JaCarta WebPass Tool

Инструкция по использованию

Версия продукта	2.12
Версия документа	1.7
Статус	Публичный
Дата	23.10.2019
Листов	46

Оглавление

1. О документе

1.1 Назначение документа

Документ представляет собой руководство по установке, настройке и использованию компонента JaCarta WebPass Tool, являющего частью программного обеспечения Единый Клиент JaCarta.

1.2 На кого ориентирован данный документ

Документ предназначен для администраторов безопасности.

1.3 Документы, рекомендуемые для предварительного прочтения (изучения)

Для полного понимания настоящего документа рекомендуется ознакомиться с документом "Единый Клиент JaCarta. Руководство администратора", содержащим подробные сведения, касающиеся системных требований, установки/удаления и настройки Единого Клиента JaCarta.

1.4 Организация документа

Документ разбит на несколько разделов:

- в разделе 2 "Общие сведения о JaCarta WebPass Tool" приведена основная информация о JaCarta WebPass Tool.
- в разделе 3 "Описание электронных ключей JaCarta WebPass" приведено описание электронных ключей JaCarta WebPass, включая описание внешнего вида, индикации, редимов работы и др.
- в разделе 4 "Установка и удаление утилиты JaCarta WebPass Tool" приведено описание системных требований к компьютеру и описание процедур установки и удаления JaCarta WebPass Tool.
- в разделе 5 "Запуск утилиты и обзор пользовательского интерфейса" содержится описание запуска JaCarta WebPass Tool и его настроек.
- в разделе 6 "Порядок работы с электронными ключами JaCarta WebPass" содержится описание основных процедур использования электронных ключей JaCarta WebPass.

В конце документа приведен предметный указатель (см. стр. 43).

1.5 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве ознакомительного материала (подробного руководства по установке и настройке JaCarta АРМ УЦ), а также в качестве справочника при работе с JaCarta АРМ УЦ.

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

1.6 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

[Поле]	Используется для выделения наименований полей, блоков, закладок экранных форм
<Кнопка>	Используется для выделения наименований кнопок

Меню:	Используется для выделения наименований пунктов меню
Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ
Термин	Используется для выделения первого и последующих вхождений определяемого в документе термина в тексте документа
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

1.7 Обозначения и сокращения

Таблица 2 — Обозначения и сокращения

ОС	Операционная система
ПО	Программное обеспечение
CCID	(Circuit Card Interface Device) – считыватель смарт-карт (это стандарт для работы со смарт-картами)
HID	(Human Interface Devices) – класс устройств для взаимодействия с человеком
JAS	(JaCarta Authentication Server) – сервер аутентификации JaCarta
JMS	(JaCarta Management System) – система управления JaCarta
OTP	(One Time Password — OTP) – одноразовый пароль
PIN	(Personal Identification Number) – личный идентификационный номер
PKI	(Public Key Infrastructure) – инфраструктура открытых ключей
SHA	(Secure Hash Algorithm) – алгоритм криптографического хеширования
USB	(Universal Serial Bus) – универсальная последовательная шина
U2F	(Universal 2nd Factor) – универсальный протокол двухфакторной аутентификации

1.8 Ключевые слова

Электронный ключ JaCarta WebPass, PIN-код администратора, слот, OTP, защищенный ресурс.

1.9 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.

1.10 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. Общие сведения о JaCarta WebPass Tool

JaCarta WebPass Tool представляет собой отдельное приложение (далее – утилита), входящее в состав программного обеспечения Единый Клиент JaCarta.

Утилита JaCarta WebPass Tool предназначена для работы с электронными ключами JaCarta WebPass и JaCarta U2F/WebPass.

Электронные ключи JaCarta WebPass предназначены для генерации одноразовых паролей (One Time Password — OTP), для создания и безопасного хранения сложного многоразового (постоянного) пароля с возможностью вставки этого пароля в экранные формы ввода, а также запуска Web-браузера и автоматического перехода по сохраненному в электронном ключе адресу Web-ресурса.

2.1 Термины и определения

Термины, используемые в настоящем документе, приведены в Таблица 3.

Таблица 3 – Термины и определения

Термин	***Определение***
Администратор	Сотрудник, отвечающий за подготовку к работе и техническое обслуживание электронного ключа
Инициализация	Установка основных параметров работы электронного ключа (подготовка к работе)
Пользователь	Конечный пользователь электронного ключа
Приложение	Программное обеспечение, установленное в память электронного ключа. Существуют следующие приложения: • OTP; • STORAGE; • U2F *. Примечание – Приложение U2F (только для электронных ключей JaCarta U2F/WebPass) управляется Web-сервисом, в котором оно используется.
Слот	Набор данных и параметров, необходимых для работы с паролями и URL.
Смарт-карта	Электронное устройство в виде пластиковой карты с электронной памятью и интегральной микросхемой
Электронный ключ	Аппаратное устройство в форм-факторе USB-токена, карты MicroSD, со стандартными встроенными операционной системой (ОС) и программным обеспечением (ПО)
PIN-код администратора	Последовательность символов, которую необходимо ввести, чтобы администратор мог совершить определенную операцию

3. Описание электронных ключей JaCarta WebPass

3.1 Общие сведения

Внешний вид электронного ключа JaCarta WebPass показан на Рисунок 1.

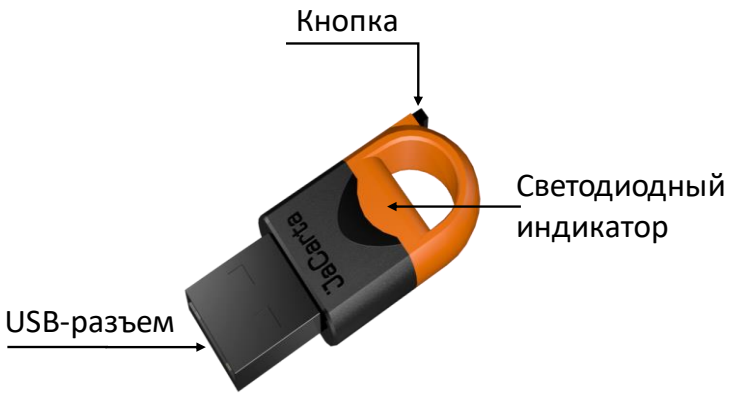


Рисунок 1 – Внешний вид электронного ключа JaCarta WebPass

Корпус электронного ключа JaCarta WebPass выполнен в форм-факторе с разъёмом USB Type A Male и состоит из двух частей разных цветов.

На корпусе электронного ключа расположена кнопка, используемая либо для генерации пароля, либо для запуска браузера. Поддерживается три варианта нажатий (подробнее см. Использование электронного ключа JaCarta WebPass).

Внутри корпуса электронного ключа расположен светодиодный индикатор, отражающий различные режимы работы (см. Рисунок 1).

В электронных ключах JaCarta WebPass для хранения информации используются три независимых слота.

Слот – набор данных и параметров, хранящихся на электронном ключе и необходимых для генерации пароля или перехода по адресу Web-ресурса (в зависимости от типа слота).

В каждом из слотов может храниться один из следующих видов информации:

- одноразовый пароль, генерируемый по заданному при инициализации алгоритму (тип слота «Одноразовый пароль»);
- многоразовый пароль, генерируемый в соответствии с заданными при инициализации критериями качества (тип слота «Пароль»);
- URL-адрес защищённого ресурса (тип слота «Интернет адрес»).

Слоты полностью независимы: инициализируются (конфигурируются), управляются и используются независимо друг от друга.

Количество активных слотов и конфигурация каждого из них задаётся при инициализации слотов.

Инициализация – Установка основных параметров работы электронного ключа (подготовка к работе).

> *В процессе инициализации слота предыдущие значения параметров слота (если они ранее были записаны в слот)* ***УДАЛЯЮТСЯ****!*

3.2 Режимы работы

В настоящее время всеми электронными ключами JaCarta WebPass поддерживается единственный режим работы – ***HID+CCID***. В этом режиме активны оба интерфейса: USB CCID и USB HID, при этом возможна, как настройка установленных приложений, так и подстановка паролей в формы ввода и автоматический запуск Web-браузера.

Электронные ключи JC-WebPass являются составным (композитным, composite) устройством USB 2.0 Full Speed с одной конфигурацией и двумя интерфейсами, реализующими два независимо функционирующих устройства USB следующих классов:

1. CCID (Circuit Card Interface Device) – считыватель смарт-карт;
2. HID (Human Interface Devices) – клавиатура.

Таким образом, на уровне операционной системы компьютера один подключенный электронный ключ JaCarta WebPass распознаётся, как два независимых устройства:

1. CCID-совместимый считыватель смарт-карт с подключённой смарт-картой;
2. Устройство ввода (HID клавиатура).

3.3 Световая индикация рабочих состояний

Электронный ключ JaCarta WebPass оснащён световым (светодиодным) индикатором состояния, который активируется при подсоединении электронного ключа к компьютеру и индицирует работу электронного ключа следующим образом:

1. Светодиод горит непрерывно – подсоединённый электронный ключ в данный момент находится в режиме ожидания и готов к работе;
2. Светодиод мигает часто – на подсоединённом электронном ключе в данный момент выполняется операция (например, создаётся сложный постоянный пароль);
3. Светодиод мигает медленно – при работе электронного ключа обнаружена ошибка.

3.4 PIN-код администратора

3.4.1 Назначение и случаи использования PIN-кода администратора

В электронных ключах JaCarta WebPass для хранения информации используются три независимых слота. При использовании утилиты JaCarta WebPass Tool для защиты слотов от несанкционированной записи и удаления хранящихся в них данных используется PIN-код администратора, общий (одинаковый) для всех трех слотов.

PIN-код администратора используется при выполнении следующих операций:

- смена PIN-кода администратора;
- инициализация слота;
- очистка слота.

Подробнее об операциях с использованием PIN-кода администратора, выполняемых с помощью утилиты JaCarta WebPass Tool см. Операции, выполняемые в приложении OTP.

3.4.2 Настройки PIN-кода по умолчанию

PIN-код администратора по умолчанию (заводские настройки): ***1234567890***

> *Инициализация слота невозможна, если значение **PIN-кода администратора по умолчанию** не было изменено на другое значение!*

PIN-код администратора, отличный от PIN-кода администратора по умолчанию, может быть установлен при производстве, либо пользователем в процессе эксплуатации электронного ключа. При смене PIN-кода необходимо указать: Текущий PIN-код администратора и Новый PIN-код администратора.

4. Установка и удаление утилиты JaCarta WebPass Tool

4.1 Описание пакетов установки

Утилита JaCarta WebPass Tool входит в состав программного комплекса Единый Клиент JaCarta. Утилита не имеет отдельного пакета установки. Установка Утилиты происходит с помощью дистрибутива Единого Клиента JaCarta. Дистрибутив Единого Клиента JaCarta включает пакеты установки, приведенные в Таблица 4.

Таблица 4 – Пакеты установки дистрибутива Единый Клиент JaCarta

Файл	***Описание***
JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi	Пакет установки для 32-разрядных операционных систем
JaCartaUnifiedClient_x.x.xx.xxx_win-x64_ru-Ru.msi	Пакет установки для 64-разрядных операционных систем

4.2 Системные требования

Системные требования к компьютеру, на котором должна быть установлена JaCarta WebPass Tool приведены в таблице 5.

Таблица 5 – Системные требования

Требование	***Содержание***
Поддерживаемые операционные системы	Microsoft Windows XP SP3 (32-бит) Microsoft Windows XP SP2 (64-бит) Microsoft Windows Vista SP2 (32/64-бит) Microsoft Windows 7 SP1 (32/64-бит) Microsoft Windows 8 (32/64-бит) Microsoft Windows 8.1 Update 1 (32/64-бит) Microsoft Windows 10 (32/64-бит) Microsoft Windows Server 2003 SP2 (32/64-бит) Microsoft Windows Server 2008 SP2 (32/64-бит) Microsoft Windows Server 2008 R2 SP1 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2
Поддерживаемые модели электронных ключей	JaCarta WebPass (модель JC600) JaCarta U2F/WebPass (модель JC603)
Необходимые аппаратные средства	USB-порт стандарта 1.1 и выше
Рекомендуемое разрешение экрана	Для корректного отображения интерфейса JaCarta WebPass Tool рекомендуется установить разрешение монитора не ниже 1024x768

4.3 Установка утилиты

Для установки утилиты JaCarta WebPass Tool необходимо выполнить следующие действия:

1. Если на компьютере не установлено ПО Единый Клиент JaCarta, запустить нужный файл установки в зависимости от разрядности операционной системы. Будет открыто окно Мастера установки Единый Клиент JaCarta (см. Рисунок 2). Перейти к следующему шагу установки с помощью нажатия на кнопку <Далее>.

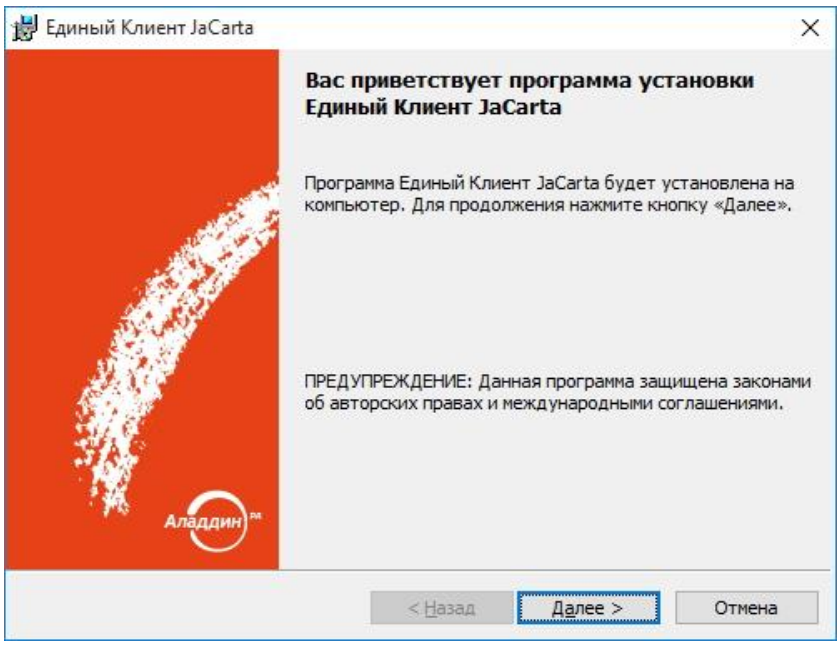


Рисунок 2 – Мастер установки Единый Клиент JaCarta

2. Если ПО Единый Клиент JaCarta уже установлено, то для установки утилиты необходимо перейти в [Приложения и возможности], выбрать в перечне Единый Клиент JaCarta и нажать кнопку <Изменить> (см. Рисунок 3).

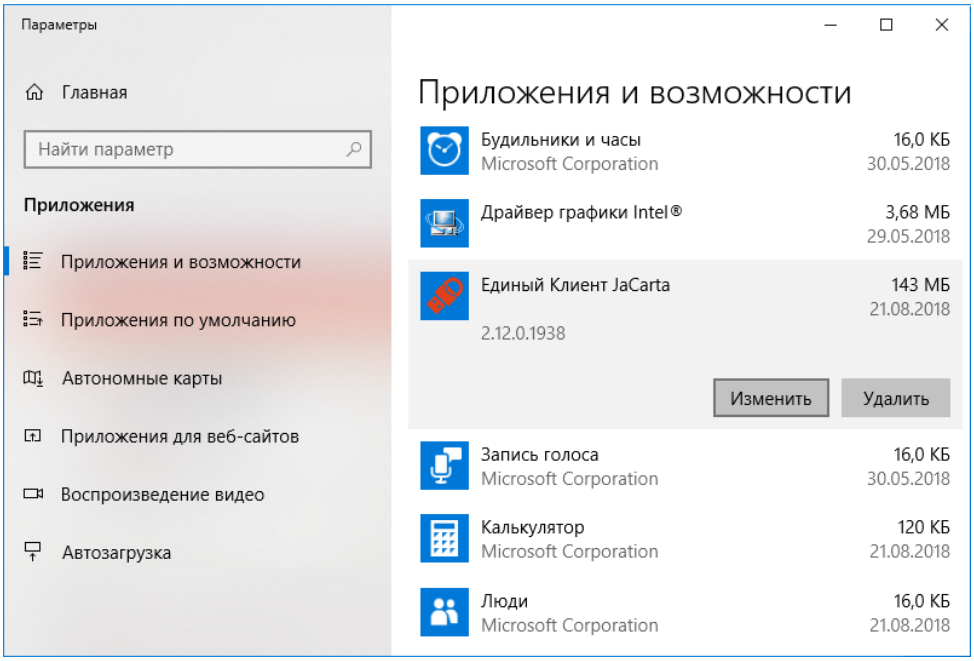


Рисунок 3 – Приложения и возможности. Изменение Единый Клиент JaCarta

3. Будет открыто окно Мастера изменений Единый Клиент JaCarta (см. Рисунок 4). Для перехода к следующему шагу необходимо нажать <Далее>.

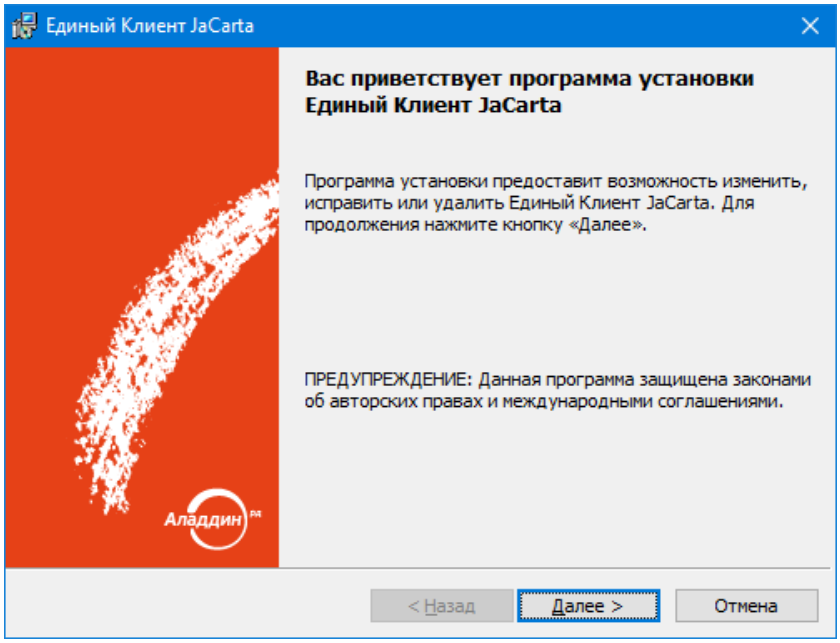


Рисунок 4 – Мастер изменений Единый Клиент JaCarta

4. Выбрать в окне [Вид установки] режим <Выборочная> (см. Рисунок 5). Перейти к следующему шагу с помощью кнопки <Далее>.

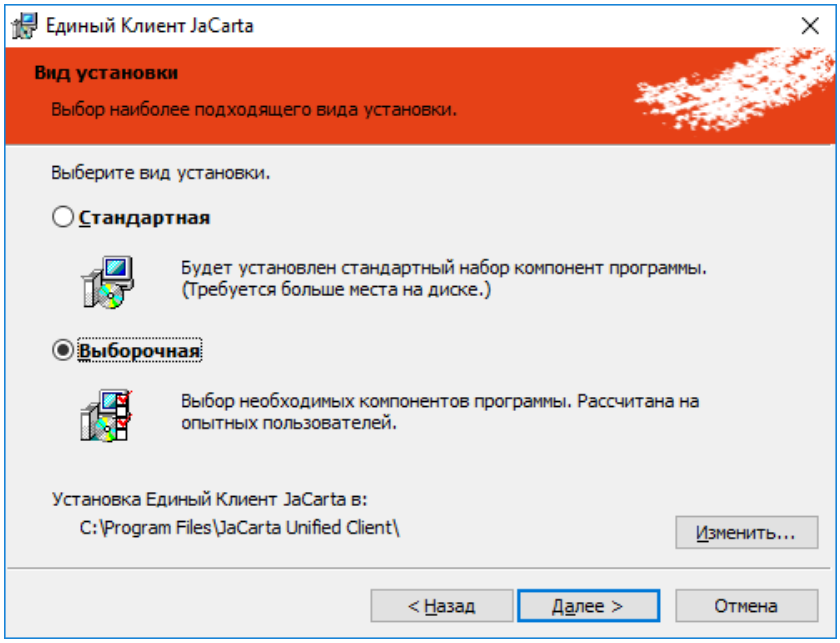


Рисунок 5 - Мастер установки Единый Клиент JaCarta. Окно [Вид установки]

5. Выбрать в окне [Изменение, исправление или удаление Единый Клиент JaCarta] режим <Изменить> (см. Рисунок 6). Перейти к следующему шагу с помощью кнопки <Далее>.

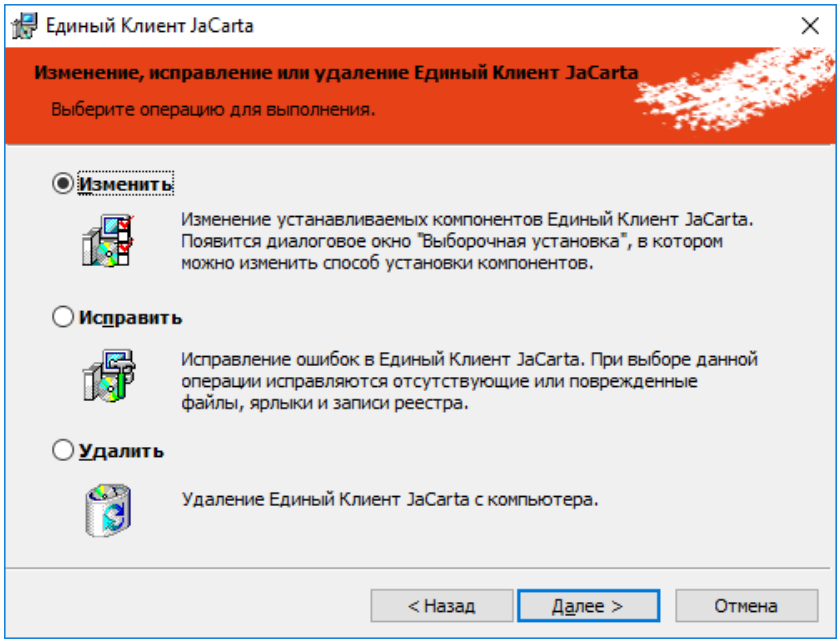


Рисунок 6 - Мастер изменений Единый Клиент JaCarta.
Окно [Изменение, исправление или удаление Единый Клиент JaCarta]

Подробное описание компонентов Единый Клиент JaCarta представлено в документе [JaCarta_UnifiedClient_2.12_AdminGuide]. Для установки компонента JaCarta WebPass Tool достаточно выбрать установку двух компонентов: [Единый клиент JaCarta] и [JaCarta WebPass Tool].

6. В окне [Выборочная установка] (см. Рисунок 7) в списке компонентов выбрать <JaCarta WebPass Tool>, раскрыть выпадающий список с помощью элемента ▼ и указать необходимую опцию установки. Нажать кнопку <Далее> для перехода к следующему шагу.

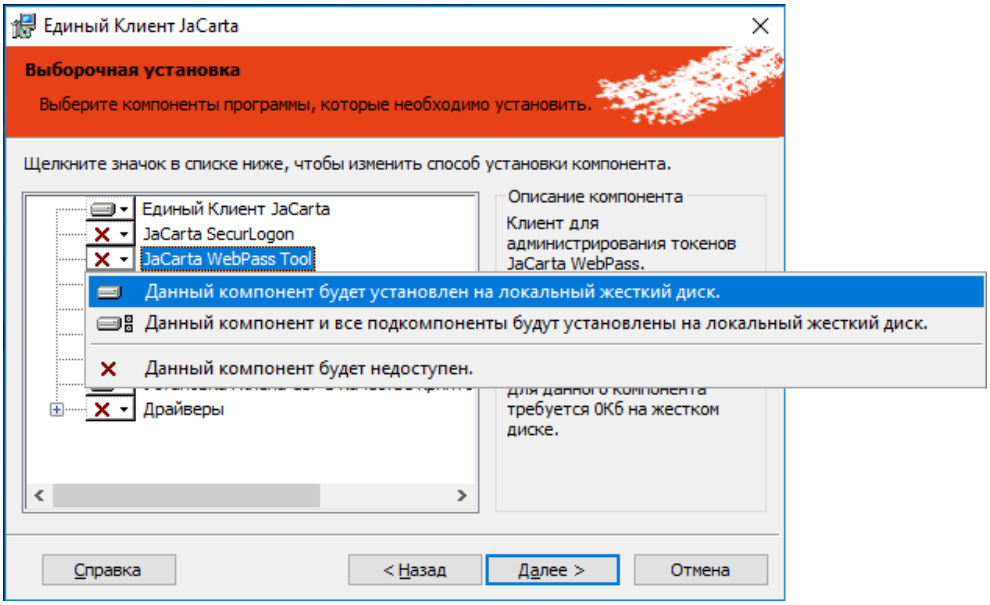


Рисунок 7 - Мастер установки Единый Клиент JaCarta. Окно [Выборочная установка]

7. В окне [Дополнительные параметры работы] необходимо выбрать способ автоматического обновления (см. Рисунок 8).

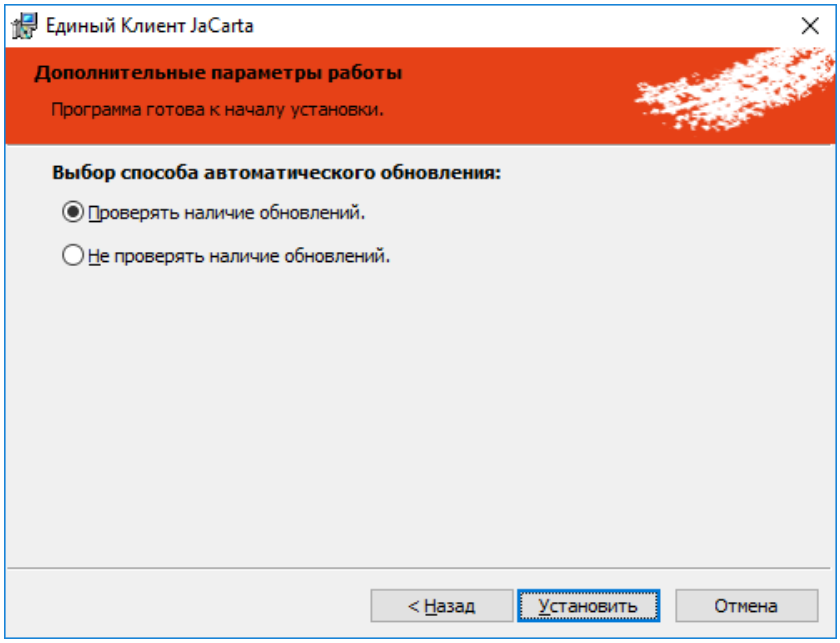


Рисунок 8 - Мастер установки Единый Клиент JaCarta. Окно [Дополнительные параметры работы]

8. После чего нажать кнопку <Установить> и перейти к процессу установки (см. Рисунок 9).

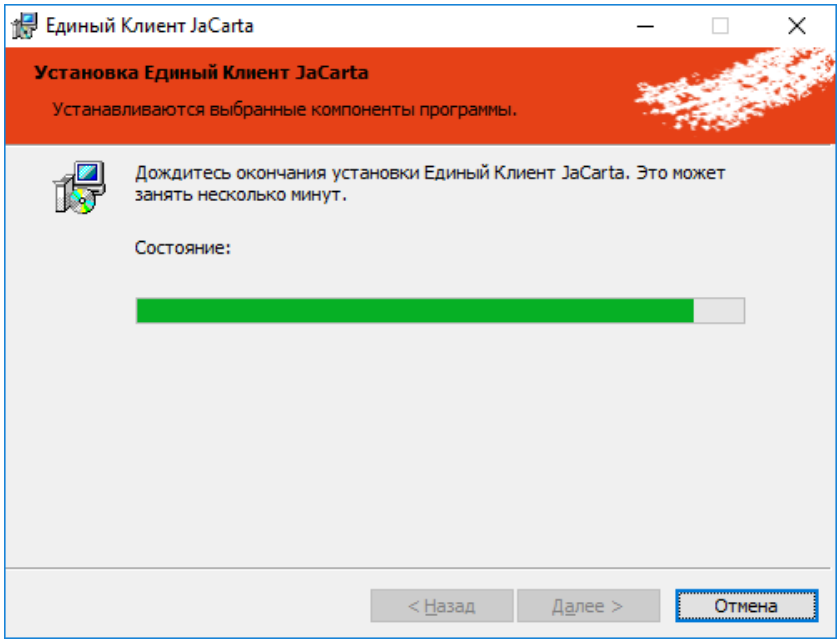


Рисунок 9 – Мастер установки Единый Клиент JaCarta. Окно [Установка Единый Клиент JaCarta]

9. По завершении установки будет отображено соответствующее окно (см Рисунок 10). Для завершения процесса установки необходимо нажать кнопку <Готово>.

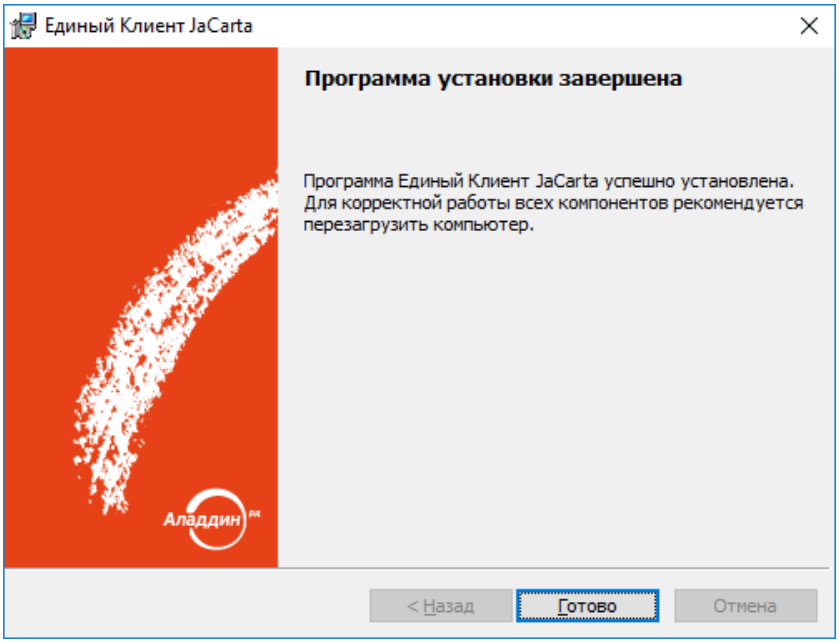


Рисунок 10 - Окно завершения установки Единый Клиент JaCarta

10. Перезагрузить компьютер, выбрав <Да> в появившемся окне (см Рисунок 11).

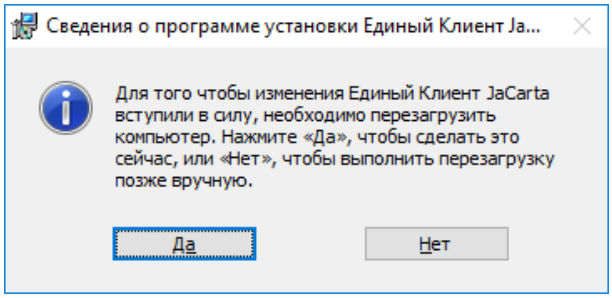


Рисунок 11 – Сообщение о необходимости перезагрузке компьютера

4.4 Удаление утилиты

Для удаления компонента JaCarta WebPass Tool необходимо выполнить следующие действия:

1. Последовательно выбрать [Пуск], [Параметры], [Приложения и возможности].

2. В окне [Приложения и возможности] выделить Единый Клиент JaCarta и нажать кнопку <Изменить> (см. Рисунок 12).

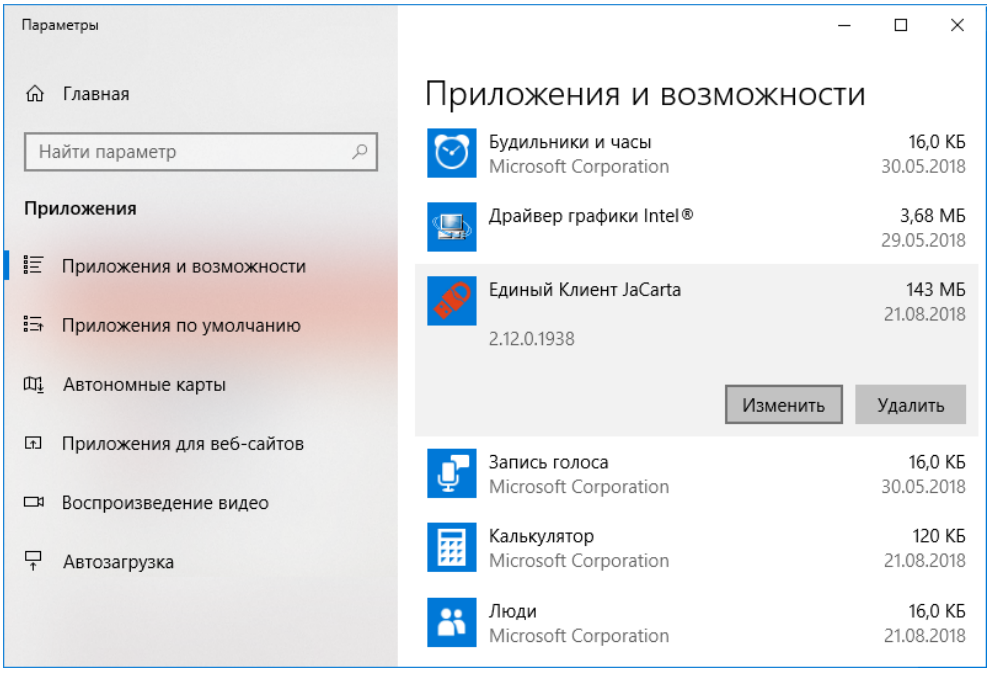


Рисунок 12 – Окно [Приложения и возможности]. Изменение Единый Клиент JaCarta

3. Будет открыто окно мастера установки Единый Клиент JaCarta (см. Рисунок 13). Для перехода к следующему шагу нажать кнопку <Далее>.

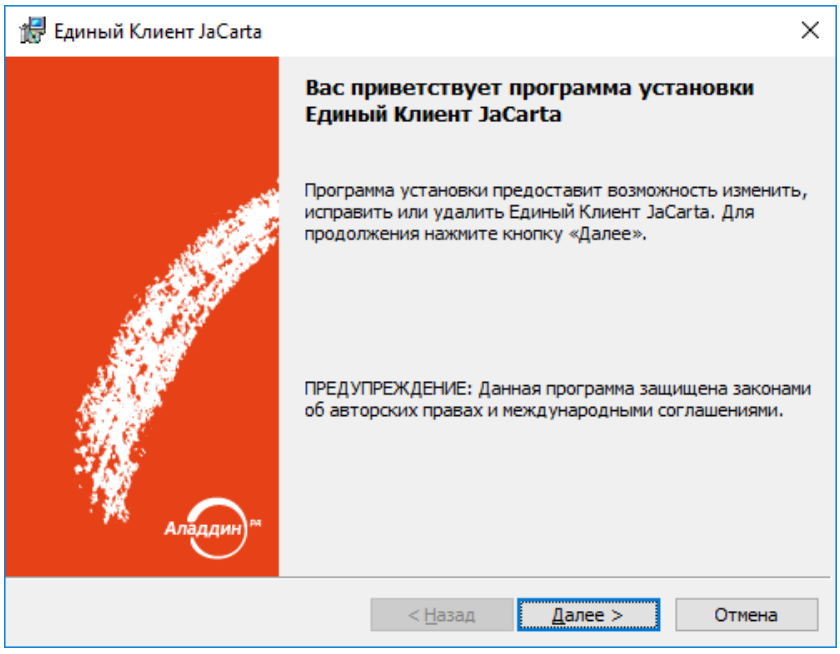


Рисунок 13 – Мастер установки Единый Клиент JaCarta

4. В окне [Изменение, исправление или удаление Единый Клиент JaCarta] (см. Рисунок 14) выбрать опцию <Изменить> и нажать кнопку <Далее>.

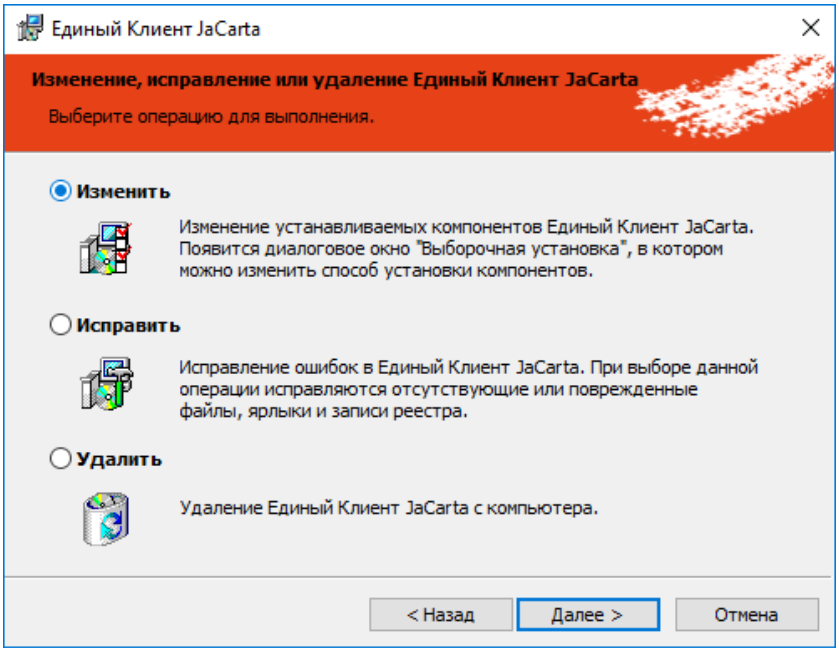


Рисунок 14 – Выбор операции мастера установки Единый Клиент JaCarta

5. Для удаления компонента JaCarta АРМ УЦ необходимо выбрать его в перечне, раскрыть выпадающий список с помощью элемента ▼ и в появившемся контекстном меню выбрать пункт <Данный компонент будет недоступен> (см. Рисунок 15). После нажать кнопку <Далее>.

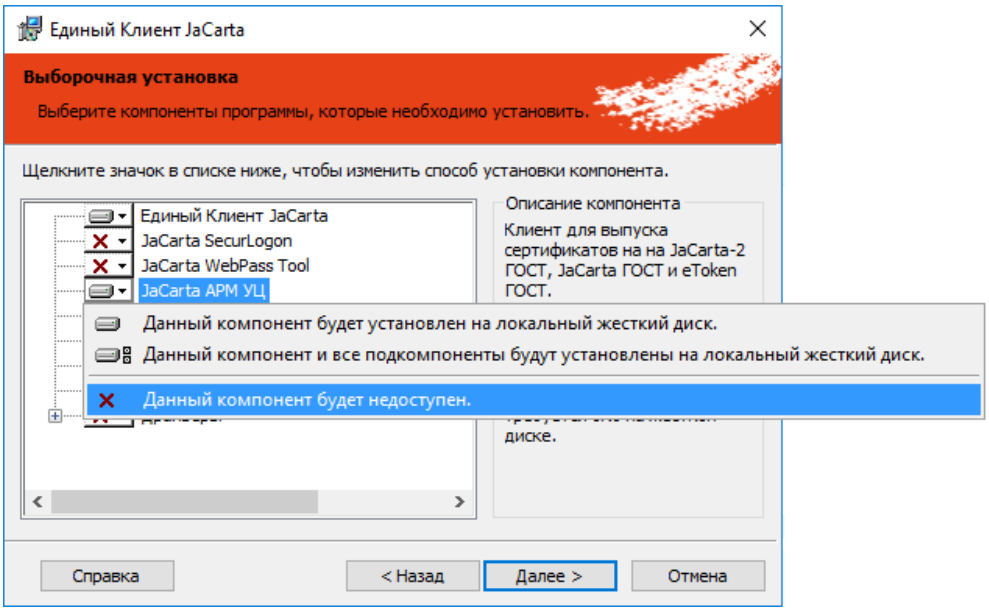


Рисунок 15 – Окно [Выборочная установка] мастера установки Единый Клиент JaCarta

6. В окне [Дополнительные параметры работы] (см. Рисунок 16) выбрать способ автоматического обновления, нажать кнопку <Изменить> и дождаться окончания удаления компонента.

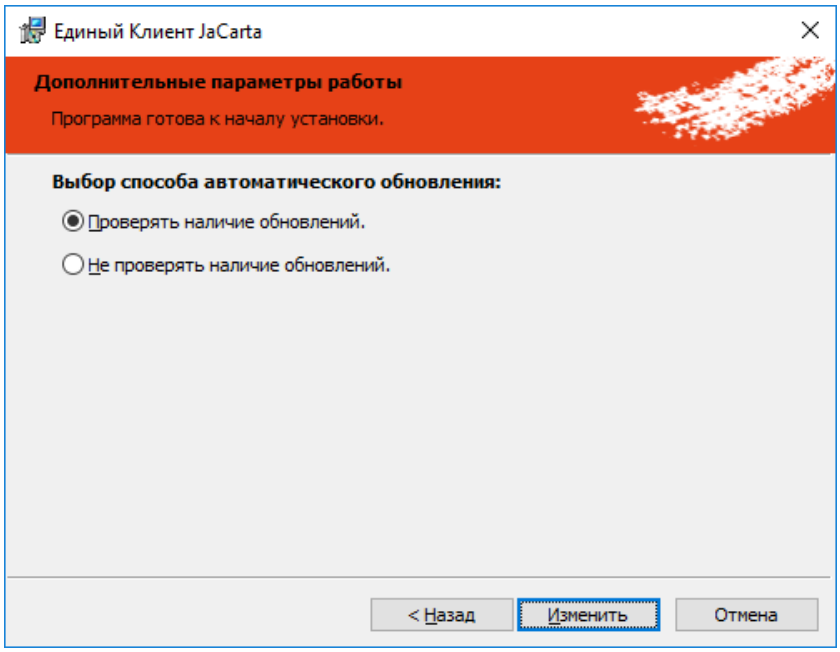


Рисунок 16 - Окно [Дополнительные параметры работы] мастера установки Единый Клиент JaCarta

7. После завершения внесения изменений программой будет отображено соответствующее окно (см. Рисунок 17).

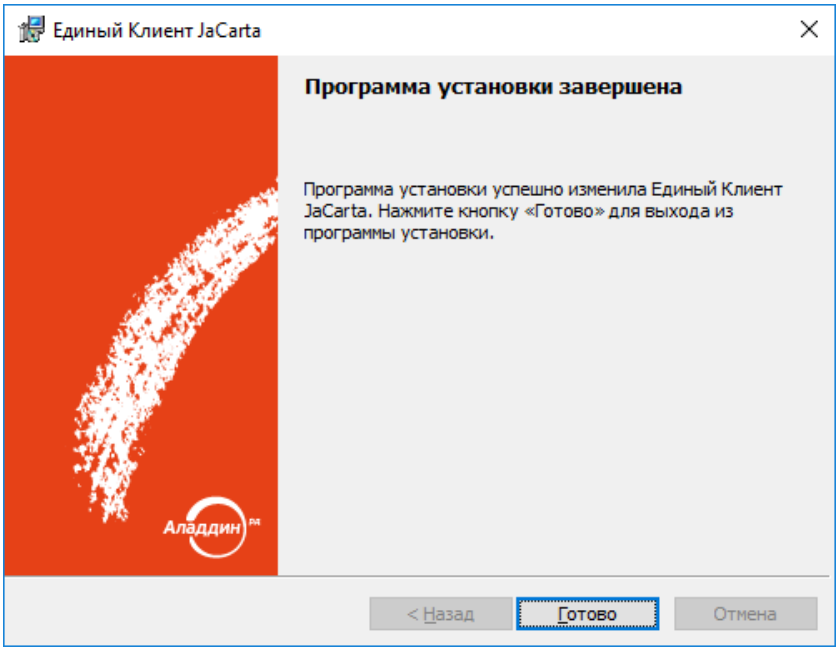


Рисунок 17 – Успешное удаление компонента с помощью мастера установки Единый Клиент JaCarta

8. Перезагрузить компьютер после отображения соответствующего предупреждения.

5. Запуск утилиты и обзор пользовательского интерфейса

5.1 Запуск утилиты JaCarta WebPass Tool

Для запуска утилиты JaCarta WebPass Tool необходимо выбрать [Пуск], раскрыть папку [Аладдин Р.Д.] и выбрать в ней [JaCarta WebPass Tool] (см. Рисунок 18).

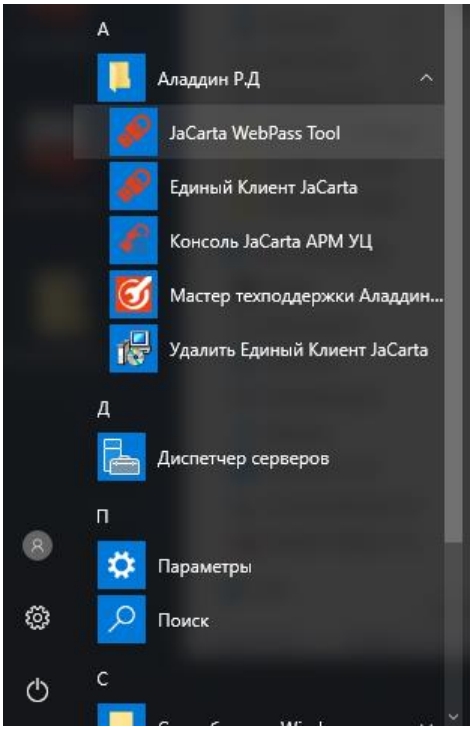


Рисунок 18 – Запуск утилиты JaCarta WebPass Tool

После запуска утилиты JaCarta WebPass Tool окно основного интерфейса будет выглядеть следующим образом (см. Рисунок 19).

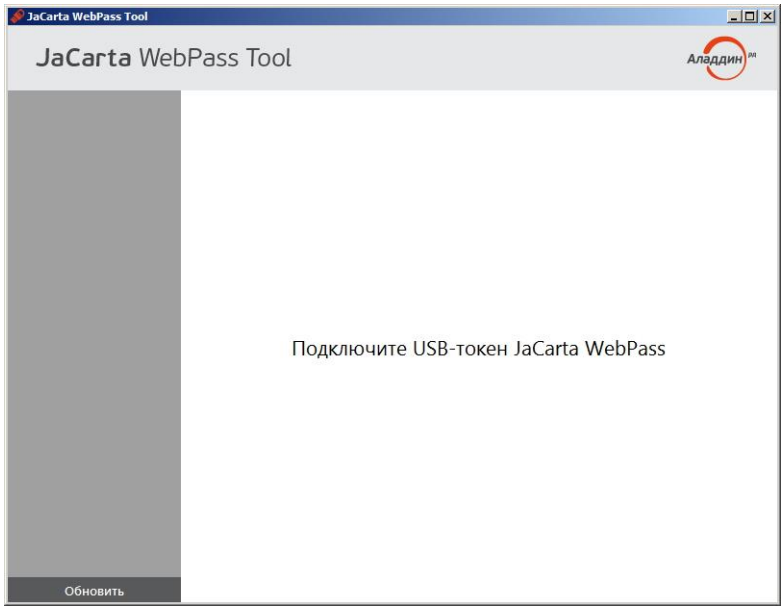


Рисунок 19 - JaCarta WebPass Tool. Главное окно

При нажатии на логотип компании Аладдин в верхнем правом углу окна – появится окно со сведениями об утилите JaCarta WebPass Tool (см. Рисунок 20).

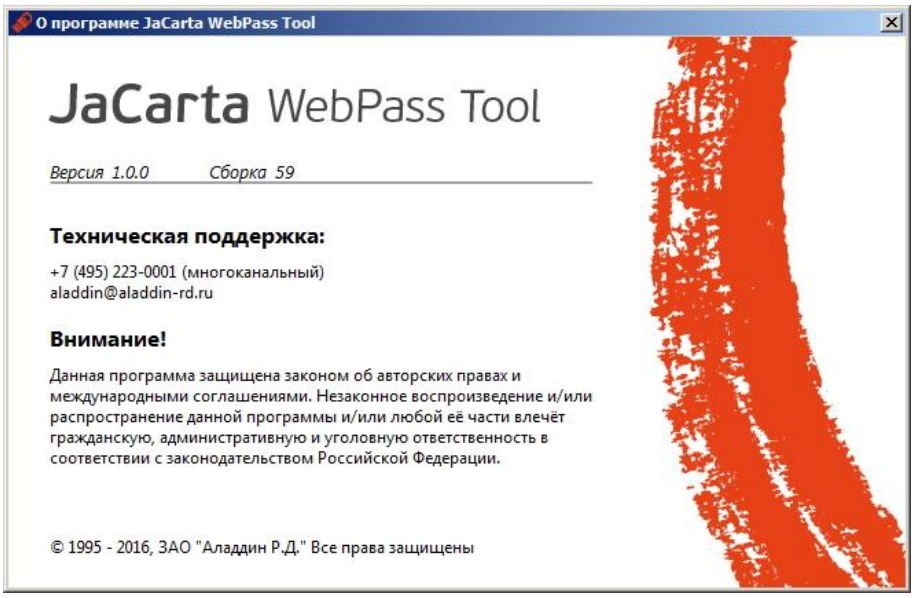


Рисунок 20 - JaCarta WebPass Tool. Окно [О программе]

Подключите электронный ключ JC-WebPass к USB-порту.

При первом подключении электронного ключа JC-WebPass к компьютеру будет выполнен поиск и установка драйверов, необходимых для работы с электронным ключом. Все драйверы будут установлены автоматически без подключения к сайту Microsoft Windows Update. Действие будет произведено один раз и при последующих подключениях этого электронного ключа JaCarta WebPass к компьютеру повторяться не будет. При подключении к данному компьютеру другого электронного ключа той же модели, диалог будет отображен повторно.

Драйвер ***смарт-карты*** не требуется для работы утилиты JaCarta WebPass Tool с электронными ключами JaCarta WebPass и не обязателен для установки.

После того, как драйвера установлены, запустите утилиту JaCarta WebPass Tool. Окно основного интерфейса будет выглядеть следующим образом:

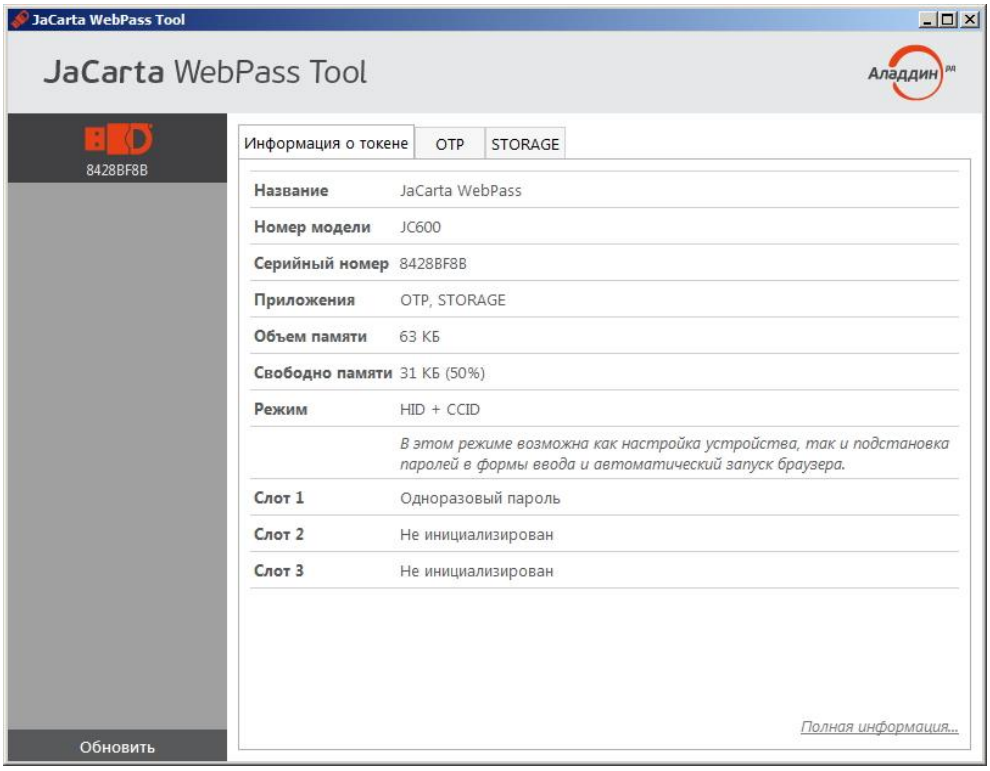


Рисунок 21 - JaCarta WebPass Tool. Главное окно после установления драйверов

В левой панели отображаются подсоединённые к компьютеру электронные ключи.

В нижней части левой панели расположена кнопка <Обновить> – для осуществления повторного поиска и опроса поддерживаемых электронных ключей (обновления списка подключенных устройств).

В правой панели окна отображаются вкладки. Описание вкладок приведено в таблице 6.

Таблица 6 - JaCarta WebPass Tool. Главное окно. Описание вкладок

Вкладка	***Описание***
Информация о токене	На этой вкладке отображаются общие сведения о выбранном электронном ключе. Чтобы отобразить подробные сведения, нажмите <<Полная информаци> (Подробнее см. "Вкладка [Информация о токене")
OTP	На этой вкладке отображаются кнопки операций, выполняемых в приложении OTP, а также интерфейс выбора одного из трех слотов электронного ключа с указанием характеристик выбранного слота
STORAGE	На этой вкладке отображается интерфейс перехода в Единый Клиент JaCarta для дальнейшей работы с приложением STORAGE

5.2 Описание вкладок

5.2.1 Вкладка [Информация о токене]

Вкладка [Информация о токене] имеет следующий вид:

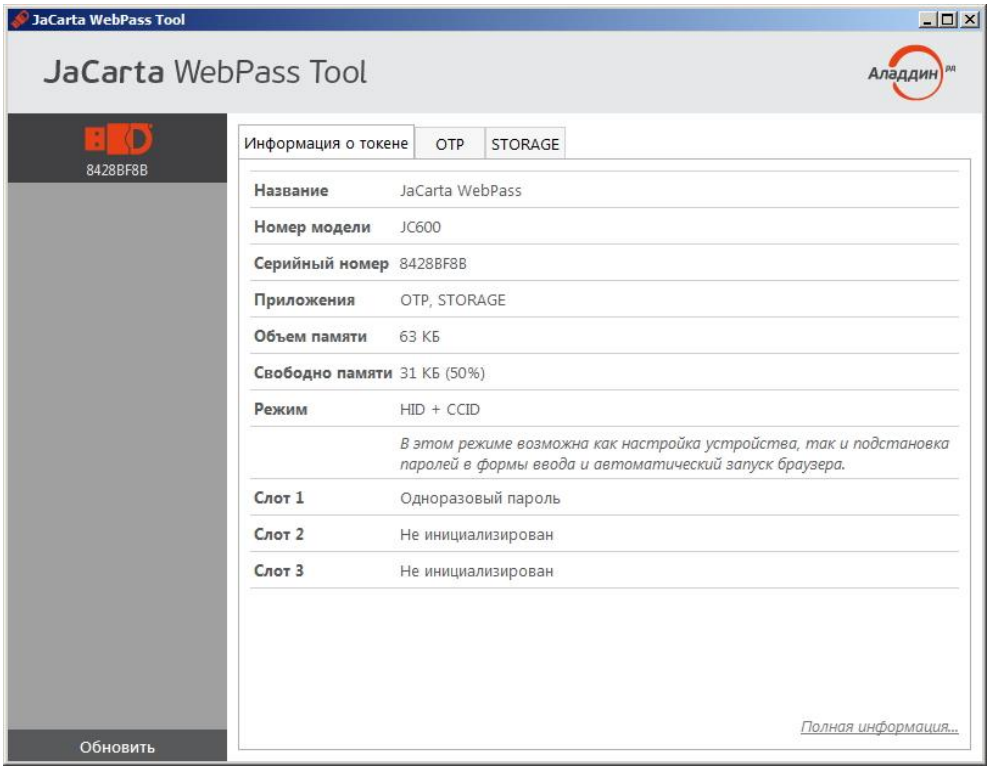


Рисунок 22 - JaCarta WebPass Tool. Вкладка [Информация о токене]

Описание отображаемых полей на вкладке [Информация о токене] приведено в таблице 7.

Таблица 7 - JaCarta WebPass Tool. Вкладка [Информация о токене]. Описание настроек

Поле	*Описание*
Название	Название модели выбранного электронного ключа
Номер модели	Номер модели выбранного электронного ключа
Серийный номер	Серийный номер выбранного электронного ключа Серийный номер электронного ключа указывается также на его корпусе
Приложения	Приложения, установленные на выбранном электронном ключе
Объем памяти	Полный объём памяти выбранного электронного ключа
Свободно памяти	Объём свободной памяти выбранного электронного ключа
Режим	Режим работы электронного ключа
Слот 1	Информация об инициализации слота, типе слота и блокировании слота
Слот 2	Информация об инициализации слота, типе слота и блокировании слота
Слот 3	Информация об инициализации слота, типе слота и блокировании слота

В нижнем правом углу вкладки располагается элемент управления <Полная информация>, нажатие на который открывает окно с подробными сведениями о выбранном электронном ключе (см. Рисунок 23).

Рисунок 23 - JaCarta WebPass Tool. Окно [Подробная информация о токене]

Описание предоставляемой информации об электронном ключе приведено в таблице 8.

Таблица 8 - JaCarta WebPass Tool. Окно [Подробная информация о токене]. Описание настроек

Поле	***Описание***
Название считывателя	Название считывателя выбранного электронного ключа
Название	Название выбранного электронного ключа
Номер модели	Номер модели выбранного электронного ключа
Серийный номер	Серийный номер микросхемы выбранного электронного ключа
Приложения	Приложения, установленные на выбранном электронном ключе
Объем памяти	Объём памяти выбранного электронного ключа
Свободно памяти	Объём свободной памяти выбранного электронного ключа
Версия прошивки	Номер версии прошивки выбранного электронного ключа
Дата производства	Дата производства выбранного электронного ключа
Режим	Режим работы выбранного электронного ключа
Код последней ошибки	Код последней ошибки выбранного электронного ключа
Количество нажатий на кнопку	Количество нажатий на кнопку выбранного электронного ключа
Количество USB подключений	Количество USB подключений выбранного электронного ключа

5.2.2 Вкладка [OTP]

Вкладка [OTP] имеет вид, представленный на рисунке ниже:

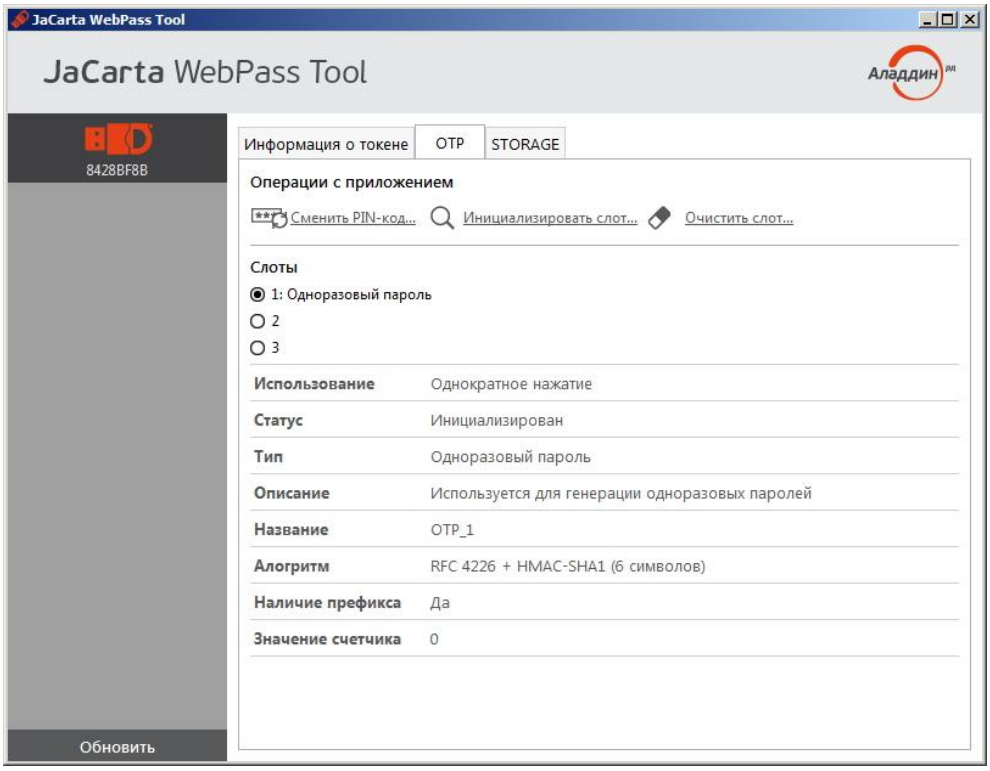


Рисунок 24 - JaCarta WebPass Tool. Вкладка [OTP]

Описание отображаемых элементов на вкладке [OTP] приведено в Таблица 9.

В зависимости от типа выбираемого слота (Одноразовый пароль/Интернет адрес/Пароль) и его статуса (Инициализирован/Не инициализирован), некоторые поля, описанные в таблице 9Таблица 9 могут отображаться, либо не отображаться на вкладке [OTP].

Таблица 9 - JaCarta WebPass Tool. Вкладка [OTP]. Описание настроек

Элемент интерфейса	***Описание***
Сегмент ***Операции с приложением***	В сегменте расположены три кнопки: •  – для смены PIN-кода электронного ключа (подробнее см. подраздел 7.2 Смена PIN-кода администратора); •  – для запуска мастера инициализации слота электронного ключа (подробнее см. раздел 7.Инициализация слотов); •  – для очистки заданных при инициализации настроек слота электронного ключа (подробнее см. раздел 9. Очистка слотов)
Сегмент ***Слоты:***	В сегменте расположены три чек бокса для выбора одного из трех слотов: ***1***, ***2*** или ***3***. После выбора слота ниже отображается информация о его характеристиках
Поле ***Использование***	Способ нажатия на кнопку электронного ключа для использования выбранного слота: • Слот №1 – однократное нажатие на кнопку; • Слот №2 – двойное нажатие на кнопку; • Слот №3 – длительное нажатие на кнопку (2-3 секунды).
Поле ***Статус***	Информация об инициализации выбранного слота или его блокировании
Поле ***Тип***	Тип выбранного слота (Одноразовый пароль/Интернет адрес/Пароль): • Одноразовый пароль – слот для генерации одноразовых паролей; • Интернет адрес – слот для хранения адреса Web-ресурса; • Пароль – слот для генерации и хранения многоразового пароля настраиваемого уровня сложности
Поле ***Описание***	Описание предназначения выбранного слота
Поле ***Название***	Название выбранного слота. Например, тип слота и номер (максимум 32 символа)
Поле ***Алгоритм***	Алгоритм вычисления одноразового пароля Поддерживается четыре алгоритма генерации одноразовых паролей (event -based алгоритмы согласно RFC 4226)
Поле ***Наличие префикса***	Сведения о наличии префикса в пароле (Да/Нет)
Поле ***Значение счетчика***	Текущее значение счетчика генераций (число от 0 до 2^{31})

Элемент интерфейса	***Описание***
Поле ***Критерии качества паролей***	Критерии качества паролей, указанные при инициализации слота: • длина пароля (количество символов от 4 до 160); • использовать в пароле английские буквы нижнего регистра (да/нет); • использовать в пароле английские буквы верхнего регистра (да/нет); • использовать в пароле цифры (да/нет); • использовать в пароле спецсимволы (да/нет)

5.2.3 Вкладка [STORAGE]

На электронных ключах JaCarta WebPass существует возможность хранения ключевых контейнеров программных СКЗИ (КриптоПро CSP и пр.). Приложение STORAGE является дополнительным приложением. Для работы с электронными ключами JaCarta WebPass переходить на вкладку STORAGE не обязательно.

Вкладка [STORAGE] имеет вид, представленный на рисунке 25.

На вкладке [STORAGE] расположена кнопка <Открыть Единый Клиент JaCarta>, при нажатии на которую запускается Единый Клиент JaCarta, после чего можно выполнить следующие операции:

- Сменить PIN-код пользователя;
- Сменить PIN-код администратора;
- Разблокировать PIN-код пользователя;
- Инициализировать электронный ключ;
- Выполнить операции с объектами, хранящимися в памяти электронного ключа (просмотр содержимого объекта, импорт, экспорт и удаление объекта).

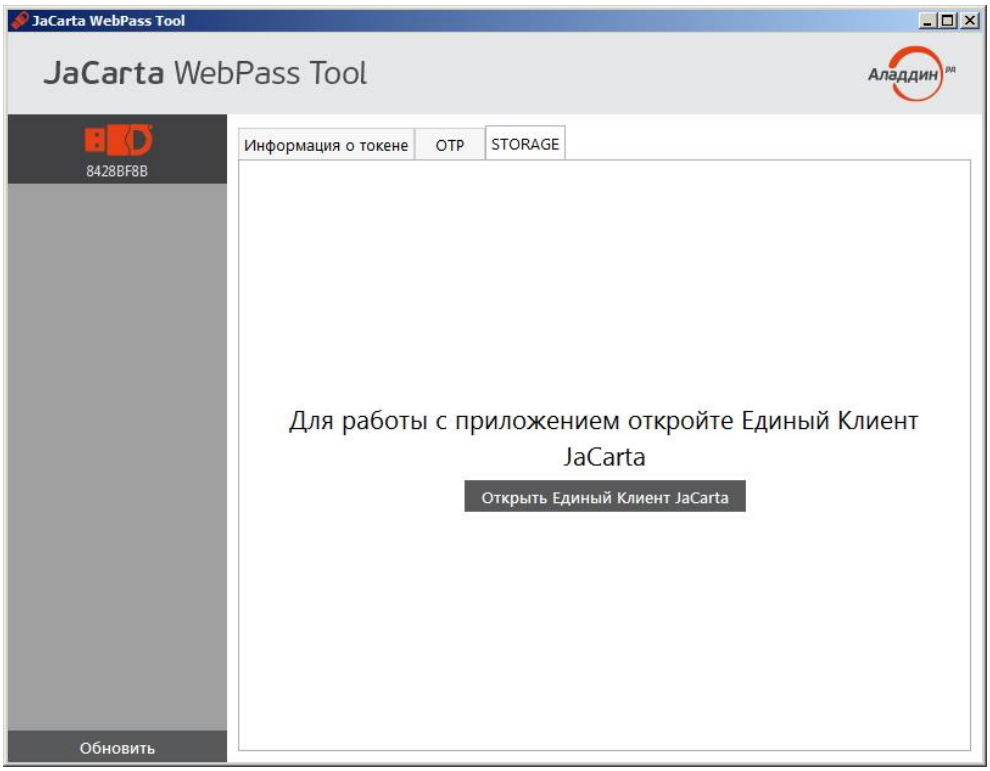


Рисунок 25 - JaCarta WebPass Tool. Вкладка [STORAGE]

Подробное описание операций в Приложении STORAGE см. в документе [Единый Клиент JaCarta. Руководство администратора - JaCarta_UnifiedClient_2.12_AdminGuide].

Подробное описание операций с объектами, хранящимися в памяти электронного ключа см. в документе [Единый Клиент JaCarta. Руководство пользователя - JaCarta_UnifiedClient_2.12_UserGuide].

5.3 Операции, выполняемые в приложении OTP

5.3.1 Смена PIN-кода администратора

Для смены PIN-кода необходимо перейти на вкладку [OTP] и нажать кнопку 

.

В появившемся окне (см. Рисунок 26) введите текущий PIN-код администратора, после чего введите новый PIN-код администратора и подтвердите его еще раз, затем нажмите кнопку <Сменить>.

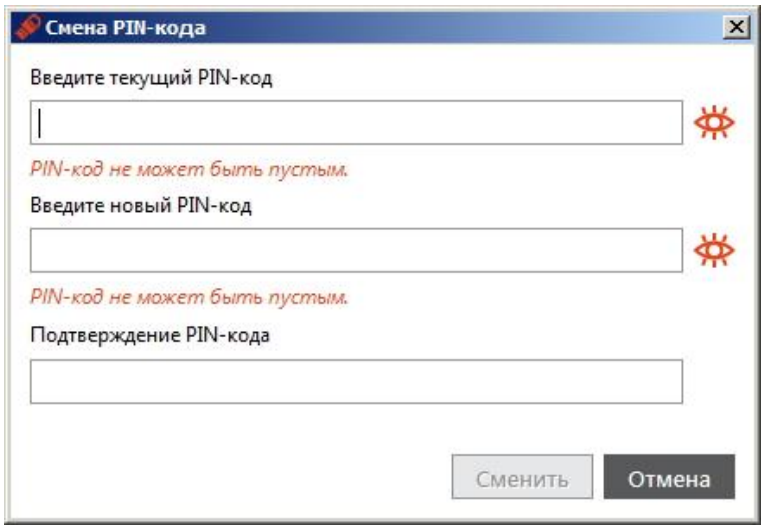


Рисунок 26 - JaCarta WebPass Tool. Вкладка [OTP]. Окно [Смена PIN-кода]

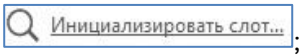
5.3.2 Инициализация слотов

Процесс инициализации слотов различается в зависимости от их типа (Одноразовый пароль/Интернет адрес/Пароль).

> *Инициализацию слота должен производить администратор. В процессе инициализации слота предыдущие значения параметров слота (если они ранее были записаны в слот)* ***УДАЛЯЮТСЯ****!*

5.3.2.1 Инициализация слота [Одноразовый пароль]

Для инициализации слота типа <Одноразовый пароль> выполните следующие действия:

1. На вкладке [OTP] выберите слот, который необходимо инициализировать;
2. Нажмите кнопку 

;

3. В окне [Мастер инициализации слота (1)] в выпадающем списке [Тип слота] выберите: <Одноразовый пароль>.

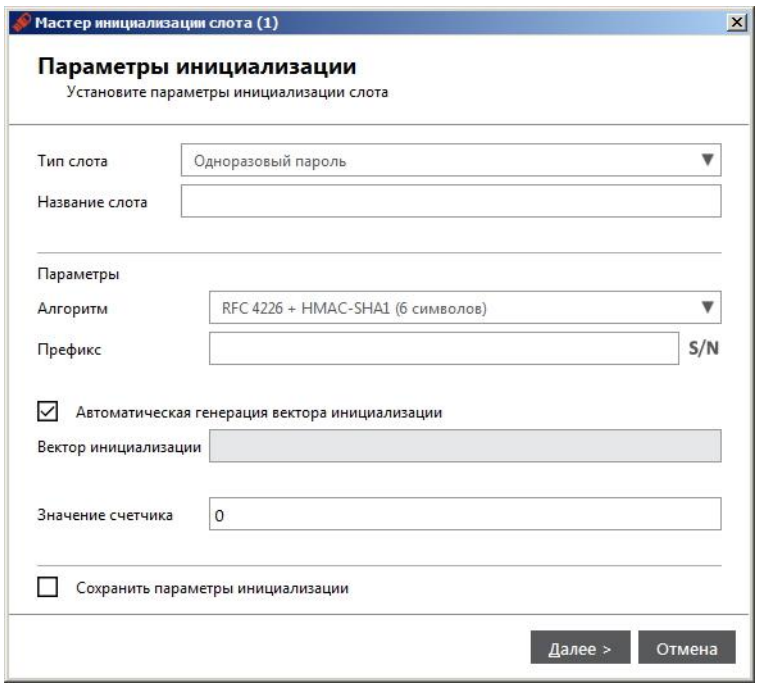


Рисунок 27 – JaCarta WebPass Tool. Окно [Мастер инициализация слота (1)]. Выбор типа слота

4. В поле [Название слота] введите название (например: OTP_1 или любой другой.

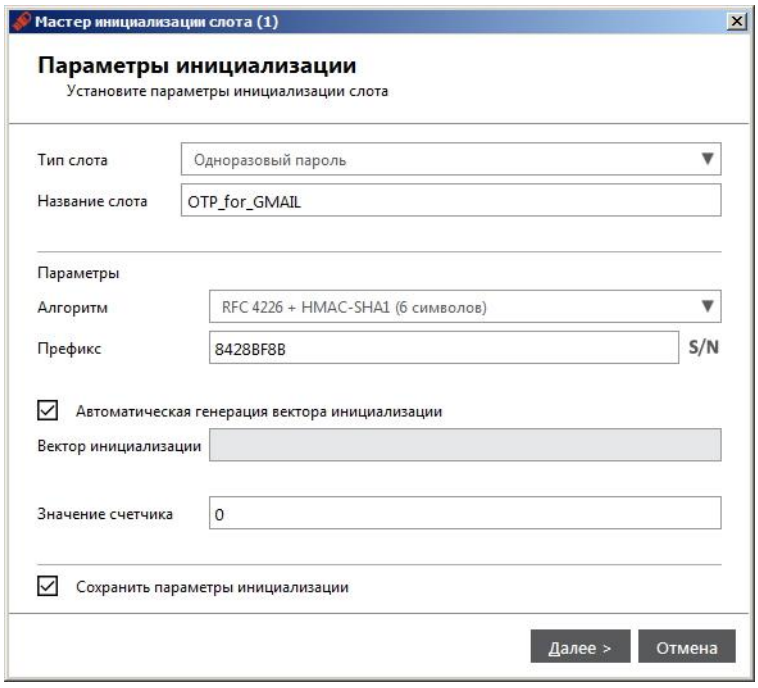


Рисунок 28 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (1)]. Задание названия слота

5. В поле [Алгоритм] из выпадающего списка выберите алгоритм вычисления одноразового пароля:
   - RFC 4226 + HMAC-SHA-1, длина одноразового пароля = 6 символов;
   - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 6 символов;
   - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 7 символов;
   - RFC 4226 + HMAC-SHA-256, длина одноразового пароля = 8 символов;

6. В поле [Префикс] при необходимости ввести префикс – введите его либо оставьте поле пустым;

На этапе инициализации существует возможность задать дополнительное постоянное значение (префикс), которое будет автоматически подставляться перед значением одноразового пароля. Таким образом, итоговое значение подставляемого пароля будет содержать больше символов, чем значение собственно одноразового пароля. Длина префикса не более 32-х символов.

При нажатии на кнопку 

в поле [Префикс] автоматически вставляется серийный номер электронного ключа.

7. Выберите опцию <Автоматическая генерация вектора инициализации> или введите последовательность из 20 символов в поле [Вектор инициализации];
8. В поле [Значение счетчика] введите значение счетчика генераций;
9. Выберите опцию <Сохранить параметры инициализации> (если необходимо сохранить настройки инициализации для последующих инициализаций других слотов);

Примечание – Существует возможность сохранить введенные параметры инициализации, чтобы в случае повторной инициализации этого слота с такими же параметрами не вводить их повторно.

10. Нажмите <Далее> и в появившемся окне (см. Рисунок 29) выберите формат конфигурационного файла: SAM/JMS/JAS;

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

11. Нажмите кнопку <Обзор> и выберите место сохранения конфигурационного файла, если файл не существует, то введите имя файла и нажмите <Сохранить>.

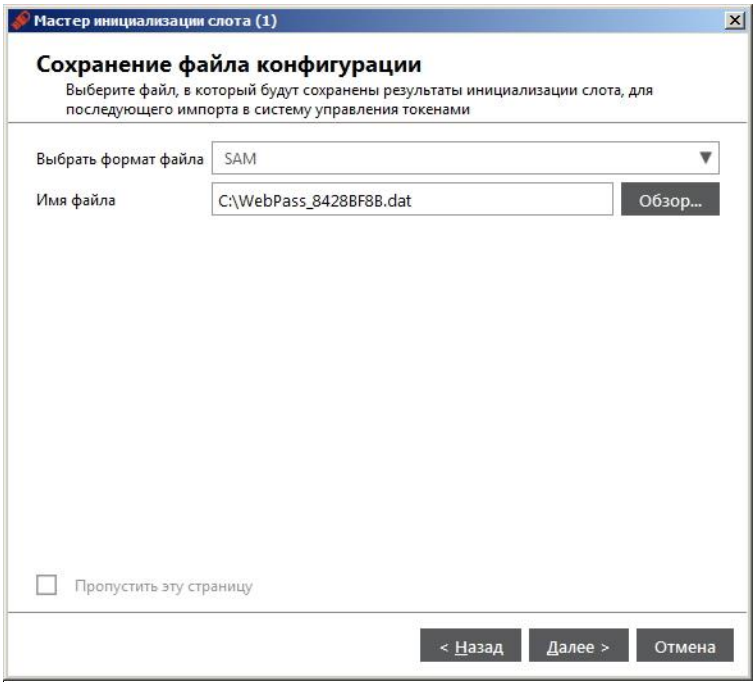


Рисунок 29 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (1)]. Сохранения файла конфигурации

12. Если конфигурационный файл создавать и сохранять не требуется, то поставьте галочку <Пропустить эту страницу>.
13. Нажмите <Далее>.
14. В появившемся окне (см. Рисунок 30) введите PIN-код администратора в одноименном поле, после чего нажмите кнопку <Выполнить>.

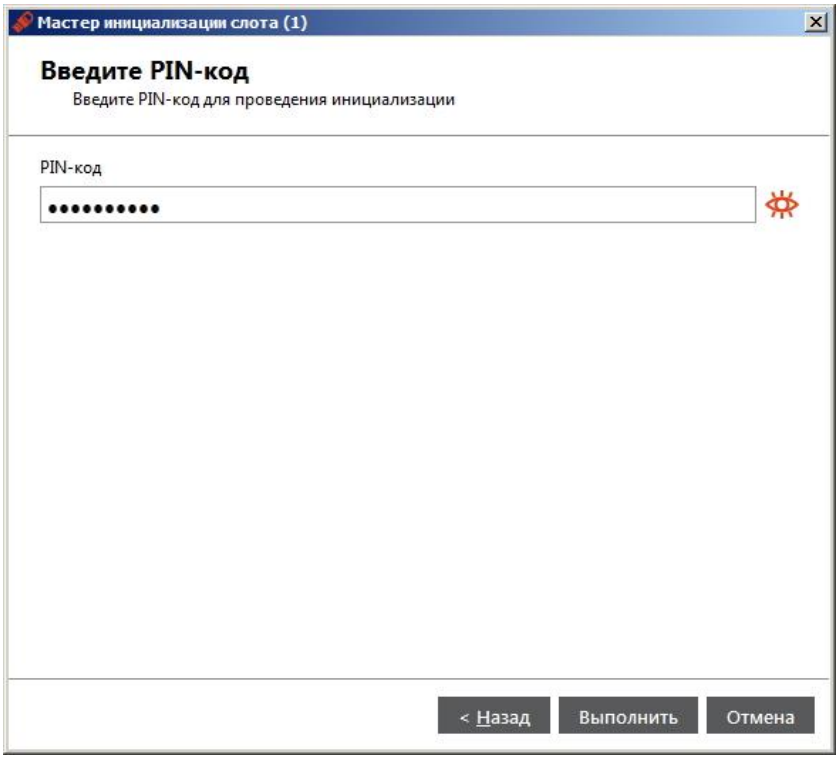


Рисунок 30 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (1)]. Ввод PIN-кода

15. Для перехода в папку с сохраненным конфигурационным файлом поставьте галочку <Выбрать файлы при помощи программы Проводник> (см. Рисунок 31). В таком случае, после нажатия кнопки <Завершить> будет открыта папка с сохраненным конфигурационным файлом.

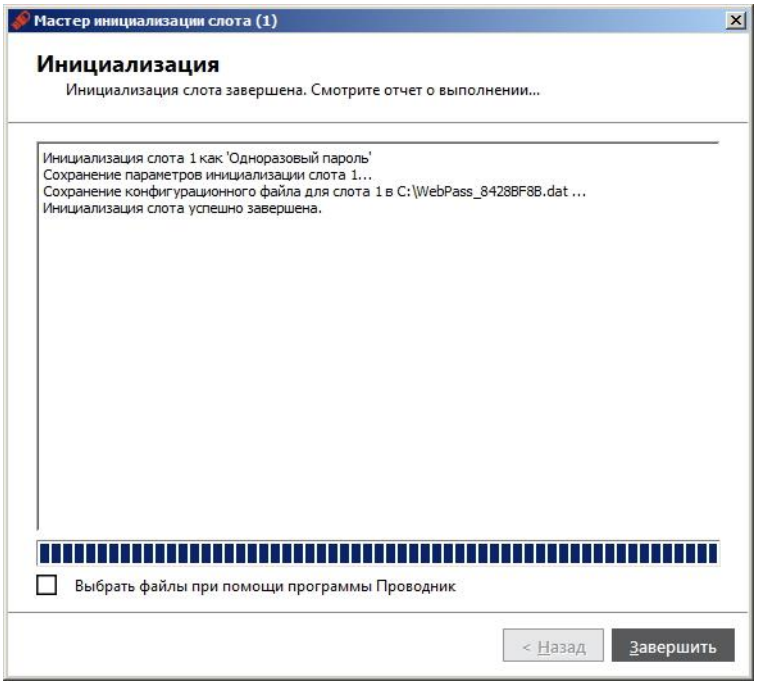
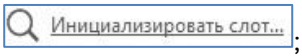


Рисунок 31 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (1)]. Процесс инициализации

16. После окончания процесса инициализации нажмите <Завершить>.

5.3.2.2 Инициализация слота [Интернет адрес]

Для инициализации слота типа <Интернет адрес> выполните следующие действия:

1. На вкладке [OTP] выберите слот, который необходимо инициализировать;
2. Нажмите кнопку 

;
3. В появившемся окне:
   - в поле [Тип слота] выберите <Интернет адрес> (см. рисунок 32) ;
   - в поле [Название слота] введите название, например: URL_1 (см. рисунок 33);
   - в поле [Операционная система] выберите тип операционной системы: Windows/Mac OS/Linux;
   - в поле [Интернет адрес] введите адрес интернет ресурса, на который будет осуществлен переход при нажатии на кнопку электронного ключа (например: http://gmail.ru);

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

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

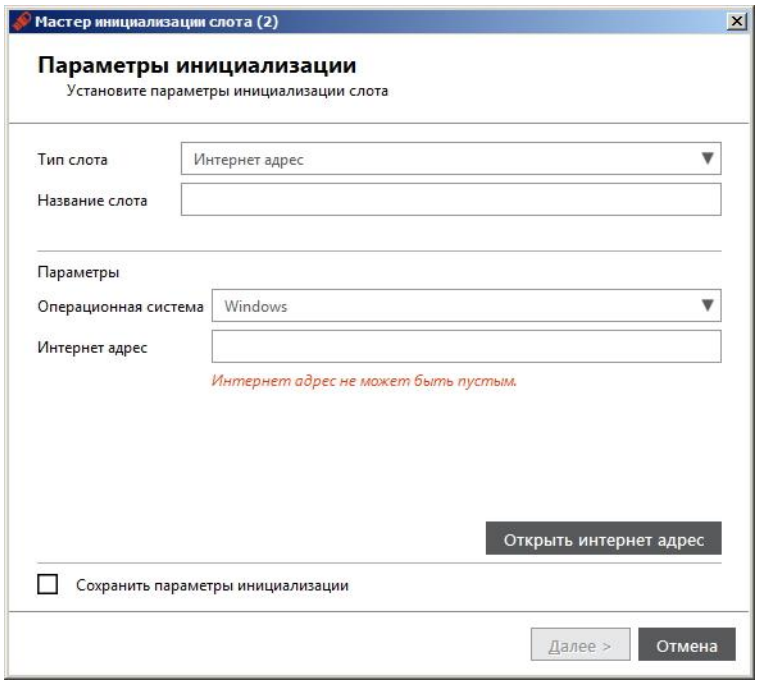


Рисунок 32 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (2)]. Выбор типа слота

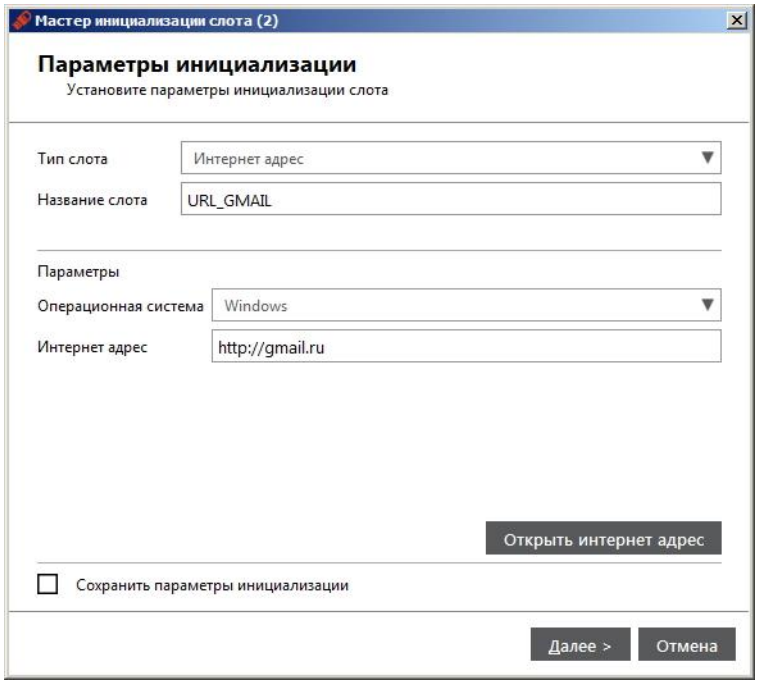


Рисунок 33 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (2)]. Параметры инициализации

4. Нажмите <Далее>. В появившемся окне введите PIN-код администратора в одноименное поле, после чего нажмите кнопку <Выполнить>.

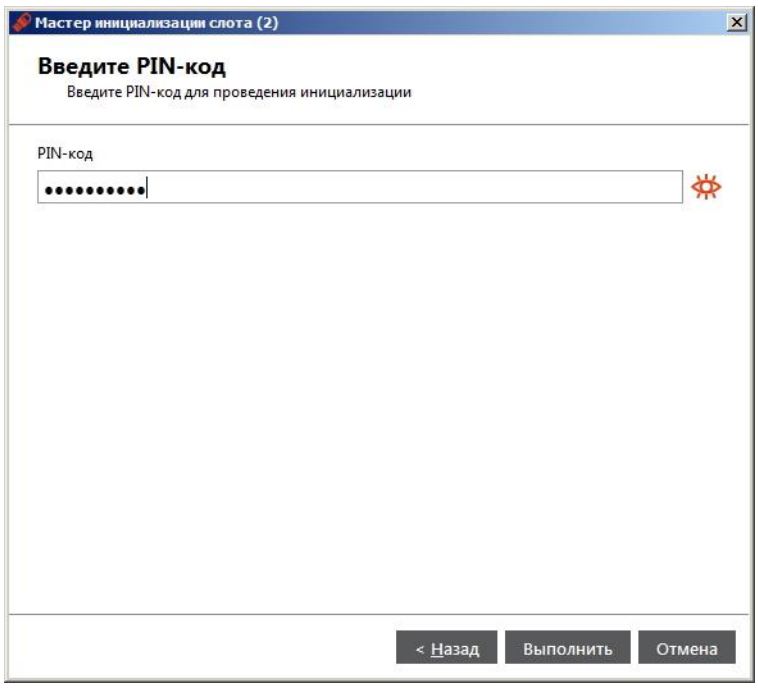


Рисунок 34 – JaCarta WebPass Tool. Окно [Мастер инициализация слота (2)]. Ввод PIN-кода

5. В появившемся окне нажмите кнопку <Завершить>.

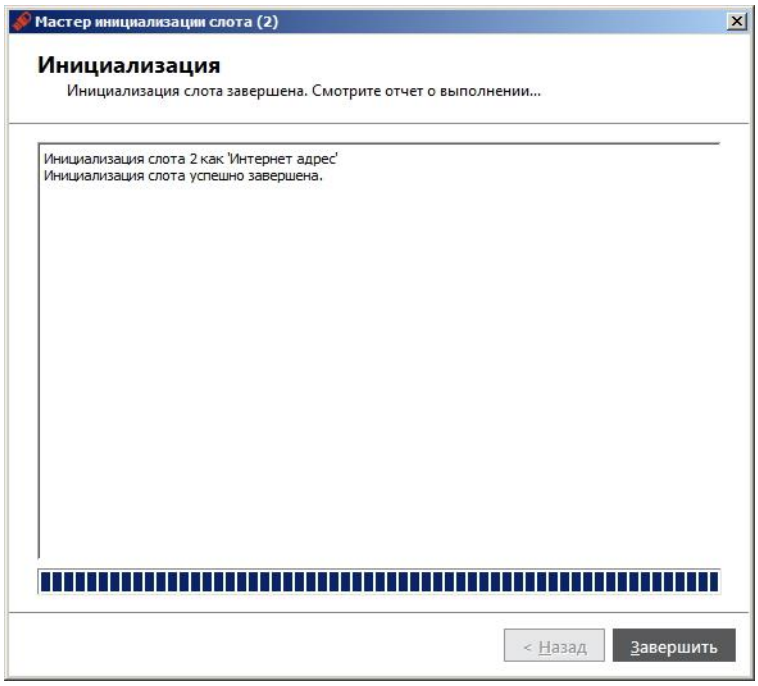


Рисунок 35 – JaCarta WebPass Tool. Окно [Мастер инициализация слота (2)]. Процесс инициализации

5.3.2.3 Инициализация слота [Пароль]

Для инициализации слота типа <Пароль> выполните следующие действия:

1. На вкладке [OTP] выберите слот, который необходимо инициализировать;
2. Нажмите кнопку 

;

3. В появившемся окне:
   - в поле [Тип слота] выберите значение <Пароль> (см. рисунок 36);
   - В поле [Название слота] введите название, например: PASS_1 (см. рисунок 37);

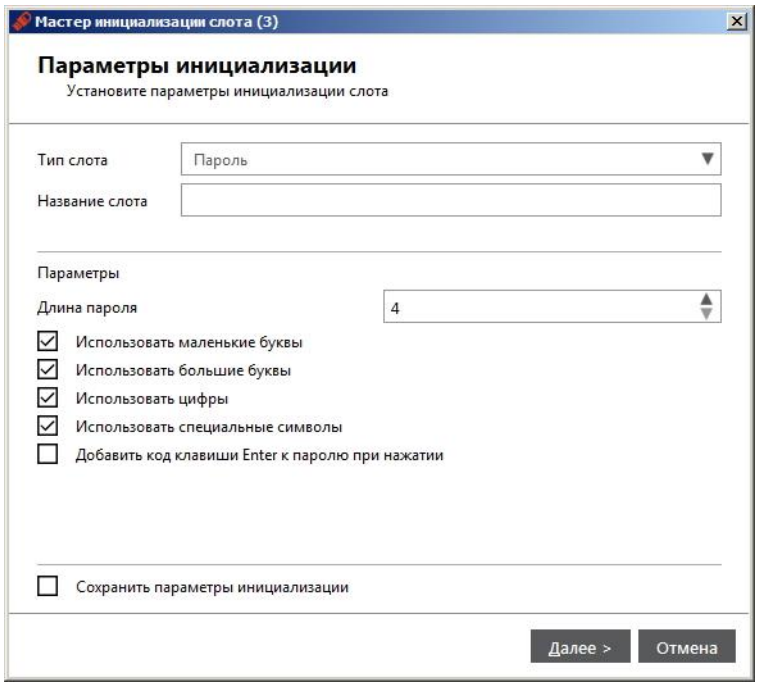


Рисунок 36 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (3)]. Выбор типа слота

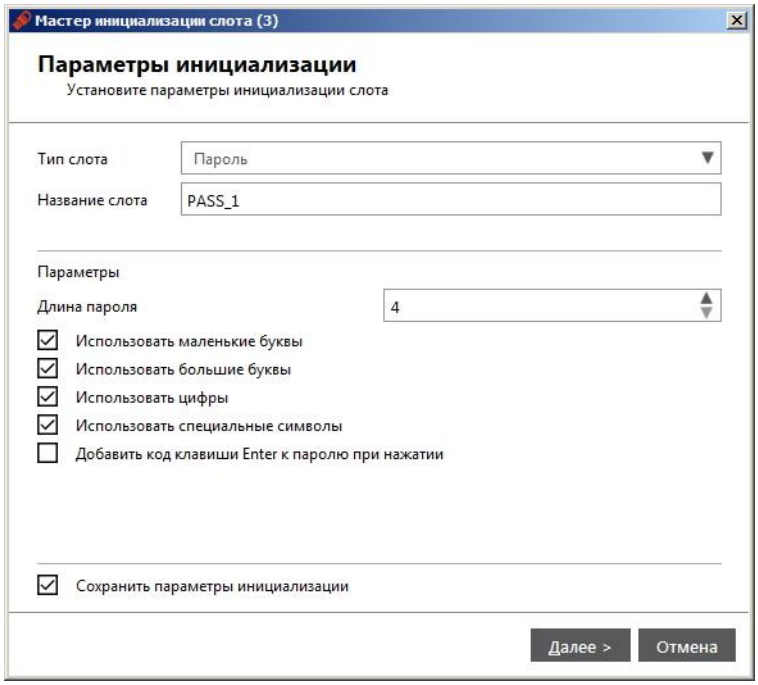


Рисунок 37 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (3)]. Название слота

Настройте параметры качества многоразового пароля:

- установите необходимую длину пароля;
- выберите (если необходимо использовать в пароле) опцию <Использовать маленькие буквы>;
- выберите (если необходимо использовать в пароле) опцию <Использовать большие буквы>;
- выберите (если необходимо использовать в пароле) опцию <Использовать цифры>;

- выберите (если необходимо использовать в пароле) опцию <Использовать специальные символы>;
- выберите (если необходимо) опцию <Добавить код клавиши Enter к паролю при нажатии>.
- Выберите опцию <Сохранить параметры инициализации> (если необходимо сохранить настройки инициализации для последующих инициализаций других слотов);

4. Нажмите <Далее> и в появившемся окне введите PIN-код в одноименном поле (дополнительную информацию см. в разделе 7 PIN-код), после чего нажмите кнопку <Выполнить>.

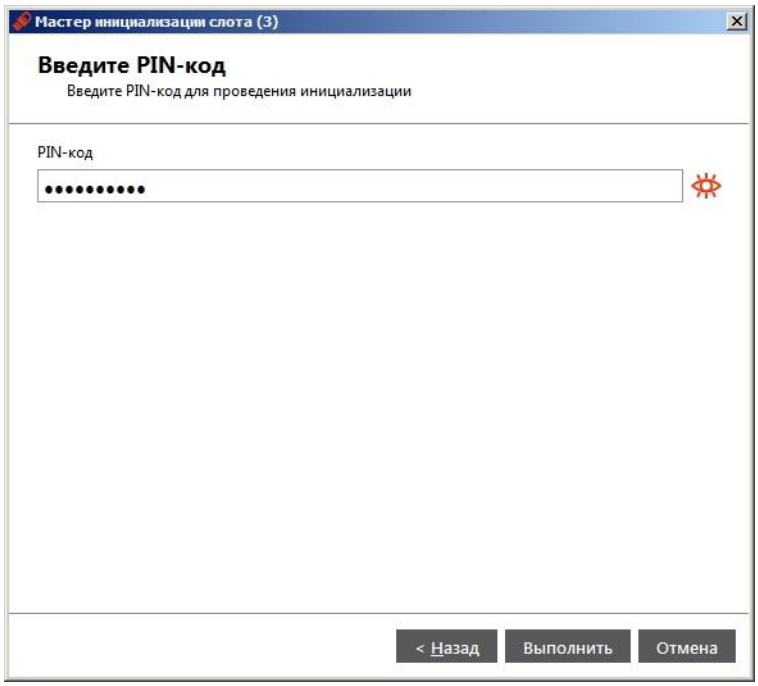


Рисунок 38 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (3)]. Ввод PIN-кода

5. Будет выполняться процесс инициализации слота. По завершении нажмите кнопку <Завершить>.

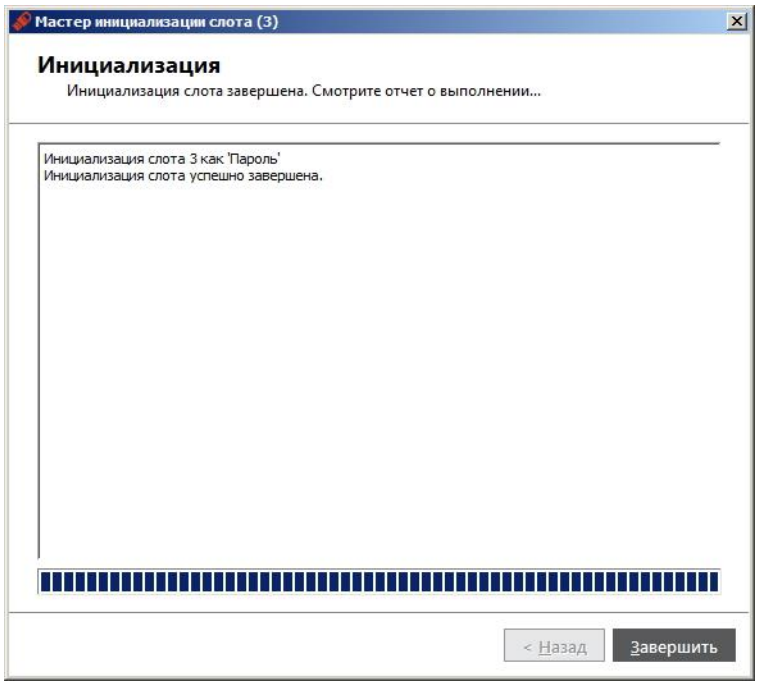


Рисунок 39 - JaCarta WebPass Tool. Окно [Мастер инициализация слота (3)]. Процесс инициализации

5.3.3 Очистка слотов

Для очистки слота выполните следующие действия:

1. На вкладке [OTP] выберите слот, который необходимо очистить;
2. Нажмите кнопку 

;
3. В появившемся окне введите PIN-код (дополнительную информацию см. в разделе 7 PIN-код), затем нажмите кнопку <Очистить>:

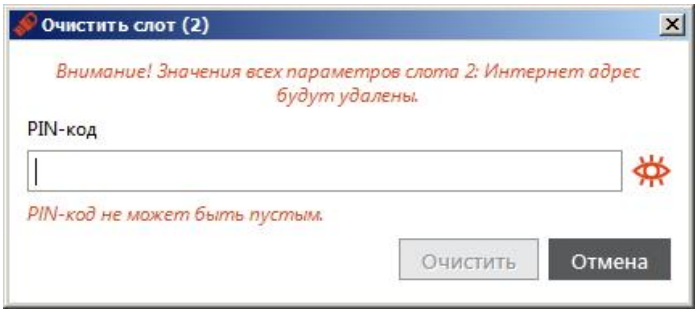


Рисунок 40 – JaCarta WebPass Tool. Окно [Очистить слот]

4. В появившемся окне нажмите <OK> для завершения:

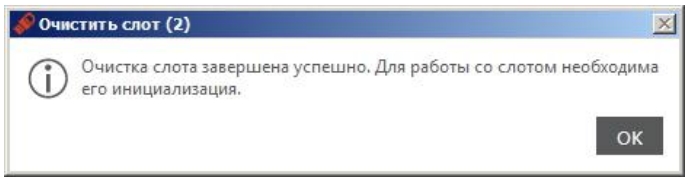


Рисунок 41 - JaCarta WebPass Tool. Информационное сообщение после процесса очистки слота

6. Порядок работы с электронными ключами JaCarta WebPass

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

6.1 Регистрация электронного ключа JaCarta WebPass

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

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

Чтобы зарегистрировать электронный ключ JaCarta WebPass, администратор должен выполнить следующие действия:

1. Подключить USB-токен к компьютеру.
2. Запустить утилиту JaCarta WebPass Tool.
3. Сгенерировать файл с расширением *.xml / *.dat с помощью утилиты JaCarta WebPass Tool.

Генерация файла с расширением *.xml / *.dat с помощью утилиты JaCarta WebPass Tool осуществляется только в процессе инициализации слота типа <Одноразовый пароль> (подробнее см. Инициализация слота).

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

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

6.2 Использование электронного ключа JaCarta WebPass

Электронный ключ JaCarta WebPass может использоваться в любых устройствах, имеющих порты USB Type A Female и поддерживающих работу с USB клавиатурами.

Для хранения информации в электронном ключе JaCarta WebPass используются три независимых слота. Каждый слот имеет свой номер:

- слот №***1***;
- слот №***2***;
- слот №***3***.

Каждый из трех слотов электронного ключа может быть настроен, как один из следующих типов слотов:

- тип слота <Одноразовый пароль>: содержит одноразовый пароль, генерируемый по заданному при инициализации алгоритму;
- тип слота <Пароль>: содержит многоразовый пароль, генерируемый в соответствии с заданными при инициализации критериями качества;
- тип слота <Интернет адрес>: содержит URL-адрес защищённого ресурса.

Различают три способа нажатия кнопки, расположенной на корпусе электронного ключа JaCarta WebPass:

- одинарное нажатие (кратковременное нажатие не более 1 секунды) – используется для получения данных из слота №1;
- двойное нажатие (аналогично двойному щелчку мыши) – используется для получения данных из слота №2;
- длительное нажатие (нажатие и удержание в нажатом состоянии в течение 2-3 секунд) – используется для получения данных из слота №3.

Для того, чтобы пользоваться электронным ключом JaCarta WebPass необходимо знать какой тип слота имеет каждый из трех слотов и какой способ нажатия используется для каждого номера слота. Таким образом, необходимо знать соответствие: №слота – Тип слота – Способ нажатия.

6.2.1 Автоматическая подстановка одноразового пароля

Для подстановки сгенерированного с помощью JaCarta WebPass одноразового пароля в экранную форму выполните следующие действия:

1. Подключите USB-токен к компьютеру.
2. Подождите, пока световой индикатор на USB-токене станет гореть непрерывно.
3. Переместите курсор в поле ввода одноразового пароля.

> *Убедитесь в том, что включена английская раскладка клавиатуры. В противном случае пароль будет введён с использованием символов кириллицы (русского алфавита).*

4. Нажмите кнопку на корпусе электронного ключа JaCarta WebPass способом, соответствующим номеру слота, с типом <Одноразовый пароль>.

6.2.2 Автоматическая подстановка многоразового пароля

Для подстановки сгенерированного с помощью JaCarta WebPass многоразового пароля в экранную форму выполните следующие действия:

1. Подключите USB-токен к компьютеру.
2. Подождите, пока световой индикатор на USB-токене станет гореть непрерывно.
3. Переместите курсор в поле ввода многоразового пароля.

> *Убедитесь в том, что включена английская раскладка клавиатуры. В противном случае пароль будет введён с использованием символов кириллицы (русского алфавита).*

Программное обеспечение для автоматической смены раскладки клавиатуры (например, Punto Switcher) может изменять алфавитные символы подставляемого пароля. Убедитесь в том, что алфавитные символы, содержащиеся в пароле, введены в английской раскладке.

4. Нажмите кнопку на корпусе электронного ключа JaCarta WebPass способом, соответствующим номеру слота, с типом <Пароль>.

6.2.3 Переход на Web-страницу защищённого ресурса

Чтобы открыть страницу защищённого ресурса, URL-адрес которого хранится в памяти электронного ключа JaCarta WebPass, выполните следующие действия:

1. Подключите USB-токен к компьютеру.
2. Подождите, пока световой индикатор на USB-токене станет гореть непрерывно.
3. Нажмите кнопку на корпусе токена JaCarta WebPass способом, соответствующим номеру слота, с типом <Интернет адрес>.

На экране отобразится окно браузера по умолчанию. Если браузер уже был запущен, то появится новое окно или вкладка, в которой будет осуществлён автоматический переход на страницу, URL-адрес которой сохранён в памяти электронного ключа JaCarta WebPass

7. Контакты

7.1 Офис (общие вопросы)

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

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

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

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

7.2 Техподдержка

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

7.3 Предметный указатель

Регистрация изменений

Версия	***Изменения***
1.7	Актуализация форматирования и верстки в соответствии с корпоративным шаблоном
1.6	Изменение шаблона
1.5	Замена скриншотов для ПО Единый Клиент JaCarta версии 2.11.
1.4	Замена скриншотов для ОС Microsoft Windows 7. Исправлены формулировки и неточности.
1.3	Исправлены ошибки в документе. Документ переименован в Руководство пользователя.
1.2	JC-WebPass заменено на JaCarta WebPass. Исправлены опечатки. Внесены смысловые правки в раздел 8.
1.1	Обновлены разделы 1, 3, 4, 6, 7.
1.0	Создание документа.

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