



Единый Клиент JaCarta

Руководство пользователя для Windows

Версия продукта	2.12
Версия документа	1.1
Статус	Публичный
Дата	23.10.2019
Листов	52

Оглавление

1.	О документе	3
1.1	Назначение документа	3
1.2	На кого ориентирован данный документ	3
1.3	Организация документа	3
1.4	Рекомендации по использованию документа	3
1.5	Соглашения по оформлению	3
1.6	Авторские права, товарные знаки, ограничения	5
1.7	Лицензионное соглашение	6
2.	Основные понятия	8
2.1	Назначение	8
2.2	Термины и определения	8
3.	Общие сведения об электронных ключах	9
3.1	Приложения, апплеты и модели электронных ключей	9
3.2	Параметры электронных ключей при поставке	11
3.3	Информация о PIN-коде пользователя	12
4.	Обзор пользовательского интерфейса	13
4.1	Запуск Единого Клиента JaCarta	13
4.2	Меню быстрого запуска	13
4.3	Режимы работы программы	14
4.3.1	Переключение между режимами	14
4.3.2	Основное окно в режиме пользователя	15
4.3.3	Основное окно в режиме администратора	16
4.4	Просмотр сведений о программе	17
4.5	Завершение работы программы	17
5.	Работа в программе в режиме пользователя	18
5.1	Просмотр информации об электронном ключе	18
5.2	Изменение метки (переименование) электронного ключа	19
5.3	Изменение PIN-кода пользователя	20
5.4	Установка PIN-кода подписи	23
5.5	Изменение PIN-кода подписи	25
5.6	Разблокирование PIN-кода подписи	27
6.	Работа в программе в режиме администратора	30
6.1	Просмотр информации о приложениях на электронном ключе	30
6.2	Повторная инициализация датчика случайных чисел	32
6.3	Диагностика приложения	34
6.4	Проверка целостности приложения	35
6.5	Операции с сертификатами в приложении электронного ключа	36
6.5.1	Создание запроса на сертификат	36
6.5.2	Импорт сертификата	39
6.5.3	Экспорт сертификата	43
6.5.4	Просмотр сертификата	45
6.6	Операции с объектами в приложении электронного ключа	46
6.6.1	Просмотр списка объектов	46
6.6.2	Удаление объектов	49
	Приложение А. Обозначения электронных ключей	50
7.	Контакты	51
7.1	Офис (общие вопросы)	51
7.2	Техподдержка	51

1. О документе

1.1 Назначение документа

Документ представляет собой руководство пользователя для ПО Единый Клиент JaCarta.

1.2 На кого ориентирован данный документ

Документ предназначен пользователей ПО Единый Клиент JaCarta, владельцев электронных ключей JaCarta/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 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 режиме пользователя" приведены операции, совершаемые в ПО Единый Клиент JaCarta в режиме пользователя;
- в разделе 6 "Работа в программе в режиме администратора" приведены операции, совершаемые в ПО Единый Клиент JaCarta в режиме администратора без ввода PIN-кода администратора электронного ключа.

1.4 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве ознакомительного материала (подробного руководства по использованию ПО Единый Клиент JaCarta), а также в качестве справочника при работе с ПО Единый Клиент JaCarta.






Документ рекомендован как для последовательного, так и для выборочного изучения.

1.5 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 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
<u>Гиперссылка</u>	Используется для выделения внешних ссылок
Ссылка [стр. 3]	Используется для выделения перекрестных ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание

	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 ЗАО "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 ЗАО "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 ЗАО "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 ЗАО "Аладдин Р.Д." без предварительного уведомления.

ЗАО "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.

ЗАО "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 ЗАО "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ЗАО "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 ЗАО "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 резкспорт 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 Закрытым акционерным обществом "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 ЗАО "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 ЗАО "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.), подтвержденные или включенные 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 нелегальным 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 ЗАО "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, возникающих 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 УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

2. Основные понятия

2.1 Назначение

Единый Клиент JaCarta представляет собой программное обеспечение, обеспечивающее работу с электронными ключами JaCarta/eToken в операционной системе Windows. С помощью Единого Клиента JaCarta можно использовать электронные ключи JaCarta для интерактивного входа в систему, электронной цифровой подписи, доступа к VPN.

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 режиме пользователя (см. п. 5 "Работа в программе в режиме пользователя").

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

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

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

Соответствие приложений, апплетов и моделей электронных ключей, работа с которыми поддерживается в macOS приведено в таблице 1.

Таблица 2 – Параметры электронных ключей при поставке

Приложение и апплет	Модели электронных ключей
Приложение PKI, реализованное апплетом Laser	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/ГОСТ/Flash JaCarta PKI/BIO JaCarta PKI/BIO/ГОСТ JaCarta PKI/ГОСТ; JaCarta-2 PKI/ГОСТ JaCarta-2 SE JaCarta-2 PKI/BIO/ГОСТ JaCarta-2 SF

Приложение и апплет	Модели электронных ключей
Приложение PKI, реализованное апплетом PRO	eToken Anywhere eToken PRO (Java) eToken NG-FLASH (Java) eToken NG-OTP (Java) JaCarta PRO JaCarta PRO/ГОСТ JaCarta PKI. Обратная совместимость с продуктами компании Aladdin JaCarta PKI/ГОСТ. Обратная совместимость с продуктами компании Aladdin JaCarta-2 PRO/ГОСТ
Приложение ГОСТ, реализованное апплетом Криптотокен	eToken ГОСТ JaCarta ГОСТ JaCarta PKI/ГОСТ JaCarta PRO/ГОСТ JaCarta PKI/ГОСТ. Обратная совместимость с продуктами компании Aladdin JaCarta ГОСТ/Flash JaCarta PKI/ГОСТ/Flash JaCarta PKI/BIO/ГОСТ.
Приложение ГОСТ, реализованное апплетом Криптотокен 2 ЭП	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ JaCarta-2 PRO/ГОСТ JaCarta-2 PKI/BIO/ГОСТ JaCarta-2 SE JaCarta SF/ГОСТ
Приложение STORAGE, реализованное апплетом DataStore	JaCarta LT JaCarta WebPass JaCarta U2F/WebPass JaCarta U2F
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass JaCarta U2F/WebPass

3.2 Параметры электронных ключей при поставке

При поставке электронные ключи имеют параметры, приведенные в таблице 2.

Таблица 3 – Параметры электронных ключей при поставке

<i>Приложение и апплет</i> <i>Параметр, операция</i>	<i>Приложение PKI апплет PRO</i>	<i>Приложение PKI апплет Laser</i>	<i>Приложение ГОСТ апплет Крипто- кен</i>	<i>Приложение ГОСТ апплет Крипто- кен 2 ЭП</i>	<i>Приложение STORAGE апплет DataStore</i>	<i>Приложение OTP апплет AladdinOTP</i>
PIN-код пользователя по умолчанию *	1234567890	11111111	не установлен	1234567890	1234567890	не установлен
PUK-код для разблокирования	не предусмотрен	не предусмотрен	не предусмотрен	может быть установ- лен как опция при заказе	не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	1234567890	00000000	1234567890	не предусмотрен	не установлен	не предусмотрен
Форматирование приложения без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после фор- матирования)	возможно	возможно	возможно	невозможно	невозможно	возможно
Форматирование приложения без назначения PIN-кода администратора	возможно	возможно	невозможно	невозможно	невозможно	операция не преду- смотрена
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом PIN-код пользо- вателя задается за- ново	... PIN-код пользо- вателя задается за- ново	... PIN-код пользо- вателя остается преж- ним	... PIN-код пользо- вателя остается преж- ним	PIN-код пользо- вателя остается прежним	операция не преду- смотрена
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	невозможно	невозможно	возможно	невозможно	невозможно
Изменение PIN-кода пользователя админи- стратором без форматирования	возможно	возможно	невозможно	невозможно	невозможно	невозможно

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

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 7 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 операция выполняется администратором, описание ее выполнения приведено в документе "Единый Клиент JaCarta 2.12. Руководство администратора для операционных систем семейства Linux".

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 🚀:

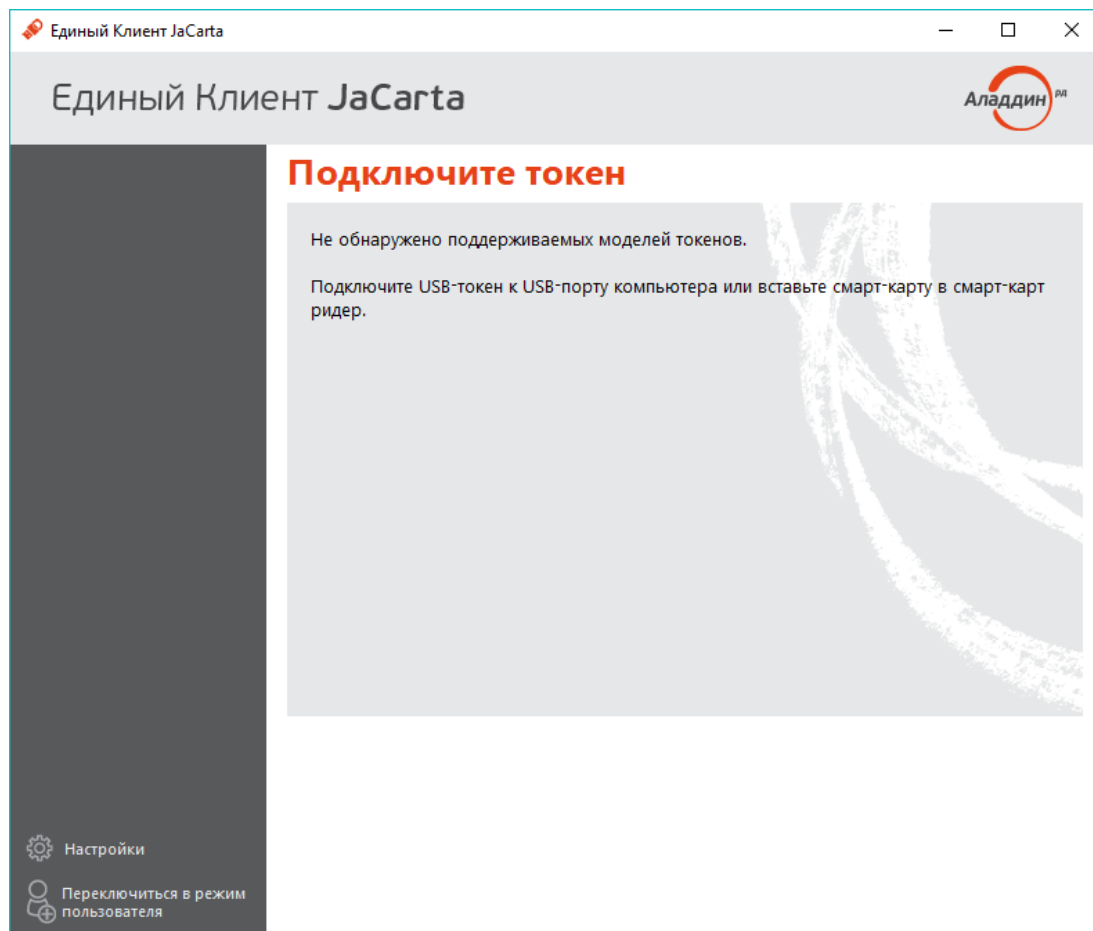



Рисунок 1 – Основное окно Единого Клиента JaCarta

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

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:

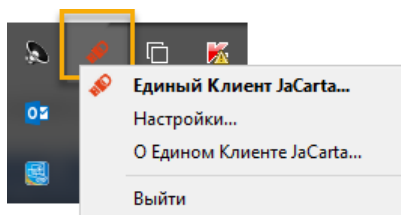



Рисунок 2 – Меню быстрого запуска Единого Клиента JaCarta

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 "Просмотр сведений о программе").
- "Выйти" – позволяет выйти из программы, при этом значок  перестает отображаться в панели управления.

4.3 Режимы работы программы

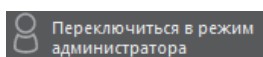
Единый Клиент JaCarta поддерживает следующие режимы работы:

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

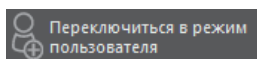
Режим администратора – позволяет просматривать подробные сведения о подсоединённых электронных ключах и предоставляет доступ к операциям над приложениями электронного ключа и объектами каждого приложения.

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 режиме пользователя;



, то вход осуществлен в режиме администратора.

► Для переключения между режимами пользователя и администратора:

1. Для переключения Единого Клиента JaCarta из режима пользователя в режим администратора нажмите кнопку "Переключиться в режим администратора".
2. Для переключения Единого Клиента JaCarta из режима администратора в режим пользователя нажмите кнопку "Переключиться в режим пользователя".

4.3.2 Основное окно в режиме пользователя

По умолчанию основное окно Единого Клиента JaCarta открывается в режиме пользователя. На рисунке ниже приведен вид основного окна в режиме пользователя с подключенным к компьютеру пользователем электронным ключом:

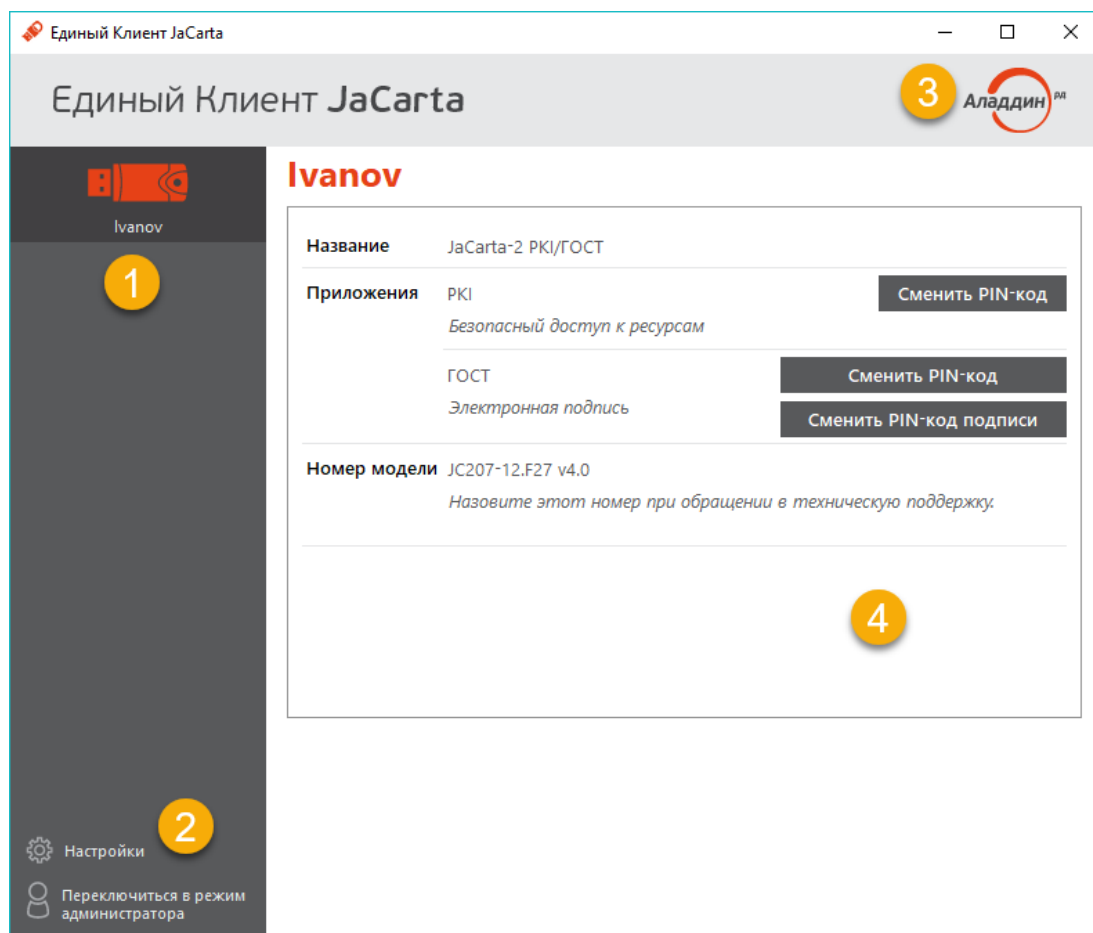


Рисунок 3 – Основное окно Единого Клиента JaCarta в режиме пользователя

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. 50
- 2** Область содержит кнопки:
"Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе "Единый Клиент JaCarta 2.12. Руководство администратора для macOS";
"Переключиться в режим администратора" – кнопка для переключения Единого Клиента JaCarta в режим администратора
- 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 режиме администратора

Вид основного окна в режиме администратора приведен на рисунке ниже:

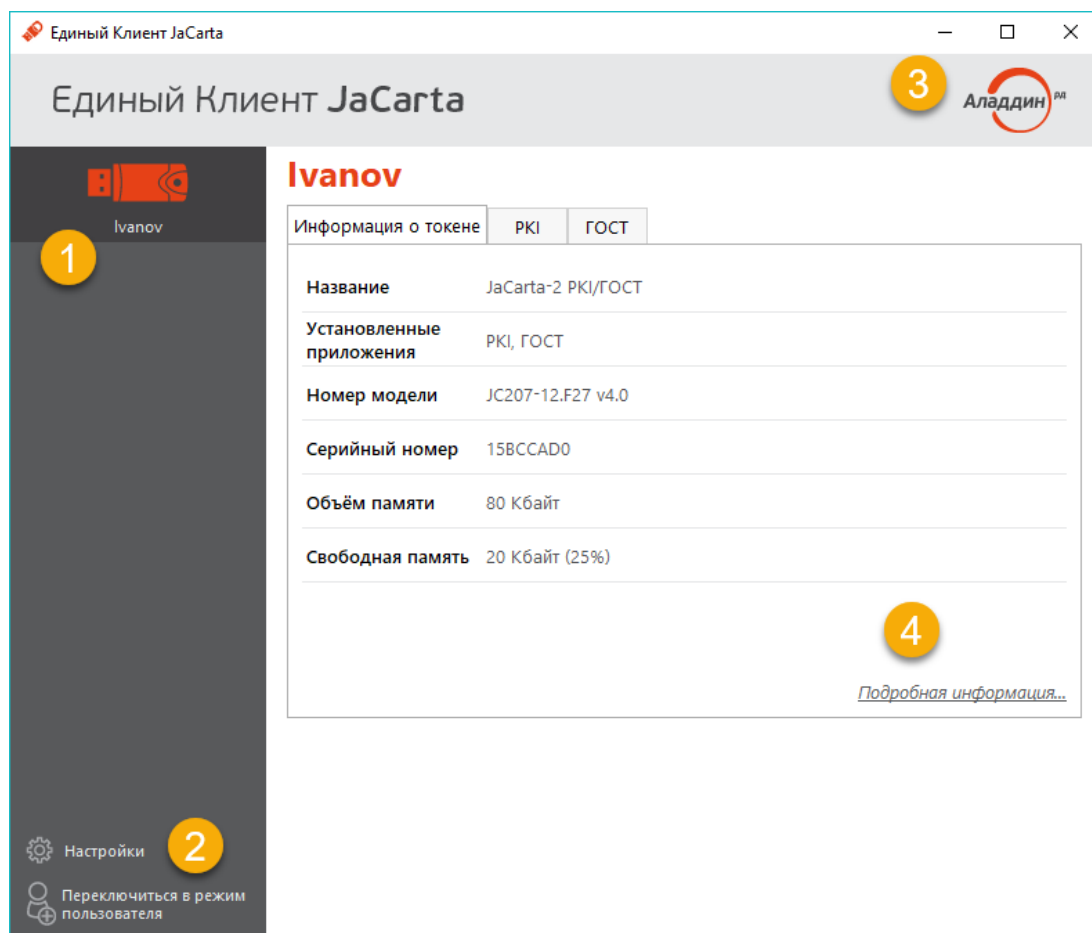


Рисунок 4 – Основное окно Единого Клиента JaCarta в режиме администратора

Основное окно в режиме администратора 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. 50
- 2 Область содержит кнопки:
"Настройки" – кнопка для вызова окна настроек программы.
"Переключиться в режим пользователя" – кнопка для переключения Единого Клиента JaCarta в режим пользователя
- 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 режиме администратора данная область представлена в виде вкладок:

- на вкладке "Информация о токене" отображается информация об электронном ключе и ссылка "Подробная информация..." (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 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:

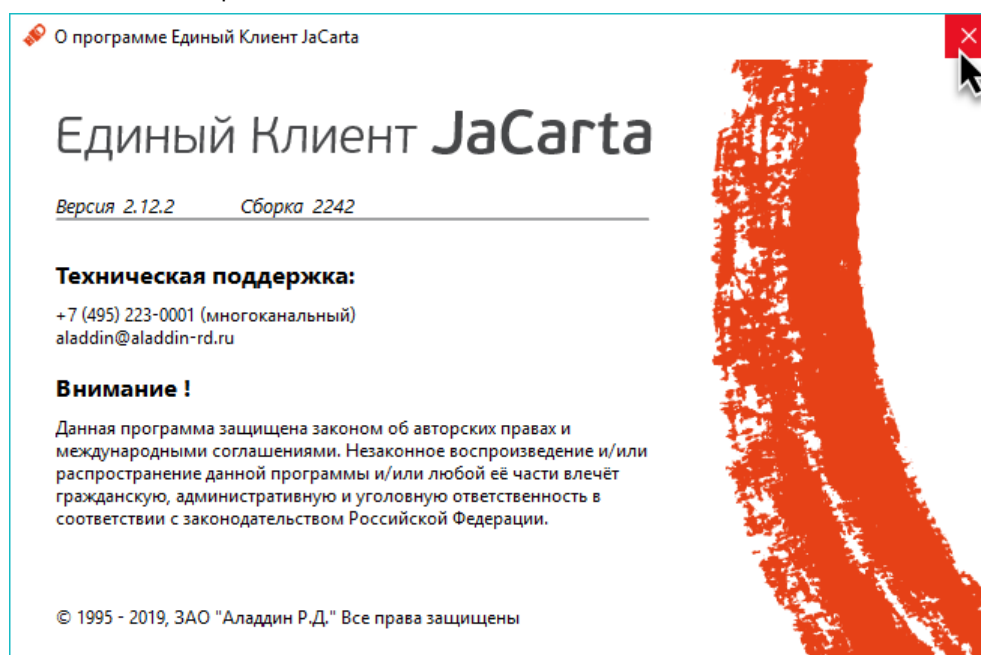



Рисунок 5 - Информационное окно «О программе»

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

4.5 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 режиме пользователя

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

- просмотр информации об электронном ключе;
- изменение метки (переименование) электронного ключа;
- изменение PIN-кода пользователя;
- установка, изменение, разблокирование PIN-кода подписи (для электронных ключей с приложением ГОСТ с апплетом Криптотокен 2 ЭП).

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 электронных ключей, то выберите значок нужного ключа в области слева:

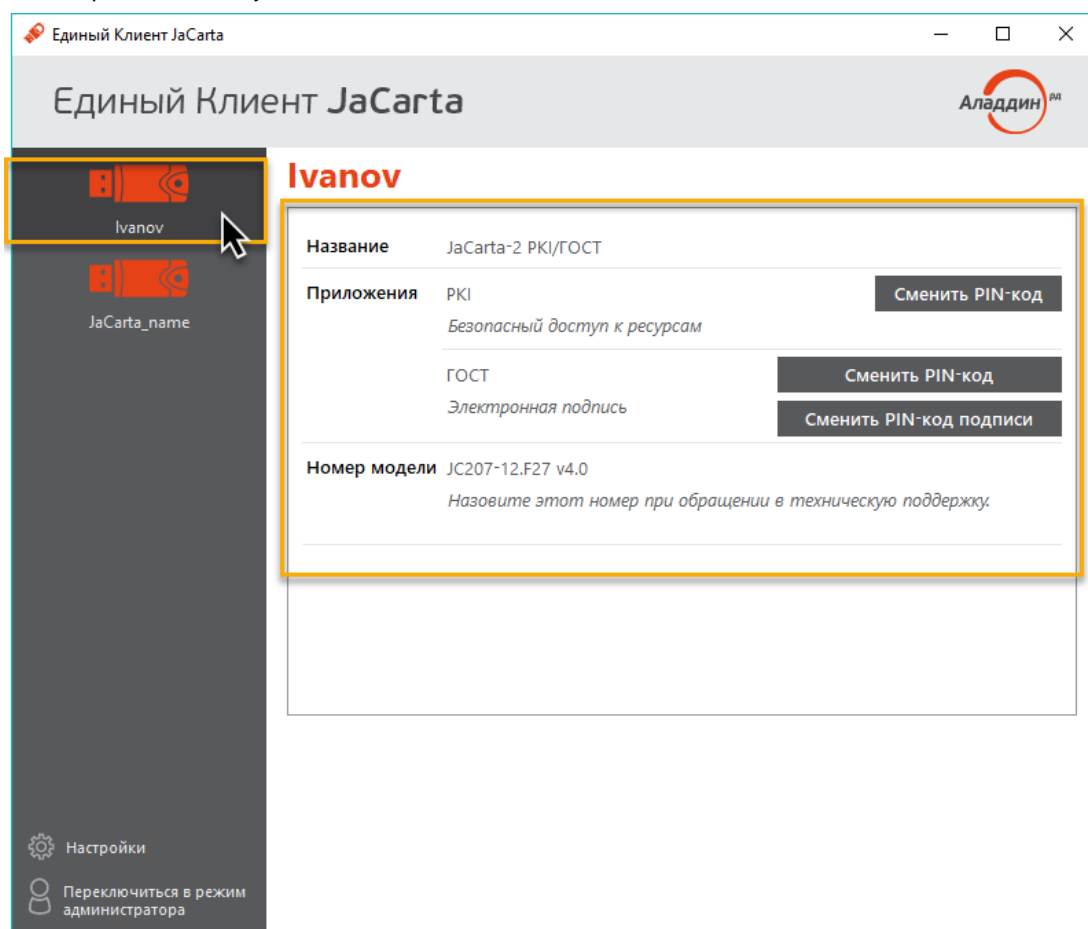


Рисунок 6 – Информация о выбранном электронном ключе в режиме пользователя

Для выбранного ключа в режиме пользователя отображается следующая информация:

- "Название" – название модели электронного ключа;
- "Приложения" – перечень приложений, установленных в памяти электронного ключа. Первым в списке отображается приоритетное на данном ключе приложение. На примере, приведенном на рисунке 6 приоритетным приложением является приложение PKI;

- "Номер модели" – номер модели выбранного ключа. В случае возникновения проблем при использовании пользователь должен сообщить этот номер в службу технической поддержки.
3. Закройте основное окно Единого Клиента JaCarta нажатием кнопки "Заккрыть" в левом верхнем углу.

5.2 Изменение метки (переименование) электронного ключа

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

► **Для изменения метки электронного ключа:**

1. Запустите Единый Клиент JaCarta и подключите электронный ключ к разьему 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 выбранного значка. Будет отображено одноименное окно:

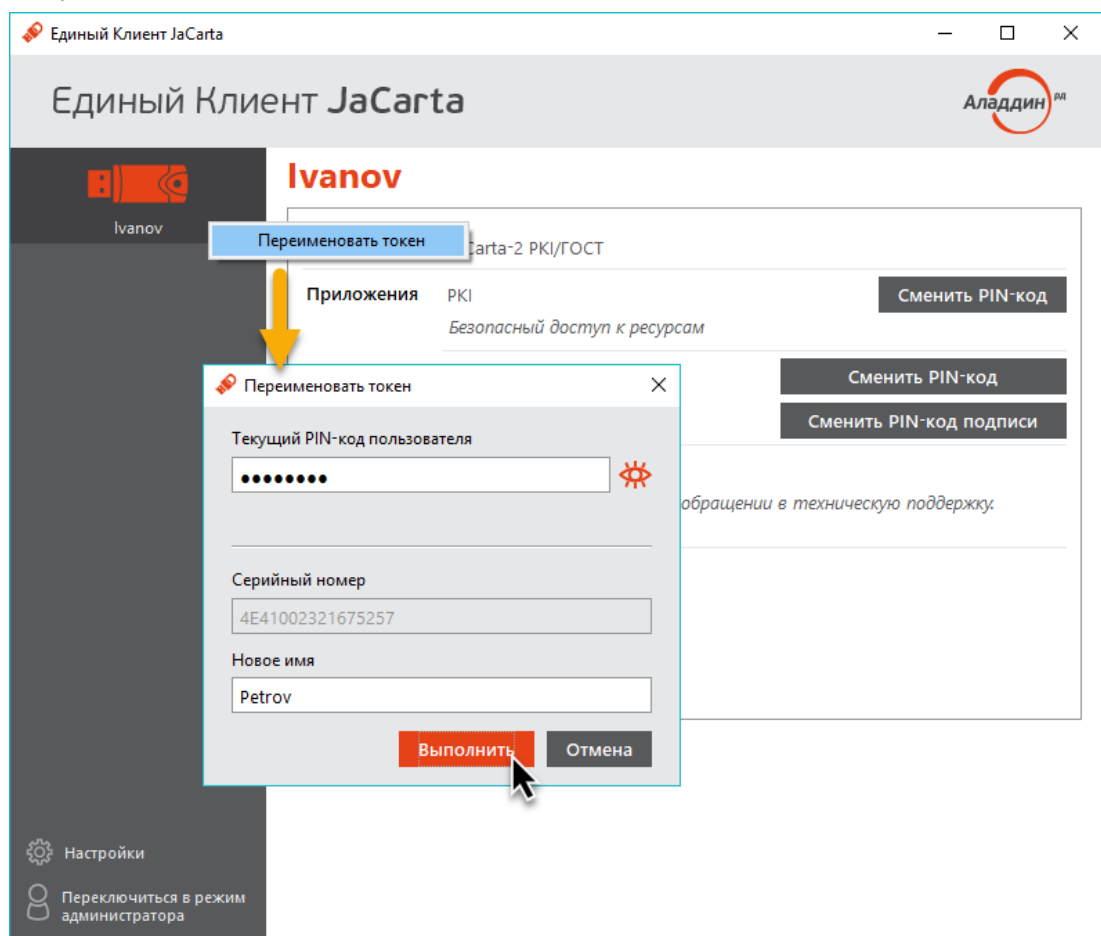


Рисунок 7 – Вызов окна "Переименовать токен" в режиме пользователя

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 "OK". В случае успешной авторизации на электронном ключе его имя будет изменено:

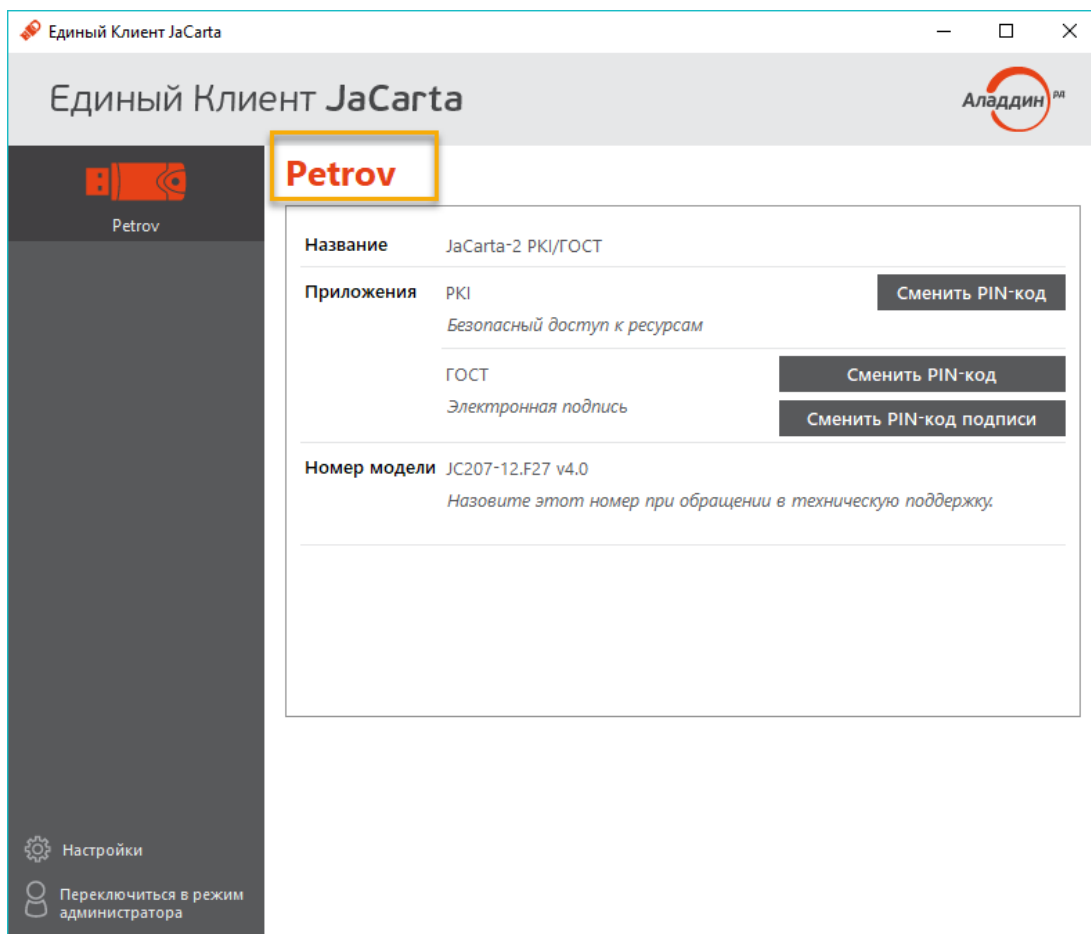


Рисунок 8 – Основное окно в режиме пользователя. Имя ключа изменено

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 режиме пользователя нажмите кнопку "Сменить PIN-код" для выбранного приложения (на скриншотах ниже приведен пример смены PIN-кода приложения PKI):

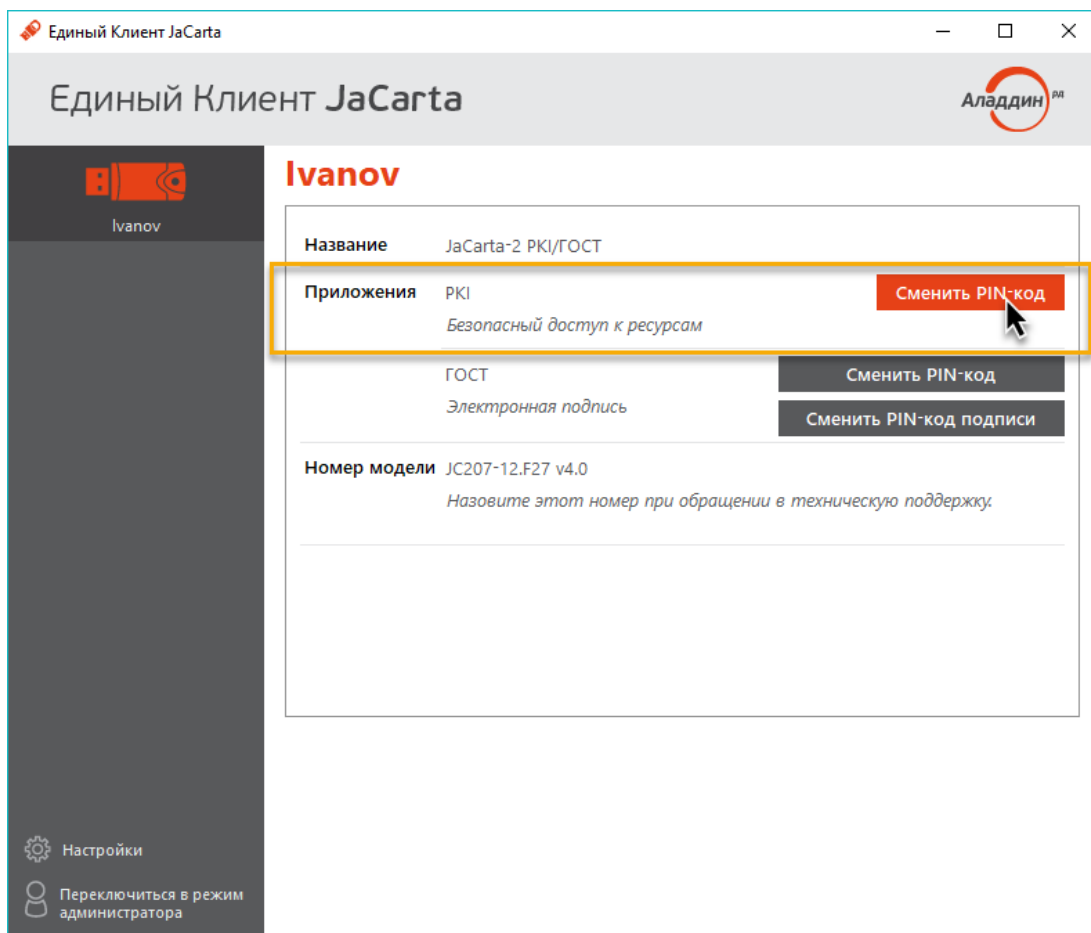


Рисунок 9 – Вызов окна "Переименовать токен" в режиме пользователя

3. Будет отображено окно для смены PIN-кода. Заполните поля в окне следующим образом (см. рисунок 10):
- в поле "Текущий PIN-код" введите PIN-код пользователя выбранного приложения (в данном примере приложения PKI);
 - в поле "Новый PIN-код" 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 6 символов.

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

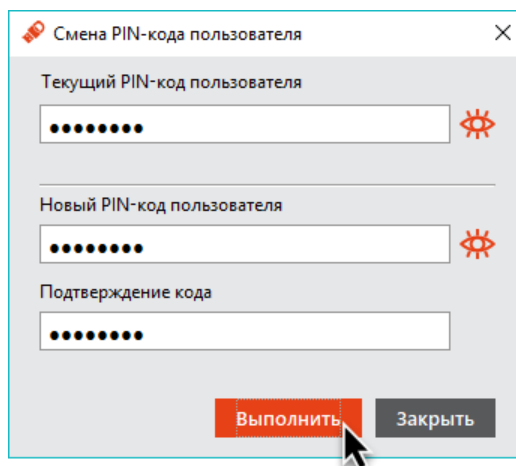


Рисунок 10 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода введены верно

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

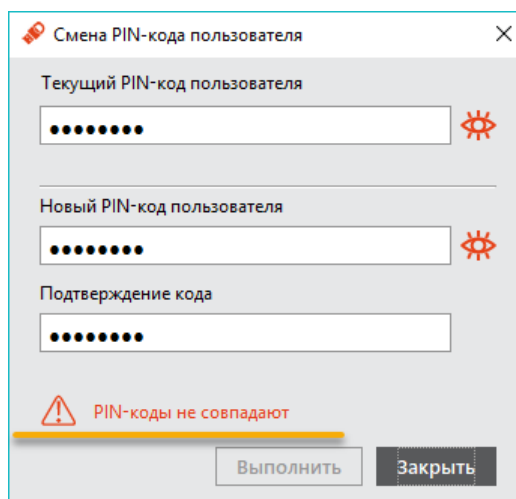




Рисунок 11 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода не совпадают

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 .

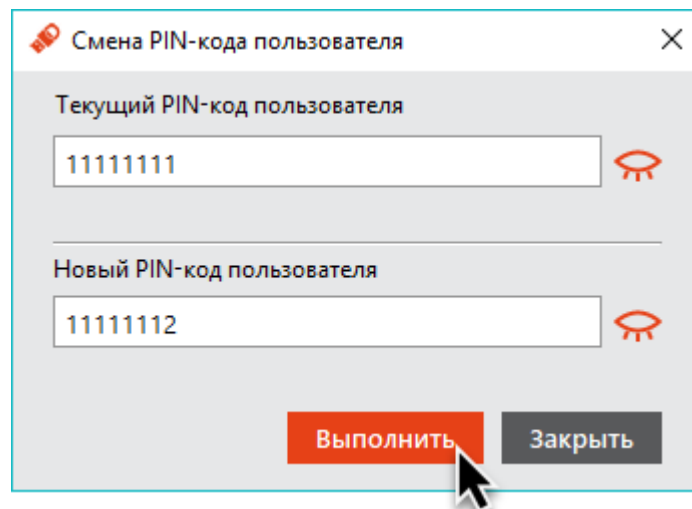


Рисунок 12 – Окно изменения PIN-кода пользователя. Отображение значений полей в явном виде

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

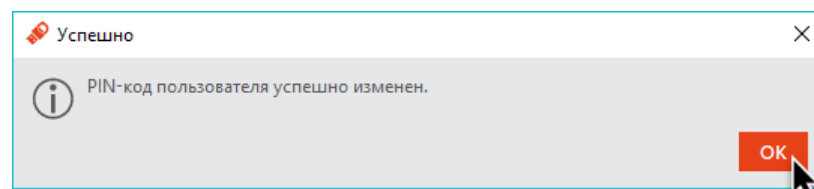


Рисунок 13 – Окно "PIN-кода пользователя изменен"

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 апплетом 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, превышающее 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 режиме пользователя нажмите кнопку "Установить PIN-код подписи" для приложения ГОСТ:

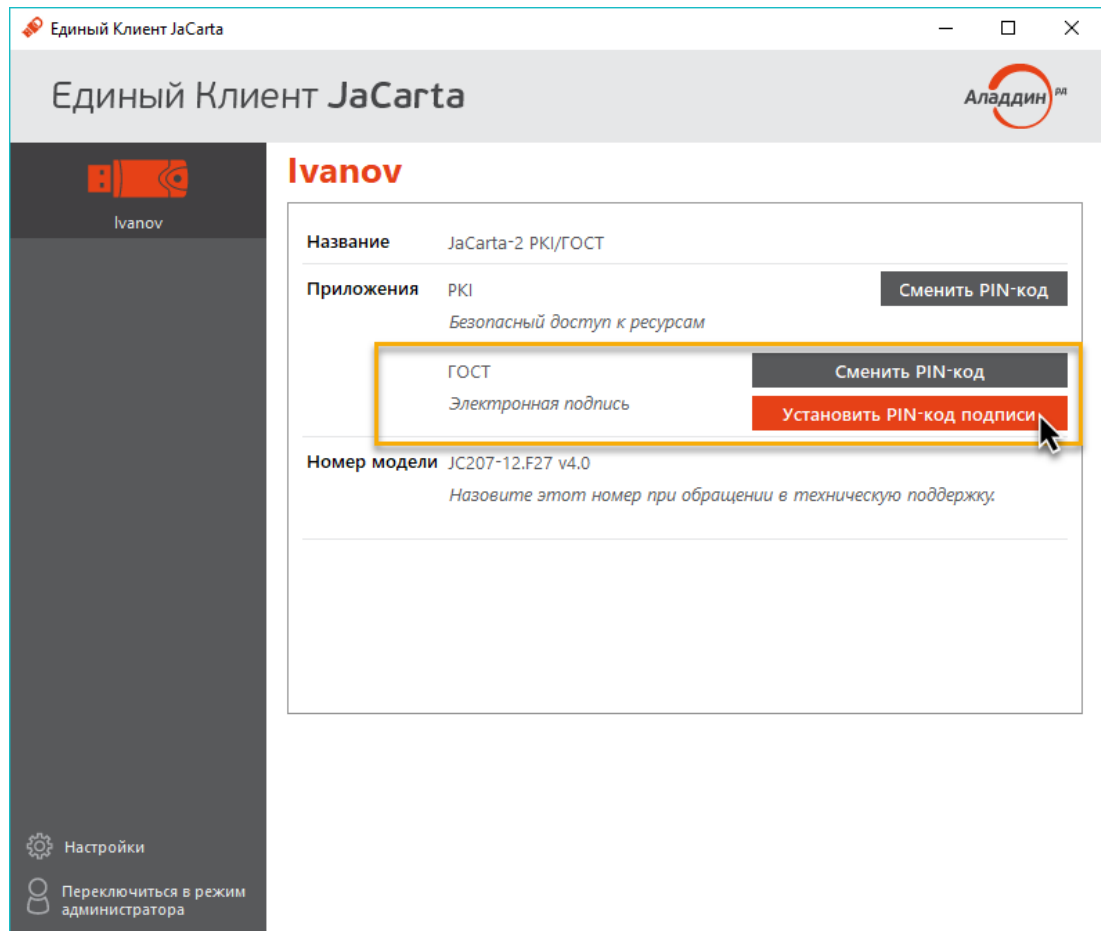




Рисунок 14 – Главное окно Единого Клиента JaCarta. Кнопка "Установить PIN-код подписи" активна

3. Будет отображено окно для установки PIN-кода подписи. Заполните поля в окне следующим образом (см. рисунок 15):
- 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 .

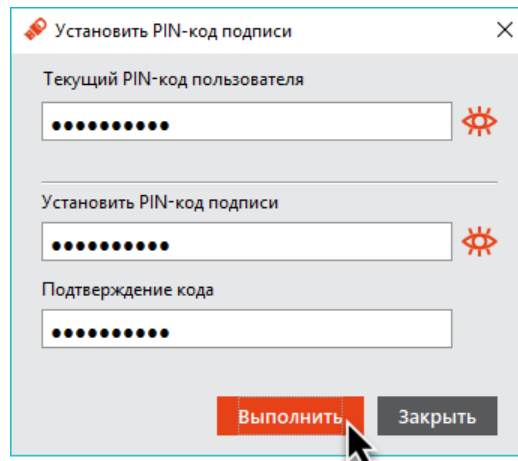


Рисунок 15 - Окно установки PIN-кода подписи. Значения PIN-кода введены верно

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

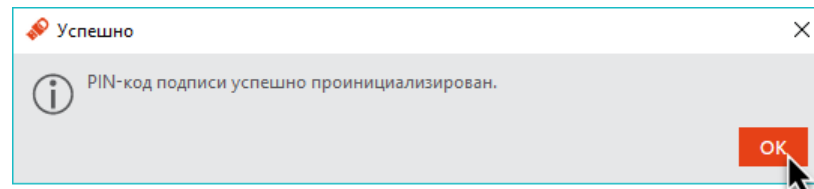


Рисунок 16 - Сообщение об успешной инициализации PIN-кода подписи

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 разьему 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 режиме пользователя нажмите кнопку "Сменить PIN-код подписи" для приложения ГОСТ:

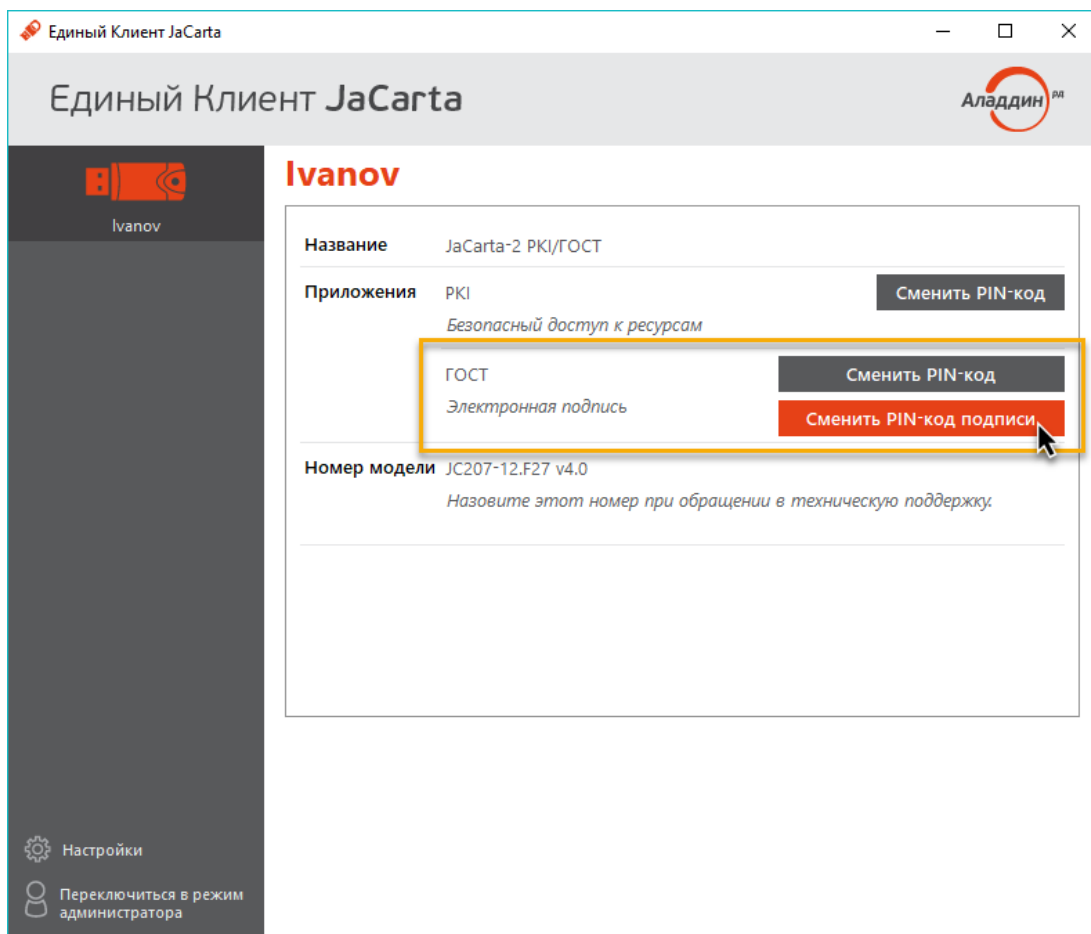




Рисунок 17 - Единый Клиент JaCarta. Главное окно

3. Будет отображено окно для изменения PIN-кода подписи. Заполните поля в окне следующим образом (см. рисунок 18):
- 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 .

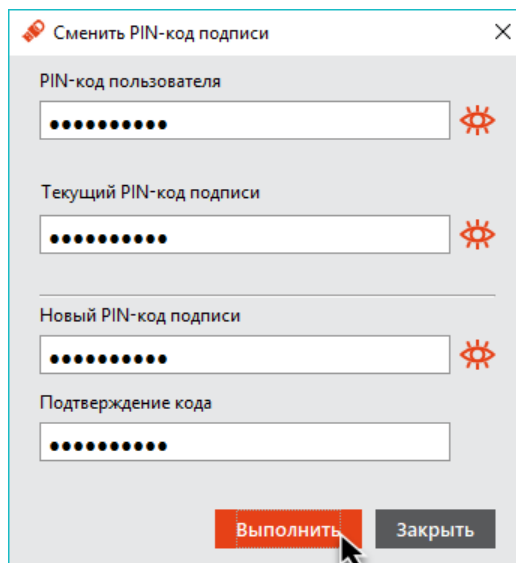


Рисунок 18 - Окно изменения PIN-кода подписи. Значения PIN-кода введены верно

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

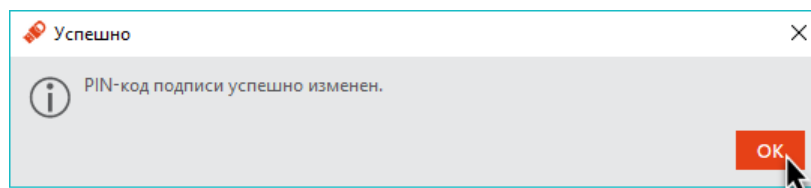


Рисунок 19 - Единый Клиент JaCarta. Окно "PIN-кода подписи установлен"

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 режиме администратора (см. п. 6 "Работа в программе в режиме администратора").

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 режиме пользователя нажмите кнопку "Разблокировать PIN-код подписи" для приложения ГОСТ:

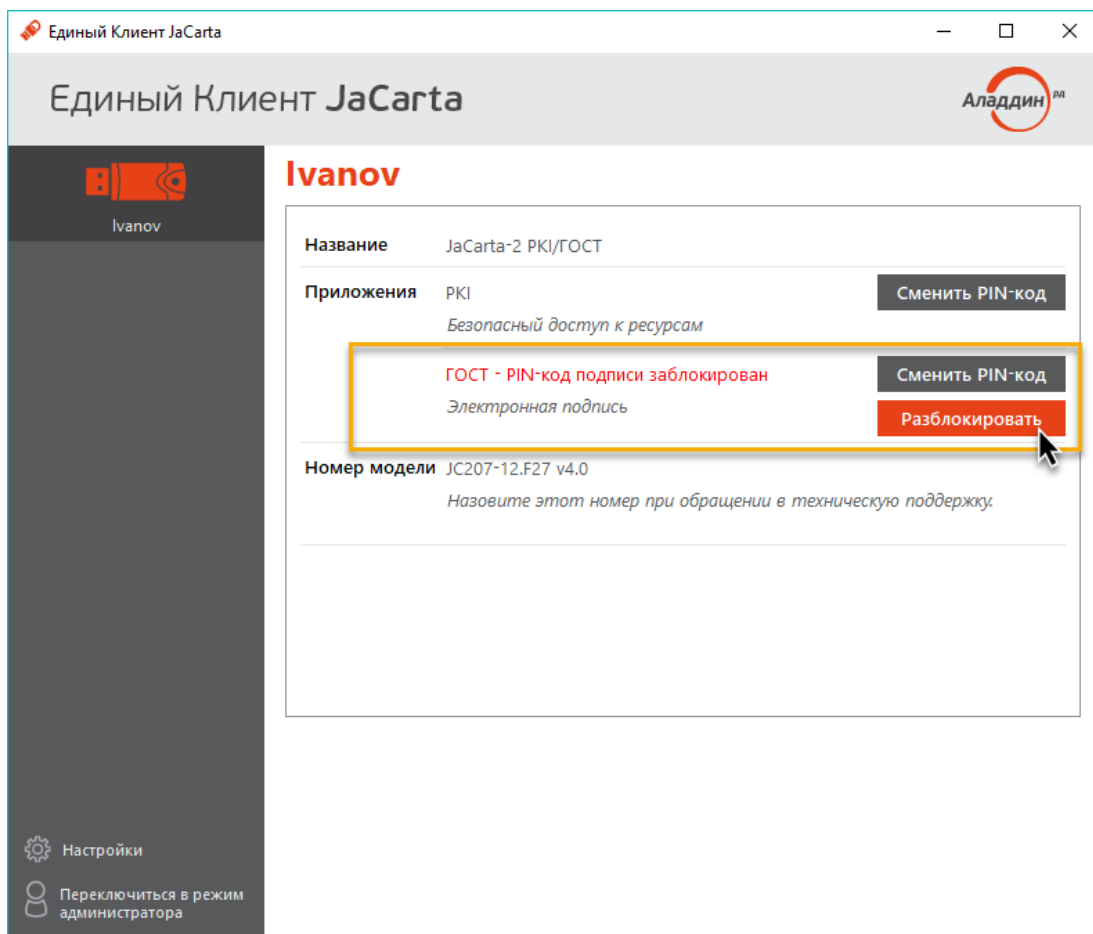


Рисунок 20 - Единый Клиент JaCarta. Главное окно, PIN-код подписи заблокирован

3. Будет отображено окно для ввода PUK-кода. В поле "Текущий PUK-код" введите текущее значение PUK-кода. Значение PUK-код по умолчанию для приложения ГОСТ – 0987654321.

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.

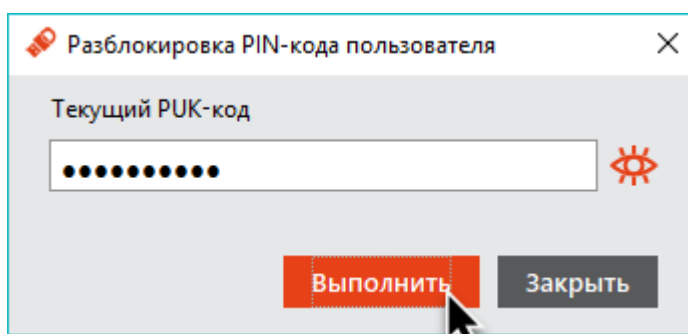


Рисунок 21 – Окно для ввода PUK-кода при разблокировании PIN-кода подписи

4. Нажмите кнопку "Разблокировать". В случае ввода верного PUK-кода будет выполнено разблокирование PIN-кода подписи. Информация об этом будет отображена в сообщении:

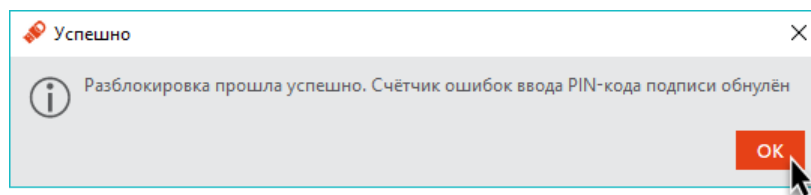


Рисунок 22 – Сообщение об успешном разблокировании PIN-кода подписи

5. Для закрытия окна сообщения нажмите кнопку "ОК".

6. Работа в программе в режиме администратора

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

- просмотр информации об электронном ключе и приложениях на электронном ключе;
- повторная инициализация датчика случайных чисел (для электронных ключей с приложением ГОСТ с апплетом Криптотокен);
- диагностика приложения (для электронных ключей с приложением ГОСТ с апплетом Криптотокен);
- проверка целостности приложения (для электронных ключей с приложением ГОСТ с апплетом Криптотокен 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 2.12. 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 немедленно, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

3. Нажмите кнопку "Переключиться в режим администратора" и во вкладке "Информация о токне" нажмите ссылку "Подробная информация..." (см. рисунок 4). Будет отображено окно "Подробная информация о токене":

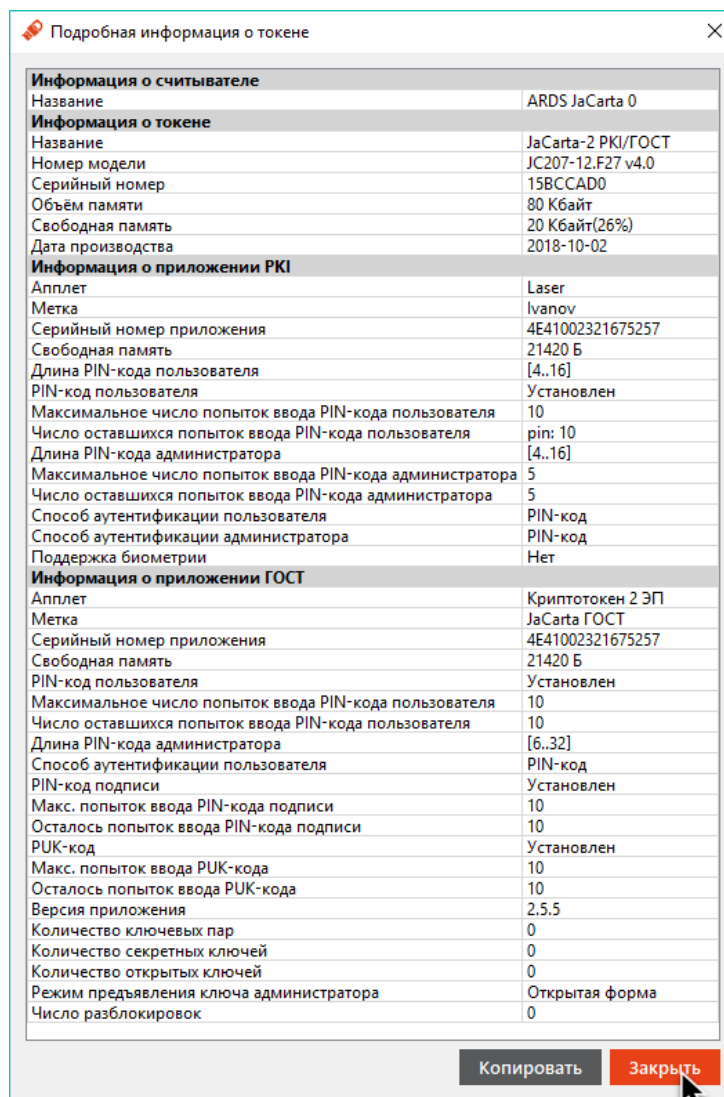


Рисунок 23 – Окно "Подробная информация о токене"

Окно "Подробная 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
 - "Объем памяти" – полный объем памяти электронного ключа;
 - "Свободной памяти" – объем 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.

- "Имя" – метка апплета.
- "Серийный номер приложения" – серийный номер электронного ключа.
Примечание. Для электронных ключей eToken серийный номер может отличаться в зависимости от приложения.
- "Свободная память" – объём свободной памяти электронного ключа.
- "Длина PIN-кода" – количество символов PIN-кода пользователя приложения.
- "PIN-код" – статус PIN-кода пользователя приложения: установлен/не установлен.
- "Максимальное количество попыток PIN-кода" – максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя.
- "Осталось попыток ввода PIN-кода" – количество неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода пользователя.
- "Длина PIN-кода администратора" – длина PIN-кода администратора выбранного приложения (только для приложений PKI, STORAGE, ГОСТ с апплетом Криптотокен).
- "Макс. попыток ввода PIN-кода администратора" – максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора (только для приложений PKI, PRO, STORAGE, ГОСТ с апплетом Криптотокен).
- "Осталось попыток ввода PIN-кода администратора" – количество неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода администратора (только для приложений PKI, PRO, STORAGE, ГОСТ с апплетом Криптотокен).
- "Способ аутентификации администратора" – установленный способ аутентификации администратора.
- "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 токена" – номер версии электронного ключа (только для приложения ГОСТ).
- "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)
- "Количество разблокировок" – количество успешно выполненных разблокировок PIN-кода пользователя (только для приложения ГОСТ с апплетом Криптотокен 2 ЭП)

6.2 Повторная инициализация датчика случайных чисел

Повторная инициализация датчика случайных чисел предусмотрена только для электронных ключей с приложением ГОСТ с апплетом Криптотокен.

Повторную инициализацию датчика случайных чисел рекомендуется выполнять не реже, чем раз в три года (36 месяцев).

Для повторной инициализации датчика случайных чисел с помощью Единого Клиента JaCarta требуется авторизация на электронном ключе с предъявлением PIN-кода пользователя

► **Для повторной инициализации датчика случайных чисел:**

1. Запустите Единый Клиент JaCarta и подключите электронный ключ с приложением ГОСТ с апплетом Криптотокен к разьему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.
2. Нажмите кнопку "Переключиться в режим администратора" и выберите вкладку "ГОСТ" для доступа к операциям приложения ГОСТ с апплетом Криптотокен:

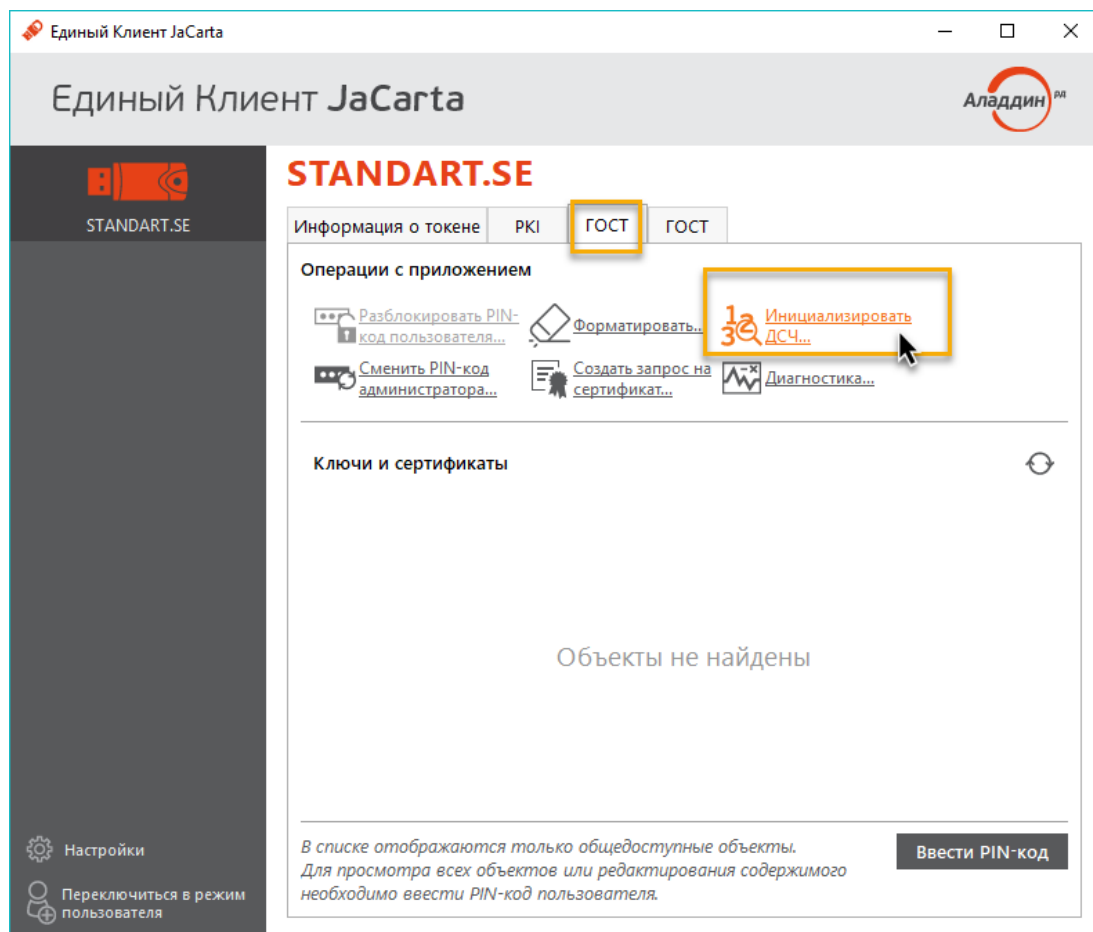


Рисунок 24 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Инициализировать ДСЧ..." активна

3. Нажмите кнопку "Инициализировать ДСЧ...". Будет отображено окно для ввода PIN-кода пользователя приложения:

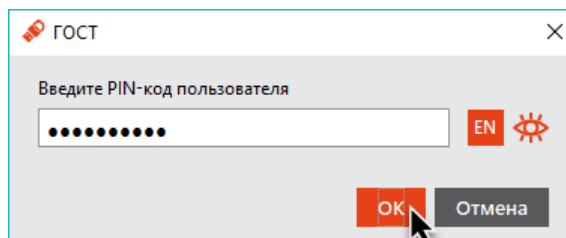


Рисунок 25 – Окно авторизации в приложении ГОСТ

4. В случае успешной авторизации в приложении будет отображено окно запуска инициализации датчика случайных чисел:

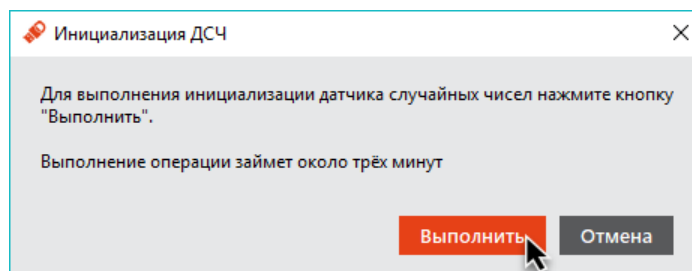


Рисунок 26 – Окно запуска инициализации датчика случайных чисел

5. Нажмите кнопку "Выполнить". Будет выполняться процедура инициализации ДСЧ. Процесс займёт некоторое время. При успешном завершении инициализации будет отображена информация об этом:

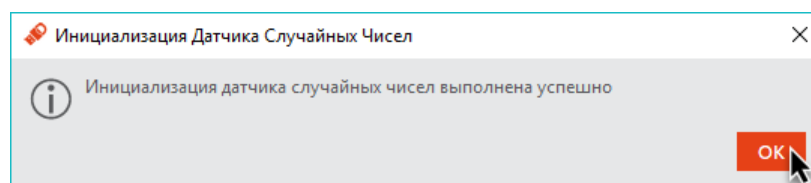


Рисунок 27 – Сообщение об окончании инициализации датчика случайных чисел

6. Нажмите кнопку "ОК" для закрытия окна.

6.3 Диагностика приложения

В ходе операции диагностики выполняется проверка работы базовой функциональности приложения. Операция диагностики предусмотрена для приложения ГОСТ с апплетом Криптотокен. 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 к разъему USB или считывателю смарт-карт компьютера. Если подключено несколько электронных ключей, то выберите значок нужного ключа в области слева.

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

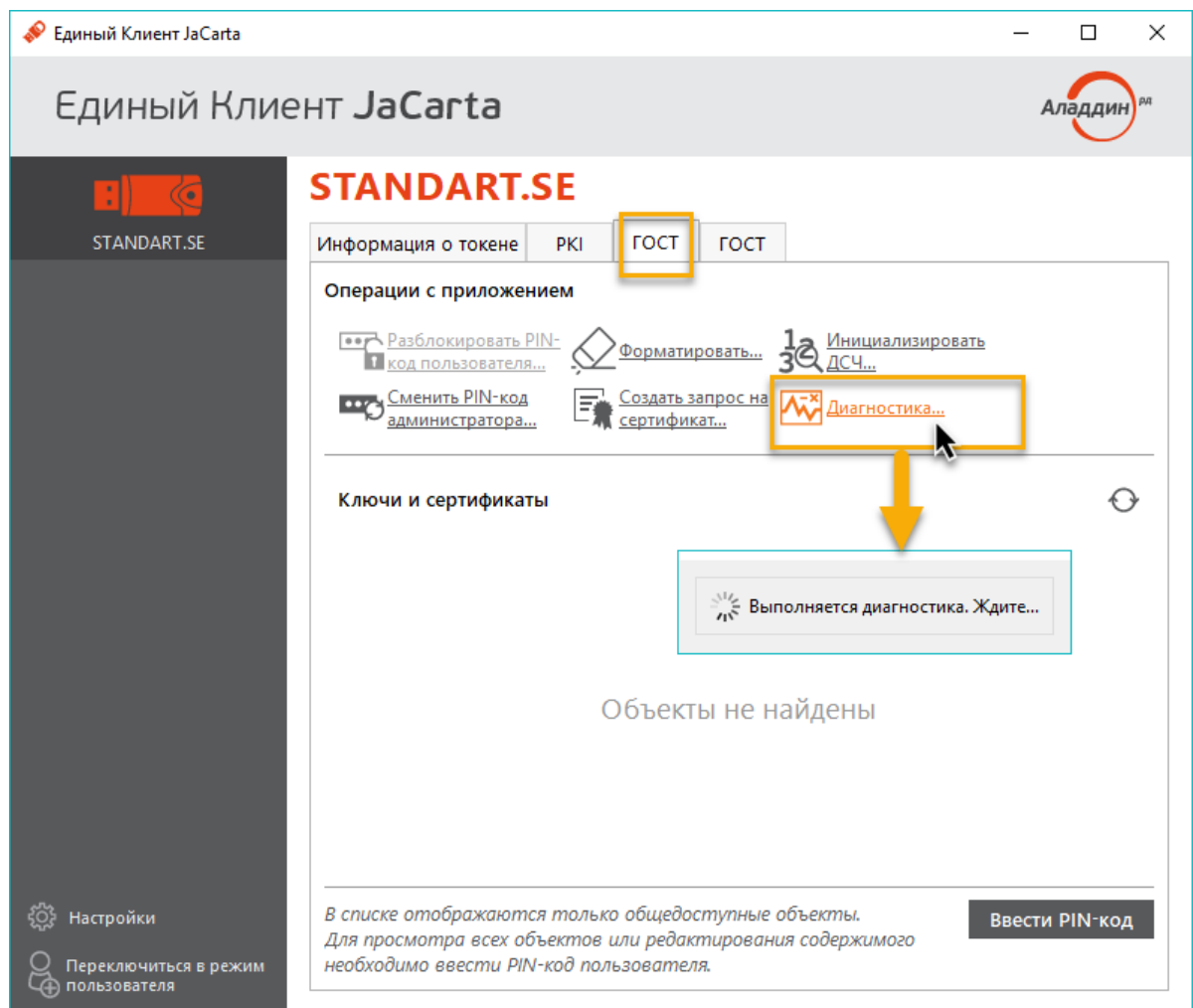


Рисунок 28 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Диагностика..." активна

- Нажмите кнопку "Диагностика". Будет выполняться диагностика приложения ГОСТ. В случае успешного завершения диагностики будет отображена информация об этом:

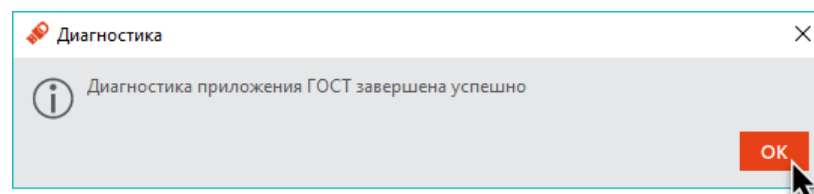


Рисунок 29 – Информация о завершении операции диагностики приложения ГОСТ

- Нажмите кнопку "OK" для закрытия окна.

6.4 Проверка целостности приложения

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

► Для диагностики приложения ГОСТ:

- 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.

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

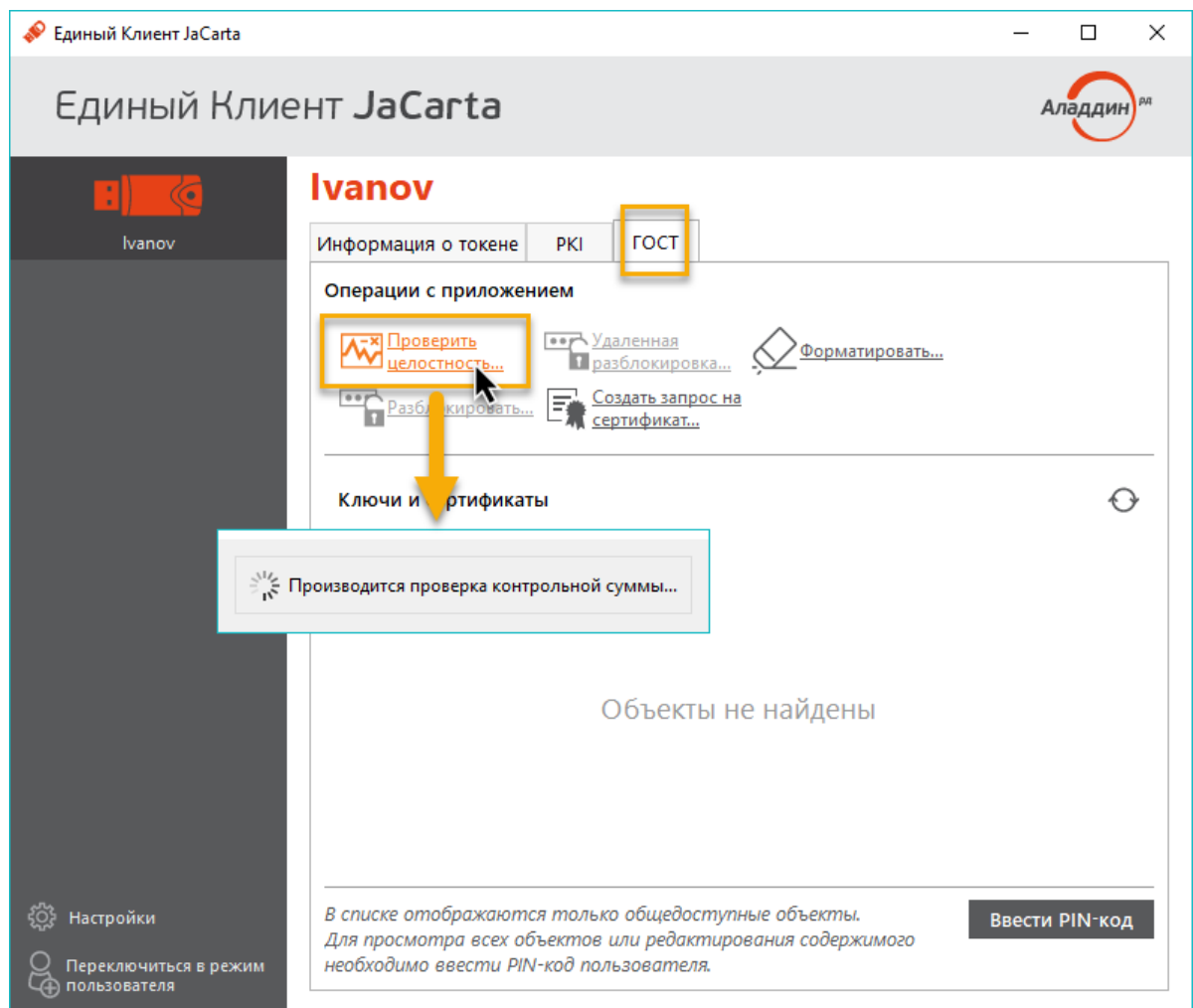


Рисунок 30 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Диагностика..." активна

- Нажмите кнопку "Проверить целостность". Будет выполняться проверка целостности приложения ГОСТ. В случае успешного завершения операции будет отображена информация об этом:

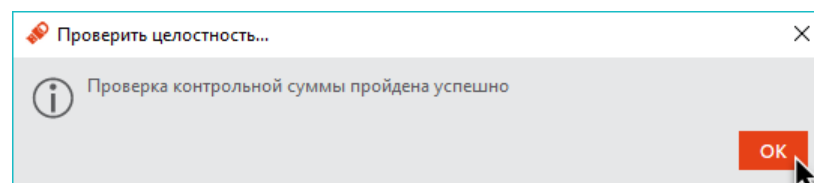


Рисунок 31 – Информация о завершении операции проверки целостности приложения ГОСТ

- Нажмите кнопку "OK" для закрытия окна.

6.5 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.

6.5.1 Создание запроса на сертификат

► Для создания запроса на сертификат:

- 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 режим администратора". Будет отображено основное окно Единого Клиента JaCarta в режиме администратора. Выберите вкладку с наименованием приложения, для которого необходимо создать запрос на сертификат (в данном примере выбрано приложение PKI) и нажмите кнопку "Создать запрос на сертификат". В появившемся окне с наименованием приложения введите PIN-код пользователя:

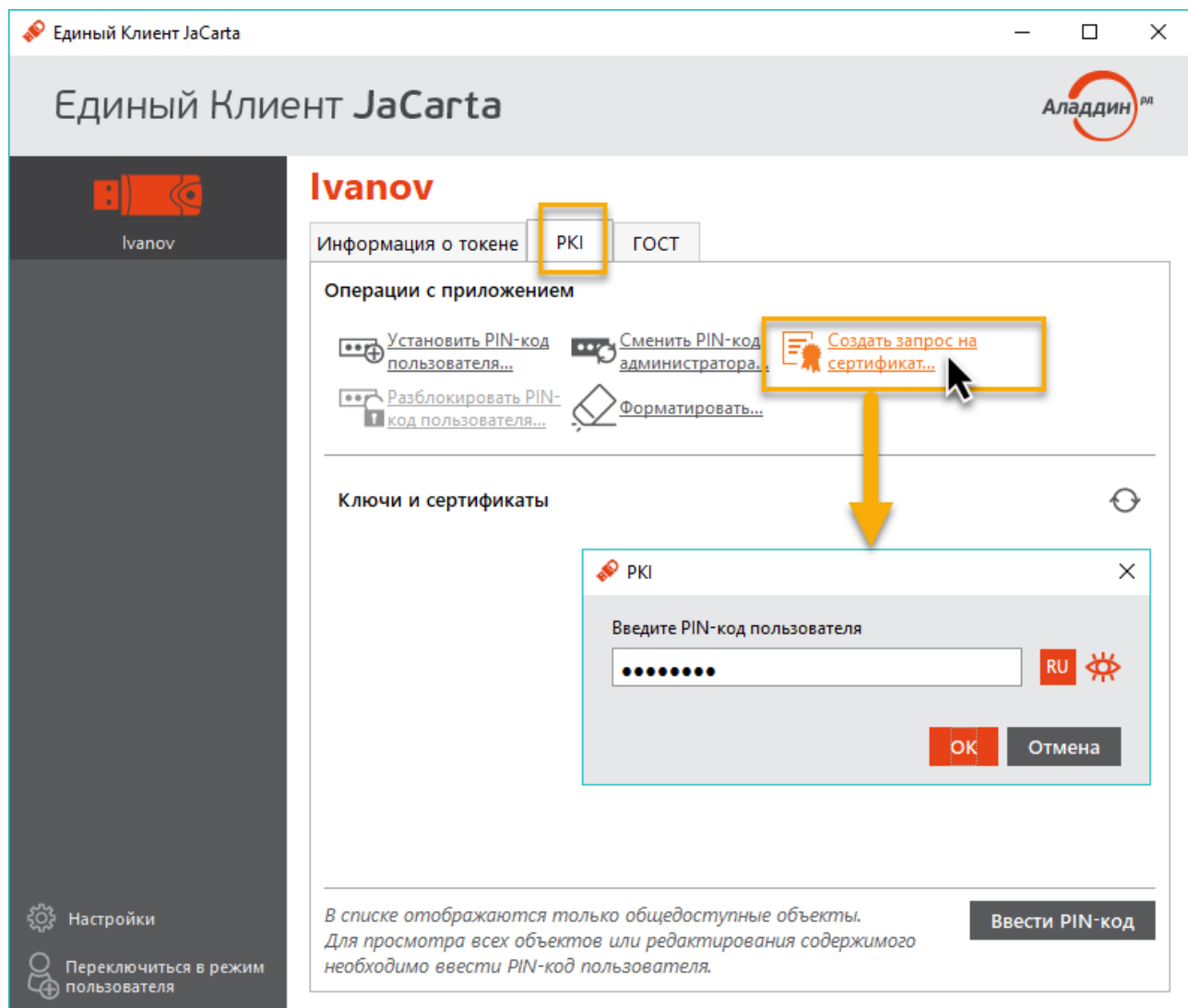


Рисунок 32 - Авторизация с помощью PIN-кода пользователя на электронном ключе в приложении PKI

3. Нажмите кнопку "OK". В случае успешной авторизации в приложении будет отображено окно "Создание запроса на сертификат" (см. рисунок 33). Заполните поля следующим образом:
- в поле "Имя" введите наименования создаваемого сертификата. Поле является обязательным для заполнения;
 - в поле "Использование ключа" установите отметку в нужных полях:
 - "цифровая подпись" (выбрано по умолчанию);
 - "неотказуемость" (выбрано по умолчанию);
 - "шифрование ключей" (выбрано по умолчанию);
 - "шифрование данных" (выбрано по умолчанию);
 - "согласование ключей";
 - "подписание сертификата с помощью ключа";
 - "подписание 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".
- 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".

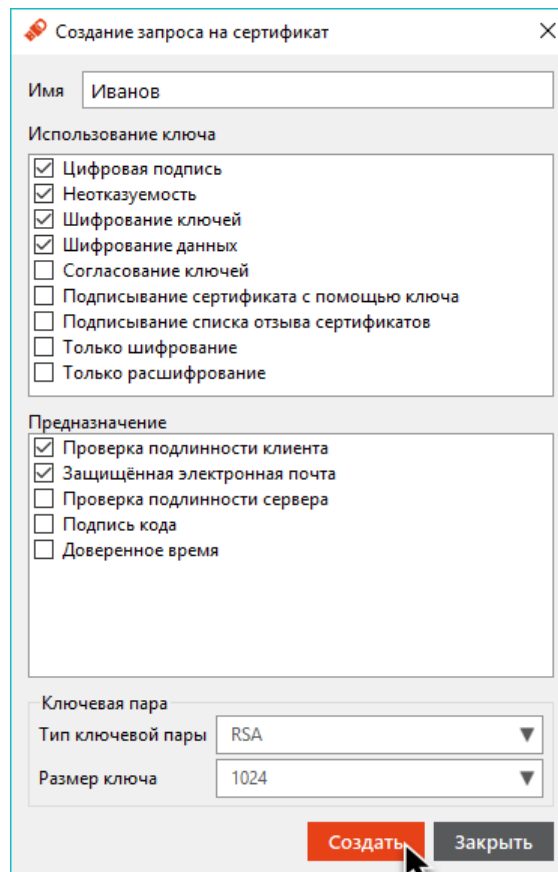


Рисунок 33 – Окно "Создание запроса на сертификат"

4. Нажмите кнопку "Создать". Будет открыто окно Проводника Windows для выбора папки сохранения запроса на сертификат. Выберите нужную папку и введите имя файла, в котором следует сохранить запрос на сертификат.
5. Нажмите кнопку "Сохранить" в окне Проводника Windows. Будет выполняться генерация ключевой пары и создание запроса на сертификат. На экране будет отображаться информация о процессе:

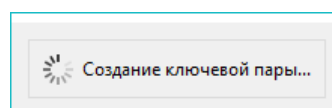


Рисунок 34 – Информация о процессе создания запроса на сертификат

По окончании процесса будет отображено окно с информацией о пути сохранения запроса на сертификат:

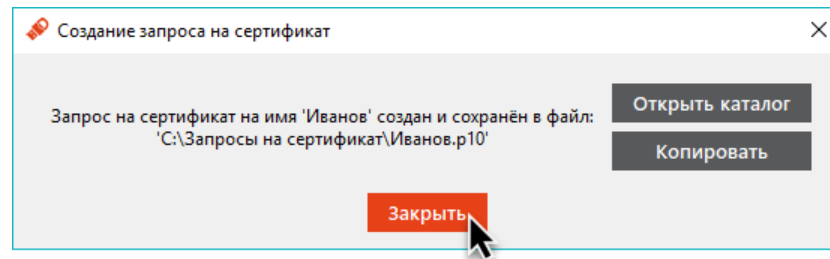


Рисунок 35 – Информация о завершении создания запроса на сертификат

6. При необходимости откройте папку в Проводнике Windows, в которой Единый Клиент JaCarta сохранил запрос на сертификат нажатием кнопки "Открыть каталог" или скопируйте запрос на сертификат в буфер обмена нажатием кнопки "Копировать".
7. Нажмите кнопку "Заккрыть" для закрытия окна "Создание запрос на сертификат".

6.5.2 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 режим администратора". Будет отображено основное окно Единого Клиента JaCarta в режиме администратора. 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:

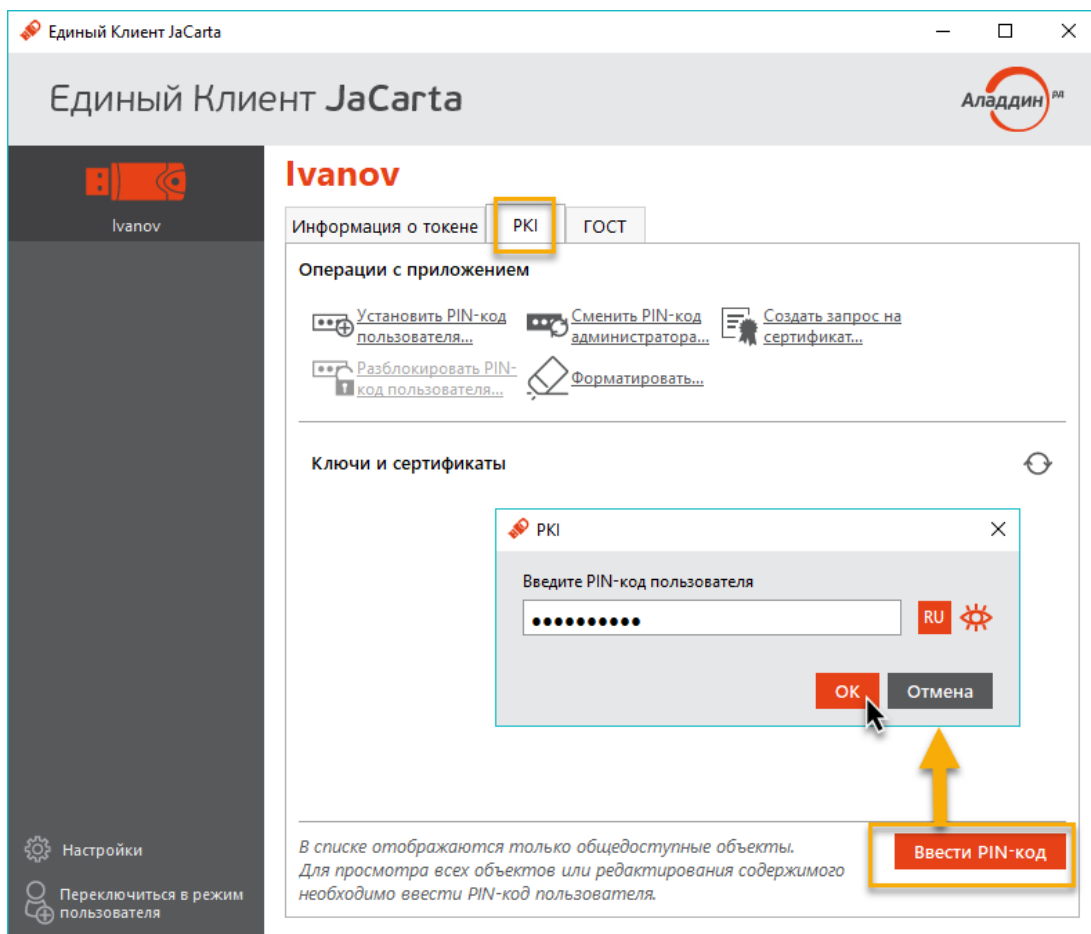


Рисунок 36 – Авторизация в приложении PKI

3. Нажмите кнопку "OK". 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:

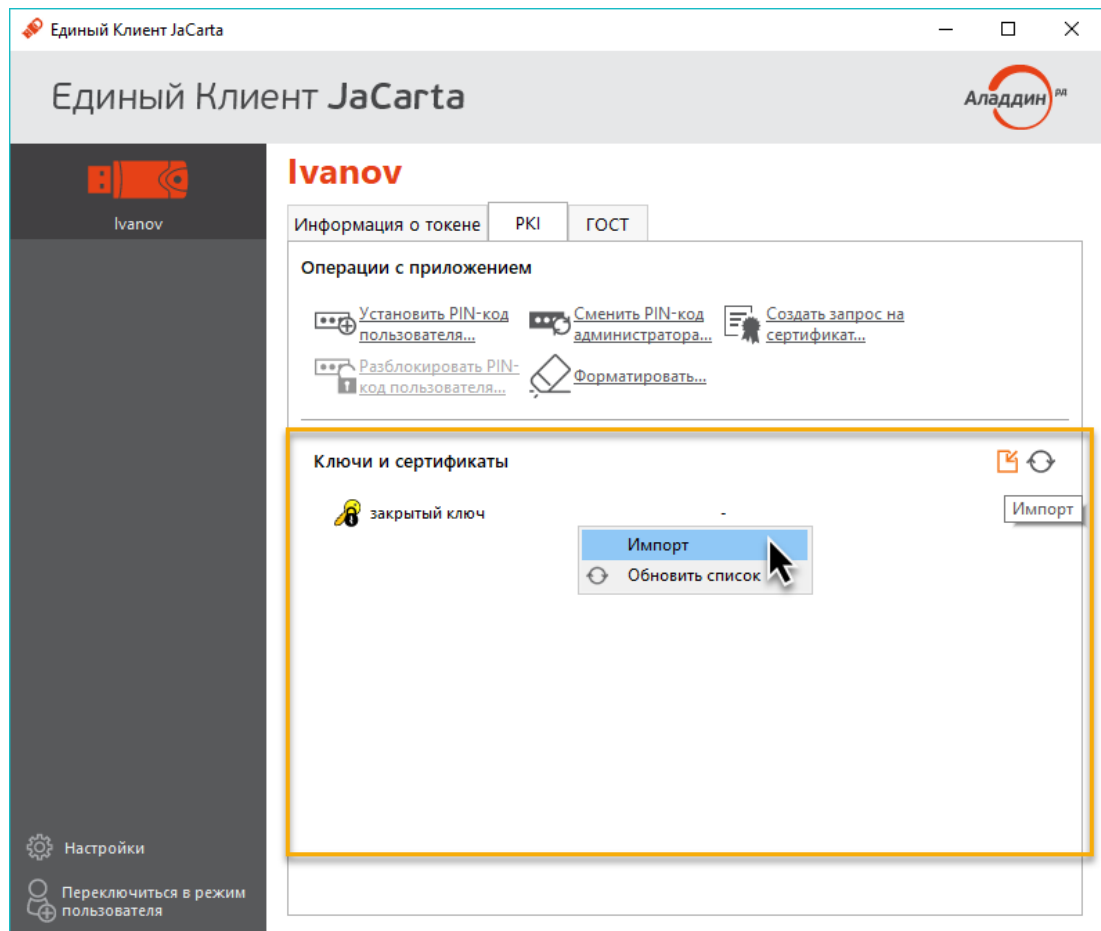



Рисунок 37 – Полный список объектов приложения и команда "Импорт"

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 импортируемым данным" укажите путь к импортируемому сертификату. Для этого нажмите кнопку "Обзор..." и в появившемся окне Проводника Windows выберите файл сертификата;
 - если импортируемый сертификат содержит защищённый паролем закрытый ключ, то введите его в поле "Введите пароль, защищающий закрытый ключ";
 - если импортируемый сертификат содержит цепочку сертификатов более высокого уровня, то для загрузки в память электронного ключа всей цепочки сертификатов установите отметку в поле "Загрузить всю цепочку";

- в поле "Задать 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.

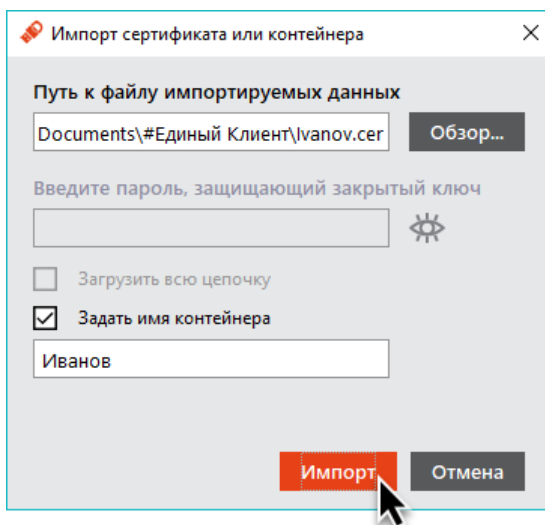


Рисунок 38 – Окно "Импорт сертификата или контейнера"

5. Нажмите кнопку "Импорт". Будет выполняться импорт сертификата в память приложения электронного ключа. ПО завершении операции на экране появится сообщение об этом:

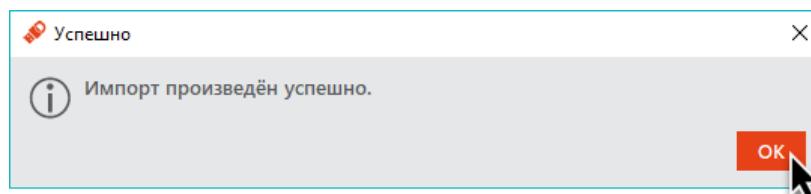


Рисунок 39 – Окно "Импорт сертификата или контейнера"

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

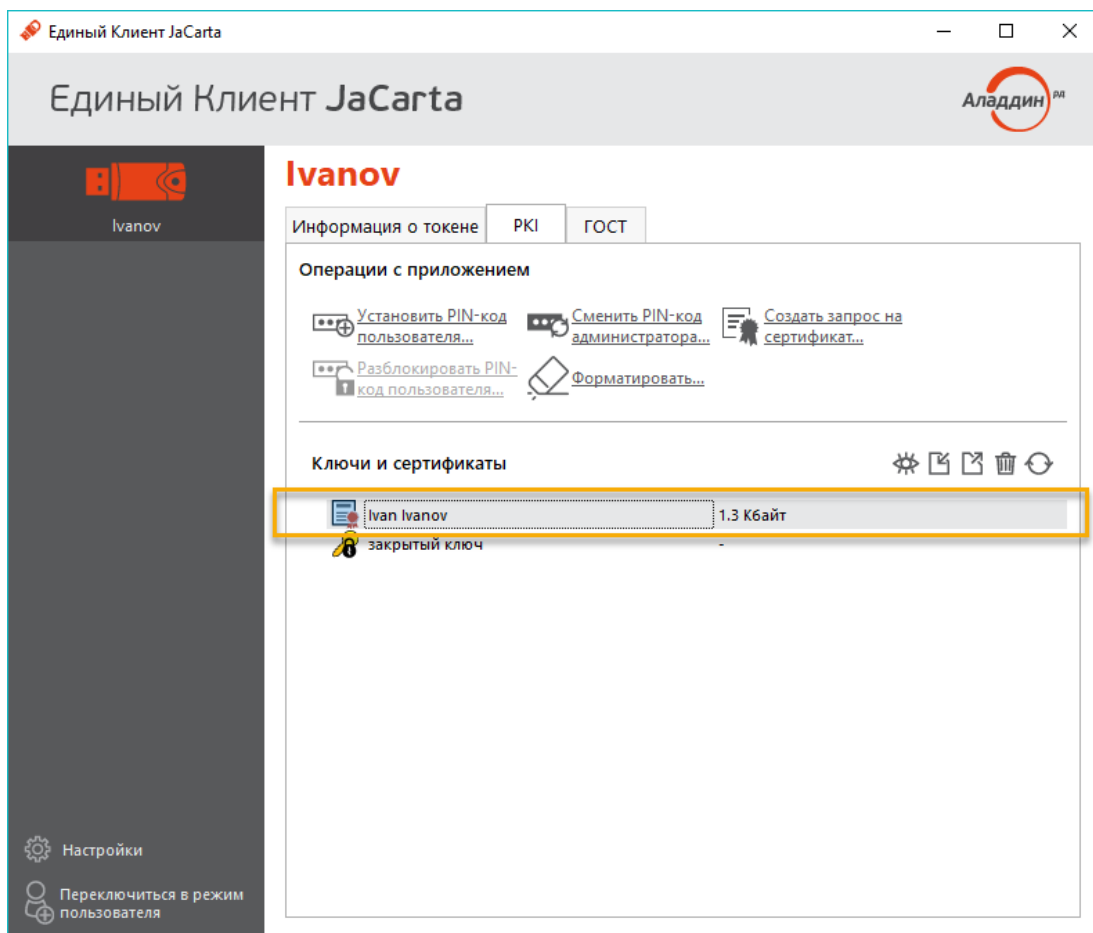



Рисунок 40 - Отображение импортированных объектов

6.5.3 Экспорт сертификата

► **Для экспорта сертификата в файл:**

- Авторизуйтесь в приложении электронного ключа, из которого необходимо экспортировать сертификат (см. п.п. 1-3 процедуры импорта сертификата в п. 6.5.2). В поле "Ключи и сертификаты"

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

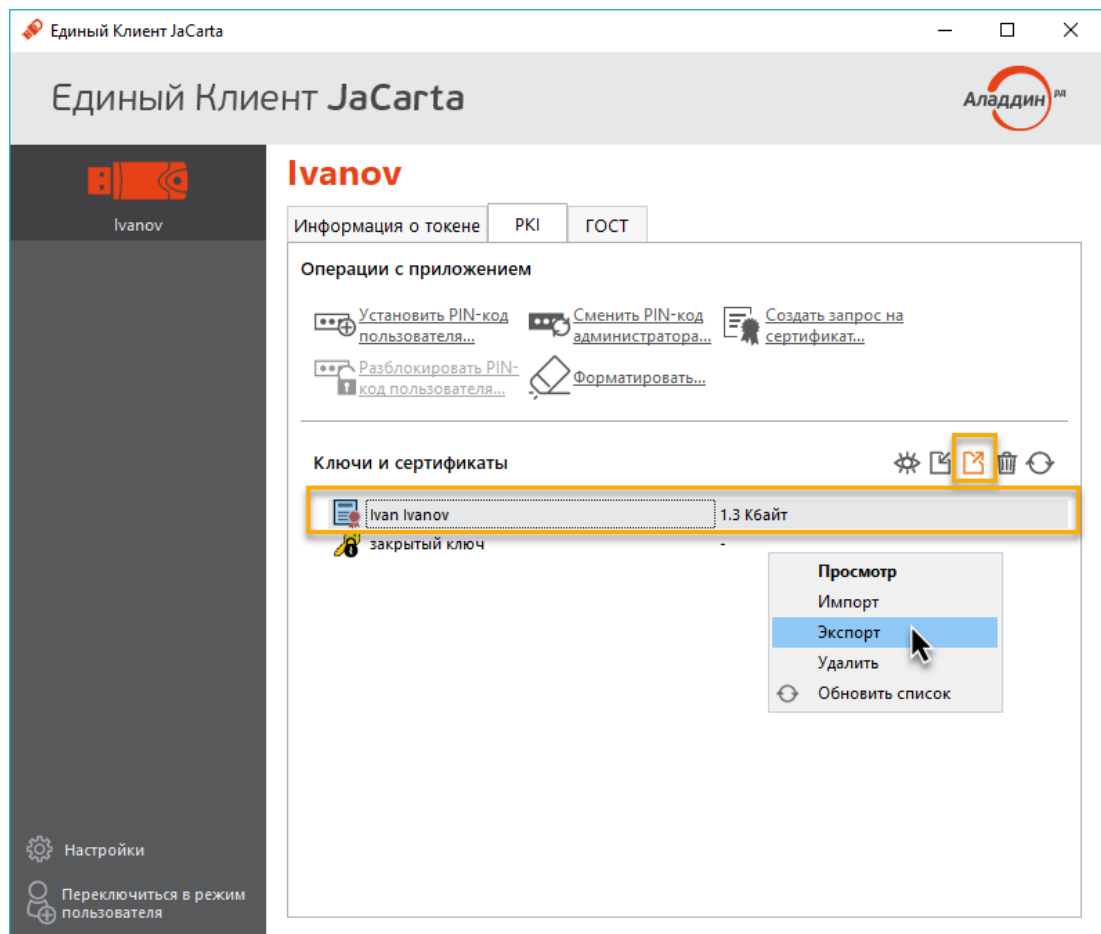


Рисунок 41 – Экспорт данных Единый Клиент JaCarta. Кнопки перехода к экспорту данных

2. Будет открыто окно для указания параметров экспорта сертификата (см. рисунок 42). Заполните поля следующим образом:
 - в поле "Укажите путь и имя файла..." укажите путь и имя файла для экспорта файла. Для этого нажмите кнопку "Обзор" и в появившемся окне Проводника Windows выберите нужную папку. Радио кнопка "В файл" при этом должна быть выбрана:

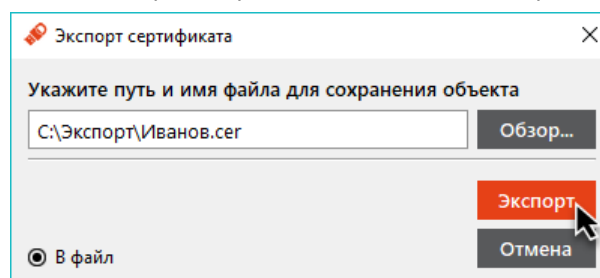


Рисунок 42 – Окно "Экспорт сертификата"

3. Нажмите кнопку "Экспорт". Будет выполняться экспорт выбранного объекта. Результат выполнения операции будет отображен в окне сообщения:

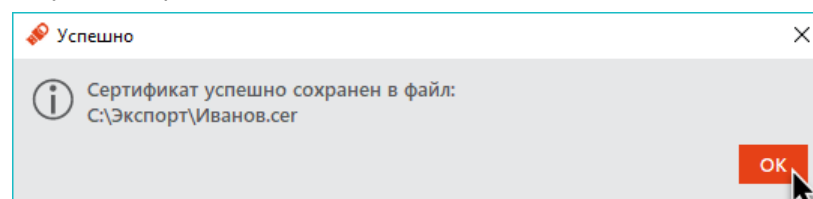



Рисунок 43 – Окно результатов экспорта

6.5.4 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. 6.5.2). В поле "Ключи и сертификаты" выберите сертификат и нажмите кнопку  или активируйте команду "Просмотр" в контекстном меню выбранного сертификата:

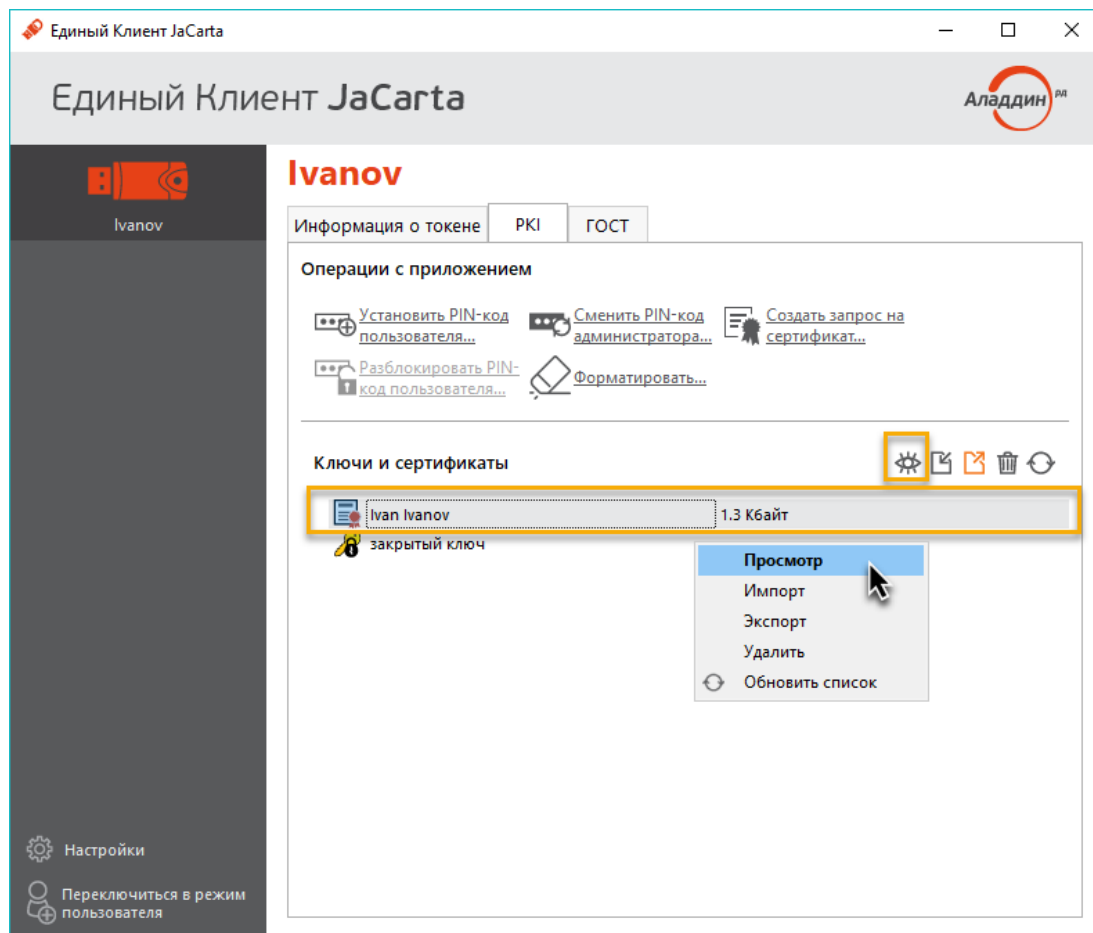


Рисунок 44 - Единый Клиент JaCarta. Кнопки перехода к просмотру сертификата

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

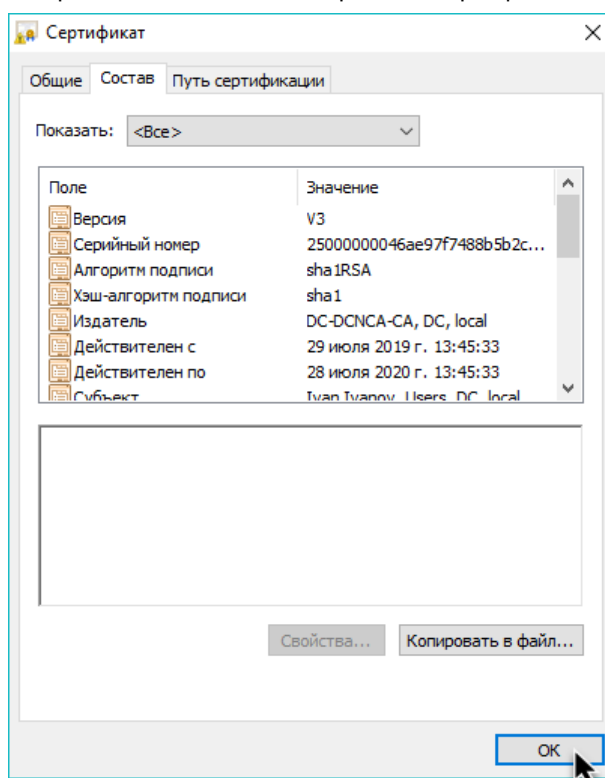


Рисунок 45 – Окно просмотра сертификата

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

6.6 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.

6.6.1 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.

- Нажмите кнопку "Переключиться в режим администратора" и выберите вкладку с наименованием нужного приложения. В поле "Ключи и сертификаты" будет отображен список общедоступных объектов, хранящихся в памяти электронного ключа (см. рисунок 46).

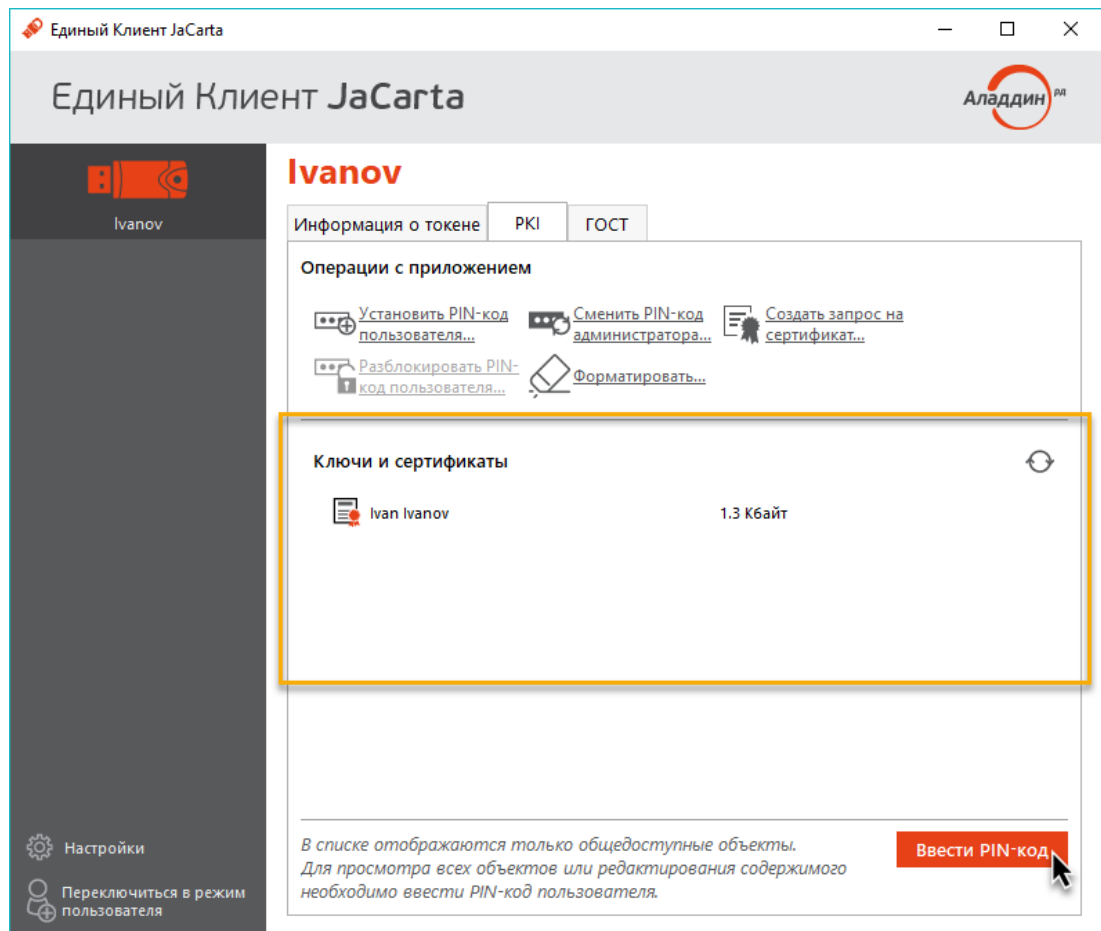


Рисунок 46 - Список общедоступных объектов в памяти электронного ключа

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

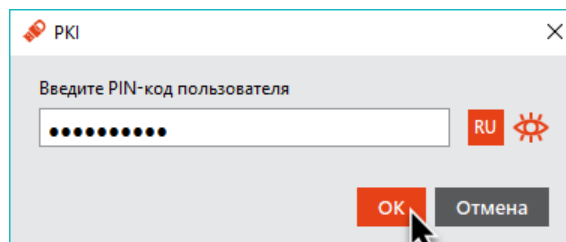


Рисунок 47 – Окно авторизации в приложении электронного ключа

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

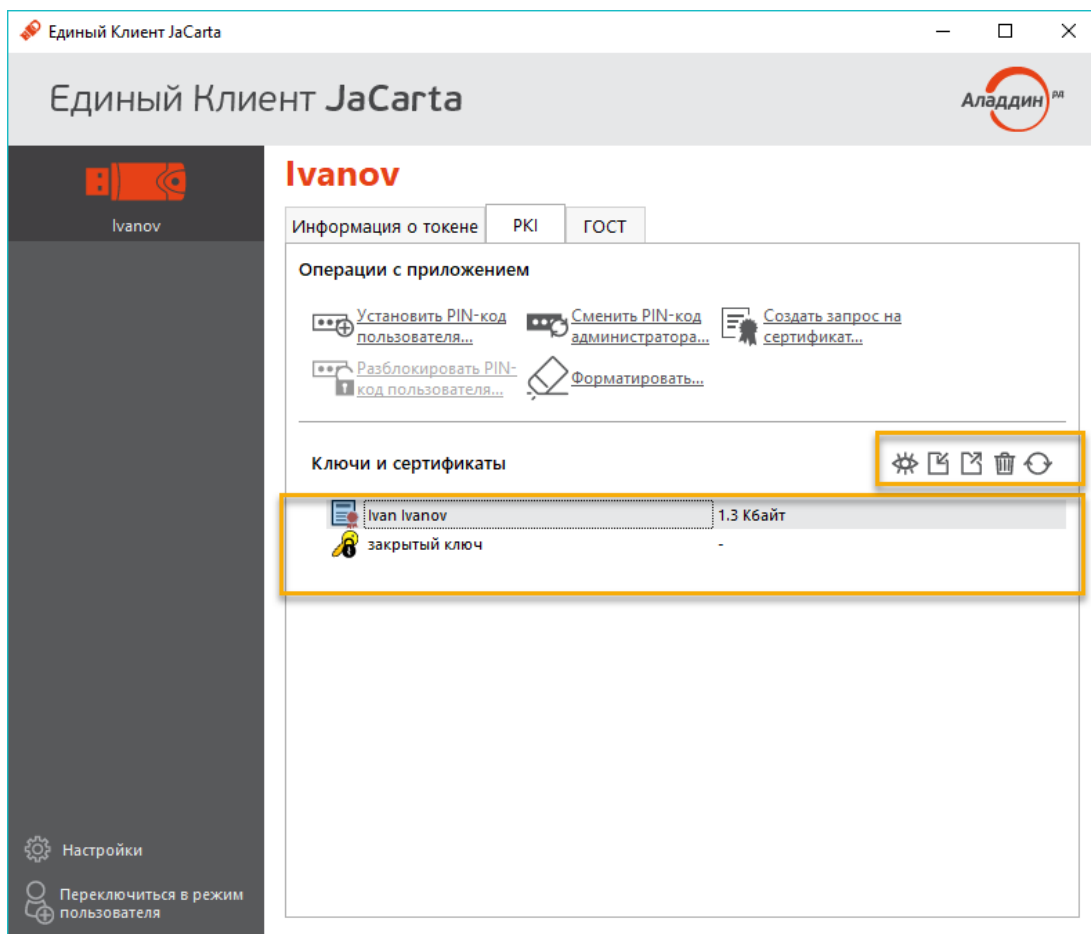



Рисунок 48 – Полный список объектов в памяти электронного ключа

6.6.2 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:

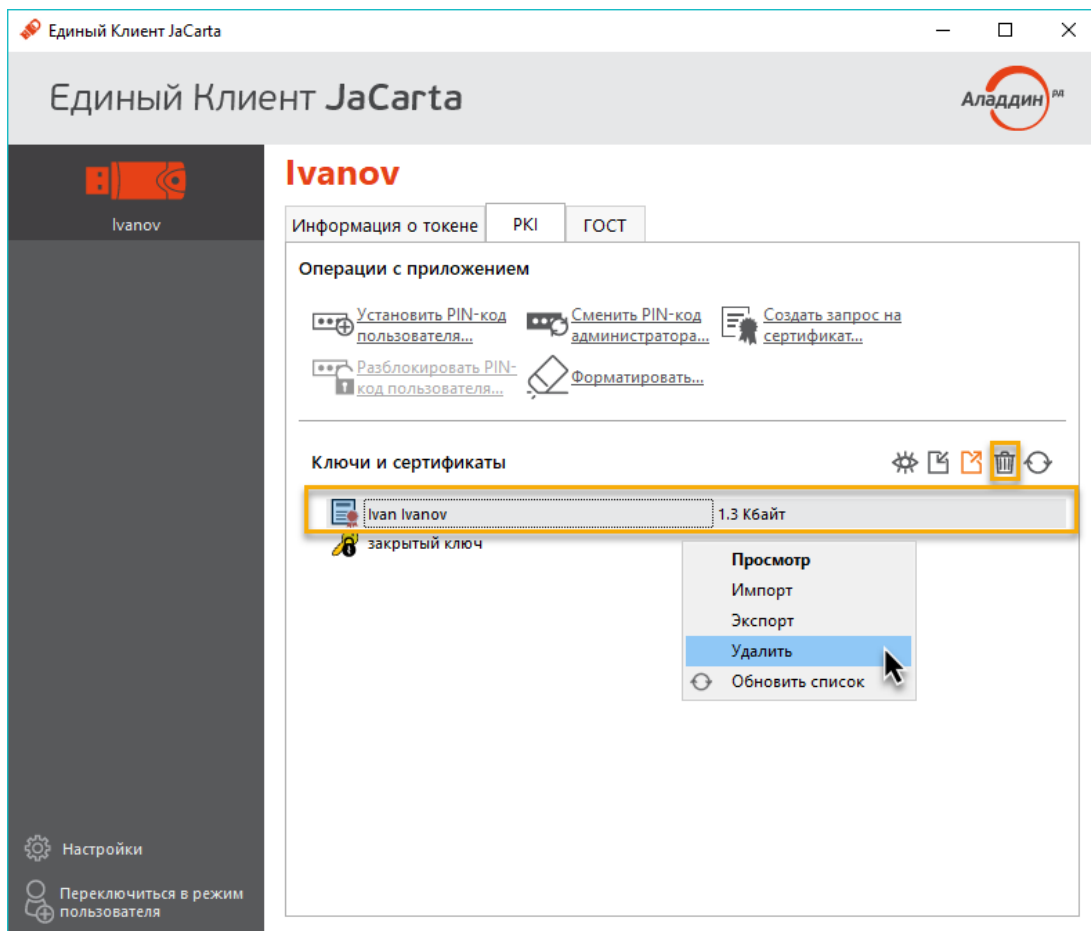


Рисунок 49 - Единый Клиент JaCarta. Кнопки перехода к удалению данных

2. Будет открыто окно для подтверждения удаления:

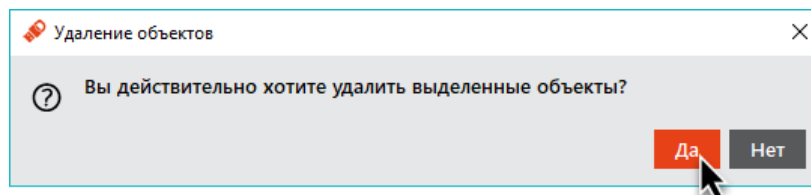
















Рисунок 50 - Окно "Удаление объектов"

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

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
	eToken PRO (Java)
	eToken NG-FLASH (Java)
	eToken NG-OTP (Java)
	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

7. Контакты

7.1 Офис (общие вопросы)

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

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: <https://www.aladdin-rd.ru>

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

7.2 Техподдержка

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

Регистрация изменений

<i>Версия</i>	<i>Изменения</i>
1.1	Обновлены скриншоты, исправлено форматирование к выходу новой сборки ЕК 2.12.2.2222
1.0	Создан документ

Коротко о компании

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

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

Основные направления

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

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
 Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
 Лицензия Министерства обороны РФ № 1384 от 22.08.16
 Система менеджмента качества компании соответствует требованиям ISO/ИСО 9001-2011
 Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15

© ЗАО "Аладдин Р.Д.", 1995 – 2019. Все права защищены
 Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru