



Средство администрирования устройств аутентификации

Единый Клиент JaCarta

Руководство пользователя для ОС Windows

Статус	Публичный
Листов	49

Оглавление

1. О документе	4
1.1 Назначение документа	4
1.2 На кого ориентирован данный документ	4
1.3 Организация документа	4
1.4 Рекомендации по использованию документа	4
1.5 Соглашения по оформлению	4
1.6 Авторские права, товарные знаки, ограничения	6
1.7 Лицензионное соглашение	6
2. Основные понятия	8
2.1 Назначение	8
2.2 Термины и определения	8
2.3 Режимы работы средства	8
2.4 Принципы безопасной работы средства	8
2.5 Функции и интерфейсы функций средства, доступные каждой роли пользователей	8
2.6 Параметры (настроек) безопасности средства, связанные с доступными пользователю функциями средства	9
2.7 Типы событий безопасности, связанные с доступными пользователю функциями средства	9
2.8 Действия после сбоев и ошибок эксплуатации средства	9
3. Общие сведения об электронных ключах	10
3.1 Приложения и модели электронных ключей	10
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 стандартном режиме	15
4.3.3 Основное окно в расширенном режиме	16
4.4 Просмотр сведений о программе	17
4.5 Завершение работы программы	17
5. Работа в программе в стандартном режиме	18
5.1 Просмотр информации об электронном ключе	18
5.2 Изменение названия (переименование) электронного ключа	19
5.3 Изменение PIN-кода пользователя	20
5.4 Разблокирование PIN-кода пользователя	23
5.4.1 Приложение PKI	23
5.4.2 Приложение ГОСТ	25
5.5 Установка PIN-кода подписи	26
5.6 Изменение PIN-кода подписи	28
5.7 Разблокирование PIN-кода подписи	29
6. Работа в программе в расширенном режиме	33
6.1 Просмотр информации о приложениях на электронном ключе	33
6.2 Диагностика целостности приложения	35
6.3 Операции с сертификатами в приложении электронного ключа	36
6.3.1 Создание запроса на сертификат	36
6.3.2 Импорт сертификата	39
6.3.3 Экспорт сертификата	42
6.3.4 Просмотр сертификата	43

6.4	Операции с объектами в приложении электронного ключа	44
6.4.1	Просмотр списка объектов.....	44
6.4.2	Удаление объектов	46
Приложение А. Обозначения электронных ключей		48
Контакты.....		49

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.

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 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.

1.4 Рекомендации по использованию документа

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







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

1.5 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице (см. Таблица 1).

Таблица 1 – Элементы оформления

Элемент	Описание
Ctrl+X	Используется для выделения сочетаний клавиш
file.exe	Используется для выделения имен файлов, каталогов, текстов программ
Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
<u>Гиперссылка</u>	Используется для выделения внешних ссылок
Ссылка [стр. 4]	Используется для выделения перекрестных ссылок

 <i>Важно</i>	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 Кыргызской Республики. Обладателем исключительных авторских и имущественных прав является ОсОО "Аладдин КГ".

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством Кыргызской Республики. При перепечатке и использовании данных материалов либо любой их части ссылки на ОсОО "Аладдин КГ" обязательны.

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

Ограничение ответственности

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

ОсОО "Аладдин КГ" 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.

ОсОО "Аладдин КГ" 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 стандартах и результатах тестирования, полученных в

независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ОсОО "Аладдин КГ" не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ОсОО "Аладдин КГ" 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 ОсОО "Аладдин КГ" 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 ОсОО "Аладдин КГ" (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 ОсОО "Аладдин КГ" 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 ОсОО "Аладдин КГ" (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.

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 Кыргызской Республики и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Кыргызской Республики 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 Кыргызской Республики.

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 Кыргызской Республики, 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 ОсОО "Аладдин КГ" 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 такого и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Кыргызской Республики (за исключением конфликта применения правовых норм), и только суд Кыргызской Республики 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 УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

2. Основные понятия

2.1 Назначение

ПО "Единый Клиент JaCarta" — программное обеспечение, предназначенное для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты.

2.2 Термины и определения

PIN-код администратора¹ – 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.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

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

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

2.3 Режимы работы средства

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

2.4 Принципы безопасной работы средства

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

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

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

2.5 Функции и интерфейсы функций средства, доступные каждой роли пользователей

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

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

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

Интерфейсы функций описаны для каждой отдельной операции, совершаемой программой.

¹ Применимо для приложения ГОСТ

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

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

Проверяемые характеристики параметров безопасности:

- знание PIN-кода;
- владение электронным ключом.

2.7 Типы событий безопасности, связанные с доступными пользователю функциями средства

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

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

2.8 Действия после сбоев и ошибок эксплуатации средства

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

Таблица 2 – Виды сбоя эксплуатации и действия в случае сбоя

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

3. Общие сведения об электронных ключах

3.1 Приложения 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.

Примечание. Наименование приложения не всегда содержится в названии модели электронного ключа. Название модели и приложения электронного ключа отображается в интерфейсе ПО "Единый Клиент JaCarta" в стандартном режиме (см. раздел 5 "Работа в программе в стандартном режиме")

Приложение определяет некоторый набор функциональности электронного ключа, характерный для решения определенного ряда задач. Так, приложение PKI обеспечивает поддержку западных криптоалгоритмов и позволяет решать широкий спектр задач аутентификации, шифрования и работы с электронной подписью в корпоративной инфраструктуре. Приложение ГОСТ обеспечивает поддержку криптоалгоритмов для решения задач аутентификации, шифрования и работы с электронной подписью в системах, требующих использования алгоритмов ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018, ГОСТ 34.13-2018.

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

Таблица 3 – Соответствие приложений и моделей электронных ключей

Приложение	Модели электронных ключей
Приложение PKI	JaCarta KG
Приложение ГОСТ	JaCarta KG

3.2 Параметры электронных ключей при поставке

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

Таблица 4 – Параметры электронных ключей при поставке

Параметр, операция	Приложение PKI	Приложение ГОСТ
PIN-код пользователя по умолчанию ²	11111111	1234567890
PUK-код для разблокирования	не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	00000000	0987654321
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	невозможно
Форматирование без назначения PIN-кода администратора	невозможно	невозможно
При разблокировании PIN-кода пользователя сбрасывается счетчик ввода неправильного PIN-кода пользователя, при этом PIN-код пользователя задается заново	... PIN-код пользователя остается прежним
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	возможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно (настраивается политикой)

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

3.3 Информация о PIN-коде пользователя

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

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

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

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

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


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

Для заблокированных приложений доступна операция разблокирования PIN-кода пользователя. Данная операция выполняется администратором, описание ее выполнения приведено в документе "KG EK. Руководство администратора для Windows".

4. Обзор пользовательского интерфейса

4.1 Запуск Единого Клиента JaCarta

► Для запуска ПО "Единый Клиент JaCarta" необходимо:

1. Запустить ПО "Единый Клиент JaCarta" из меню "Пуск" или с панели быстрого доступа;
2. Откроется основное окно ПО "Единый Клиент JaCarta" (см. Рисунок 1), при этом в панели управления в нижней части экрана появится значок вызова меню быстрого запуска программы . По умолчанию основное окно Единого Клиента JaCarta открывается в стандартном режиме;

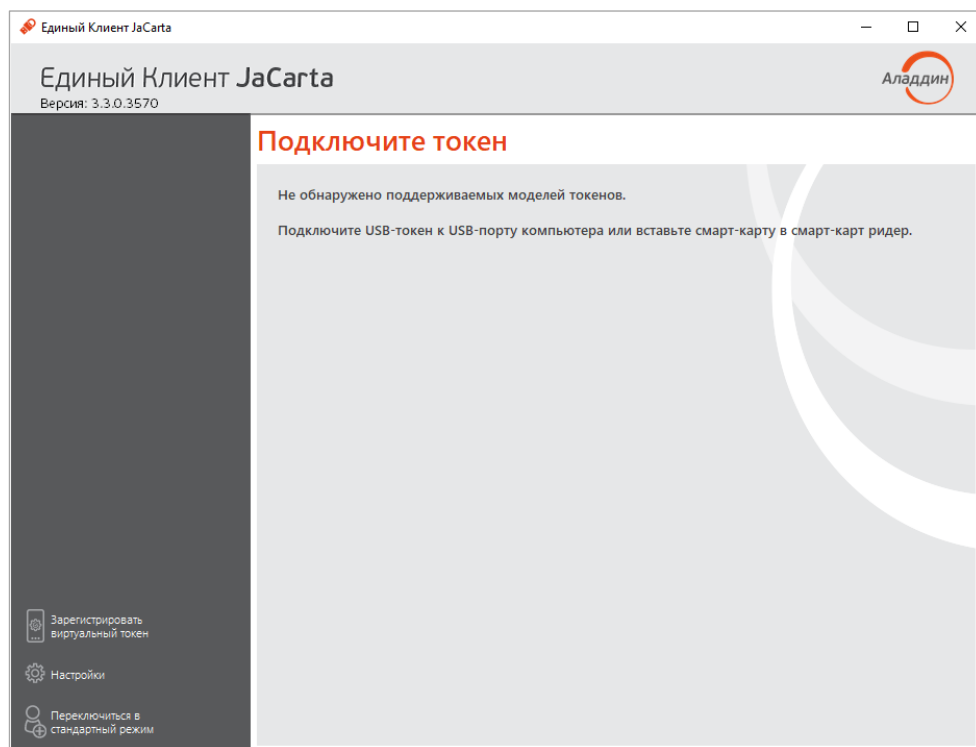




Рисунок 1 – Основное окно ПО "Единый Клиент JaCarta"

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

4.2 Меню быстрого запуска

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

Для вызова меню быстрого запуска необходимо открыть контекстное меню значка  в панели управления (см. Рисунок 2).

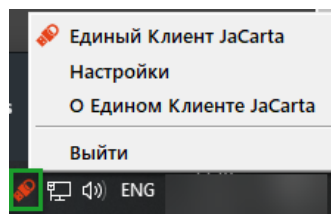



Рисунок 2 – Меню быстрого запуска Единого Клиента JaCarta

Меню быстрого запуска содержит следующие команды:

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

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

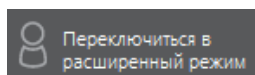
4.3 Режимы работы программы

Единый Клиент JaCarta поддерживает следующие режимы работы:

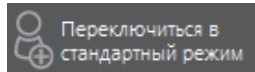
1. **Стандартный режим** – позволяет просматривать краткие сведения о подсоединённых электронных ключах, сменить PIN-код пользователя, назначить или изменить PIN-код подписи, изменить метку электронного ключа.
2. **Расширенный режим** – позволяет просматривать подробные сведения о подсоединённых электронных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

4.3.1 Переключение между режимами

Чтобы определить в каком режиме открыто окно 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 необходимо:

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

4.3.2 Основное окно в стандартном режиме

По умолчанию основное окно Единого Клиента JaCarta открывается в стандартном режиме. На рисунке (см. Рисунок 3) приведен вид основного окна в стандартном режиме с подключенным к компьютеру пользователем электронным ключом.

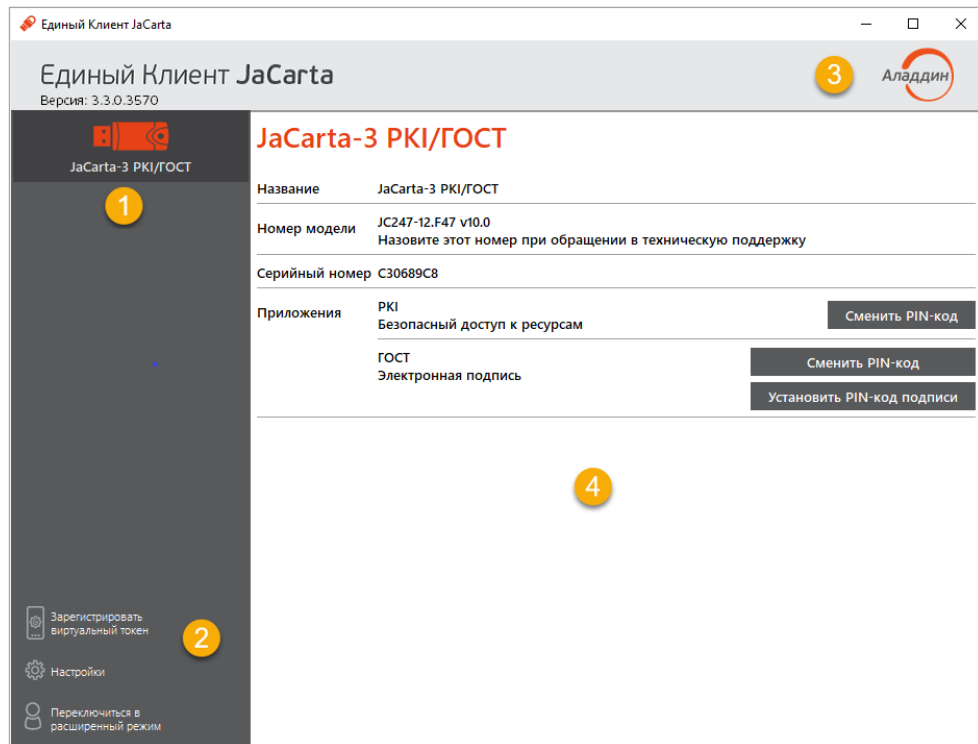


Рисунок 3 – Основное окно Единого Клиента JaCarta в стандартном режиме

Основное окно в стандартном режиме содержит следующие области:

- 1 Область для отображения подсоединенных к компьютеру электронных ключей.
Если к компьютеру пользователя Единого Клиента JaCarta не подсоединен ни один электронный ключ, то данная область пуста.
Если подсоединено несколько электронных ключей, то для работы с конкретным ключом 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 (Приложение А. Обозначения электронных ключей)
- 2 Область содержит кнопки:
 - "Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе "KG EK. Руководство администратора для 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

На рисунке (см. Рисунок 4) приведен вид основного окна в расширенном режиме с подключенным к компьютеру пользователя электронным ключом.

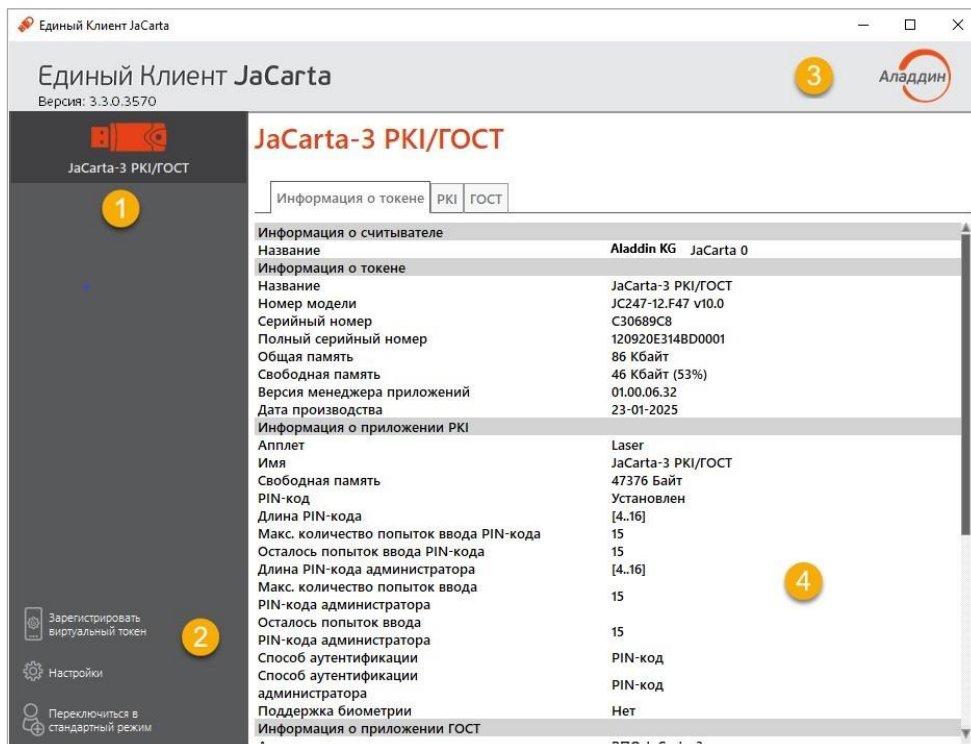


Рисунок 4 – Основное окно Единого Клиента JaCarta в расширенном режиме

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 щелкнуть значок нужного ключа, после чего в области 4 будет отображен полный список его свойств.
Вид значка, обозначающий подключенный электронный ключ различается в зависимости от типа ключа. Перечень значков приведен в приложении (Приложение А. Обозначения электронных ключей)
- 2 Область содержит кнопки:
 - "Настройки" – кнопка для вызова окна настроек программы. Описание работы с настройками приведено в документе "KG EK. Руководство администратора для Windows";
 - "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. 4.3.1 "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 (см. Рисунок 4) электронный ключ содержит приложение PKI и приложение ГОСТ, поэтому данная область содержит вкладку "Информация о токене", 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 необходимо:

1. В основном окне программы нажать кнопку с логотипом компании в верхнем правом углу либо активируете 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 (см. Рисунок 5);

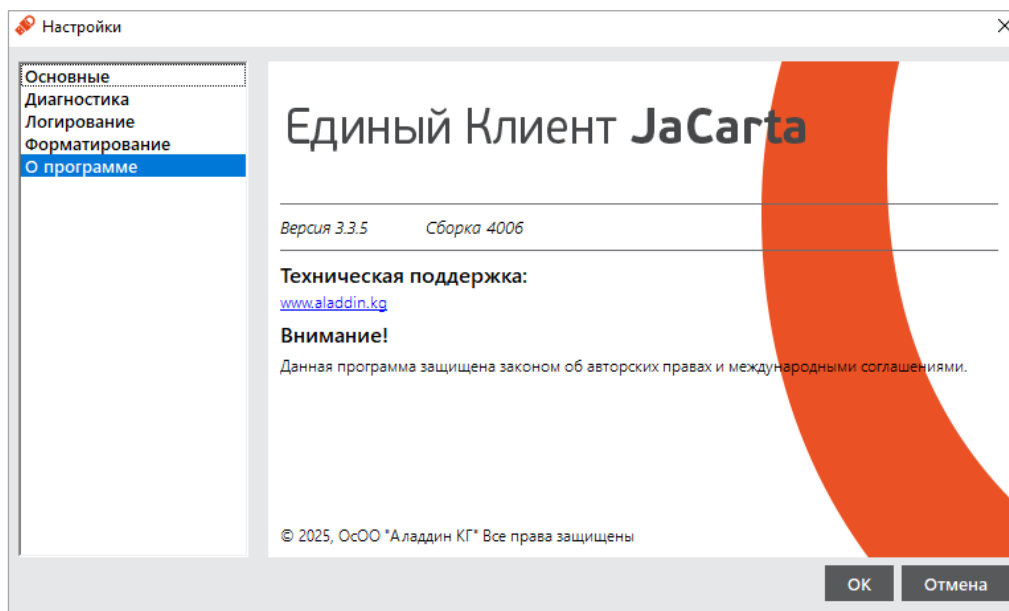



Рисунок 5 - Окно "О программе"

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

4.5 Завершение работы программы

- Для завершения работы программы необходимо:

1. Активировать 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).

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 необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева (см. Рисунок 6).

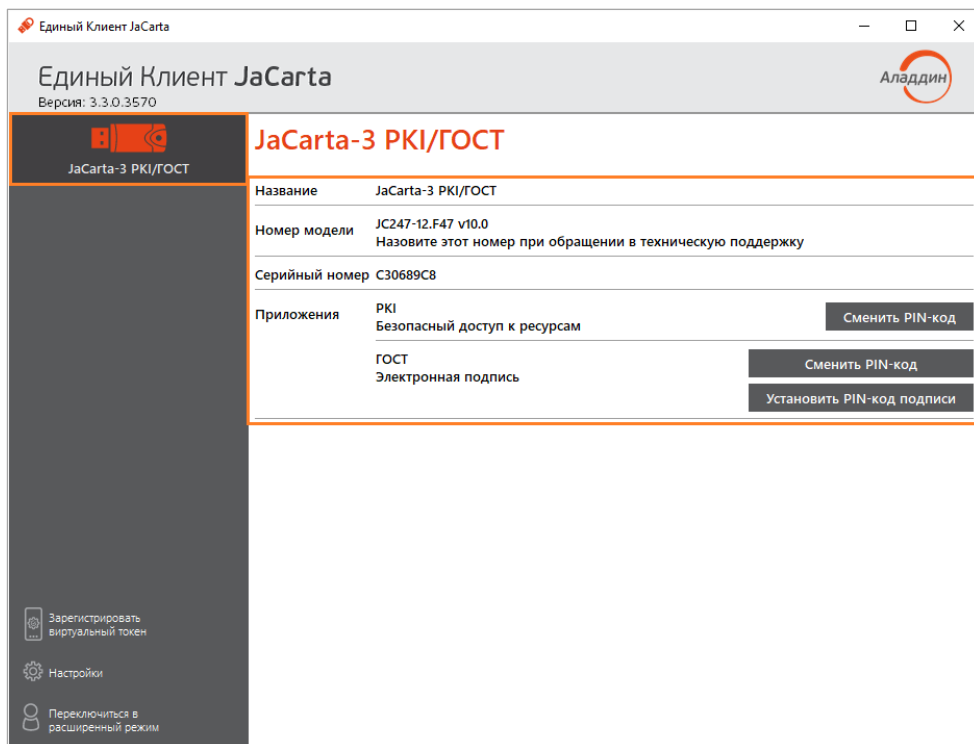


Рисунок 6 – Информация о выбранном электронном ключе в стандартном режиме

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 (см. Рисунок 6) приоритетным приложением является приложение PKI.
3. Закрывать основное окно Единого Клиента JaCarta нажатием кнопки "Закрывать" 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 необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Активировать команду "Переименовать токен" в контекстном меню (нажатием правой кнопки мыши) выбранного значка (см. Рисунок 7);

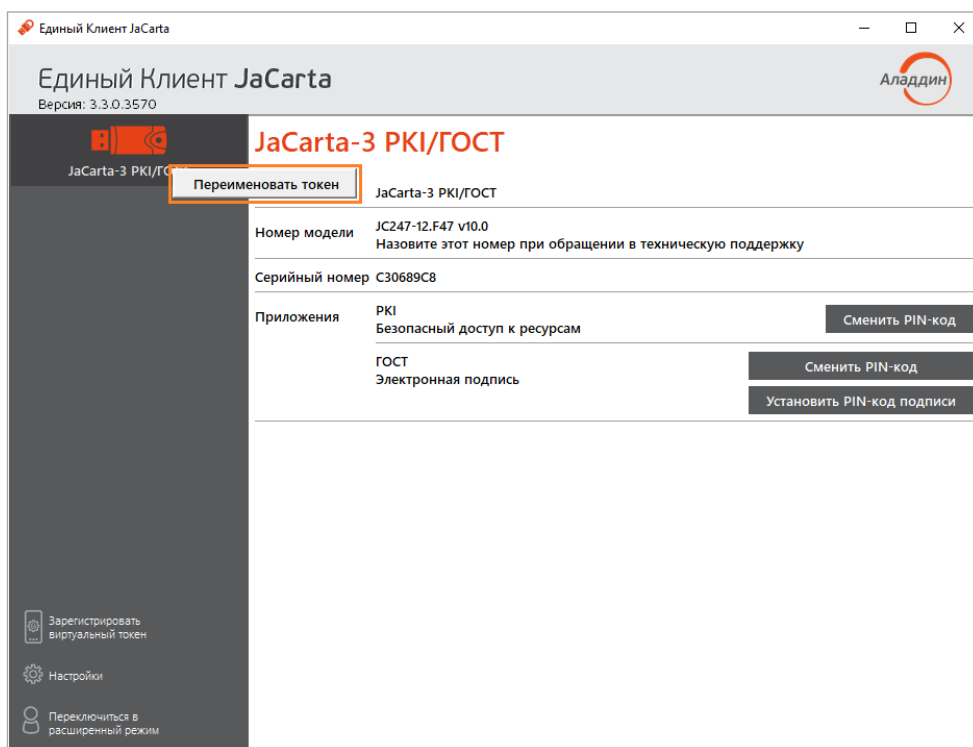


Рисунок 7 – Вызов окна "Переименовать токен" в стандартном режиме

4. Будет отображено одноименное окно (см. Рисунок 8);

Рисунок 8 – Окно "Переименовать токен" в стандартном режиме

5. В окне "Переименовать токен" заполнить следующие поля:
 - в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя. Если на электронном ключе установлено несколько приложений, то ввести PIN-код приложения, которое является приоритетным – это приложение отображается первым в списке установленных приложений в основном окне;
 - в поле "Новое имя" ввести новое имя электронного ключа.
6. Нажать кнопку "OK". В случае успешной авторизации на электронном ключе его имя будет изменено (см. Рисунок 9).

Рисунок 9 – Основное окно в стандартном режиме. Имя ключа изменено

5.3 Изменение PIN-кода пользователя

В случае отображения в окне Единого Клиента JaCarta сообщения о том, что установлен PIN-код по умолчанию (см. Рисунок 10), рекомендуется сменить PIN-код пользователя.

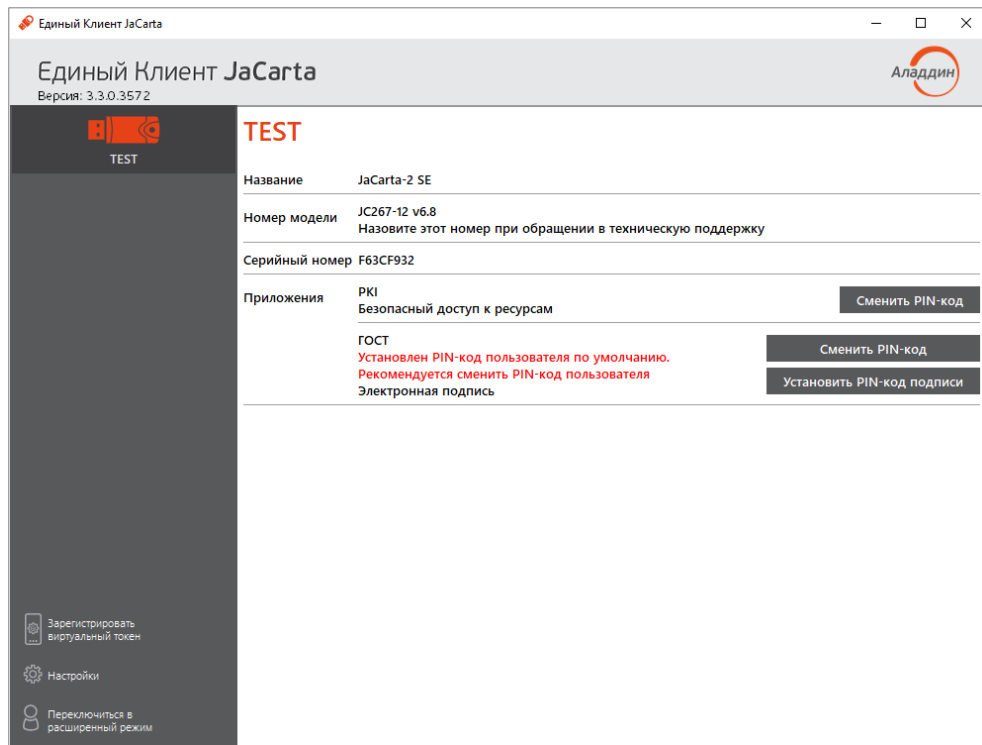


Рисунок 10 – Окно Единого Клиента JaCarta



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

► Для изменения PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Сменить PIN-код" для выбранного приложения. На рисунке (см. Рисунок 11) приведен пример смены PIN-кода приложения PKI;

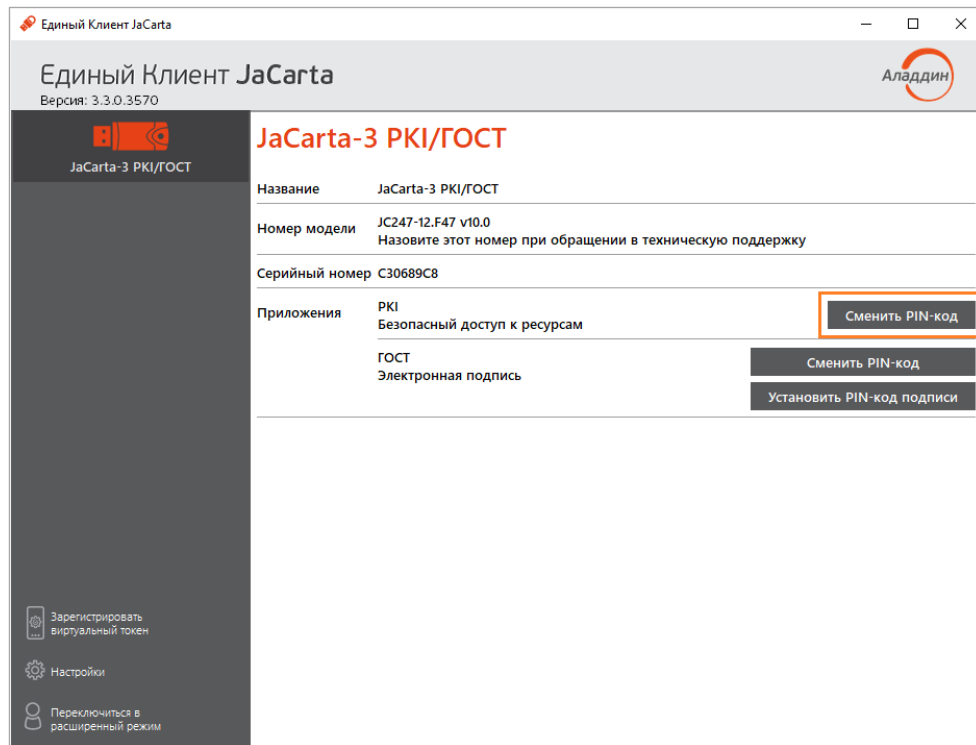


Рисунок 11 – Вызов окна "Переименовать токен" в стандартном режиме

4. В окне "Сменить PIN-код" заполнить следующие поля (см. Рисунок 12):

- в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя выбранного приложения (в данном примере приложения PKI);
- в поле "Новый PIN-код пользователя" ввести значение нового PIN-кода пользователя;
При задании нового PIN-кода рекомендуется использовать буквы только латинского алфавита (abc...z, ABC...Z), цифры (123...0) и спецсимволы (~!@#...). Использование пробела и символов кириллицы недопустимо. Минимальная длина PIN-кода пользователя составляет 4 символа.
- в поле "Подтвердить PIN-код пользователя" ввести значение нового PIN-кода пользователя повторно.

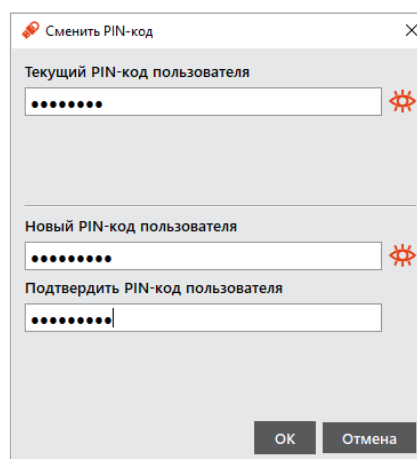


Рисунок 12 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода введены верно

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 "OK" неактивна) до тех пор, пока не будет введено другое значение PIN-кода (см. Рисунок 13).

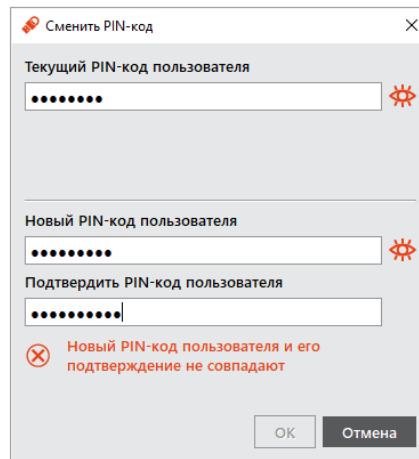




Рисунок 13 – Окно изменения PIN-кода пользователя. Значения нового PIN-кода не совпадают

По умолчанию введенные значения PIN-кода показаны в скрытом виде. Чтобы показать их в явном виде нажать кнопку . Для возвращения к отображению в скрытом виде нажать кнопку  (см. Рисунок 14).

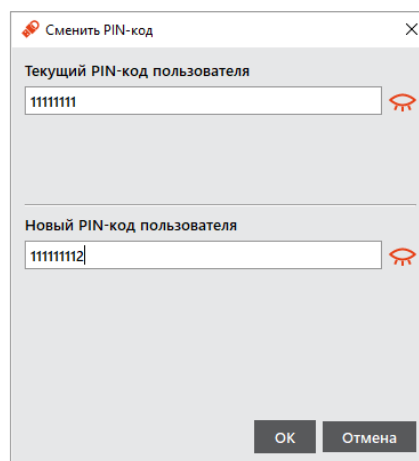


Рисунок 14 – Окно изменения PIN-кода пользователя. Отображение значений полей в явном виде

5. Нажать кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-кода пользователя будет изменен (см. Рисунок 15);

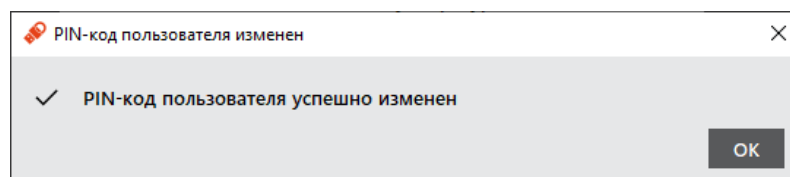


Рисунок 15 – Окно "PIN-кода пользователя изменен"

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

5.4 Разблокирование PIN-кода пользователя



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

5.4.1 Приложение PKI

- ▶ Для разблокирования PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";

2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. 16). Иначе кнопка заблокирована;



Рисунок 16 - Элемент управления "Разблокировать PIN-код"

4. Далее будет открыто окно "Разблокировать PIN-код" (см. Рисунок 17);
5. В поле "PIN-код администратора" ввести текущий PIN-код администратора;
6. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новый PIN-код пользователя и нажать кнопку "ОК";

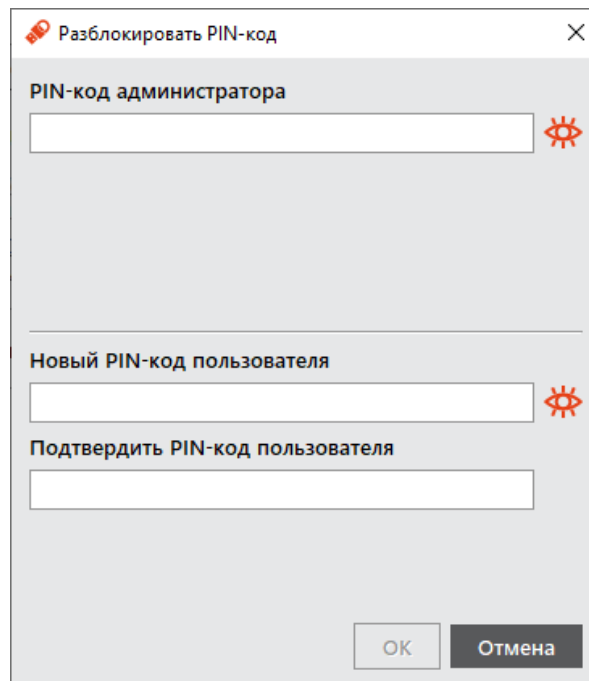


Рисунок 17 - Разблокировка PIN-кода пользователя

7. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение – нажать кнопку "ОК", чтобы закрыть его (см. Рисунок 18).

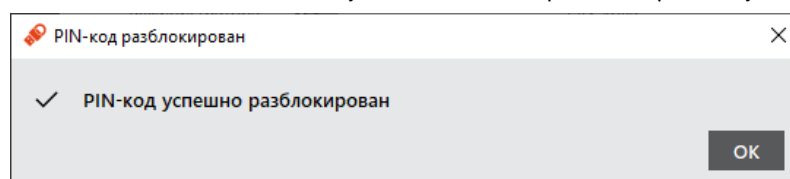


Рисунок 18 - Сообщение об успешной разблокировке PIN-кода пользователя

5.4.2 Приложение ГОСТ



Для того чтобы разблокировать PIN-код пользователя, электронный ключ должен быть проинициализирован PIN-кодом администратора.

► Для разблокирования PIN-кода пользователя необходимо:

1. Подключить электронный ключ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнения дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. Рисунок 19);

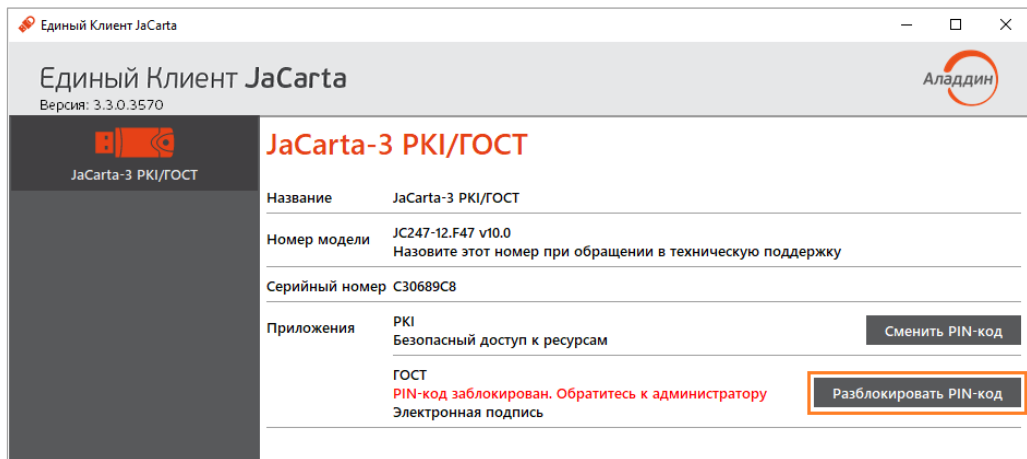


Рисунок 19 - Элемент управления "Разблокировать PIN-код"

4. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода" (см. Рисунок 20);

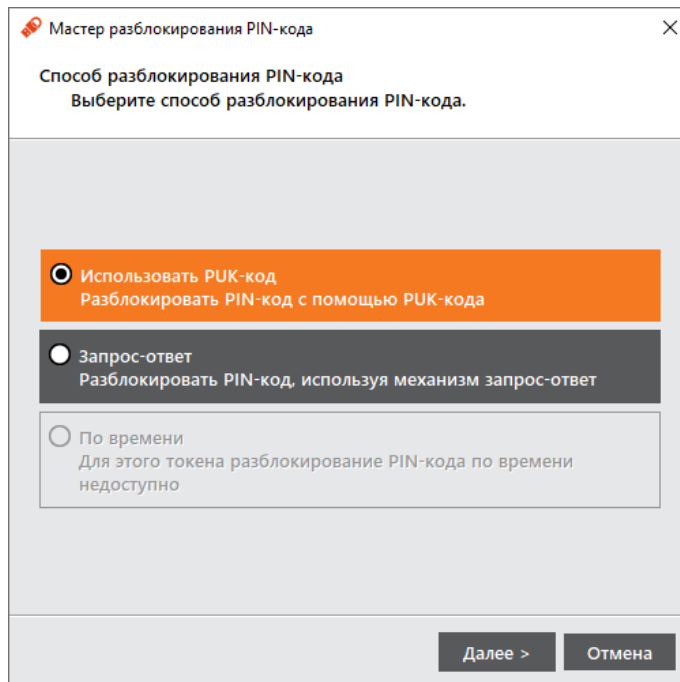


Рисунок 20 - Окно "Разблокировка PIN-кода пользователя"

5. Выбрать пункт "Использовать PUK-код" и нажать кнопку "Далее";

6. В поле "PUK-код" ввести текущий PUK-код³, после чего нажать кнопку "Далее";
7. При успешной разблокировке отобразится соответствующее сообщение. Для его закрытия нажать кнопку "Завершить" (см. Рисунок 21).

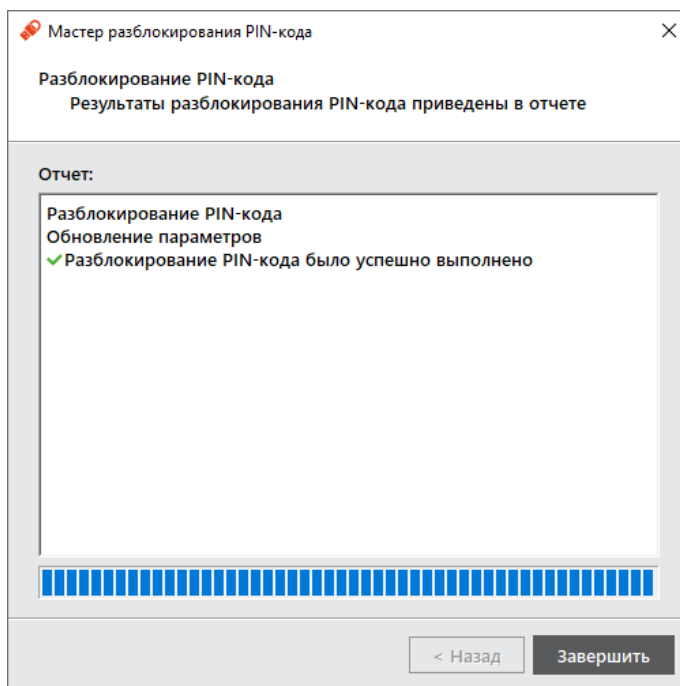


Рисунок 21 - Информационное сообщение об успешной разблокировке PIN-кода пользователя

5.5 Установка PIN-кода подписи



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



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

После установки PIN-кода подписи доступна операция изменения PIN-кода подписи (см. подраздел 5.6 "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. подраздел 5.7 "Разблокирование PIN-кода подписи").

► Для установки PIN-кода подписи необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Установить PIN-код подписи" для приложения ГОСТ (см. Рисунок 22);

³ Для приложения ГОСТ будет запрашиваться PIN-код администратора.





Рисунок 22 – Главное окно Единого Клиента JaCarta. Кнопка "Установить PIN-код подписи" активна

4. В окне "Установить PIN-код подписи" заполнить следующие поля (см. Рисунок 23):

- в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя приложения ГОСТ;
- в поле "Установить PIN-код подписи" ввести значение нового PIN-кода подписи;

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

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

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

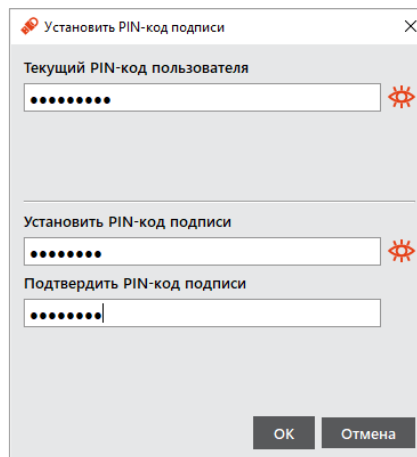


Рисунок 23 - Окно установки PIN-кода подписи. Значения PIN-кода введены верно

5. Нажать кнопку "ОК". В случае успешной аутентификации в приложении электронного ключа PIN-код подписи будет установлен. На экране появится сообщение об этом (см. Рисунок 24);

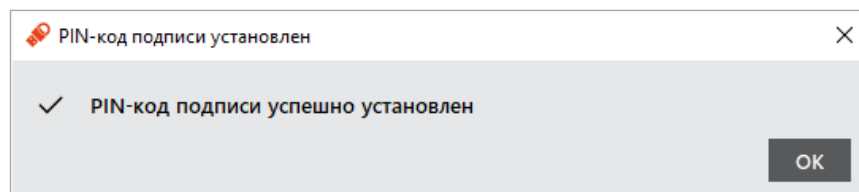


Рисунок 24 - Сообщение об успешной инициализации PIN-кода подписи

6. Нажать кнопку "ОК" в окне сообщения.

5.6 Изменение PIN-кода подписи



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

► Для изменения PIN-кода подписи необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разьему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Сменить PIN-код подписи" для приложения ГОСТ (см. Рисунок 25);

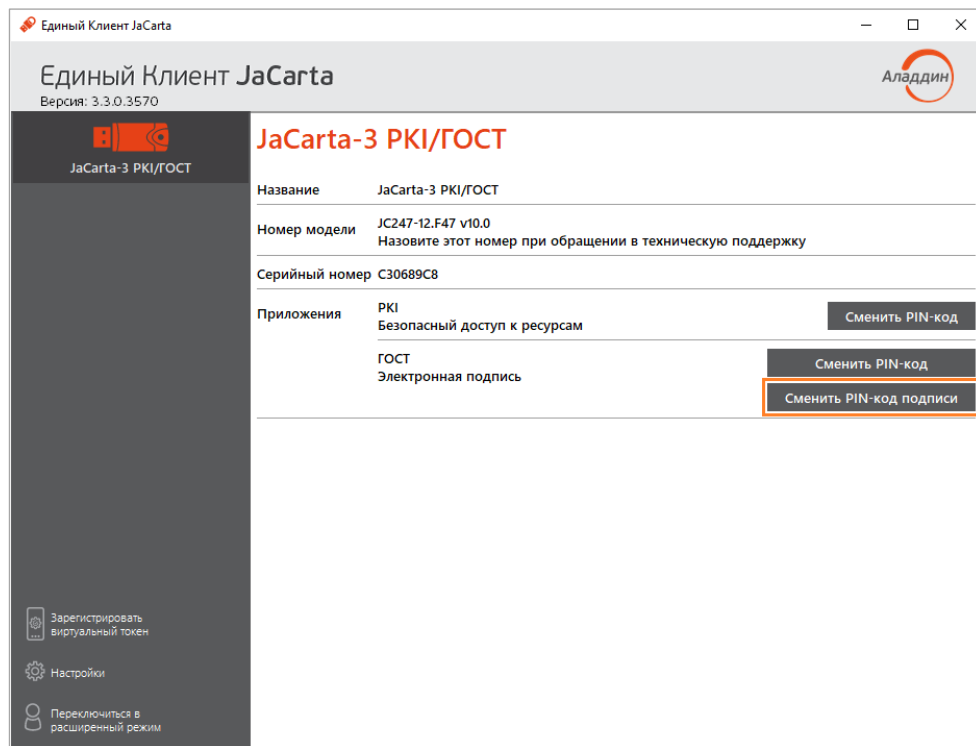




Рисунок 25 - Единый Клиент JaCarta. Главное окно

4. В окне "Сменить PIN-код подписи" заполнить следующие поля (см. Рисунок 26):
 - в поле "Текущий PIN-код пользователя" ввести PIN-код пользователя выбранного приложения (в данном примере приложения ГОСТ);
 - в поле "Текущий PIN-код подписи" ввести PIN-кода подписи;
 - в поле "Новый PIN-код подписи" ввести значение нового PIN-кода подписи. При этом новое значение PIN-кода подписи не должно совпадать с его текущим значением. Если значения совпадают, то будет отображено сообщение об этом и операция не будет продолжена до тех пор, пока не будет введено другое значение PIN-кода.

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

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

По умолчанию введенные значения PIN-кода показаны в скрытом виде. Чтобы показать их в явном виде нажать кнопку  (см. Рисунок 26). Для возвращения к отображению в скрытом виде нажать кнопку .

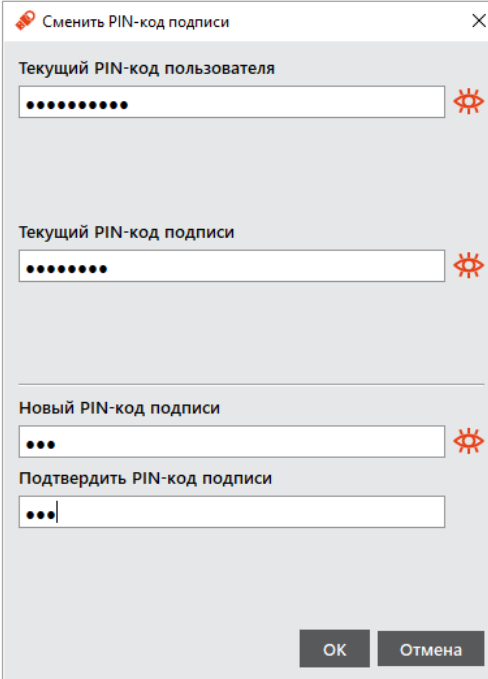


Рисунок 26 - Окно изменения PIN-кода подписи. Значения PIN-кода введены верно

5. Нажать кнопку "OK". В случае успешной аутентификации в приложении электронного ключа PIN-кода подписи будет установлен. На экране появится сообщение об этом (см. Рисунок 27);

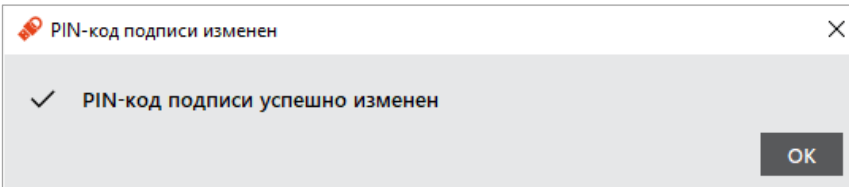


Рисунок 27 – Сообщение об успешном изменении PIN-кода подписи

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

5.7 Разблокирование PIN-кода подписи



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

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

Для выполнения операции разблокирования PIN-кода подписи требуется предъявление PUK-кода⁴ данного приложения электронного ключа. Информация об установке PUK-кода отображается в основном окне Единого Клиента JaCarta в расширенном режиме (см. раздел 6 "Работа в программе в расширенном режиме").

Если PUK-код не установлен, то необходимо обратиться к администратору для разблокирования PIN-кода подписи.

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

► Для разблокирования PIN-кода подписи необходимо:

1. Подключить электронный ключ с приложением ГОСТ к разъему USB компьютера и запустить ПО "Единый Клиент JaCarta";
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. В основном окне Единого клиента JaCarta в стандартном режиме нажать кнопку "Разблокировать PIN-код подписи" для приложения ГОСТ (см. Рисунок 28);

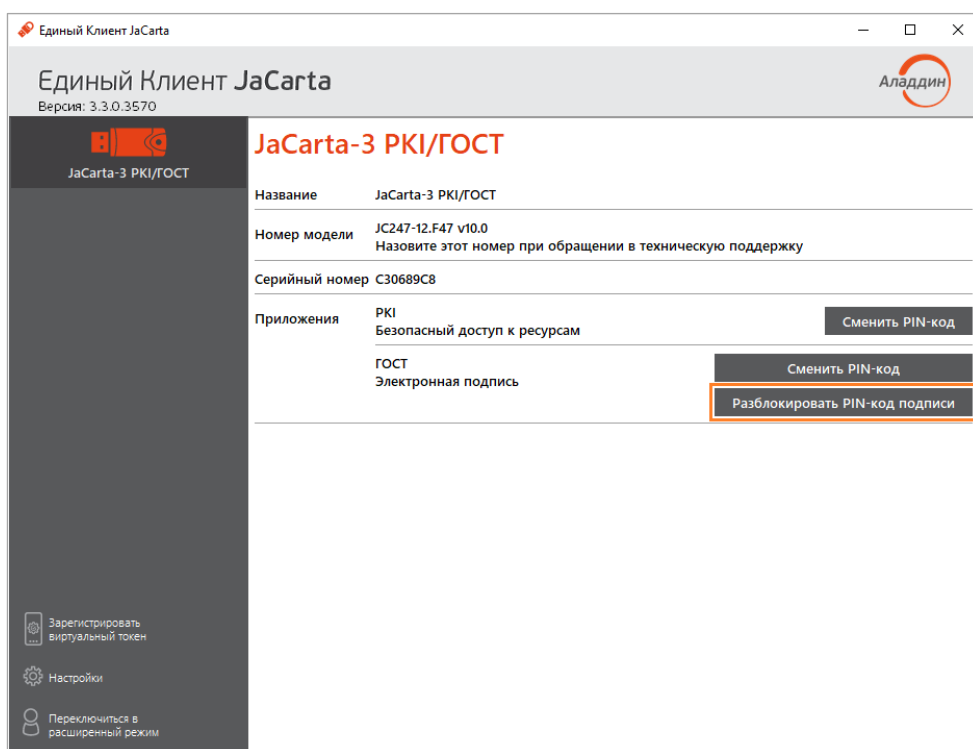


Рисунок 28 - PIN-код подписи заблокирован

⁴ Для приложения ГОСТ будет запрашиваться PIN-код администратора.

4. Будет отображено окно с выбором способа разблокирования PIN-кода (см. Рисунок 29);

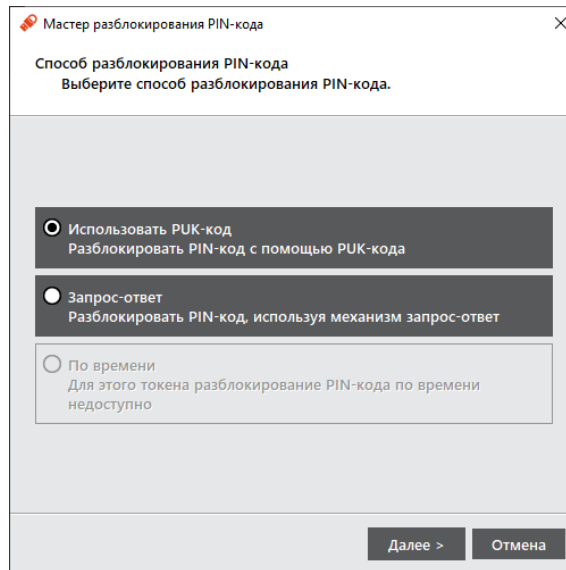


Рисунок 29 – Окно для ввода PUK-кода при разблокировании PIN-кода подписи

5. В окне выбора способа разблокирования PIN-кода необходимо выбрать желаемый способ разблокирования;
6. Если был выбран способ разблокирования PIN-кода с использованием PUK-кода, будет отображено окно для ввода PUK-кода⁵. В поле "PUK-код" необходимо ввести 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 необходимо обратиться к администратору безопасности.

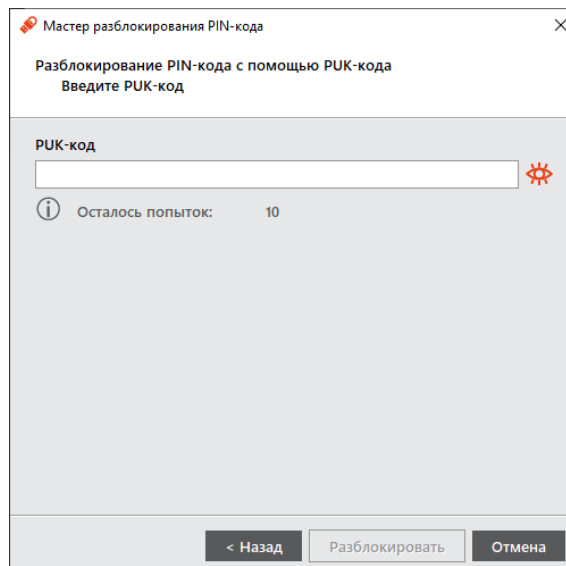


Рисунок 30 – Окно для ввода PUK-кода при разблокировании PIN-кода подписи

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

⁵ Для приложения ГОСТ будет запрашиваться PIN-код администратора.

Мастер разблокирования PIN-кода

Разблокирование PIN-кода с помощью механизма запрос-ответ
Передайте запрос вашему администратору безопасности и введите полученный ответ

Запрос

4E3900202465304D0000

Ответ

< Назад Далее > Отмена

Рисунок 31 – 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);
- 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 "KG JC EK. 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 необходимо:

1. Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Нажать кнопку "Переключиться в расширенный режим" и на вкладке "Информация о токене" будет отображена подробная информация о токене (см. Рисунок 32).

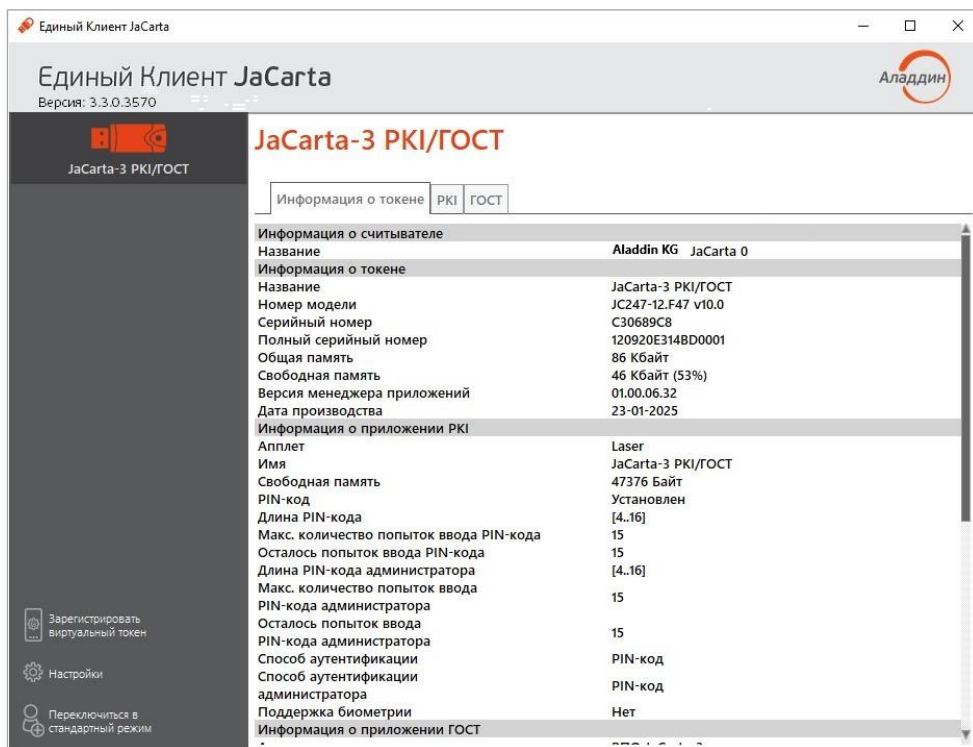


Рисунок 32 – Окно "Подробная информация о токене"

Вкладка "Информация о токене" содержит следующую 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;
 - "Версия менеджера приложений" – версия менеджера приложений 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>";
 - "Имя" – название электронного ключа;
 - "Свободная память" – объём свободной памяти электронного ключа;
 - "PIN-код" – статус PIN-кода пользователя приложения: установлен/не установлен;
 - "Длина PIN-кода пользователя" – количество символов PIN-кода пользователя приложения;
 - "Макс. количество попыток ввода 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);
 - "Макс. количество попыток ввода PIN-кода администратора" – максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора (только для приложений PKI);
 - "Осталось попыток ввода PIN-кода администратора" – количество неверных попыток ввода PIN-кода администратора до блокировки возможности использования PIN-кода администратора (только для приложений PKI);
 - "Способ аутентификации" – 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);
 - "Макс. попыток ввода PUK-код" – максимально допустимое количество неверных последовательных попыток ввода PUK-кода (только для приложения ГОСТ);
 - "Осталось попыток ввода PUK-кода" – количество оставшихся попыток ввода PUK-кода;
 - "Версия приложения" – номер версии установленного для приложения ГОСТ;
 - "Количество ключевых пар" – количество ключевых пар, хранящихся на токене на текущий момент (только для приложения ГОСТ);
 - "Количество секретных ключей" – количество секретных ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ);

- "Количество открытых ключей" – количество открытых ключей, хранящихся на токене на текущий момент (только для приложения ГОСТ);
- "Режим предъявления ключа администратора" – установленный режим предъявления ключа администратора (только для приложения ГОСТ);
- "Число разблокировок" – количество успешно выполненных разблокировок PIN-кода пользователя (только для приложения ГОСТ).

6.2 Диагностика целостности приложения



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

► Для диагностики приложения ГОСТ необходимо:

1. Подключить электронный ключ к разьему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти во вкладку "ГОСТ" для доступа к операциям приложения ГОСТ и нажать кнопку "Диагностика" (см. Рисунок 33);

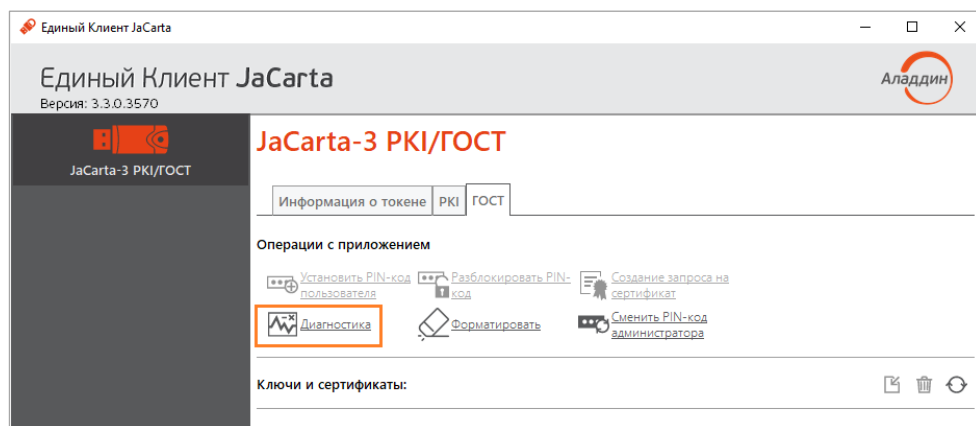


Рисунок 33 – Вкладка "ГОСТ" в основном окне Единого Клиента JaCarta. Кнопка "Диагностика..." активна

4. Подтвердить выполнение диагностики. Будет выполняться диагностика целостности приложения ГОСТ (см. Рисунок 34);

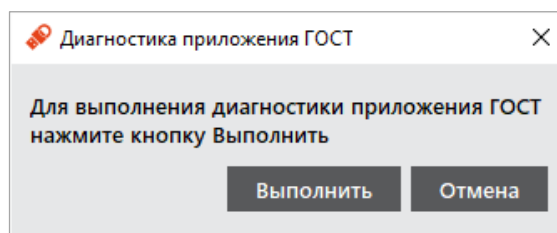


Рисунок 34 – Окно подтверждения диагностики

5. В случае успешного завершения операции будет отображена информация об этом. Нажать кнопку "ОК" для закрытия окна (см. Рисунок 34).

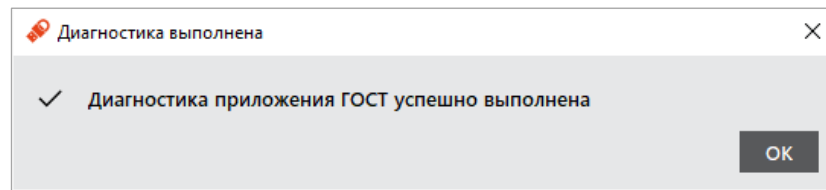


Рисунок 35 – Сообщение об успешном выполнении диагностики

6.3 Операции с сертификатами в приложении электронного ключа



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

6.3.1 Создание запроса на сертификат

► Для создания запроса на сертификат необходимо:

1. Подключить электронный ключ к разьему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Перейти на вкладку с наименованием приложения, для которого необходимо создать запрос на сертификат (в данном примере выбрано приложение PKI) и нажать кнопку "Создание запроса на сертификат". Кнопка активна при вводе PIN-кода пользователя (см. Рисунок 36);



Рисунок 36 – Кнопка "Создание запроса на сертификат"

4. В окне "Мастер создания запроса на сертификат" заполнить следующие поля (см. Рисунок 37):
 - в поле "Имя" ввести наименование создаваемого сертификата. Поле является обязательным для заполнения;
 - в раскрывающемся списке "Тип ключевой пары" выбрать алгоритм шифрования "RSA" (задан по умолчанию) либо "ЕС";

- в раскрывающемся списке "Размер ключа" выбрать размер открытого ключа. По умолчанию выбрано значение "1024".

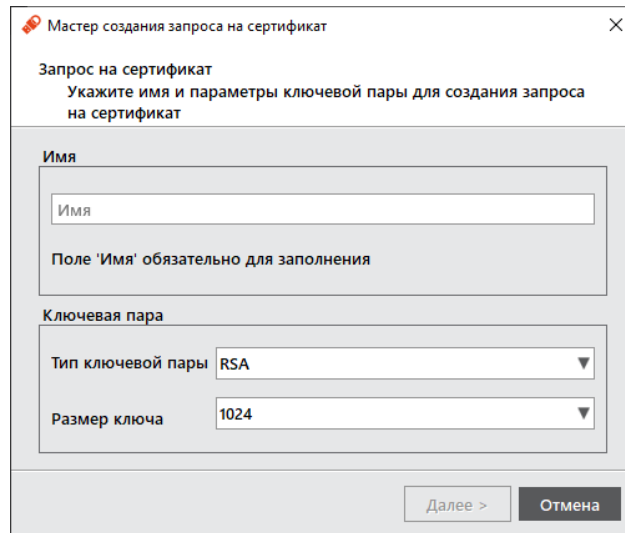


Рисунок 37 – Окно "Мастер создания запроса на сертификат"

5. Нажать 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. Выбрать нужную папку и при желании выбрать имя файла, в котором следует сохранить запрос на сертификат. Выбрать формат файла для запроса из предложенных (см. Рисунок 38);

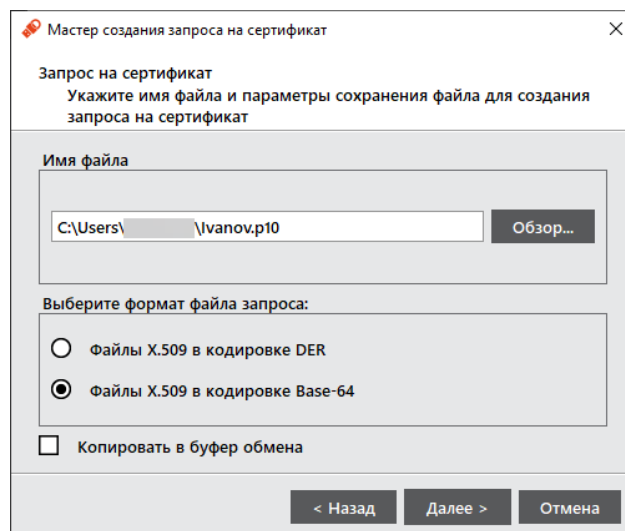


Рисунок 38 – Окно "Мастер создания запроса на сертификат"

6. Нажать кнопку "Далее". Будет открыто окно выбора опций при создании запроса на сертификат (см. Рисунок 39). Выбрать желаемые опции из списка:
 - в поле "Использование ключа" установить отметку в нужных полях:
 - "Электронная подпись" (выбрано по умолчанию);
 - "Неотказуемость" (выбрано по умолчанию);
 - "Шифрование ключей" (выбрано по умолчанию);
 - "Шифрование данных" (выбрано по умолчанию);
 - "Согласование ключей";
 - "Подписывание сертификата с помощью ключа";
 - "Подписывание списка отзыва сертификатов";

- "Только шифрование";
- "Только расшифрование";
- в поле "Предназначение" установить отметку в нужных полях:
 - "Проверка подлинности клиента" (выбрано по умолчанию);
 - "Защищённая электронная почта" (выбрано по умолчанию);
 - "Проверка подлинности сервера";
 - "Подпись кода";
 - "Доверенное время".

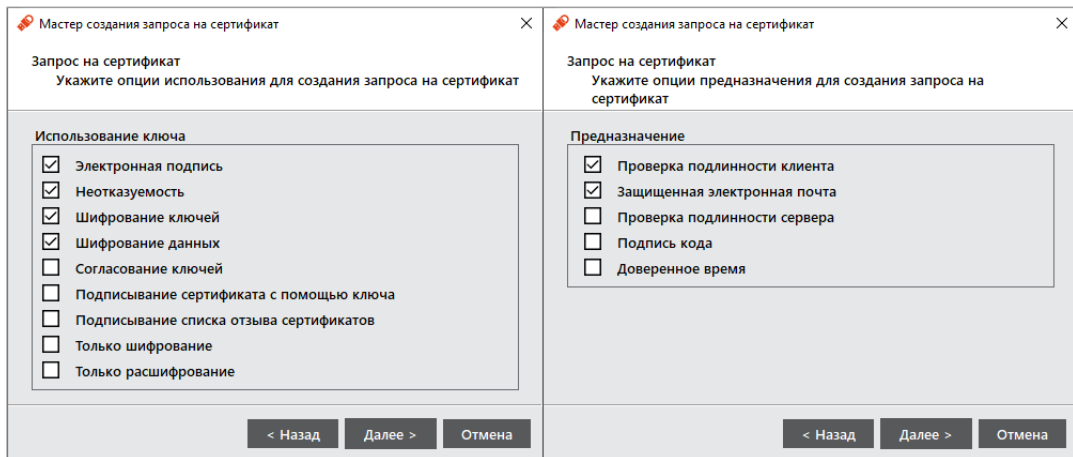


Рисунок 39 – Окна "Мастер создания запроса на сертификат", выбор опций при создании запроса на сертификат

7. Нажать кнопку "Далее". Будет открыто окно подтверждения выбранных параметров создания запроса на сертификат;
8. Если все заполнено верно, нажать 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 (см. Рисунок 40).

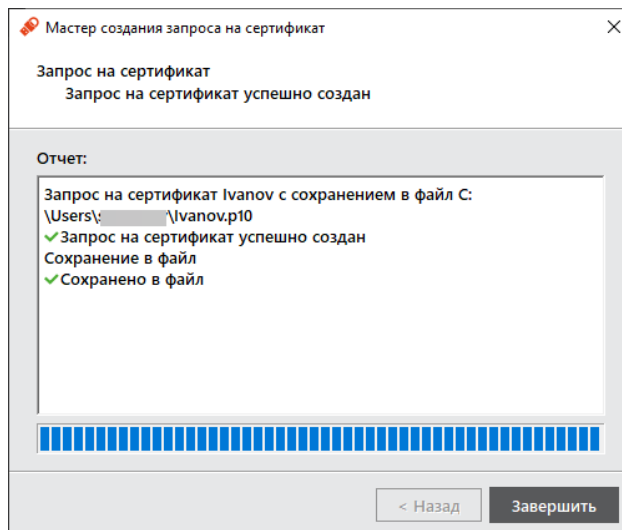


Рисунок 40 – Информация о завершении создания запроса на сертификат

9. Нажать 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 необходимо:

1. Подключить электронный ключ к разьему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
2. Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
3. Выбрать вкладку с наименованием приложения, в которое следует импортировать сертификат (в данном примере выбрано приложение PKI) и нажать кнопку "Ввести PIN-код" (см. Рисунок 41);

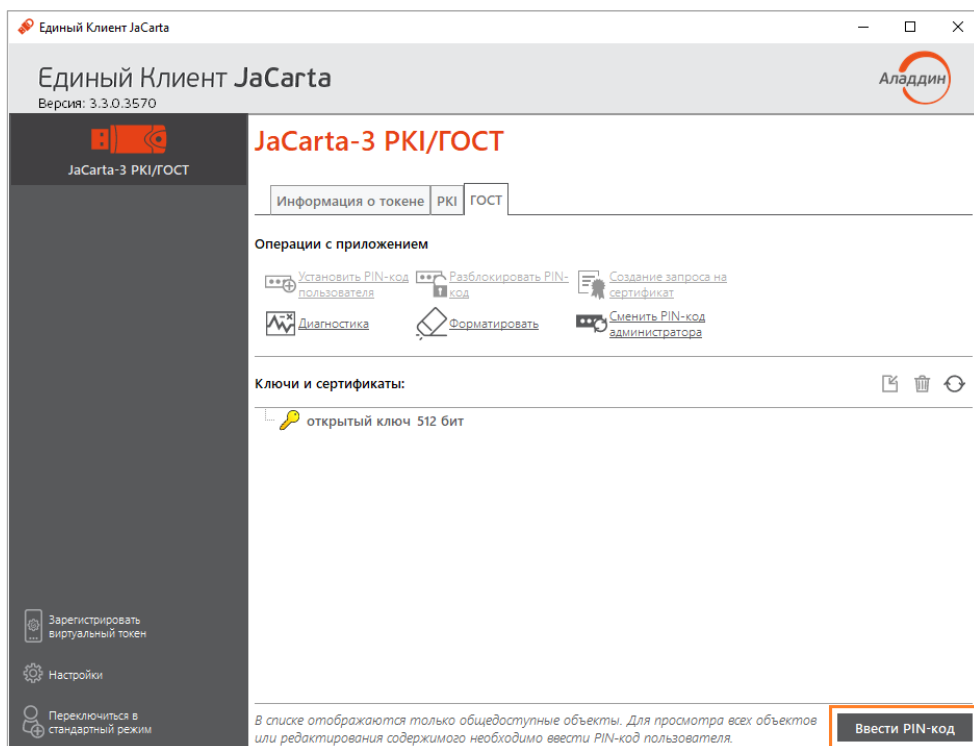


Рисунок 41 – Авторизация в приложении PKI

4. В появившемся окне с наименованием приложения ввести PIN-код пользователя данного приложения (см. Рисунок 42). Нажать кнопку "ОК";

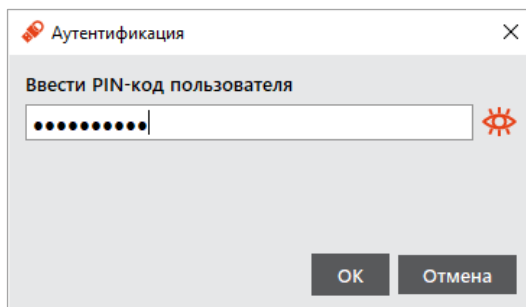


Рисунок 42 – Окно "Аутентификация"

5. В случае успешной авторизации в приложении в поле "Ключи и сертификаты" будет отображен полный список объектов данного приложения и станут доступны кнопки для выполнения операций над объектами (см. Рисунок 43);

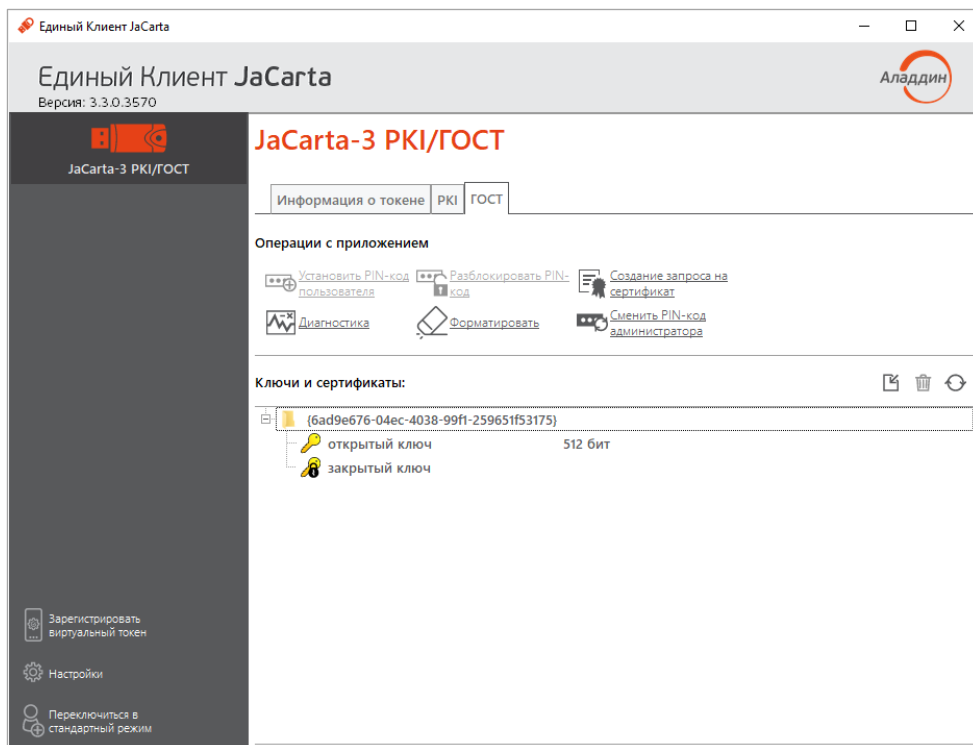



Рисунок 43 – Полный список объектов приложения и команда "Импорт"

6. Нажать кнопку  или вызвать контекстное меню в поле "Ключи и сертификаты" и выбрать команду "Импорт";
7. В окне "Мастер импорта сертификата" заполнить следующие поля (см. Рисунок 44):
 - в поле "Путь к файлу импортируемых данных" указать путь к импортируемому сертификату. Для этого нажать кнопку "Обзор..." и в появившемся окне Проводника Windows выбрать файл сертификата;
 - в поле "Имя контейнера" установить отметку, чтобы вручную задать имя контейнера, в который будет импортирован сертификат. В поле ниже ввести имя контейнера. Если отметка не установлена, то имя контейнера будет сгенерировано автоматически;

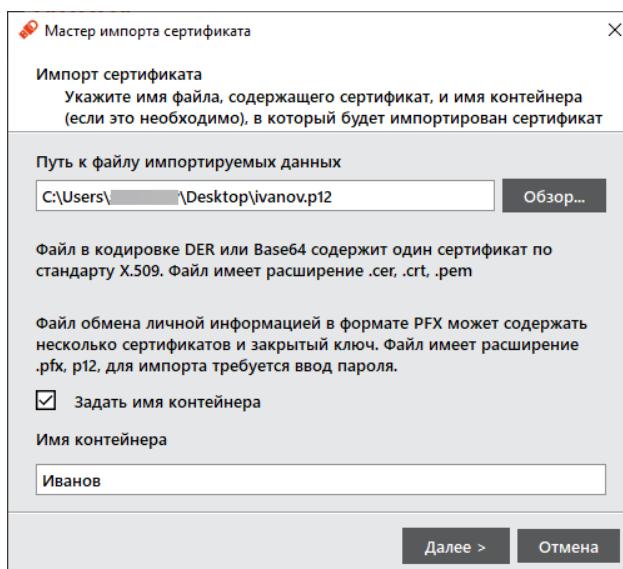


Рисунок 44 – Окно "Импорт сертификата или контейнера"

8. Нажать кнопку "Далее". Если импортируемый сертификат содержит защищённый паролем закрытый ключ, то ввести его в открывшемся окне;

9. При нажатии кнопки "Далее" Будет выполняться импорт сертификата в память приложения электронного ключа. По окончании операции на экране появится сообщение об этом (см. Рисунок 45);

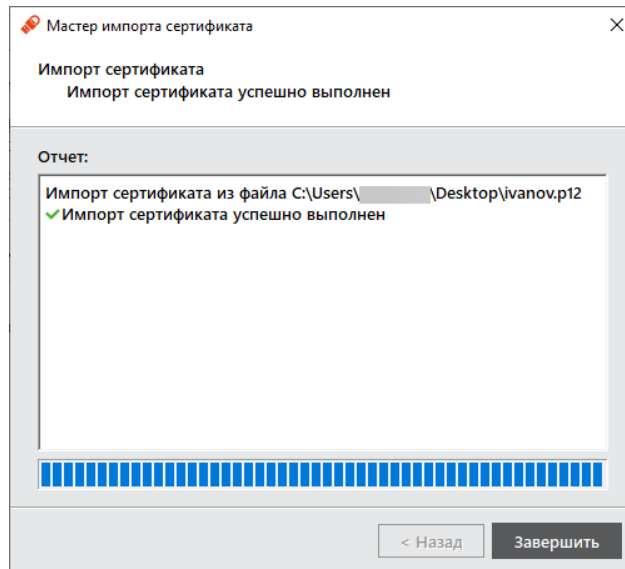


Рисунок 45 – Окно "Импорт сертификата или контейнера"

10. Нажать 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 (см.).

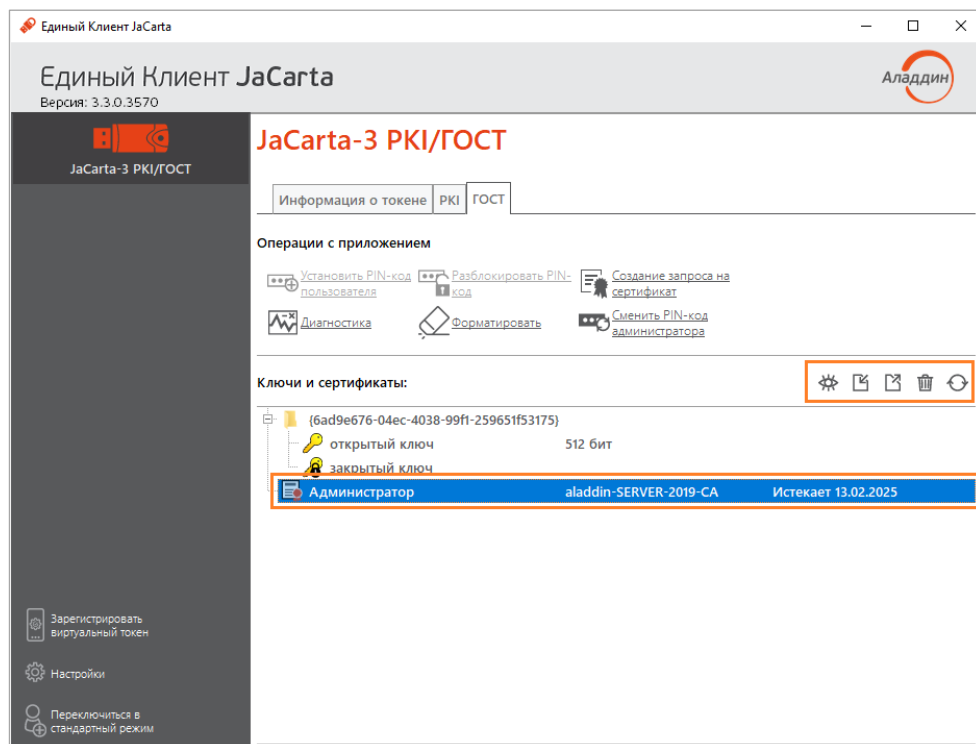



Рисунок 46 – Отображение импортированных объектов

6.3.3 Экспорт сертификата

► Для экспорта сертификата в файл необходимо:

1. Авторизоваться в приложении электронного ключа, из которого необходимо экспортировать сертификат (см. п.п. 1-3 процедуры импорта сертификата в п. 6.3.2). В поле "Ключи и сертификаты" выбрать экспортируемый объект и нажать кнопку  или активировать команду "Экспорт в файл" контекстного меню объекта (см. Рисунок 47);

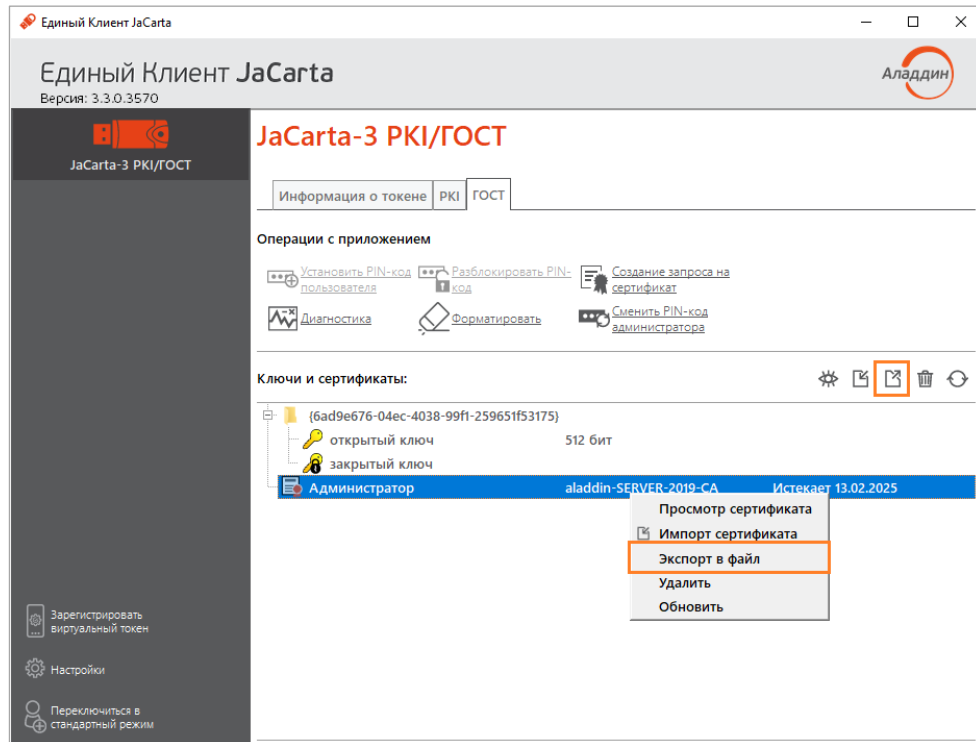


Рисунок 47 – Экспорт данных Единый Клиент JaCarta. Кнопки перехода к экспорту данных

2. В окне "Мастер экспорта сертификата" заполнить следующие поля (см. Рисунок 48):
 - в поле "Путь к файлу для экспорта" указать путь и имя файла для экспорта файла. Для этого нажать кнопку "Обзор..." и в появившемся окне Проводника Windows выбрать нужную папку. Выбрать необходимый тип файла для экспорта (по умолчанию выбран тип "Файл в формате Base64");

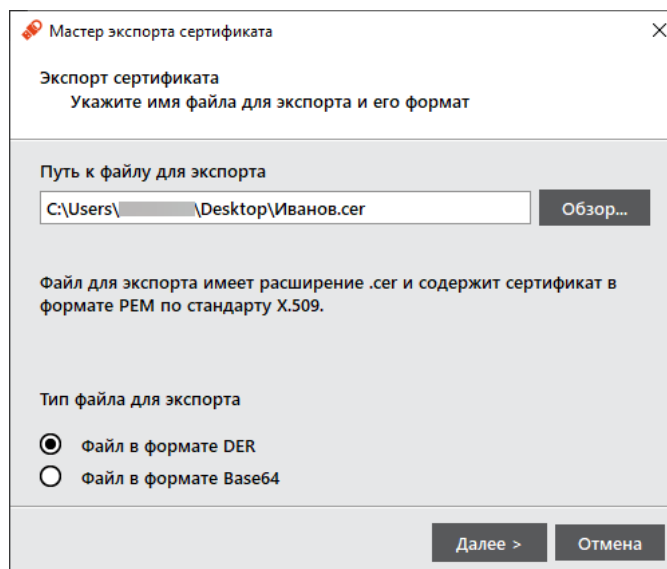


Рисунок 48 – Окно "Экспорт сертификата"

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

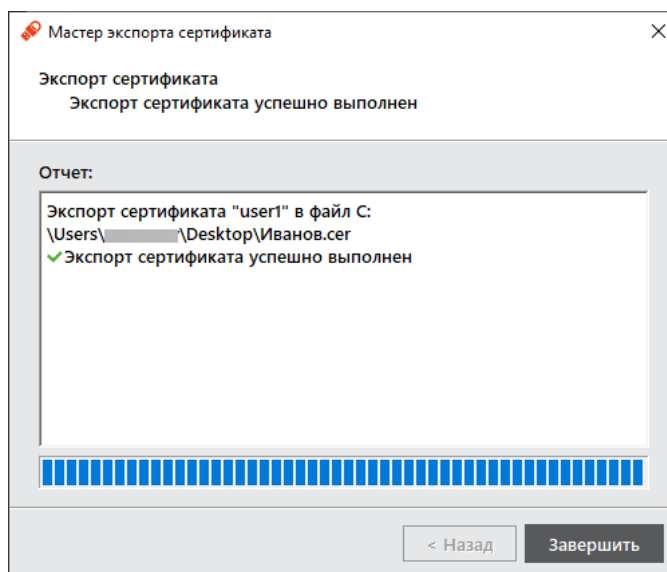



Рисунок 49 – Окно результатов экспорта

6.3.4 Просмотр сертификата

► Для просмотра сертификата необходимо:

1. Авторизоваться 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" выбрать сертификат и нажать кнопку  или активировать команду "Просмотр сертификата" в контекстном меню выбранного сертификата (см. Рисунок 50);

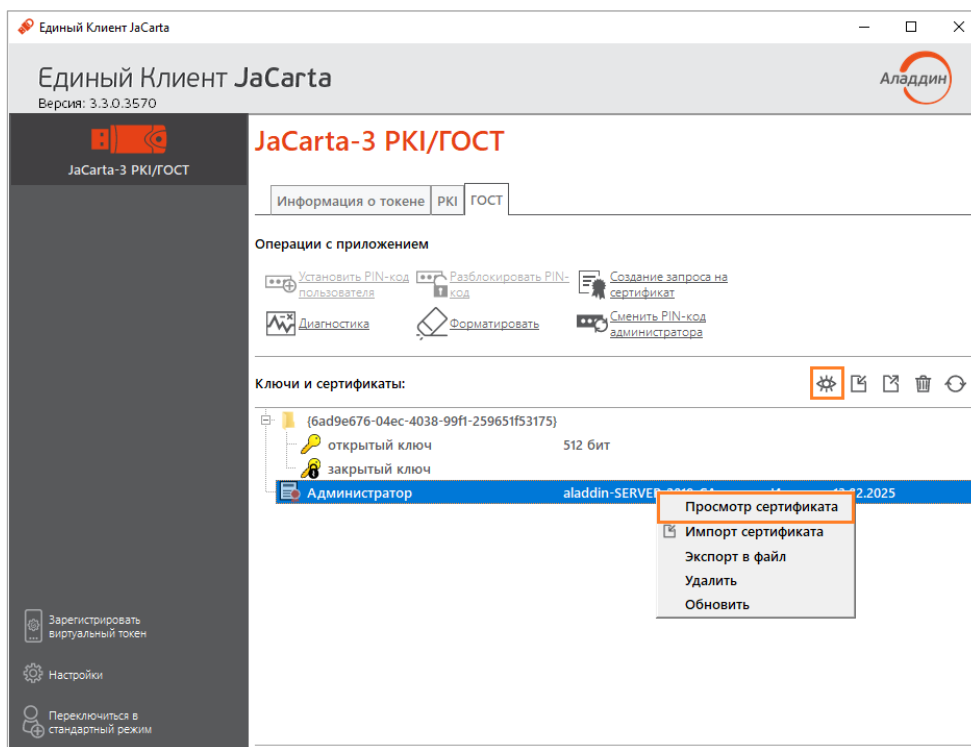


Рисунок 50 - Кнопки перехода к просмотру сертификата

- Будет открыто окно, содержащее сведения о выбранном сертификате (см. Рисунок 51);

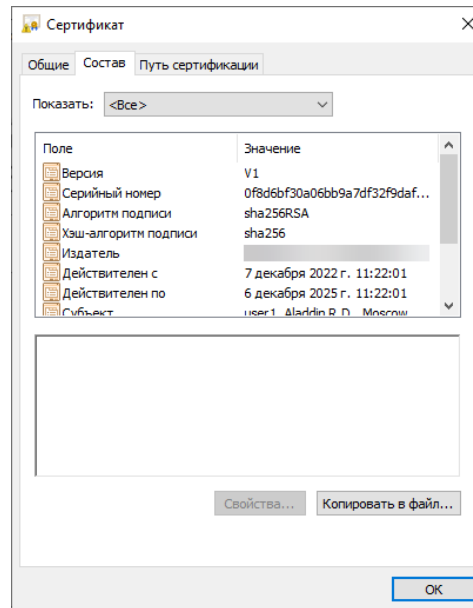


Рисунок 51 – Окно просмотра сертификата

- Для выхода из окна просмотра нажать кнопку "ОК".

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 необходимо:

- Подключить электронный ключ к разъему USB компьютера, запустить ПО "Единый Клиент JaCarta" и переключиться в расширенный режим;
- Информация об электронном ключе будет отображена в основном окне, выполнение дополнительных действий не требуется. Если подключено несколько электронных ключей, то выбрать значок нужного ключа в области слева;
- Выбрать вкладку с наименованием нужного приложения. В поле "Ключи и сертификаты" будет отображен список общедоступных объектов, хранящихся в памяти электронного ключа (см. Рисунок 52);

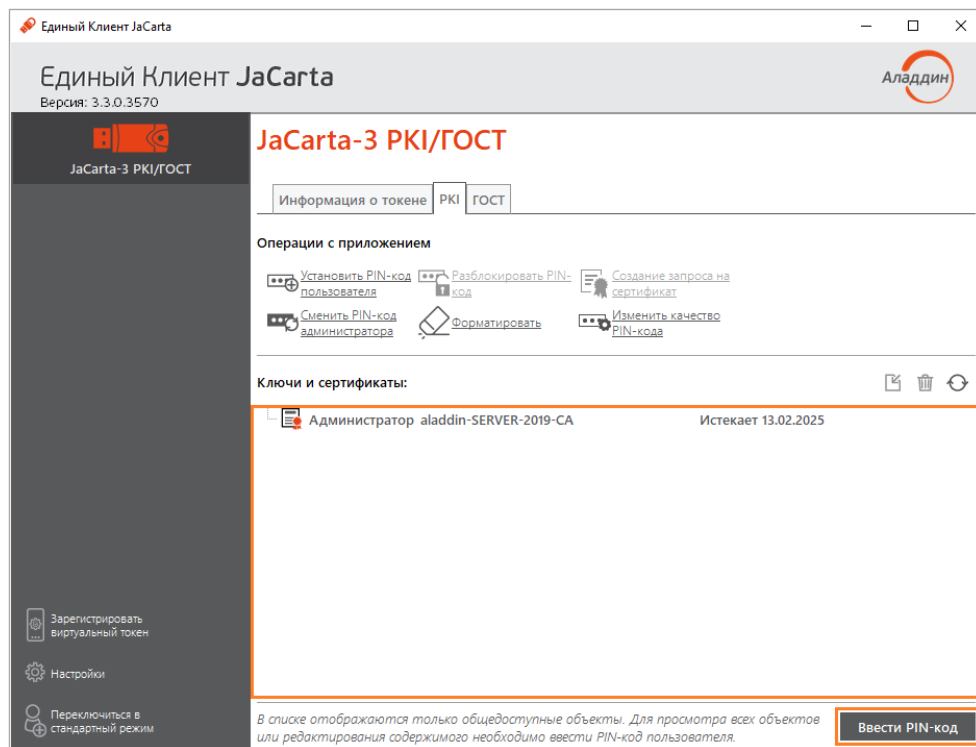


Рисунок 52 - Список общедоступных объектов в памяти электронного ключа

4. Нажать кнопку "Ввести PIN-код", в появившемся окне "Авторизация" ввести PIN-код пользователя для выбранного приложения (см. Рисунок 53);

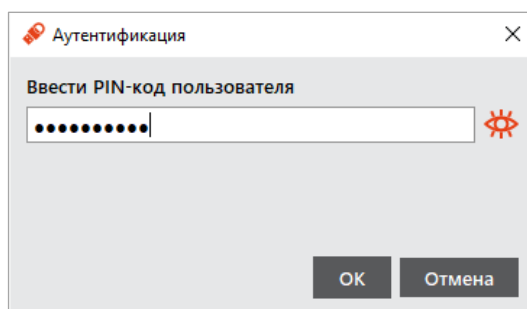


Рисунок 53 – Окно аутентификации в приложении электронного ключа

5. После успешной авторизации будет доступен для просмотра полный список объектов, а также появятся кнопки для управления объектами (см. Рисунок 54).

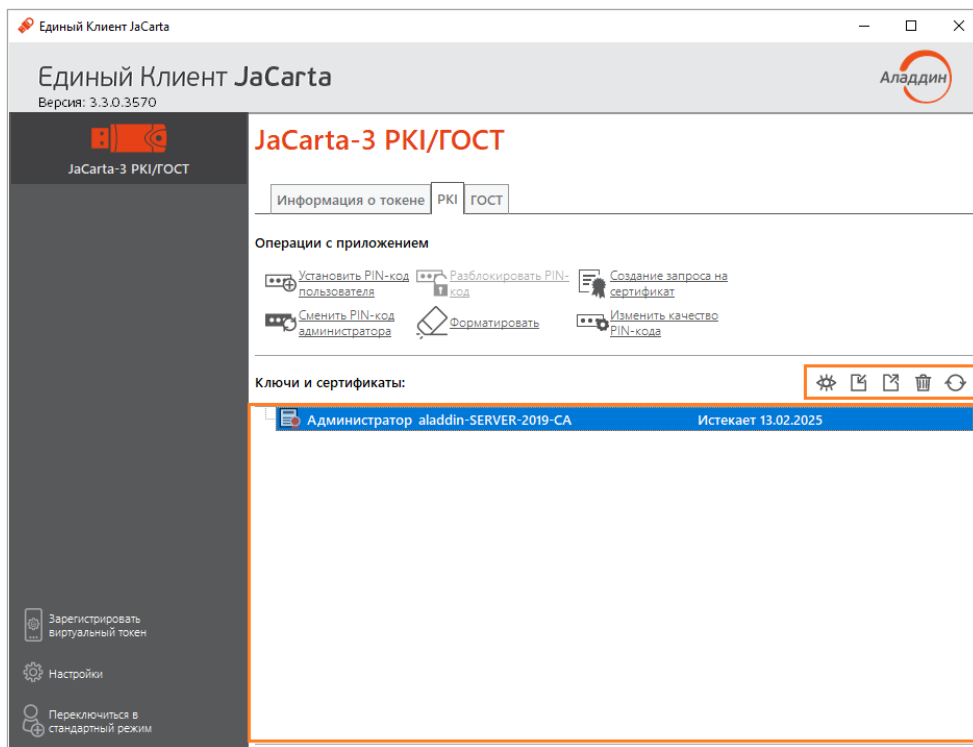



Рисунок 54 – Полный список объектов в памяти электронного ключа

6.4.2 Удаление объектов

► Для удаления объекта необходимо:

1. Авторизоваться в приложении электронного ключа, из которого необходимо удалить объект. В поле "Ключи и сертификаты" выбрать удаляемый объект и нажать кнопку  или активировать команду "Удалить" контекстного меню объекта (см. Рисунок 55);

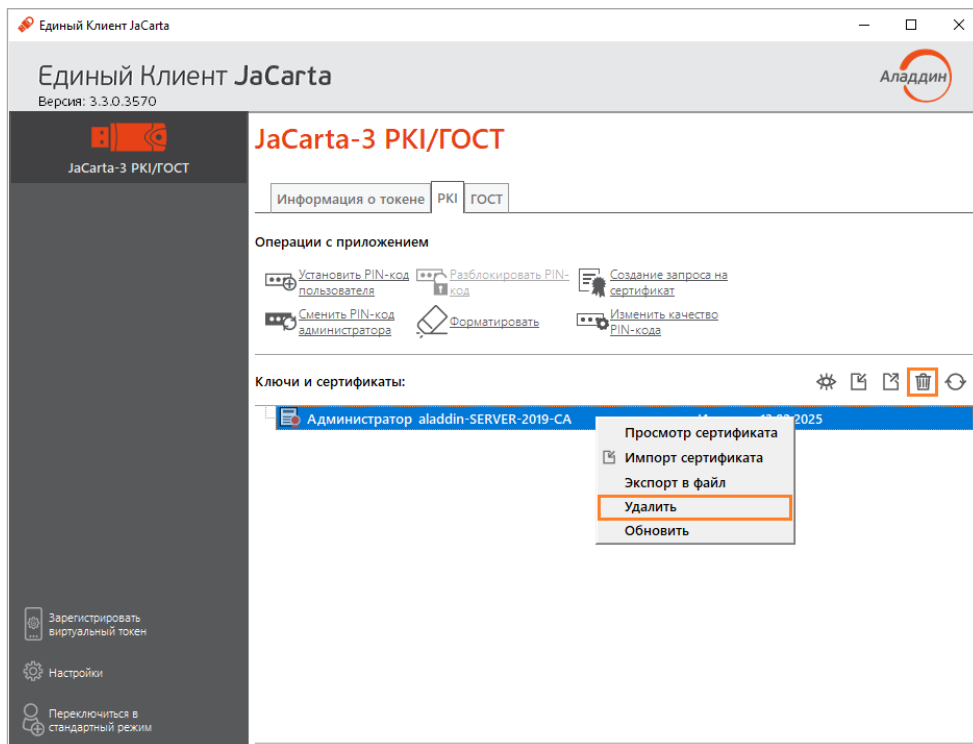


Рисунок 55 - Кнопки перехода к удалению данных

2. Будет открыто окно для подтверждения удаления (см. Рисунок 56);

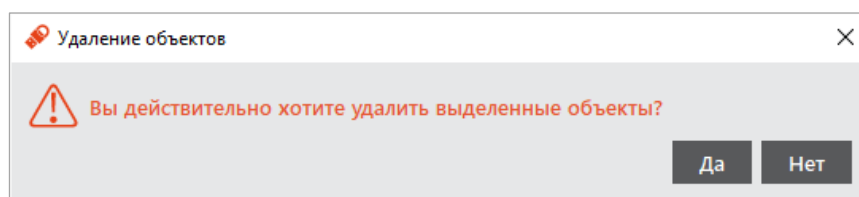



Рисунок 56 - Окно "Удаление объектов"

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

Приложение А. Обозначения электронных ключей

Обозначение	Описание
	USB-токен JaCarta в корпусе XL

Контакты

Адрес: 720005, Кыргызская Республика, г. Бишкек, Октябрьский район, ул. Байтик-Баатыра, д.19, кв.1-2-3

Телефон: +996 770 394 790

Web: <https://aladdin.kg>

ⁱ Также могут поддерживаться следующие модели электронных ключей: JaCarta PKI, JaCarta PKI/Flash, JaCarta-2 PKI/ГОСТ, JaCarta-2 PKI/ГОСТ/Flash, JaCarta-3 PKI, JaCarta-3 PKI/ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 ГОСТ, JaCarta-3 ГОСТ.