Единый Клиент JaCarta

Руководство администратора для Windows

Обозначение документа	АЛДЕ.467669.015РЭ3
Статус	Публичный
Листов	98

Оглавление

1. О документе

1.1 Назначение документа

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

1.2 На кого ориентирован данный документ

Документ предназначен для пользователей ПО "Единый Клиент JaCarta", владельцев электронных ключей JaCarta/eToken, владеющих PIN-кодом администратора электронного ключа, а также для администраторов безопасности.

1.3 Организация документа

Документ разбит на несколько разделов:

- в разделе 2 "Основные понятия" приведено назначение ПО "Единый Клиент JaCarta" и перечень терминов и сокращений, используемых в документе;
- в разделе 3 "Общие сведения об электронных ключах" содержится информация о приложениях, апплетах электронных ключей, для работы с которыми предназначено ПО "Единый Клиент JaCarta", а также параметры электронных ключей при поставке;
- в разделе 4 "Установка программы" содержится описание процедуры установки ПО "Единый Клиент JaCarta" с помощью мастера установки и в режиме командной строки;
- в разделе 5 "Изменение, исправление, удаление программы" содержится описание процедур изменения, удаления ПО "Единый Клиент JaCarta" с помощью мастера установки и в режиме командной строки;
- в разделе 6 "Настройка работы программы" подробно описаны настройки ПО "Единый Клиент JaCarta";
- в разделе 7 "Форматирование электронных ключей" описаны основные приемы форматирования различных моделей электронных ключей;
- в разделе 8 "Операции с PIN-кодом пользователя и PIN-кодом администратора" приведен порядок выполнения операций с PIN-кодом пользователя и PIN-кодом администратора для различных моделей электронных ключей;
- в разделе 9 описана установка, удаление и основные принципы работы с драйвером виртуального считывателя JaCarta Virtual Reader – компонентом ПО "Единый Клиент JaCarta";
- в разделе 10 содержится описание процедуры синхронизация паролей электронного ключа и учетной записи домена Windows;

1.4 Рекомендации по использованию документа

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

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

1.5 Соглашения по оформлению

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

Таблица 1 — Элементы оформления

Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ

Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
Гиперссылка	Используется для выделения внешних ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме
	Ссылка, примечание, заметка
	Совет
	Загрузка (адрес для загрузки ПО, документа)
	Вопрос

1.6 Авторские права, товарные знаки, ограничения

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

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

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

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

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

1.7 Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

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

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

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

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

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

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

Требования к использованию

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

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

Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;

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

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена. Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

2. Основные понятия

2.1 Назначение программы

ПО «Единый Клиент JaCarta» — программное обеспечение, предназначенное для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты. Версия для Microsoft Windows включает в себя компонент JaCarta SecurLogon.

Единый Клиент JaCarta может функционировать в обычном или гостевом режиме.

Гостевой режим предусматривает возможность просмотра информации о подключенном электронном ключе без ввода аутентификационных данных пользователя или администратора.

2.2 Термины и определения

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

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

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

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

Апплет – программное обеспечение, реализующее функциональность приложения электронного ключа.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

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

Форматирование – процедура установка основных параметров работы электронного ключа, выполняемая администратором.

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

3. Общие сведения об электронных ключах

3.1 Приложения, апплеты и модели электронных ключей

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

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

> ***Примечание.*** *Наименование приложения не всегда содержится в названии модели электронного ключа. Например, в модели ключей JaCarta PKI установлено приложение PKI, но в модели JaCarta LT установлено приложение STORAGE. Название модели и приложения электронного ключа отображается в интерфейсе ПО "Единый Клиент JaCarta" в стандартном режиме*

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

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

> ***Пример.*** *В моделях электронных ключей JaCarta PKI и JaCarta PRO установлено приложение PKI, но в модели JaCarta PKI данное приложение реализовано апплетом Laser, а в модели JaCarta PRO – апплетом PRO. Название апплета/приложения конкретного приложения отображается в интерфейсе ПО "Единый Клиент JaCarta" в расширенном режиме*

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

Таблица 2 – Соответствие приложений, апплетов и моделей электронных ключей

Апплет или приложение	**Модели электронных ключей**
Приложение PKI, реализованное апплетом Laser	JaCarta Remote Access; JaCarta PKI; JaCarta PKI/Flash; JaCarta PKI/BIO; JaCarta PKI/WebPass; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 SE; JaCarta SecurBIO; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SF; Aladdin LiveOffice; Aladdin LiveOffice Common Edition Виртуальный токен[1]
Приложение PKI, реализованное апплетом PRO	JaCarta PRO; eToken PRO Anywhere; eToken NG-OTP (Java); JaCarta-2 PRO/ГОСТ
Приложение STORAGE, реализованное апплетом Datastore	JaCarta LT; JaCarta WebPass; JaCarta U2F
Приложение ГОСТ, реализованное апплетом Криптотокен 2 ЭП	JaCarta Remote Access; JaCarta SF/ГОСТ; JaCarta-2 ГОСТ; JaCarta-2 PKI/ГОСТ; JaCarta-2 PKI/ГОСТ/Flash; JaCarta-2 PRO/ГОСТ; JaCarta-2 PKI/BIO/ГОСТ; JaCarta-2 SE; JaCarta SecurBIO; JaCarta-2 SF; Aladdin LiveOffice; Aladdin LiveOffice Common Edition
Приложение OTP, реализованное апплетом AladdinOTP	JaCarta WebPass; JaCarta U2F/WebPass; JaCarta PKI/WebPass

[1] Описание виртуального токена, процесс регистрации, работы с ним см. в документе «MFA JC EK. Руководство пользователя для Windows»

3.2 Параметры электронных ключей при поставке

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

Таблица 3 – Параметры электронных ключей при поставке

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

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

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

3.3 Операции с электронными ключами

Доступные операции с электронными ключами, с указанием нужного режима работы и необходимости аутентификации для совершения операции приведены в таблице 4.

Таблица 4 – Перечень операций с электронными ключами

Приложение и апплет / Операция в ЕК JaCarta ↓	Приложение PKI апплет PRO	Приложение PKI апплет Laser	Приложение ГОСТ апплет Криптотокен 2 ЭП	Приложение STORAGE апплет Datastore	Приложение OTP апплет AladdinOTP
Форматирование электронного ключа	PIN-код не требуется	Требуется PIN-код администратора	Требуется PIN-код пользователя	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода пользователя администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Не доступно	Функциональность отсутствует
Смена своего PIN-кода пользователем	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя
Смена своего PIN-кода администратором	Требуется PIN-код администратора	Требуется PIN-код администратора	Не доступно	Требуется PIN-код администратора	Функциональность отсутствует
Установка (смена) PIN-кода подписи пользователем	Не доступно	Не доступно	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует
Разблокирование PIN-кода пользователя в присутствии администратора	Требуется PIN-код администратора	Требуется PIN-код администратора	Требуется PUK-код	Требуется PIN-код администратора	Функциональность отсутствует
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	Не доступно	Функциональность отсутствует
Операции с объектами в памяти электронных ключей	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Функциональность отсутствует
Просмотр кратких сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется
Просмотр полных сведений о подсоединённом электронном ключе	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется	PIN-код не требуется
Создание запроса на сертификат	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Требуется PIN-код пользователя	Не доступно	Функциональность отсутствует

4. Установка программы

4.1 Системные требования

Системные требования к компьютеру, на котором устанавливается ПО "Единый Клиент JaCarta" приведены в таблице 5.

Таблица 5 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Microsoft Windows 7 (32/64-бит): Professional, Enterprise, Ultimate[4] Microsoft Windows 8.1 (32/64-бит): Core, Pro, Enterprise Microsoft Windows 10 (32/64-бит): Home, Professional, Enterprise Microsoft Windows 11 Microsoft Windows Server 2008 R2 SP1: Standard, Enterprise, Datacenter[3] Microsoft Windows Server 2012: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2012 R2: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022
Поддерживаемые модели электронных ключей	Электронные ключи eToken: • eToken PRO Anywhere; • eToken NG-OTP (Java) Электронные ключи JaCarta: • JaCarta Remote Access; • JaCarta LT; • JaCarta PKI; • JaCarta PKI/Flash; • JaCarta PKI/BIO; • JaCarta PKI/WebPass; • JaCarta WebPass; • JaCarta PRO; • JaCarta SF; • JaCarta SF/ГОСТ; • JaCarta FlashDiode; • JaCarta NFC; • JaCarta-2 ГОСТ; • JaCarta-2 ГОСТ NFC; • JaCarta-2 PKI/ГОСТ; • JaCarta-2 PKI/ГОСТ/Flash; • JaCarta-2 PRO/ГОСТ; • JaCarta-2 PKI/BIO/ГОСТ; • JaCarta-2 SE; • JaCarta-2 SF; • JaCarta-3; • JaCarta-3 PKI; • JaCarta-3 PKI/ГОСТ/Flash; • Aladdin LiveOffice;

[4] В связи с прекращением поддержки и выпуска обновлений разработчиком данных операционных систем рекомендуется применять дополнительные меры защиты, перечисленные в информационном сообщении ФСТЭК от 20 января 2020 г. N 240/24/250

Требование	Содержание
	• Aladdin LiveOffice Common Edition
Аппаратные средства	Для USB-токенов используется USB-порт. Для смарт-карт необходимо наличие подключённого считывателя смарт-карт, например, смарт-карт ридера JCR721. Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование: • USB-порт через переходник microUSB-to-USB. Для Type-C токенов используется USB Type-C порт
Разрешение экрана	Рекомендуется не ниже 1024x768

4.2 Описание пакетов установки

Описание пакетов установки ПО "Единый Клиент JaCarta" приведено в таблице *6*.

Таблица 6 –Пакеты установки ПО "Единый Клиент JaCarta"

Файл	Описание
JaCartaUnifiedClient_3.x.xxx.xxxx_win-x64_ru-Ru.msi	Пакет установки для 64-х разрядных операционных систем Microsoft Windows
JaCartaUnifiedClient_3.x.xxx.xxxx_win-x86_ru-Ru.msi	Пакет установки для 32-х разрядных операционных систем Microsoft Windows

При приемке дистрибутива необходимо выполнять контроль (периодический контроль) основных характеристик, таких как контрольная сумма (КС) эталонного дистрибутива и КС неизменяемых файлов.

Контрольные суммы исполняемых файлов установленного приведены в документе «Средство многофакторной аутентификации JaCarta-3. Формуляр. Часть 1».

Контрольные суммы исполняемых файлов установленного приведены в документе «Средство многофакторной аутентификации JaCarta-3. Формуляр. Часть 2. Свидетельства об упаковывании, приемке и маркировке».

4.3 Обязательные меры предосторожности

Перед установкой ПО «Единый Клиент JaCarta» необходимо ознакомиться со всеми представленными ниже мерами предосторожности

1. ПО "Единый Клиент JaCarta" уже содержит модуль JC-Client, поэтому *не рекомендуется* устанавливать JC-Client на компьютер с установленным ПО "Единый Клиент JaCarta". Отдельная дополнительная установка JC-Client может нарушить настройки ПО "Единый Клиент JaCarta" и вызвать ошибки при последующих установках и удалениях этих приложений.
2. Особенности установки и работы совместно с ПО "JaCarta Management System":
   – ПО "Единый Клиент JaCarta" версии 3.0 совместимо с ПО "JaCarta Management System" версии 3.7 и выше.
   – ПО "Единый Клиент JaCarta" версии 2.13 совместимо с ПО "JaCarta Management System" версии 3.4 и выше.
   – ПО "Единый Клиент JaCarta" версии 2.11 совместимо с ПО "JaCarta Management System" версии 3.1.
3. Для установки минидрайвера PRO из состава ПО "Единый Клиент JaCarta" необходимо убедиться, что на компьютере не установлено программное обеспечение ПО "SafeNet Authentication Client", ПО "eToken PKI Client" или ПО "SafeNet Minidriver". Если такое ПО установлено, его необходимо удалить до начала установки минидрайвера PRO.
4. Для работы со смарт-карт ридерами ASEDrive IIIe Bio необходимо установить компонент поддержки биометрии и модуль поддержки смарт-карт ридеров ASEDrive IIIe Bio.
5. Во время установки ПО "Единый Клиент JaCarta" версии 2.13 и более поздних версий на Windows 7 и Windows Server 2008 R2 с помощью мастера установки и в режиме командной строки в Windows будут

отображаться сообщения об установке драйверов, требующие подтверждения для продолжения установки. Устранить вывод подобных сообщений позволяет предварительная установка двух обновлений Windows: KB3033929 (доступно для загрузки на сайте Microsoft) и KB2921916. В связи с окончанием поддержки Windows 7 компанией Microsoft рекомендуется уточнить способ получения обновления KB2921916 у технической поддержки АО "Аладдин Р.Д." (см. п. 12.2 Техподдержка).

6. При установке ПО "Единый Клиент JaCarta" версии 2.13 и более поздних версий на Windows 7 и Windows Server 2008 R2 через групповые политики предварительная установка обновлений Windows KB3033929 (доступно для загрузки на сайте Microsoft) и KB2921916 является обязательной. Способ получения обновления KB2921916 рекомендуется уточнить у технической поддержки АО "Аладдин Р.Д." (см. п. 12.2 Техподдержка).
7. Установку модулей поддержки стоит осуществлять только при наличии проблем функционирования программного обеспечения, для которого устанавливается модуль поддержки. Подобные проблемы могут быть связаны с прекращением поддержки и выпуска обновлений ПО сторонних производителей, в таком случае модуль поддержки обеспечит возможность работы со сторонним ПО, увеличит скорость работы стороннего ПО с некоторыми моделями токенов JaCarta и обеспечит оптимизацию взаимодействия.
8. Извлечение токена или смарт-карты при записи или считывании информации может привести к выходу устройства из строя. Для обеспечения корректного функционирования токенов и смарт-карт, перед извлечением устройства необходимо дождаться завершения процесса записи или считывания информации.

4.4 Установка программы с помощью мастера установки

Перед установкой ПО «Единый Клиент JaCarta» необходимо ознакомиться с содержанием пункта 4.3 "Обязательные меры предосторожности"

Для установки ПО "Единый Клиент JaCarta" с помощью мастера установки:

1. Войдите в систему под учетной записью с правами администратора и запустите пакет установки ПО "Единый Клиент JaCarta" (имена пакетов установки ПО "Единый Клиент JaCarta" приведены в п. 4.2 "Описание пакетов установки"). Будет отображено стартовое окно установки программы:

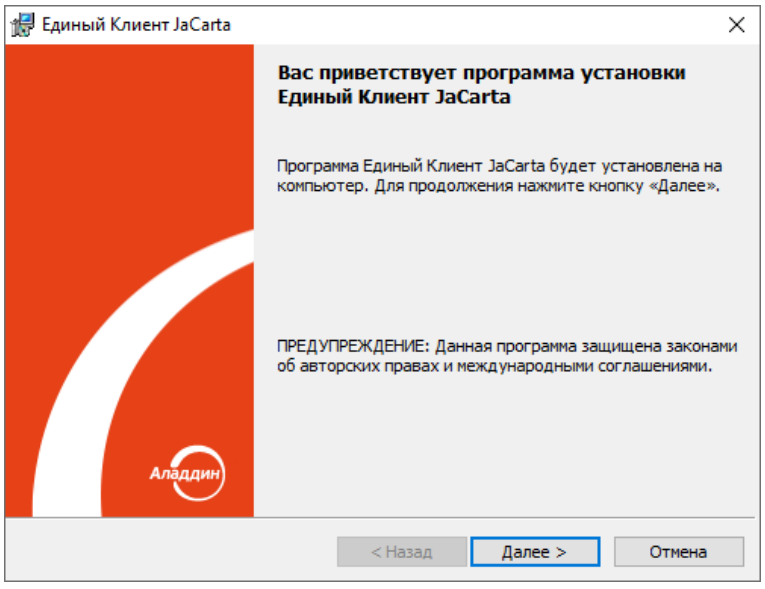


Рисунок 1 - Окно приветствия мастера установки ПО "Единый Клиент JaCarta"

2. Нажмите кнопку "Далее". Будет отображено окно с "Лицензионное соглашение" (Рисунок 2). Ознакомьтесь с текстом лицензионного соглашения.

   2.1. Если вы не согласны с условиями Лицензионного соглашения, выберите пункт "Я не принимаю условия Лицензионного соглашения" и нажмите кнопку "Отмена". Установка ПО "Единый Клиент JaCarta" будет прекращена.

2.2. Если вы согласны с условиями Лицензионного соглашения, выберите пункт "Я принимаю условия Лицензионного соглашения".

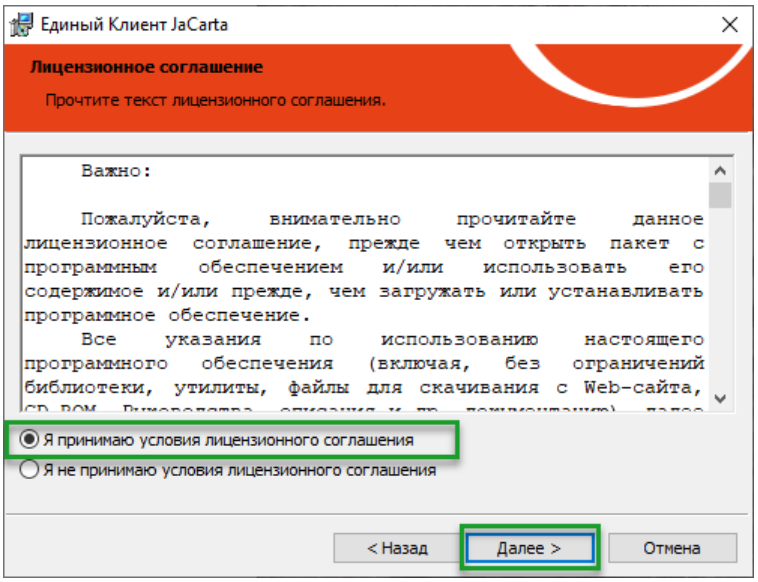


Рисунок 2 - Окно "Лицензионное соглашение" мастера установки ПО "Единый Клиент JaCarta"

3. Нажмите кнопку "Далее". Будет открыто окно "Вид установки" (Рисунок 3). Выберите вид установки программы и при необходимости измените путь ее установки:

   – выберите значение "Стандартная" (по умолчанию) для установки стандартного набора компонентов: Единый Клиент JaCarta, Минидрайвер PRO, Управление токеном, Поддержка биометрии. В случае выбора стандартной установки перейдите к выполнению шага 5 данной процедуры.

   – выберите значение "Выборочная" для выбора из указанного набора компонентов.

Примечание. Компонент "Единый Клиент JaCarta" является обязательным и устанавливается всегда, независимо от выбранного типа установки.

   – при необходимости измените указанный по умолчанию путь установки программы. Для этого нажмите кнопку "Изменить..." и в открывшемся окне Проводника Windows выберите нужную папку.

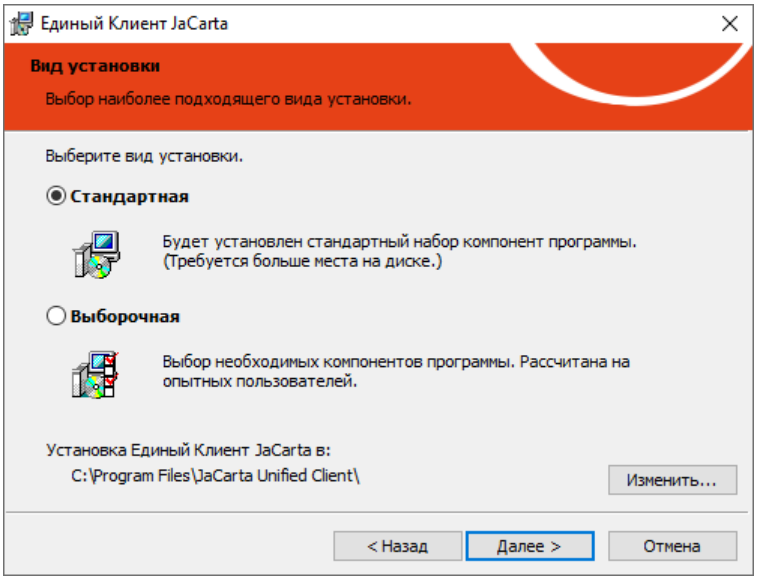


Рисунок 3 - Окно "Вид установки" мастера установки ПО "Единый Клиент JaCarta"

4. Нажмите кнопку "Далее". В случае выборочной установки будет отображено окно для выбора из следующего набора компонент:

   - Минидрайвер PRO;
   - JaCarta SecurLogon;

- Управление токеном;
- Поддержка биометрии;
- Драйвер JaCarta Virtual Reader.

Примечание. Подробнее о работе JaCarta Virtual Reader см. п. 9 "Драйвер виртуального считывателя JaCarta".

Примечание. Описание компонентов приведено в приложении А.

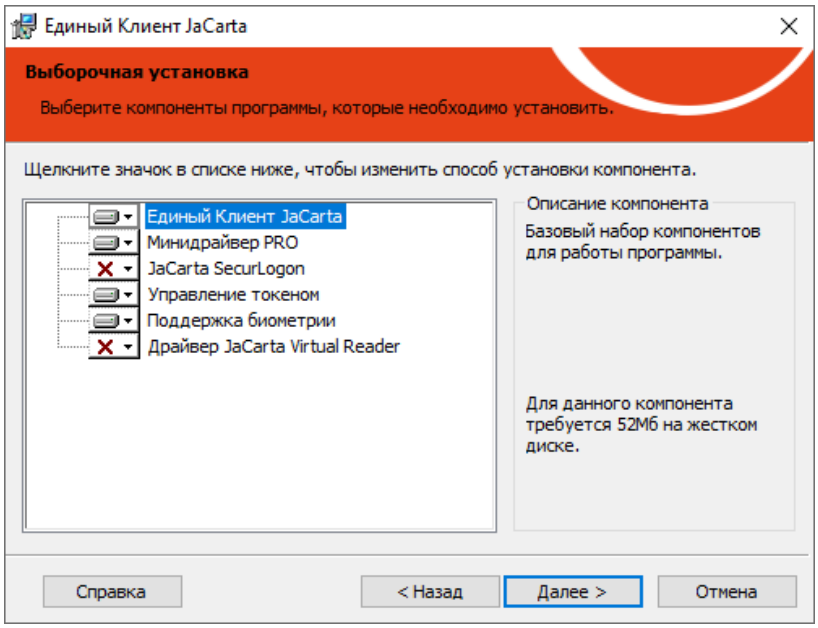


Рисунок 4 - Окно "Выборочная установка" мастера установки ПО "Единый Клиент JaCarta"

Для установки требуемого компонента в окне "Выборочная установка" в строке с названием нужного компонента нажмите значок ▼ и в выпадающем списке выберите необходимую опцию установки (см. рисунок 5):

- "Данный компонент будет установлен на локальный жесткий диск";
- "Данный компонент и все подкомпоненты будут установлены на локальный жесткий диск"
- "Данный компонент будет недоступен".

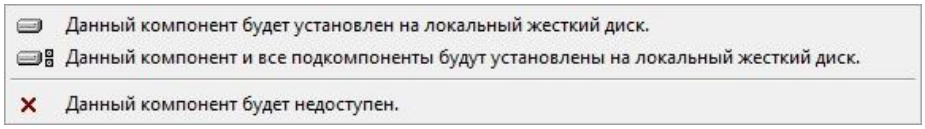


Рисунок 5 – Опции установки компонента

При нажатии на кнопку "Справка" будет открыто окно "Советы по выборочной установке", содержащее подробное описание состояний установки компонентов:

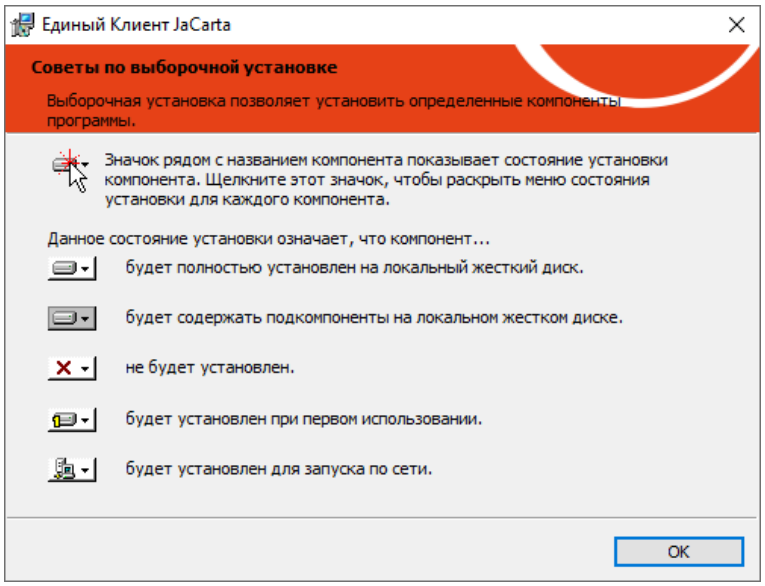


Рисунок 6 - Окно "Советы по выборочной установке" мастера установки ПО "Единый Клиент JaCarta"

5. Если на шаге 3 был выбран вид установки "Выборочная", то будет отображено окно "Дополнительные параметры работы" (см. Рисунок 7). С помощью одноименной галочки можно добавить Единый Клиент JaCarta в автозагрузку при старте операционной системы;

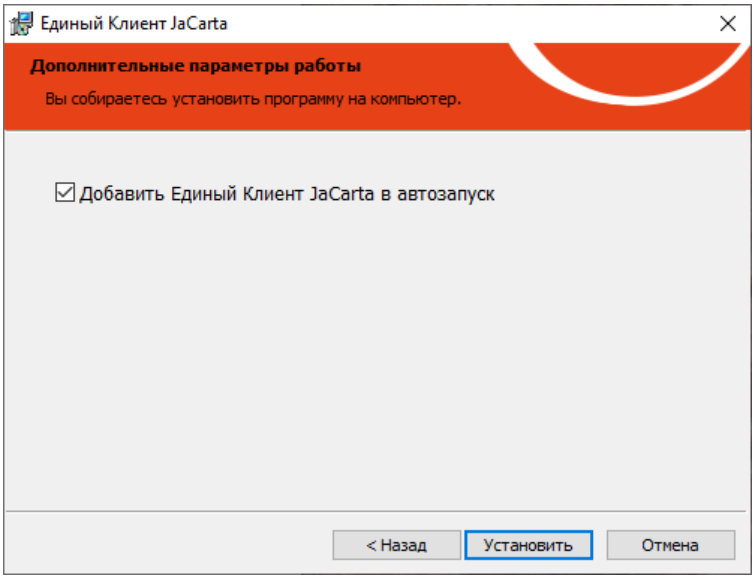


Рисунок 7 - Окно "Дополнительные параметры работы" мастера установки ПО "Единый Клиент JaCarta"

> *Если была выбрана установка "Стандартная", то Единый Клиент JaCarta будет автоматически добавлен в автозагрузку*

6. Нажмите кнопку "Установить". Будет выполняться установка выбранных компонентов ПО "Единый Клиент JaCarta". Ход установки отображается в виде индикатора:

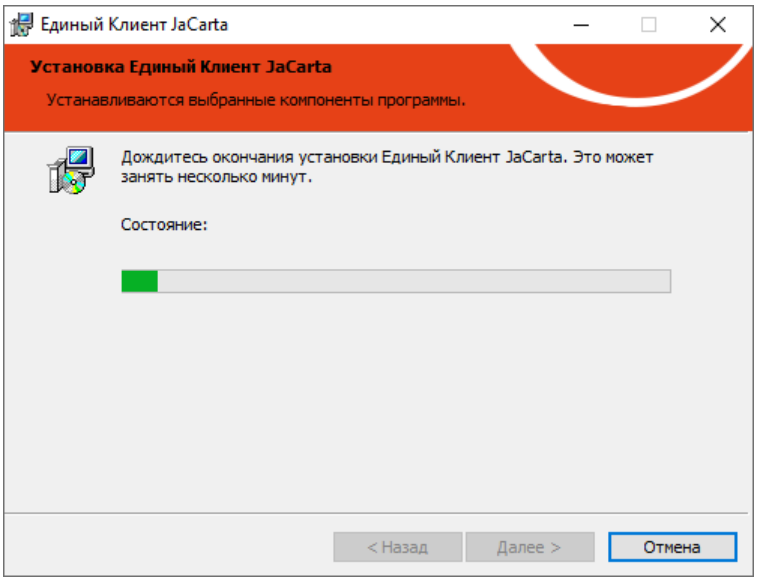


Рисунок 8 - Процесс установки ПО "Единый Клиент JaCarta"

7. После завершения установки отобразится следующее окно с информацией о завершении установки:

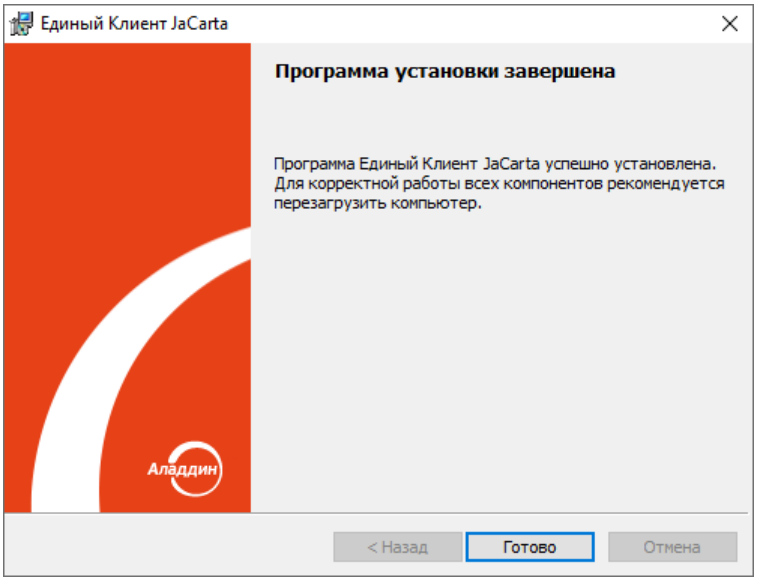


Рисунок 9 - Окно завершения установки ПО "Единый Клиент JaCarta"

8. Нажмите кнопку "Готово". Перезагрузите компьютер, если будет отображено соответствующее предупреждение:

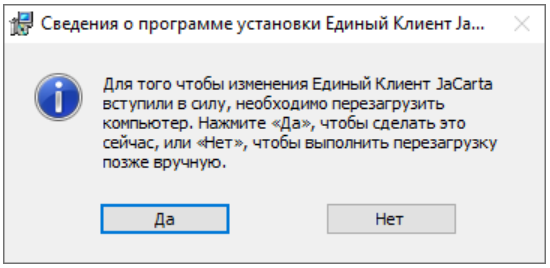


Рисунок 10 - Сведения о программе установки ПО "Единый Клиент JaCarta"

9. Будет выполнена перезагрузка компьютера. После завершения перезагрузки ПО "Единый Клиент JaCarta" готово к работе.

4.5 Установка программы в режиме командной строки

> *Перед установкой ПО «Единый Клиент JaCarta» необходимо ознакомиться с содержанием пункта 4.3 "Обязательные меры предосторожности"*

Установка программы в режиме командной строки выполняется с помощью Windows Installer – средства установки, изменения и выполнения операций из командной строки.

Совет. Для получения справки по Windows Installer активируйте команду меню "Пуск → Служебные – Windows → Выполнить". В появившемся окне "Выполнить" введите команду "msiexec" и нажмите кнопку "ОК". Будет открыто окно "Установщик Windows" со справкой о программе.

Имена пакетов установки ПО "Единый Клиент JaCarta" приведены в п. 4.2 "Описание пакетов установки".

Для установки ПО "Единый Клиент JaCarta" в режиме командной строки:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения и запустите приложение "Командная строка" от имени администратора. Для этого выберите меню "Пуск → Служебные – Windows → Командная строка" и активируйте команду "Дополнительно → Запуск от имени администратора".
3. В командной строке введите команду установки ПО "Единый Клиент JaCarta" с помощью Windows Installer с необходимыми параметрами, например:

```
msiexec /i C:\файл_установки_Единого_Клиента_JaCarta.msi
```

4.5.1 Параметры для установки программы в режиме командной строки

При установке программы в режиме командной строки существует возможность задавать особые параметры ПО "Единый Клиент JaCarta" и их значения. Для задания параметров используйте следующий формат:

```
msiexec /i файл_установки_Единого_Клиента_JaCarta.msi ПАРАМЕТР=ЗНАЧЕНИЕ ПАРАМЕТР=ЗНАЧЕНИЕ /qb
```

Список параметров установки ПО "Единый Клиент JaCarta" при его установке в режиме командной строки представлен в таблице 7.

Таблица 7 – Параметры для установки ПО "Единый Клиент JaCarta" в режиме командной строки

Параметр	Значение	Описание
INSTALL_BIO	0	Не устанавливать поддержку биометрии
	1	Установить поддержку биометрии
INSTALL_PRO_MD	0	Не устанавливать минидрайвер для токенов PRO
	1	Установить минидрайвер для токенов PRO
INSTALL_SECURLOGON	0	Не устанавливать компонент SecurLogon
	1	Установить компонент SecurLogon
INSTALL_JACARTA_VR_DRIVER	0	Не устанавливать драйвер виртуального считывателя JaCarta Virtual Reader
	1	Установить драйвер виртуального считывателя JaCarta Virtual Reader
INSTALL_TOKEN_MNG	0	Установить компонент Управление токеном
	1	Не устанавливать компонент Управление токеном
INSTALL_CERTS		Сертификаты для проверки подписи драйверов
INSTALL_DIFXAPI		Difxapi.dll для работы custom actions исправляющих установку драйверов

Параметр	Значение	Описание
CERTS_EXPIRING_WARNING_VISIBLE	0	Не отображать предупреждения об истекающем сроке действия сертификата
	1	Отображать предупреждения об истекающем сроке действия сертификата
CERTS_EXPIRED_WARNING_VISIBLE	0	Не отображать предупреждения об истекшем сроке действия сертификата
	1	Отображать предупреждения об истекшем сроке действия сертификата
DISABLE_CPRO_SC_REGISTRY	0	Оставляет регистрацию в Winlogon для считывателей JaCarta в КриптоПро CSP
	1	Удаляет регистрацию из Winlogon для считывателей JaCarta в КриптоПро CSP
ADD_JCUC_AUTORUN	""	ПО "Единый Клиент JaCarta" не будет добавлен в автозапуск *Комментарий: параметр необходимо задать СТРОГО в следующем виде:* `ADD_JCUC_AUTORUN=""`
	1	ПО "Единый Клиент JaCarta" будет добавлен в автозапуск
INSTALL_PIN_EXPIRATION_AS_DIALOG	0	Не выводить уведомление об истечении времени жизни PIN-кода в диалоговом окне (для JaCarta PKI и JaCarta PRO)
	1	Выводить уведомление об истечении времени жизни PIN-кода в диалоговом окне (для JaCarta PKI и JaCarta PRO)
INSTALL_NUMBER_DAYS_TO_PIN_EXPIRE	0	Не отображать уведомление об истекающем PIN-коде
	от 1 до 365	Задаёт за сколько дней до истечения времени жизни PIN-кода выводить уведомление
LANGUAGE	RU	Использовать русский язык интерфейса ПО "Единый Клиент JaCarta"
	EN	Использовать английский язык интерфейса ПО "Единый Клиент JaCarta"
SYNCPINDOMAIN	Имя домена	Использовать указанное имя домена для функциональности "Синхронизация паролей электронного ключа и учетной записи домена Windows" (см. раздел 10)

Пример. Команда установки ПО "Единый Клиент JaCarta" в режиме командной строки в случае задания дополнительных параметров:

```
msiexec.exe /i C:\JaCartaUnifiedClient_3.X.XXXX_win-x64_ru-Ru.msi
INSTALL_JACARTA_VR_DRIVER=1 /qb
```

В данном примере будет выполнена установка ПО "Единый Клиент JaCarta" со следующими параметрами:

- `INSTALL_JACARTA_VR_DRIVER=1` – установить драйвер виртуального считывателя JaCarta Virtual Reader;

- `/qb` – ключ Windows Installer, в соответствии с которым будет отображён ход установки, при этом не никаких вопросов пользователю задано не будет, также и не будет отображаться кнопка "Cancel" ("Отмена").

4.6 Отображение команды "Управление токеном" на экране блокировки Windows

После завершения установки ПО "Единый Клиент JaCarta" и перехода в экран блокировки Windows, будет отображена команда "Управление токеном". Она отображается, если в ходе установки был выбраны один из следующих видов: "Стандартная" или "Выборочная с компонентом Управление токеном".

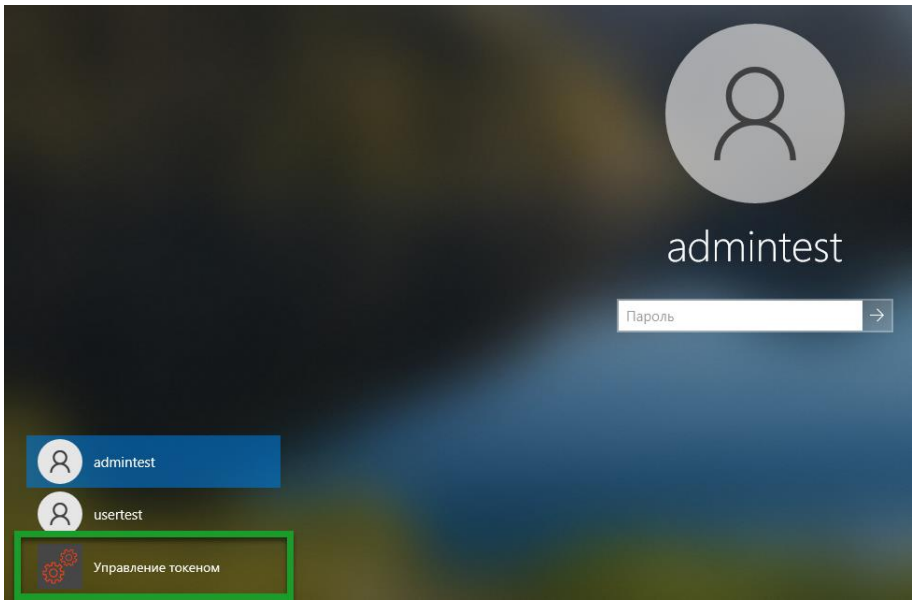


Рисунок 11 - Элемент управления на экране блокировки Windows

Скрыть отображение данного элемента управления можно с помощью удаления компонента "Управление токеном". Для этого необходимо последовательно выбрать "Панель управления", "Программы и компоненты", "Единый Клиент JaCarta" и нажать кнопку "Изменить". После чего исключить компонент "Управление токеном" из установленных компонентов:

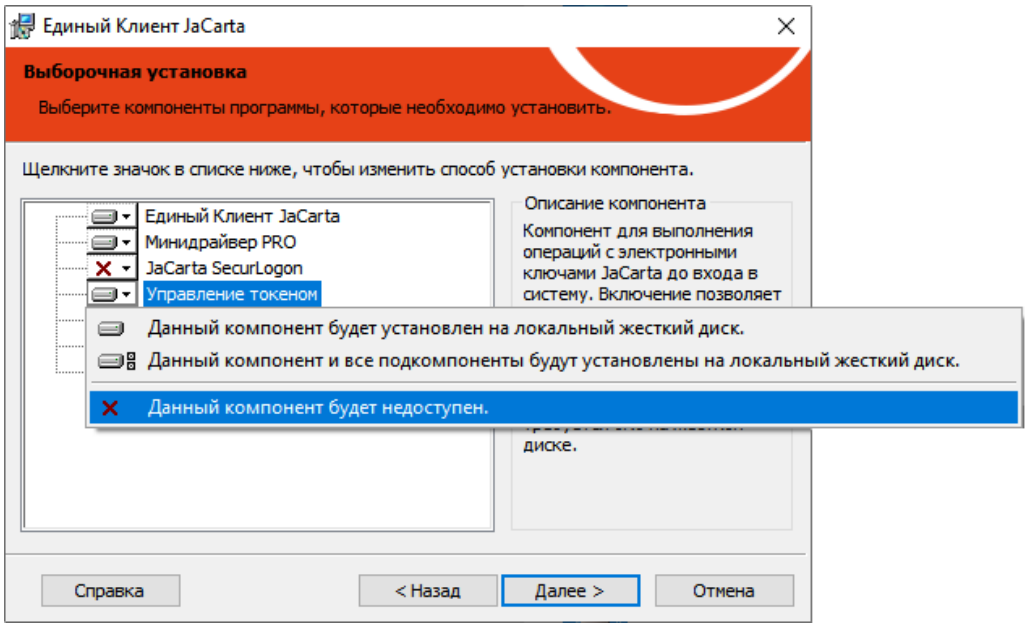


Рисунок 12 - Исключение компонента "Управление токеном"

5. Изменение, исправление, удаление программы

> *Перед удалением или обновлением ПО "Единый Клиент JaCarta" обязательно убедитесь в том, что на вашем компьютере настроена хотя бы одна учетная запись, которая позволяет входить с административными полномочиями при помощи логина и пароля, то есть без использования токенов и смарт-карт.*

5.1 Изменение программы

Изменение ПО "Единый Клиент JaCarta" включает в себя изменение перечня его установленных компонентов.

Для изменения ПО "Единый Клиент JaCarta":

1. Для изменения ПО "Единый Клиент JaCarta" перейдите в меню "Пуск → Параметры → Приложения → Приложения и возможности". Будет открыто окно (Рисунок 13):

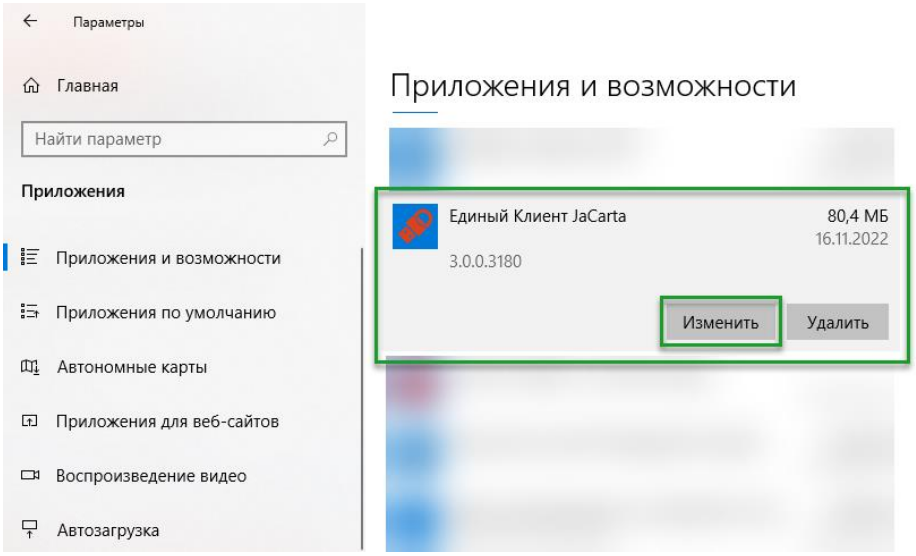


Рисунок 13 – Приложения и возможности. Изменение программы

2. В списке установленных программ выберите "Единый Клиент JaCarta" и нажмите кнопку "Изменить". Отобразится окно приветствия мастера установки:

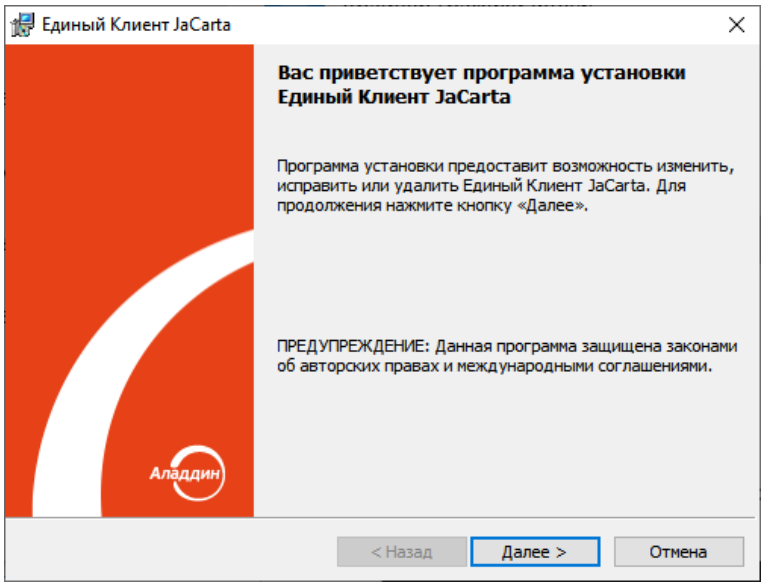


Рисунок 14 - Окно приветствия мастера установки

3. Нажмите кнопку "Далее". В появившемся окне "Изменение, исправление или удаление Единый Клиент JaCarta" выберите опцию "Изменить":

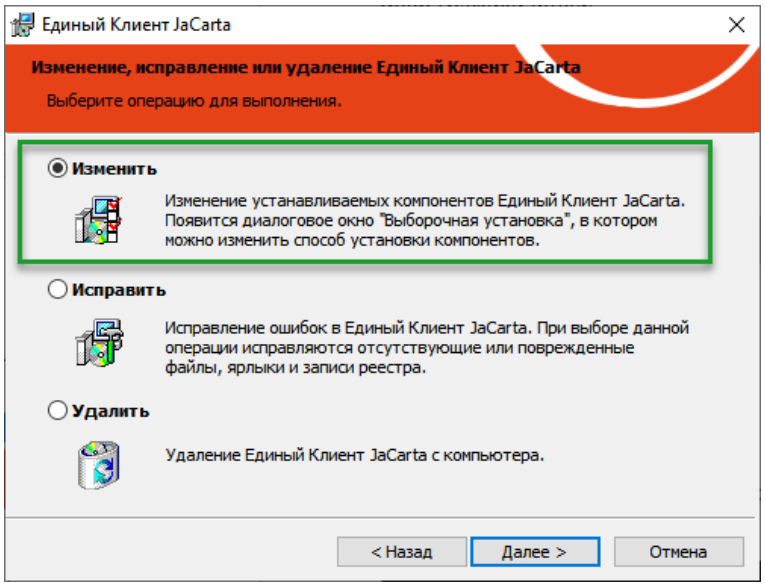


Рисунок 15 - Изменение, исправление или удаление ПО "Единый Клиент JaCarta"

4. Нажмите кнопку "Далее". Будет отображено окно "Выборочная установка компонентов ПО "Единый Клиент JaCarta" для изменения перечня установленных компонентов ПО "Единый Клиент JaCarta" (см. рисунок 4).
5. Выполняйте шаги 4–9 процедуры установки ПО "Единый Клиент JaCarta" (см. п. 4.4 "Установка программы с помощью мастера установки").

5.2 Исправление программы

Исправление программы позволяет добавить отсутствующие или исправить поврежденные файлы, ярлыки и записи реестра ПО "Единый Клиент JaCarta".
Перед запуском процедуры исправления убедитесь, что пакет установки ПО "Единый Клиент JaCarta" хранится по тому же пути, что и в ходе его установки.

Для исправления ПО "Единый Клиент JaCarta":

1. Выполните шаги 1, 2 процедуры изменения программы (см. п. 5.1 "Изменение программы").

2. В окне "Изменение, исправление или удаление ПО "Единый Клиент JaCarta" (см. рисунок 15) выберите опцию "Исправить".
3. Нажмите кнопку "Далее". Будет отображено окно "Исправление программы":

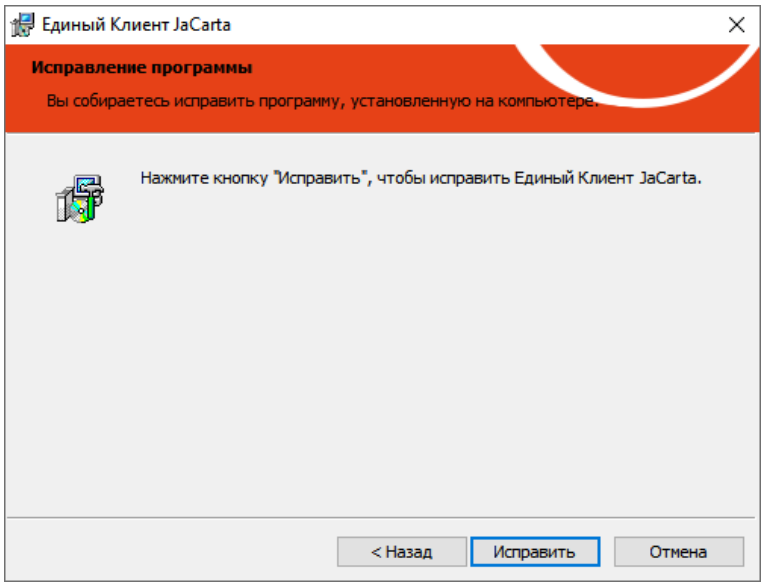


Рисунок 16 - Исправление программы

4. Нажмите кнопку "Исправить". Будет выполняться поиск пакета установки ПО "Единый Клиент JaCarta" по тому же пути, что и в ходе его установки.

5.3 Удаление программы

5.3.1 Удаление программы с помощью мастера удаления

Для удаления ПО "Единый Клиент JaCarta":

1. Активируйте меню "Пуск → Алладин Р.Д. – Удалить ПО "Единый Клиент JaCarta". На экране будет отображено сообщение:

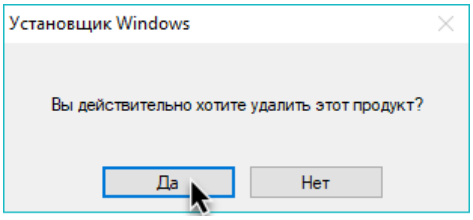


Рисунок 17 – Подтверждения удаления ПО "Единый Клиента JaCarta"

2. Нажмите кнопку "Да" в окне сообщения. Будет выполняться удаление программы. По окончании на экране появится сообщение с предложением перезагрузки компьютера:

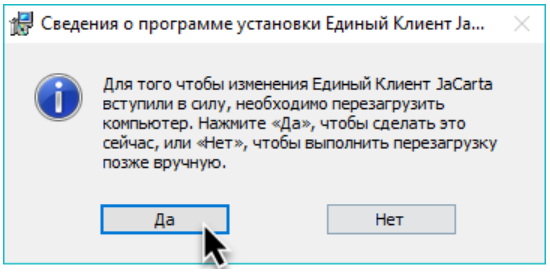


Рисунок 18 – Предложение перезагрузки компьютера

3. Нажмите кнопку "Да". Будет выполняться перезагрузка компьютера. По окончание перезагрузки процедура удаления Единого Клиент JaCarta будет завершена.

5.3.2 Удаление программы в режиме командной строки

Для удаления ПО "Единый Клиент JaCarta" в режиме командной строки:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Запустите интерпретатор командной строки от имени администратора.
4. Выполните команду msiexec в следующем формате:

```
msiexec /x JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi
```

   где `JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi` – имя установочного файла ПО "Единый Клиент JaCarta" для 32-битной платформы.
   Для 64-битной платформы замените это имя на `JaCartaUnifiedClient_x.x.xx.xxx_win-x64_ru-Ru.msi`. Чтобы выполнить удаление в полуавтоматическом режиме, то есть без необходимости подтверждения действий, добавьте в конце строки параметр `/q`.
5. После того как ПО "Единый Клиент JaCarta" будет удален, перезагрузите компьютер.

6. Настройка работы программы и устройств

Для настройки ПО "Единый Клиент JaCarta":

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

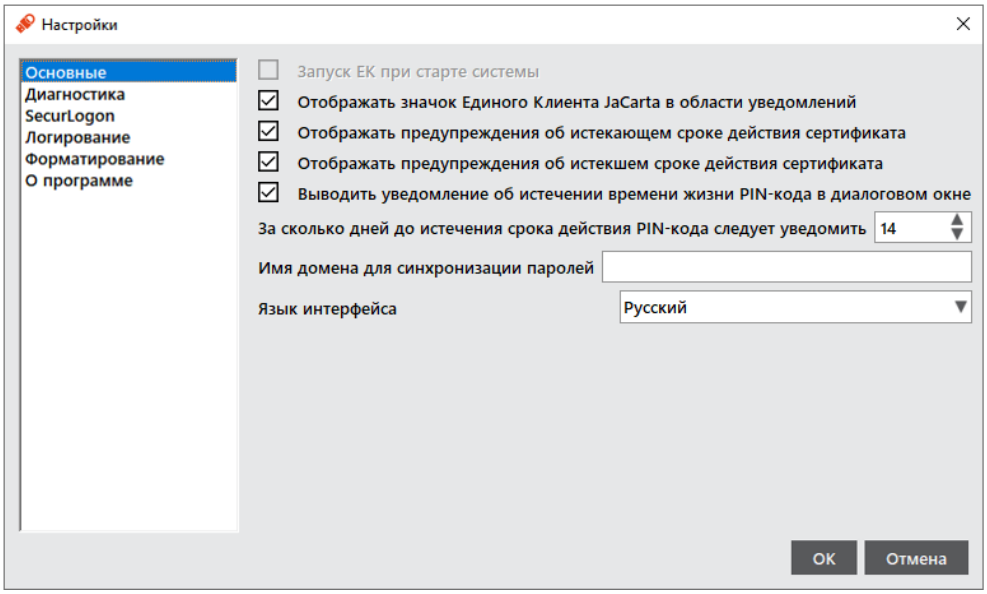


Рисунок 19 - Окно "Настройки". Вкладка "Основные"

2. Перейдите к нужной вкладке:
   - "Основные" – содержит основные настройки ПО "Единый Клиент JaCarta";
   - "Диагностика" – позволяет выполнить проверку целостности продукта;
   - "SecurLogon"[5] – содержит информацию о лицензии SecurLogon;
   - "Логирование" – содержит настройки логирования ПО "Единый Клиент JaCarta";
   - "Форматирование" – позволяет выбрать режим работы мастера форматирования по умолчанию;
   - "О программе" – содержит информацию о версии ПО "Единый Клиент JaCarta" и способах связи с технической поддержкой.
3. Внесите необходимые изменения в настройки и нажмите кнопку "OK". Изменения будут сохранены, окно настроек будет закрыто. Для выхода из окна настроек без сохранения внесенных изменений нажмите на кнопку "Отмена".

6.1 Вкладка "Основные"

Описание настроек на вкладке "Основные" приведено в таблице 8.

Таблица 8 – Вкладка "Основные". Описание настроек

Настройка	Описание
Запуск ЕК при старте системы	Данная настройка отвечает за добавление в автозагрузку Единый Клиент JaCarta. Для того чтобы настройка стала доступной для редактирования необходимо запустить Единый Клиент JaCarta от имени администратора
Отображать значок Единого Клиента JaCarta в области уведомлений	Определяет, будет ли отображаться элемент управления  в области уведомлений

[5] Вкладка "SecurLogon" может отсутствовать, если не был установлен компонент JaCarta SecurLogon. Подробнее об установке компонента см. п. 4.4 "Установка программы с помощью мастера установки"

Отображать предупреждения об истекающем сроке действия сертификата	Определяет, будет ли отображаться предупреждение об истекающем сроке действия сертификата, хранимом в памяти приложения
Отображать предупреждения об истекшем сроке действия сертификата	Определяет, будет ли отображаться предупреждение об истекшем сроке действия сертификата, хранимом в памяти приложения
Выводить уведомление об истечении времени жизни PIN-кода в диалоговом окне	Определяет, будет ли отображаться уведомление об истечении времени жизни PIN-кода в диалоговом окне (для JaCarta PKI и JaCarta PRO)
За сколько дней до истечения срока действия PIN-кода следует уведомить	Определяет, за сколько дней до истечения времени жизни PIN-кода выводить уведомление. Доступные значения от 1 до 365 дней. При значении равном 0 уведомление не выводится
Имя домена для синхронизации паролей	Содержит поле для отображения имени домена Windows, в котором зарегистрирована учетная запись пользователя. После ввода имени домена становится доступной кнопка смены PIN-кода и пароля домена. Описание процедуры смены PIN-кода и пароля домена приведено в разделе 10. Синхронизация паролей электронного ключа и учетной записи домена Windows
Язык интерфейса	Позволяет выбрать язык интерфейса ПО "Единый Клиент JaCarta"

6.2 Вкладка "Диагностика"

Описание настроек вкладки "Диагностика" (см. рисунок 20) приведено в таблице 9.

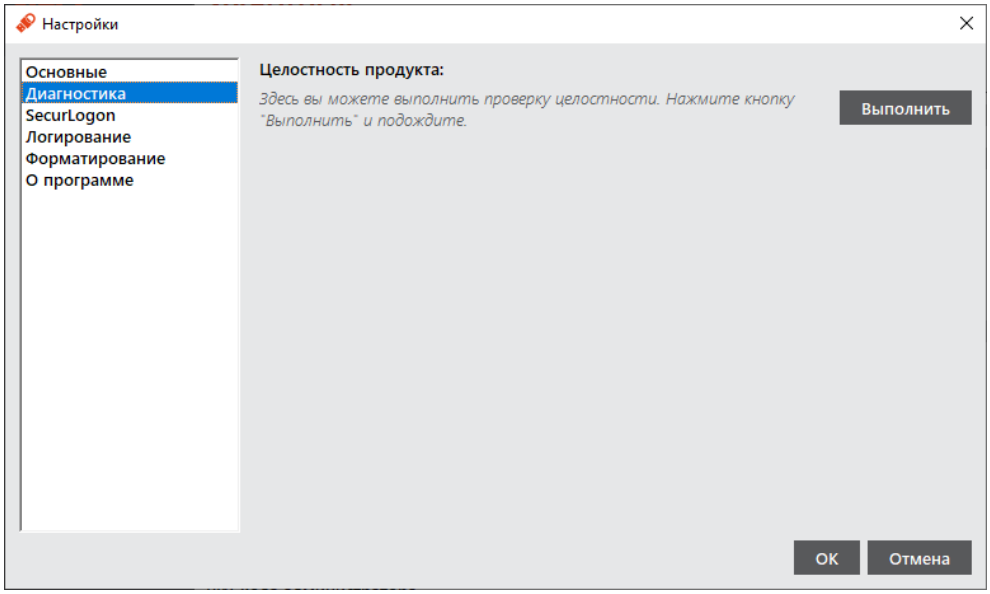


Рисунок 20 - Окно "Настройки". Вкладка "Диагностика"

Таблица 9 - Вкладка "Диагностика". Описание настроек

Настройка	**Описание**
Выполнить	Выполняется проверка целостности ПО "Единый Клиент JaCarta" с последующим отображением результатов проверки (см. рисунок 21)

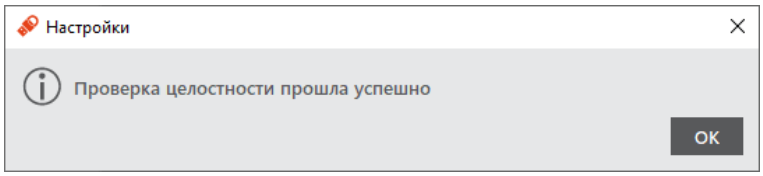


Рисунок 21 - Сообщение о результате проверки целостности

6.3 Вкладка "SecurLogon"

Если в ходе установки ПО "Единый Клиент JaCarta" был установлен компонент SecurLogon, то вкладка "SecurLogon" будет отображена в окне "Настройки" (см. рисунок 22). Описание настроек вкладки приведено в таблице 10.

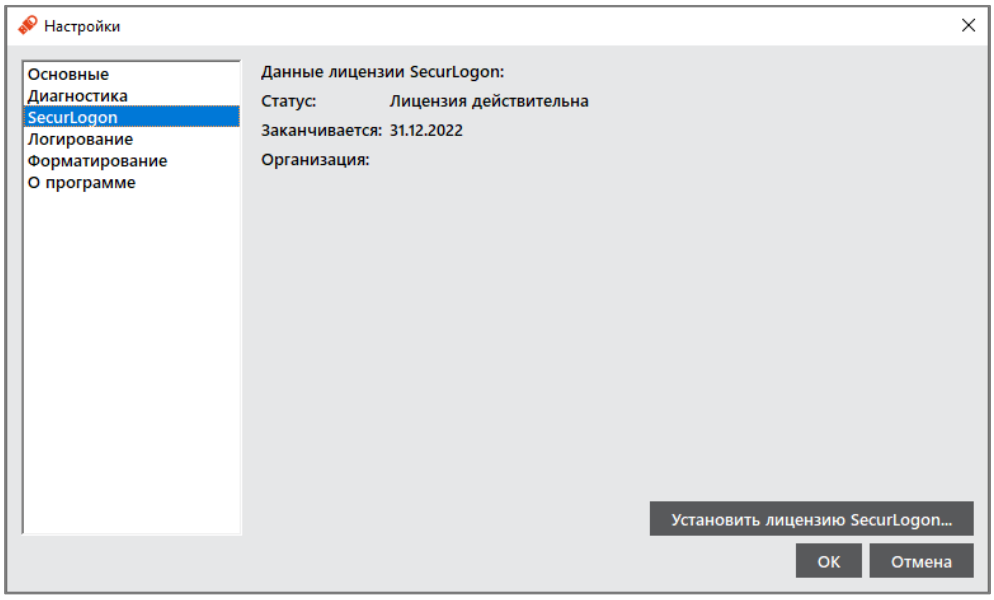


Рисунок 22 - Окно "Настройки". Вкладка "SecurLogon"

Подробнее про работу с продуктом JaCarta SecurLogon см. документ "JaCarta SecurLogon. Руководство администратора".

Таблица 10 - Вкладка "SecurLogon". Описание настроек

Настройка	Описание
Установить лицензию SecurLogon	Открывает диалоговое окно для выбора и установки файла лицензии ПО JaCarta SecurLogon с последующим отображением информации о статусе лицензии

6.4 Вкладка "Логирование"

Во вкладке "Логирование" определяются настройки логирования ПО "Единый Клиент JaCarta" и Единой библиотеки PKCS #11. Описание окна "Настройки" на вкладке "Логирование" (см. рисунок 23) приведено в таблице 11.

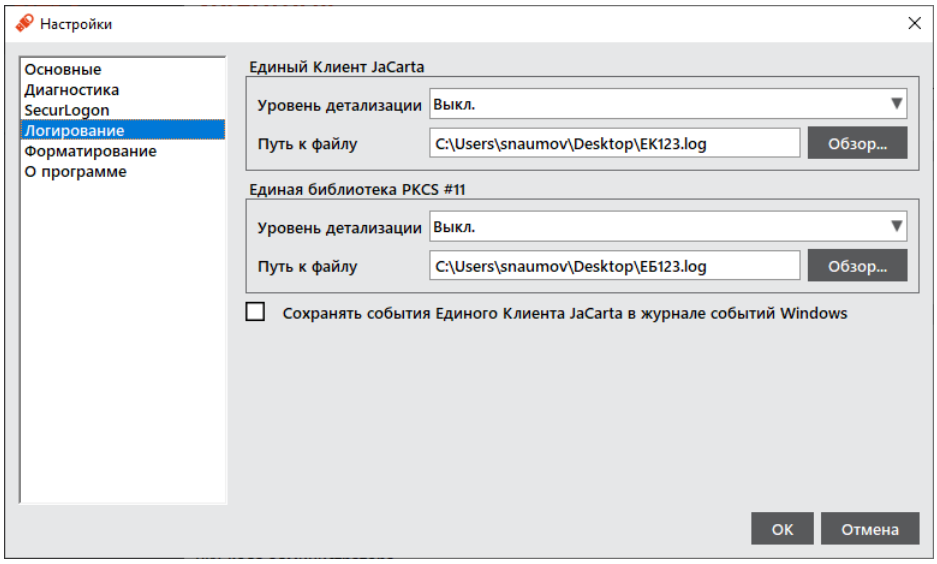


Рисунок 23 - Окно "Настройки". Вкладка "Логирование"

Таблица 11 - Вкладка "Логирование". Описание настроек

Настройка	Описание
Сегмент "Единый Клиент JaCarta"	Задает настройки логирования ПО "Единый Клиент JaCarta": • "Уровень детализации" – для выбора опций: Выключен / Стандартный / Расширенный. • Поле "Путь к файлу" – для отображения пути к файлу с логами. • Кнопка "Обзор" – для указания места расположения файла с логами
Сегмент "Единая библиотека PKCS #11"	Задает настройки логирования Единой библиотеки PKCS #11: • "Уровень детализации" – для выбора опций: Выключен / Стандартный / Расширенный. • Поле "Путь к файлу" – для отображения пути к файлу с логами. • Кнопка "Обзор" – для указания места расположения файла с логами
Флажок "Сохранять события Единого Клиента JaCarta в журнале событий Windows"	После установки флажка, в журнал событий Windows (Event Viewer) будут записаны следующие события Единого Клиента JaCarta: • Запуск и завершение работы ПО "Единый Клиент JaCarta"; • Подключение и отключение токена или смарт-карты; • Успешная или неуспешная аутентификация в приложение; • Успешная или неуспешная смена PIN-кода пользователя и администратора; • Форматирование приложения; • Разблокировка токена. Для активации флажка необходимо запустить Единый Клиент JaCarta с правами администратора. Записанные события будут отображены в разделе "Журналы Windows -> Приложения" операционной системы. Описание событий, сохраняемых в журнал событий Windows, представлено ниже (Таблица 12)

Таблица 12 - Описание событий, сохраняемых в журнал событий Windows

Уровень	Код события	Описание	Подробности
[Info]	Код события: 1001	Выполнен запуск программы "Единый Клиент JaCarta"	Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Error]	Код события: 1002	Ошибка запуска программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1003	Выполнено завершение работы программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1004	Ошибка контроля целостности программы "Единый Клиент JaCarta"	Ошибка: [код ошибки] Версия: [номер версии] Изготовитель: АО "Аладдин Р. Д."
[Info]	Код события: 1005	Выполнено подключение устройства	Модель, Серийный номер, Метка
[Info]	Код события: 1006	Выполнено отключение устройства	Модель, Серийный номер, Метка
[Info\Error]	Код события: 1007	Выполнена попытка аутентификации пользователя в приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности аутентификации: Результат, Апплет, Остаток попыток аутентификации
[Info\Error]	Код события: 1008	Выполнена попытка изменения PIN-кода [пользователя/администратора] приложения [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности изменения PIN-кода [пользователя/администратора]: Результат, Апплет
[Warning]	Код события: 1009	Заблокировано приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности блокировки: Апплет Причина блокировки: достижение предельного числа последовательных неудачных попыток предъявления PIN-кода пользователя
[Info]	Код события: 1010	Разблокировано приложение [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности разблокировки: Апплет
[Info\Error]	Код события: 1011	Выполнена попытка форматирования приложения [имя приложения] в устройстве	Модель, Серийный номер, Метка Подробности форматирования: Результат, Апплет
[Warning]	Код события: 1020	Необходимо сменить PIN-код пользователя для приложения [имя приложения]	Модель, Серийный номер, Апплет
[Warning]	Код события: 1020	Срок действия PIN-кода пользователя для приложения [имя приложения] истекает [дата]	Модель, Серийный номер, Апплет

6.5 Вкладка "Форматирование"

Во вкладке "Форматирование" определяется режим работы мастера форматирования приложений, который будет использоваться по умолчанию.

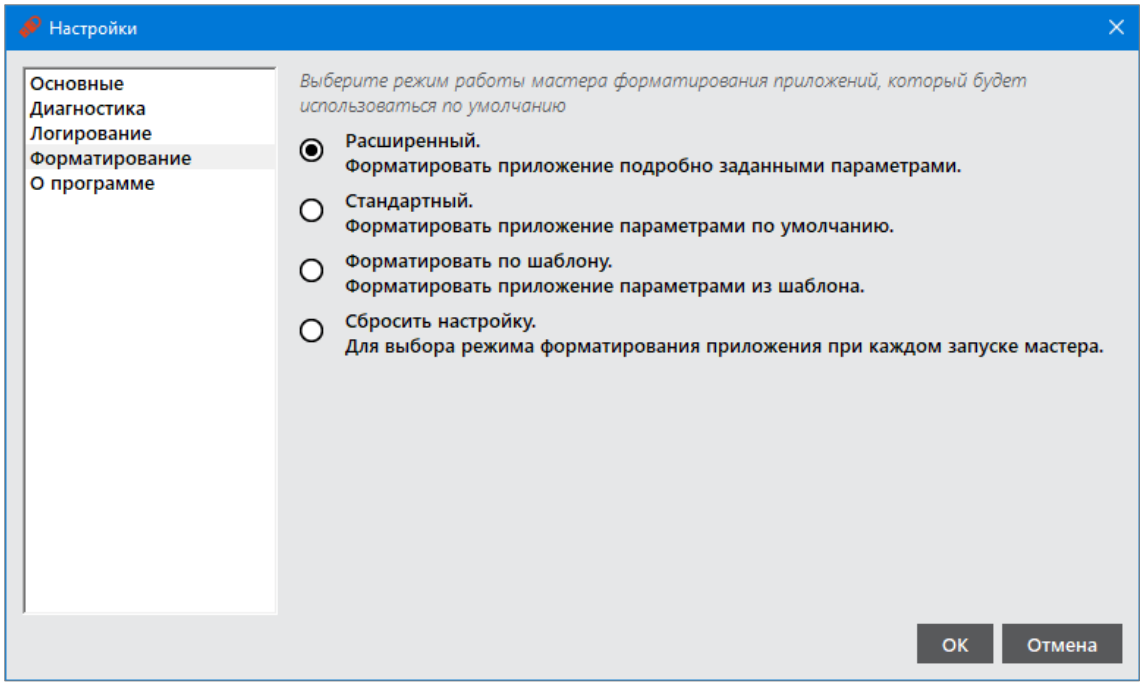


Рисунок 24 – Окно "Настройки". Вкладка "Форматирование"

Описание окна "Настройки" на вкладке "Форматирование" (см. Рисунок 24) приведено в таблице 13.

Таблица 13 – Вкладка "Форматирование". Описание настроек

Настройка	Описание
Расширенный	По умолчанию будет использоваться расширенный режим форматирования, позволяющий задать параметры форматирования
Стандартный	По умолчанию будет использоваться стандартный режим форматирования параметрами по умолчанию
Форматировать по шаблону	По умолчанию будет использоваться режим форматирования по ранее настроенному шаблону
Сбросить настройку	При выборе опции режим форматирования будет определяться при каждом запуске мастера форматирования

6.6 Смарт-карт ридер JCR: изменение режима работы

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

Для изменения режима работы:

1. Подсоединить смарт-карт ридер JCR к компьютеру.
2. Вставить смарт-карту в смарт-карт ридер JCR и запустить ПО "Единый Клиент JaCarta.

3. Выбрать нужную смарт-карту в левой панели окна ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим (по умолчанию выбран стандартный) (см. Рисунок 25).

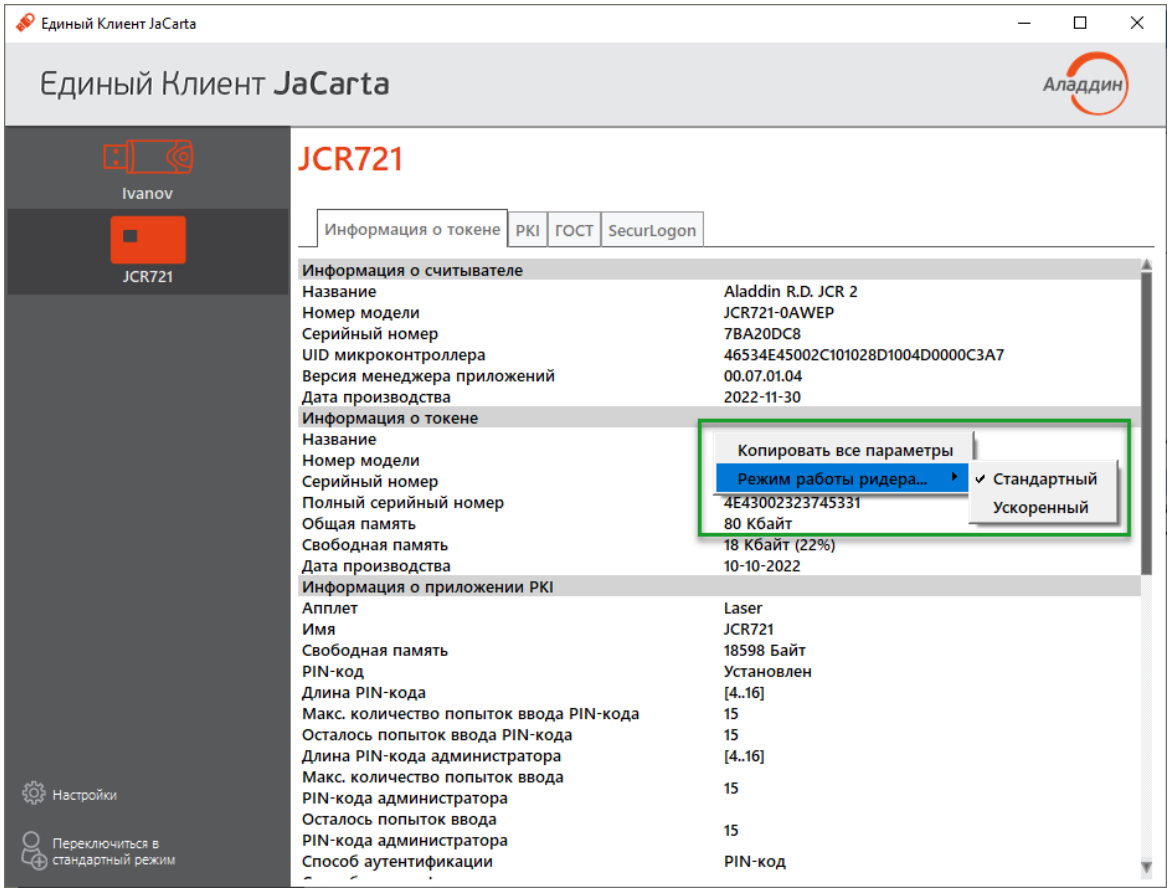


Рисунок 25 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

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

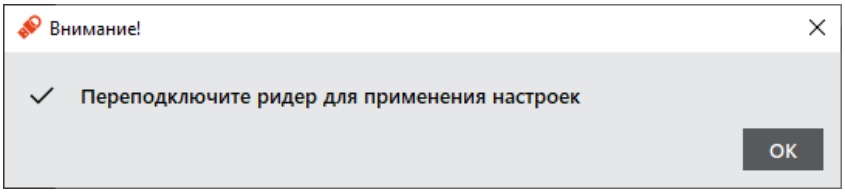


Рисунок 26 – Информационное сообщение о переподключении ридера

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

6. Нажать кнопку "OK" для закрытия сообщения.

6.7 Aladdin SecurBIO: изменение типа биометрической системы смарт-карт ридера

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

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

Для изменения режима работы:

1. Подсоединить биометрический смарт-карт ридер Aladdin SecurBIO Reader к компьютеру.
2. Вставить персональную смарт-карту в биометрический смарт-карт ридер Aladdin SecurBIO Reader и запустить ПО "Единый Клиент JaCarta".
3. Выбрать нужную смарт-карту в левой панели окна ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
4. Во вкладке "Информация о токене" вызвать контекстное меню и выбрать желаемый режим работы биометрической системы (по умолчанию выбран стандартный режим) (см. Рисунок 25).

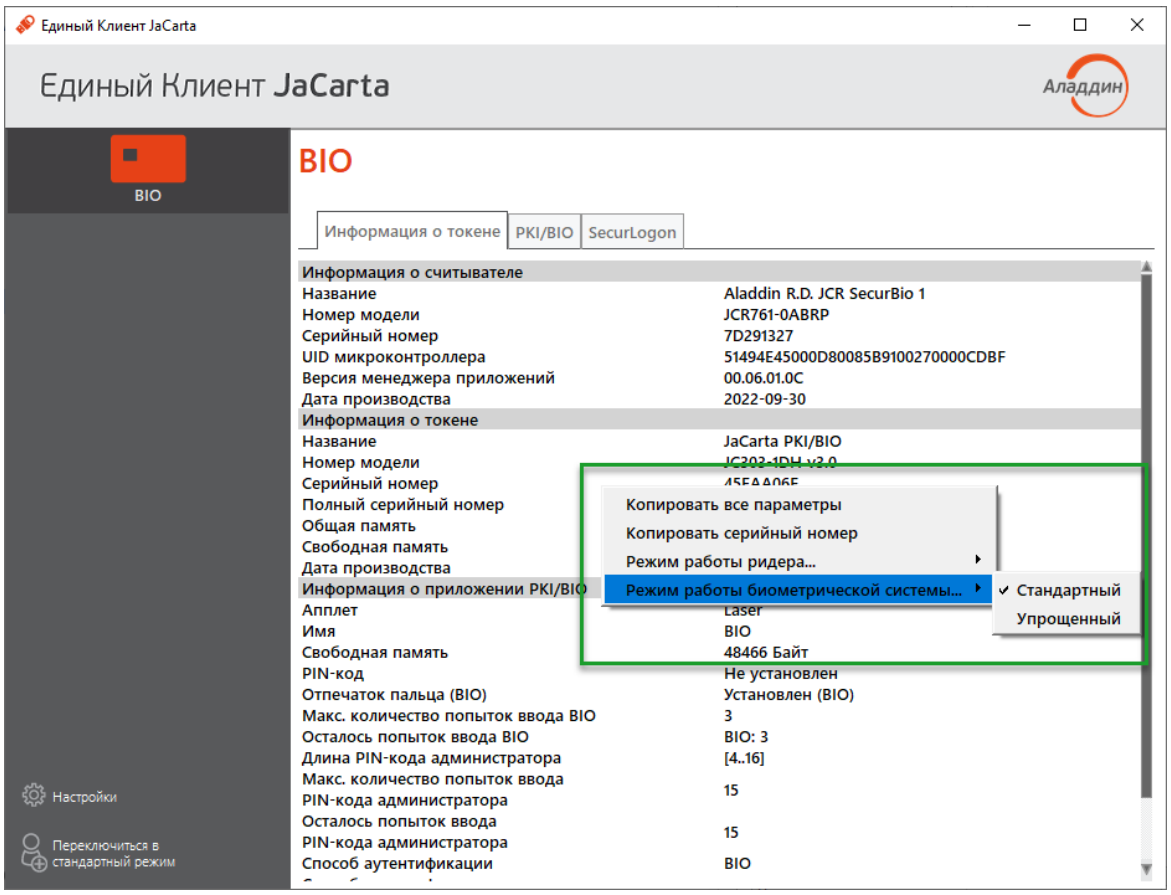


Рисунок 27 – Вкладка "Информация о токене". Контекстное меню выбора режима работы ридера

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

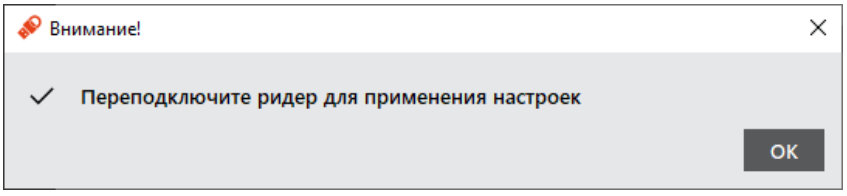


Рисунок 28 – Информационное сообщение о переподключении ридера

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

6. Нажать кнопку "OK" для закрытия сообщения.

6.8 JaCarta SecurBIO: настройка и работа

JaCarta SecurBIO - ключевой носитель информации (USB-токен) со встроенным сканером отпечатков пальцев.

JaCarta SecurBIO идентичен токену, однако контроль доступа к ключевому носителю усилен за счет биометрической идентификации по отпечатку пальца.

JaCarta SecurBIO является CCID-совместимым USB-устройством и сочетает в одном корпусе ёмкостный сканер отпечатков пальцев, вибромотор, светодиоды и другие компоненты.

В данном разделе описаны настройка (регистрация отпечатков пальцев, сброс к заводским настройкам, смена режима биометрической идентификации и т.д.) и работа с JaCartaBIO.

Перед первым использованием JaCarta SecurBIO рекомендуется сменить PIN-код администратора, установленный по умолчанию от приложения BIO Manager.

В Таблица 14 указаны PIN-коды от приложения BIO Manager.

Таблица 14 - PIN-коды приложения BIO Manager

Параметр	**Приложение BIO Manager**
PIN-код администратора по умолчанию	1234567890
PIN-код пользователя по умолчанию	не предусмотрен
PIN-код сброса к заводским настройкам	0801378717

6.8.1 Изменение PIN-код администратора

Для смены PIN-кода администратора необходимо выполнить следующие действия:

1. Подсоединить электронный ключ JaCarta SecurBIO к компьютеру;
2. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим;
3. Перейти на вкладку [BIO manager] и нажать кнопку <Сменить PIN-код> (см. Рисунок 29);

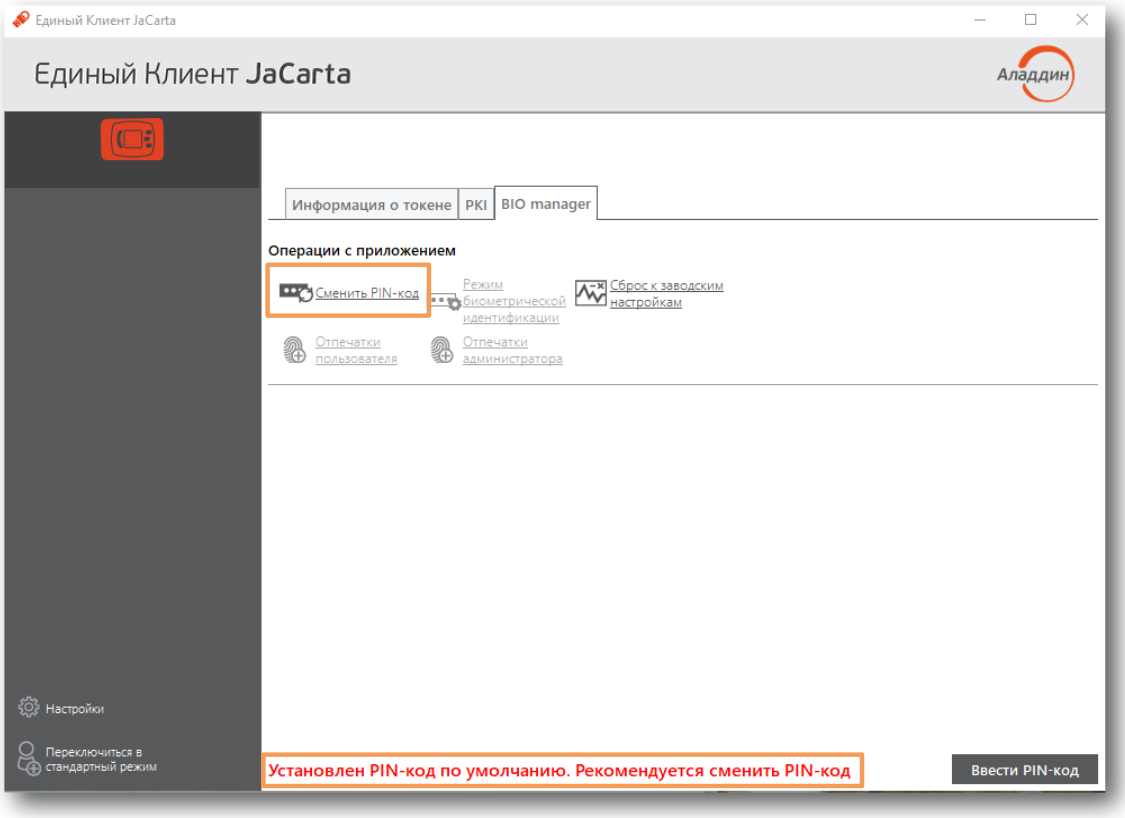


Рисунок 29 - Вкладка [BIO manager]. Элемент управления <Сменить PIN-код>

До смены PIN-кода по умолчанию на вкладке [BIO manager] отображается уведомление о необходимости смены PIN-кода Администратора по умолчанию.

4. В открывшимся окне [Сменить PIN-код] введите текущий PIN-код (**по умолчанию 1234567890**), новый PIN-код и нажмите кнопку <OK> (Рисунок 30);

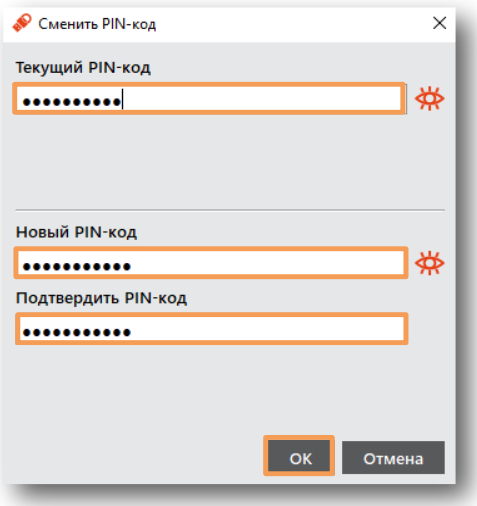


Рисунок 30 — Окно [Сменить PIN-код]

5. После завершения процесса смены PIN-кода администратора появится окно с результатом его выполнения (Рисунок 31). Нажмите кнопку <OK>.

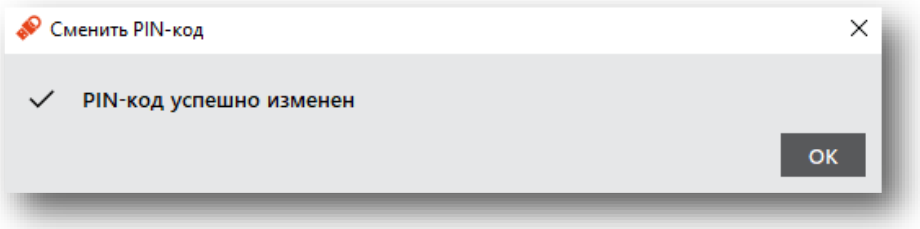


Рисунок 31 — Окно [Сменить PIN-код] с результатом

6.8.2 Ввод PIN-кода Администратора от BIO Manager

> *Для использования функций с регистрацией отпечатков пальцев пользователя и администратора необходимо ввести PIN-код администратора. Без его ввода эти функции неактивны (Рисунок 32)!*

1. Перейти на вкладку [BIO manager], нажать кнопку <Ввести PIN-код> (Рисунок 32);

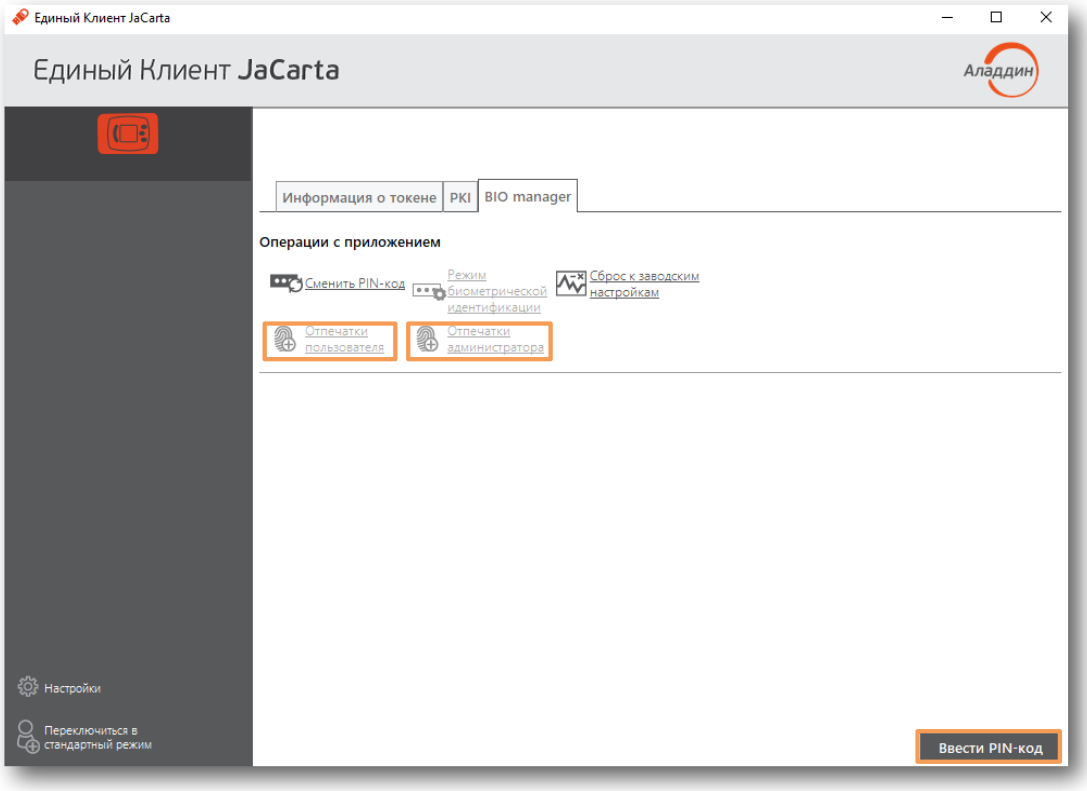


Рисунок 32 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

До начала администрирования USB-токена рекомендуется сменить PIN-код по умолчанию на новый PIN-код (см. п. 6.8.1)

2. В открывшимся окне [Аутентификация] ввести текущий PIN-код и нажать кнопку <OK> (Рисунок 33);

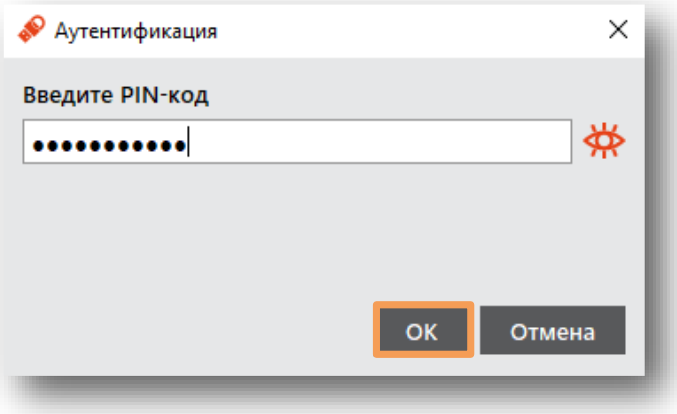


Рисунок 33 — Окно [Аутентификация]

3. После ввода PIN-кода кнопка <Ввести PIN-код> пропадет и становятся активными кнопки <Отпечатки пользователя> и <Отпечатки администратора> (Рисунок 34).

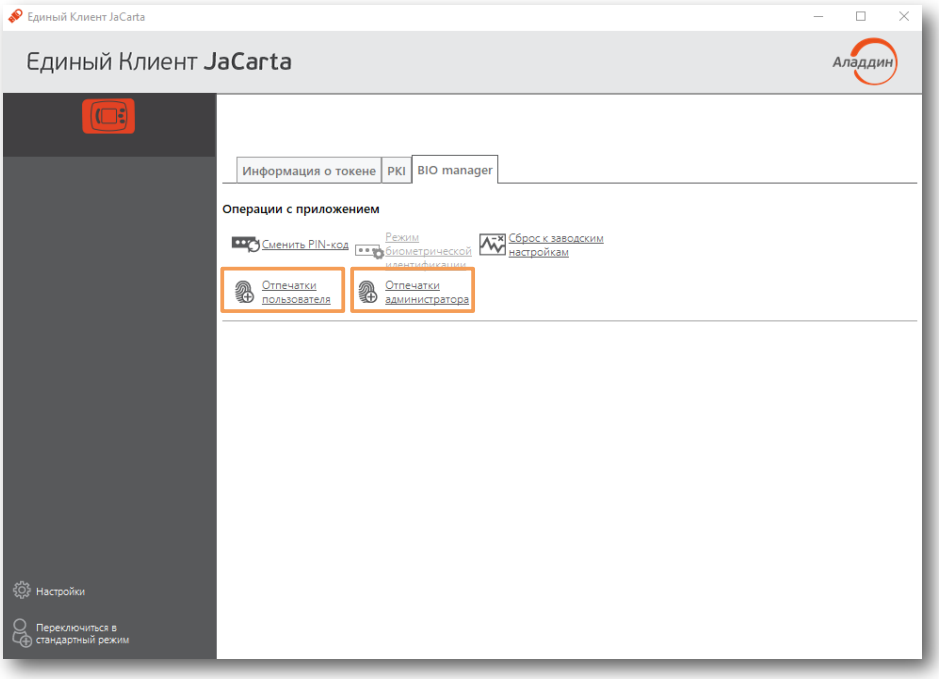


Рисунок 34 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

6.8.3 Регистрация отпечатков пальцев администратора

Для добавления отпечатков пальцев администратора необходимо выполнить следующие действия:

1. Перейти на вкладку [BIO manager] и ввести PIN-код администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно зарегистрировать отпечатки пальцев.

2. На вкладке [BIO manager] нажать кнопку <Отпечатки администратора> (Рисунок 35);

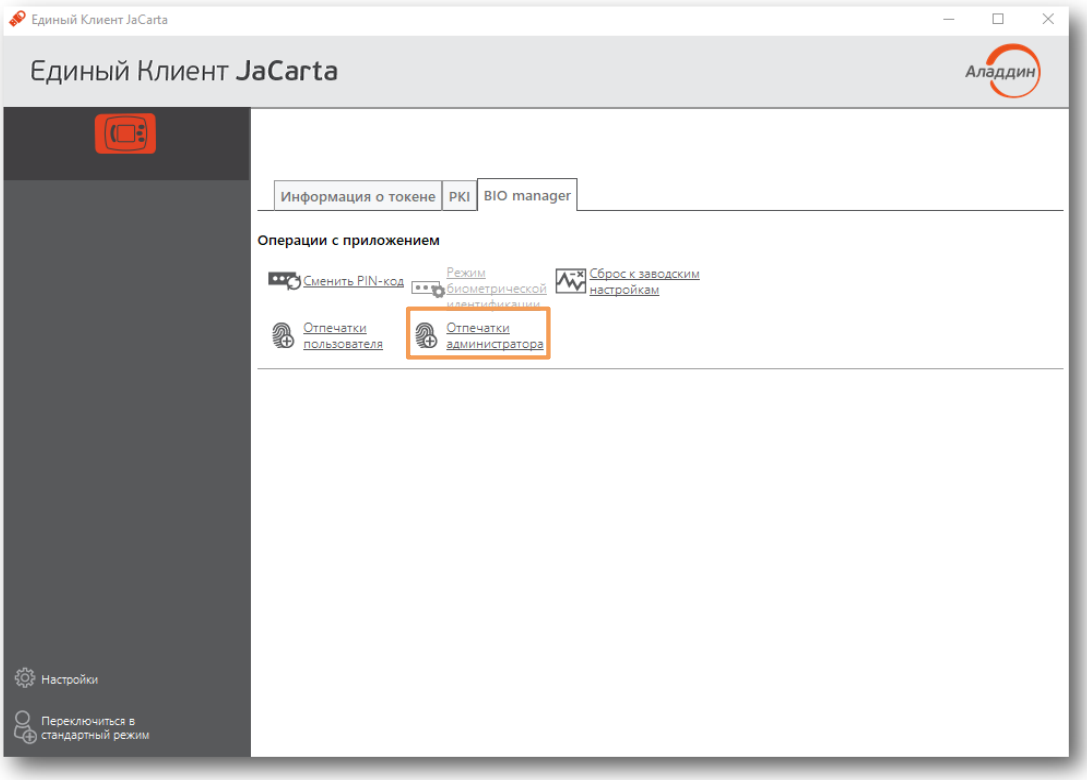


Рисунок 35 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

3. Будет открыто окно [Регистрация отпечатков] (Рисунок 36). В окне [Регистрация отпечатков] схематично изображены 2 отпечатка ладоней - левая и правая - и ячейки выбора пальца для регистрации;

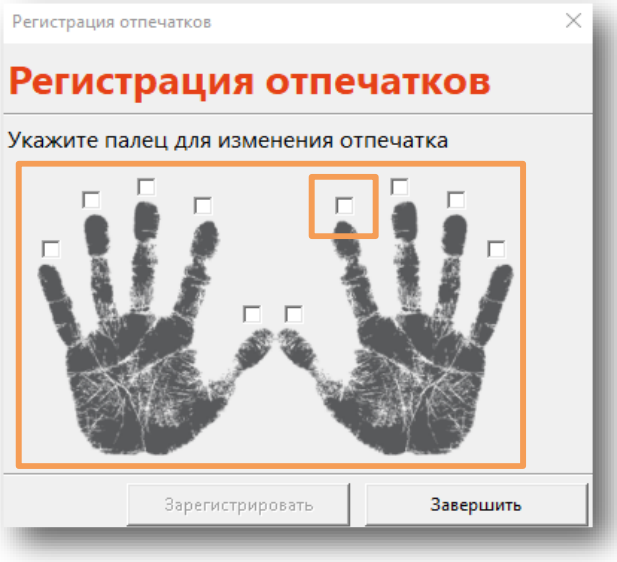


Рисунок 36 — Окно [Регистрация отпечатков]

4. Отметить флажком выбранный палец (Рисунок 37), при этом индикатор на USB-токене начнет прерывисто гореть (быстро) красным цветом;

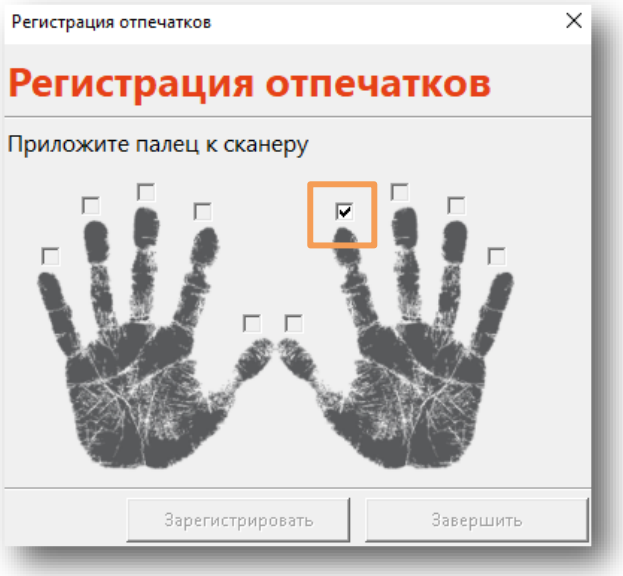


Рисунок 37 — Окно [Регистрация отпечатков]

5. Приложите палец к сканеру (администратор);

В USB-токене используется ёмкостный сканер отпечатков пальцев, поэтому палец необходимо прикладывать с небольшим усилием для более четкого сканирования и определения контрольных точек

6. После того, как палец будет приложен, начнется формирование эталонного шаблона отпечатка пальца, при этом в окне [Регистрация отпечатков] появится надпись «Шаблон отпечатка изготовлен, поднимите палец» (Рисунок 38);

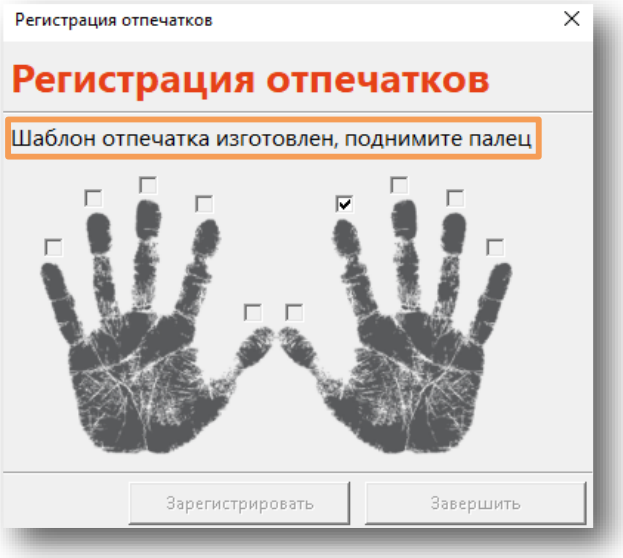


Рисунок 38 — Окно [Регистрация отпечатков]

7. Приложите палец к сканеру повторно для проверки сформированного эталонного шаблона, при этом индикатор на USB-токене будет прерывисто гореть (быстро) красным цветом (Рисунок 39);

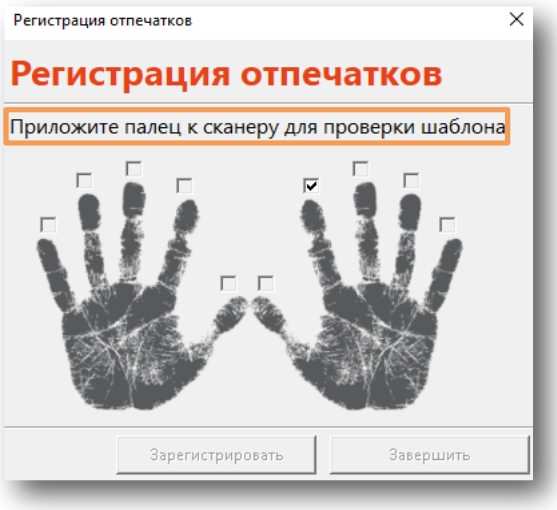


Рисунок 39 — Окно [Регистрация отпечатков]

8. В случае успешной проверки эталонного шаблона появится окно [Успешно], нажмите кнопку <OK> (Рисунок 40);

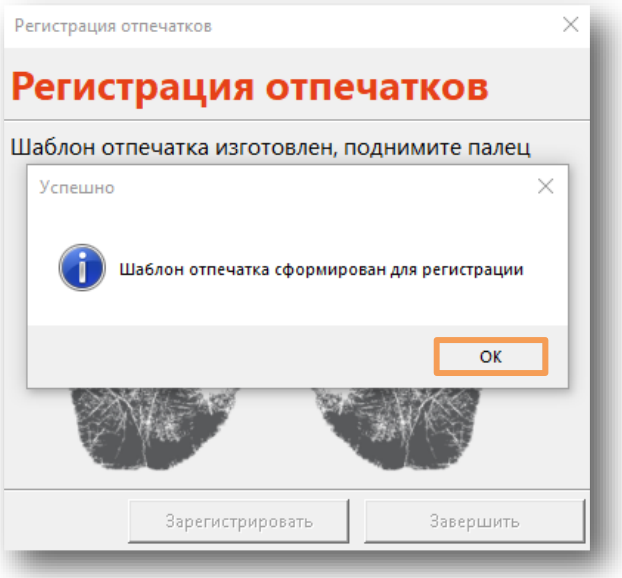


Рисунок 40 — Окно [Успешно]

9. После эталонный шаблон необходимо зарегистрировать на USB-токене: нажмите кнопку <Зарегистрировать> в окне [Регистрация отпечатков] (Рисунок 41);

Если после формирования эталонного шаблона нажать на кнопку закрытия окна (не нажимая кнопку <Зарегистрировать>), то эталонный шаблон отпечатка пальца не зарегистрируется на USB-токене!

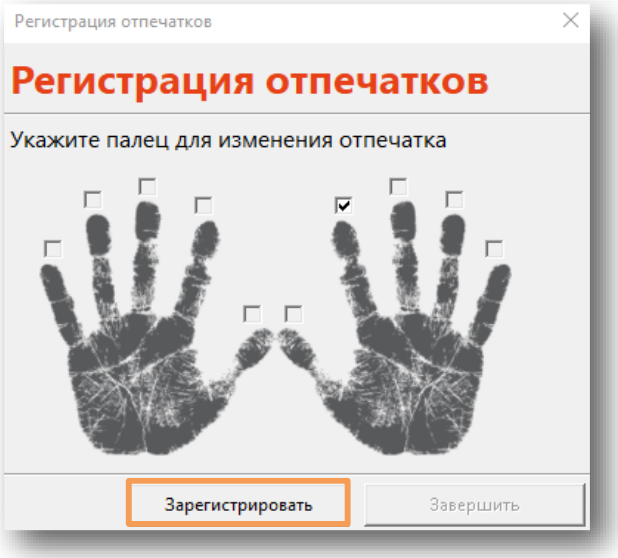


Рисунок 41 — Окно [Регистрация отпечатков]

10. После регистрации эталонного шаблона отпечатка пальца появится окно [Успешно], нажмите кнопку <OK> (Рисунок 42).

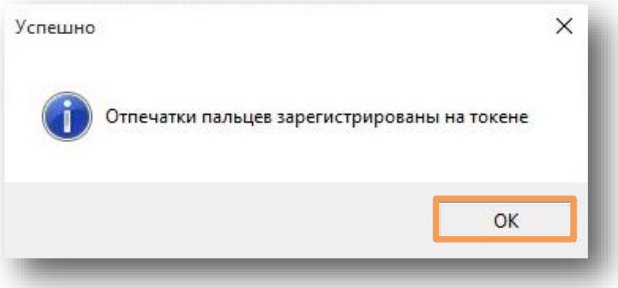


Рисунок 42 — Окно [Успешно]

6.8.4 Регистрация отпечатков пальцев пользователя

Для добавления отпечатков пальцев пользователя необходимо выполнить следующие действия:

1. Перейти на вкладку [BIO manager] и ввести PIN-код Администратора (см. п. 6.8.2);

Без ввода PIN-кода Администратора невозможно зарегистрировать отпечатки пальцев.

2. На вкладке [BIO manager] нажать кнопку <Отпечатки пользователя> (Рисунок 43);

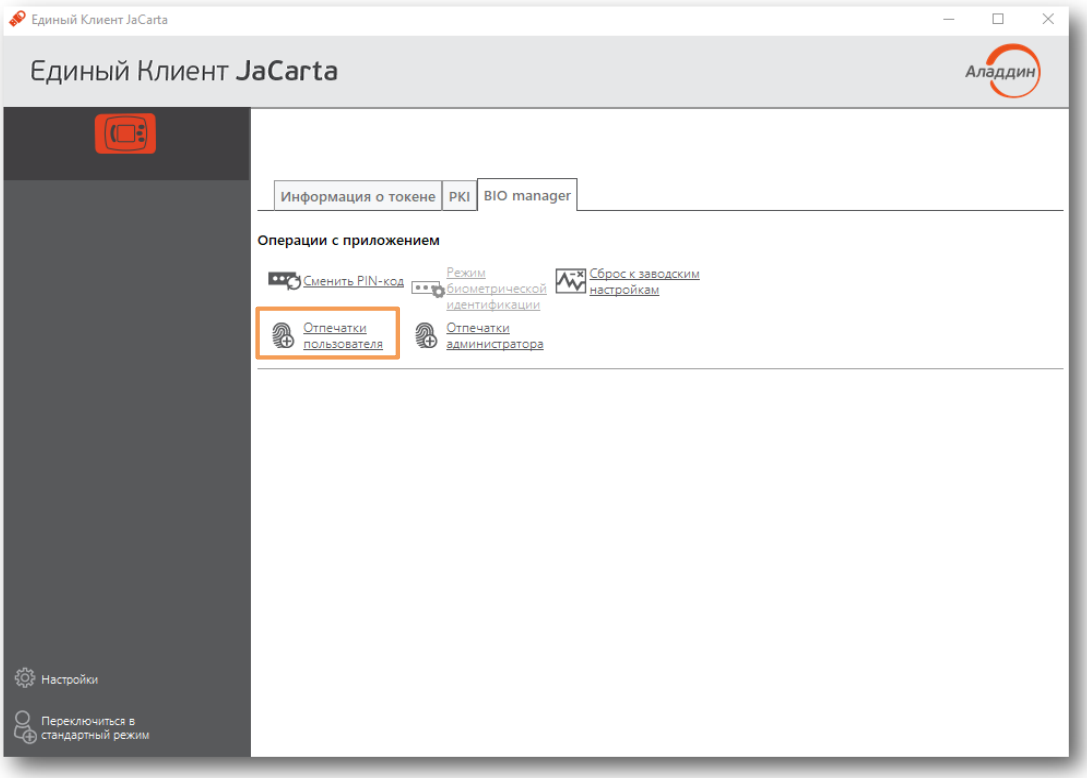


Рисунок 43 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

3. После появится окно [Регистрация отпечатков] (см. Рисунок 59). Процесс регистрации отпечатков пользователя полностью аналогичен процессу регистрации отпечатков администратора: см. п. 6.8.3, шаги 3-10.

Если после формирования эталонного шаблона нажать на кнопку закрытия окна (не нажимая кнопку <Зарегистрировать>), то эталонный шаблон отпечатка пальца не зарегистрируется на USB-токене!

Рекомендуется зарегистрировать минимум 3 разных отпечатков пальцев Пользователя!

6.8.5 Смена режима биометрической идентификации

Переключение режимов биометрической идентификации обеспечивает возможность выключения функционала биометрической идентификации при аппаратной недоступности сканера отпечатков пальцев или при отсутствии возможности выполнить успешную биометрическую идентификацию (например, палец поврежден).

Доступные режимы:

- Включено – режим работы, при котором на USB-токене зарегистрирован хотя бы 1 отпечаток пальца пользователя, в результате чего токен подключается после предварительной биометрической идентификации;
- Отключено – режим работы, при котором игнорируется база эталонных шаблонов отпечатков пальца пользователя, в результате чего USB-токен подключается без запроса предварительной биометрической идентификации. USB-токен работает в данном режиме до регистрации отпечатков пальцев пользователя.

Для смены режима необходимо:

1. Перейти на вкладку [BIO manager] и ввести PIN-код администратора (см. п. 6.8.2);

Без ввода PIN-кода администратора невозможно поменять режим биометрической идентификации

Если отпечатки пальцев пользователя не зарегистрированы, то невозможно изменить режим биометрической идентификации

2. На вкладке [BIO manager] нажать кнопку <Режим биометрической идентификации> (Рисунок 44);

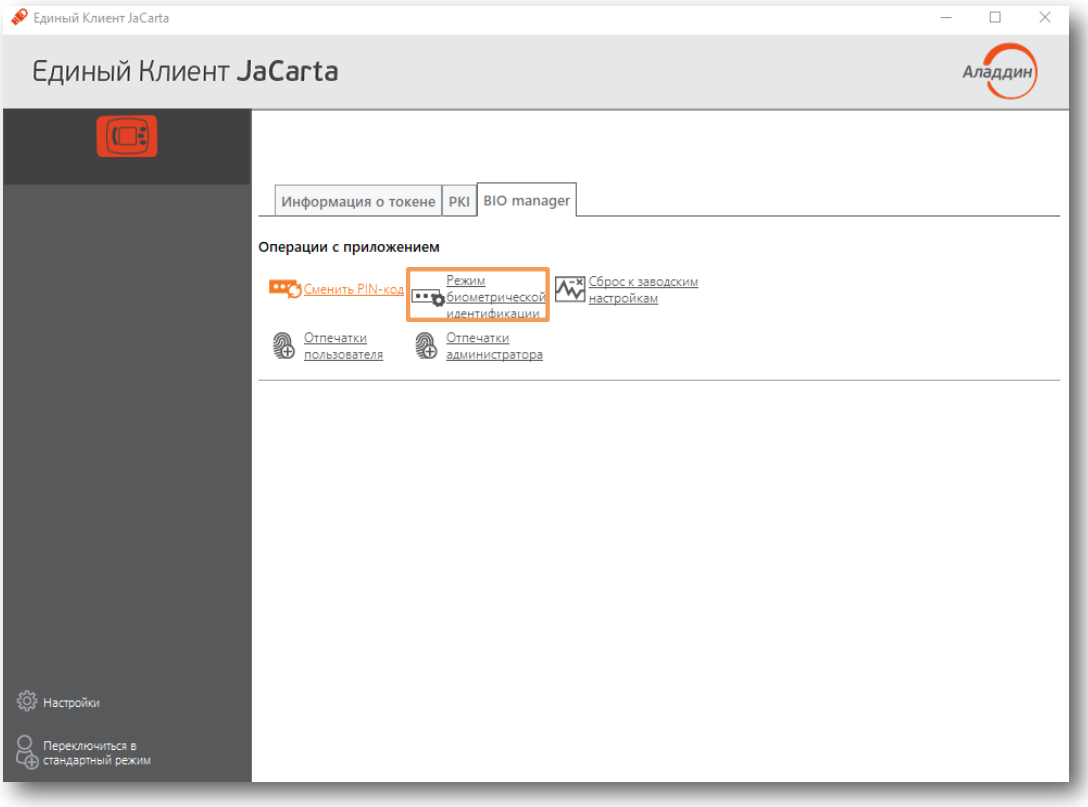


Рисунок 44 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

3. В открывшемся окне [Режим биометрической идентификации] выбрать один из двух режимов (например, <Отключено>) и нажмите кнопку <OK> (Рисунок 45);

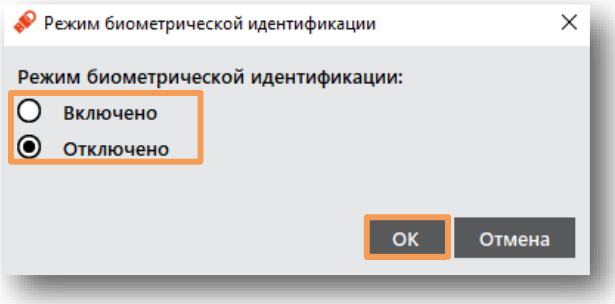


Рисунок 45 – Окно [Режим биометрической идентификации]

4. После завершения процесса смены режима биометрической идентификации появится окно с просьбой о переподключении USB-токена (Рисунок 46). Нажмите кнопку <OK>;

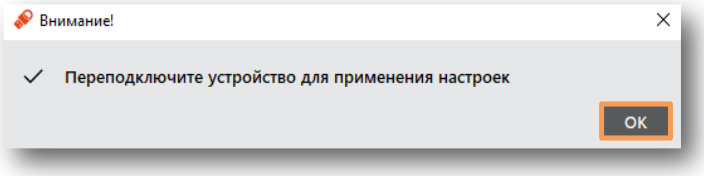


Рисунок 46 — Окно [Внимание!]

5. Переподключите USB-токен.

Режим биометрической идентификации будет изменен.

6.8.6 Сброс к заводским настройкам

Для сброса к заводским необходимо:

1. Подсоедините токен к USB-порту компьютера, при этом индикатор на токене должен загореться зеленым цветом, а также сработать вибромотор;
2. Перейти на вкладку [BIO manager], нажать кнопку <Сброс к заводским настройкам> (Рисунок 47);

В процессе сброса к заводским настройкам все данные из памяти USB -токена удаляются

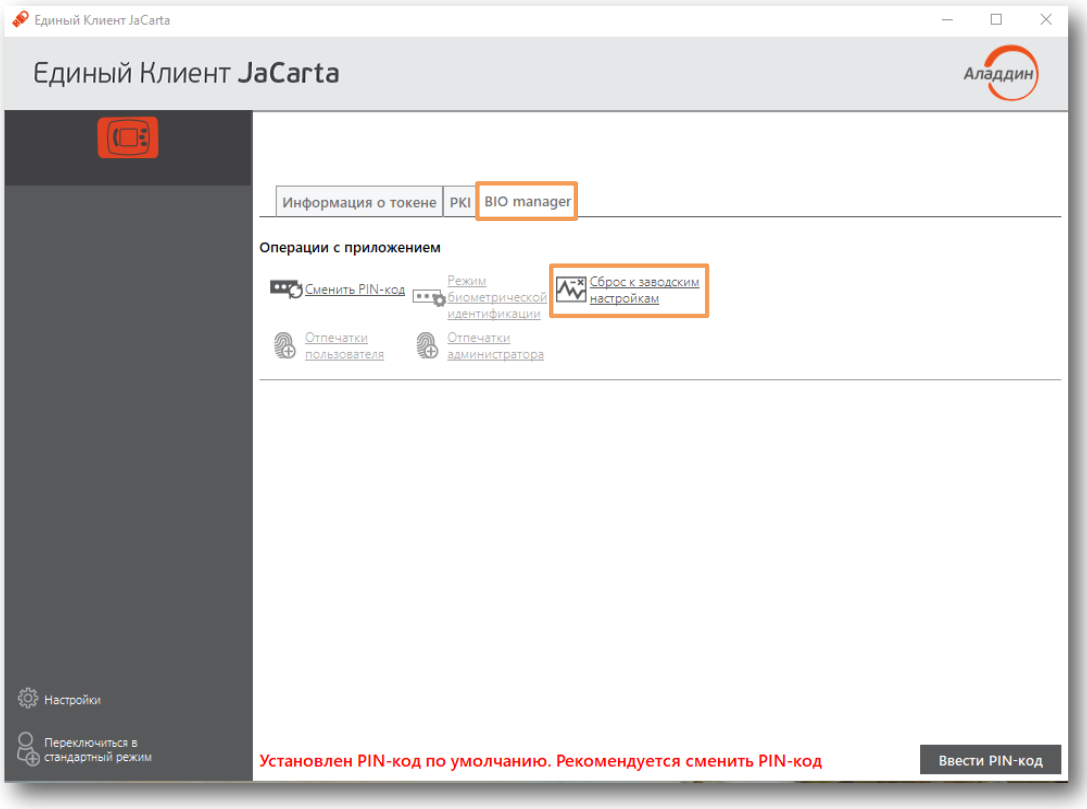


Рисунок 47 — Окно Единого Клиента JaCarta. Вкладка [BIO manager]

3. В открывшемся окне [Сброс к заводским настройкам] ввести PIN-код сброса и поставить флажок в строке <Подтверждение сброса к заводским настройкам>. Нажать кнопку <OK> (Рисунок 48);

PIN-код сброса к заводским настройкам – 0801378717

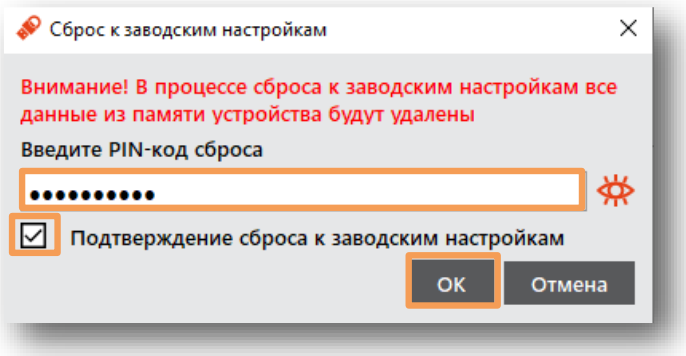


Рисунок 48 — Окно [Сброс к заводским настройкам]

4. После завершения процесса сброса к заводским настройкам появится окно с результатом его выполнения (Рисунок 49). Нажмите кнопку <OK>.

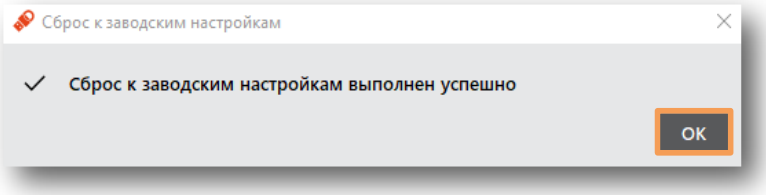


Рисунок 49 — Окно [Сброс к заводским настройкам] с результатом

> *Если в режиме администрирования (например, после того как выполнить идентификацию не удалось) сделать сброс к заводским настройкам, то для появления приложения PKI или ГОСТ необходимо переподключить USB-токен!*

> *После сброса к заводским настройкам необходимо выполнить форматирование приложения PKI или ГОСТ!*

6.9 JaCarta WebPass. Регистрация электронного ключа

Перед использованием электронного ключа JaCarta WebPass необходимо зарегистрировать его на сервере аутентификации (например, JaCarta Authentication Server) и/или в системах управления жизненным циклом электронных ключей (таких, как JaCarta Management System, Token Management System, SafeNet Authentication Manager).

> *Регистрация электронного ключа выполняется администратором сервера аутентификации или системы управления жизненным циклом электронных ключей*

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

Для регистрации электронного ключа:

1. Подключить электронный ключ JaCarta WebPass к компьютеру и запустить Единый Клиент JaCarta;
2. Сгенерировать файл с расширением *.xml / *.dat. Для этого необходимо инициализировать слот с типом "Одноразовый пароль", в результате чего будет создан файл с расширением *.xml / *.dat (подробнее см. документ *Единый Клиент JaCarta. Руководство пользователя для Windows*, п. "Инициализация слота типом "Одноразовый пароль");

3. Загрузить на сервер аутентификации или в систему управления жизненным циклом электронных ключей (далее – сервер/система) полученный файл с расширением *.xml / *.dat;
4. На сервере/в системе выполнить регистрацию токена с помощью экспорта файла с расширением *.xml/ *.dat согласно документации на сервер/систему;
5. После регистрации электронного ключа на сервере/в системе ключ может быть выдан пользователю для использования.

Примечание. После регистрации электронного ключа на сервере/в системе, в случае необходимости все слоты ключа могут быть инициализированы неоднократное количество раз. После повторной инициализации слотов проходить процедуру регистрации ключа на сервере/в системе не требуется.

6.10 Настройка программы через групповые политики с помощью административных шаблонов

Для запуска административного шаблона Единый Клиент JaCarta и отображения его настроек необходимо выполнить следующие действия:

1. Нажать на клавиатуре сочетание клавиш `Win+R`, в появившемся окне набрать `gpedit.msc` и нажать <OK> (Рисунок 50);

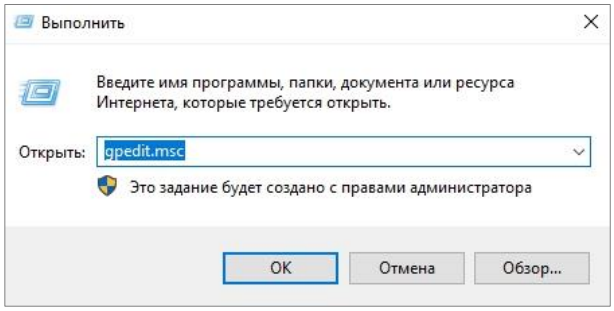


Рисунок 50 - Вызов окна командной строки

2. В открывшемся окне [Редактор локальной групповой политики] последовательно выбрать [Конфигурация компьютера], [Административные шаблоны], [Компоненты Windows], [Единый Клиент JaCarta] (Рисунок 51);

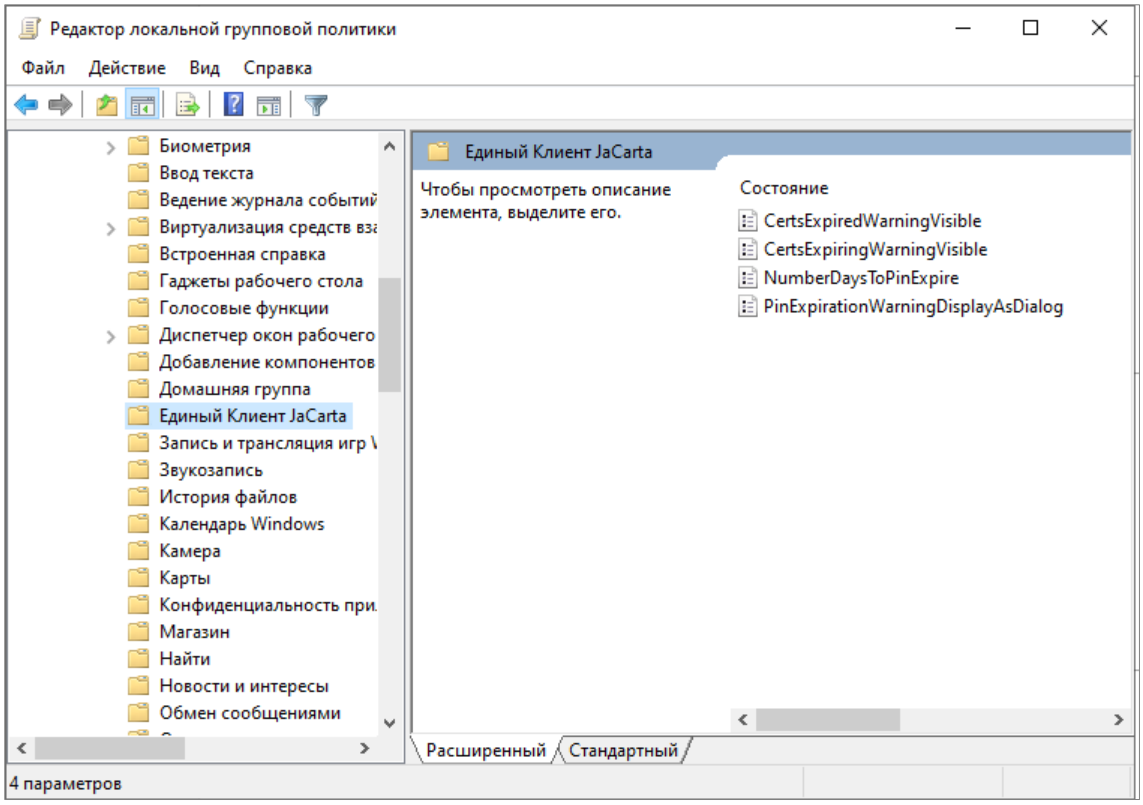


Рисунок 51 – Окно [Редактор локальной групповой политики]

Редактирование административного шаблона Единый Клиент JaCarta происходит путем изменения значения параметров политик, входящих в шаблон.

Описание настроек административного шаблона Единый Клиент JaCarta с указанием значений параметров политик по умолчанию приведены ниже (Таблица 15).

Таблица 15 – Настройки административного шаблона

Название параметра	**Описание**	**Допустимые значения**	**Значение по умолчанию до распространения групповых политик[6)]**	**Значение по умолчанию в шаблоне[7)]**
CertsExpiredWarningVisible (**Отображать предупреждение об истекшем сертификате**)	Определяет отображать или не отображать предупреждения об истекшем сроке действия сертификата	<Не задано> – будет использовано значение, заданное в разделе "Настройки" Единого Клиента JaCarta; <Включено> – пользователю будут отображаться предупреждения об истекшем сроке действия сертификата; <Отключено> – пользователю не будут отображаться предупреждения об истекшем сроке действия сертификата	Включено	Не задано

[6] Данные значение применяются сразу после установки Единого клиента JaCarta

[7] Применяются после распространения групповых политик, если в административный шаблон не было внесено никаких изменений

CertsExpiringWarningVisible (**Отображать предупреждение об истекающем сертификате**)	Определяет отображать или не отображать предупреждения об истекающем сроке действия сертификата	<Не задано> – будет использовано значение, заданное в разделе "Настройки" Единого Клиента JaCarta; <Включено> – пользователю будут отображаться предупреждения об истекающем сроке действия сертификата; <Отключено> – пользователю не будут отображаться предупреждения об истекающем сроке действия сертификата	Включено	Не задано
NumberDaysToPinExpire **(За сколько дней выводить уведомление об истечении времени жизни PIN-кода)**	Задаёт за сколько дней до истечения времени жизни PIN-кода выводить уведомление	<Не задано> – будет использовано значение, заданное в разделе "Настройки" Единого Клиента JaCarta; <Включено> – станет доступным для редактирования соответствующее поле, в котором нужно указать количество дней от 0 до 365, при значении равном 0 – не выводить уведомление; <Отключено> – настройка не применяется	14 дней	Не задано
PinExpirationWarningDisplayAsDialog (**Уведомление об истечении времени жизни PIN-кода в диалоговом окне**)	Определяет выводить уведомление об истечении времени жизни PIN-кода в диалоговом окне	<Не задано> – будет использовано значение, заданное в разделе "Настройки" Единого Клиента JaCarta; <Включено> – пользователю будет выводиться уведомление об истечении времени жизни PIN-кода в диалоговом окне; <Отключено> – пользователю будет выводиться уведомление об истечении времени жизни PIN-кода в трее	Отключено	Не задано

7. Форматирование электронных ключей

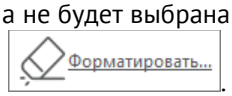
Во время форматирования задаются основные параметры работы электронных ключей. После процесса форматирования электронный ключ следует передать конечному пользователю.

> *Важно! При форматировании приложений электронных ключей будут удалены все данные, хранящиеся в памяти приложения (сертификаты, ключи).*

7.1 Форматирование приложения PKI с апплетом PRO

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

Для подготовки электронного ключа к работе:

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

. Будет открыто окно "Мастер форматирования приложения PKI" (Рисунок 52).

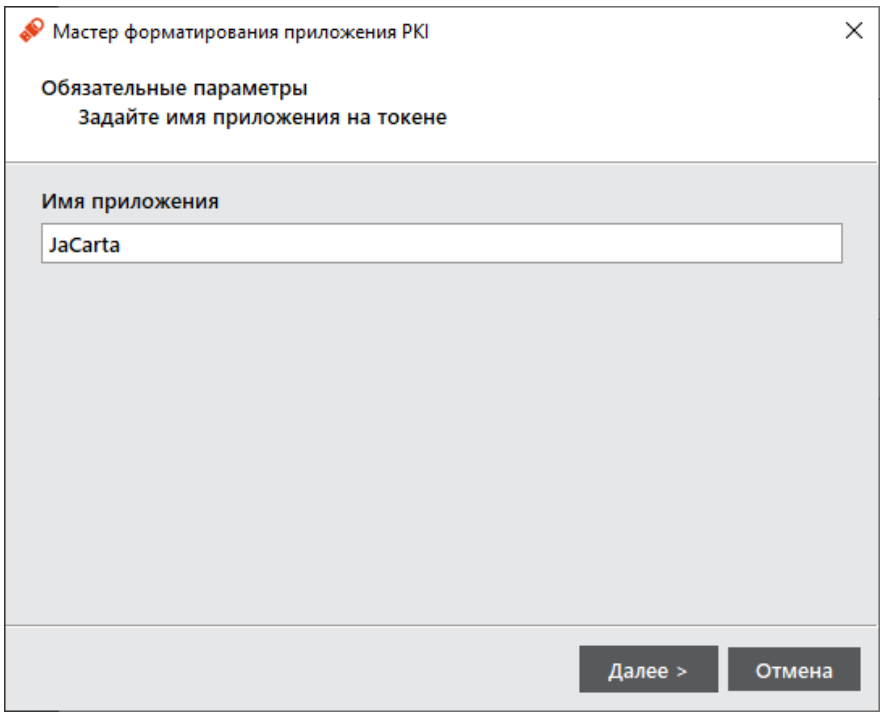


Рисунок 52 – Мастер форматирования приложения PKI. Обязательные параметры

5. В мастере форматирования приложения PKI нужно задать имя приложения.
6. Будет открыто окно настройки параметров PIN-кода.

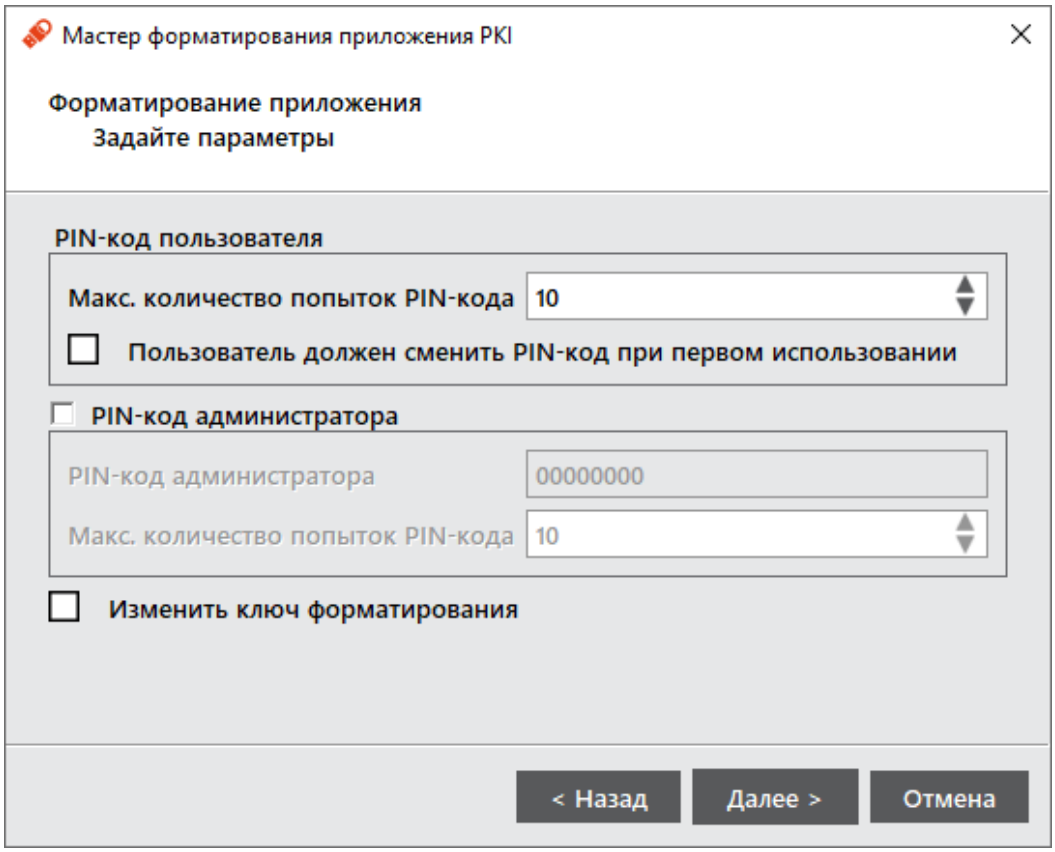


Рисунок 53 – Мастер форматирования приложения PKI. Форматирование приложения. Указание параметров

7. Произвести настройки параметров, руководствуясь описанием в таблице 16.

Таблица 16 – Форматирование приложения. Расширенные параметры форматирования токена

Секция	Поле	Описание
PIN-код пользователя	Макс. количество попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована
	Пользователь должен сменить PIN-код при первом использовании	Если флажок установлен, пользователь должен будет сменить PIN-код пользователя при первом использовании электронного ключа. В противном случае он не сможет продолжить работу с этим электронным ключом
PIN-код администратора	PIN-код администратора	Ввести значение PIN-кода администратора (поле активно при установленном флажке "PIN-код администратора")
	Макс. количество попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода администратора, после которого возможность использования PIN-кода администратора будет заблокирована

Секция	Поле	Описание
Изменить ключ форматирования		Если флажок установлен, то при нажатии кнопки "Далее" будет открыто окно для установки значения ключа форматирования

8. Если был установлен флажок "Изменить ключ форматирования", окно примет вид, приведенный на рисунке ниже (Рисунок 54).

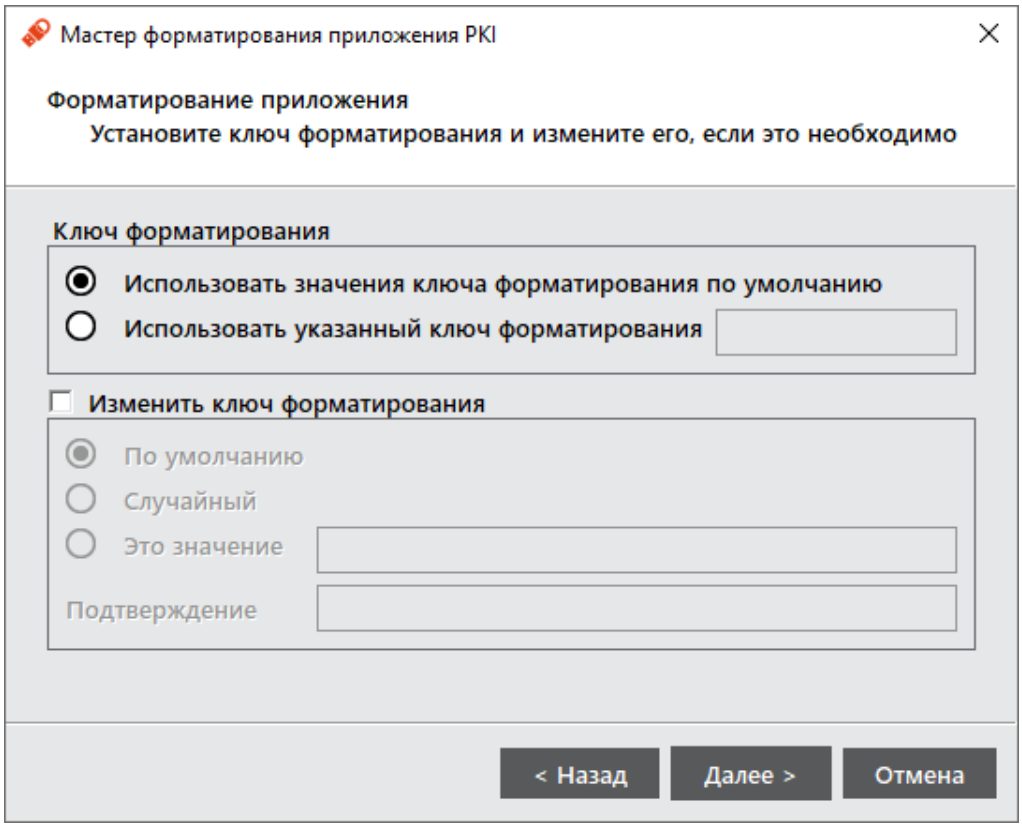


Рисунок 54 – Мастер форматирования приложения PKI. Установка ключа форматирования

9. Выполнить настройку. Описание дополнительных настроек на вкладке "Политика PIN-кода" приведено ниже (Таблица 17).

Таблица 17 – Мастер форматирования приложения PKI. Установка ключа форматирования

Секция	Поле	Описание
Ключ форматирования	Использовать значения ключа форматирования по умолчанию	Если опция выбрана, будет использоваться ключ форматирования по умолчанию
	Использовать указанный ключ форматирования	Если опция выбрана, возможен ввод выбранного ключа форматирования в соответствующее поле
Изменить ключ форматирования	По умолчанию	Опция становится доступна если выбран флажок "Изменить ключ форматирования". Устанавливает ключ форматирования по умолчанию
	Случайный	Изменение ключа форматирования на случайное значение для предотвращения

Секция	Поле	Описание
		последующего доступа к функции форматирования электронного ключа
	Это значение	Указывается новый ключ форматирования
	Подтверждение	Подтверждение нового ключа форматирования

10. Нажать кнопку "Далее". Откроется окно настройки качества PIN-кода (Рисунок 55). При установке в текущем окне флажка "Включить расширенные настройки качества PIN-кода", при нажатии кнопки "Далее" будет открыто окно установки расширенных настроек качества PIN-кода (Рисунок 56).

Настройки на данной вкладке относятся только к PIN-коду пользователя.

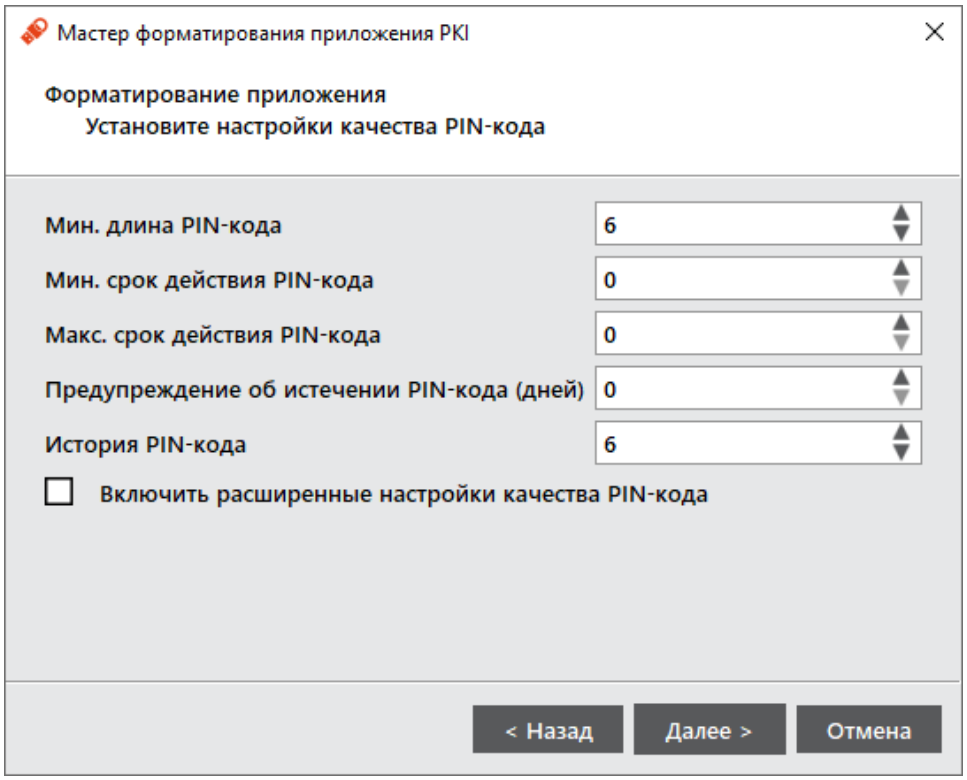


Рисунок 55 – Форматирование приложения PKI. Настройки качества PIN-кода

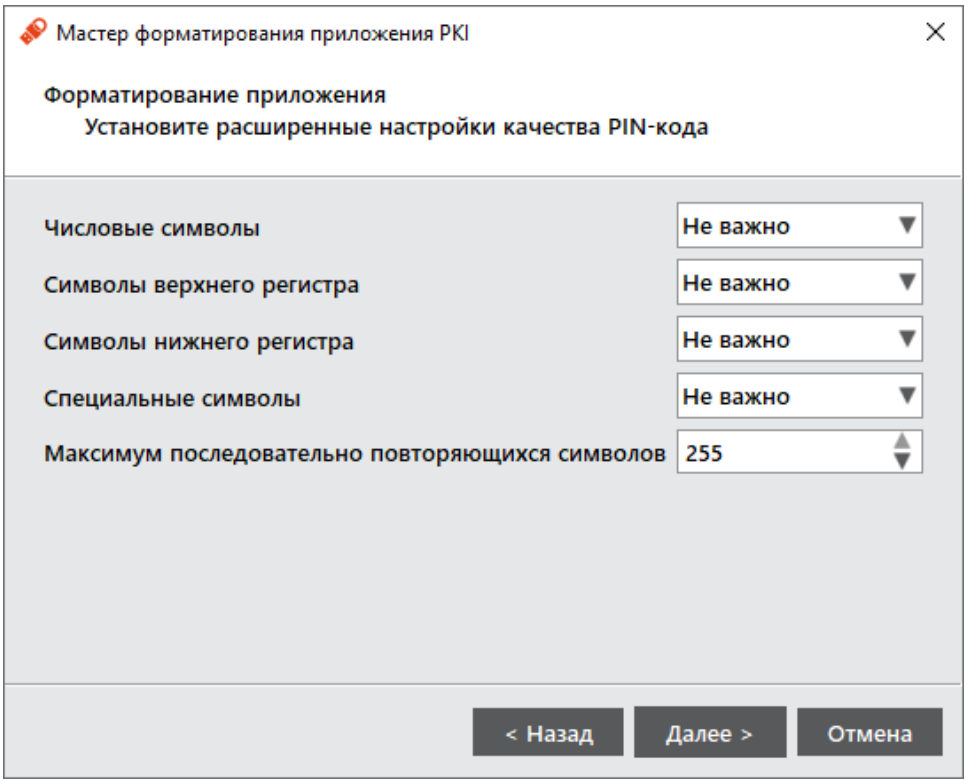


Рисунок 56 - Расширенные параметры форматирования токена. Расширенные настройки качества PIN-кода

11. Выполнить настройку. Описание дополнительных настроек на вкладке "Политика PIN-кода" приведено таблице 18.

Таблица 18 –Расширенные параметры форматирования токена. Политика PIN-кода

Секция	Поле	Описание
Базовые политики PIN-кода пользователя	Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде
	Мин. срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
	Макс. срок действия PIN-кода	Максимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
	Предупреждение об истечении PIN-кода (дней)	За сколько дней до окончания срока действия PIN-кода пользователя автоматически будет отправлено соответствующее уведомление
	История PIN-кода	Число использовавшихся ранее PIN-кодов пользователя, которые нельзя использовать при назначении нового PIN-кода пользователя. Например, если установлено значение "3", невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх ранее использованных
Включить расширенные настройка качества PIN-кода		Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя
	Числовые символы	Выпадающий список содержит варианты использования цифр в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
	Символы верхнего регистра	Выпадающий список содержит варианты использования алфавитных символов верхнего регистра в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
	Символы нижнего регистра	Выпадающий список содержит варианты использования алфавитных символов нижнего регистра в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
	Специальные символы	Выпадающий список содержит варианты использования специальных символов в PIN-коде пользователя: • Не важно • Запрещено • Обязательно
	Максимум последовательно повторяющихся символов	Использование идущих подряд одинаковых символов. Список содержит поле с возможностью выбора значения из диапазона от 0 до 255

12. Нажать кнопку "Далее". Будет открыто окно для выбора нового PIN-кода пользователя (Рисунок 57).

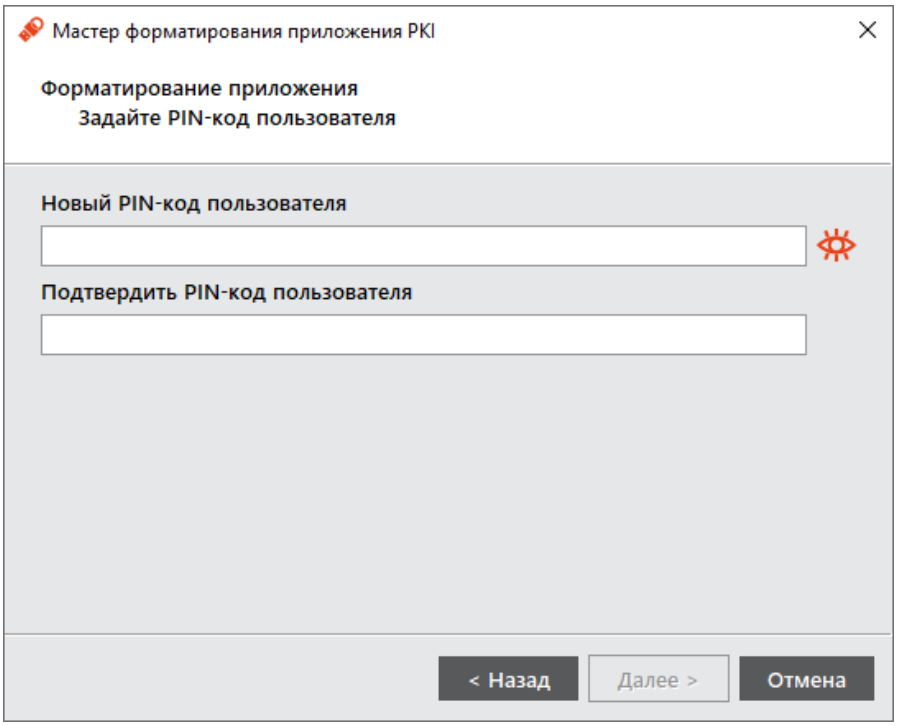


Рисунок 57 – Форматирование приложения PKI. Указание PIN-кода пользователя

13. Необходимо указать новый PIN-код пользователя, подтвердить его повторным вводом и нажать кнопку "Далее". Будет открыто окно подтверждения установленных в процессе форматирования настроек.
14. Нажать кнопку "Подтвердить". Начнётся процесс форматирования. При успешном процессе форматирования отобразится соответствующее сообщение – нажмите "Завершить" для закрытия мастера форматирования.

7.2 Форматирование приложения PKI с апплетом Laser

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

7.2.1 Настройки форматирования

Для подготовки электронного ключа к работе необходимо выполнить следующие действия.

1. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
2. Подсоединить электронный ключ к компьютеру, выбрать его в левой панели интерфейса ПО "Единый Клиент JaCarta" и в центральной части окна выберите вкладку "PKI".
3. Нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения PKI". Выбрать режим "Расширенный" (см. Рисунок 58).

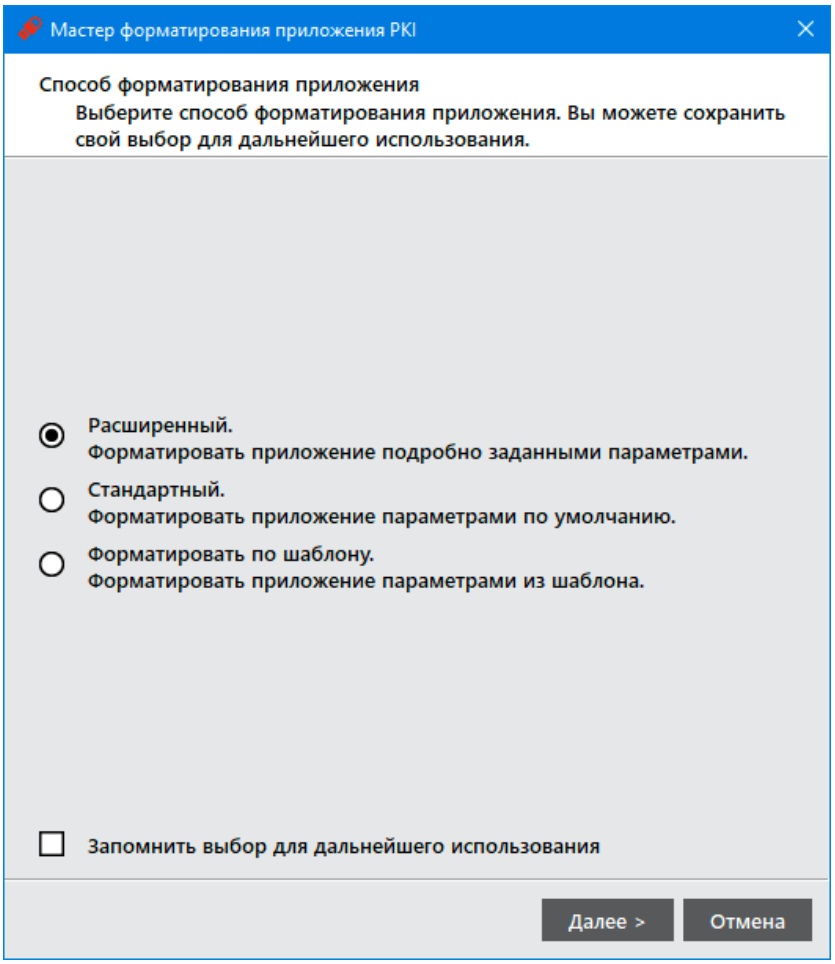


Рисунок 58 - Мастер форматирование приложения PKI. Выбор режима форматирования

4. Выполнить настройку (см. Рисунок 59). Описание параметров настройки качества PIN-кода администратора приведено в таблице 19.

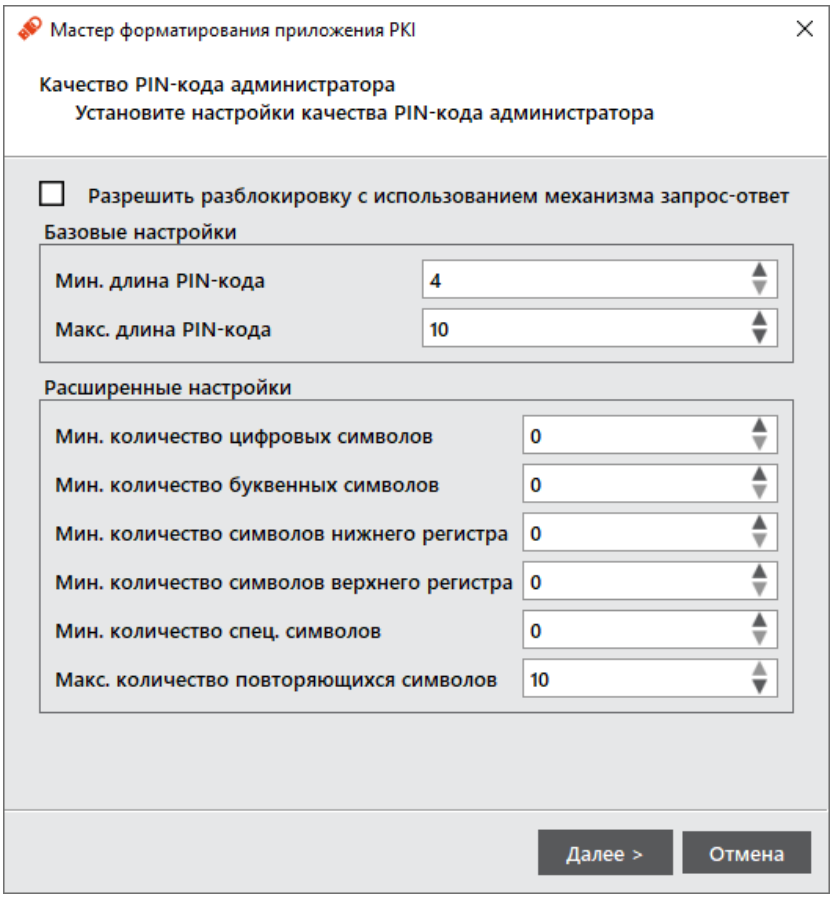


Рисунок 59 – Мастер форматирование приложения PKI. Настройка качества PIN-кода администратора

Таблица 19 – Параметры настройки качества PIN-кода администратора

Секция	Настройка	Описание
Разрешить разблокировку с использованием механизма запрос-ответ		При установке флажка после форматирования появляется возможность разблокировать электронный ключ в удалённом режиме, используя механизм "запрос-ответ". Для этого также в поле PIN-код администратора необходимо задать значение ключа 3DES, который будет выполнять функцию PIN-кода администратора
Базовые настройки	Мин. длина PIN-кода	Минимальное число символов в PIN-коде
	Макс. длина PIN-кода	Максимальное число символов в PIN-коде
Расширенные настройки	Мин. количество цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Мин. количество буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде
	Мин. количество символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
	Мин. количество символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде

Секция	Настройка	Описание
	Мин. количество спец. символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
	Макс. количество повторяющихся символов	Определяет число повторяющихся символов в любом месте PIN-кода

5. Нажмите "Далее". Будет открыто окно для указания нового PIN-кода администратора (Рисунок 60).

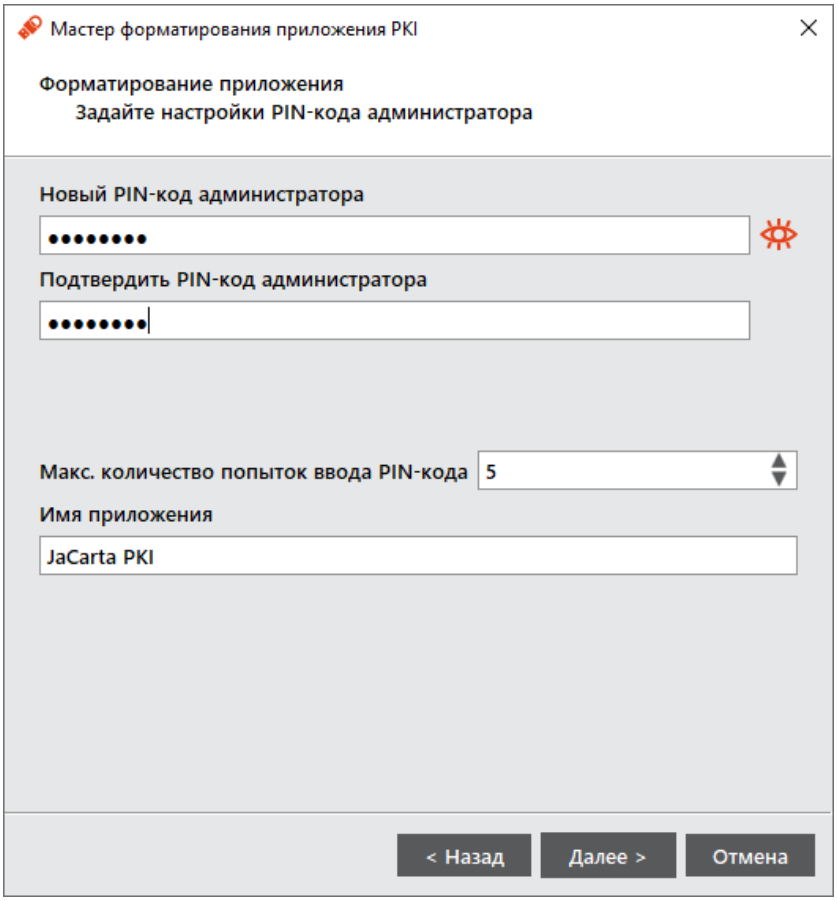


Рисунок 60 - Расширенные параметры форматирования токена

6. Выполнить настройку PIN-кода администратора согласно описанию параметров настройки PIN-кода, приведенному в таблице 20.

Таблица 20 – Параметры настройки PIN-кода администратора

Поле	Описание
Новый PIN-код администратора	Ввести новый PIN-код администратора
Подтвердить PIN-код администратора	Ввести подтверждение нового PIN-кода администратора
Макс. количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора

Имя приложения	Поле для ввода названия электронного ключа (например, имени будущего владельца)

7. Нажать "Далее". Будет открыто окно настройки PIN-кода пользователя (Рисунок 61).

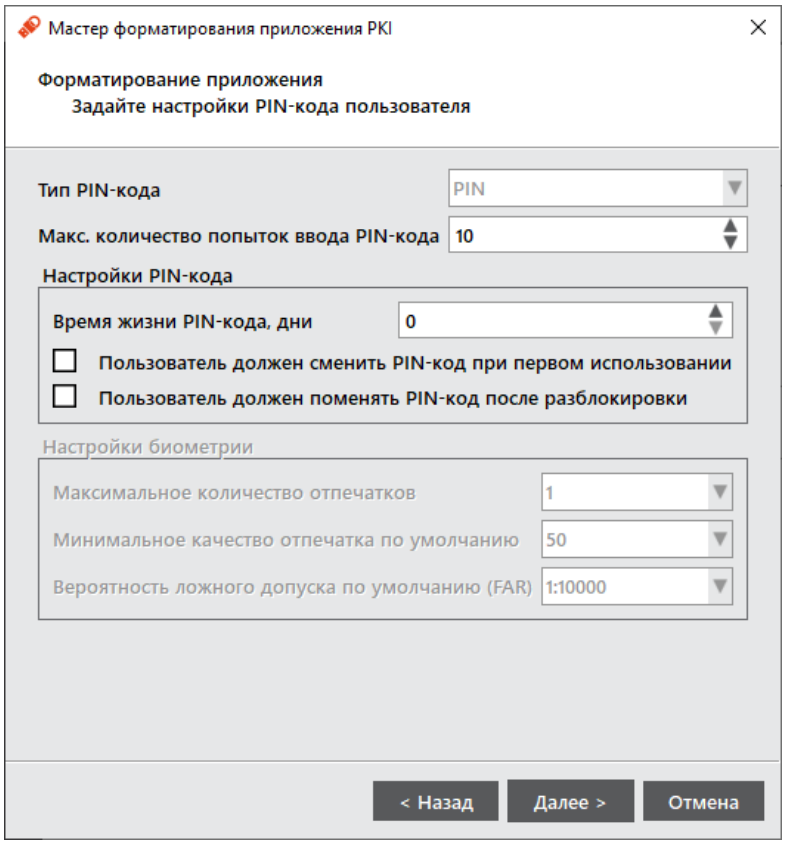


Рисунок 61 – Форматирование приложения. Указание PIN-кода администратора

8. Выполнить настройку PIN-кода пользователя согласно описанию параметров настройки PIN-кода, приведенному в таблице 21.

Таблица 21 – Параметры настройки PIN-кода пользователя

Секция	Настройка	Описание
	Тип PIN-кода	Возможны четыре варианта: • PIN – для аутентификации пользователь должен ввести PIN-код пользователя; • BIO – для аутентификации пользователь должен приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN или BIO – для аутентификации пользователь должен сделать одно из двух: ввести PIN-код пользователя или приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN и BIO – для аутентификации пользователь должен как ввести PIN-код пользователя, так и приложить палец к сканеру отпечатков

Секция	Настройка	Описание
		пальцев (только для электронных ключей с приложением PKI/BIO)
	Макс. количество попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя
Настройки PIN-кода	Время жизни PIN-кода, дни	Количество дней, спустя которое пользователь должен будет сменить PIN-код пользователя
	Пользователь должен сменить PIN-код при первом использовании	При установке флажка пользователю будет необходимо сменить PIN-код при первом использовании электронного ключа
	Пользователь должен поменять PIN-код после разблокировки	При установке флажка пользователю будет необходимо сменить PIN-код после разблокировки электронного ключа
Настройки биометрии	Максимальное количество отпечатков	Определяет максимальное количество отпечатков пальцев пользователя, которое можно сохранить в памяти электронного ключа JaCarta (от 1 до 10). В каждом конкретном случае пользователь сможет выбрать, какой отпечаток пальца использовать. Минимальное рекомендуемое значение: 2
	Минимальное качество отпечатка по умолчанию	Определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться
	Вероятность ложного допуска по умолчанию (FAR)	Определяет вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000

9. Нажать кнопку "Далее". Будет необходимо задать настройки качества PIN-кода пользователя. Окно настроек качества PIN-кода пользователя представлено на рисунке 62. Описание настроек качества PIN-кода пользователя приведено в таблице 22.

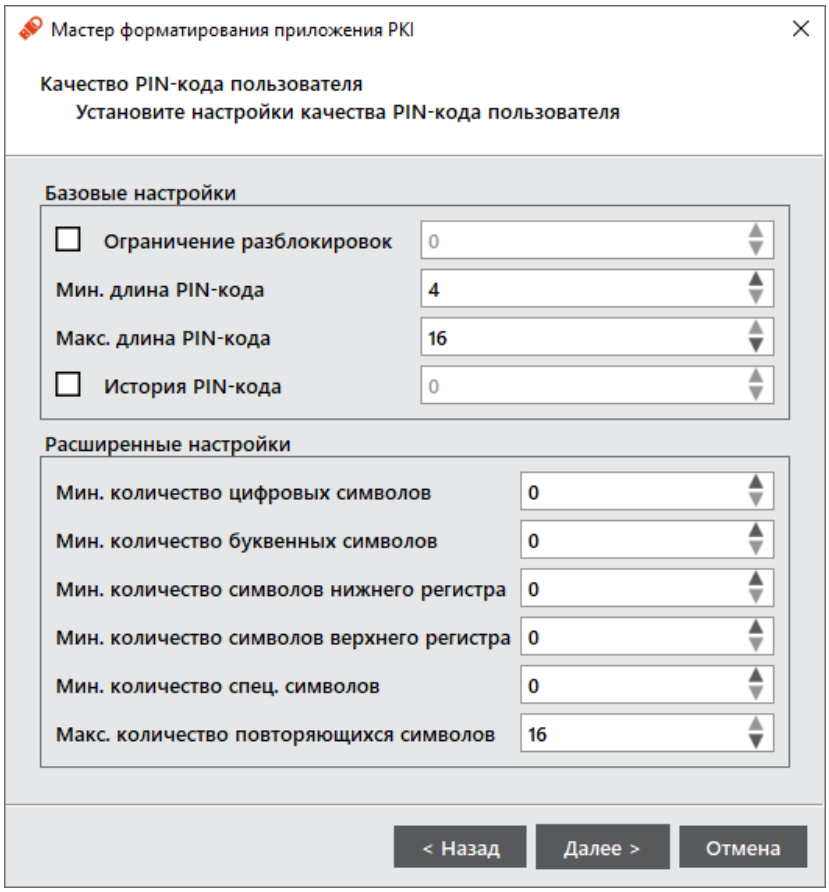


Рисунок 62 - Форматирование токена. Качество PIN-кода пользователя

При задании настроек к качеству PIN-кода рекомендуется следующее:

- использовать буквы только латинского алфавита (abc…z, ABC…Z), цифры (123…0) и спецсимволы (~!@#…);
- минимальная длина PIN-кода – 6 символов.

При задании PIN-кода недопустимо использование пробела и символов кириллицы

10. Нажмите "ОК" для сохранения настроек.

Таблица 22 - Форматирование токена. Окно "Качество PIN-кода пользователя"

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

Секция	Настройка	Описание
	История PIN-кода	Количество последних использованных PIN-кодов пользователя, значения которых нельзя задать для нового PIN-кода пользователя. Например, если установлено значение "3", невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх последних использованных. Допустимые значения от 1 до 10. Ввод значений в поле возможен после установки соответствующего флажка.
Расширенные настройки PIN-кода	Мин. количество цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Мин. количество буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде
	Мин. количество символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
	Мин. количество символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде
	Мин. количество специальных символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
	Макс. количество повторов символов	Определяет число повторяющихся символов в любом месте PIN-кода

11. На шаге "Форматирование приложения" отображаются все заданные на предыдущих шагах настройки в таблице "Отчет". При постановке галочки "Сохранение параметров форматирования в файл шаблона форматирования" все настройки из таблицы будут сохранены в файл (*.ftf) шаблона. Про работу с шаблоном см. в п. 7.2.2.

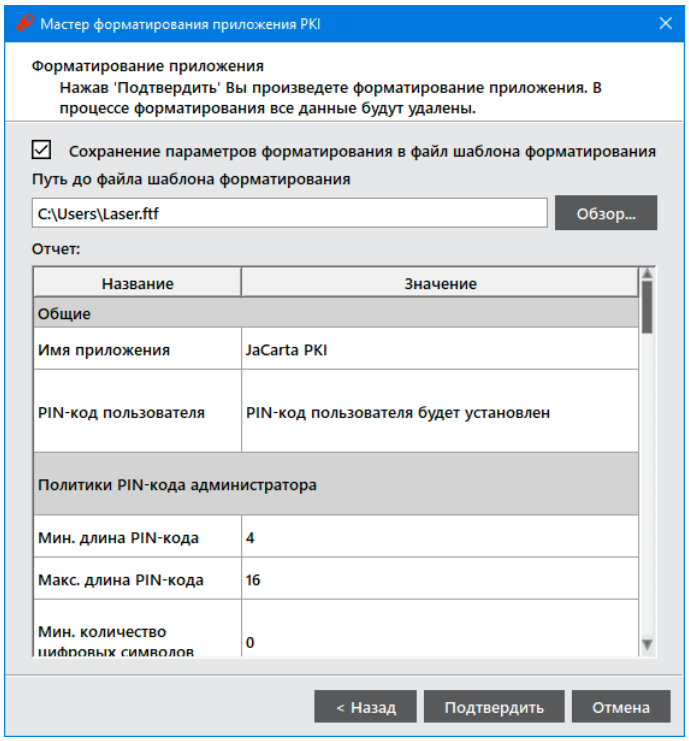


Рисунок 63 - Форматирование токена. Сохранение настроек форматирования в файл шаблона

12. Нажмите кнопку "Далее". В окне форматирования электронного ключа нажмите "Подтвердить". Будет осуществлено форматирование электронного ключа с установленными параметрами.

> *Если вы инициализируете электронный ключ с поддержкой биометрии следует руководствоваться п.7.2.3 Форматирование с биометрическими параметрами.*

13. В случае успешного форматирования токена отобразится соответствующее сообщение (Рисунок 64).

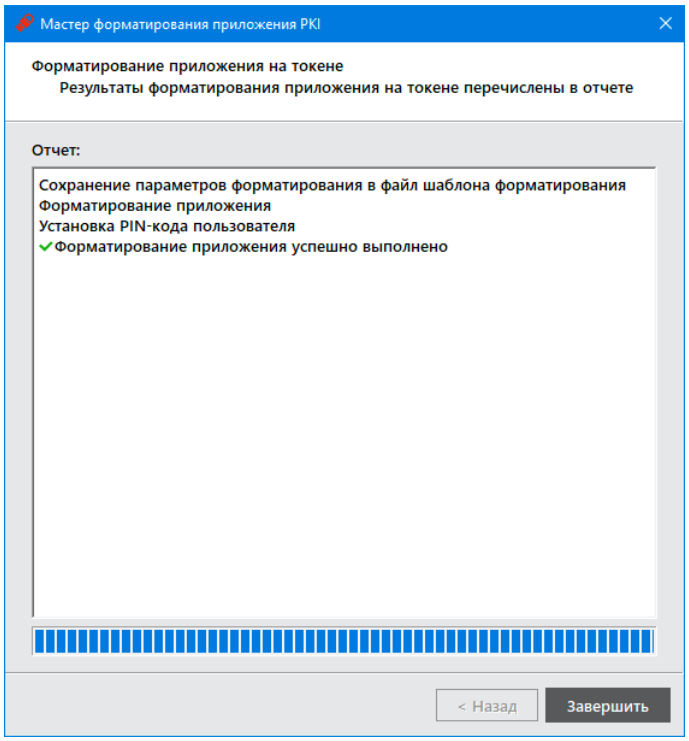


Рисунок 64 - Форматирование токена. Результат процесса форматирования

7.2.2 Форматирование по шаблону

Использование заранее настроенного шаблона при форматировании токена позволяет значительно ускорить сам процесс и сделать единообразным стиль выпущенных электронных ключей.

Для подготовки электронного ключа к форматированию необходим:

1. Нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения PKI". Выбрать режим "Форматировать по шаблону" (Рисунок 65). Нажать кнопку "Далее";

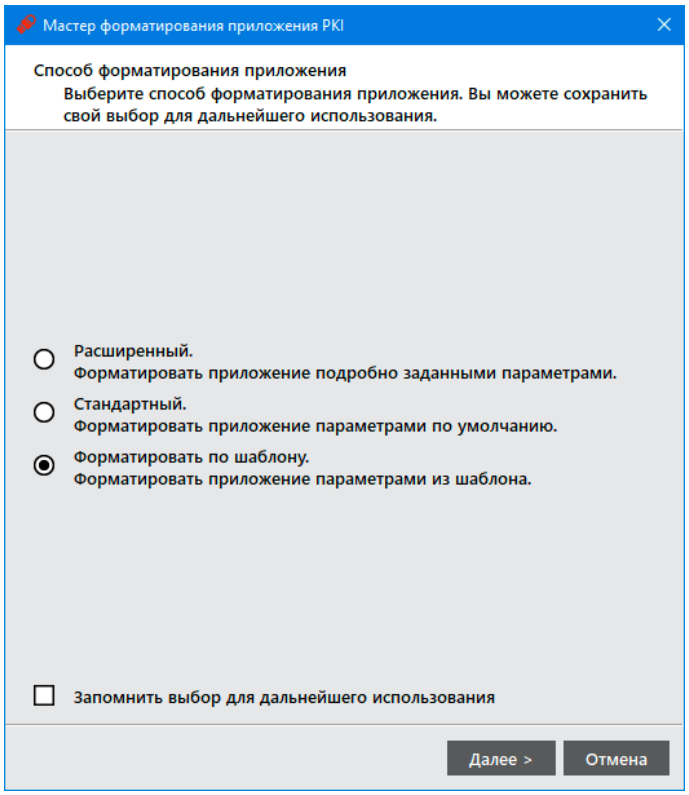


Рисунок 65 - Мастер форматирование приложения PKI. Форматирование по шаблону. Выбор режима

2. На следующем шаге (Рисунок 66) выбрать необходимый шаблон с помощью кнопки "Обзор", задать имя электронного ключа в поле "Имя приложения". Нажать "Далее";

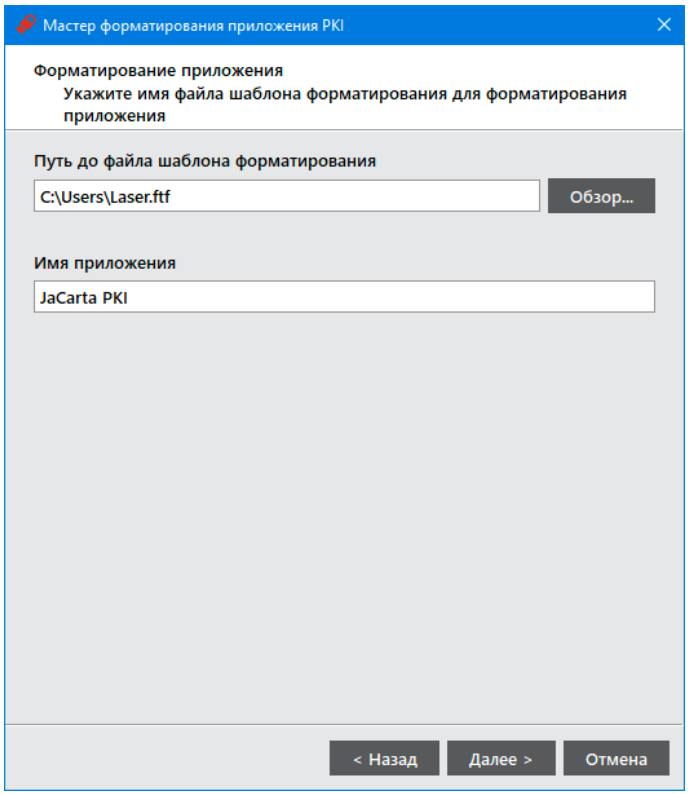


Рисунок 66 - Мастер форматирование приложения PKI. Форматирование по шаблону. Выбор шаблона

3. На шаге "Форматирование приложения" отображаются заданные настройки шаблона (Рисунок 67). Нажать кнопку "Подтвердить" для начала процесса форматирования;

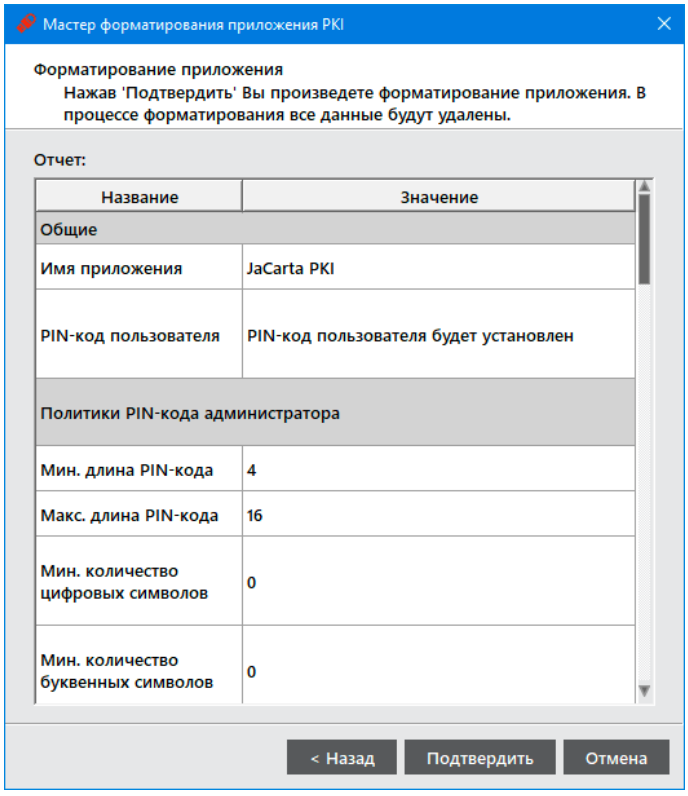


Рисунок 67 - Мастер форматирование приложения PKI. Форматирование по шаблону. Настройки

4. В случае успешного форматирования токена отобразится соответствующее сообщение (Рисунок 68).

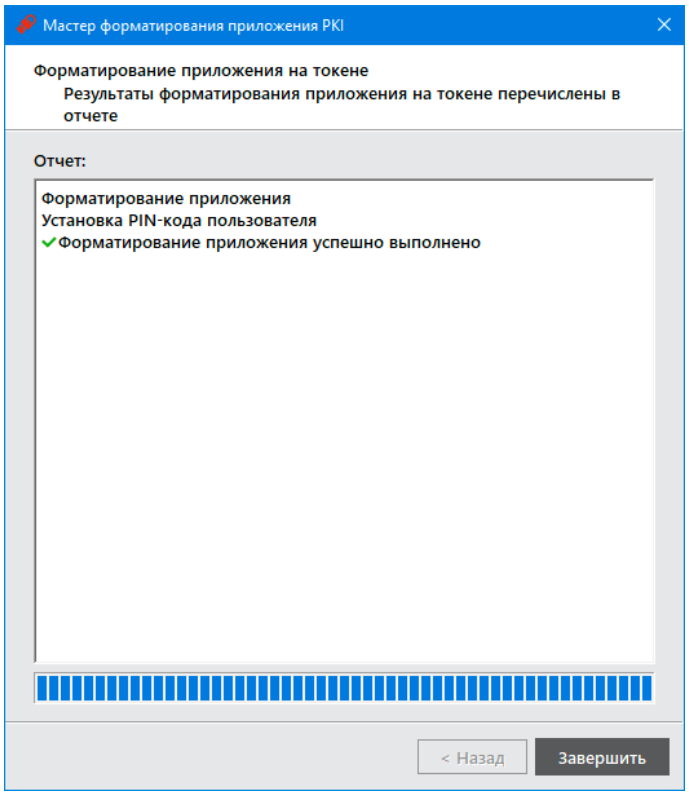


Рисунок 68 - Форматирование токена. Форматирование по шаблону. Отчет

7.2.3 Форматирование с биометрическими параметрами

Если вы форматируете электронный ключ с биометрическими настройками, через некоторое время после запуска процесса форматирования отобразится окно "Регистрация отпечатков".

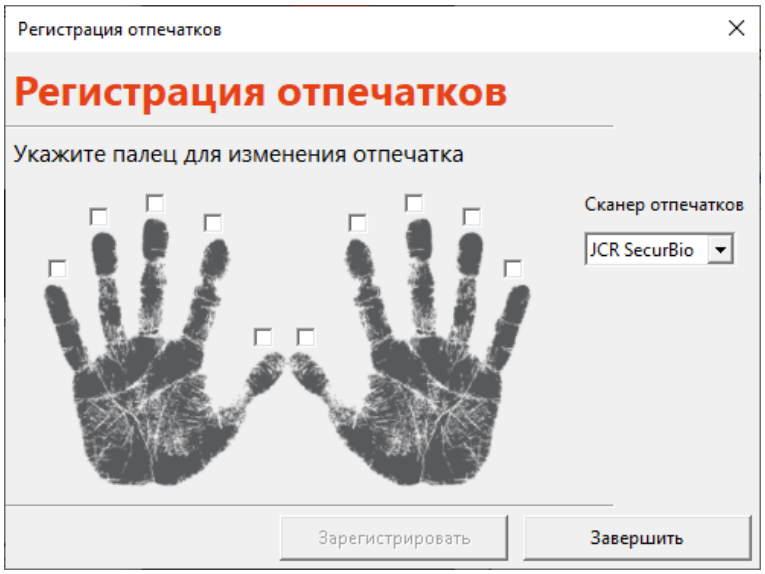


Рисунок 69 - Регистрация отпечатков

1. На схематическом изображении ладоней выберите палец, отпечаток которого будет отсканирован во время форматирования.

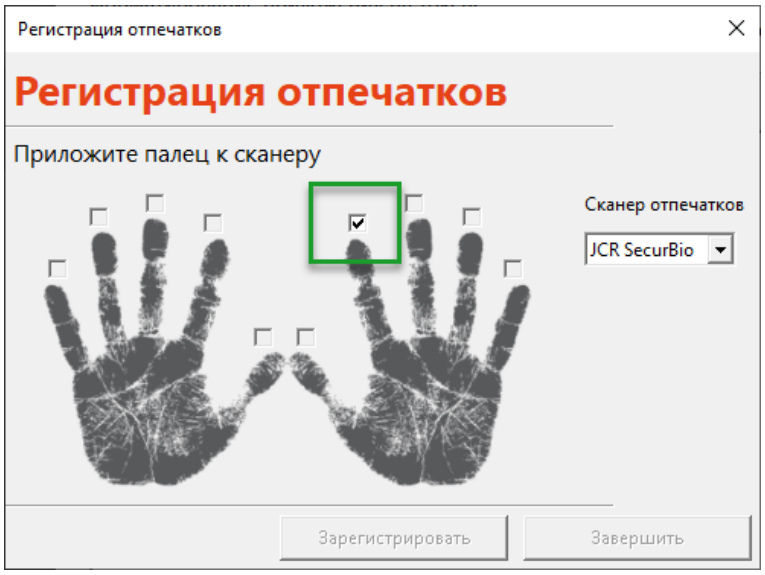


Рисунок 70 - Выбор пальца для сканирования

2. Будущий владелец электронного ключа должен приложить отмеченный палец к сканеру отпечатков пальцев. В зависимости от типа используемого смарт-карт ридера, после считывания отпечаток пальца отобразится в поле "Сканер отпечатков".
3. В окне регистрации отпечатков станет доступной для нажатия кнопка "Зарегистрировать". Нажмите кнопку "Зарегистрировать". При необходимости измените дополнительные параметры сканирования. Описание дополнительных параметров сканирования приведено в таблице 23.

Таблица 23 - Окно "Регистрация отпечатков". Описание настроек

Настройка	Описание
Сканер отпечатков	Используемый сканер отпечатков пальцев
Качество	С помощью выпадающего списка задать граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться
Вероятность ложного допуска	С помощью выпадающего списка задать вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000. Рекомендуемое значение: 1:10000

4. Будет отображено информационное окно с результатом регистрации отпечатка (см. рисунок 71). Для закрытия окна нажмите кнопку "ОК".

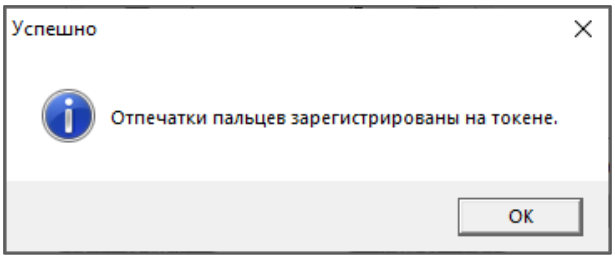


Рисунок 71 - Сообщение о регистрации отпечатка пальца

5. При успешном завершении форматирования отобразится соответствующее сообщение. Нажмите кнопку "Завершить" для закрытия окна форматирования.

В случае неоднократных затруднений при создании шаблона отпечатка пальца возможно переключение смарт-карт ридера в упрощенный режим работы. Подробнее см. пп. 6.7.

7.3 Форматирование приложения STORAGE

Для подготовки электронного ключа к работе:

1. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
2. Подсоединить нужный электронный ключ к компьютеру, выбрать его в левой панели и в центральной части окна выбрать вкладку "STORAGE".
3. Нажать кнопку "Форматировать". Будет открыто окно "Мастер форматирования приложения STORAGE".

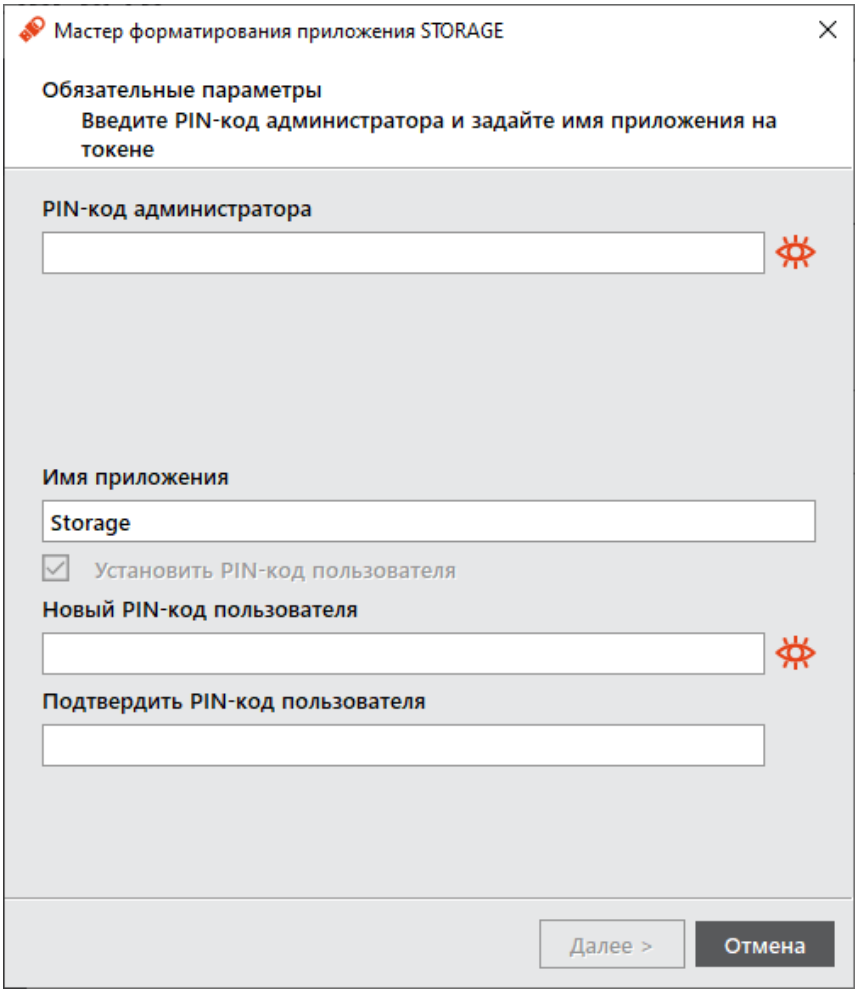


Рисунок 72 - Форматирование приложения

4. Выполнить настройку. Описание настроек форматирования электронного ключа приведено в таблице 24:

Таблица 24 - Форматирование приложения. Описание настроек

Настройка	Описание
PIN-код администратора	Поле для ввода текущего PIN-код администратора
Имя приложения	Поле для ввода названия электронного ключа (например, имени будущего владельца)
Установить PIN-код пользователя	Приложение STORAGE не может быть форматировано без PIN-кода пользователя, поэтому нельзя снять флажок
Новый PIN-код пользователя	Поле для ввода нового значения PIN-кода пользователя (поле активно, только если установлен флажок "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Поле для ввода подтверждения нового значения PIN-кода пользователя. (Поле активно, только если установлен флажок "Установить PIN-код пользователя")

5. Нажмите кнопку "Подтвердить" в окне подтверждения.
6. При успешном форматировании будет отображено соответствующее сообщение. Нажмите кнопку "Завершить" для закрытия окна форматирования.

7.4 Форматирование приложения ГОСТ с апплетом Криптотокен 2 ЭП

Для подготовки электронного ключа к работе:

1. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
2. Подсоединить нужный электронный ключ к компьютеру, выбрать его в левой панели и в центральной части окна перейти на вкладку "ГОСТ".
3. Нажать кнопку "Форматировать". Будет открыто окно "Форматирование приложения пользователем".

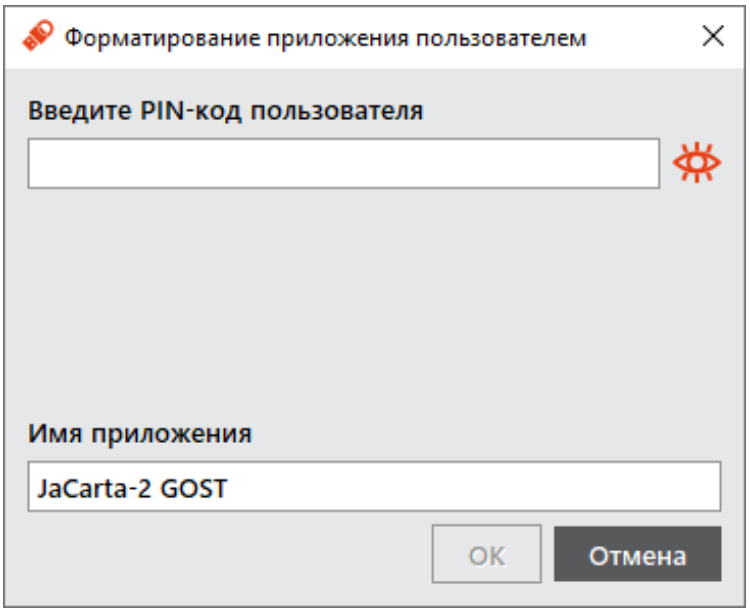


Рисунок 73 - Форматирование приложения пользователем

4. Заполнить поля "Имя приложения" и "Введите PIN-код пользователя", после чего нажмите кнопку "ОК".
5. В информационном окне о результатах форматирования нажать кнопку "ОК" для завершения процесса.

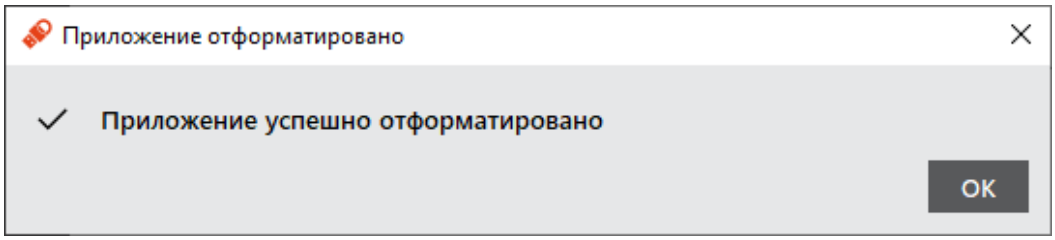


Рисунок 74 - Сообщение о результатах процесса форматирования

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

8.1 Установка (смена) PIN-кода пользователя администратором

Для некоторых приложений администратор может задать PIN-код пользователя, если он не был назначен во время форматирования. Также администратор может сменить текущий PIN-код пользователя.

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

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

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

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

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

Для смены PIN-кода пользователя администратором:

1. Подсоединить электронный ключ, на котором необходимо установить/сменить PIN-код пользователя. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
2. В левой панели выбрать нужный электронный ключ. В центральной части окна перейти на вкладку, соответствующую приложению, для которого необходимо назначить (сменить) PIN-код пользователя.
3. Нажать кнопку "Установить PIN-код пользователя". Будет открыто окно "Установить PIN-код пользователя":

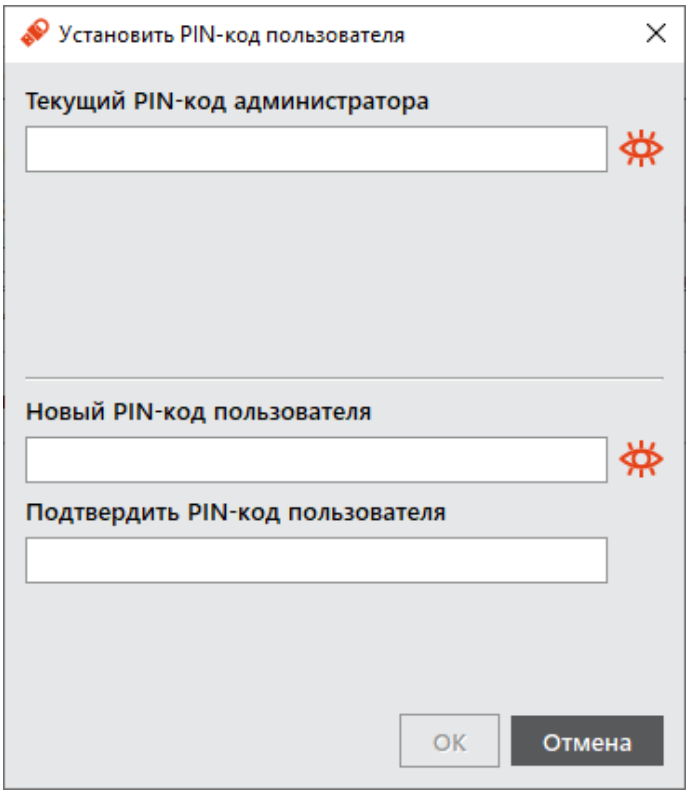


Рисунок 75 - Окно "Установить PIN-код пользователя"

4. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
5. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" указать соответственно новый PIN-код пользователя и подтвердить его повторным вводом.
6. Нажать кнопку "OK".
7. При успешной установке нового PIN-кода пользователя отобразится соответствующее сообщение, нажмите "OK" для его закрытия.

8.2 Разблокирование PIN-кода пользователя в присутствии администратора

Если пользователь превысил максимальное допустимое число последовательных неверных попыток ввода PIN-кода, то он блокируется. Процедура разблокировки PIN-кода пользователя различается в зависимости от приложения, установленного в память электронного ключа:

- PKI и PKI/BIO – после разблокировки администратор должен установить новый PIN-код пользователя.
- ГОСТ и STORAGE – разблокировка обнуляет счётчик неверных попыток доступа, значение PIN-кода пользователя остаётся прежним.

8.2.1 Приложение PKI и PKI/BIO

Для разблокирования PIN-кода пользователя:

1. Подсоединить электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
3. В левой панели ПО "Единый Клиент JaCarta" выбрать нужный электронный ключ и в центральной части перейти на вкладку "PKI".
4. Если PIN-код пользователя заблокирован кнопка "Разблокировать PIN-код" будет доступна для нажатия (см. рисунок 76). Иначе кнопка заблокирована.

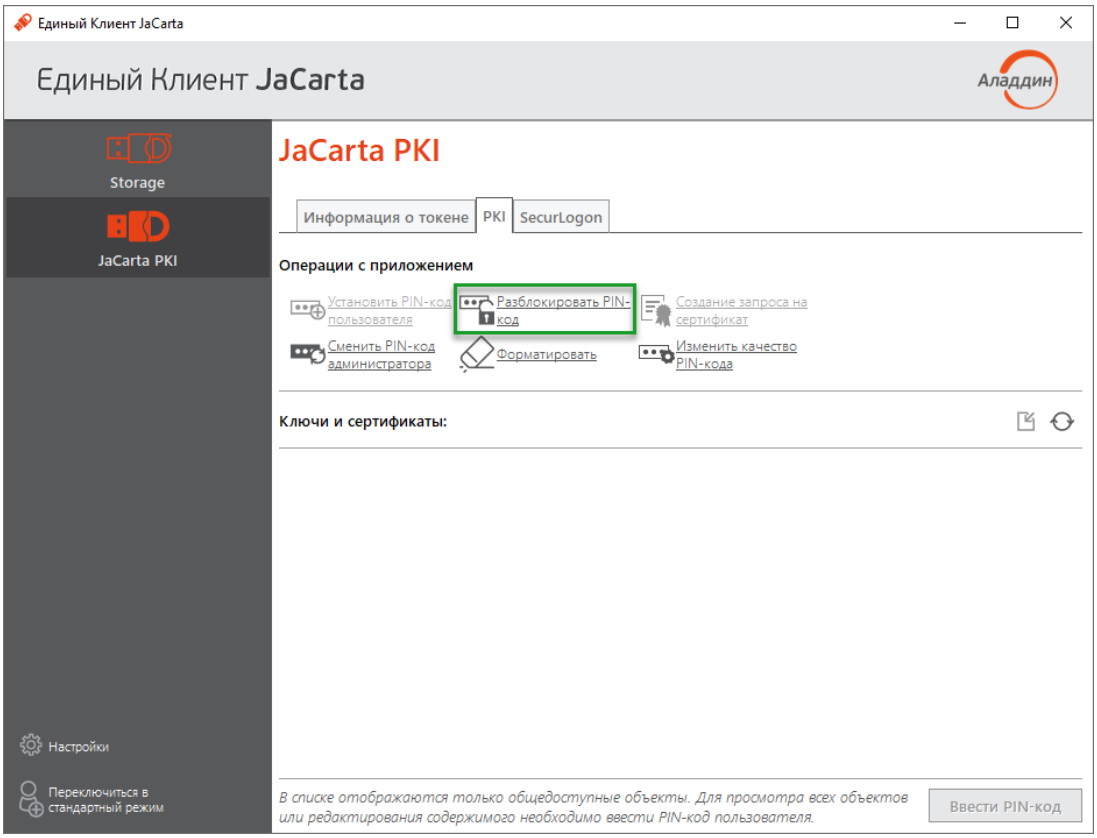


Рисунок 76 - Элемент управления "Разблокировать PIN-код"

5. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Разблокировать PIN-код":

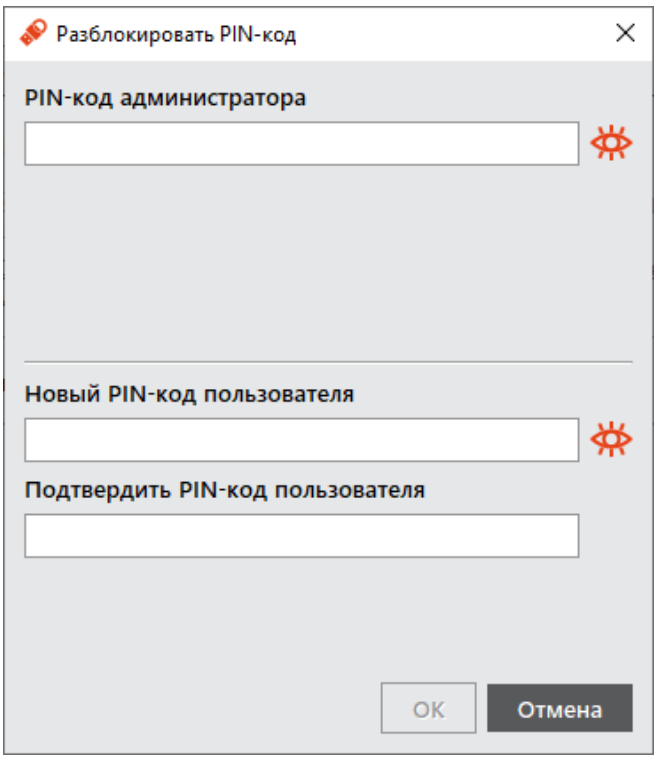


Рисунок 77 - Разблокировка PIN-кода пользователя

6. В поле "PIN-код администратора" ввести текущий PIN-код администратора.
7. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новый PIN-код пользователя и нажать кнопку "OK".

8. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение – нажать кнопку "OK", чтобы закрыть его.

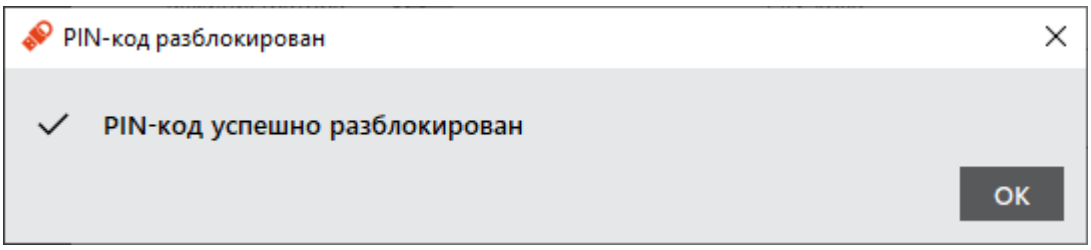


Рисунок 78 - Сообщение об успешной разблокировке PIN-кода пользователя

8.2.2 Приложение STORAGE

Для разблокирования PIN-кода пользователя:

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

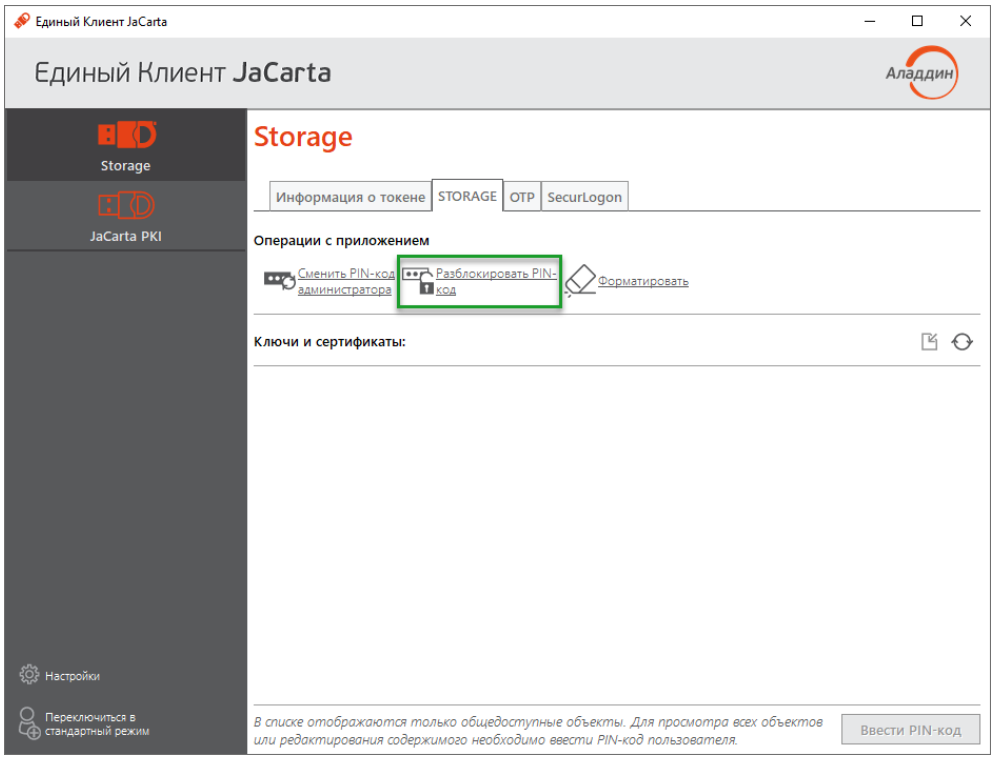


Рисунок 79 - Элемент управления "Разблокировать PIN-код"

5. После нажатия на кнопку "Разблокировать PIN-код" будет открыто окно "Разблокировать PIN-код".

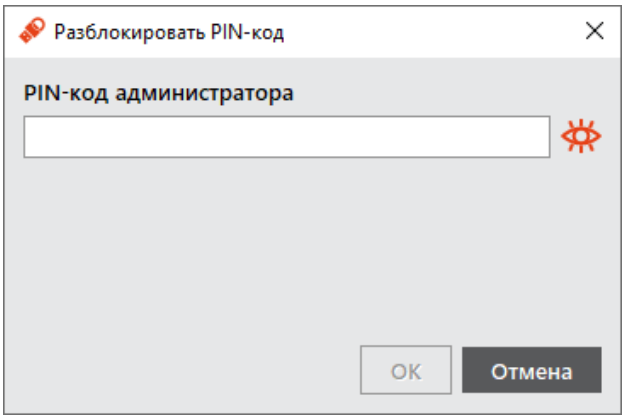


Рисунок 80 - Окно "Разблокировать PIN-код"

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

При разблокировке PIN-кода пользователя сбрасывается счётчик неверных попыток ввода PIN-кода пользователя, при этом само значение PIN-кода пользователя остаётся неизменным. При необходимости изменить значение PIN-кода пользователя воспользуйтесь процедурой форматирования. В этом случае все данные с ключа будут удалены.

7. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение. Нажать кнопку "OK", чтобы закрыть его.

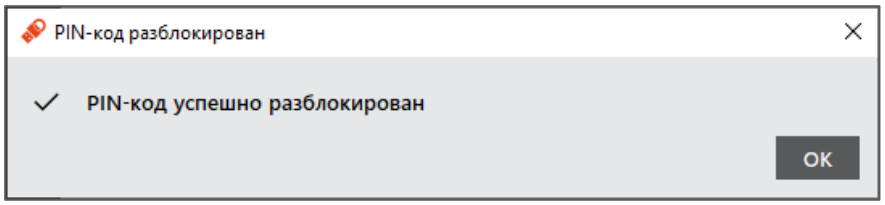


Рисунок 81 - Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.2.3 Приложение ГОСТ с апплетом Криптотокен 2 ЭП

Для того чтобы разблокировать PIN-код пользователя, электронный ключ с апплетом Криптотокен 2 ЭП должен быть проинициализирован с заданным PUK-кодом.

Для разблокирования PIN-кода пользователя:

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

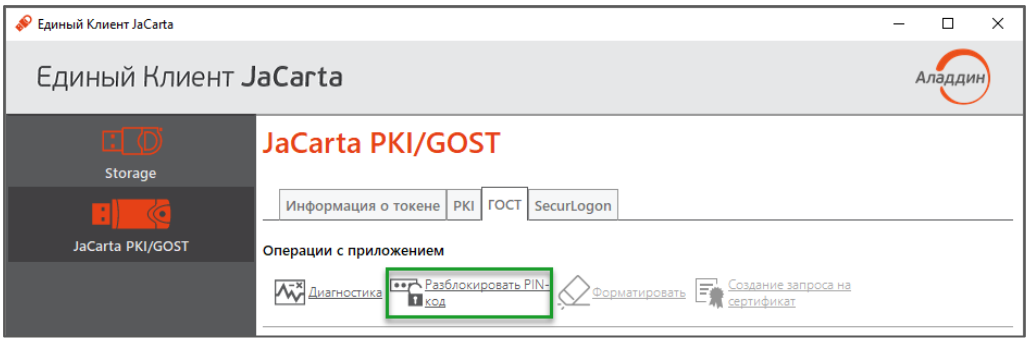


Рисунок 82 - Элемент управления "Разблокировать PIN-код"

5. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокировки PIN-кода".

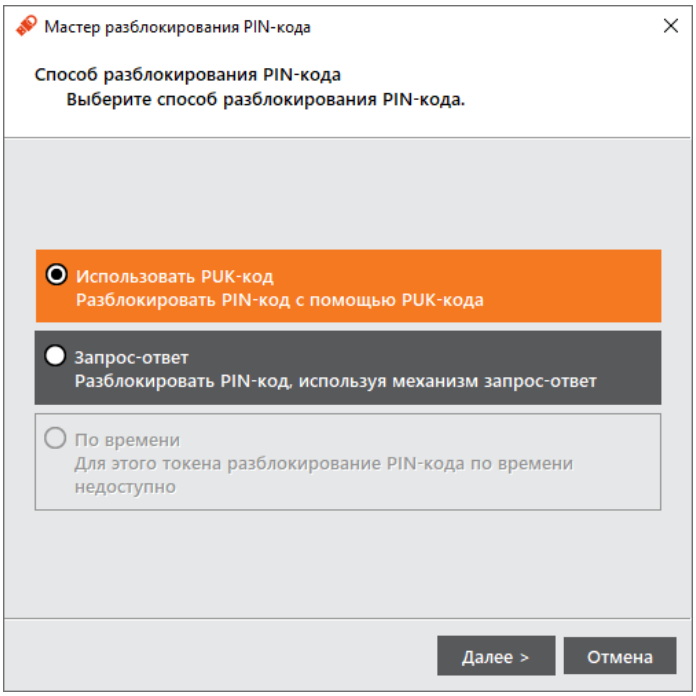


Рисунок 83 - Окно "Разблокировка PIN-кода пользователя"

6. Выбрать пункт "Использовать PUK-код" и нажать кнопку "Далее".
7. В поле "PUK-код" ввести текущий PUK-код, после чего нажать кнопку "Далее".
8. При успешной разблокировке отобразится соответствующее сообщение. Для его закрытия нажать кнопку "Завершить".

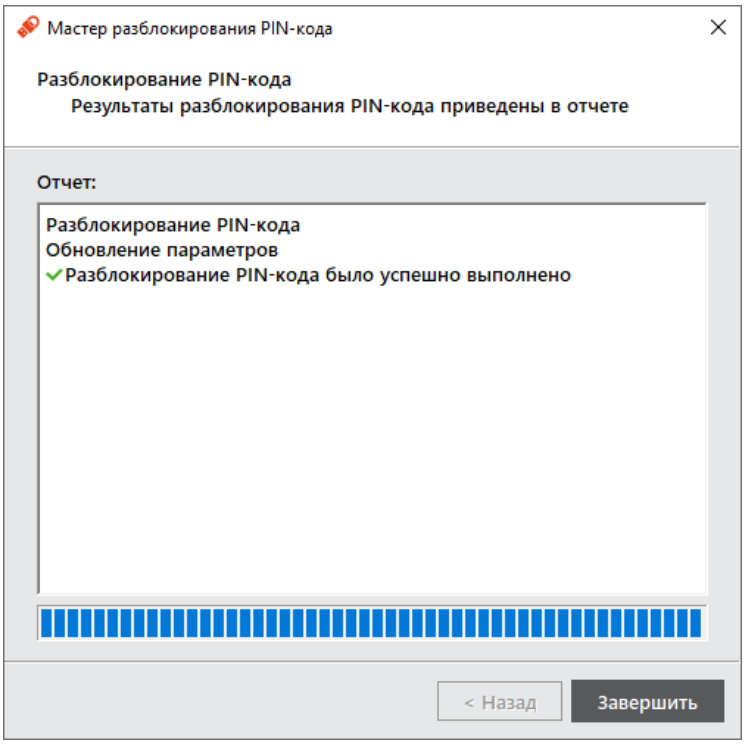


Рисунок 84 - Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

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

8.3.1 Приложение PKI и PKI/BIO

В результате разблокирования PIN-кода пользователя электронного ключа с приложением PKI или PKI/BIO выполняется назначение нового PIN-кода пользователя и сброс до нуля счетчика попыток ввода неверного PIN-кода пользователя.

Разблокировка PIN-кода пользователя электронного ключа с приложением PKI или PKI/BIO в удалённом режиме возможна при выполнении следующих условий:

- в организации должна быть установлена система учёта и управления аппаратных средств аутентификации; в настоящем документе для примера будет использоваться система JaCarta Management System (JMS);
- электронный ключ, подлежащий разблокированию, должен быть зарегистрирован в системе учёта и управления аппаратных средств аутентификации до момента его блокировки;
- для приложения PKI с апплетом PRO электронный ключ должен быть отформатирован с заданным PIN-кодом администратора (см. п. 7.1 Форматирование приложения PKI с апплетом PRO);
- для приложения PKI и PKI/BIO с апплетом Laser электронный ключ должен быть отформатирован с возможностью разблокировки по механизму "запрос-ответ" и в качестве PIN-кода администратора задать ключ 3DES (см. п. 7.2 Форматирование приложения PKI с апплетом Laser).

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

Для разблокирования PIN-кода пользователя в удалённом режиме:

1. Проинструктировать пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом к компьютеру и запустить ПО "Единый Клиент JaCarta". Окно ПО "Единый Клиент JaCarta" у пользователя в стандартном режиме будет выглядеть как на рисунке 85.

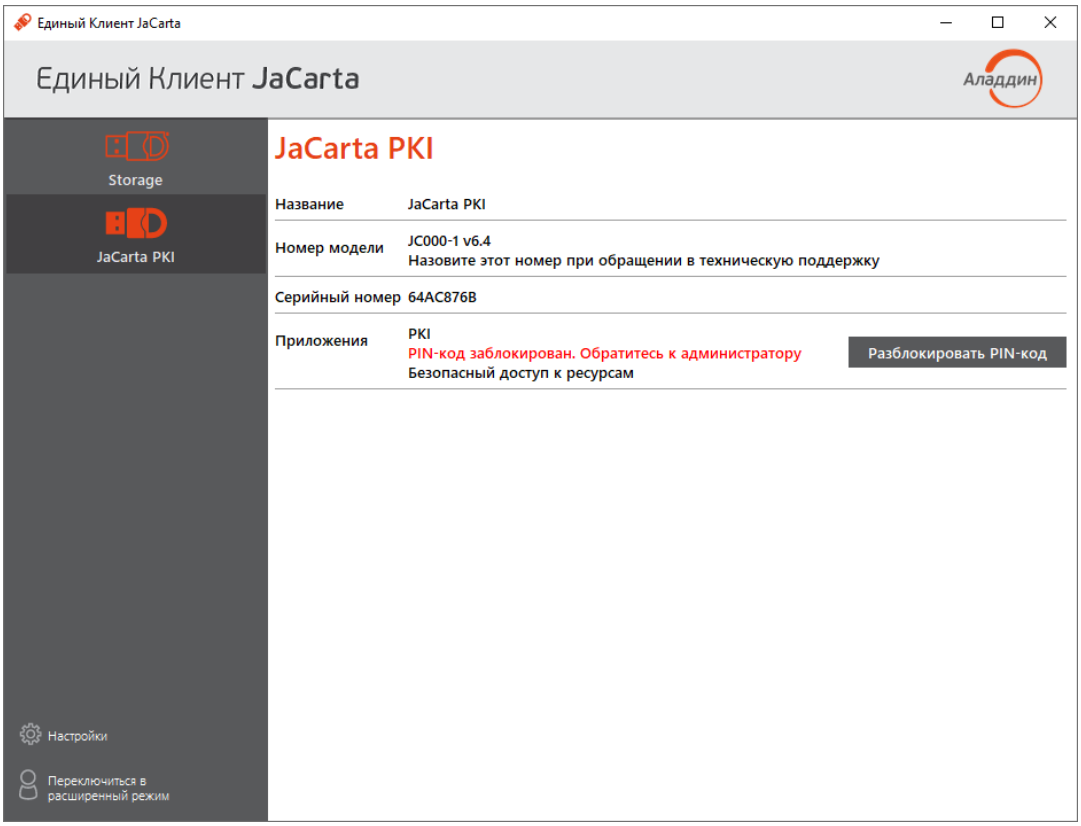


Рисунок 85 –Отображение заблокированного PIN-кода у пользователя

2. Пользователь должен нажать кнопку "Разблокировать PIN-код". На экране пользователя будет открыто окно "Разблокировать PIN-код" (см. рисунок 86). Нужно выбрать способ разблокирования "Запрос-ответ" и нажать кнопку "Далее".

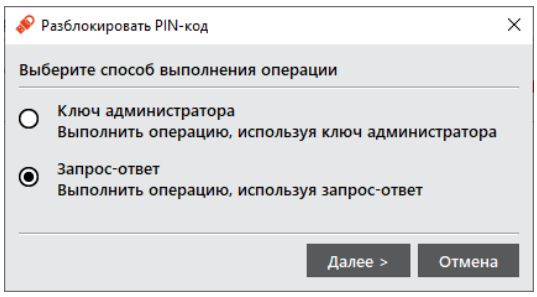


Рисунок 86 - Разблокировка PIN-кода пользователя

3. На экране пользователя будет открыто окно "Разблокировать PIN-код" (см. рисунок 87). В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" пользователь должен ввести новое значение PIN-кода пользователя и его подтверждение соответственно.

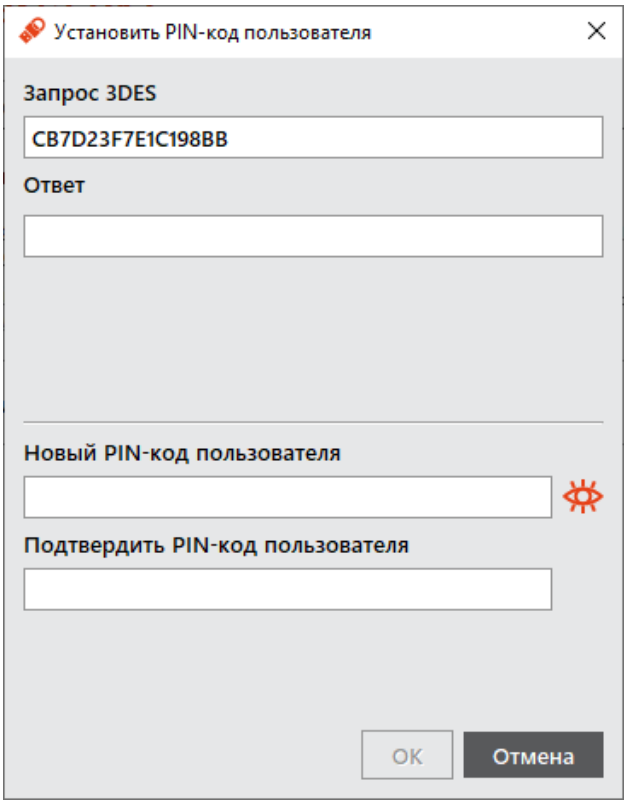


Рисунок 87 - Окно "Запрос/Ответ: JaCarta PKI"

4. Пользователь должен продиктовать администратору код запроса, сгенерированный в поле "Запрос 3DES".
5. Администратор, используя интерфейс Консоли управления JMS, должен открыть окно удалённой разблокировки. Для этого необходимо нажать на кнопку "Удаленная разблокировка".

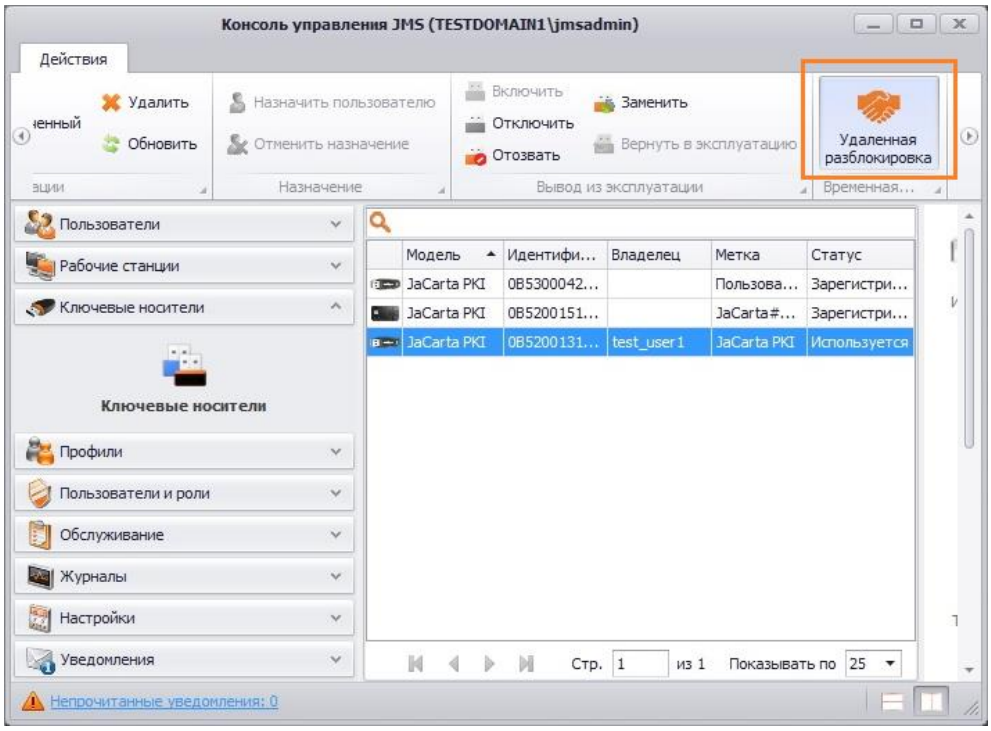


Рисунок 88 - Консоль управления JMS. Удаленная разблокировка

6. Будет открыто окно "Удаленная разблокировка" (см. рисунок 89).

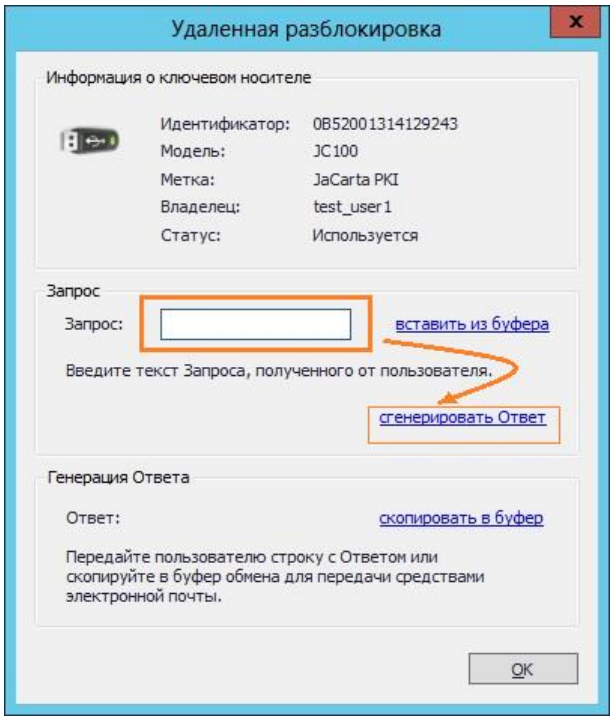


Рисунок 89 - Консоль управления JMS. Окно "Удаленная разблокировка"

7. Администратор в поле "Запрос" должен ввести код запроса, который сообщил пользователь. После должен нажать кнопку "сгенерировать Ответ". Код ответа будет отображен в соответствующем поле "Ответ" (см. рисунок 90).

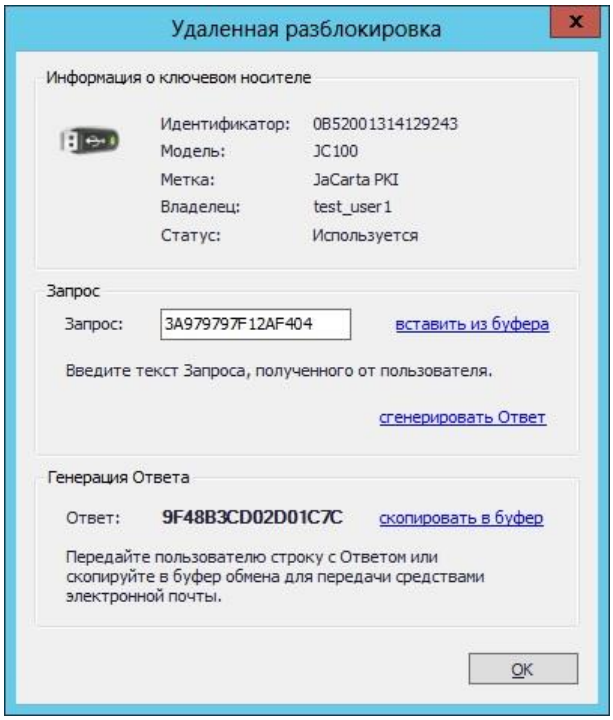


Рисунок 90 - Консоль управления JMS. Окно "Удаленная разблокировка". Сгенерированный ответ

8. Администратор должен продиктовать пользователю код ответа.
9. Пользователь должен ввести код ответа в соответствующем поле "Ответ" (см. рисунок 91) и подтвердить ввод нажатием кнопки "OK".

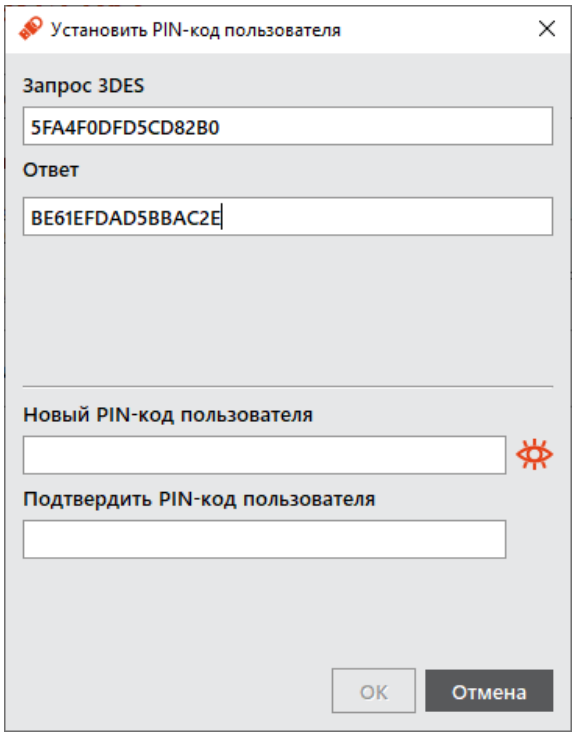


Рисунок 91 - Окно "Запрос/Ответ: JaCarta PKI". Ввод сгенерированного ответа

10. При корректно введенном коде ответа на экране пользователя будет отображено информационное сообщение об успешности операции (см. рисунок 92).

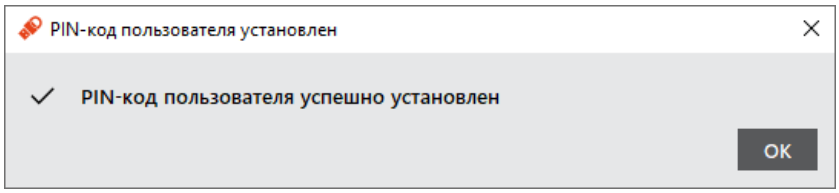


Рисунок 92 - Сообщение об успешной разблокировке PIN-кода пользователя в удаленном режиме

8.4 Изменение PIN-кода администратора

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

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

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

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

Для смены PIN-кода администратора:

1. Подсоединить электронный ключ, на котором необходимо сменить PIN-код администратора, к компьютеру.
2. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
3. В левой панели выбрать нужный электронный ключ и перейти на вкладку, соответствующую приложению, для которого необходимо изменить PIN-код администратора.
4. Нажать кнопку "Сменить PIN-код администратора". Будет открыто окно "Сменить PIN-код администратора" (см. рисунок 93).

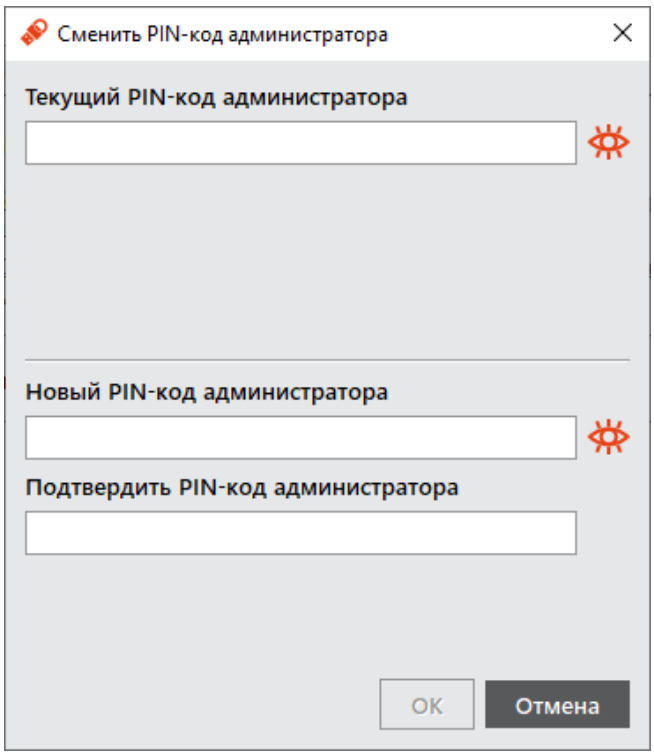


Рисунок 93 - Окно "Смена PIN-кода администратора"

5. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
6. В полях "Новый PIN-код администратора" и "Подтвердить PIN-код администратора" ввести новый PIN-код администратора и его подтверждение соответственно.
7. Нажать кнопку "OK".
8. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение. Для его закрытия необходимо нажать кнопку "OK".

8.5 Изменение качества PIN-кода пользователя для приложения PKI

Изменение качества PIN-кода возможно выполнить без форматирования электронного ключа.

Для изменения качества PIN-кода:

1. Подсоединить электронный ключ, на котором необходимо изменить качество PIN-кода пользователя, к компьютеру.
2. Запустить ПО "Единый Клиент JaCarta" и перейти в расширенный режим.
3. В левой панели выбрать нужный электронный ключ и перейти на вкладку, соответствующую приложению PKI. Окно примет вид, указанный на рисунке ниже (Рисунок 94). Нажать кнопку "Изменить качество PIN-кода".

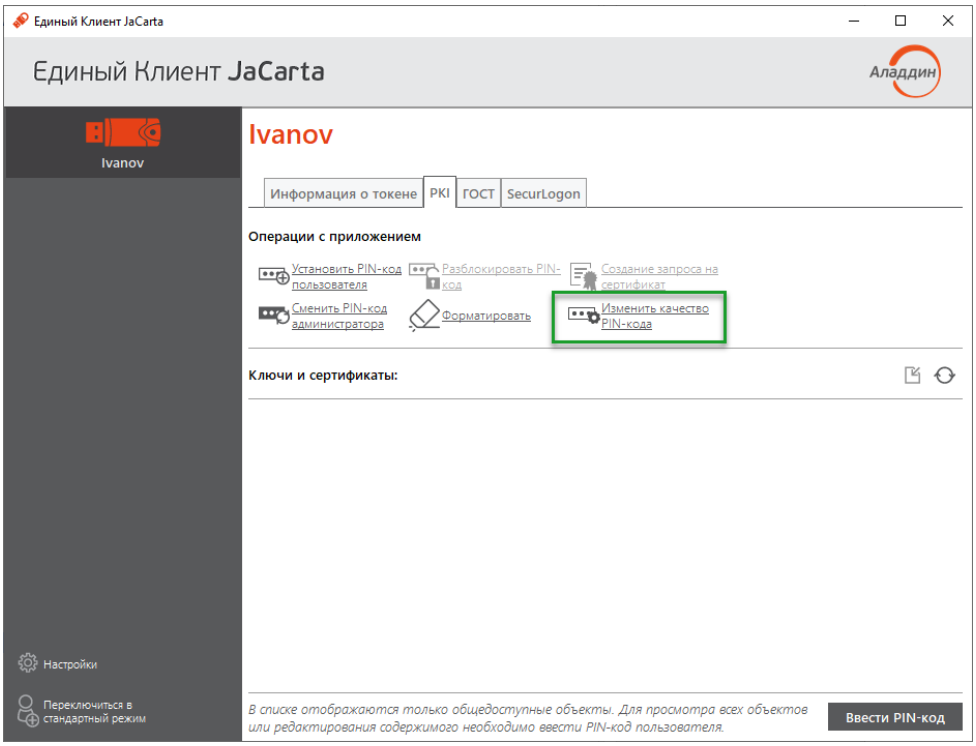


Рисунок 94 - Окно "Единый Клиент JaCarta". Кнопка "Изменить качество PIN-кода"

4. Будет открыто окно аутентификации для ввода PIN-кода администратора. После ввода PIN-кода администратора будет открыто окно мастера изменения качества PIN-кода пользователя для приложения PKI (Рисунок 95).

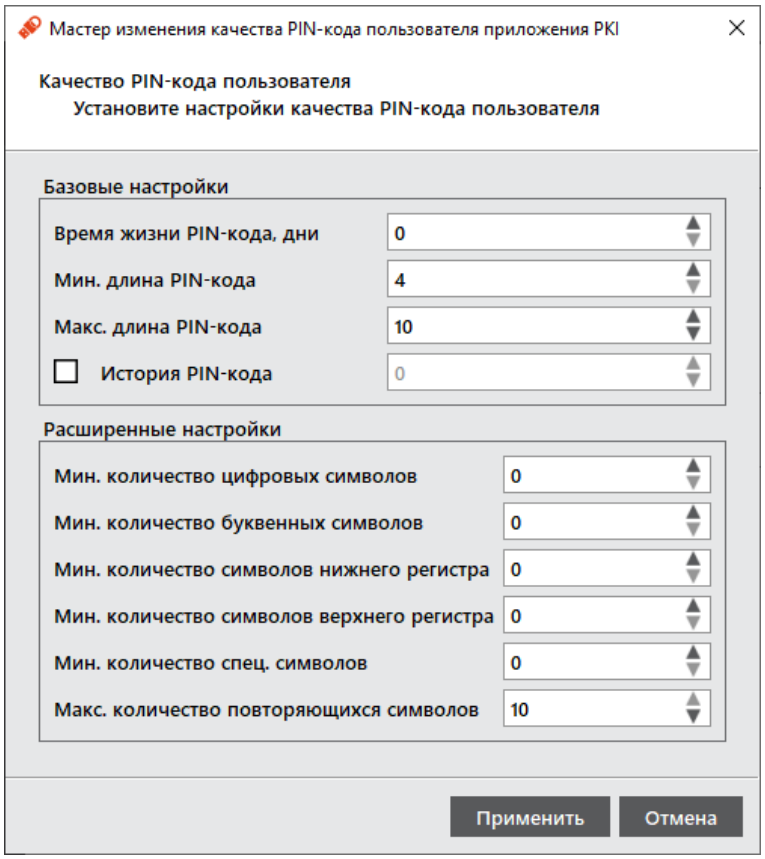


Рисунок 95 - Окно "Мастер изменения качества PIN-кода пользователя приложения PKI"

5. Измените настройки качества PIN-кода желаемым образом и нажмите кнопку "Применить".

6. Будет открыто окно для назначения нового PIN-кода пользователя. Укажите новый PIN-код и его подтверждение и нажмите кнопку "ОК".
7. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение. Для его закрытия необходимо нажать кнопку "ОК".

9. Драйвер виртуального считывателя JaCarta Virtual Reader

Драйвер виртуального считывателя JaCarta Virtual Reader представляет собой прослойку между реальным USB-устройством и менеджером ресурсов смарт-карт операционной системы Windows.

Драйвер виртуального считывателя JaCarta Virtual Reader обеспечивает работоспособность устройств JaCarta в VDI (Citrix, VMware, в том числе, Horizon) и в RDP-сессиях при использовании некоторых приложений, например, MMC консоли в режиме выпуска сертификатов.

9.1 Установка JaCarta Virtual Reader

Драйвер виртуального считывателя JaCarta Virtual Reader может быть установлен на компьютер в ходе установки ПО "Единый Клиент JaCarta"; если этого не произошло, то он может быть установлен позже как с помощью мастера установки ПО "Единый Клиент JaCarta", так и средствами командной строки Windows.

> *При установке драйвера с помощью мастера установки по умолчанию устанавливаются два драйвера виртуальных считывателей. Для установки другого количества драйверов (допускается устанавливать от 1 до 10 драйверов) используйте способ установки средствами командной строки Windows.*

Драйвер виртуального считывателя JaCarta Virtual Reader устанавливается на операционные системы Microsoft Windows 7 и выше разрядностями x64 и x86.

Для установки драйвера виртуального считывателя JaCarta Virtual Reader с помощью мастера установки:

1. Выполните шаги 1-4 процедуры изменения ПО "Единый Клиент JaCarta" (см. п. 5.1 "Изменение программы").
2. На шаге 4 выбора компонент в окне "Выборочная установка" раскройте список компонента "Драйверы", выберите компонент "Поддержка JaCarta Virtual Reader" и нажмите значок . Выберите значение "Данный компонент и все подкомпоненты будет установлены на локальный жесткий диск".

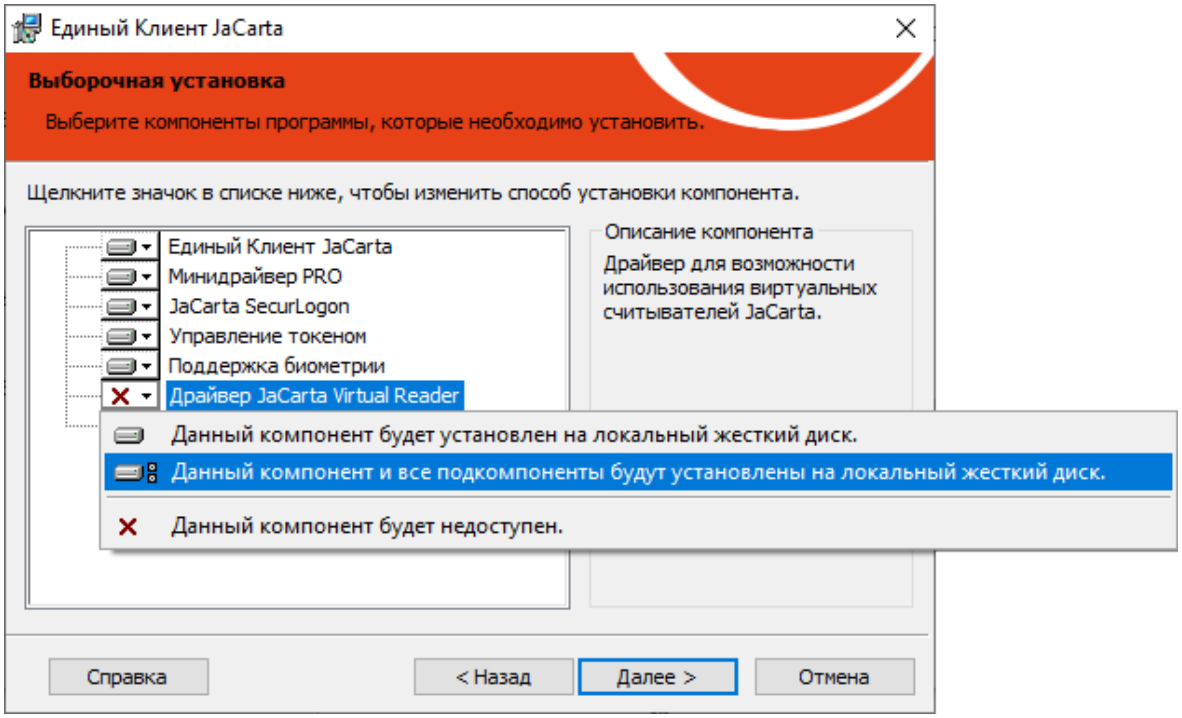


Рисунок 96 - Установка драйвера виртуального считывателя JaCarta Virtual Reader с помощью мастера установки

3. Продолжайте выполнение изменения ПО "Единый Клиент JaCarta" (см. п. 5.1 "Изменение программы").
4. После завершения изменения необходимо перезагрузить компьютер.
5. Установленные виртуальные считыватели будут отображены в разделе "Устройства чтения смарт-карт" в окне "Диспетчер устройств". По умолчанию устанавливается два считывателя:

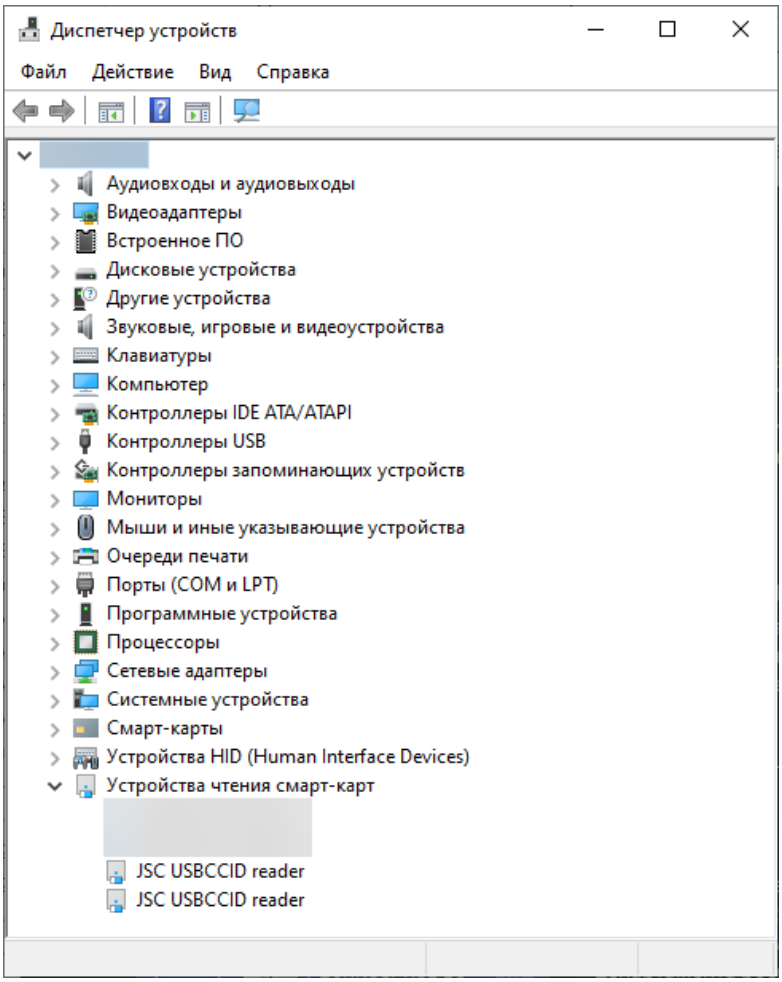


Рисунок 97 - Установленный драйверы виртуального считывателя JaCarta Virtual Reader в окне "Диспетчер устройств"

Для установки драйвера виртуального считывателя JaCarta Virtual Reader средствами командной строки Windows:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Запустите интерпретатор командной строки от имени администратора.
4. Выполните команду msiexec со следующими параметрами:

```
msiexec /i файл_инсталляции_Единого_Клиента_JaCarta.msi /quiet INSTALL_JACARTA_VR_DRIVER=1
IFD_READERS=2
```

где:

- `файл_инсталляции_Единого_Клиента_JaCarta.msi` – название файла инсталляции (см. п. 4.2 "Описание пакетов установки");
- `/quiet` – тихий режим установки;
- `INSTALL_JACARTA_VR_DRIVER=1` – значение параметра "1" является признаком установки компонента (см. п. 4.5.1 "Параметры для установки программы в режиме командной строки");
- `IFD_READERS=2` – параметр, значение которого определяет количество устанавливаемых драйверов виртуальных считывателей. Параметр может принимать значения от 1 до 10.

9.2 Удаление JaCarta Virtual Reader

Драйвер виртуального считывателя JaCarta Virtual Reader может быть удален с компьютера, при этом остальные компоненты ПО "Единый Клиент JaCarta" не будут изменены.

Для удаления драйвера виртуального считывателя JaCarta Virtual Reader:

1. Выполните шаги 1-4 процедуры изменения ПО "Единый Клиент JaCarta" (см. п. 5.1 "Изменение программы").
2. На шаге 4 выбора компонент в окне "Выборочная установка" раскройте список компонента "Драйверы", выберите компонент "Поддержка JaCarta Virtual Reader" и нажмите значок ▼. Выберите значение "Данный компонент будет недоступен".

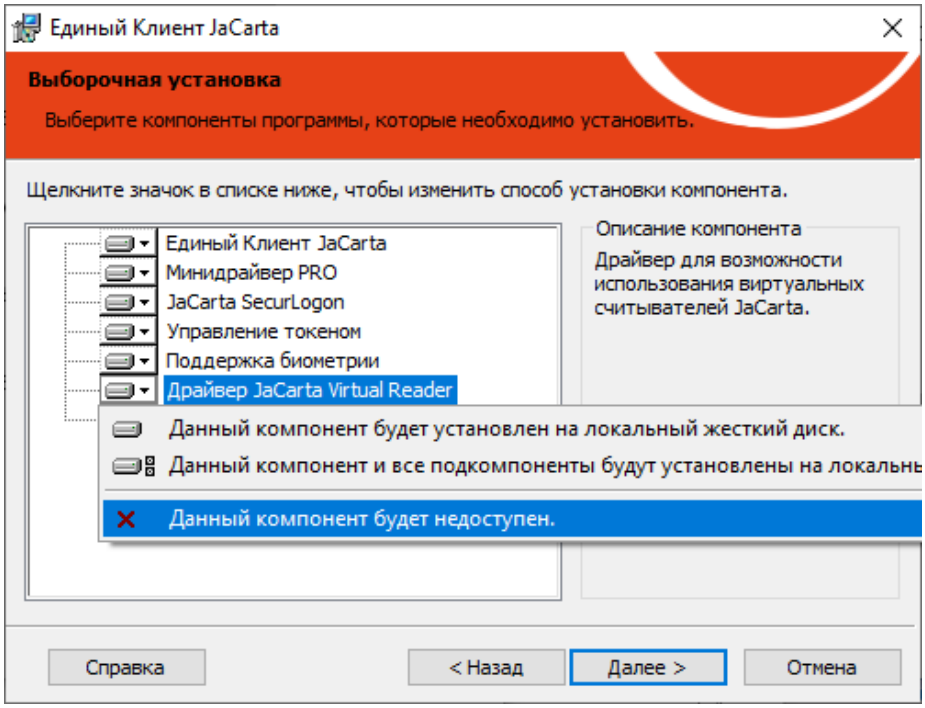


Рисунок 98 - Удаление драйвера виртуального считывателя JaCarta Virtual Reader

3. Продолжайте выполнение удаления ПО "Единый Клиент JaCarta" (см. п. 5.1 "Изменение программы").

9.3 Работа JaCarta Virtual Reader

Драйвер виртуального считывателя JaCarta Virtual Reader загружается на среднем этапе загрузки ОС, в ходе создания PnP менеджером корневых перечисляемых устройств. Виртуальные считыватели загружаются вместе с ОС и работают постоянно, пока не завершит работу ОС или они не будут деинсталлированы в ходе удаления компонента "Поддержка JaCarta Virtual Reader", а также в случаи полной деинсталляции ПО "Единый Клиент JaCarta".

При подключении обслуживаемого устройства виртуальный драйвер регистрирует себя как скрытое функциональное устройство над реальным USB-устройством, тип которого "Считыватель смарт-карт". Драйвер логически связывает скрытое устройство с присутствовавшем до него виртуальным устройством. После этого драйвер виртуального считывателя передает управление виртуальному считывателю, который оповещает ОС о подключении в него устройства "Смарт-карта". При отключении USB устройства из виртуального считывателя "извлекается" смарт карта.

10. Синхронизация паролей электронного ключа и учетной записи домена Windows

ПО "Единый Клиент JaCarta" позволяет проводить синхронизацию PIN-кода электронного ключа с паролем учетной записи пользователя, который запрашивается при входе в домен Windows.

Пароль учетной записи пользователя (пароль домена) синхронизируется с PIN-кодом электронного ключа. При последующих изменениях PIN-кода электронного ключа пароль учетной записи пользователя (доменный пароль) вводить не требуется.

В случае рассинхронизации паролей или смены администратором AD пароля учетной записи пользователя (доменного пароля) необходимо произвести повторную синхронизацию паролей.

Если пароль не соответствует требованиям к качеству одной из политик синхронизация невозможна.

Примечание. Синхронизация PIN-кода электронного ключа с паролем учетной записи пользователя возможна только для приложений PKI (в том числе с апплетом PRO) и PKI/BIO.

Для синхронизации PIN-кода пользователя и пароля учетной записи домена Windows:

1. Зайти в редактор реестра с правами администратора.
2. В разделе `HKEY_LOCAL_MACHINE/SOFTWARE/AladdinRD/JCUC/SyncPin` создать строковый параметр с именем `Domain` и задать ему значение имени домена (в данном случае для примера используется значение "testdomain.lab").
   Настройка может так же быть выполнена по ключу SYNCPINDOMAIN (см. пункт 4.5.1).

   Примечание. Если раздел `SyncPin` отсутствует, то необходимо создать по указанному адресу раздел с указанным именем.
3. В левом нижнем углу основного окна ПО "Единый Клиент JaCarta" нажать кнопку "Настройки" - Настройки.
4. В открывшемся окне "Настройки" во вкладке "Основные" в поле "Имя домена для синхронизации паролей" должно быть отображено введенное на шаге 2 имя домена. Нажать кнопку "ОК".

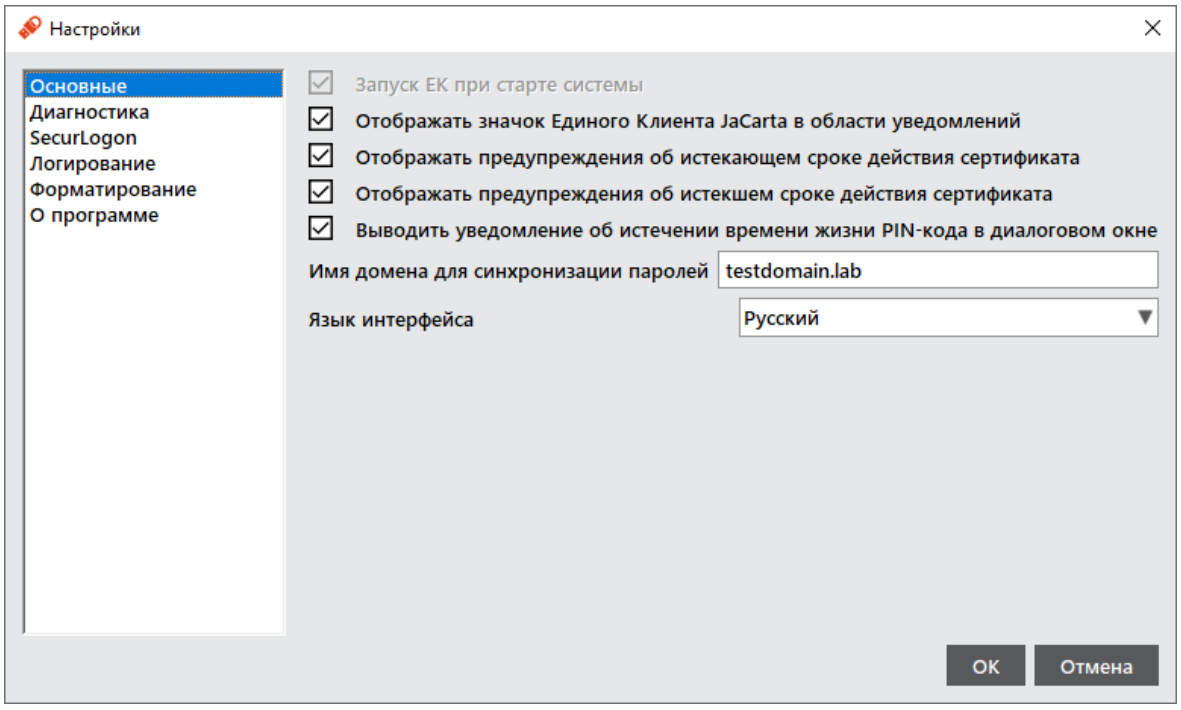


Рисунок 99 - Окно "Настройки". Вкладка "Основные"

5. Закрыть окно ПО "Единый Клиент JaCarta".
6. В Меню быстрого запуска элемента в области уведомлений активировать команду "Выйти".

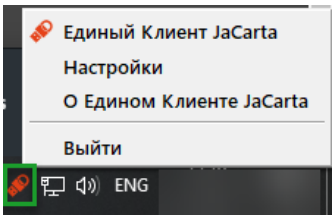


Рисунок 100 – Панель задач Windows. Выход из программы ПО "Единый Клиент JaCarta"

7. Заново открыть ПО "Единый Клиент JaCarta", последовательно выбрав: "Пуск → Аладдин Р.Д. → Единый Клиент JaCarta". В открывшемся основном окне в стандартном режиме будет доступна кнопка "Сменить PIN-код и пароль домена".

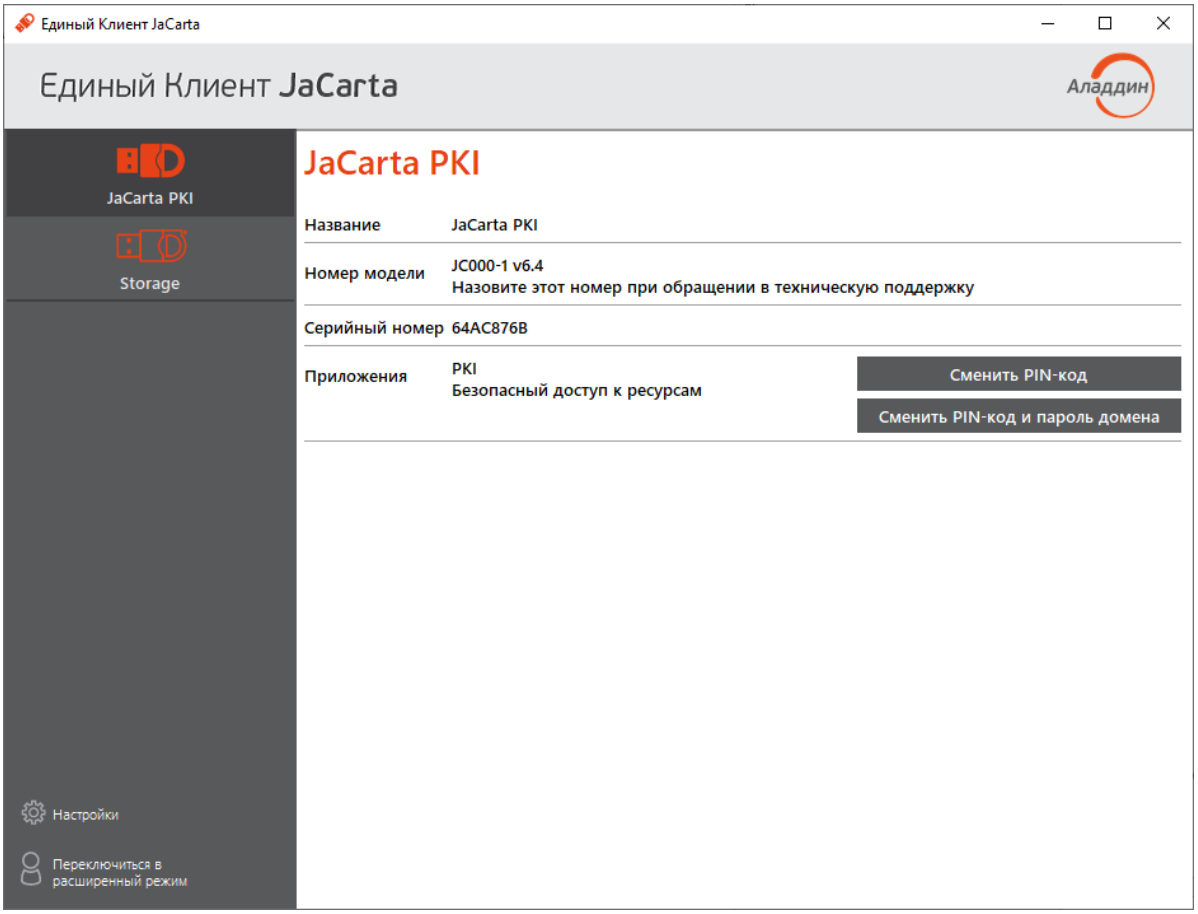


Рисунок 101 - Доступная кнопка "Сменить PIN-код и пароль домена"

Примечание. Опция "Сменить PIN-код и пароль домена" появится также в Меню быстрого запуска, которое можно запустить на панели задач в области уведомлений, нажав правой кнопкой мыши на значок .

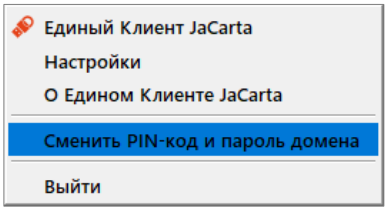


Рисунок 102 - Меню быстрого запуска ПО "Единый Клиент JaCarta" с командой "Сменить PIN-код и пароль домена"

8. Нажать кнопку "Сменить PIN-код и пароль домена". Будет открыто окно "Сменить PIN-код и пароль домена".

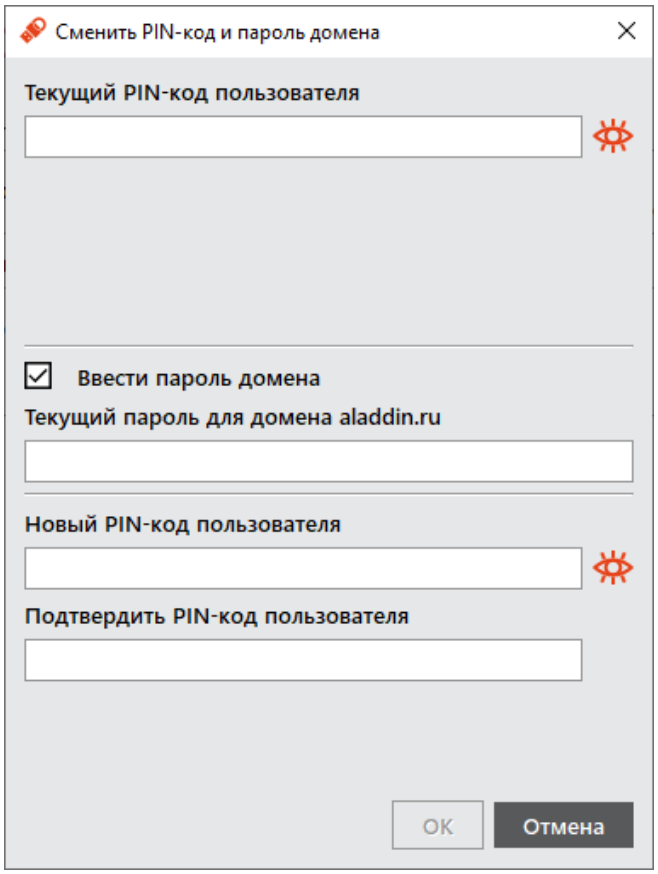


Рисунок 103 - Окно "Смена PIN-кода и пароля домена"

9. Заполнить поля следующим образом:
   - в поле "Текущий PIN-код пользователя" ввести значение текущего PIN-кода пользователя;
   - при установке флажка "Ввести пароль домена" в диалоговом окне будет добавлено поле "Текущий пароль домена <наименование домена>". Ввести пароль для указанного домена. Если флажок не установлен, значение пароля домена будет взято из поля "Текущий PIN-код пользователя" (подразумевается, что пароль домена и PIN-код пользователя уже синхронизированы);
   - в поле "Новый PIN-код пользователя" ввести значение нового PIN-кода пользователя;
   - в поле "Подтверждение кода" ввести значение нового PIN-кода пользователя повторно.
10. Нажать кнопку "OK".
    - Если введенный пароль пользователя не отвечает требованиям к качеству пароля, то будет отображено окно с описанием ошибки:

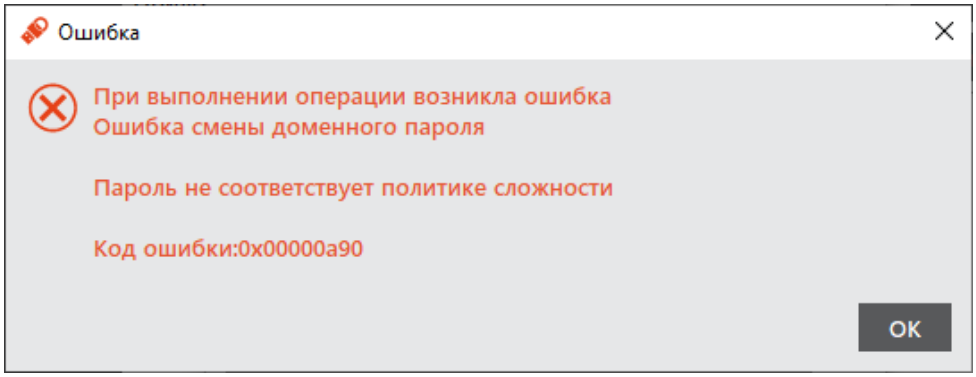


Рисунок 104 - Ошибка при смене доменного пароля

    - При успешной смене доменного пароля будет отображено окно с информацией об этом:

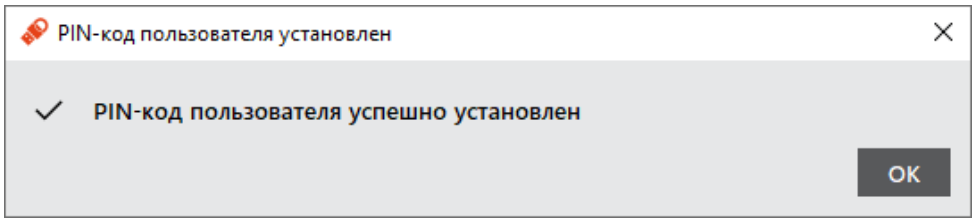


Рисунок 105 - Сообщение об успешной смене доменного пароля

11. Поддержка безопасности программного средства

В рамках поддержки безопасности изготовитель (производитель) программного средства Единый Клиент JaCarta» осуществляет комплекс мероприятий по внесению в программное средство следующих изменений:

- изменения в имеющиеся функции безопасности или изменения, связанные с добавлением новых функций безопасности. Изменения вносятся по решению изготовителя (производителя) в рамках повышение качества функционирования программы, ее совершенствования и/или расширения функциональных возможностей;
- исправления, связанные с устранением недостатков безопасности, обусловленных программными дефектами и уязвимостями, и недекларированных возможностей программного средства.

Поддержка безопасности включает:

- устранение недостатков и программных дефектов, а также уязвимостей и недекларированных возможностей программного средства;
- информирование владельцев (пользователей) об обновлении программного средства;
- доведение до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию;
- информирование об окончании производства и (или) поддержки безопасности программного средства.

Устранение недостатков безопасности изготовителем (производителем) предусматривает:

- получение сведений о недостатках от владельцев (пользователей) программного средства путем приема и отработки сообщений о недостатках безопасности и запросов на исправление этих недостатков;
- устранение недостатков средства путем внесения исправлений и доработки программного средства или его отдельных компонентов, а также разработку иных мер, снижающих возможность эксплуатации уязвимостей;
- формирование (представление) исправлений и доработок в виде обновлений программного средства, которые необходимо применить для устранения недостатка безопасности или подготовка промежуточных решений, содержащие компенсирующие меры по защите информации или ограничения по применению программного средства, и снижающих возможность эксплуатации недостатков (уязвимостей). Компенсирующие меры необходимо реализовать и применять до выпуска исправления, устраняющего недостаток безопасности. Разработка компенсирующих мер по защите информации или ограничений по применению средства осуществляются не позднее 48 часов с момента выявления недостатка. Доработка средства (формирование (представление) исправлений и доработок) или разработка мер по защите информации, нейтрализующих недостаток безопасности, осуществляется в срок не более 60 дней с момента выявления недостатка.

Информирование об обновлении программного средства включает:

- публикацию информации о выпуске обновлений, в том числе исправлений недостатков безопасности, и доведение ее до владельцев (пользователей) программного средства. Сведения о наличии обновления публикуются на Web-сайте изготовителя (производителя) в разделе «Техническая поддержка» (https://aladdin-rd.ru/support) и доводятся до владельцев (пользователей) программного средства с использованием их контактных данных[8], зарегистрированных у изготовителя (производителя) посредством отправки сообщений на электронные адреса;
- доведение информации о недостатках программного средства, а также о компенсирующих мерах по защите информации или ограничений по применению программы до каждого из владельцев (пользователей) программного средства осуществляется не позднее 48 часов с момента выявления недостатка. При доведении информации о недостатках до владельцев (пользователей) подлинность и целостность доводимой информации, при необходимости, обеспечивается за счет применения квалифицированной электронной подписи изготовителя (производителя).

Сведения о наличии обновлений содержит описание недостатка безопасности, устраняемого предоставленным обновлением, предписанное корректирующее действие и соответствующее руководство по его выполнению. Автоматическое обновление сертифицированного программного средства не осуществляется.

[8] С целью своевременного получения информации о недостатках безопасности и мерах по их устранению владельцы программного средства должны обеспечить актуальность контактных данных, предоставленных изготовителю (производителю).

Доведение до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию предусматривает:

- возможность получения обновления с информационного ресурса изготовителя (производителя). Владелец (пользователь) программного средства для получения доступа к обновлениям и возможности их загрузки должен (при необходимости) получить от изготовителя (производителя) авторизационные данные.
- возможность получения обновления средства способами, обеспечивающими его целостность. При доведении обновлений программного средства до владельцев (пользователей) подлинность и целостность обновлений обеспечивается за счет применения квалифицированной электронной подписи изготовителя (производителя).

При необходимости может использоваться другой способ доведения до владельцев (пользователей) обновлений программного средства и изменений в эксплуатационную документацию, при этом предписание о его использовании включено в сведения о выпуске обновления.

Выпуск обновления может являться реакцией на рекламацию (обращение) владельца программного средства, может быть направлен на устранение обнаруженных недостатков безопасности или может формироваться в рамках совершенствования программного средства изготовителем (производителем).

Обновления для устранения обнаруженных недостатков безопасности выпускаются изготовителем (производителем) и могут включать следующие корректирующие действия:

- исправления, которые необходимо применить для устранения недостатка безопасности;
- промежуточные решения, содержащие компенсирующие меры. Компенсирующие меры необходимо реализовать и применять до выпуска исправления, устраняющего недостаток безопасности.

Корректирующие действия, направленные на устранение уязвимостей программного средства, должны быть реализованы владельцем (пользователем) программного средства в сроки, рекомендованные изготовителем (производителем).

Получение и применение владельцем (пользователем) программного средства обновлений, содержащих исправления, включает:

- получение файлов обновлений программного средства и соответствующих им контрольных сумм с использованием электронной почты или путем загрузки с Web-сайта изготовителя (производителя) по адресу https://aladdin-rd.ru/support;
- проверку квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления;

Примечание – Для проверки квалифицированной электронной подписи изготовителя (производителя) могут использоваться общедоступные сервисы информационно-телекоммуникационной сети общего пользования, например, (https://www.gosuslugi.ru/eds).

- применение обновлений, содержащих исправления, если: результаты проверки квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм подтвердили их целостность и подлинность;

Примечание – Если результаты проверки квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм не подтвердили их целостность и подлинность, то необходимо обратится в службу технической поддержки и действовать в соответствии с ее указаниями.

- значения контрольных сумм файлов, полученные от изготовителя (производителя) при загрузке обновлений, принимаются в качестве эталонных значений контрольных сумм файлов установочных пакетов и исполняемых файлов программного средства.

Порядок применения обновлений определяется настоящим документом, если сведения о наличии обновления не предписывают другой последовательности действий.

Об окончании производства и (или) поддержки безопасности программного средства владельцы (пользователи) информируются не позднее чем за 1 год до окончания производства и (или) поддержки безопасности средства.

Приложение А
Компоненты ПО "Единый Клиент JaCarta"

Название компонента	Описание
Минидрайвер PRO	Минидрайвер для поддержки работы токенов PRO с Microsoft CSP
JaCarta SecurLogon	Для обеспечения двухфакторной аутентификации с использованием электронных ключей JaCarta и eToken в ОС Microsoft Windows
Управление токеном	Для возможности выполнять операции с токеном до входа пользователя в систему
Поддержка биометрии	Добавляет возможность использования биометрических считывателей и электронных ключей JaCarta
Драйвер поддержки JaCarta Virtual Reader	Для возможности использования виртуальных считывателей JaCarta

12. Контакты

12.1 Офис (общие вопросы)

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

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

E-mail: aladdin@aladdin.ru (общий)

Web: https://www.aladdin.ru

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

12.2 Техподдержка

Контакты службы техподдержки:

Телефон: +7 (499) 702-3968

Web: www.aladdin.ru/support

Коротко о компании

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

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

Основные направления

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

Лицензии

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

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

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru