Единый Клиент JaCarta

Руководство администратора для Windows

Версия продукта	2.12
Версия документа	1.1
Статус	Публичный
Дата	23.10.2019
Листов	113

Оглавление

1. О документе

1.1 Назначение документа

Документ представляет собой руководство пользователя для ПО Единый Клиент JaCarta.

1.2 На кого ориентирован данный документ

Документ предназначен для пользователей ПО Единый Клиент JaCarta, владельцев электронных ключей JaCarta/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, 10 даны указания по работе с компонентами ПО Единый Клиент JaCarta – виртуальным считывателем JaCarta CCID, утилитой JaCarta АРМ УЦ;
- в разделе 11 содержится описание процедуры синхронизация паролей электронного ключа и учетной записи домена Windows;
- в разделе 12 "Мастер техподдержки" приведено описание активации сбора диагностической информации об аварийных ситуациях, случившихся у пользователей с последующей отправкой собранной информации в службу технической поддержки компании Аладдин Р.Д.

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

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

Вы гарантируете, что будете соблюдать накладываемые на экспорт и 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 Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

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

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

Права и собственность

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

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), 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 ЗАО "Аладдин Р.Д." за это ПО.

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, 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

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

2.2 Термины и определения

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

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

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

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

Апплет – программное обеспечение, реализующее функциональность приложения электронного ключа.

Приложение – программное обеспечение, установленное в памяти электронного ключа.

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

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 Единого Клиента JaCarta в режиме пользователя.*

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

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

Пример. *В моделях электронных ключей JaCarta PKI и JaCarta PRO установлено приложение PKI, но в модели JaCarta PKI данное приложение реализовано апплетом Laser, а в модели JaCarta PRO –апплетом PRO. Название апплета конкретного приложения отображается в интерфейсе Единого Клиента JaCarta в режиме администратора.*

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

Таблица 2 – Параметры электронных ключей при поставке

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

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

3.2 Параметры электронных ключей при поставке

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

Таблица 3 – Параметры электронных ключей при поставке

Приложение и апплет / **Параметр, операция**	**Приложение PKI апплет PRO**	**Приложение PKI апплет Laser**	**Приложение ГОСТ апплет Криптотокен**	**Приложение ГОСТ апплет Криптотокен 2 ЭП**	**Приложение STORAGE апплет DataStore**	**Приложение OTP апплет AladdinOTP**
PIN-код пользователя по умолчанию	1234567890	11111111	не установлен	1234567890	1234567890	не установлен
PUK-код для разблокирования	не предусмотрен	не предусмотрен	не предусмотрен		не предусмотрен	не предусмотрен
PIN-код администратора по умолчанию	1234567890	00000000	1234567890	не предусмотрен	не установлен	не предусмотрен
Форматирование без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после форматирования)	возможно	возможно	возможно	невозможно	невозможно	возможно
Форматирование без назначения PIN-кода администратора	возможно	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	PIN-код пользователя остается прежним	операция не предусмотрена
Разблокирование PIN-кода пользователя в удалённом режиме	возможно	невозможно	невозможно	возможно	невозможно	невозможно
Изменение PIN-кода пользователя администратором без форматирования	возможно	возможно	невозможно	невозможно	невозможно	невозможно

* Значение PUK-кода указано для электронных ключей, поставляющихся отформатированными. Исключением являются модель JaCarta-2 SE/PKI/ГОСТ, которая содержит приложение ГОСТ с апплетом Критотокен 2 ЭП – она поставляются с PUK-кодом по умолчанию 1234567890

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 3.

Таблица 4 – Перечень операций с электронными ключами

Приложение и апплет / Операция в Единый Клиент JaCarta ↓	Приложение PKI апплет PRO	Приложение PKI апплет Laser	Приложение ГОСТ апплет Криптотокен	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 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	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	Требуется PIN-код пользователя
Смена своего PIN-кода администратором	Требуется PIN-код администратора	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	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 PIN-код администратора	Требуется PUK-код	Не доступно	Функциональность отсутствует
Удаленное разблокирование PIN-кода пользователя	PIN-код не требуется	Не доступно	Не доступно	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	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	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	PIN-код не требуется
Создание запроса на сертификат	Требуется PIN-код пользователя	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 Единый Клиент JaCarta приведены в таблице 4.

Таблица 5 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Microsoft Windows Server 2008 SP2 (32/64-бит): Standard, Enterprise, Datacenter Microsoft Windows 7 SP1 (32/64-бит): Professional, Enterprise, Ultimate Microsoft Windows Server 2008 R2 SP1: Standard, Enterprise, Datacenter Microsoft Windows 8.1 (32/64-бит): Core, Pro, Enterprise Microsoft Windows 10 (32/64-бит): Home, Professional, Enterprise Microsoft Windows Server 2012: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2012 R2: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2016
Поддерживаемые модели электронных ключей	Электронные ключи eToken: • eToken PRO (Java) • eToken NG-FLASH (Java) • eToken NG-OTP (Java) • eToken ГОСТ Электронные ключи JaCarta: • JaCarta PKI • JaCarta PRO • JaCarta ГОСТ • JaCarta LT • JaCarta ГОСТ/Flash • JaCarta PKI/Flash • JaCarta PRO/ГОСТ • JaCarta PKI/ГОСТ • JaCarta PKI/ГОСТ/Flash • JaCarta SF/ГОСТ • JaCarta-2 ГОСТ • JaCarta-2 PKI/ГОСТ • JaCarta-2 SE/PKI/ГОСТ • JaCarta-2 SF • JaCarta-2 PRO/ГОСТ • JaCarta WebPass • JaCarta U2F/WebPass • JaCarta U2F
Аппаратные средства	Для USB-токенов используется USB-порт. Для смарт-карт необходимо наличие подключённого считывателя смарт-карт. Для электронных ключей в форм-факторе microSD можно использовать следующее оборудование: • разъём microSD; • разъём SD через переходник microSD-to-SD;

Требование	Содержание
	• USB-порт через переходник microSD-to-USB. 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

Дистрибутив Единого Клиента JaCarta включает пакеты установки, приведенные в таблице *5*.

Таблица 6 – Перечень пакетов установки дистрибутива Единый Клиент JaCarta

Файл	Описание
JaCartaUnifiedClient_2.12.2.2260_win-x64_ru-Ru.msi	Пакет установки для 64-х разрядных операционных систем Microsoft Windows
JaCartaUnifiedClient_2.12.2.2260_win-x86_ru-Ru.msi	Пакет установки для 32-х разрядных операционных систем Microsoft Windows

4.3 Обязательные меры предосторожности

> *Единый Клиент JaCarta уже содержит модуль JC-Client, поэтому не рекомендуется устанавливать JC-Client на компьютер с установленным Единым Клиентом JaCarta. Отдельная дополнительная установка JC-Client может нарушить настройки Единого Клиента JaCarta и вызвать ошибки при последующих установках и удалениях этих приложений.*

4.3.1 Особенности работы с JaCarta microSD

При работе с JaCarta microSD на планшетах, оснащенных ОС Microsoft Windows 8.x, могут возникнуть проблемы при переходе в энергосберегающий режим и обратно. Рекомендуется использовать JaCarta microUSB-токен вместо JaCarta microSD на планшетах с ОС Microsoft Windows 8.x и выше.

4.3.2 Особенности установки и работы совместно с JMS

- Единый Клиент JaCarta 2.12 совместим с JMS 3.4+
- Единый Клиент JaCarta 2.11 совместим с JMS 3.1.
- Единый Клиент JaCarta 2.9 совместим с JMS 2.2 и 2.3.
- Единый Клиент JaCarta 2.8 рекомендуется использовать с более ранними версиями JMS.
- Единый Клиент JaCarta 2.7 не рекомендуется использовать совместно с JMS.

4.3.3 Особенности использования электронных ключей eToken CryptoPro и JaCarta CryptoPro

Для использования электронных ключей eToken CryptoPro и JaCarta CryptoPro необходимо, чтобы на компьютере было установлено программное обеспечения для работы с СКЗИ Крипто-Про ФКН CSP.

4.4 Установка программы с помощью мастера установки

Для установки Единого Клиента JaCarta с помощью мастера установки:

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

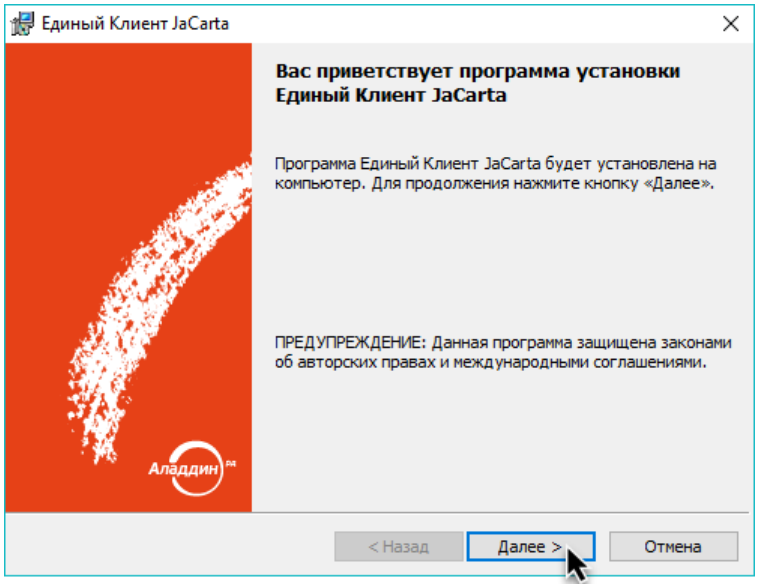


Рисунок 1 - Окно приветствия мастера установки Единый Клиент JaCarta

2. Нажмите кнопку "Далее". Будет отображено окно с "Лицензионное соглашение". 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 Единого Клиента JaCarta будет прекращена.

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

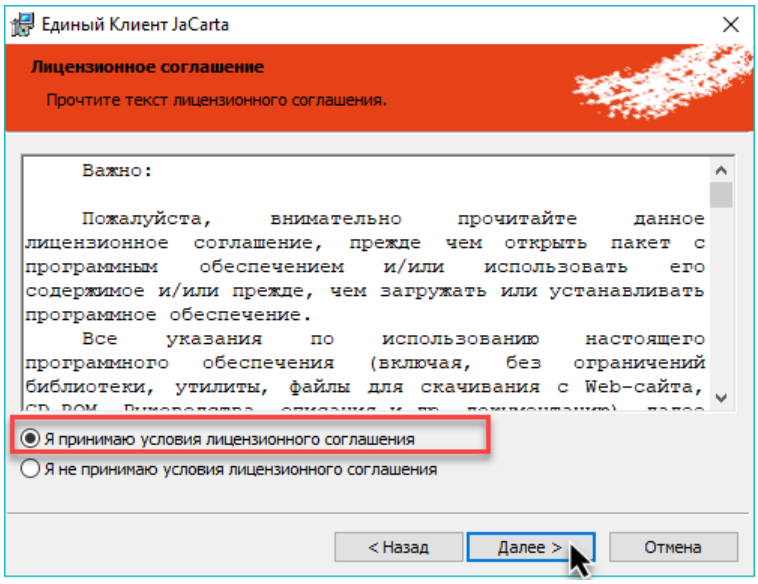


Рисунок 2 - Окно "Лицензионное соглашение" мастера установки Единый Клиент JaCarta

3. Нажмите кнопку "Далее". Будет открыто окно "Вид установки" (см. 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", "Управление токеном", "Поддержка биометрии", "Установка Athena CSP в качестве криптопровайдера по умолчанию". 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.

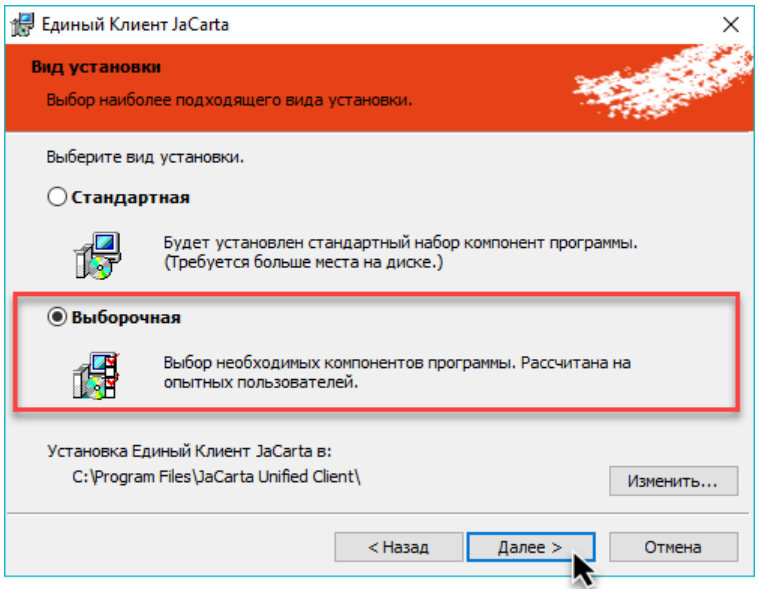


Рисунок 3 - Окно "Вид установки" мастера установки Единый Клиент JaCarta

4. Нажмите кнопку "Далее". В случае выборочной установки будет отображено окно для выбора из следующего набора компонент:
   - JaCarta SecurLogon;
   - JaCarta WebPass Tool;
   - JaCarta АРМ УЦ;
   - Управление токеном;
   - Поддержка биометрии;
   - Установка Athena CSP в качестве криптопровайдера по умолчанию;
   - Драйверы:
     - Поддержка JaCarta Virtual Reader;
     - Поддержка работы устаревших моделей JaCarta в продуктах VMware;
     - Поддержка JaCarta PKI с обратной совместимостью;
     - Поддержка JaCarta Secure MicroSD;
     - Поддержка eToken PRO 32K/64K (USB eToken Driver).

Примечание. Описание компонентов приведено в приложении А.

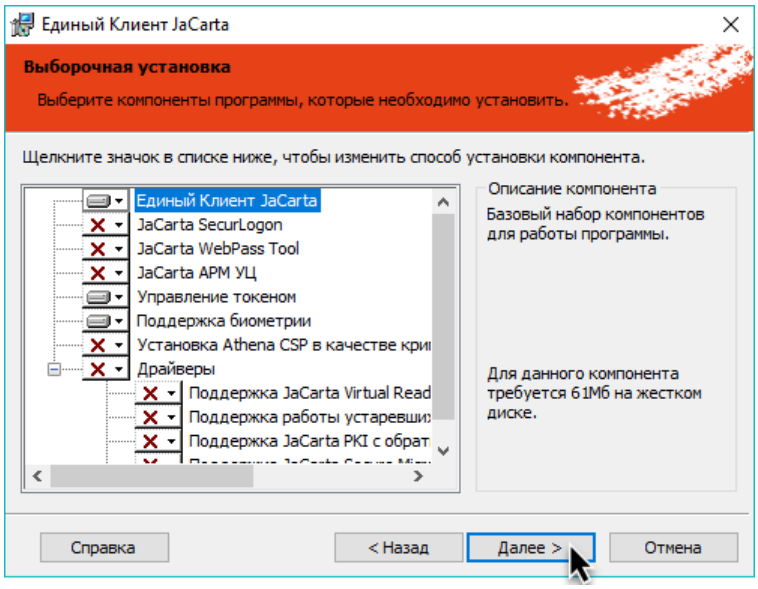


Рисунок 4 - Окно "Выборочная установка" мастера установки Единый Клиент JaCarta

Для установки требуемого компонента в окне "Выборочная установка" в строке с названием нужного компонента нажмите на значок ▼ и в выпадающем списке выберите необходимую опцию установки:

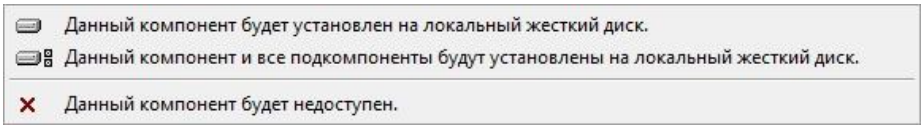


Рисунок 5 – Опции установки компонента

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

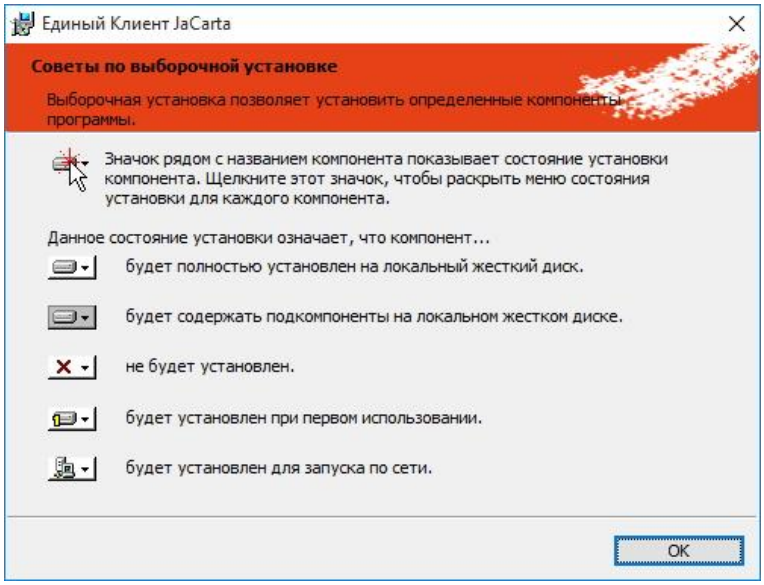


Рисунок 6 - Окно "Советы по выборочной установке" мастера установки Единый Клиент JaCarta

5. Нажмите "Далее" в окне "Выборочная установка". Будет отображено окно "Установка программы":

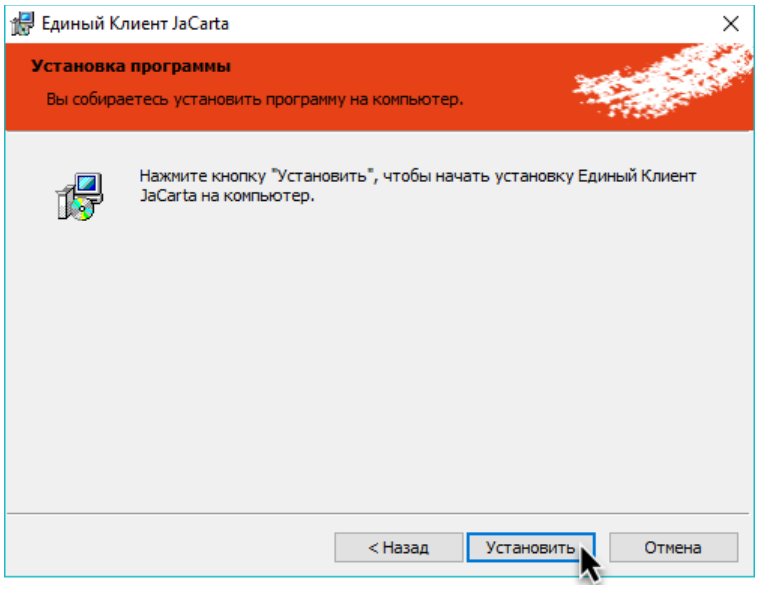


Рисунок 7 - Окно "Установка программы" мастера установки Единый Клиент JaCarta

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

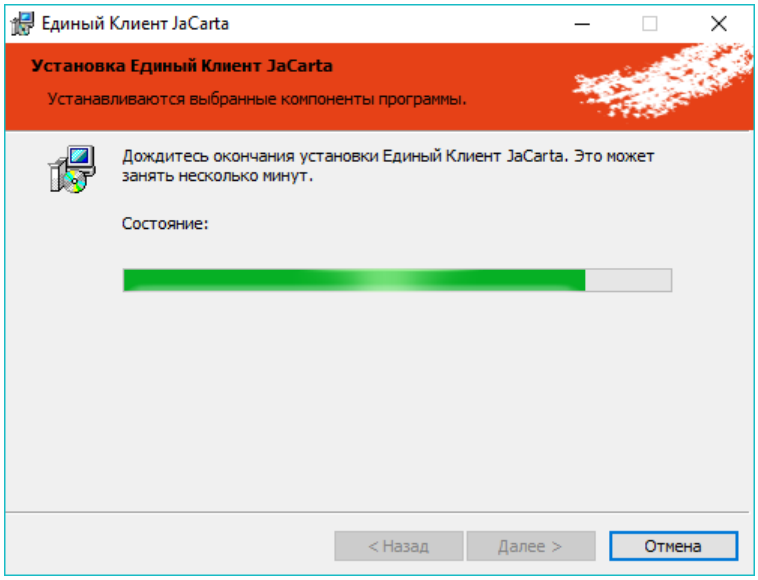


Рисунок 8 - Процесс установки Единый Клиент JaCarta

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

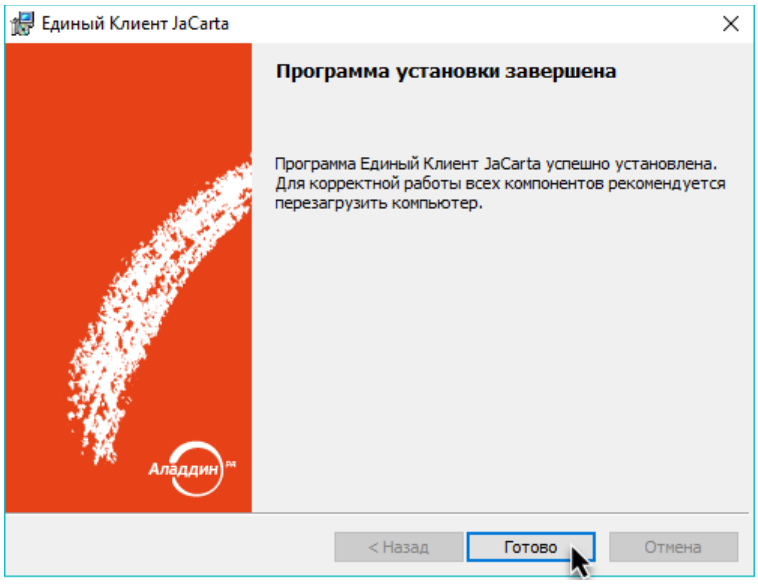


Рисунок 9 - Окно завершения установки Единый Клиент JaCarta

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

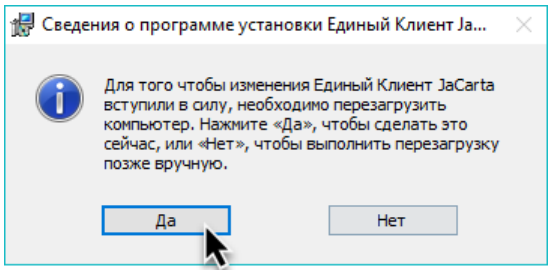


Рисунок 10 - Окно "Сведения о программе установки Единый Клиент JaCarta"

9. Будет выполнена перезагрузка компьютера, после завершения Единый Клиент JaCarta готов к работе.

4.5 Особенности установки Единый Клиент JaCarta на ОС Microsoft Windows XP с установленным антивирусом Dr.Web

Если установка Единый Клиент JaCarta происходит на компьютере с ОС Microsoft Windows XP и с установленным антивирусом Dr.Web, то перед установкой Единый Клиент JaCarta необходимо выполнить следующие действия:

1. Запустить **SpIDer Agent,** нажав значок на панели задач в области уведомлений.
2. Разблокировать **SpIDer Agent.** Для внесения изменений нажать кнопку :

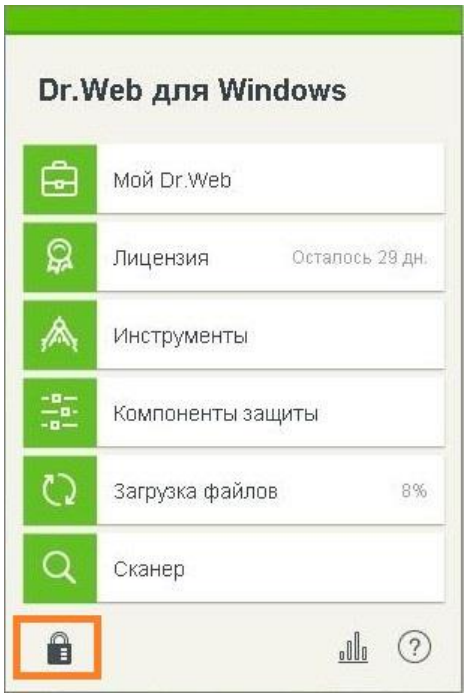


Рисунок 11 – Антивирус Dr.Web. Разблокировка элементов управления

3. Нажать появившуюся кнопку "Настройки" - :

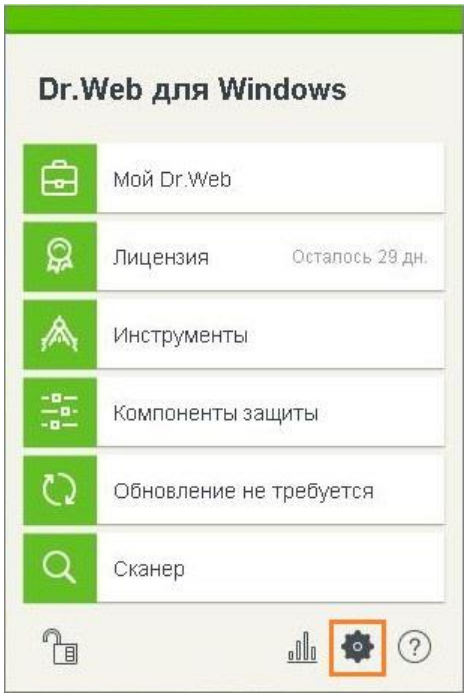


Рисунок 12 – Антивирус Dr.Web. Элемент управления "Настройки"

4. В окне "Настройки" выбрать опцию "Компоненты защиты":

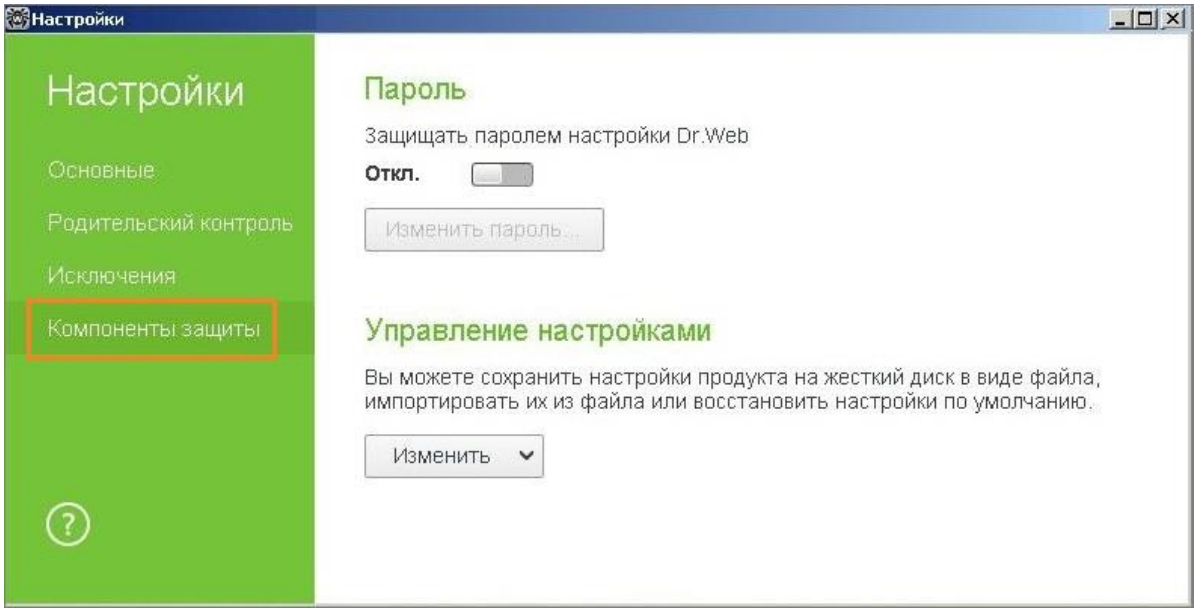


Рисунок 13 – Антивирус Dr.Web. Окно "Настройки"

5. В окне "Компоненты защиты" выбрать опцию "Превентивная защита" и установить для объектов параметр "Разрешать"**:**

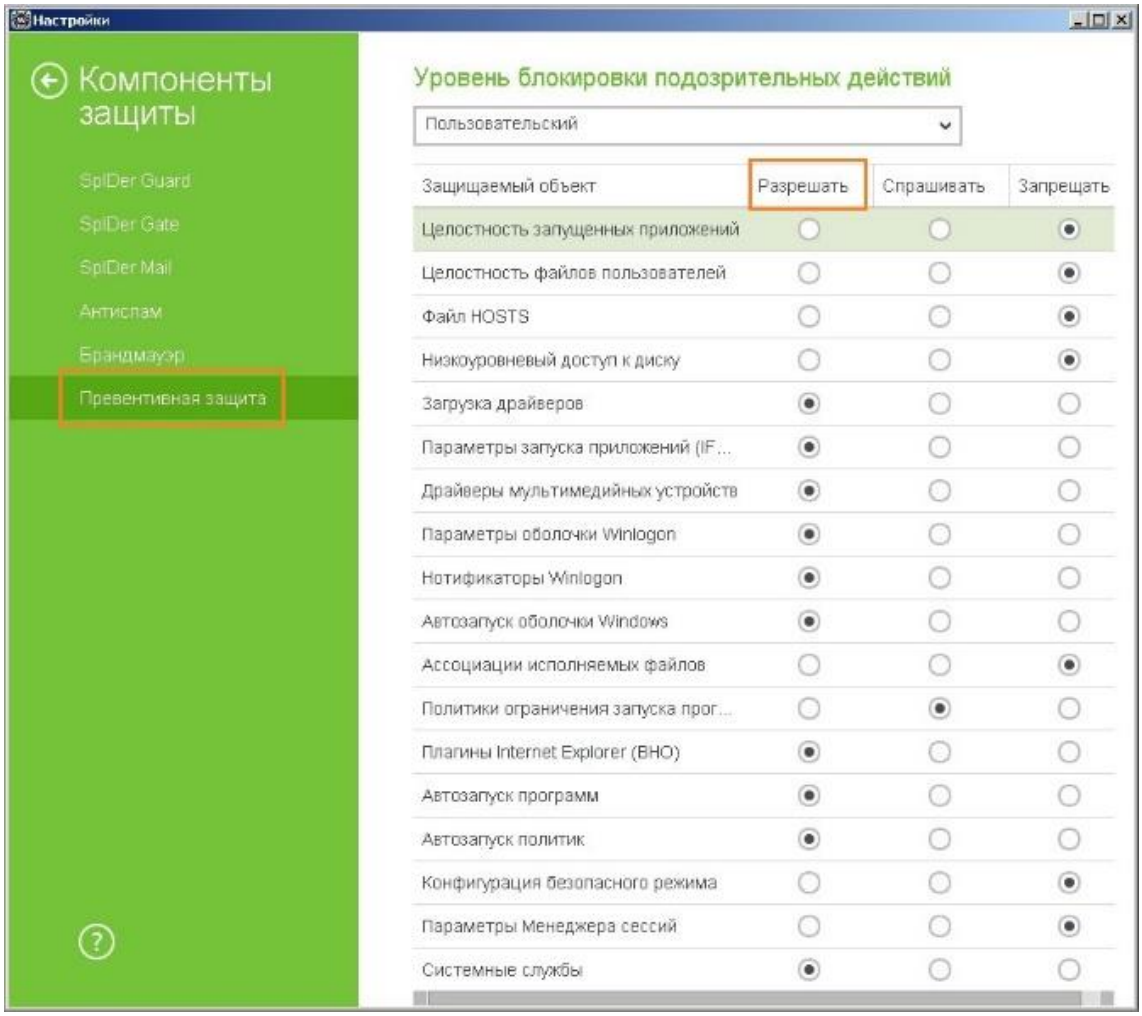


Рисунок 14 – Антивирус Dr.Web. Окно "Компоненты защиты"

6. Закрыть окно "Настройки" и установить Единый Клиент JaCarta (см. п. 4.4 "Установка программы с помощью мастера установки").

Если при установке ПО Единый Клиент JaCarta будет выбрана опция "Проверять наличие обновлений", то после перезагрузки ОС может появиться окно, представленное на Рисунок 15.

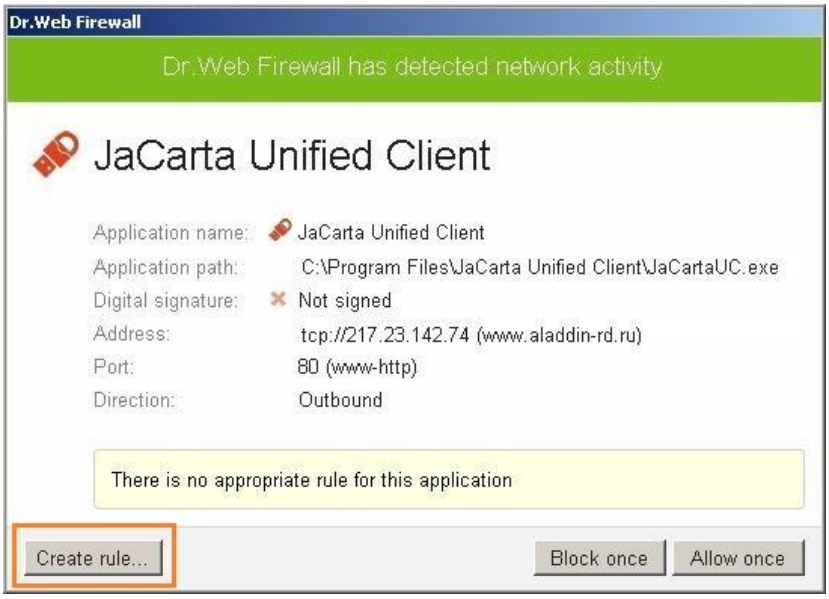


Рисунок 15 - Антивирус Dr.Web. Информационное окно

После появления данного окна необходимо создать правило для Dr.Web, согласно которому ПО Единый Клиент JaCarta сможет обращаться по адресу www.aladdin-rd.ru для проверки наличия обновлений и их установки.

Для создания правила следует нажать кнопку "Create rule". Далее в появившемся окне (см. Рисунок 16) необходимо раскрыть выпадающий список и выбрать одно из значений: "Allow network connections for application on 80" или "Allow all network connections" или "Create custom rule". После нажать "OK".

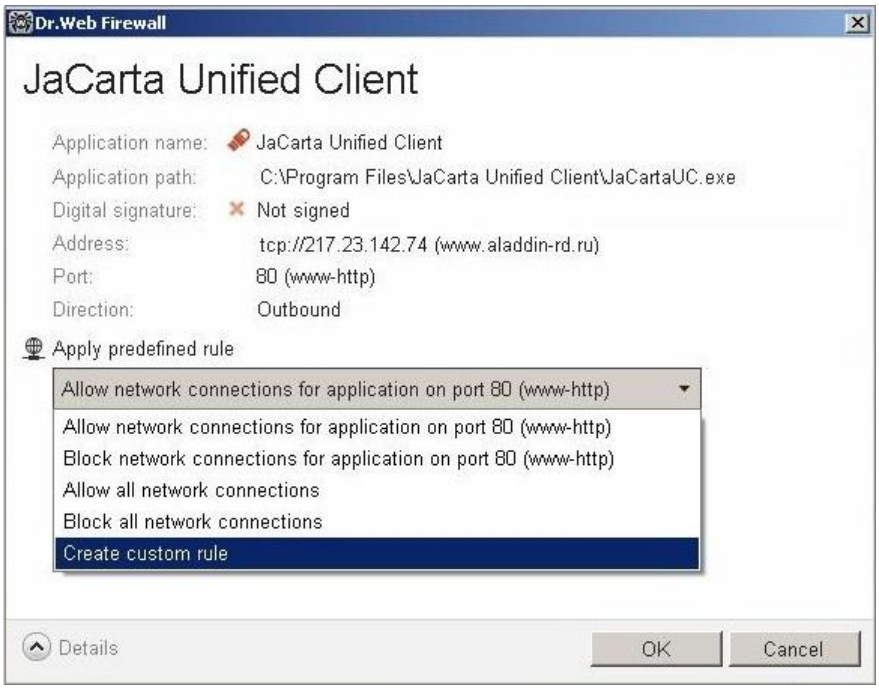


Рисунок 16 - Антивирус Dr.Web. Выбор правила

В случае, если была выбрана опция "Create custom rule", будет отображено окно (см. Рисунок 17), в котором необходимо нажать "OK" для завершения.

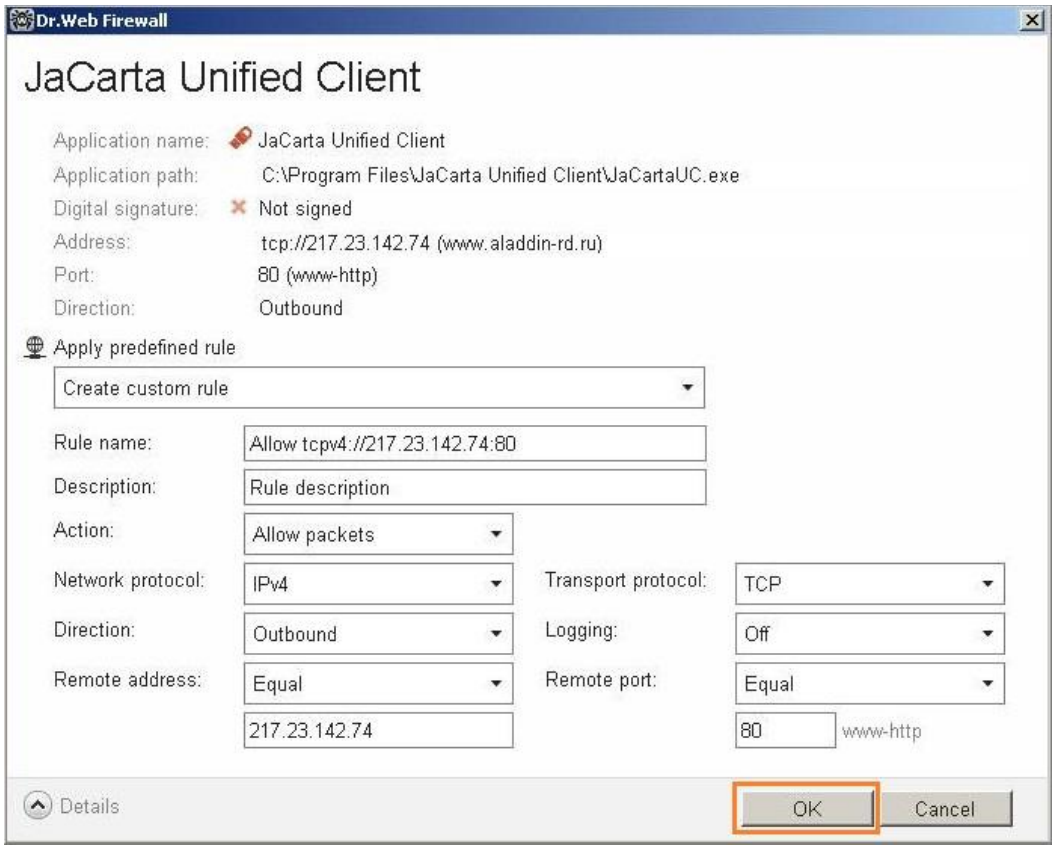


Рисунок 17- Антивирус Dr.Web. Завершение настройки правила

4.6 Установка программы в режиме командной строки

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 "OK". Будет открыто окно "Установщик Windows" со справкой о программе.

Имена пакетов установки Единого Клиента JaCarta приведены в п. 4.2 "Описание пакетов установки".

Для установки Единого Клиента 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 Единого Клиента JaCarta с помощью Windows Installer с необходимыми параметрами, например:

```
msiexec /i C:\JaCartaUnifiedClient_2.12.2.2260_win-x64_ru-Ru.msi
```

4.6.1 Параметры Единого Клиента JaCarta при установке в режиме командной строки

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

```
msiexec /i JaCartaUnifiedClient_2.12.2.2260_win-x64_ru-Ru.msi ПАРА-
МЕТР=ЗНАЧЕНИЕ ПАРАМЕТР=ЗНАЧЕНИЕ /qb
```

Список параметров установки Единый Клиент JaCarta при его установке в режиме командной строки представлен в таблице 6.

Таблица 7 – Параметры для установки Единого Клиента JaCarta в режиме командной строки

Параметр	Значение	Описание
INSTALL_BIO	0	Не устанавливать поддержку биометрии
	1	Установить поддержку биометрии
INSTALL_SECURLOGON	0	Не устанавливать Установить компонент SecurLogon
	1	Установить компонент SecurLogon
INSTALL_GINA	0	Установить GINA для биометрии (Microsoft Windows XP)
	1	Не устанавливать GINA для биометрии (Microsoft Windows XP)
INSTALL_CRYPTOPRO_JCP	0	Не устанавливать поддержку для CPRO JCP
	1	Установить поддержку для CPRO JCP. Установка возможна только при наличии установленного CPRO JCP и JRE.
INSTALL_CRYPTOPRO_CSP	0	Не устанавливать поддержку для CPRO CSP
	1	Установить поддержку для CPRO CSP. Установка возможна только при наличии установленного CPRO CSP
INSTALL_SIGNALCOM_CSP	0	Не устанавливать поддержку для SCOM CSP
	1	Установить поддержку для SCOM CSP Установка возможна только при наличии установленного SCOM CSP
INSTALL_BIO_CITRIX	0	Не устанавливать клиентский компонентов Citrix для биометрии
	1	Установить клиентский компонент Citrix для биометрии (0 или 1). Установка возможна только при наличии установленного Citrix-client
INSTALL_JACARTA_VR_DRIVER	0	Не устанавливать драйвер для возможности использования виртуальных считывателей JaCarta
	1	Установить драйвер для возможности использования виртуальных считывателей JaCarta
INSTALL_CCID_FIX	0	Не устанавливать драйвер поддержки работы с устаревшими моделями токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware
	1	Установить драйвер поддержки работы с устаревшими моделями токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware
INSTALL_JCPRO_CLIENT	0	Не устанавливать драйвер поддержки работы с моделями токенов JaCarta PKI с обратной совместимостью
	1	Установить драйвер поддержки работы с моделями токенов JaCarta PKI с обратной совместимостью
INSTALL_MICROSD_SC_READER	0	Не устанавливать драйвер поддержки работы с моделями токенов JaCarta в форм-факторе Secure MicroSD

Параметр	Значение	Описание
	1	Установить драйвера поддержки работы с моделями токенов JaCarta в форм-факторе Secure MicroSD
INSTALL_ASEDRIVE	0	Не устанавливать драйвер для возможности работы с устаревшими моделями смарт-карт ридеров Athena
	1	Установить драйвер для возможности работы с устаревшими моделями смарт-карт ридеров Athena
INSTALL_JACARTA_CCID_DRIVER	0	Не устанавливать драйвер для возможности использования JaCarta на Windows 8.1 x64
	1	Установить драйвер для возможности использования JaCarta на Windows 8.1 x64
INSTALL_ATHENA_CSP	0	Не устанавливать криптопровайдер Athena CSP
	1	Установить криптопровайдер Athena CSP
INSTALL_DEF_ATHENA_CSP	0	Установить Athena CSP в качестве криптопровайдера по умолчанию
	1	Не устанавливать Athena CSP в качестве криптопровайдера по умолчанию
INSTALL_JCWEBPASS	0	Не устанавливать утилиту JaCarta WebPass Tool
	1	Установить утилиту JaCarta WebPass Tool
INSTALL_TOKEN_MNG	0	Установить компонент Управление токеном
	1	Не устанавливать компонент Управление токеном
INSTALL_CA_MANAGER	0	Установить утилиту АРМ УЦ
	1	Не устанавливать утилиту АРМ УЦ
INSTALL_CERTS		Сертификаты для проверки подписи драйверов
INSTALL_MSVC80_CRT		Runtime от MS Visual Studio 2005 (для корректной работы частей от JC-Client)
INSTALL_MSVC90_CRT		Runtime от MS Visual Studio 2008 (для корректной работы JaCarta АРМ УЦ)
INSTALL_DIFXAPI		Difxapi.dll для работы custom actions исправляющих установку драйверов
INSTALL_JC_CLIENT		Установка JC-Client 6.40

Пример. Команда установки Единого Клиента JaCarta в режиме командной строки в случае задания дополнительных параметров:

```
msiexec.exe /i C:\JaCartaUnifiedClient_2.12.2.2260_win-x64_ru-Ru.msi
INSTALL_CCID_FIX=0 INSTALL_JCPRO_CLIENT=0 INSTALL_MICROSD_SC_READER=0
/qb
```

В данном примере будет выполнена установка Единого Клиента JaCarta со следующими параметрами:

- `INSTALL_CCID_FIX=0` – не устанавливать драйвер поддержки работы с устаревшими моделями токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware;

- `INSTALL_JCPRO_CLIENT=0` – не устанавливать драйвер поддержки работы с моделями токенов JaCarta PKI с обратной совместимостью;
- `INSTALL_MICROSD_SC_READER=0` – не устанавливать драйвер поддержки работы с моделями токенов JaCarta в форм-факторе Secure MicroSD;
- `/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").

4.7 Особенности отображения плитки Управление токеном после установки Единый Клиент JaCarta

После завершения установки Единый клиент JaCarta и перехода в экран блокировки Windows, будет отображен элемент управления "Управление токеном". Он появляется в случае, если в ходе установки был выбраны один из следующих видов: "Стандартная" или "Выборочная с компонентом Управление токеном" (см. Рисунок 18**).**

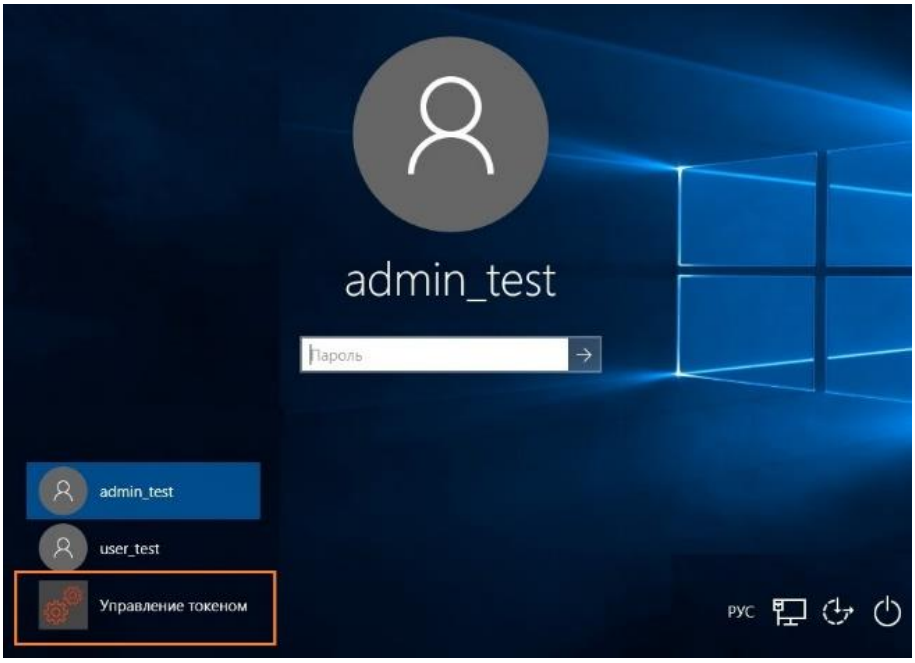


Рисунок 18 - Элемент управления на экране блокировки Windows

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:

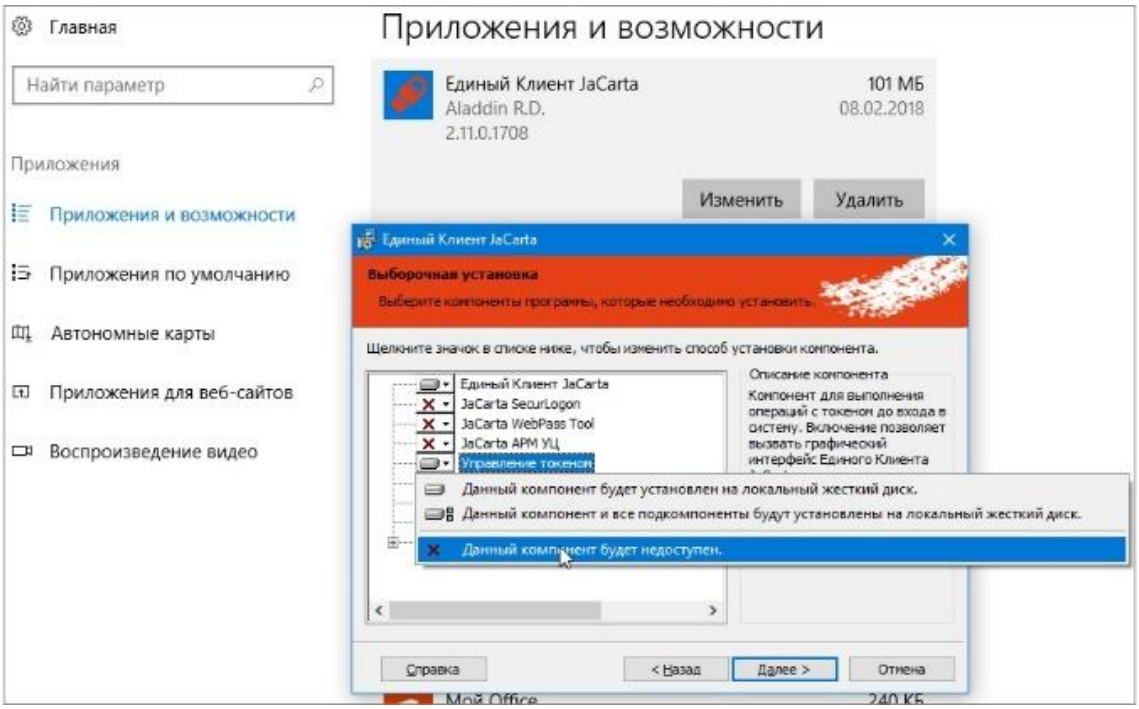


Рисунок 19 - Исключение компонента "Управление токеном"

5. Изменение, исправление, удаление программы

> *Перед удалением или обновлением Единого Клиента 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 Единого Клиента JaCarta включает в себя изменение перечня его установленных компонентов.

Для изменения Единого Клиента JaCarta:

1. Программы и компоненты". Будет открыто одноименное окно:

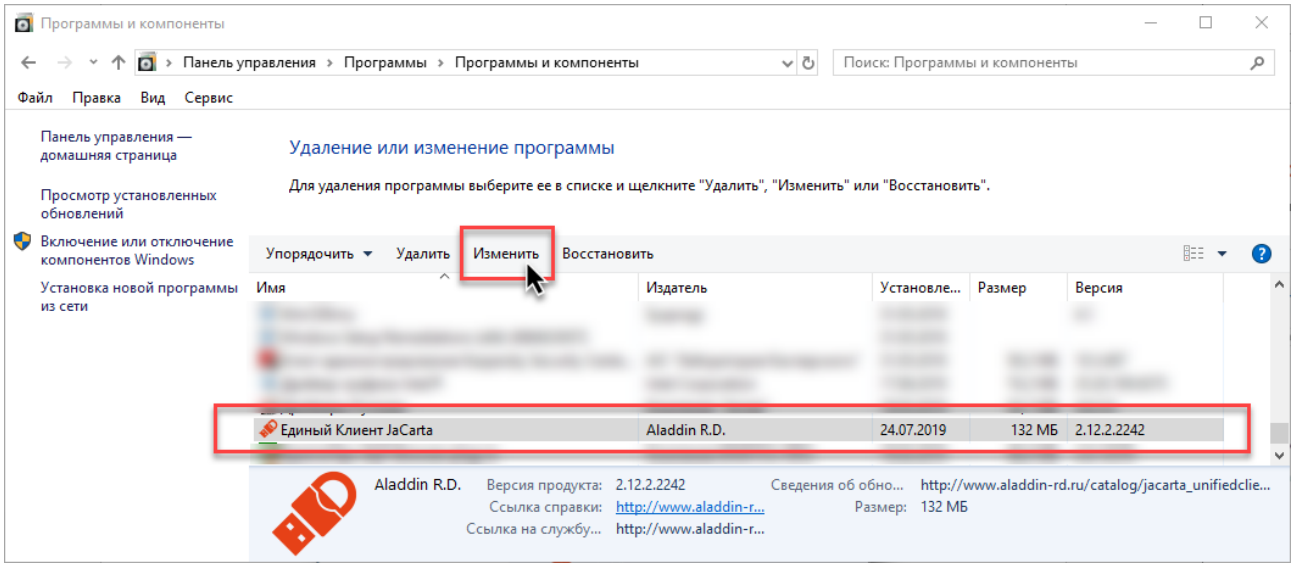


Рисунок 20 - Окно "Программы и компоненты". Изменение программы

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

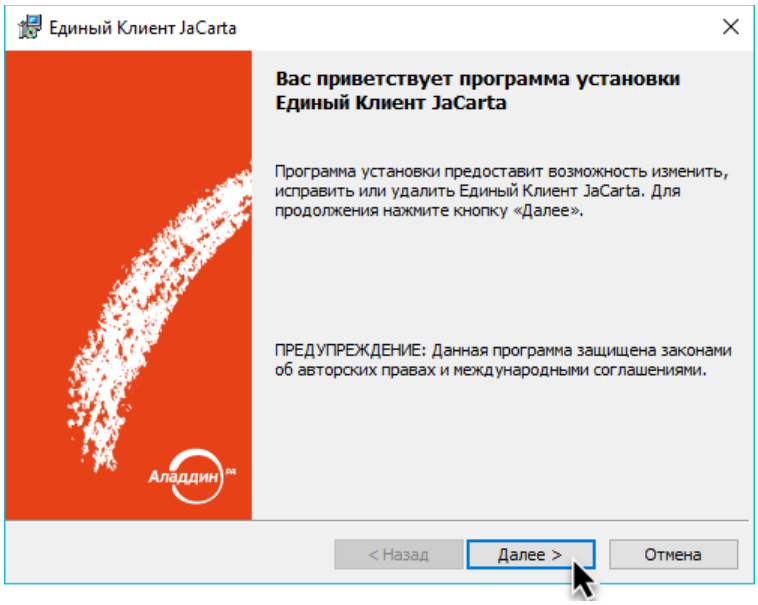


Рисунок 21 - Единый Клиент JaCarta. Окно приветствия мастера установки

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

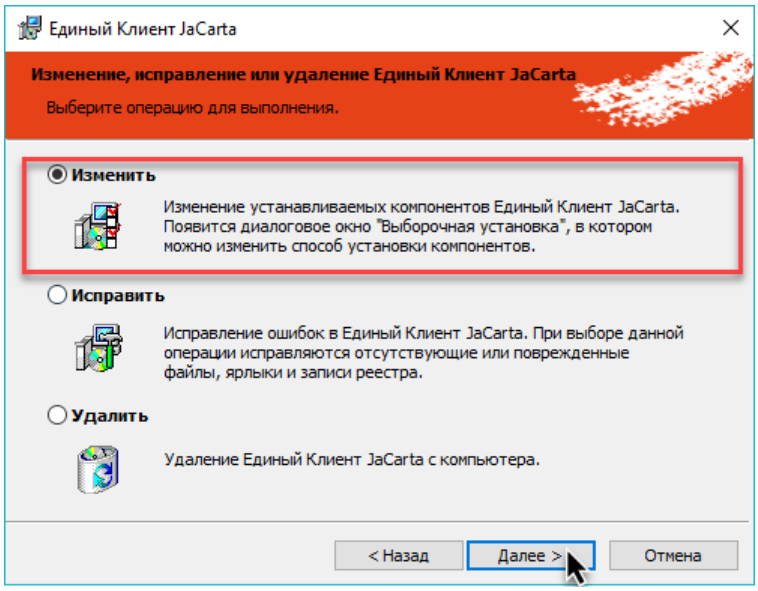


Рисунок 22 - Окно "Изменение, исправление или удаление Единый Клиент JaCarta"

4. Нажмите кнопку "Далее". Будет отображено окно "Выборочная установка компонентов Единый клиент JaCarta", в котором возможно изменить перечень установленных компонентов Единый Клиент JaCarta

5.2 Исправление программы

Исправление программы позволяет добавить отсутствующие или исправить поврежденные файлы, ярлыки и записи реестра Единый Клиент JaCarta.

Перед запуском процедуры исправления убедитесь, что пакет установки Единого Клиента JaCarta хранится по тому же пути, что и в ходе его установки.

Для исправления Единого Клиента JaCarta:

1. Выполните шаги 1, 2 процедуры изменения программы (см. п. 5.1 "Изменение программы").
2. В окне "Изменение, исправление или удаление Единый Клиент JaCarta" (см. рисунок 22) выберите опцию "Исправить".
3. Нажмите кнопку "Далее". Будет отображено окно "Исправление программы":

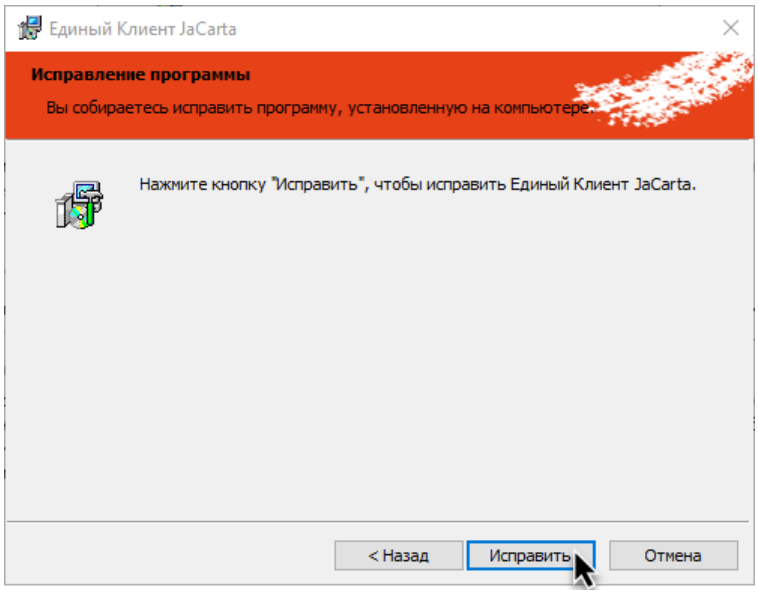


Рисунок 23 - Окно "Исправление программы"

4. Нажмите кнопку "Исправить". Будет выполняться поиск пакета установки Единого Клиента 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 Единого Клиента JaCarta:

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

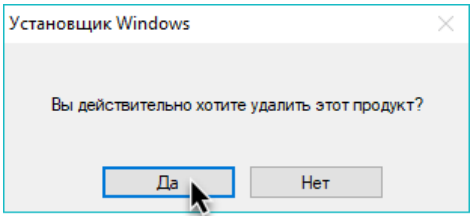


Рисунок 24 – Подтверждения удаления Единого Клиента JaCarta

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

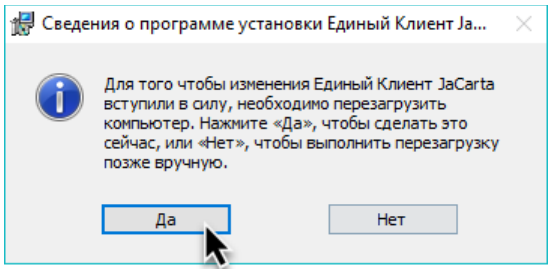


Рисунок 25 - Окно "Сведения о программе установки Единый Клиент JaCarta"

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 Единого Клиента 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 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 Единый Клиент JaCarta будет удален, перезагрузите компьютер.

6. Настройка работы программы

Для настройки Единого Клиента JaCarta:

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

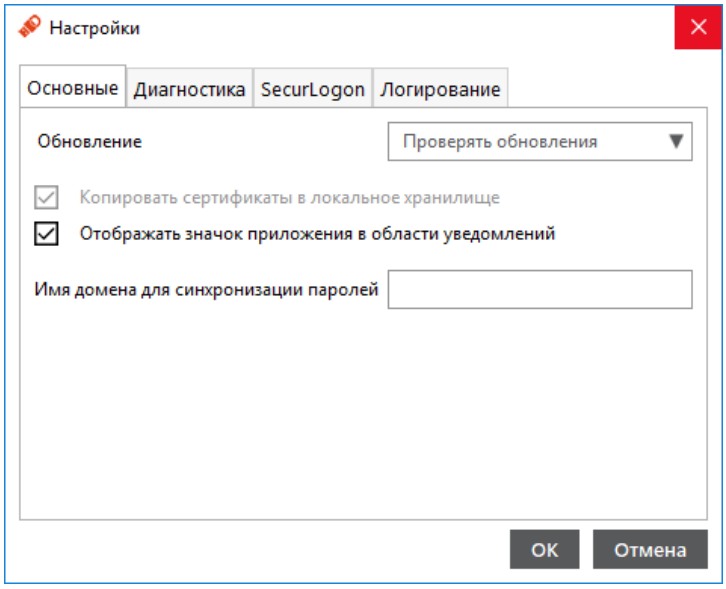


Рисунок 26 - Окно "Настройки". Вкладка "Основные"

2. Перейдите к нужной вкладке:
   - "Основные" – содержит основные настройки Единого Клиента JaCarta;
   - "Диагностика" – содержит команду для проверки целостности продукта;
   - "Логирование" – содержит настройки логирования Единого Клиента JaCarta;
   - "SecurLogon"[1];
   - "О программе" – предоставляет информацию о версии Единого Клиента JaCarta.
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"

6.2 Вкладка "Основные"

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

Таблица 8 – Вкладка "Основные". Описание настроек

Настройка	Описание
Обновление	Выпадающий список содержит два пункта: • "Не проверять обновления" - Единый Клиент JaCarta не будет проверять наличие обновлений;

[1] 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"

	• "Проверять обновления" - Единый Клиент JaCarta будет проверять наличие обновлений
Копировать сертификаты в локальное хранилище	Настройка нередактируемая в рамках работы с Единый Клиент JaCarta. Если флажок установлен, сертификаты в памяти подсоединённых электронных ключей будут копироваться в локальное хранилище сертификатов. Если необходимо снять данную галочку, необходимо в режиме изменения настроек запустить установку Единый Клиент JaCarta и на шаге "Дополнительные параметры работы" снять галочку "Установить для всех пользователей".
Отображать значок приложения в области уведомлений	Определяет, будет ли отображаться элемент управления  в области уведомлений.
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 11.Синхронизация паролей электронного ключа и учетной записи домена Windows.

6.3 Вкладка "Диагностика"

Описание настроек вкладки "Диагностика" (см. Рисунок 27) приведено в Таблица 9.

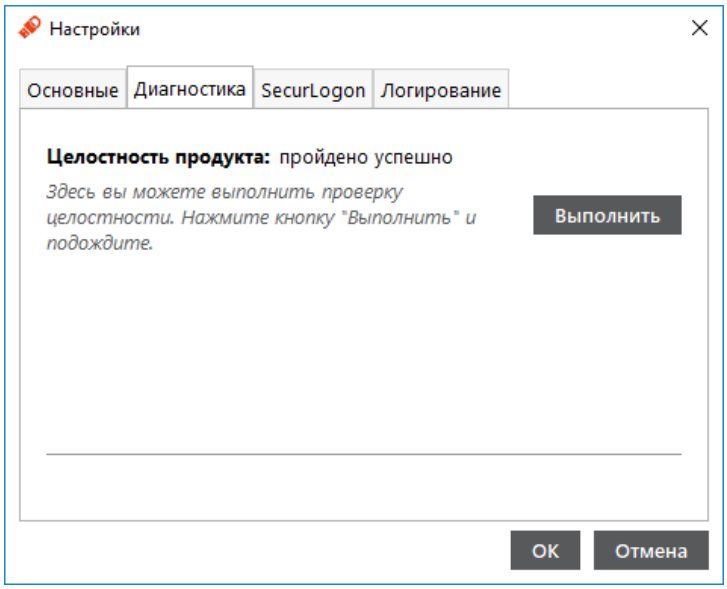


Рисунок 27 - Единый клиент JaCarta. Окно "Настройки". Вкладка "Диагностика"

Таблица 9 - Вкладка "Диагностика". Описание настроек

Настройка	Описание
Выполнить	Выполняется проверка целостности Единого Клиента JaCarta с последующим отображением результатов проверки (см. Рисунок 28)

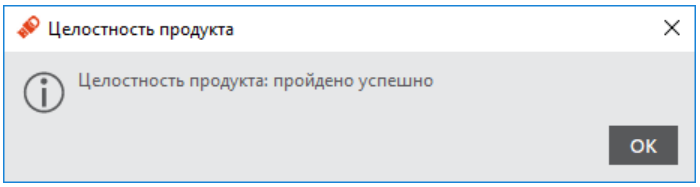


Рисунок 28 - Единый клиент JaCarta. Окно "Настройки". Вкладка "Диагностика". Информационное окно о результат проверки целостности

6.4 Вкладка "SecurLogon"

Если в ходе установки Единого Клиента JaCarta был установлен компонент SecurLogon, то вкладка "SecurLogon" будет отображена в окне "Настройки" (см. Рисунок 29). Описание настроек вкладки приведено в Таблица 10.

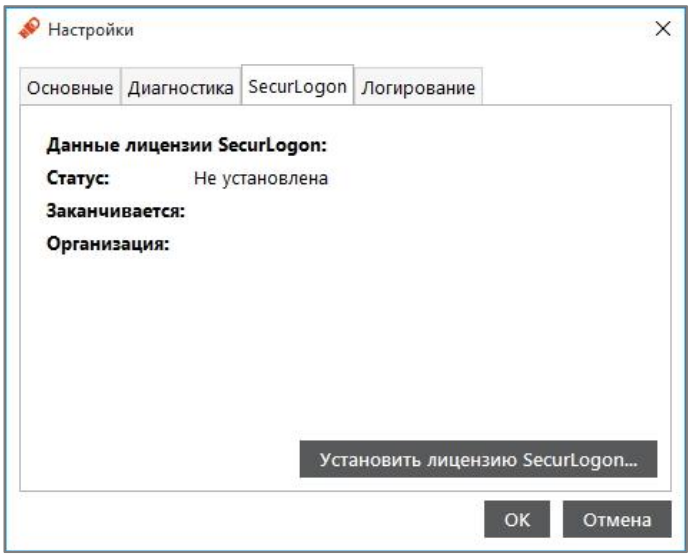


Рисунок 29 - Единый клиент JaCarta. Окно "Настройки". Вкладка "Диагностика"

Подробнее про работу с продуктом JaCarta Securlogon см. документе "JaCarta_SecurLogon_1.2_AdminGuide".

Таблица 10 - Вкладка "SecurLogon". Описание настроек

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

6.5 Вкладка "Логирование"

Описание окна "Настройки" на вкладке "Логирование" (см. Рисунок 30) приведено в Таблица 11.

> *Внимание! Подробнее об изменении настроек логирования через редактор реестра см. документ "Единый Клиент JaCarta. Инструкция по сбору диагностической информации".*
>
> *Подробные сведения о включении и настройках логирования так же изложены в базе знаний: http://kbp.aladdin-rd.ru/index.php?View=entry&EntryID=95*

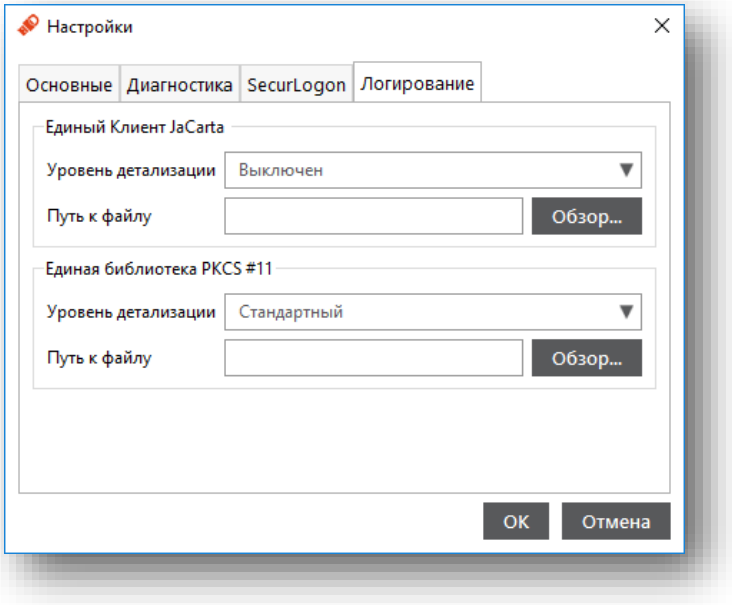


Рисунок 30 - Единый клиент JaCarta. Окно "Настройки". Вкладка "Логирование"

Таблица 11 - Вкладка "Логирование". Описание настроек

Настройка	Описание
Сегмент "Единый Клиент JaCarta"	Задает настройки логирования Единого Клиента JaCarta: • "Уровень детализации" – для выбора опций: Выключен / Стандартный. • 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

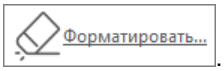
7. Форматирование электронных ключей

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

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 Единый Клиент JaCarta и переключитесь в режим администратора.
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" - 

. Отобразится окно "Форматирование приложения".

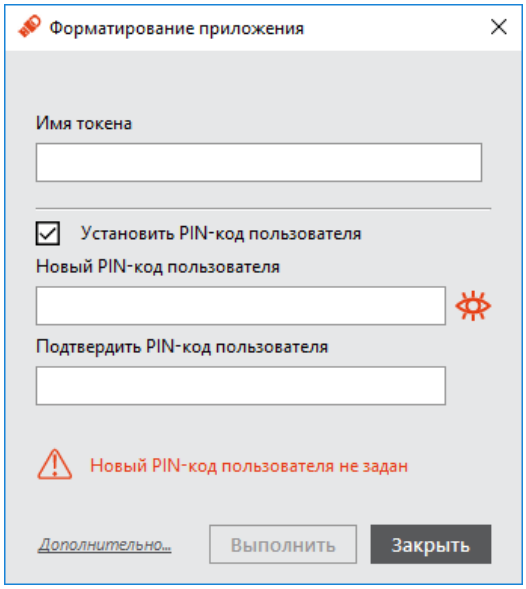


Рисунок 31 - Единый клиент JaCarta. Вкладка "PKI". Окно "Форматирование приложения"

5. Заполнить поля данными в соответствии с описанием, приведенным в Таблица 12.

Таблица 12 – Форматирование приложения. Окно "Форматирование приложения". Описание настроек

Поле	Описание
Имя токена	Задать в поле название электронного ключа (например, имя будущего владельца)
Установить PIN-код пользователя	Установить флажок, если нужно задать PIN-код пользователя на этапе форматирования. Если флажок отсутствует, PIN-код пользователя во время форматирования установлен не будет – его можно будет установить позже (для этого потребуется PIN-код администратора)

Новый PIN-код пользователя	Ввести значение PIN-кода пользователя (данное поле активно установленном флажке "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Повторно ввести значение PIN-кода пользователя

6. Для настройки дополнительных параметров форматирования нажмите кнопку "Дополнительно", в противном случае переходите к шагу 15 настоящей процедуры. После нажатия на кнопку "Дополнительно" будет открыто окно "Расширенные параметры форматирования токена" (см. Рисунок 32).

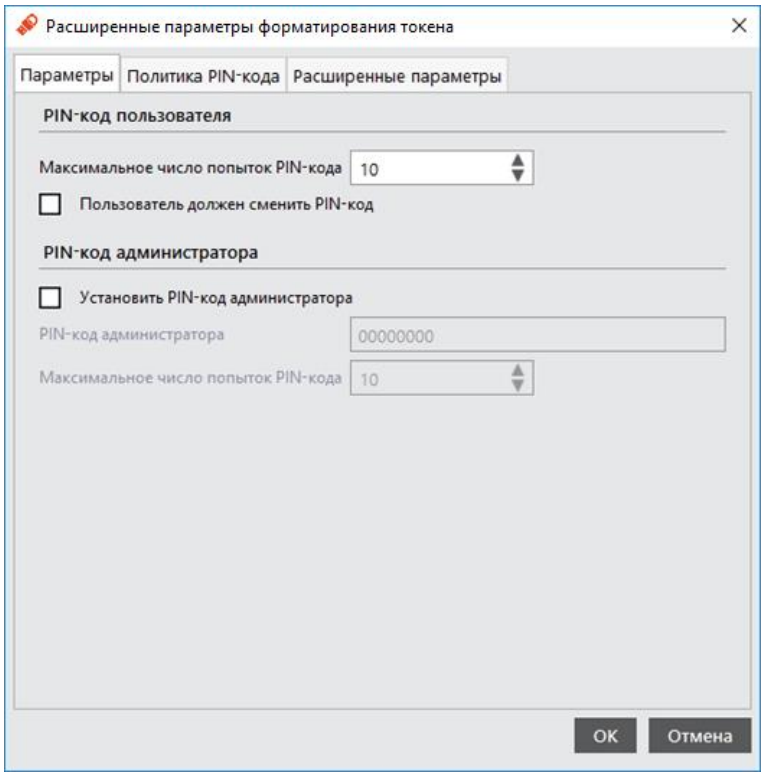


Рисунок 32 - Единый клиент JaCarta. Форматирование приложения. Окно "Расширенные параметры форматирования токена"

7. Произвести настройки параметров, руководствуясь описанием, приведенным в Таблица 13.

Таблица 13 – Форматирование приложения. Окно "Расширенные параметры форматирования токена"

Секция	Поле	Описание
PIN-код пользователя	Максимальное число 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	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	Установить PIN-код администратора	Если флажок установлен, в процессе форматирования будет задан PIN-код администратора

PIN-код администратора	Ввести значение PIN-кода администратора (поле активно при установленном флажке "Установить PIN-код администратора")
Максимальное число попыток PIN-кода	Максимальное количество неверных последовательных попыток ввода PIN-кода администратора, после которого возможность использования PIN-кода администратора будет заблокирована

8. Перейти на вкладку "Политика PIN-кода". Окно примет вид, приведенный на Рисунок 33.

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

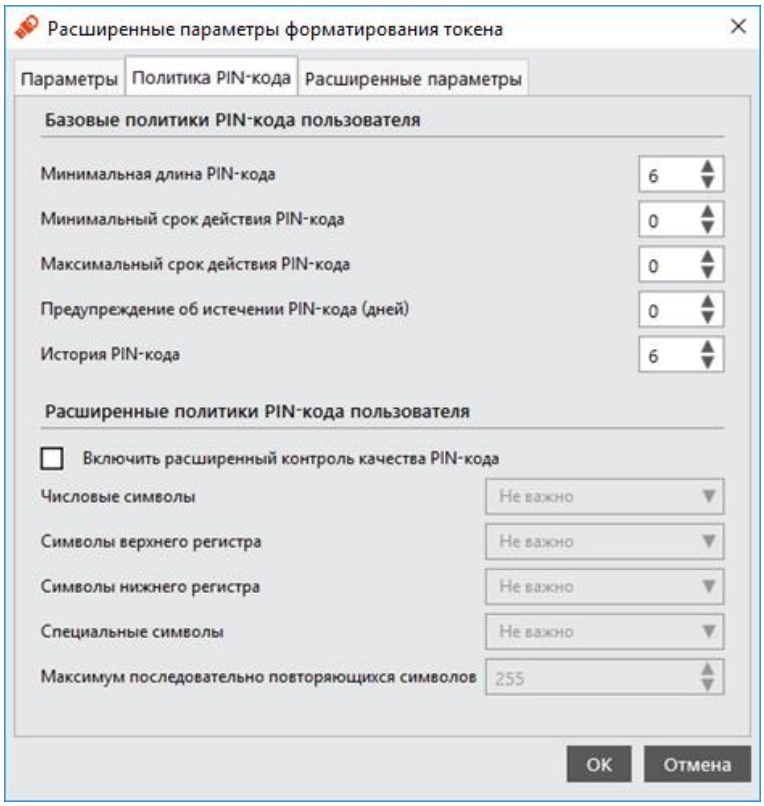


Рисунок 33 - Единый клиент JaCarta. Форматирование токена. Окно "Расширенные параметры форматирования токена". Вкладка "Политика PIN-кода"

9. Выполнить настройку. Описание дополнительных настроек на вкладке "Политика PIN-кода" приведено в Таблица 14.

Таблица 14 – Форматирование приложения. Окно "Расширенные параметры форматирования токена". Вкладка "Политика PIN-кода"

Секция	Поле	Описание
	Минимальная длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде

Базовые политики PIN-кода пользователя	Минимальный срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя
	Максимальный 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
Расширенные политики PIN-кода пользователя	Включить расширенный контроль 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

10. Перейти на вкладку "Расширенные параметры" (см. Рисунок 34).

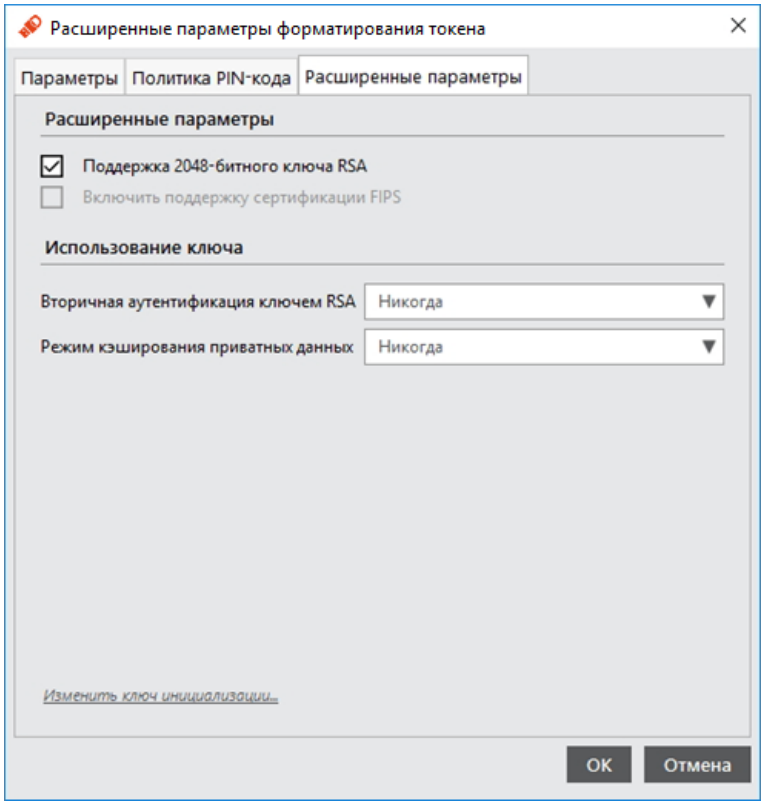


Рисунок 34 - Единый клиент JaCarta. Форматирование токена. Окно "Расширенные параметры форматирования токена". Вкладка "Расширенные параметры"

Выполнить настройку. Описание дополнительных настроек на вкладке "Расширенные параметры" приведено в Таблица 15.

Таблица 15 - Форматирование токена. Окно "Расширенные параметры форматирования токена". Вкладка "Расширенные параметры"

Секция	Поле	Описание
Расширенные параметры	Поддержка 2048-битного ключа RSA	Выбрать пункт для поддержки 2048-битных ключей RSA. Электронные ключи eToken PRO 32/64k не поддерживают эту опцию
	Включить поддержку сертификации FIPS	Выбрать пункт для форматирования устройств в режиме соответствия стандарту FIPS. FIPS (Federal Information Processing Standards) – утвержденный правительством США набор стандартов, направленных на улучшение управления и использования компьютерных и телекоммуникационных систем связи
Использование ключа	Вторичная аутентификация ключом RSA	Список содержит четыре пункта: • "Никогда" – вторичная аутентификация не производится; • "Предлагать по требованию приложения (Prompt conditional)" - в этом

	режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность; • "Всегда запрашивать у пользователя (Prompt always)" – при генерации RSA ключа, каждый раз запрашивается дополнительный пароль RSA для доступа к этому ключу. Однако пользователь может и не задавать дополнительный пароль, при этом генерация ключа продолжится без использования дополнительного пароля RSA; • "Всегда (Mandatory)" –при создании ключа RSA будет предложено задать дополнительный пароль для доступа к ключу. При нажатии кнопки "OK" генерируется ключ, введенный пароль используется в качестве дополнительного пароля RSA для этого ключа
Режим кэширования приватных данных	Список содержит три пункта: • "Никогда" – кэширование не производится; • "При входе пользователя" – кэширование производится при входе пользователя, данные сохраняются в кэше до завершения сеанса входа; • "Всегда" – кэширование производится всегда

11. Нажмите "OK", чтобы закрыть окно расширенных параметров форматирования электронного ключа.
12. В окне "Форматирование приложения" нажмите "Выполнить".
13. Подтвердите свой выбор в отобразившемся окне предупреждения.
14. При успешном процессе форматирования отобразится соответствующее сообщение – нажмите "OK", чтобы закрыть его.

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. Для выполнения форматирования необходим текущий PIN-код администратора.

7.2.1 Настройки форматирования

Для подготовки электронного ключа к работе необходимо выполнить следующие действия.

1. Запустить Единый Клиент JaCarta и перейти в режим администратора.

2. Подсоединить электронный ключ к компьютеру, выбрать его в левой панели интерфейса Единый Клиент JaCarta и в центральной части окна выберите вкладку "PKI".
3. Нажать кнопку "Форматировать". Будет открыто окно "Форматирование приложения" (см. Рисунок 35).

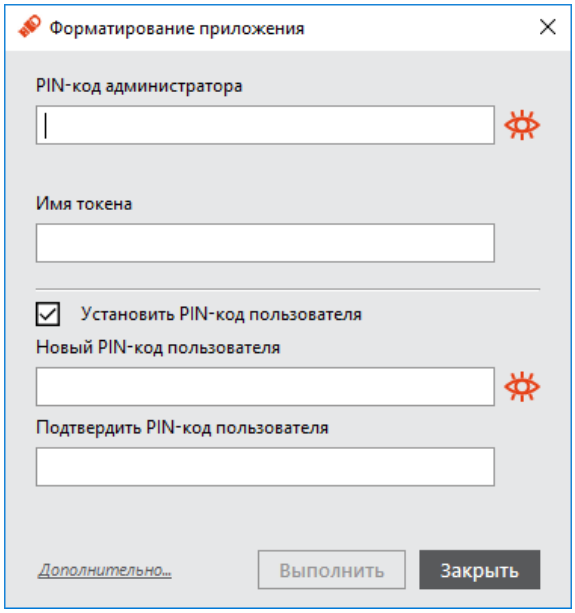


Рисунок 35 - Единый клиент JaCarta. Форматирование токена. Окно "Форматирование приложения"

4. Выполнить настройку. Описание общих параметров форматирования приведено в Таблица 16.

Таблица 16 – Окно "Форматирование приложения"

Поле	Описание
PIN-код администратора	Ввести текущий PIN-код администратора
Имя токена	Ввести название электронного ключа (например, это могут быть имя и фамилия будущего владельца)
Установить PIN-код пользователя	Установить флажок, если хотите задать PIN-код пользователя во время форматирования. Можно не задавать PIN-код пользователя, если: • используется электронный ключ с приложением PKI/BIO, и вы хотите установить для пользователя только биометрическую аутентификацию (подробнее см. Таблица 17); • необходимо задать PIN-код пользователя позже. В этом случае для последующей установки PIN-кода пользователя необходимо будет предъявить PIN-код администратора
Новый PIN-код пользователя	Ввести новый PIN-код пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")
Подтвердить PIN-код пользователя	Ввести подтверждение нового PIN-кода пользователя (поле активно, если установлен флажок "Установить PIN-код пользователя")

5. Для настройки дополнительных параметров форматирования нажмите кнопку "Дополнительно", в противном случае переходите к шагу 13 настоящей процедуры. После нажатия "Дополнительно" будет открыто окно "Расширенные параметры форматирования токена" (см. Рисунок 36).

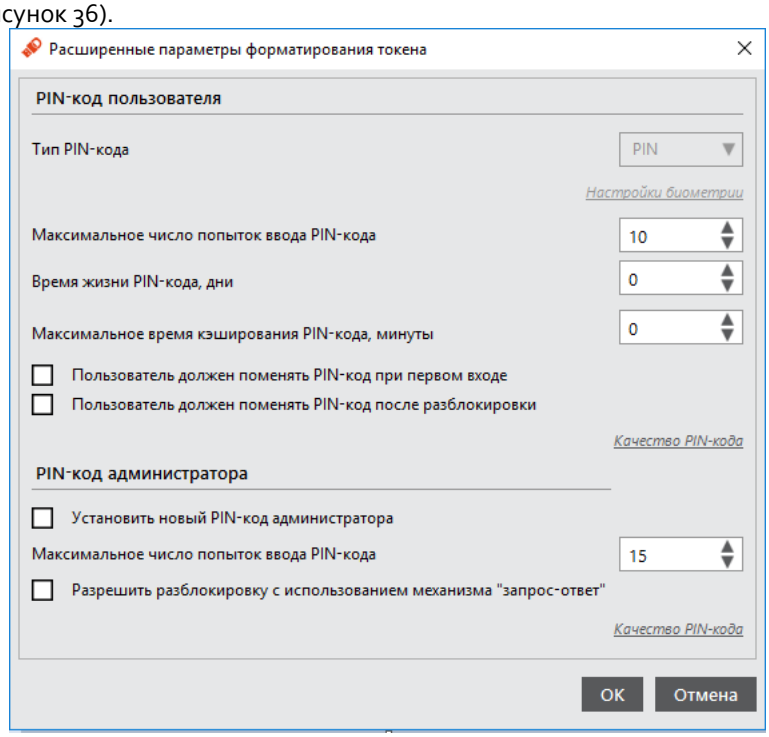


Рисунок 36 - Единый клиент JaCarta. Форматирование токена. Окно "Расширенные параметры форматирования токена"

6. Выполнить настройку согласно описанию расширенных параметров форматирования, приведенному в Таблица 17.

Таблица 17 - Единый клиент JaCarta. Форматирование токена. Окно "Расширенные параметры форматирования токена"

Секция	Настройка	Описание
PIN-код пользователя	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 пальцев (только для электронных ключей с приложением PKI/BIO)
	Максимальное число попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя

	Время жизни PIN-кода	Количество дней, спустя которое пользователь должен будет сменить PIN-код пользователя
	Максимальное время кэширования PIN-кода	В течение какого времени (в минутах) PIN-код пользователя будет кэшироваться на компьютере, к которому подсоединён электронный ключ
	Пользователь должен поменять PIN-код при первом входе	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
PIN-код администратора	Установить новый PIN-код администратора	Установка флажка делает доступными поля для ввода нового PIN-кода администратора и для его повторного подтверждения
	PIN-код администратора	Введите значение нового PIN-кода администратора. Ключ администратора может быть: • значением, соответствующим установленному качеству паролей (см. качество PIN-кода ниже); • ключом 3DES (если установлен флажок "Разрешить разблокировку с использованием механизма “запрос-ответ”")
	Максимальное число попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора
	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

7. Задать настройки качества PIN-кода пользователя и PIN-кода администратора можно с помощью элемента управления "Качество PIN-кода" в соответствующих секциях. Окно настроек качества PIN-кода пользователя представлено на Рисунок 37. Описание настроек качества PIN-кода приведено в Таблица 18.

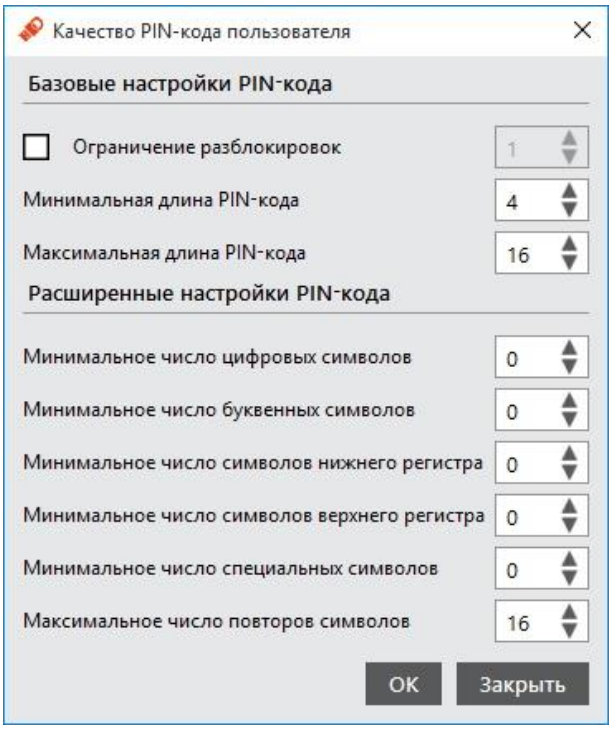


Рисунок 37 - Единый клиент JaCarta. Форматирование токена. Окно "Качество PIN-кода пользователя"

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

8. Нажмите "OK" для сохранения настроек.

Таблица 18 - Единый клиент JaCarta. Форматирование токена. Окно "Качество PIN-кода пользователя"

Секция	Настройка	Описание
Базовые настройки PIN-кода	Ограничение разблокировок	Установите флажок и задайте количество возможных разблокировок заблокированного PIN-кода
	Минимальная длина PIN-кода	Минимальное число символов в PIN-коде
	Максимальная длина PIN-кода	Максимальное число символов в PIN-коде
Расширенные настройки PIN-кода	Минимальное число цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Минимальное число буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде

Минимальное число символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
Минимальное число символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде
Минимальное число специальных символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
Максимальное число повторов символов	Определяет число повторяющихся символов в любом месте PIN-кода

9. Выполните следующие действия в зависимости от приложения, установленного на электронном ключе:
   - **PKI** – переходите к шагу 13 настоящей процедуры.
   - **PKI/BIO** – если в поле "Тип PIN-кода" выбрано значение "BIO", "PIN или BIO" или "PIN и BIO", нажмите "Настройки биометрии". Будет открыто окно "Настройки биометрии" (см. Рисунок 38).

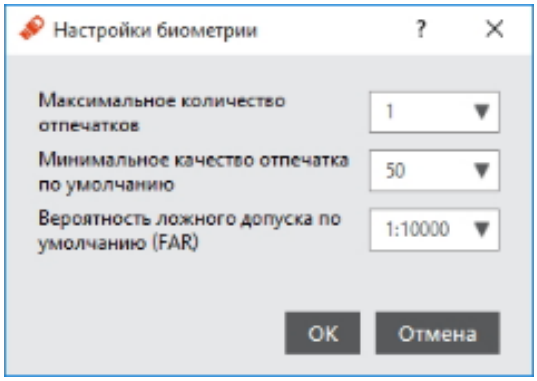


Рисунок 38 - Единый клиент JaCarta. Форматирование токена. Окно "Настройки биометрии"

10. Осуществить настройку параметров, описание которых приведено Таблица 19.

Таблица 19 - Единый клиент JaCarta. Форматирование токена. Окно "Настройки биометрии"

Настройка	**Описание**
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 иденти-

фикации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000

11. Нажмите "OK", чтобы сохранить изменения настроек биометрии.
12. Нажмите "OK", чтобы закрыть окно дополнительных настроек форматирования.
13. В окне форматирования электронного ключа нажмите "Выполнить" и подтвердите свой выбор в отобразившемся окне предупреждения.

Если вы инициализируете электронный ключ с поддержкой биометрии следует руководствоваться п.7.2.2.Форматирование с биометрическими параметрами.

14. В случае успешного форматирования токена отобразится соответствующее сообщение. Для его закрытия необходимо нажать кнопку "OK".

7.2.2 Форматирование с биометрическими параметрами

Если вы форматируете электронный ключ с биометрическими настройками, через некоторое время после запуска процесса форматирования отобразится окно "Регистрация отпечатков" (см. Рисунок 39).

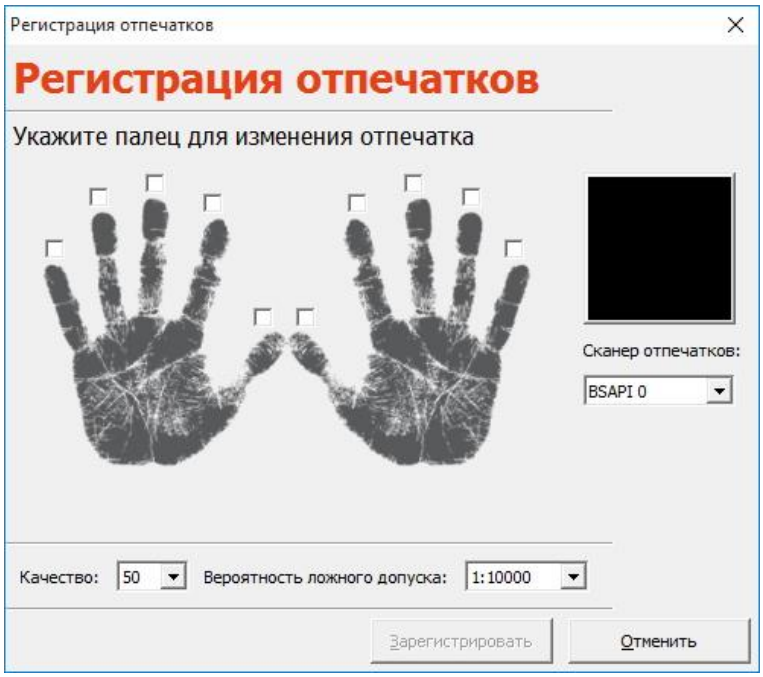


Рисунок 39 - Единый клиент JaCarta. Окно "Регистрация отпечатков"

1. На схематическом изображении ладоней отметьте галочкой палец, который будет отсканирован во время форматирования (см. Рисунок 40).

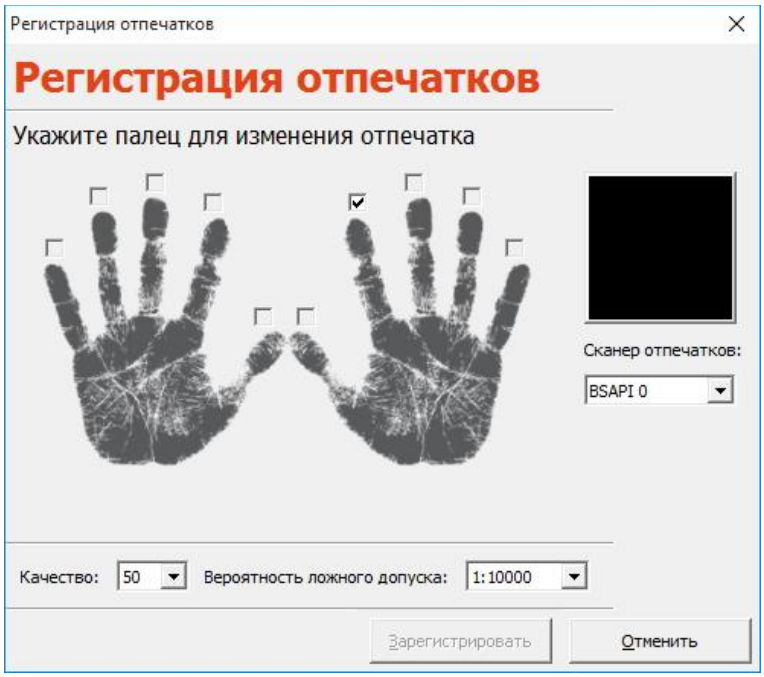


Рисунок 40 - Единый клиент JaCarta. Окно "Регистрация отпечатков". Выбор пальца для сканирования

2. При необходимости измените дополнительные параметры сканирования. Описание дополнительных параметров сканирования приведено в Таблица 20.

Таблица 20 - Единый клиент JaCarta. 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

3. Будущий владелец электронного ключа должен приложить отмеченный палец к сканеру отпечатков пальцев. После считывания отпечаток пальца отобразится в окне (см. Рисунок 41).

Рисунок 41 - Единый клиент JaCarta. Окно "Регистрация отпечатков". Результат считывания отпечатка пальца

4. После того, как приложенный палец будет убран со сканера отпечатков, будет отображено информационное окно (см. Рисунок 42). Для закрытия окна нажмите кнопку "OK".

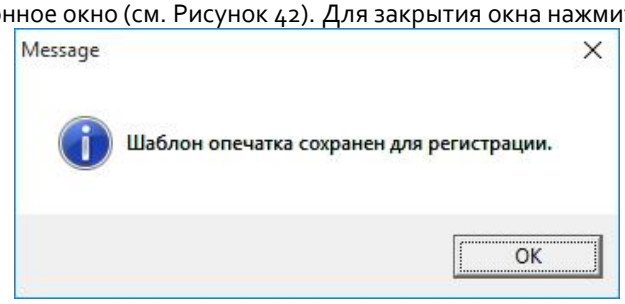


Рисунок 42 - Единый клиент JaCarta. Окно "Регистрация отпечатков". Информационное сообщение о сохранении отпечатка

5. В окне регистрации отпечатков станет доступной для нажатия кнопка "Зарегистрировать". Нажмите кнопку "Зарегистрировать". Будет отображено информационное окно с результатом регистрации отпечатка (см. Рисунок 43). Для закрытия окна нажмите кнопку "OK".

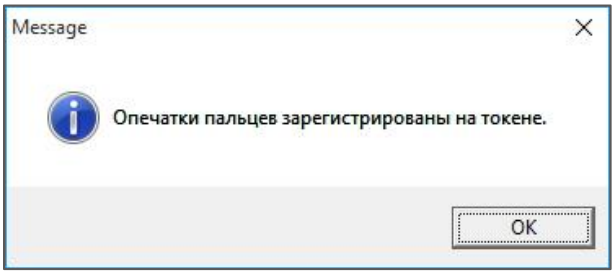


Рисунок 43 - Единый клиент JaCarta. Окно "Регистрация отпечатков". Информационное сообщение о регистрации отпечатка

6. Если в настройках форматирования было указано, что в памяти электронного ключа нужно сохранить несколько отпечатков пальцев, повторите необходимые шаги настоящей процедуры для сохранения их всех.
7. При успешном завершении форматирования отобразится соответствующее сообщение (см. Рисунок 44). Нажмите "OK" для его закрытия.

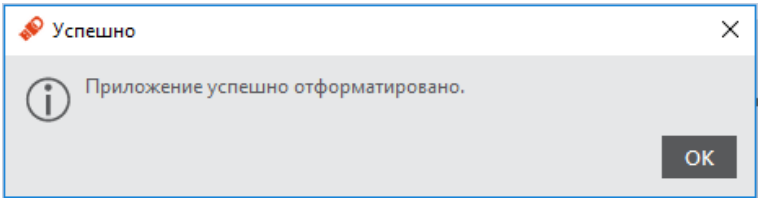


Рисунок 44 - Единый клиент JaCarta. Окно "Регистрация отпечатков". Информационное сообщение о форматировании приложения

7.3 Форматирование приложения ГОСТ и STORAGE

Для подготовки электронного ключа к работе:

1. Запустить Единый Клиент JaCarta и перейти в режим администратора.
2. Подсоединить нужный электронный ключ к компьютеру, выбрать его в левой панели и в центральной части окна в зависимости от того, какое приложение установлено на ключе, выбрать вкладку "ГОСТ" или "STORAGE".
3. Нажать кнопку "Форматировать". Будет открыто окно "Форматирование приложения" (см. Рисунок 45).

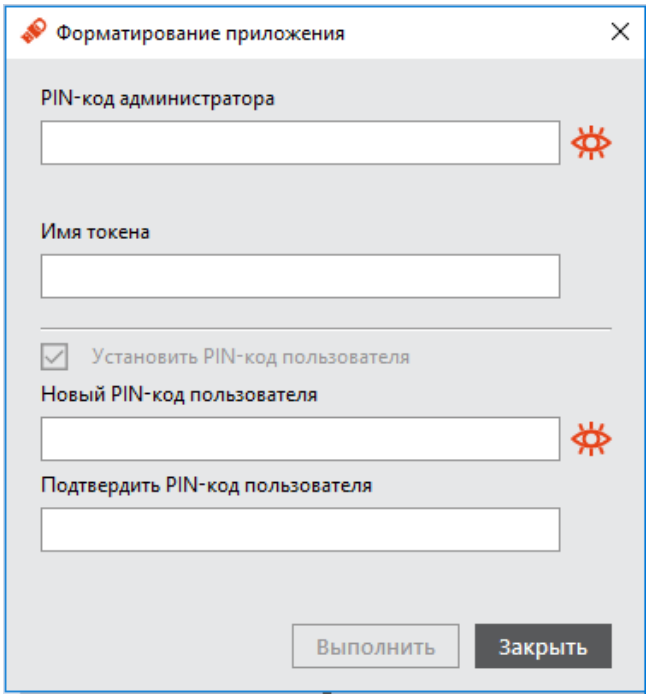


Рисунок 45 - Единый клиент JaCarta. Окно "Форматирование приложения"

4. Выполнить настройку. Описание настроек форматирования электронного ключа приведено ниже:

Таблица 21 - Единый клиент JaCarta. Окно "Форматирование приложения". Описание настроек

Настройка	Описание

PIN-код администратора	Поле для ввода текущего PIN-код администратора
Имя токена	Поле для ввода названия форматируемого приложения
Установить PIN-код пользователя	• Для форматирования приложения ГОСТ – установить флажок, если необходимо задать PIN-код пользователя на этапе форматирования. Также можно снять флажок и задать PIN-код пользователя позже; • Для форматирования приложения STORAGE - 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 "Выполнить" и подтвердите свой выбор в окне с предупреждающим сообщением.
6. При успешного форматирования будет отображено соответствующее сообщение. Нажмите кнопку "ОК" для его закрытия.

7.4 Приложение ГОСТ с апплетом Криптотокен 2

Для подготовки электронного ключа к работе:

1. Запустить Единый клиент JaCarta и перейти в режим администратора.
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 пользователем". Будет открыто окно "Форматирование приложения пользователем" (см. **Ошибка! Источник ссылки не найден.**).

Рисунок 46 - Единый клиент JaCarta. Окно "Форматирование приложения пользователем"

4. Заполнить поля "Имя токена" и "Введите PIN-код пользователя", после чего нажмите кнопку "Выполнить".
5. Будет отображено информационное сообщение с информацией о том, что в ходе процесса форматирования все данные будут удалены из памяти токена (см. Рисунок 47). Для продолжения процесса форматирования приложения необходимо нажать кнопку "Продолжить".

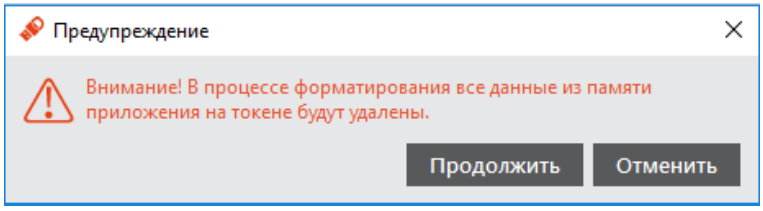


Рисунок 47 - Единый клиент JaCarta. Окно "Предупреждение"

6. В информационном окне о результатах форматирования (см. Рисунок 48) нажать кнопку "OK" для завершения процесса.

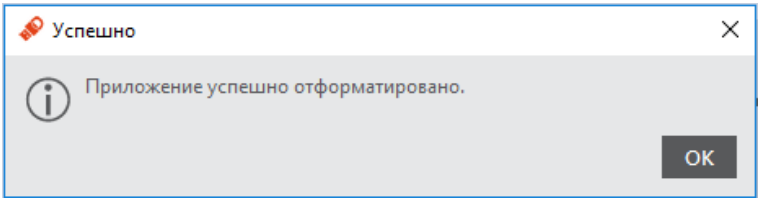


Рисунок 48 - Единый клиент JaCarta. Информационное сообщение о результатах процесса форматирования

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 7 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 Единый Клиент JaCarta, перейдя на вкладку "Информация о токене" и посмотрев значение, указанное в поле "Осталось попыток ввода PIN-кода".

Для смены PIN-код пользователя администратором:

1. Подсоединить электронный ключ, на котором необходимо установить/сменить PIN-код пользователя. Запустить Единый Клиент JaCarta и перейти в режим администратора.
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 "Установка PIN-кода пользователя":

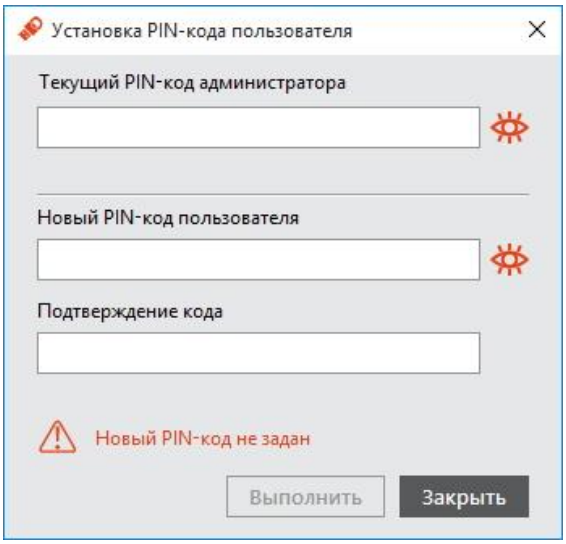


Рисунок 49 - Окно "Установка PIN-кода пользователя"

4. В поле "Текущий PIN-код администратора" ввести текущий PIN-код администратора.
5. В полях "Новый PIN-код пользователя" и "Подтверждение PIN-кода" указать соответственно новый PIN-код пользователя и подтверждение.
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-код пользователя:

1. Подсоединить электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустить Единый Клиент JaCarta и перейти в режим администратора.
3. В левой панели Единого Клиента JaCarta выбрать нужный электронный ключ и в центральной части перейти на вкладку "PKI".
4. Если PIN-код пользователя заблокирован кнопка "Разблокировать PIN-код пользователя" будет доступна для нажатия (см. Рисунок 50). Иначе кнопка заблокирована.

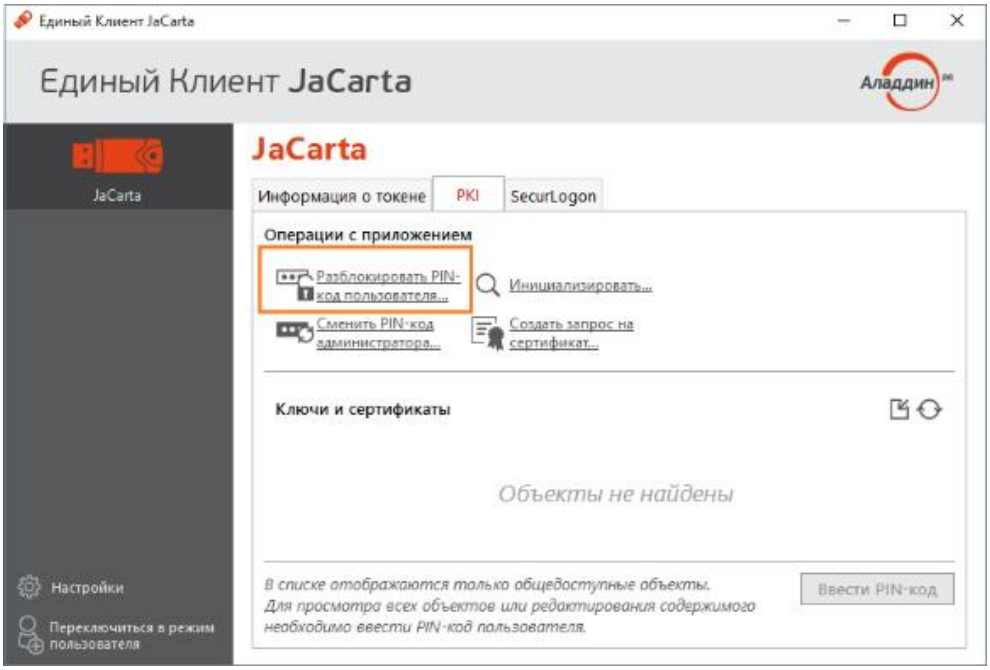


Рисунок 50 - Единый клиент JaCarta. Элемент управления "Разблокировать PIN-код"

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

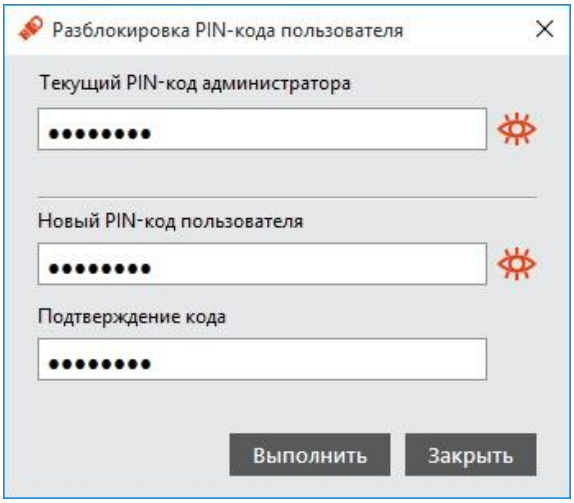


Рисунок 51 - Единый клиент JaCarta. Окно "Разблокировать PIN-кода"

6. В поле "PIN-код администратора" ввести текущий PIN-код администратора.
7. В полях "Новый PIN-код пользователя" и "Подтвердить PIN-код пользователя" ввести новые PIN-код пользователя и его подтверждение соответственно. После чего нажать кнопку "OK".
8. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение (см. Рисунок 52) – нажать кнопку "OK", чтобы закрыть его.

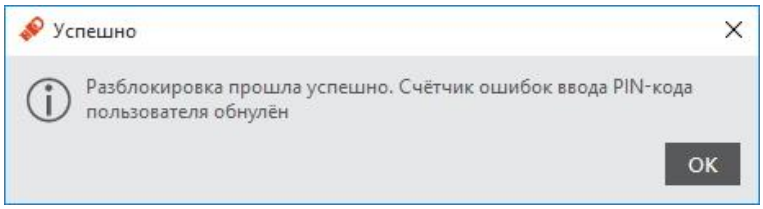


Рисунок 52 - Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.2.2 Приложение ГОСТ с апплетом Криптотокен и приложение STORAGE

Для разблокирования PIN-код пользователя:

1. Подсоединить электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустить Единый Клиент JaCarta и перейти в режим администратора.
3. В левой панели Единого Клиента JaCarta выбрать нужный электронный ключ и в центральной части перейти на вкладку "ГОСТ" или "STORAGE".
4. Если PIN-код пользователя заблокирован, кнопка "Разблокировать PIN-код " будет доступна для нажатия (см. Рисунок 53)

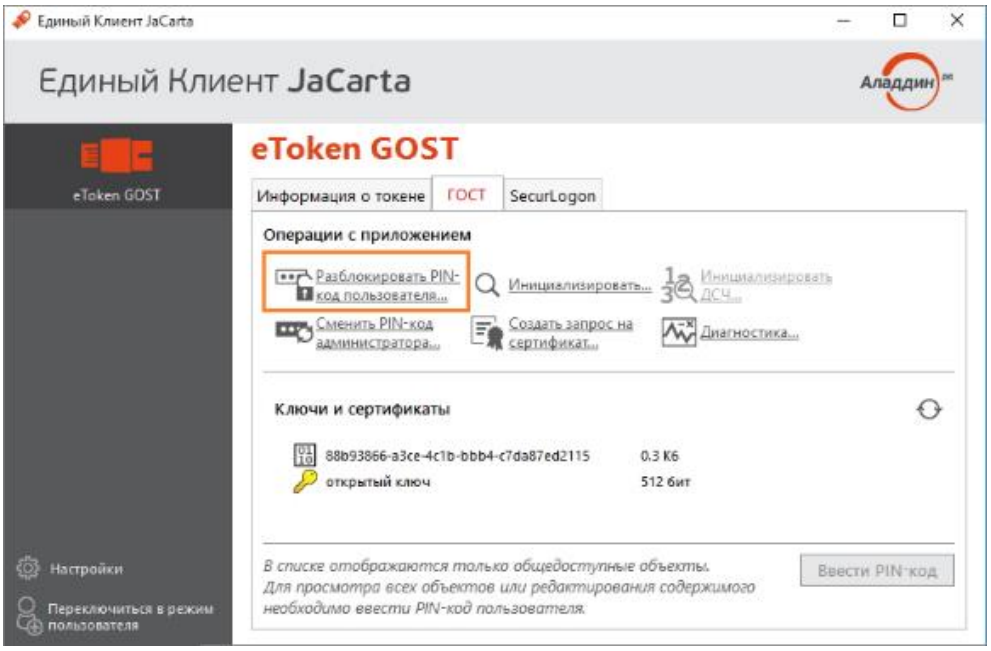


Рисунок 53 - Единый клиент JaCarta. Элемент управления "Разблокировать PIN-код"

5. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно с предупреждением о том, что в ходе процесса разблокировки будет обнулен счетчик попыток ввода PIN-кода (см. Рисунок 54).

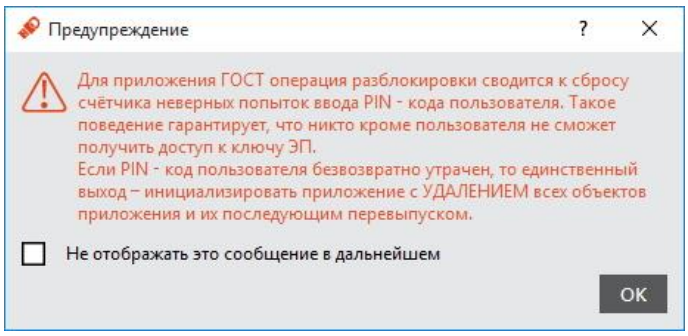


Рисунок 54 - Единый клиент JaCarta. Окно с предупреждением об обнуление счетчика ввода PIN-кода

6. Нажать кнопку "OK" для продолжения процесса разблокировки. Будет открыто окно "Разблокировать PIN-код" (см. Рисунок 55).

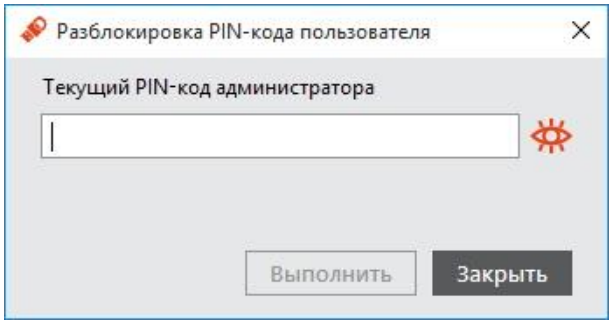


Рисунок 55 - Единый клиент JaCarta. Окно "Разблокировать PIN-код"

7. 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.

8. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. Рисунок 56). Нажать кнопку "OK", чтобы закрыть его.

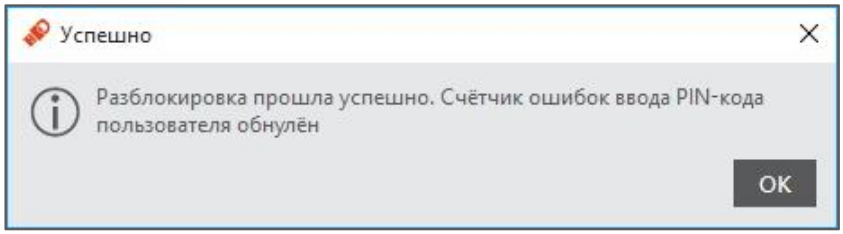


Рисунок 56 - Единый клиент JaCarta. Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.2.3 Приложение ГОСТ с апплетом Криптотокен 2

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

Для разблокирования PIN-код пользователя:

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

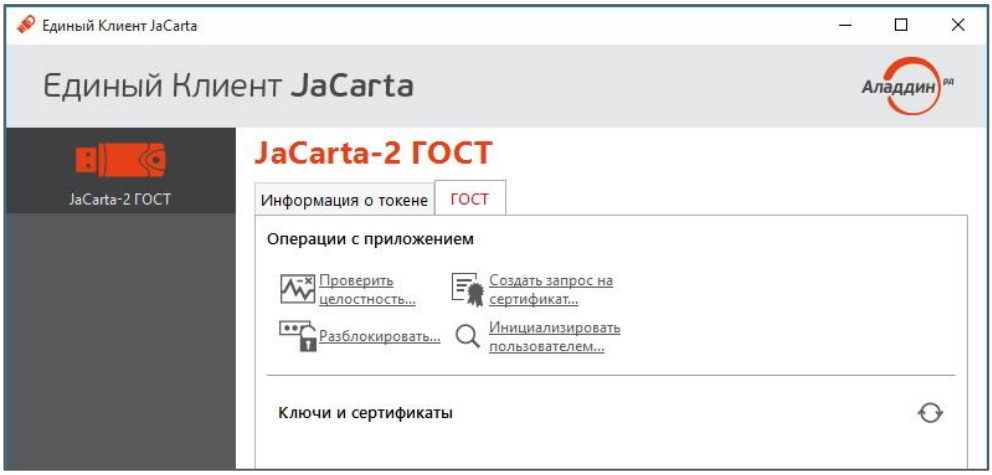


Рисунок 57 - Элемент управления "Разблокировать PIN-код пользователя"

5. После нажатия на кнопку "Разблокировать PIN-код пользователя" будет открыто окно "Мастер разблокирования PIN-кода пользователя" (см. Рисунок 58).

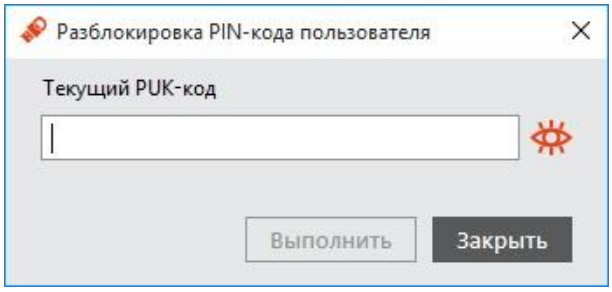


Рисунок 58 - Единый клиент JaCarta. Окно "РазблокировкаPIN-кода пользователя"

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

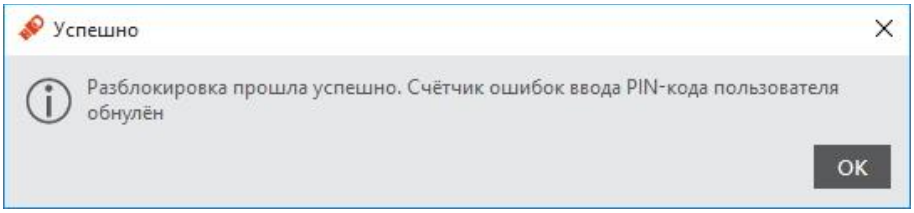


Рисунок 59 - Единый клиент JaCarta. Информационное сообщение об успешной разблокировке PIN-кода пользователя

8.3 Разблокирование PIN-кода пользователя в удалённом режиме

Разблокировка PIN-кода пользователя в удалённом режиме доступна только для электронных ключей с приложениями PKI с апплетом PRO и приложением ГОСТ с апплетом Криптотокен 2.

8.3.1 Приложение PKI с апплетом PRO

В результате разблокирования PIN-кода пользователя электронного ключа с приложением PKI с апплетом PRO 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 PRO 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;
- электронный ключ должен быть отформатирован с заданным PIN-кодом администратора (см. п. 7.1 Форматирование приложения PKI с апплетом PRO).

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 разблокировки PIN-код пользователя в удалённом режиме необходимо выполнить следующие действия:

1. Проинструктировать пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом к компьютеру и запустить Единый Клиент JaCarta. Окно Единый Клиент JaCarta у пользователя будет выглядеть как на Рисунок 60.

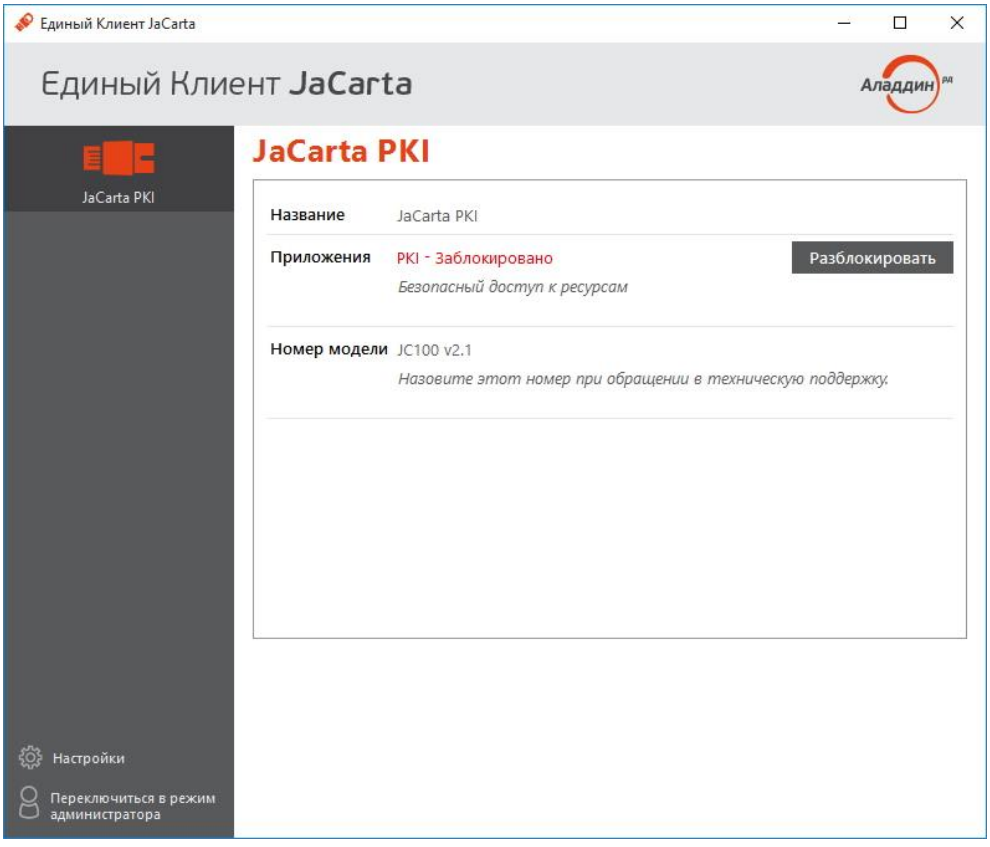


Рисунок 60 – Единый Клиент JaCarta. Отображение заблокированного PIN-кода у пользователя

1. Пользователь должен нажать кнопку "Разблокировать". На экране пользователя будет открыто окно "Разблокировка PIN-кода пользователя" (см. Рисунок 61).

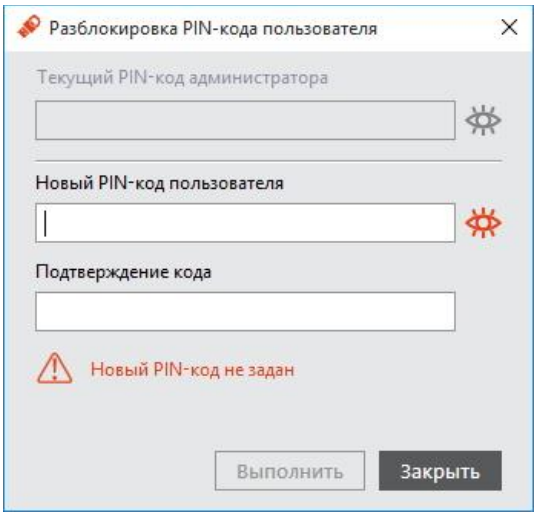


Рисунок 61 - Единый Клиент JaCarta. Окно "Разблокировка PIN-кода пользователя"

2. В полях "Новый PIN-код пользователя" и "Подтверждение PIN-кода" пользователь должен ввести новое значение PIN-кода пользователя и его подтверждение соответственно. После чего пользователь должен нажать кнопку "Выполнить". На экране пользователя будет открыто окно "Запрос/Ответ: JaCarta PKI" (см. Рисунок 62).

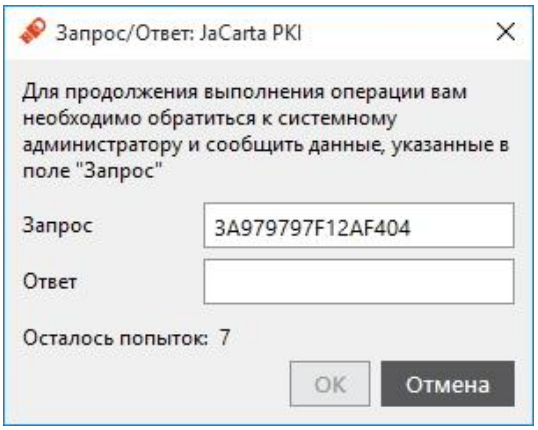


Рисунок 62 - Единый Клиент JaCarta. Окно "Запрос/Ответ: JaCarta PKI"

3. Пользователь должен продиктовать администратору код запроса, сгенерированный в поле "Запрос".

4. Администратор, используя интерфейс Консоли управления JMS, должен открыть окно удалённой разблокировки. Для этого необходимо нажать на кнопку "Удаленная разблокировка" (см. Рисунок 63).

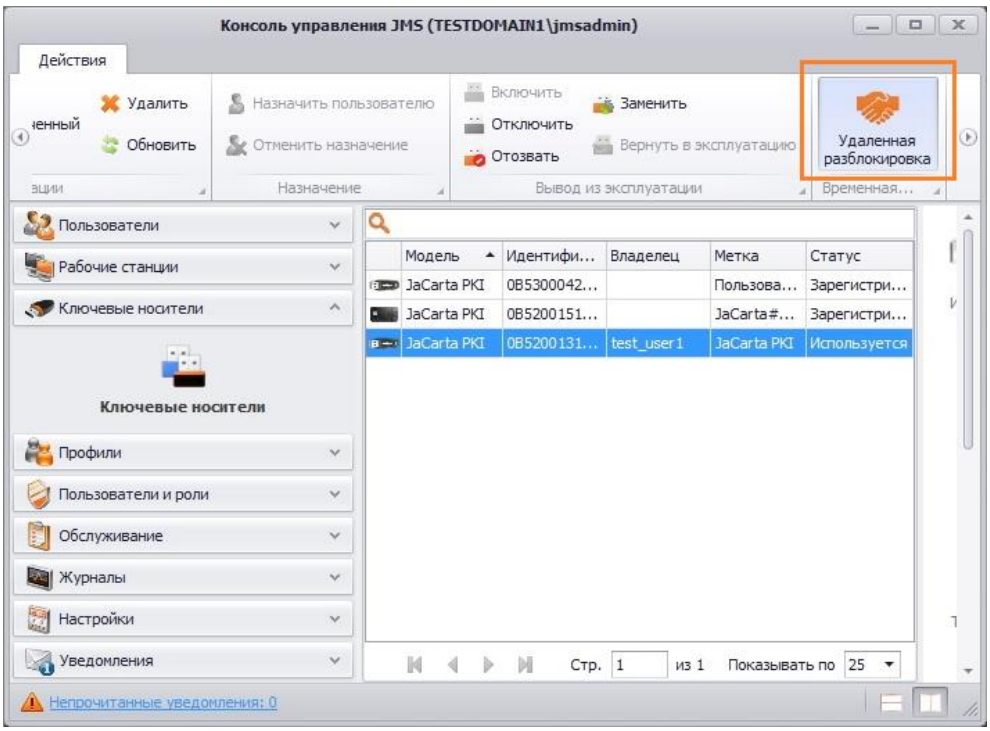


Рисунок 63 - Консоль управления JMS. Удаленная разблокировка

5. Будет открыто окно "Удаленная разблокировка" (см. Рисунок 64).

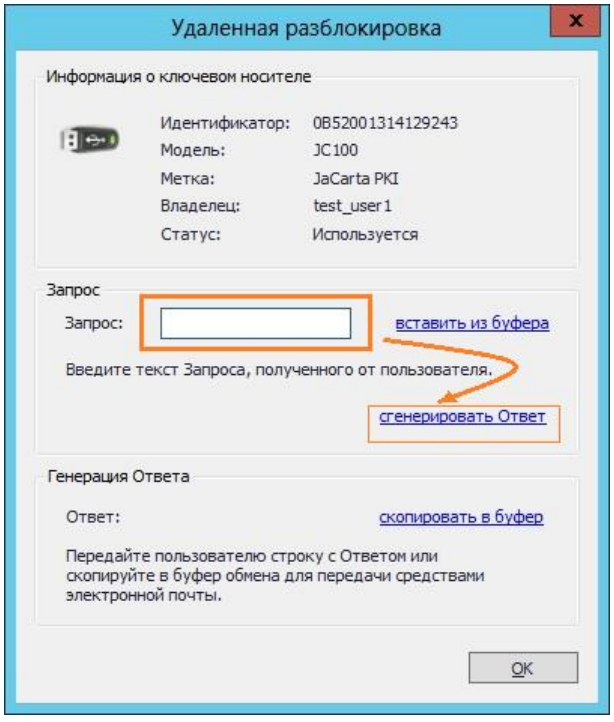


Рисунок 64 - Консоль управления JMS. Окно "Удаленная разблокировка"

6. 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 65).

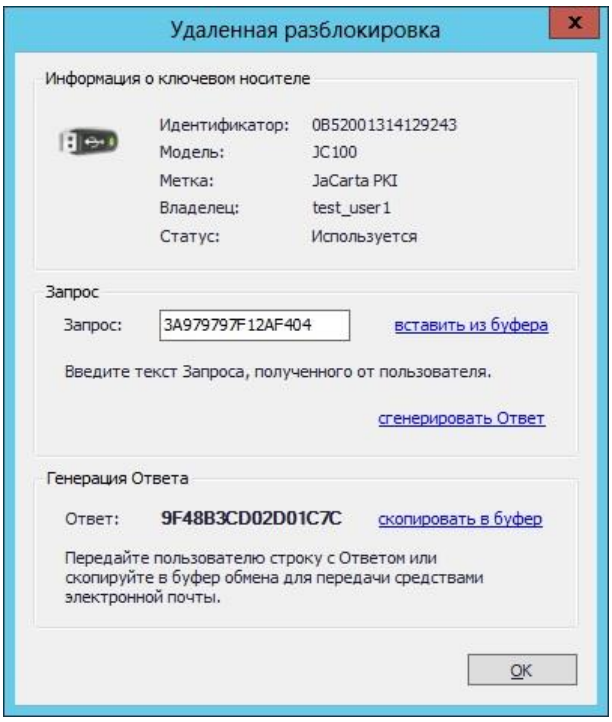


Рисунок 65 - Консоль управления JMS. Окно "Удаленная разблокировка". Сгенерированный ответ

7. Администратор должен продиктовать пользователю код ответа.
8. Пользователь должен ввести код ответа в соответствующем поле "Ответ" (см. Рисунок 66) и подтвердить ввод нажатием кнопки "OK".

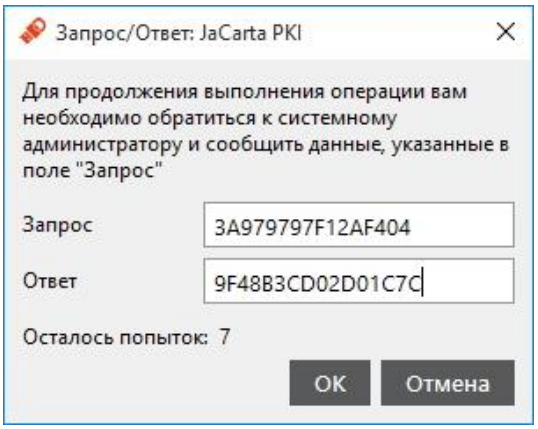


Рисунок 66 - Единый Клиент JaCarta. Окно "Запрос/Ответ: JaCarta PKI". Ввод сгенерированного ответа

9. При корректно введенном коде ответа на экране пользователя будет отображено информационное сообщение об успешности операции (см. Рисунок 67).

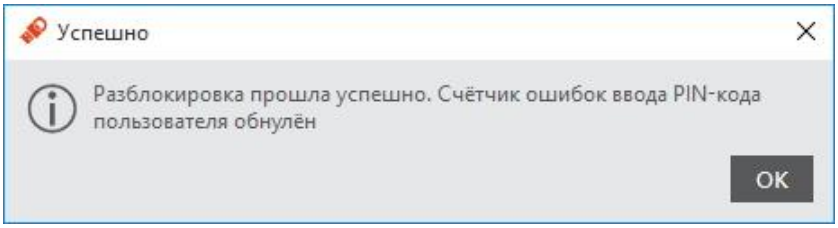


Рисунок 67 - Информационное сообщение об успешной разблокировке PIN-кода пользователя в удаленном режиме

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 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 Единый Клиент JaCarta и перейти в режим администратора.
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-кода администратора" (см. Рисунок 68).

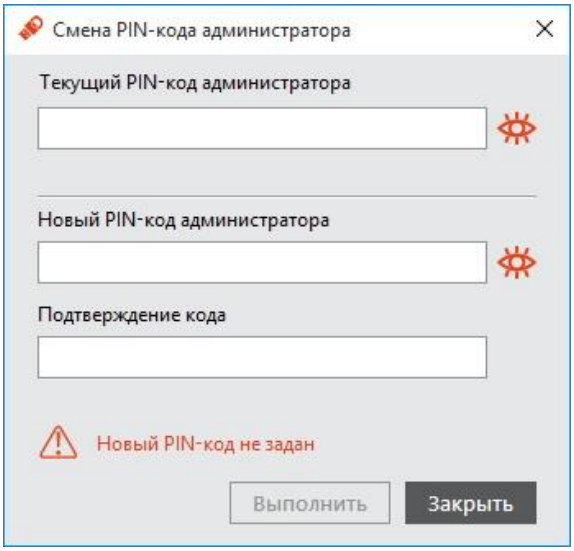


Рисунок 68 - Единый Клиент JaCarta. Окно "Сменить PIN-кода администратора"

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.

Новый PIN-код администратора должен отличаться от текущего, иначе будет отображено информационное сообщение об этом и кнопка "OK" будет недоступна для нажатия.

7. Нажать кнопку "OK".
8. При успешной смене PIN-кода администратора будет отображено соответствующее сообщение. Для его закрытия необходимо нажать кнопку "OK".

9. Виртуальный считыватель JaCarta CCID

Виртуальный считыватель JaCarta CCID представляет собой прослойку между реальным USB-устройством и менеджером ресурсов смарт-карт операционной системы Windows. JaCarta CCID 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 CCID

Виртуальный драйвер JaCarta CCID устанавливается на операционные системы Microsoft Windows Vista и выше, разрядностями x64 и x86.

Установить виртуальный драйвер JaCarta CCID можно двумя способами: через программу мастер установки Единый Клиент JaCarta или с помощью командной строки.

Процесс установки с помощью мастера установки Единый Клиент JaCarta описан в п. 5. Изменение. На шаге выбора компонента (в окне "Выборочная установка") необходимо раскрыть выпадающий список компонента "Драйверы" и выбрать пункт "Поддержка JaCarta Virtual Reader" (см. Рисунок 69). По умолчанию устанавливаются 2 виртуальных считывателя.

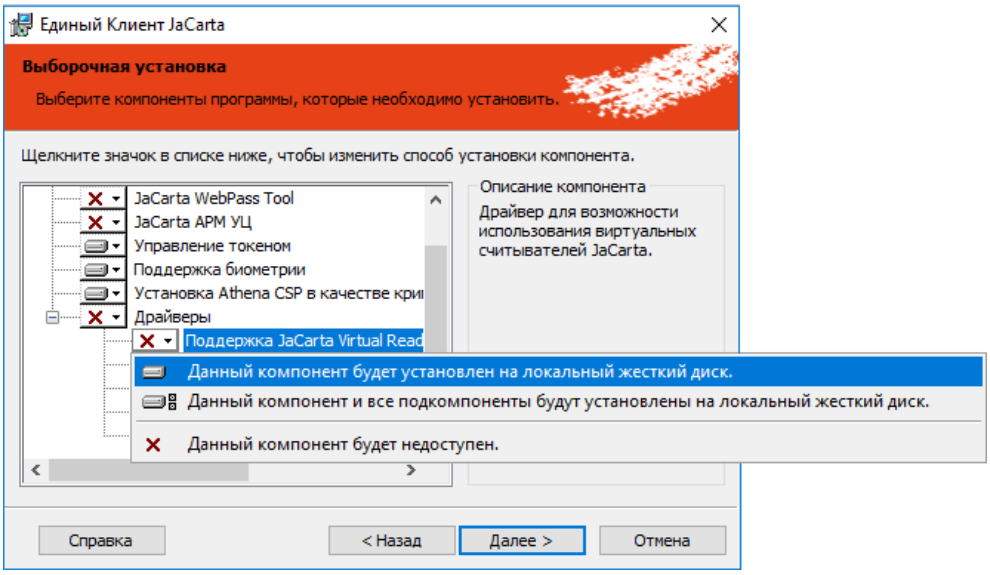


Рисунок 69 - Окно "Выборочная установка" мастера установки Единый Клиент JaCarta

В командной строке необходимо ввести `msiexec` со следующими параметрами:

```
msiexec /i JacartaCcid_x64_ru-RU.msi /quiet INSTALL_JAC-
ARTA_VR_DRIVER=1 IFD_READERS=2
```

где

- `JacartaCcid_x64_ru-RU.msi` – название файла инсталляции (для 32-битных платформ Microsoft Windows указать `JacartaCcid_x86_ru-RU.msi`);
- `/quiet` – тихий режим установки;
- `IFD_READERS` – количество создаваемых виртуальных считывателей (принимает значение от 1 до 10). По умолчанию задано 2 считывателя.

9.2 Подробнее об установке с помощью командной строки описано в п. 4.4. Установка программы с помощью мастера установки

Для установки Единого Клиента JaCarta с помощью мастера установки:

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

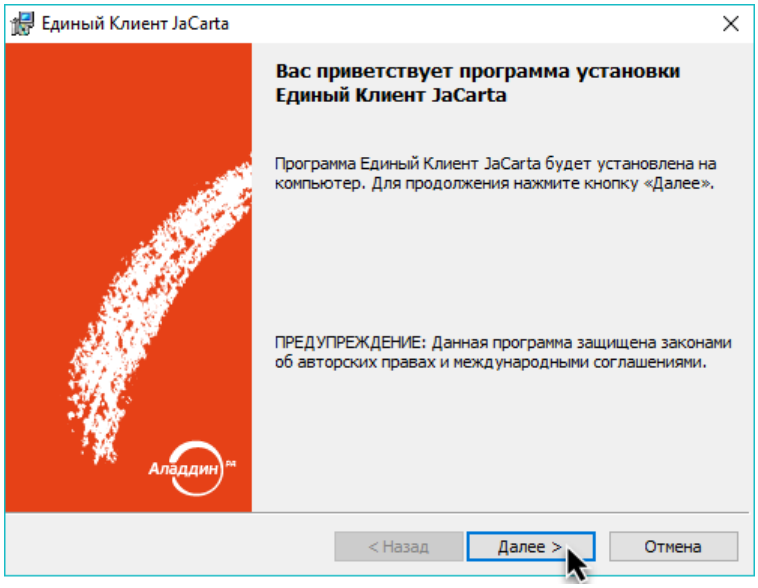


Рисунок 1 - Окно приветствия мастера установки Единый Клиент JaCarta

10. Нажмите кнопку "Далее". Будет отображено окно с "Лицензионное соглашение". Ознакомьтесь с текстом лицензионного соглашения.
    10.1. Если вы не согласны с условиями Лицензионного соглашения, выберите пункт "Я не принимаю условия Лицензионного соглашения" и нажмите кнопку "Отмена". Установка Единого Клиента JaCarta будет прекращена.
    10.2. Если вы согласны с условиями Лицензионного соглашения, выберите пункт "Я принимаю условия Лицензионного соглашения".

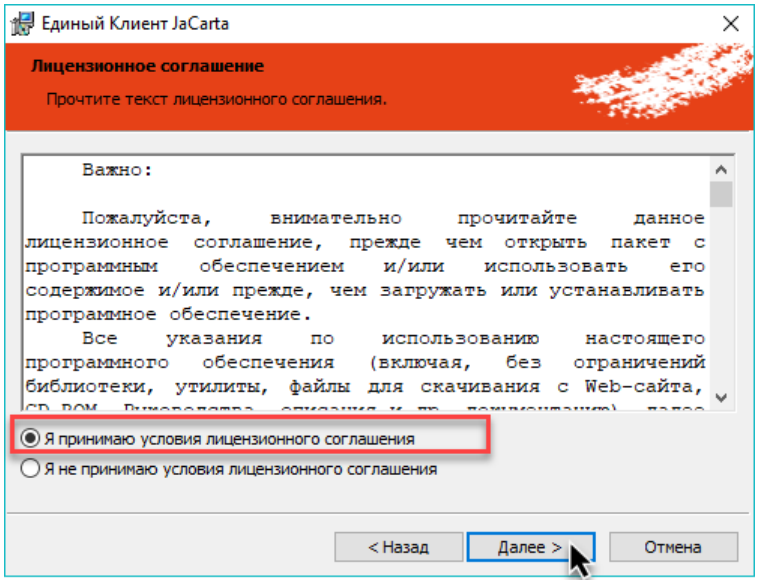


Рисунок 2 - Окно "Лицензионное соглашение" мастера установки Единый Клиент JaCarta

11. Нажмите кнопку "Далее". Будет открыто окно "Вид установки" (см. 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", "Управление токеном", "Поддержка биометрии", "Установка Athena CSP в качестве криптопровайдера по умолчанию". 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.

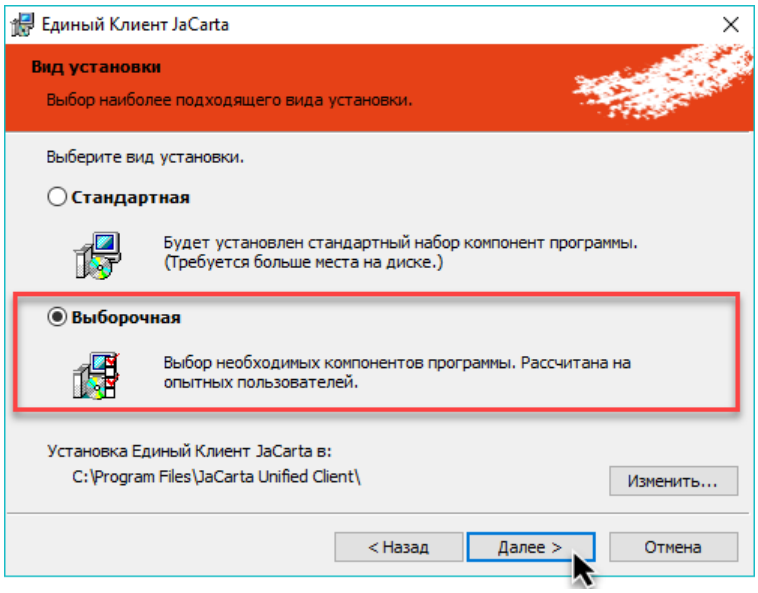


Рисунок 3 - Окно "Вид установки" мастера установки Единый Клиент JaCarta

12. Нажмите кнопку "Далее". В случае выборочной установки будет отображено окно для выбора из следующего набора компонент:
   - JaCarta SecurLogon;
   - JaCarta WebPass Tool;
   - JaCarta АРМ УЦ;
   - Управление токеном;
   - Поддержка биометрии;
   - Установка Athena CSP в качестве криптопровайдера по умолчанию;
   - Драйверы:
     - Поддержка JaCarta Virtual Reader;
     - Поддержка работы устаревших моделей JaCarta в продуктах VMware;
     - Поддержка JaCarta PKI с обратной совместимостью;
     - Поддержка JaCarta Secure MicroSD;
     - Поддержка eToken PRO 32K/64K (USB eToken Driver).

   Примечание. Описание компонентов приведено в приложении А.

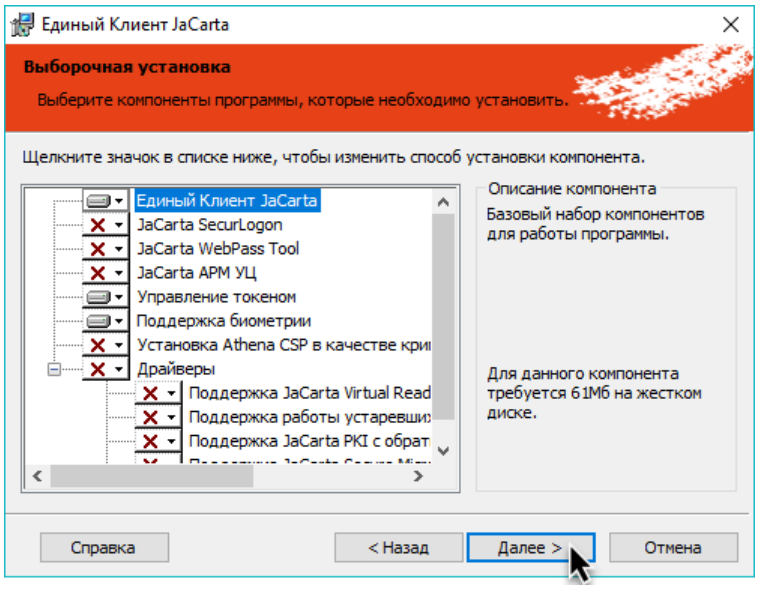


Рисунок 4 - Окно "Выборочная установка" мастера установки Единый Клиент JaCarta

Для установки требуемого компонента в окне "Выборочная установка" в строке с названием нужного компонента нажмите на значок ▼ и в выпадающем списке выберите необходимую опцию установки:

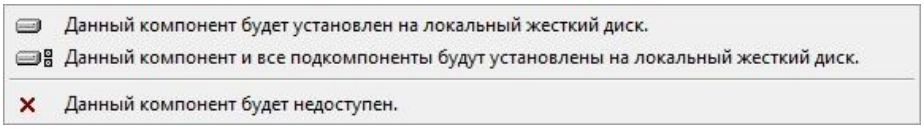


Рисунок 5 – Опции установки компонента

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

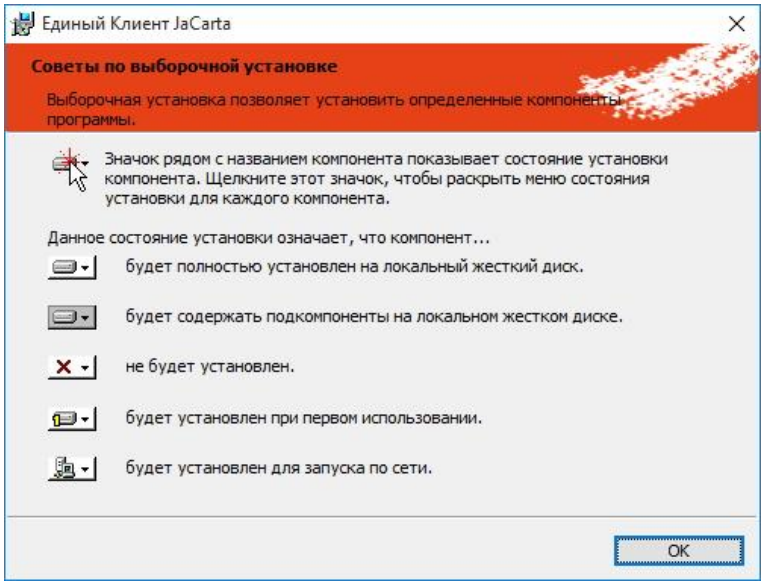


Рисунок 6 - Окно "Советы по выборочной установке" мастера установки Единый Клиент JaCarta

13. Нажмите "Далее" в окне "Выборочная установка". Будет отображено окно "Установка программы":

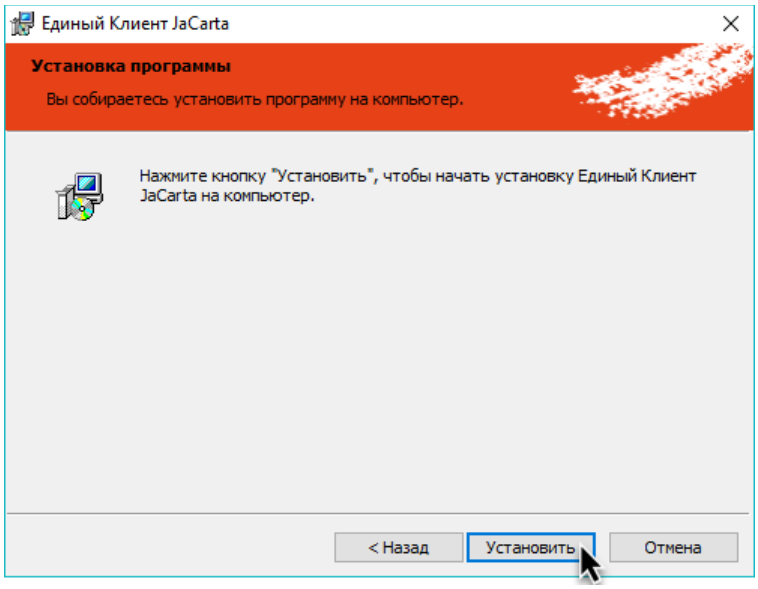


Рисунок 7 - Окно "Установка программы" мастера установки Единый Клиент JaCarta

14. Нажмите кнопку "Установить". Будет выполняться установка выбранных компонентов Единого Клиента JaCarta. Ход установки отображается в окне " Установка Единый Клиент JaCarta" в виде индикатора:

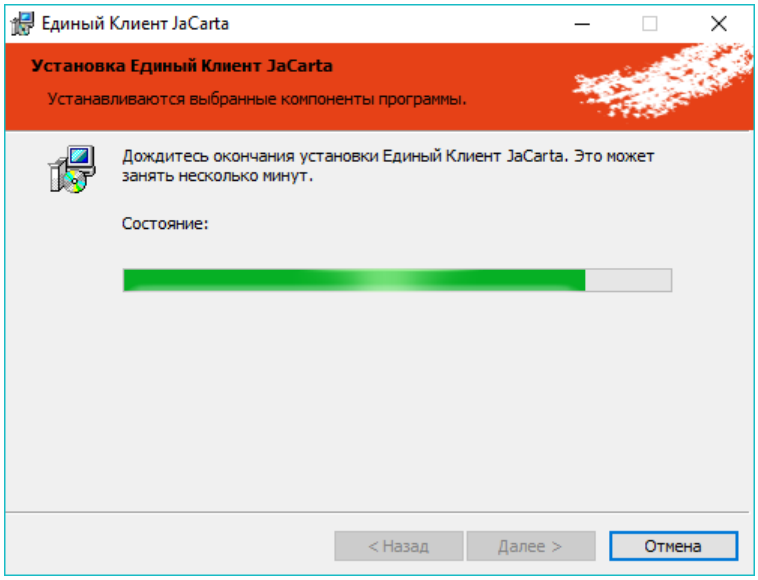


Рисунок 8 - Процесс установки Единый Клиент JaCarta

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

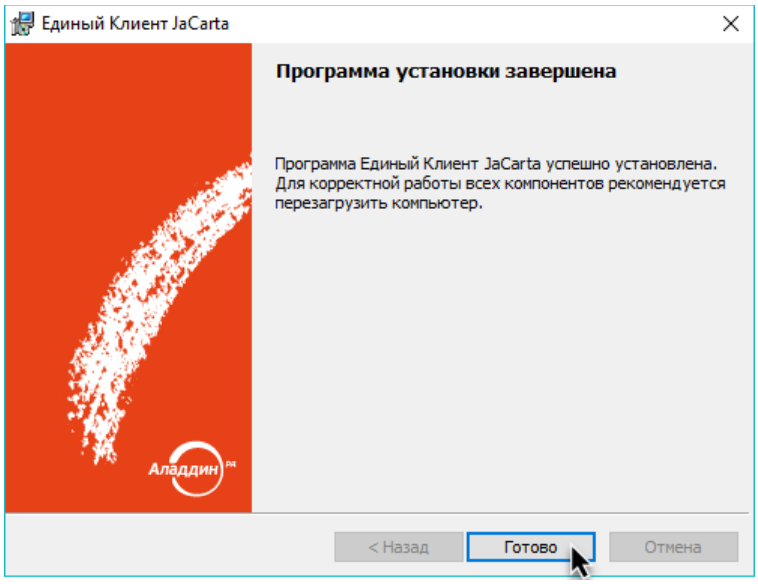


Рисунок 9 - Окно завершения установки Единый Клиент JaCarta

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

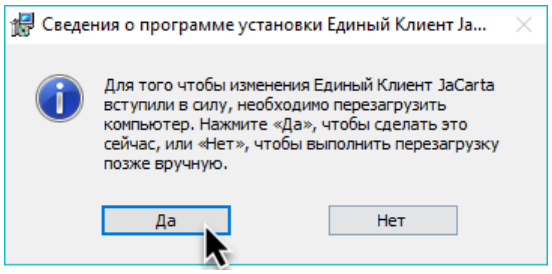


Рисунок 10 - Окно "Сведения о программе установки Единый Клиент JaCarta"

17. Будет выполнена перезагрузка компьютера, после завершения Единый Клиент JaCarta готов к работе.

9.3 Особенности установки Единый Клиент JaCarta на ОС Microsoft Windows XP с установленным антивирусом Dr.Web

Если установка Единый Клиент JaCarta происходит на компьютере с ОС Microsoft Windows XP и с установленным антивирусом Dr.Web, то перед установкой Единый Клиент JaCarta необходимо выполнить следующие действия:

18. Запустить **SpIDer Agent,** нажав значок на панели задач в области уведомлений.
19. Разблокировать **SpIDer Agent.** Для внесения изменений нажать кнопку :

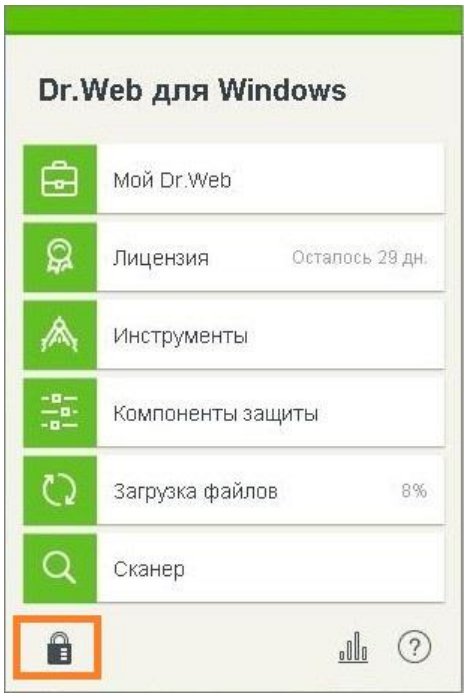


Рисунок 11 – Антивирус Dr.Web. Разблокировка элементов управления

20. Нажать появившуюся кнопку "Настройки" - :

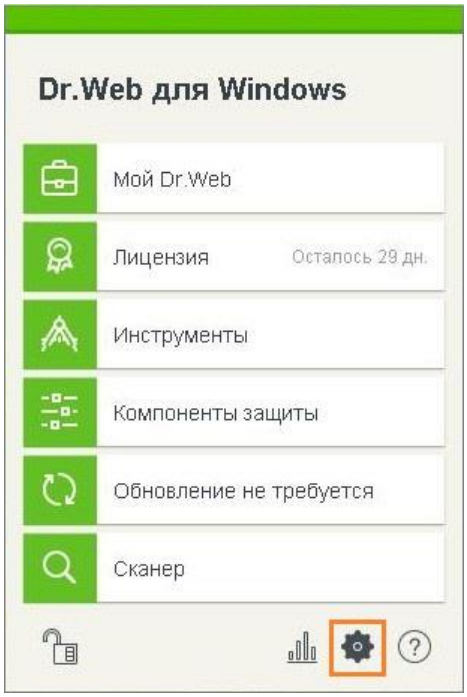


Рисунок 12 – Антивирус Dr.Web. Элемент управления "Настройки"

21. В окне "Настройки" выбрать опцию "Компоненты защиты":

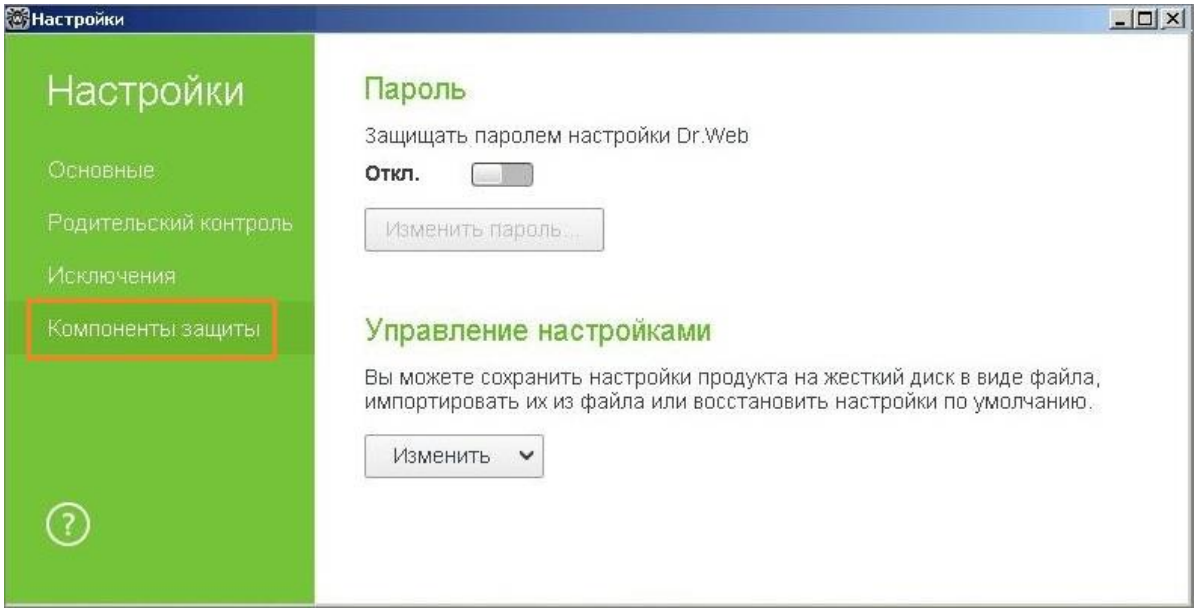


Рисунок 13 – Антивирус Dr.Web. Окно "Настройки"

22. В окне "Компоненты защиты" выбрать опцию "Превентивная защита" и установить для объектов параметр "Разрешать":

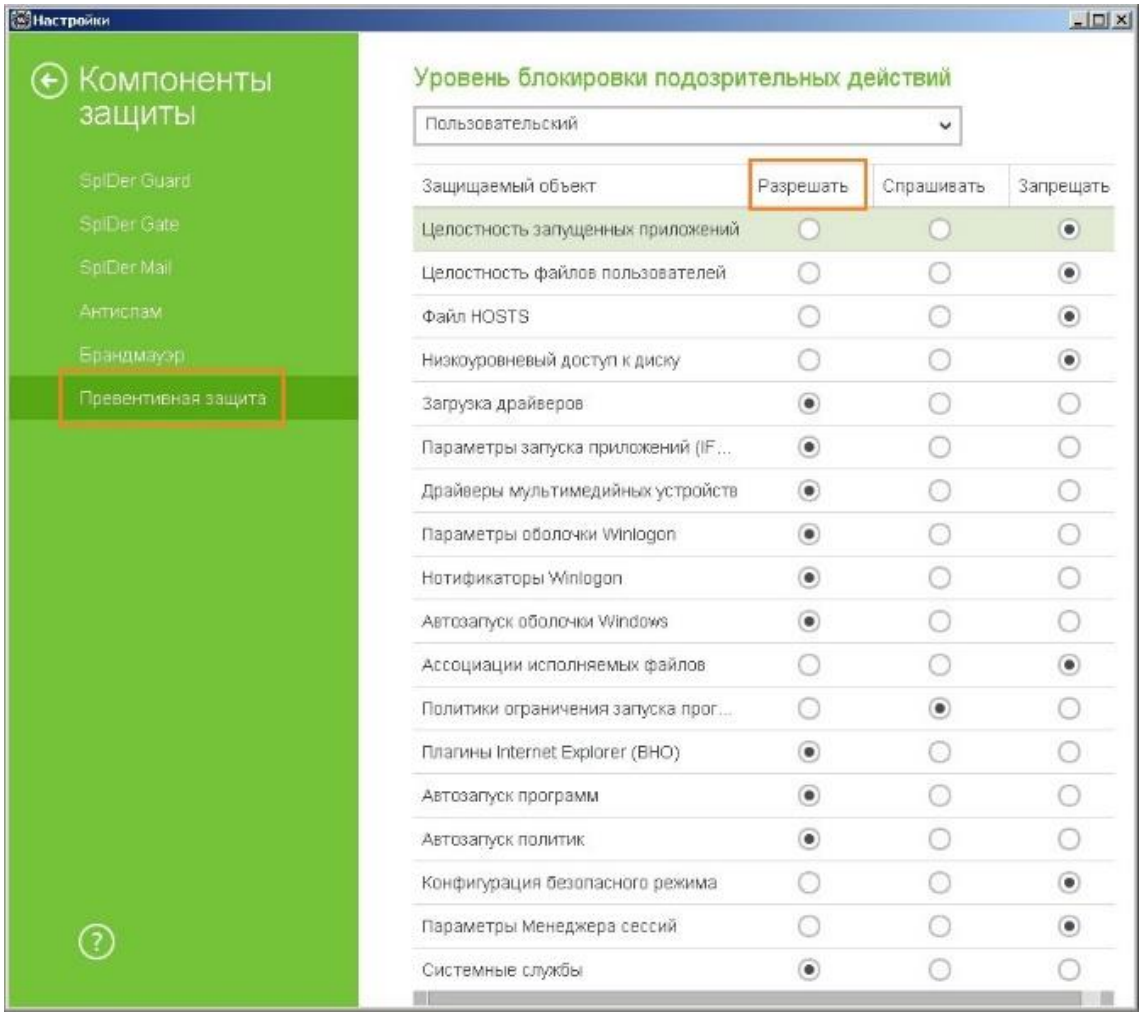


Рисунок 14 – Антивирус Dr.Web. Окно "Компоненты защиты"

23. Закрыть окно "Настройки" и установить Единый Клиент JaCarta (см. п. 4.4 "Установка программы с помощью мастера установки").

Если при установке ПО Единый Клиент JaCarta будет выбрана опция "Проверять наличие обновлений", то после перезагрузки ОС может появиться окно, представленное на Рисунок 15.

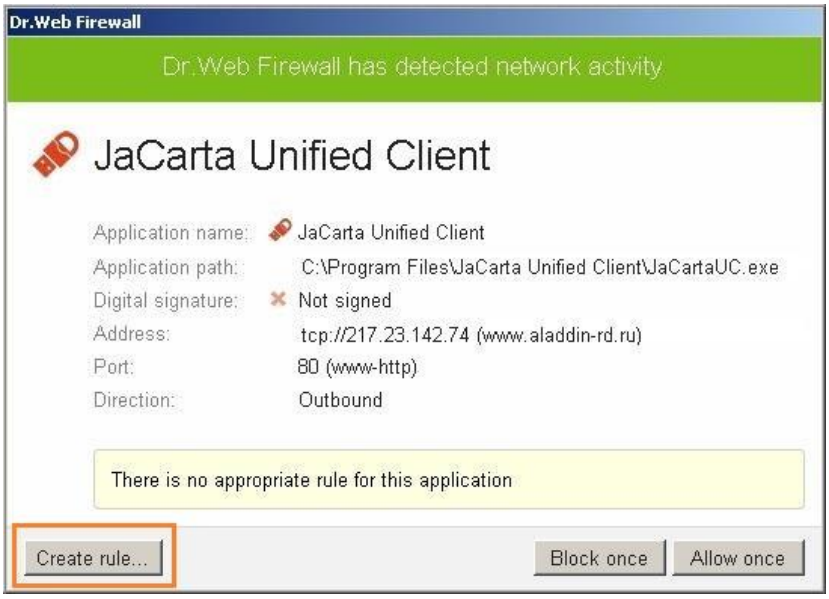


Рисунок 15 - Антивирус Dr.Web. Информационное окно

После появления данного окна необходимо создать правило для Dr.Web, согласно которому ПО Единый Клиент JaCarta сможет обращаться по адресу www.aladdin-rd.ru для проверки наличия обновлений и их установки.

Для создания правила следует нажать кнопку "Create rule". Далее в появившемся окне (см. Рисунок 16) необходимо раскрыть выпадающий список и выбрать одно из значений: "Allow network connections for application on 80" или "Allow all network connections" или "Create custom rule". После нажать "OK".

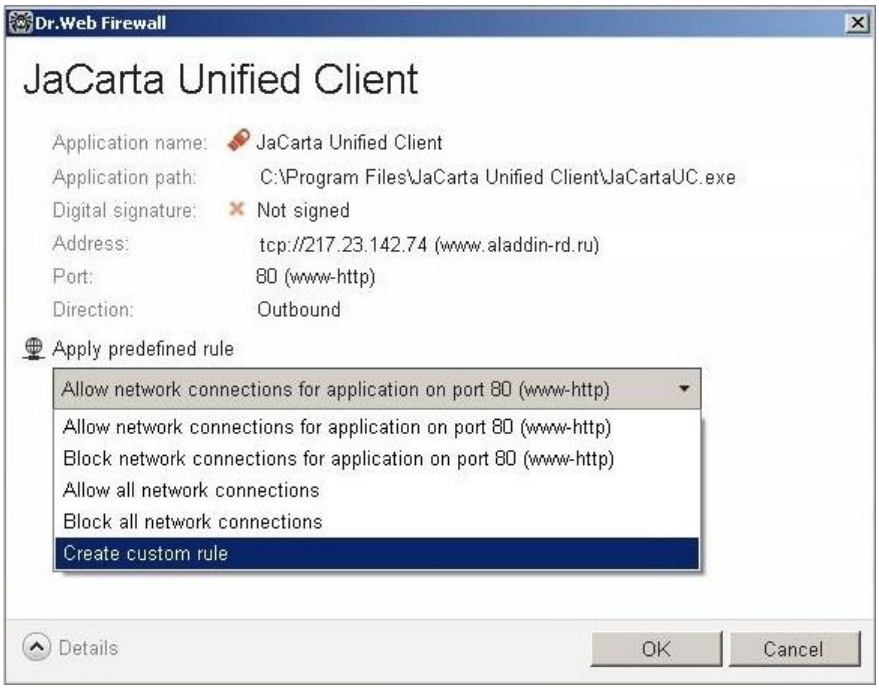


Рисунок 16 - Антивирус Dr.Web. Выбор правила

В случае, если была выбрана опция "Create custom rule", будет отображено окно (см. Рисунок 17), в котором необходимо нажать "OK" для завершения.

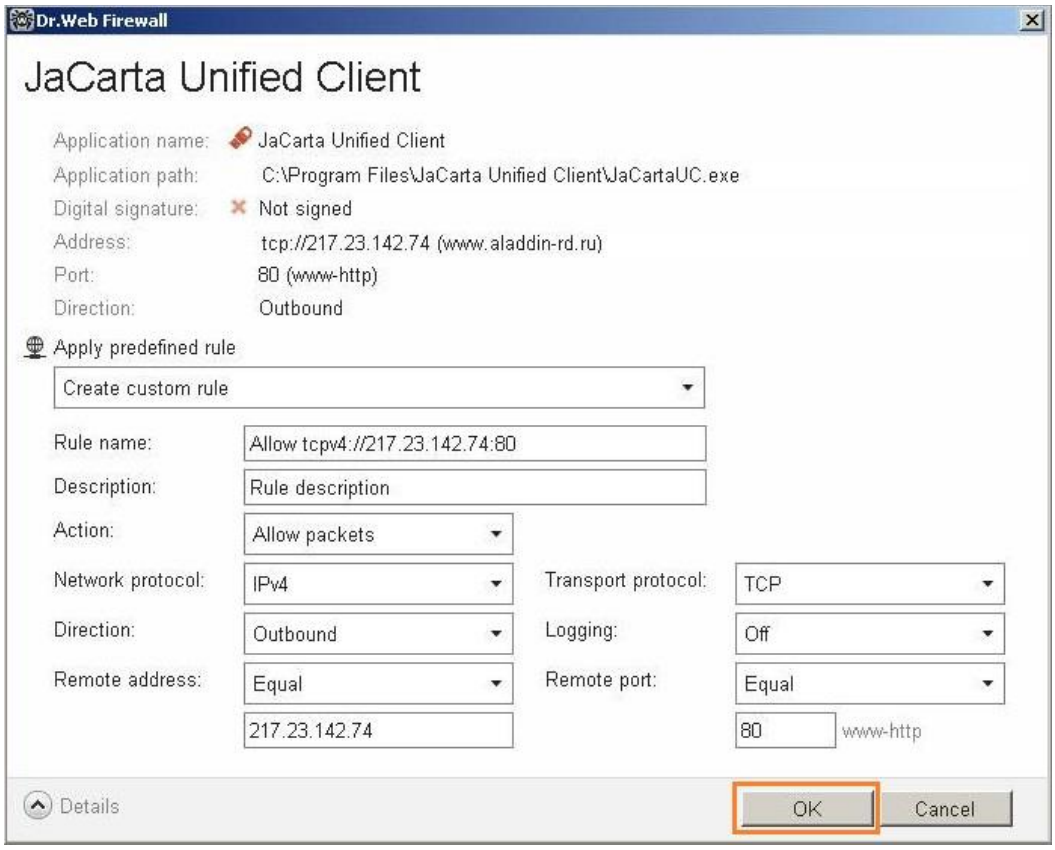


Рисунок 17- Антивирус Dr.Web. Завершение настройки правила

Установка программы в режиме командной строки.

9.4 Работа JaCarta CCID

Драйвер виртуального считывателя JaCarta CCID 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 изменения числа виртуальных считывателей, а также в случаи полной деинсталляции.

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. Операции, производимые с помощью утилиты JaCarta АРМ УЦ

С помощью утилиты АРМ УЦ возможно осуществлять следующие действия:

- Генерировать ключевые пары с использованием встроенных криптографических возможностей электронных ключей JaCarta ГОСТ и eToken ГОСТ;
- Формировать запросы к удостоверяющему центру на получение сертификата открытого ключа;
- Производить запись полученных сертификатов в память электронных ключей JaCarta ГОСТ и eToken ГОСТ.

Подробные сведения об операциях, производимых с помощью утилиты АРМ УЦ приведены в документе "JaCarta_Workstation_CA_2.0_AdminGuide - *АРМ УЦ. Руководство администратора*".

11. Синхронизация паролей электронного ключа и учетной записи домена Windows

> *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 и, 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.*

> *В случаях, когда пароль не соответствует требованиям к качеству одной из политик синхронизация невозможна.*

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-код пользователя и пароль учетной записи домена Windows необходимо выполнить следующие действия:

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.

Если раздела `SyncPin` нет, то необходимо создать по указанному адресу раздел с указанным именем.

3. В левом нижнем углу нажать кнопку "Настройки" - 

.
4. На вкладке "Основные" в поле "Имя домена для синхронизации паролей" (см. Рисунок 70) должно быть отображено введенное ранее в редакторе реестра (см. п.2) имя домена. Нажать кнопку "OK".

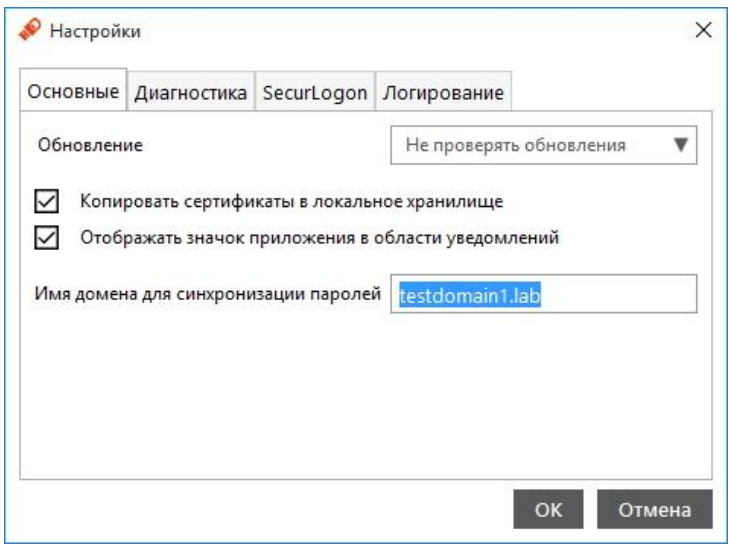


Рисунок 70 - Единый Клиент JaCarta. Окно "Настройки". Вкладка "Основные"

5. Закрыть окно Единый Клиент JaCarta.

6. На панели задач в области уведомлений раскрыть панель запущенных программ (см. Рисунок 71). Вызвать контекстное меню у элемента и выбрать пункт Меню: "Выйти".

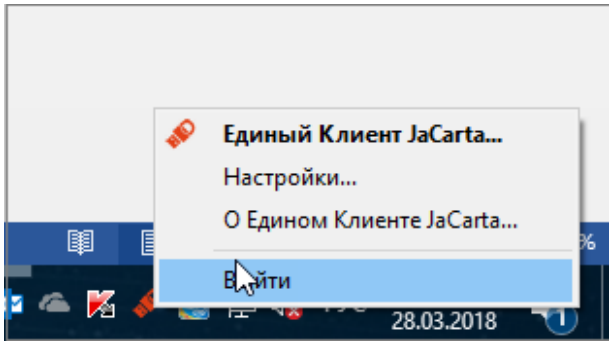


Рисунок 71 – Панель задач Windows. Выход из программы Единый Клиент JaCarta

7. Последовательно выбрать: "Пуск", "Аладдин Р.Д.", "Единый Клиент JaCarta".
8. В окне Единый Клиент JaCarta в режиме пользователя будет доступна кнопка "Сменить PIN-код и пароль домена" (см. Рисунок 72).

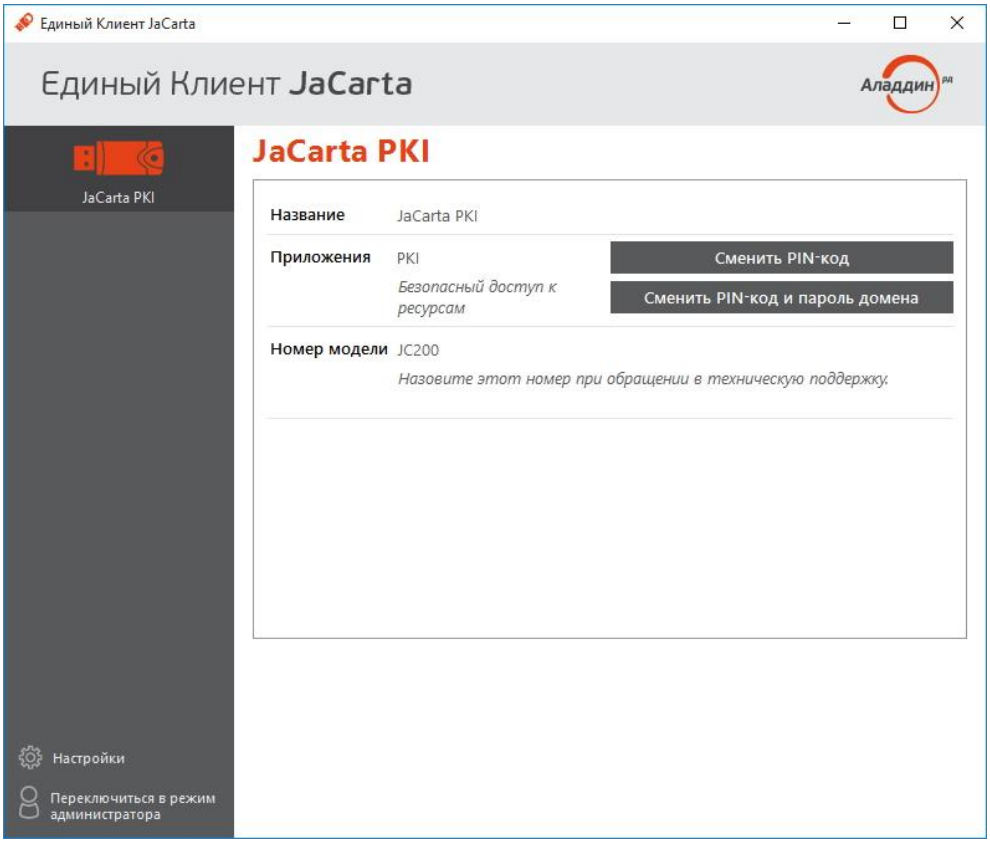


Рисунок 72 - Единый Клиент JaCarta. Доступная кнопка "Сменить PIN-код и пароль домена"

Опция "Сменить PIN-код и пароль домена" появится и в Меню быстрого запуска (см. Рисунок 73), которое можно запустить на панели задач в области уведомлений, нажав правой кнопкой мыши на значок .

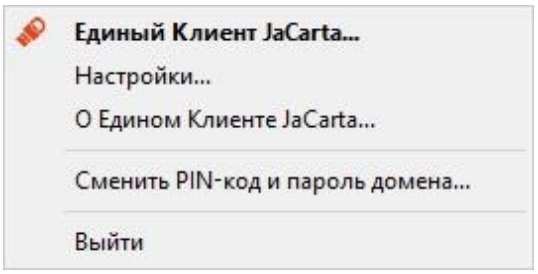


Рисунок 73 - Единый Клиент JaCarta. Меню быстрого запуска

9. Нажать кнопку "Сменить PIN-код и пароль домена". Будет открыто окно "Смена PIN-кода и пароля домена" (см. Рисунок 74).

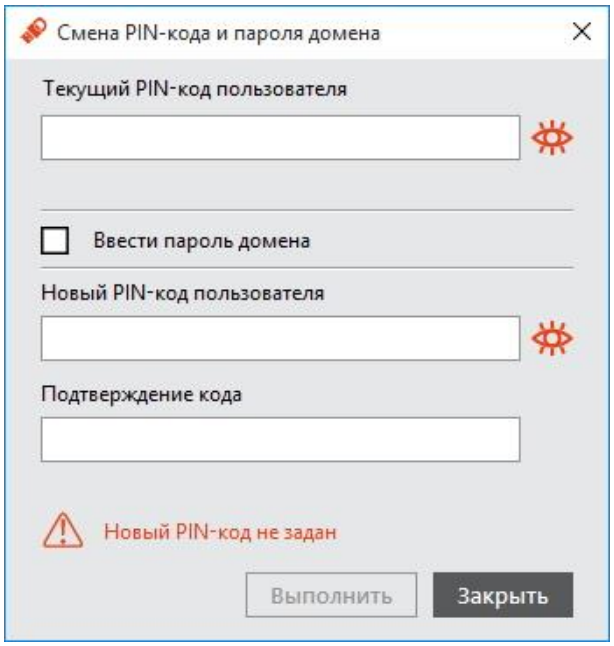


Рисунок 74 - Единый Клиент JaCarta. Окно "Смена PIN-кода и пароля домена"

10. Ввести текущий PIN-код пользователя, после чего указать новый PIN-код пользователя и его подтверждение.

11. При выборе опции "Ввести пароль домена" в диалоговом окне будет добавлено поле для ввода пароля домена (см. Рисунок 75).

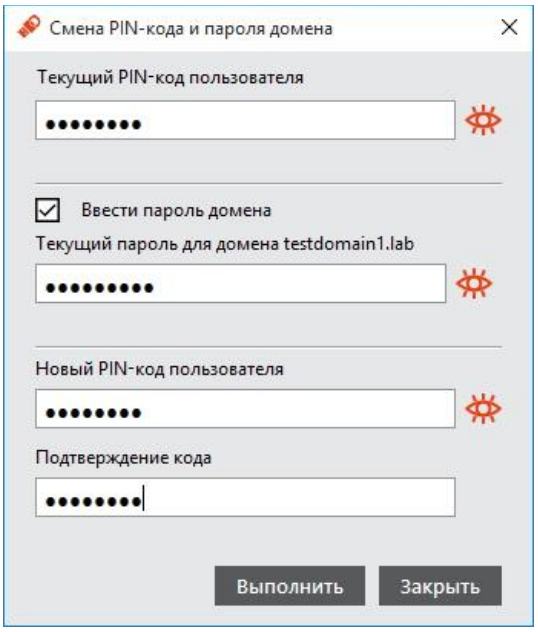


Рисунок 75 - Единый Клиент JaCarta. Окно "Смена PIN-кода и пароля домена"

12. Ввести текущий пароль домена, после чего ввести новый PIN-код пользователя и повторно подтвердить его.
13. Нажать кнопку "Выполнить".
14. В случае, если введенный пароль пользователя не отвечает требованиям к качеству пароля, будет отображено окно с описанием ошибки (см. Рисунок 76).

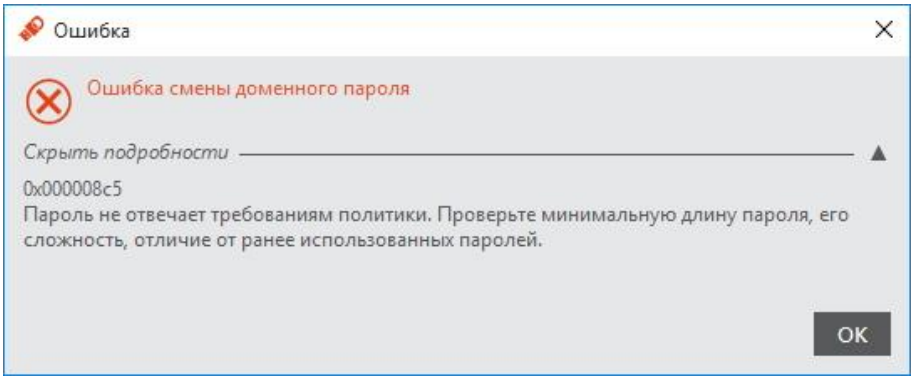


Рисунок 76 - Единый Клиент JaCarta. Ошибка при смене доменного пароля

15. При успешной смене доменного пароля будет отображено информационное окно:

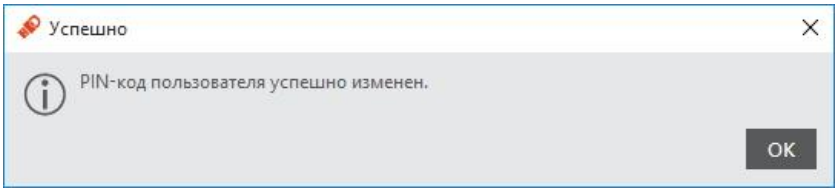


Рисунок 77 - Единый Клиент JaCarta. Информационное сообщение об успешной смене доменного пароля

12. Мастер техподдержки

В Едином Клиенте JaCarta существует возможность сбора диагностической информации об аварийных ситуациях, случившихся у пользователей с последующей отправкой собранной информации в службу технической поддержки компании Аладдин Р.Д.

Мастер техподдержки позволяет сформировать архив с диагностический информацией о текущем состоянии ПО Единый Клиент JaCarta и конфигурации компьютера, на котором установлен Единый Клиент JaCarta, а также по выбору пользователя позволяет: сохранить этот архив на диск или отправить в службу технической поддержки компании Аладдин Р.Д.

Подробнее о настройках логирования см. п. 6.5 "Вкладка "Логирование".

Для запуска Мастера техподдержки:

1. Выбрать последовательно "Пуск", "Аладдин Р.Д.", "Мастер техподдержки Аладдин Р.Д.".
2. Будет открыто окно "Мастер техподдержки 'Аладдин Р.Д.'" (см. Рисунок 78). Нажать кнопку "Далее" для перехода к следующему шагу.

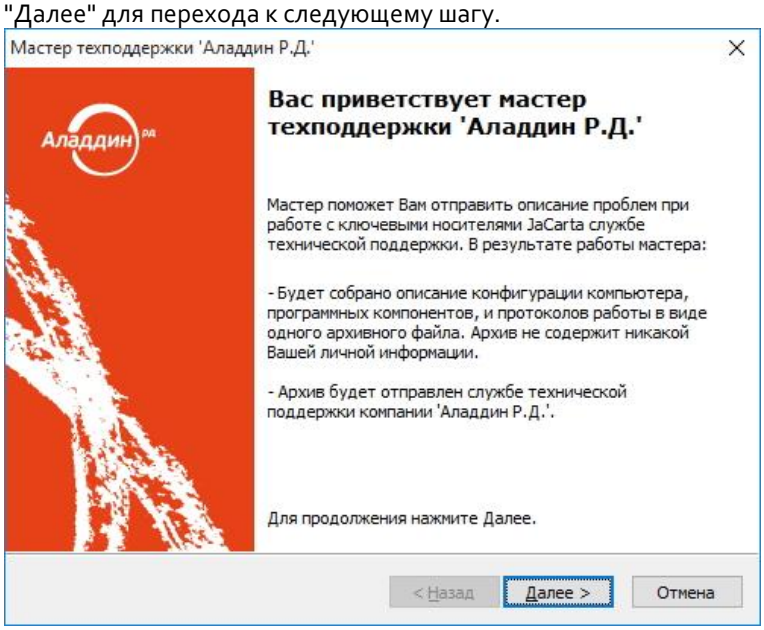


Рисунок 78 – Мастер техподдержки 'Аладдин Р.Д.'

3. В окне "Логирование и воспроизведение проблемы" (см. Рисунок 79) ознакомиться и выполнить все перечисленные в этом окне действия, затем выбрать опцию "Я подтверждаю, что все сделал согласно приведенной выше инструкции". После чего нажать кнопку "Далее".

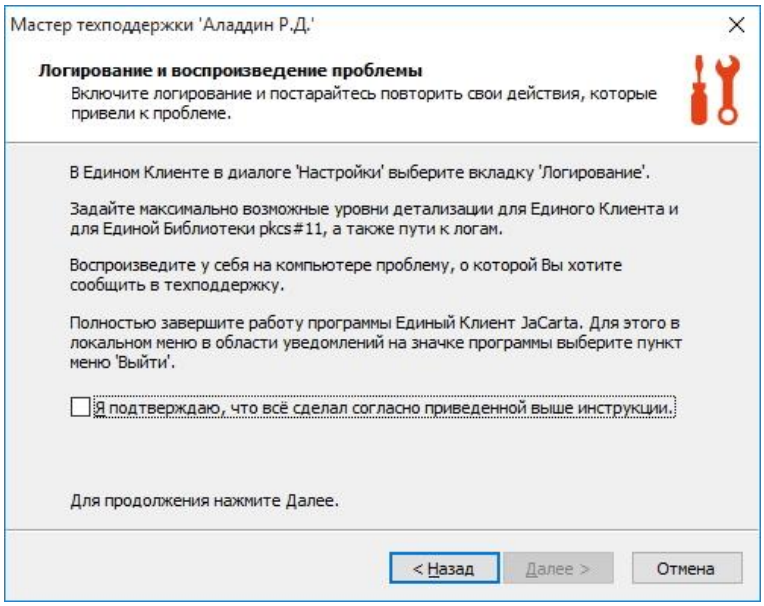


Рисунок 79 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Логирование и воспроизведение проблемы"

4. В окне "Определение конфигурации компьютера" (см. Рисунок 80) можно изменить место сохранения файла с диагностической информацией. Для этого необходимо нажать кнопку "Изменить", указать место сохранения, после чего нажать "Сохранить". Если место сохранения файла с диагностической информацией менять не нужно, то оставьте место сохранения, указанное по умолчанию. После чего нажать кнопку "Далее".

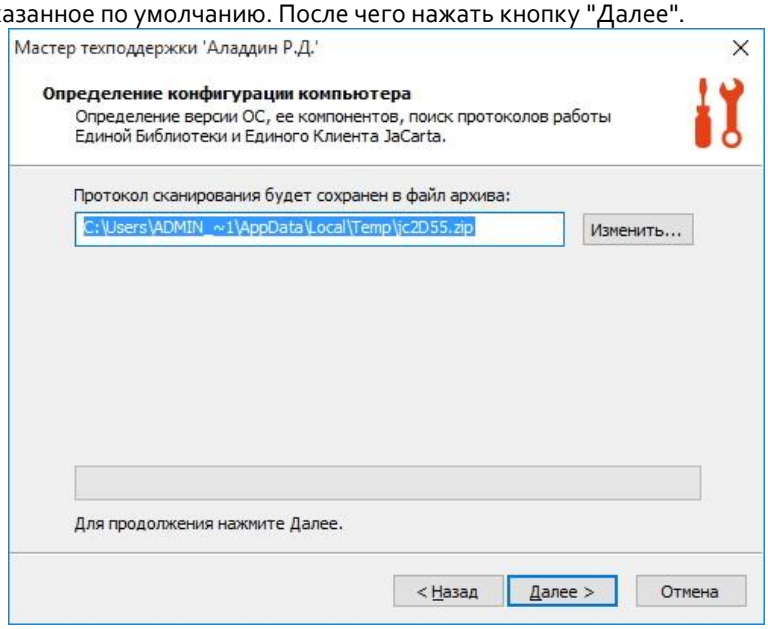


Рисунок 80 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Определение конфигурации компьютера"

5. Мастер техподдержки начнет процесс сбора диагностической информации (см. Рисунок 81). Дождитесь окончания процесса.

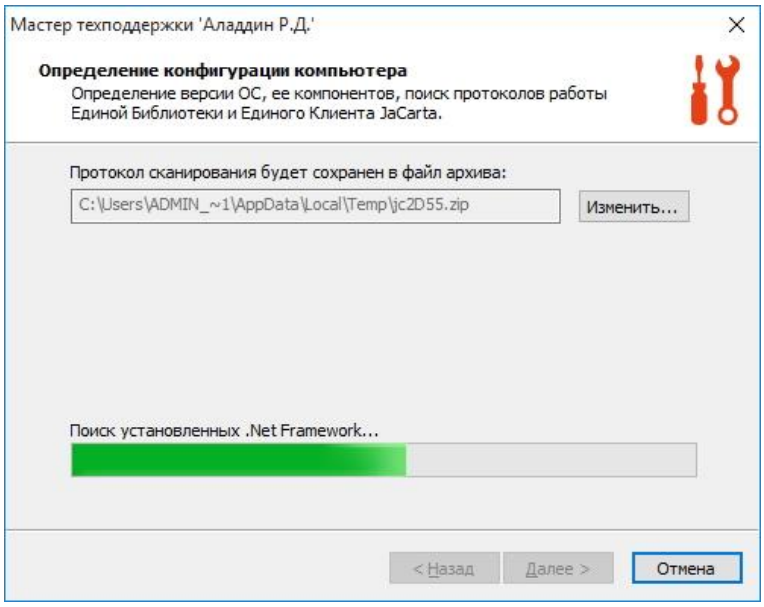


Рисунок 81 - Мастер техподдержки 'Аладдин Р.Д.'. Процесс сбора диагностической информации

6. В появившемся окне "Архивация протоколов" (см. Рисунок 82) будут указаны созданные файлы логирования. Нажать кнопку "Далее".

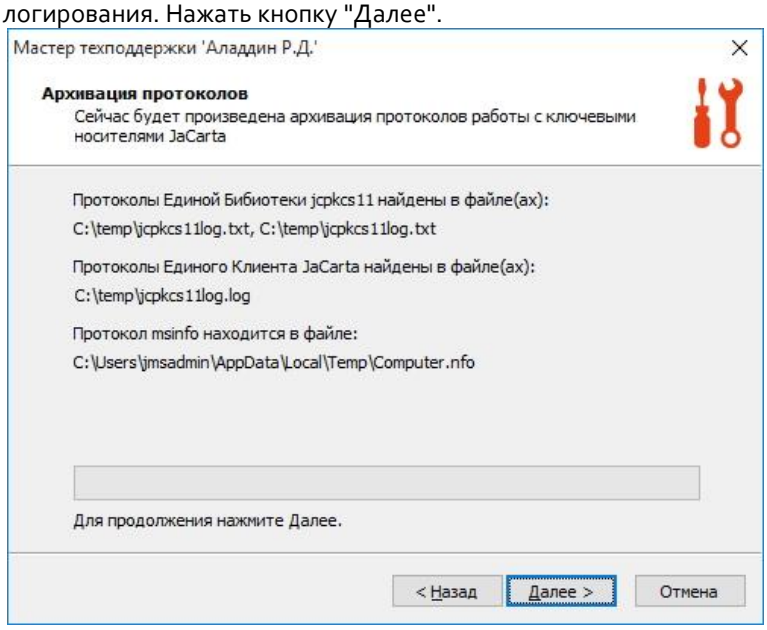


Рисунок 82 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Архивация протоколов"

7. В окне "Описание проблемы" (см. Рисунок 83) заполнить поле "Описание проблемы", а в поле "E-mail адрес для обратной связи" указать свой адрес электронной почты, после чего нажать кнопку "Далее".

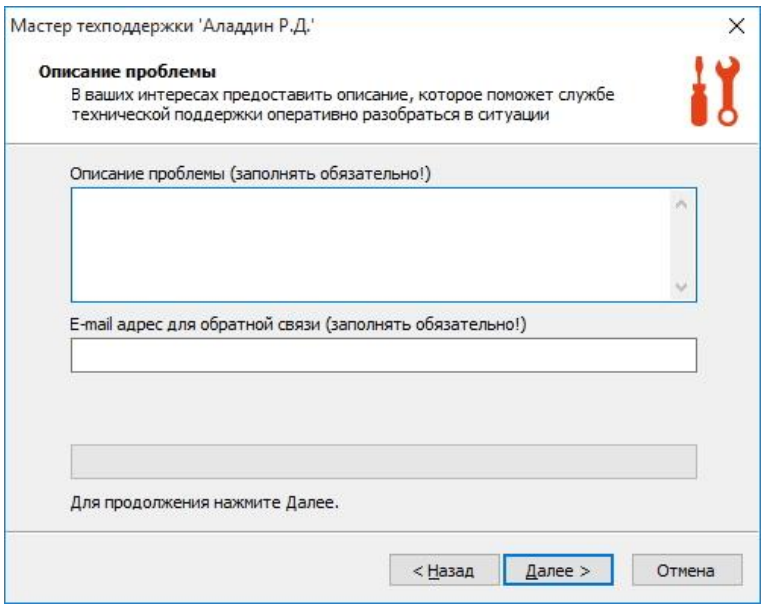


Рисунок 83 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Описание проблемы"

8. В появившемся окне (см. Рисунок 84) выбрать способ отправки результатов сбора диагностической информации в службу технической поддержки компании Аладдин Р.Д., после чего нажать кнопку "Далее".

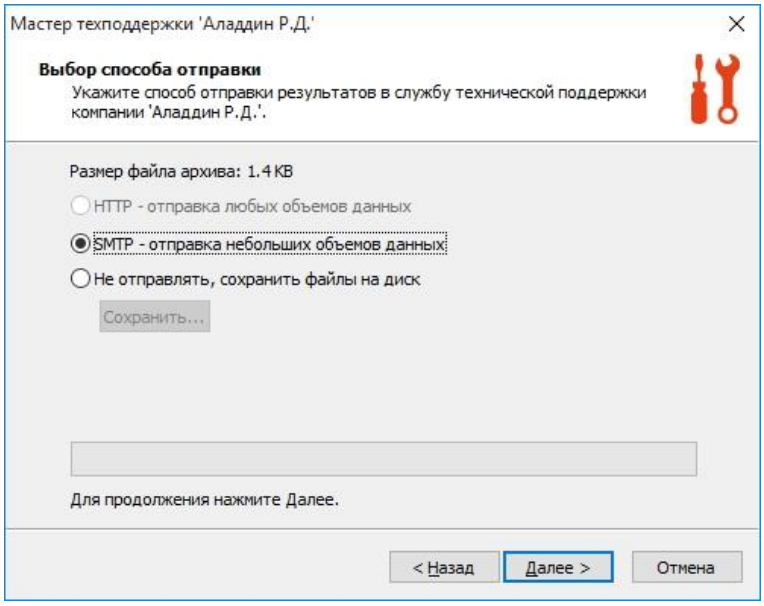


Рисунок 84 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Описание проблемы"

9. Если был выбран способ "Не отправлять, сохранить файлы на диск" (см. Рисунок 85), то станет доступной кнопка "Сохранить", после нажатия на которую отобразится диалоговое окно "Сохранение" (см. Рисунок 86)

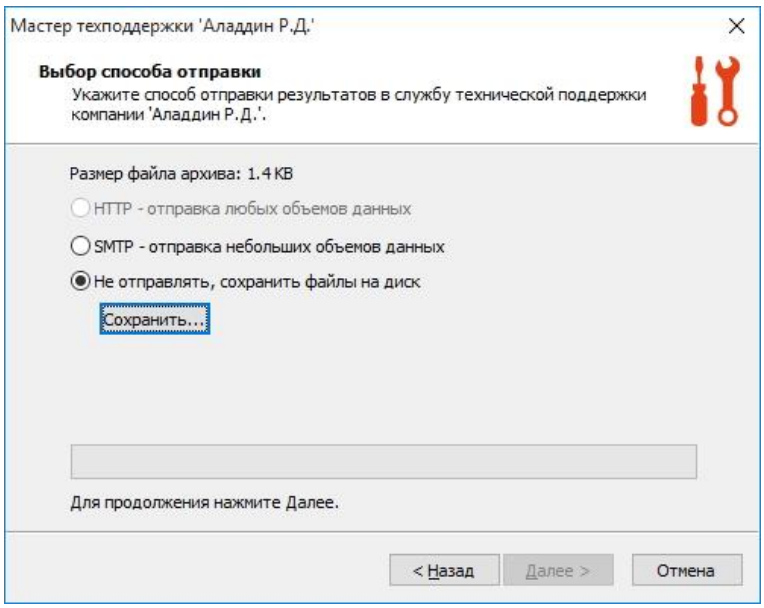


Рисунок 85 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Описание проблемы". Выбран способ "Не отправлять, сохранить файлы на диск"

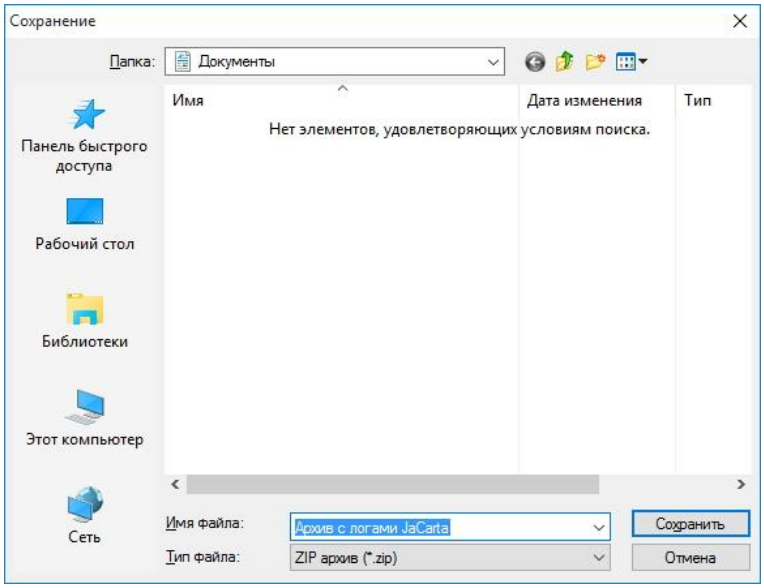


Рисунок 86 – Диалоговое окно для сохранения архива с логами

9.1.1. Указать место сохранения файла с логами JaCarta и нажать кнопку "Сохранить" (см. Рисунок 86).

9.1.2. Аналогичную процедуру выполнить для сохранения файла сопроводительного письма (см. Рисунок 87).

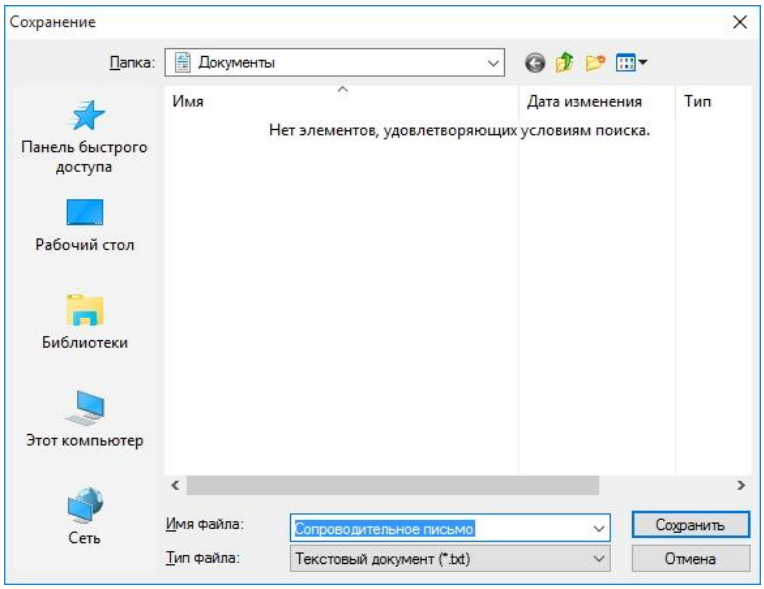


Рисунок 87 - Диалоговое окно для сохранения сопроводительного письма

10. Если был выбран способ отправки "SMTP – отправка небольших объемов данных", то после нажатия на кнопку "Далее" (при условии, что на компьютере установлена и настроена программа MS Outlook) будет открыто окно "Отправка результатов по почте" (см. Рисунок 88).

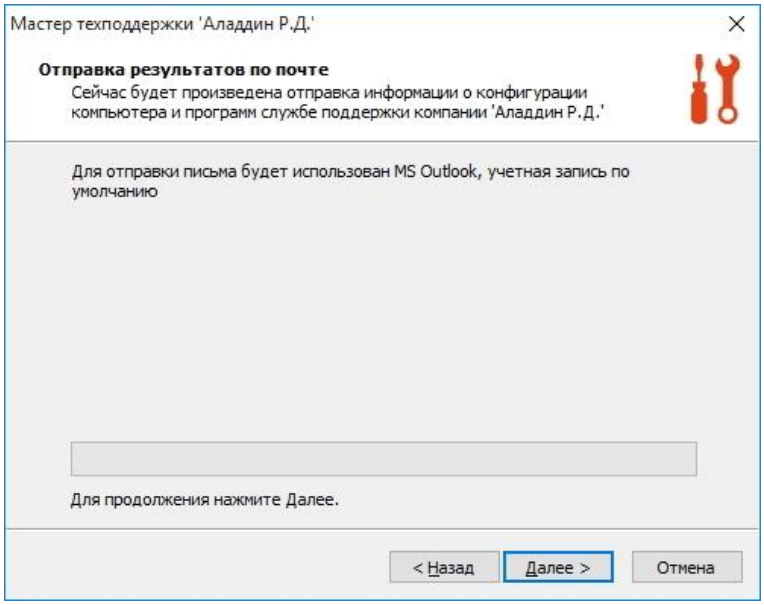


Рисунок 88 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Отправка результатов по почте"

11. Если на компьютере не установлен почтовый клиент MS Outlook, необходимо заполнить поля "Адрес" и "Порт" данными (см. Рисунок 89). Убедиться в их корректности можно с помощью кнопки "Проверить".

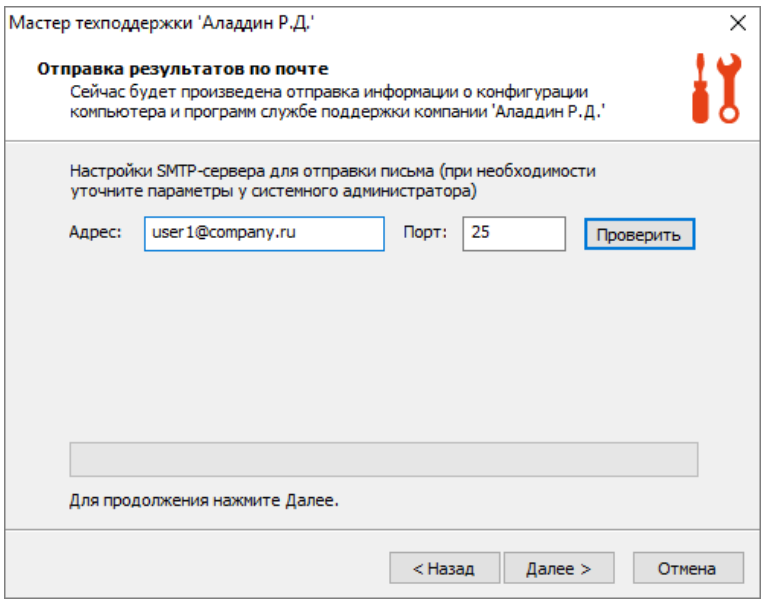


Рисунок 89 - Мастер техподдержки 'Аладдин Р.Д.'. Окно "Отправка результатов по почте"

12. Нажать кнопку "Далее". Письмо-запрос технической поддержки с Вашими диагностическими данными будет отправлено по адресу support.jc@aladdin-rd.ru.
13. В окне завершения мастера техподдержки (см. Рисунок 90) нажать кнопку "Готово".

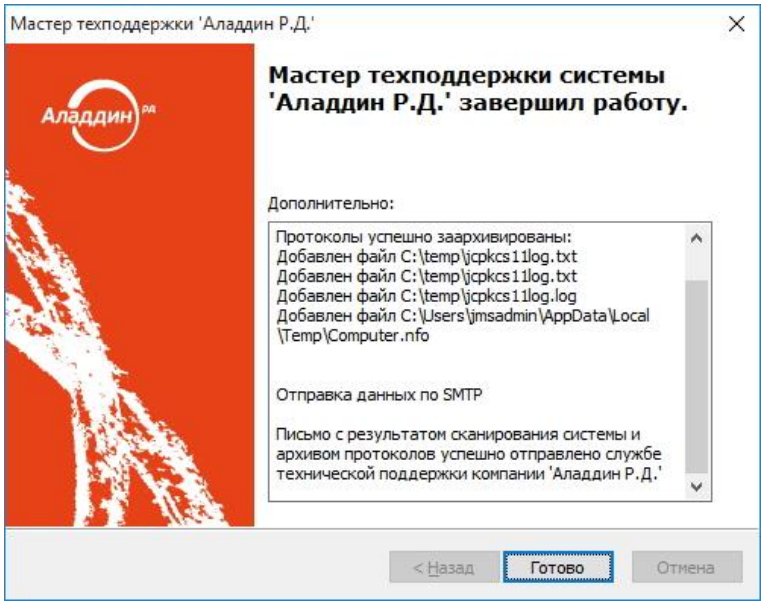


Рисунок 90 – Окно завершения Мастер техподдержки 'Аладдин Р.Д.'

Приложение А Компоненты Единого Клиента JaCarta

Название компонента	Описание
JaCarta SecurLogon	Для обеспечения двухфакторной аутентификации с использованием электронных ключей JaCarta и eToken в ОС Microsoft Windows
JaCarta WebPass Tool	Для возможности администрирования токенов JaCarta WebPass
JaCarta АРМ УЦ	Позволяет генерировать ключевые пары с использованием встроенных криптографических возможностей электронных ключей JaCarta ГОСТ и eToken ГОСТ, а также формировать запросы к удостоверяющему центру на получение сертификата открытого ключа и записывать полученные сертификаты в память электронного ключа
Управление токеном	Для возможности выполнять операции с токеном до входа пользователя в систему
Поддержка биометрии	Добавляет возможность использования биометрических считывателей и электронных ключей JaCarta BIO
Установка Athena CSP в качестве криптопровайдера по умолчанию	Для использования Athena CSP криптопровайдером по умолчанию. В противном случае (в случае отмены установки этого компонента) криптопровайдером по умолчанию будет Microsoft Base Smart Card CSP.
Драйверы – Поддержка JaCarta Virtual Reader	Для возможности использования виртуальных считывателей JaCarta
Драйверы – Поддержка работы устаревших моделей JaCarta в продуктах VMware	Для возможности использования токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware
Драйверы – Поддержка JaCarta PKI с обратной совместимостью	Для возможности использования токенов JaCarta PKI с обратной совместимостью
Драйверы – Поддержка JaCarta Secure MicroSD	Для возможности использования токенов JaCarta в форм-факторе Secure MicroSD
Драйверы – Поддержка eToken PRO 32K/64K (USB eToken Driver)	Для возможности использования устаревших моделей eToken PRO 32K/64K

13. Контакты

13.1 Офис (общие вопросы)

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

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

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

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

13.2 Техподдержка

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

Регистрация изменений

Версия	Изменения
1.1	Обновлены скриншоты, исправлено форматирование к выходу новой сборки ЕК 2.12.2.2222
1.0	*Создан документ*

Коротко о компании

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

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

Основные направления

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

Лицензии

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

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

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