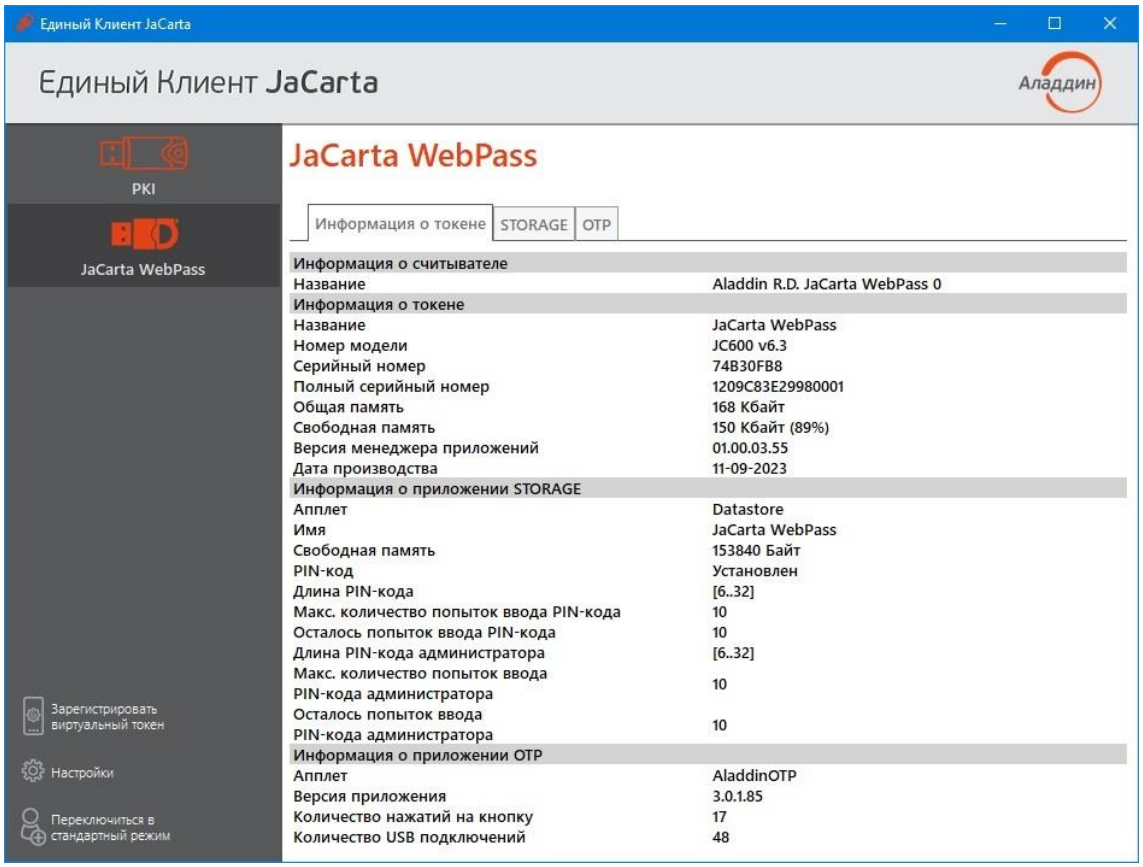


Рисунок 54 – Единого Клиента JaCarta с подключенным электронным ключом JaCarta WebPass

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:

1. Подключите электронный ключ к USB-порту. В основном окне утилиты перейдите к вкладке "OTP" и нажмите кнопку "Сменить PIN-код". Будет отображено одноименное окно (см. Рисунок 55);

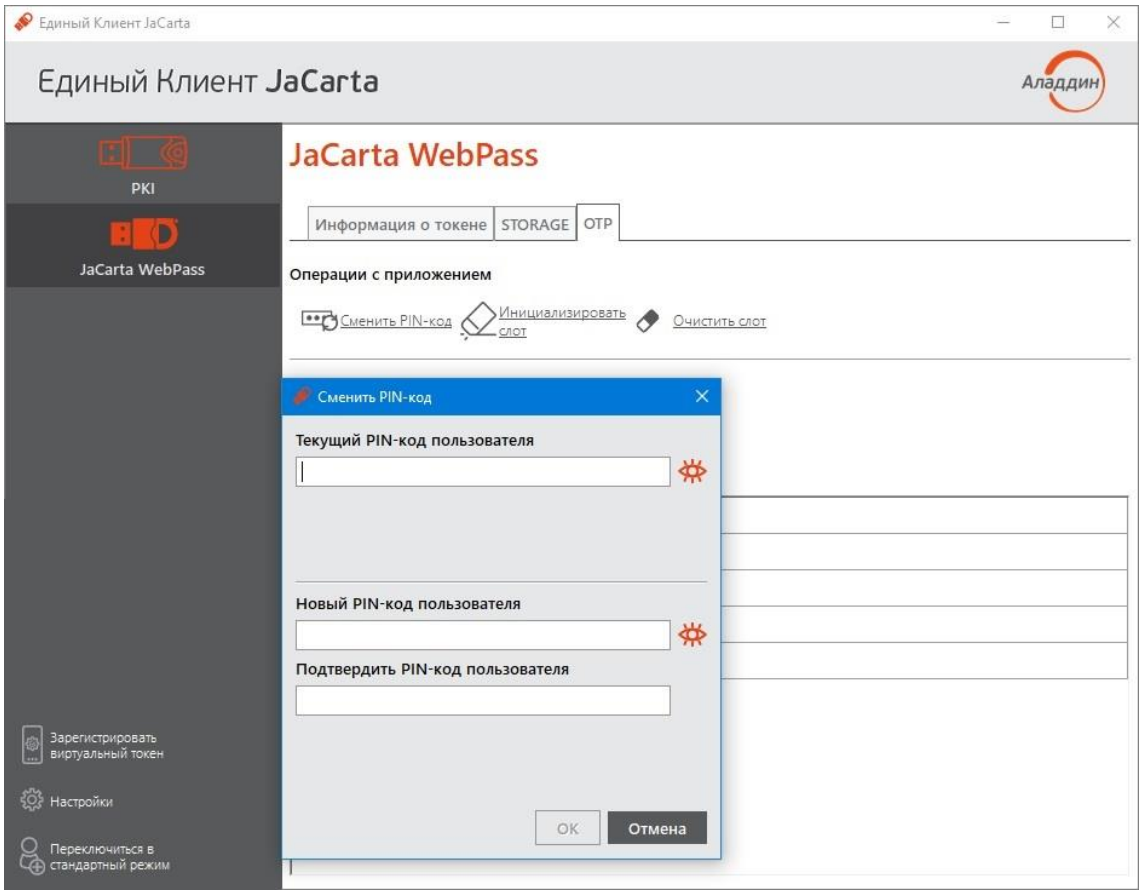


Рисунок 55 - Вызов окна "Смена PIN-кода"

2. В окне "Сменить PIN-код" введите текущий PIN-код, после введите новый PIN-код и подтвердите его, затем нажмите кнопку "OK". PIN-код электронного ключа будет изменен. На экране будет отображено окно с информацией об этом (см. Рисунок 56);

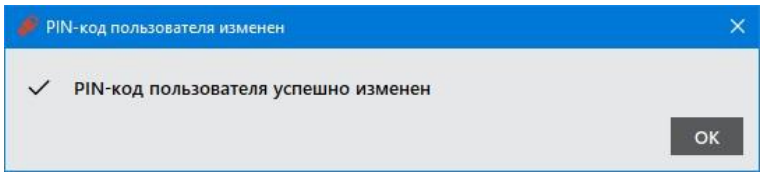


Рисунок 56 - Сообщение об успешной смене PIN-кода

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

7.2.2 Просмотр сведений о слотах

Для просмотра информации о слоте:

1. Подключите электронный ключ к USB-порту. В основном окне перейдите к вкладе "OTP" и выберите нужный слот. В нижней части окна будет отображена информация о параметрах инициализации и способе использования слота.
   Ниже (см.) приведен вид вкладки "OTP" по умолчанию (т.е. ни один из слотов не инициализирован) с выбранным слотом 1.

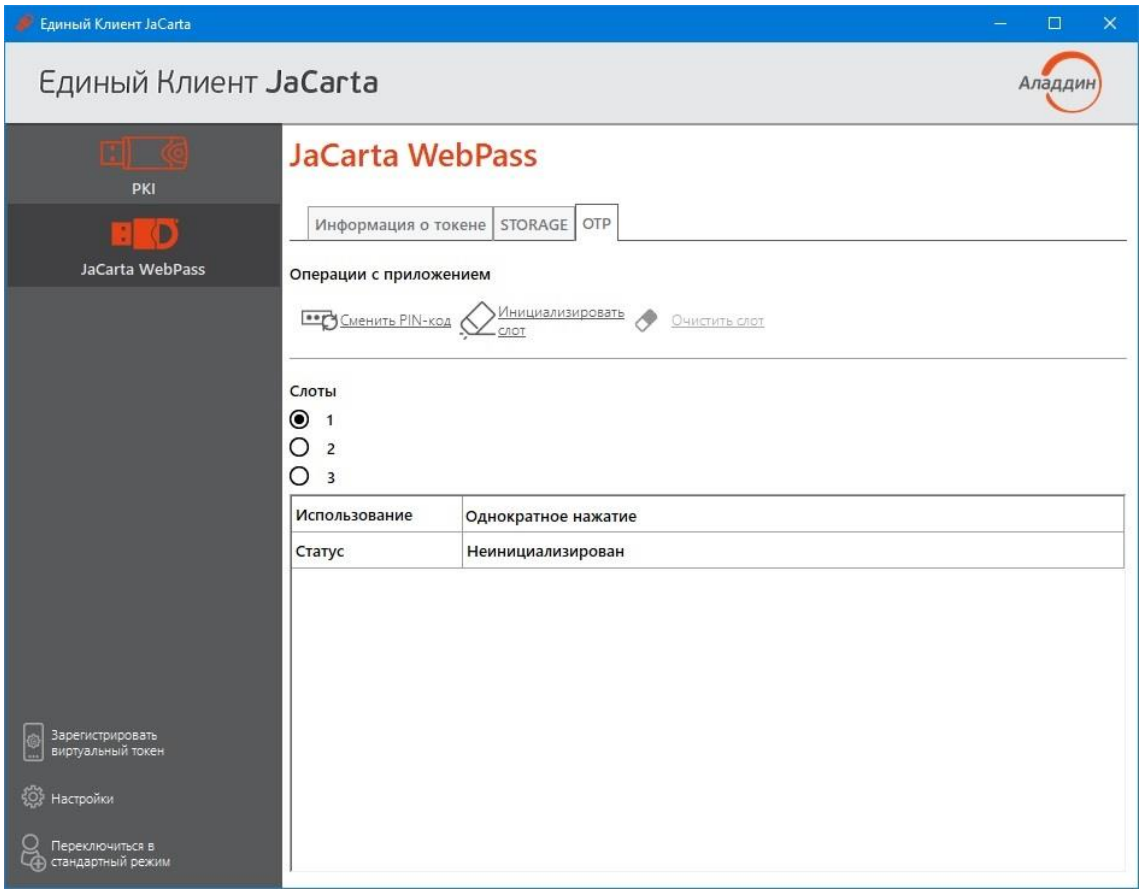


Рисунок 57 - Вкладка "OTP", просмотр информации о слоте 1 (ни один из слотов не инициализирован)

На Рисунок 58 приведен вид вкладки "OTP" с инициализированными слотами 1, 2, 3 с выбранным слотом 3.

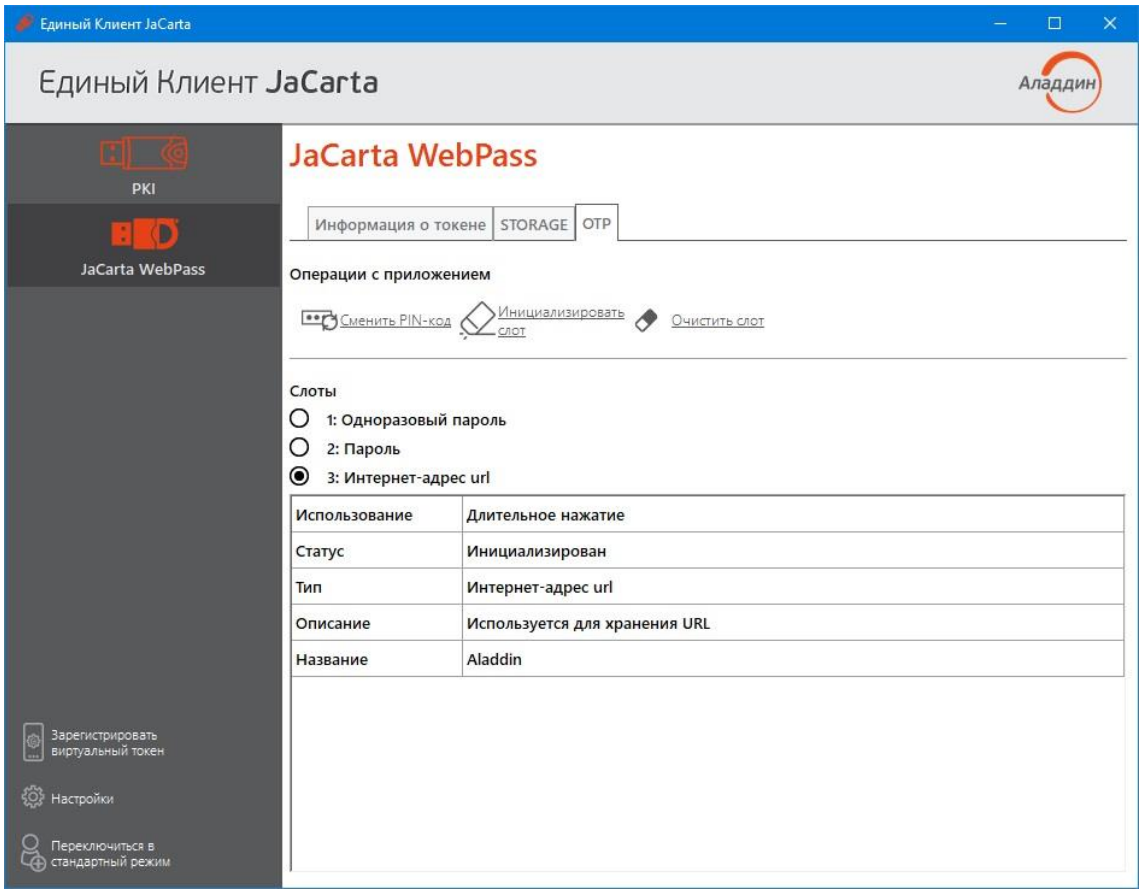


Рисунок 58 - Вкладка "OTP", просмотр информации о слоте 3 (все слоты инициализированы)

Ниже (см. Таблица 4Таблица 4) приведено описание полей, в которых отображается информация о слотах.

Таблица 4 - 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"
Поле "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" – 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

7.2.3 Управление слотами

В слот электронного ключа JaCarta WebPass можно записать 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. 7.2.3.4) и повторной инициализации слота. При повторной инициализации данные, записанные в ходе предыдущей инициализации, удаляются и заменяются новыми данными.

7.2.3.1 Инициализация слота типом "Одноразовый пароль"

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

Для инициализации слота типом "Одноразовый пароль":

1. На вкладке "OTP" выберите тот слот, в который необходимо записать одноразовый пароль и нажмите кнопку "Инициализировать слот" (см. Рисунок 59);

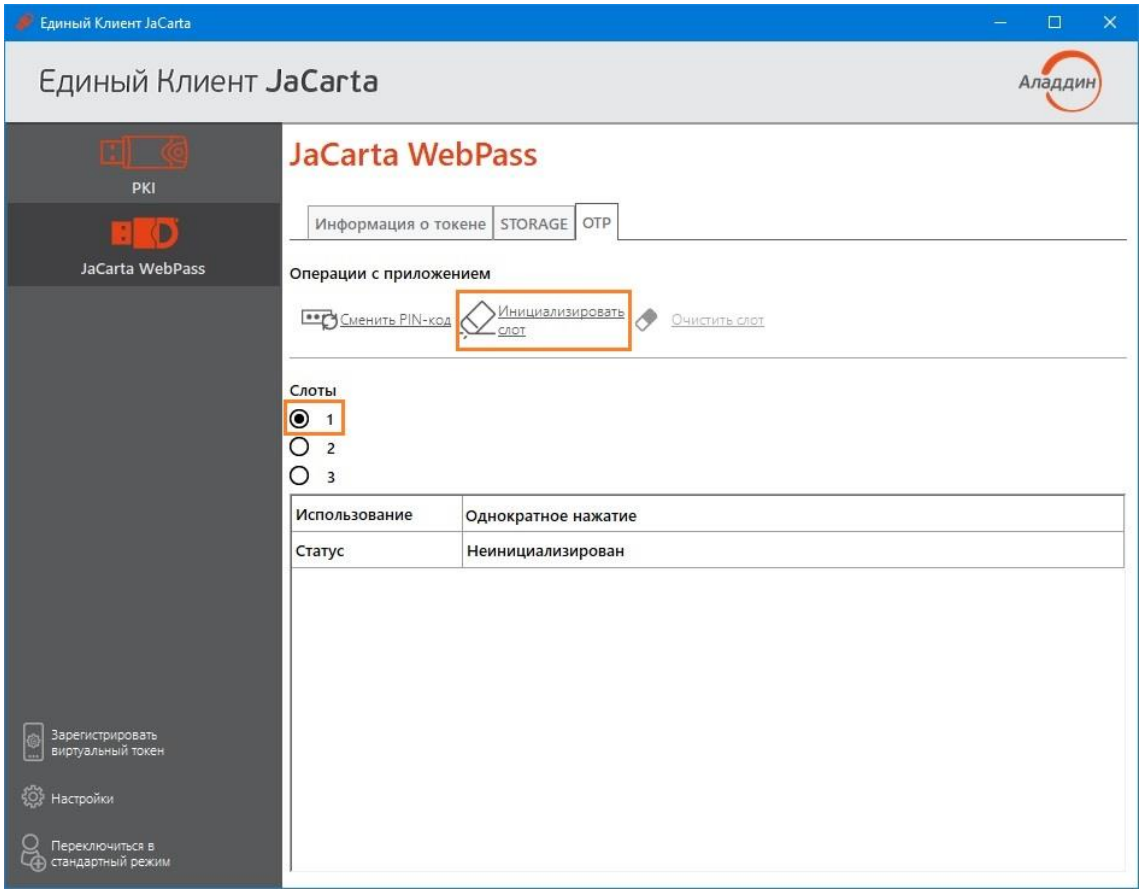


Рисунок 59 - Вкладка "OTP", выбора слота 1 для инициализации типом "Одноразовый пароль"

2. Будет открыто стартовое окно Мастер инициализации слота (см. Рисунок 60).

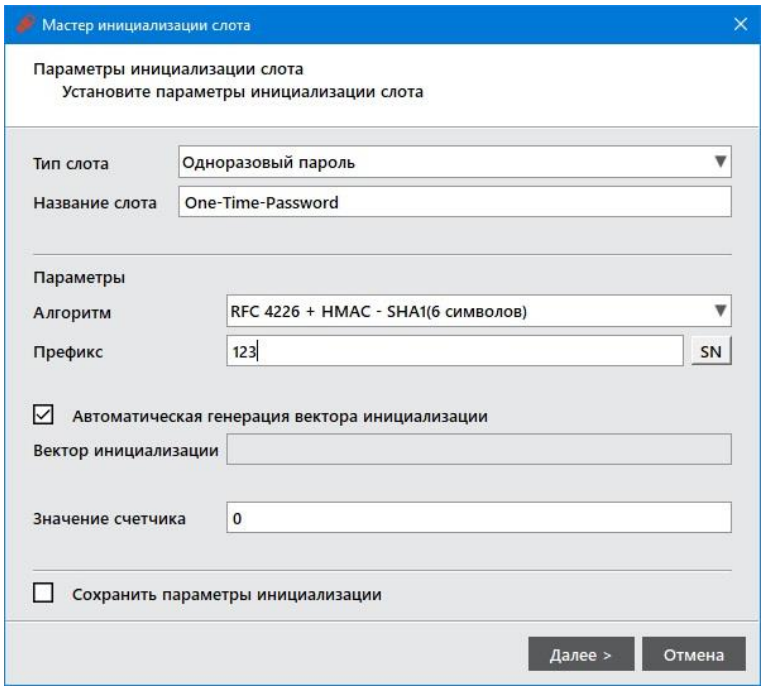


Рисунок 60 - Инициализация слота типом "Одноразовый пароль"

Заполните поля в Мастере инициализации слота в соответсвии со следующим описанием:

– в поле "Тип слота" выбрать в выпадающем списке значение "Одноразовый пароль";
– в поле "Название слота" введите название слота. Длина поля не должна превышать 32 символа;
– в поле "Алгоритм" из выпадающего 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 указать префикс – дополнительное постоянное значение, которое будет автоматически подставляться перед значением одноразового пароля. Таким образом, итоговое значение подставляемого пароля будет содержать больше символов, чем значение одноразового пароля. Для ввода префикса:
  - введите нужное значение с клавиатуры (не более 32-х символов);
  - нажмите кнопку SN для автоматической вставки серийного номера электронного ключа в качестве префикса;
– выберите опцию "Автоматическая генерация вектора инициализации" или введите последовательность из 20 символов в поле "Вектор инициализации";
– в поле "Значение счетчика" введите значение счетчика генераций;
– выберите опцию "Сохранить параметры инициализации" для сохранения введенных настроек инициализации для последующих инициализаций других слотов.

Нажмите кнопку "Далее";

3. В окне "Сохранение файла конфигурации" (см. Рисунок 61) при необходимости укажите формат и имя файла, в который будут сохранены результаты инициализации слота.

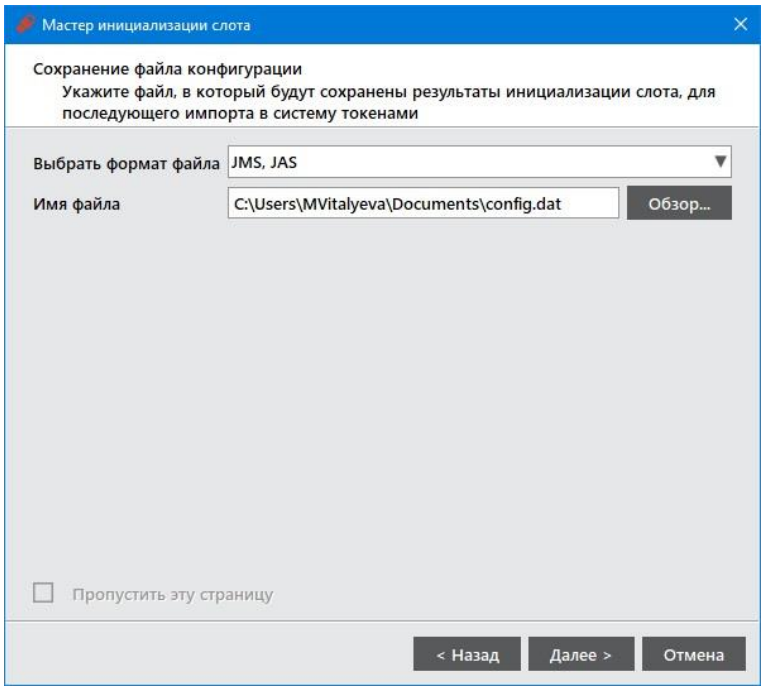


Рисунок 61 - Инициализация слота типом "Одноразовый пароль". Сохранение файла конфигурации

*Для регистрации электронного ключа JaCarta WebPass в системах JMS/JAS необходимо создать конфигурационный файл с информацией о результатах инициализации слота на данном электронном ключе. Конфигурационный файл представляет собой файл с расширением *.xml или *.dat и используется для поддержки работы электронного ключа в системах JMS/JAS.*

- в поле "Выбрать формат файла" выбрать в выпадающем списке формат конфигурационного файла из предлагаемых значений - "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 введите его имя и нажмите "Сохранить".

Нажмите кнопку "Далее".

4. На следующем шаге введите PIN-код электронного ключа в одноименное поле (см. Рисунок 62). После нажмите кнопку "Далее".

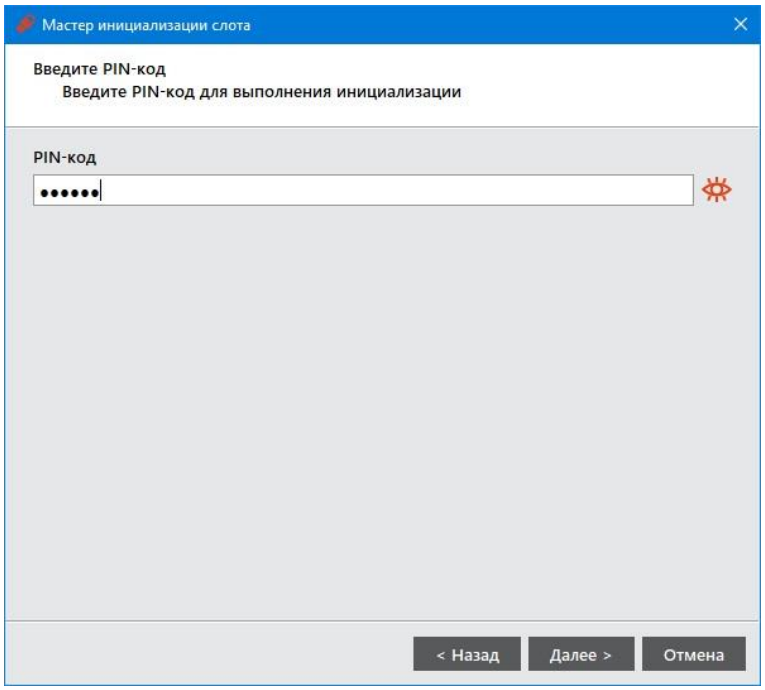


Рисунок 62 - Инициализация слота типом "Одноразовый пароль". Ввод PIN-кода

5. Далее будет отображаться настройки, установленные на предыдущих шагах, с которыми будет проходить процесс инициализации (см. Рисунок 63). Если все настройки указаны верно, нажмите кнопку кнопку "Выполнить" для запуска инициализации.

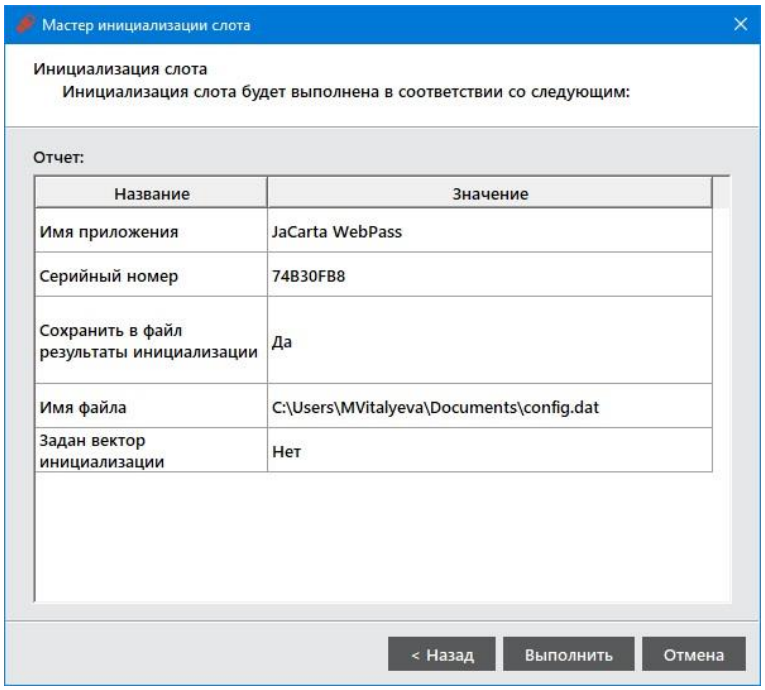


Рисунок 63 - Инициализация слота типом "Одноразовый пароль". Заданные настройки

6. Будет отображен отчет по выполненной инициализации (см. Рисунок 64). Для закрытия окна нажать кнопку "Завершить".

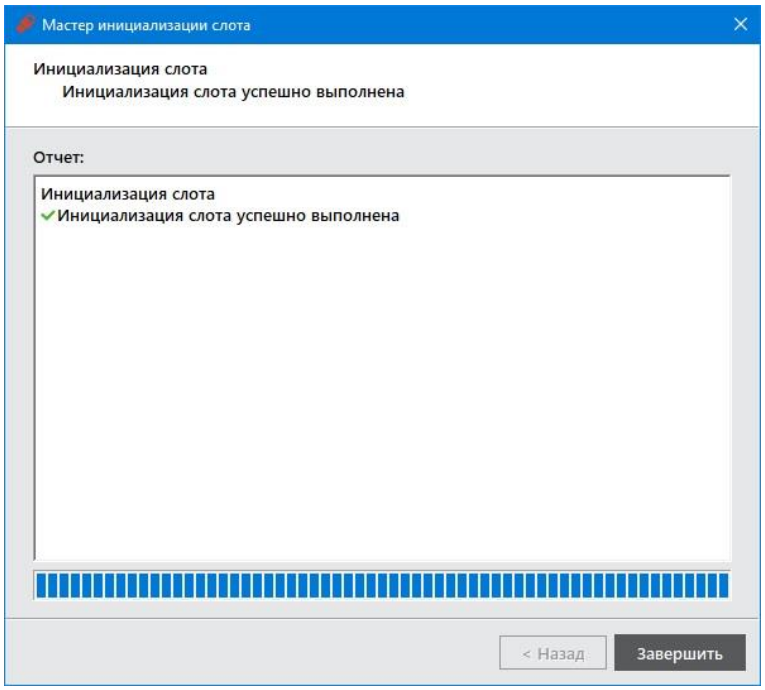


Рисунок 64 - Завершение инициализации слота

7. Окно Мастера инициализиции слота будет закрыто. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Одноразовый пароль" (см. Рисунок 65).

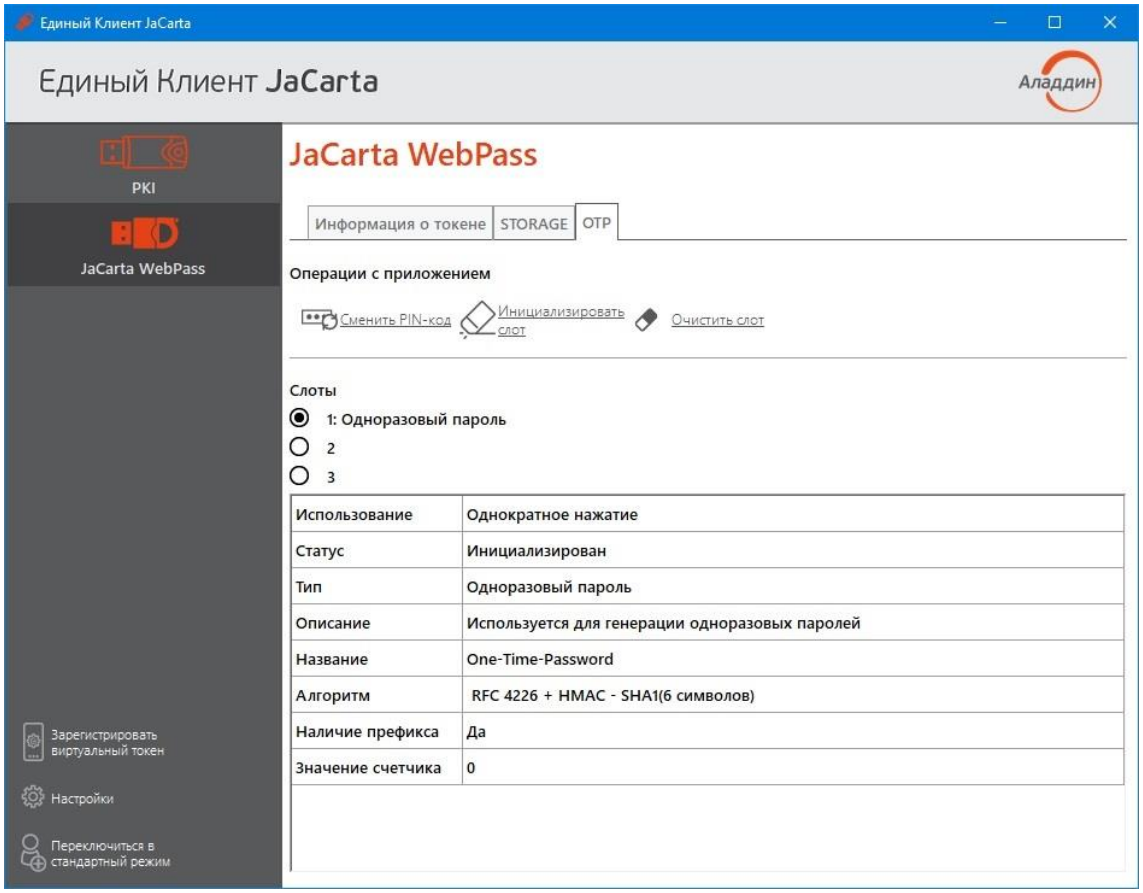


Рисунок 65 - Слот 1 инициализирован типом "Одноразовый пароль"

7.2.3.2 Инициализация слота типом "Пароль"

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

Для инициализации слота типом "Пароль":

1. На вкладке "OTP" выберите тот слот, в который необходимо записать многоразовый пароль и нажмите кнопку "Инициализировать слот" (см. Р*исунок 66*).

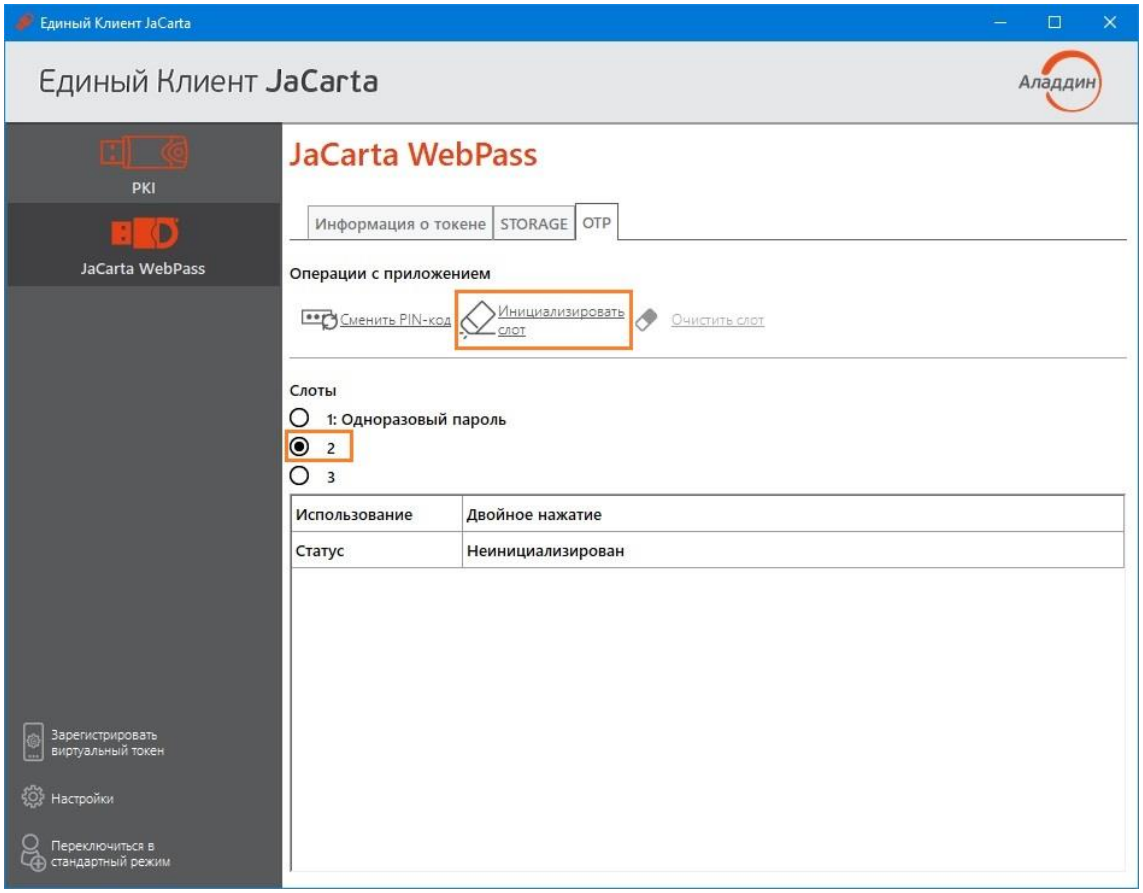


Рисунок 66 - Вкладка "OTP". Выбора слота 2 для инициализации "Пароль"

2. Будет открыто стартовое окно Мастера инициализации слота (см. Рисунок 67).

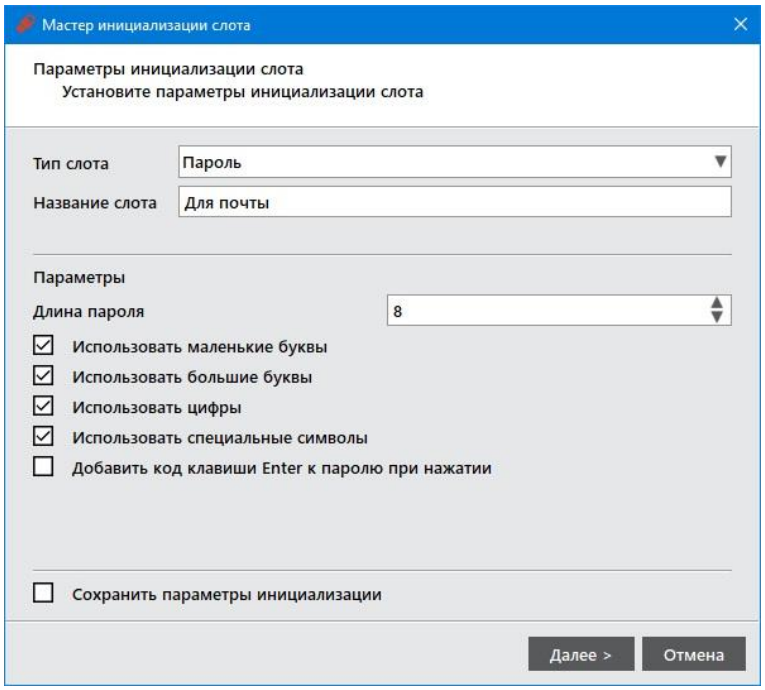


Рисунок 67 – Инициализация слота типом "Пароль". Выбор параметров инициализации

Заполните поля мастера следующим образом:

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

Нажмите кнопку "Далее".

3. Далее прохождение Мастера аналогично шагам 4-6 п.7.2.3.1.
4. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Пароль" (см. Рисунок 68).

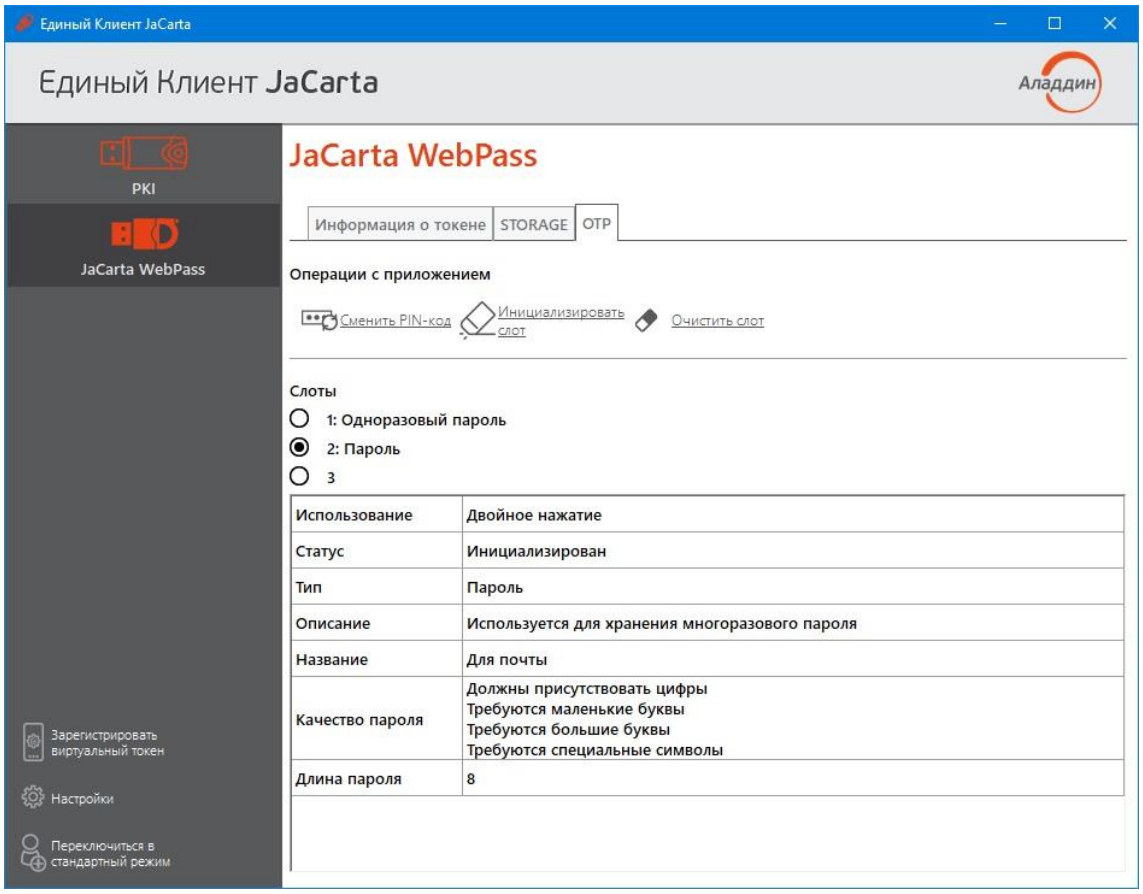


Рисунок 68 - Слот 2 инициализирован типом "Пароль"

7.2.3.3 Инициализация слота типом "Интернет-адрес url"

Для инициализации слота типом "Пароль":

1. На вкладке "OTP" выберите тот слот, в который необходимо записать многоразовый пароль и нажмите кнопку "Инициализировать слот" (см. Рисунок 69).

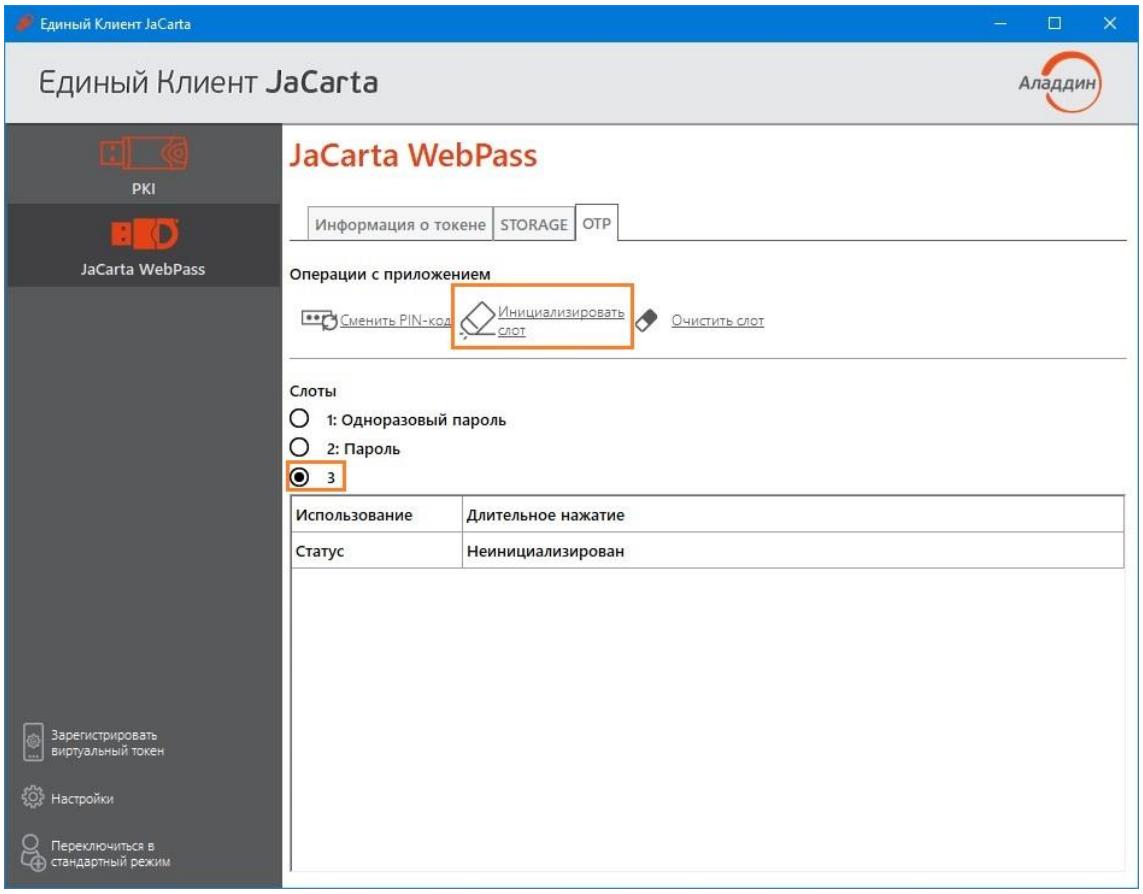


Рисунок 69 - Вкладка "OTP". Выбора слота 3 для инициализации

2. Будет открыто стартовое окно Мастера инициализации слота (см. Рисунок 70).

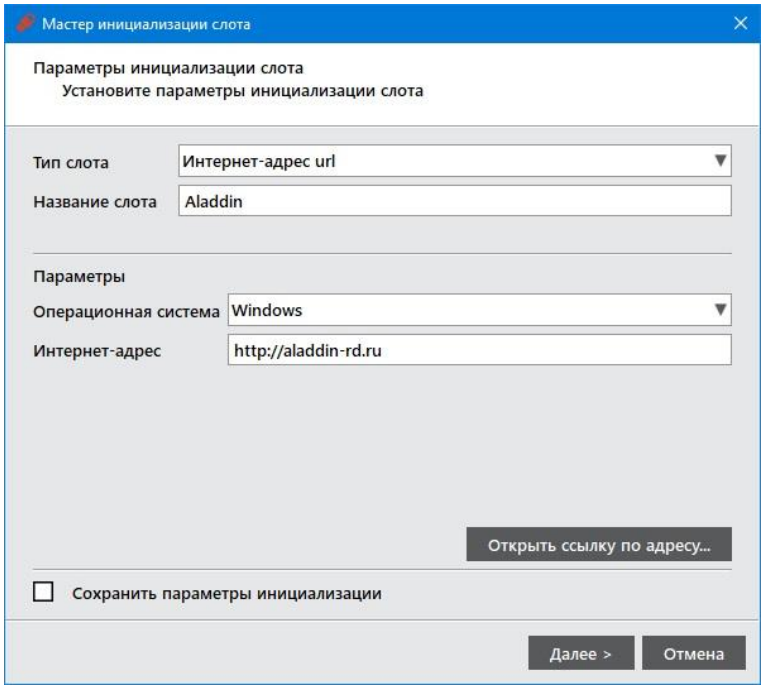


Рисунок 70 - Инициализация слота типом ""Интернет-адрес url". Выбор параметров инициализации

Заполните поля настроек следующим образом:

- В поле "Тип слота" выберите значение "Интернет-адрес url";
- В поле "Название слота" введите название, например, Aladdin. Длина поля не должна превышать 32 символа;
- В поле "Операционная система" выберите тип операционной системы: Windows, Mac OS, Linux;
- В поле "Интернет-адрес" введите адрес интернет-ресурса, на который будет осуществлен переход при нажатии на кнопку электронного ключа (например, https://aladdin.ru);

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

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

Нажмите кнопку "Далее".

3. Далее прохождение Мастера аналогично шагам 4-6 п.7.2.3.1.
4. На вкладке "OTP" будут отображены свойства слота, инициализированного типом "Интернет-адрес url" (см. Рисунок 71).

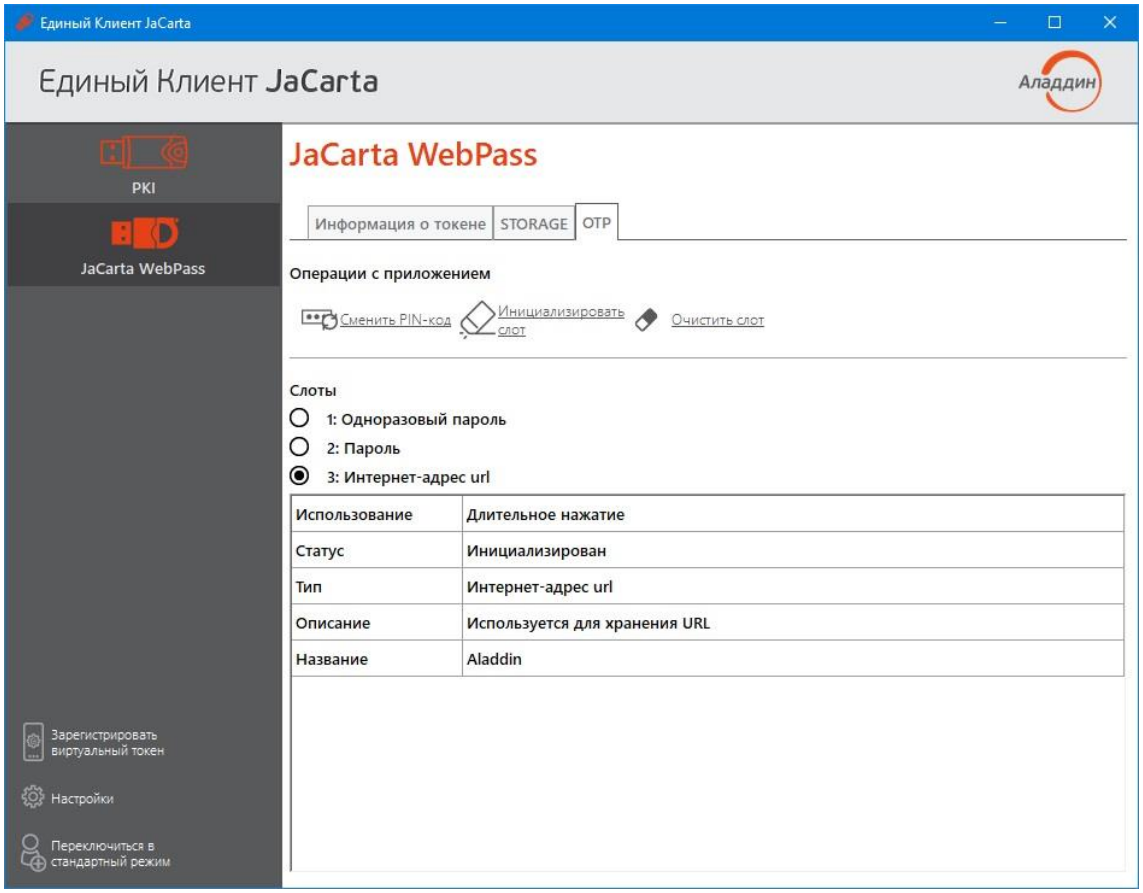


Рисунок 71 - Слот 3 инициализирован типом ""Интернет-адрес url"

7.2.3.4 Очистка слота

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

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:

1. На вкладке "OTP" выберите тот слот, который необходимо очистить. Нажмите кнопку "Очистить слот". Будет открыто окно "Очистить слот" (см. Рисунок 72).

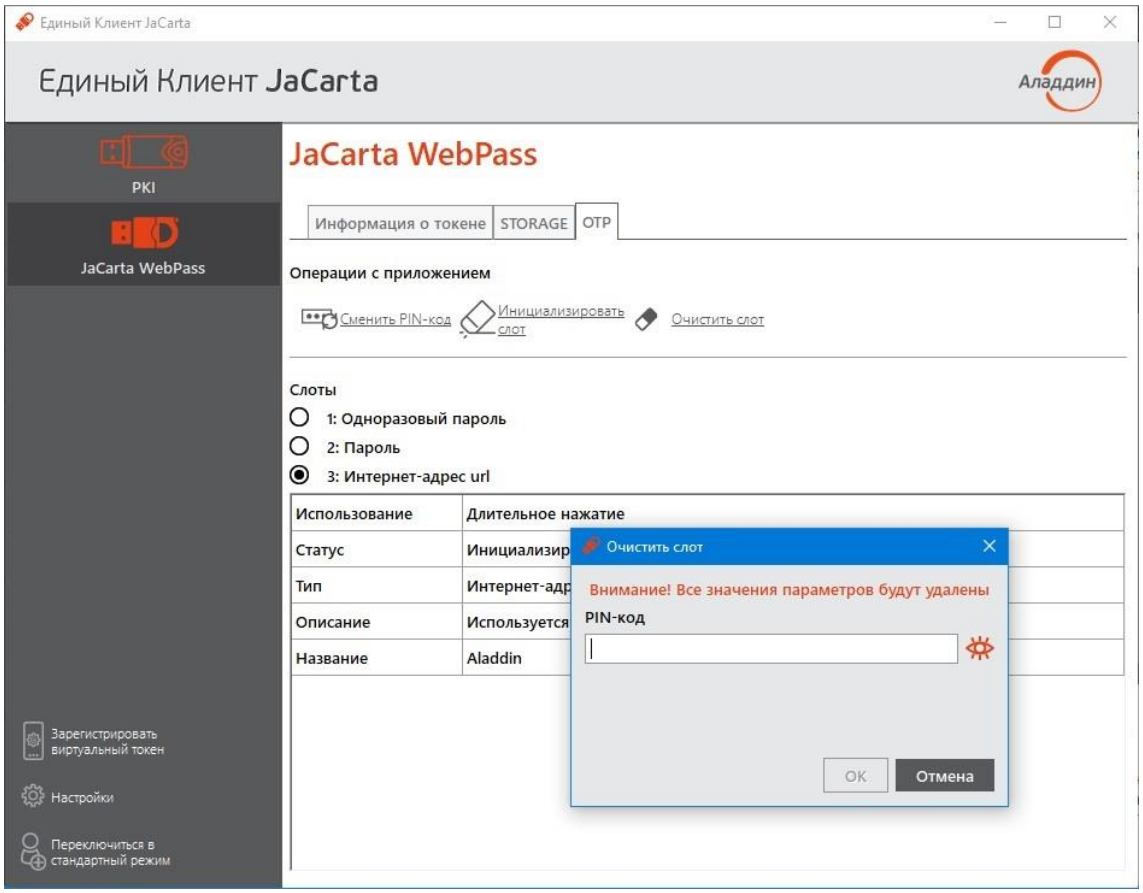


Рисунок 72 – Очистка слота

2. В поле "PIN-код" в окне "Очистить слот" введите PIN-код электронного ключа и нажмите кнопку "OK".
3. Будет выполняться очистка слота. По ее завершении данные, хранящиеся в слоте будут удалены. На экране будет отображена информация об этом (см. Рисунок 73).

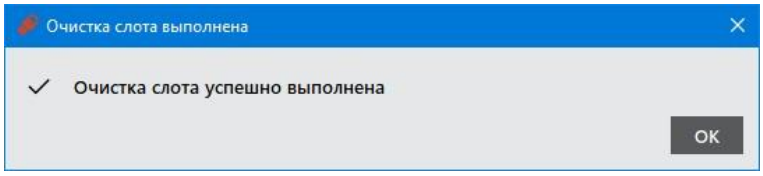


Рисунок 73 – Сообщение о завершении очистки слота

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
	USB Type-C токен в металлическом корпусе
	Тип электронного ключа не определён
	Электронный ключ находится на стадии определения

8. Контакты

8.1 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.

8.2 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 и ФСБ.

Лицензии

- Компания имеет все необходимые лицензии ФСТЭК России и ФСБ России для проектирования, производства и поддержки СЗИ и СКЗИ.
- Система менеджмента качества компании соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012.