Средство аутентификации и безопасного хранения информации пользователей JaCarta

JaCarta WebPass Tool

Инструкция по использованию

Обозначение документа	RU.АЛДЕ.03.01.019-01 34 03
Статус	Публичный
Листов	42

Оглавление

1. О документе

1.1 Назначение документа

Документ представляет собой руководство по установке, настройке и использованию утилиты JaCarta WebPass Tool, являющейся 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)

Если на компьютере, на котором предполагается работа с утилитой JaCarta WebPass Tool не установлено ПО "Единый Клиент JaCarta", то 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 об утилите JaCarta WebPass Tool" приведена основная информация о JaCarta WebPass Tool.
- в разделе 3 "Установка и удаление утилиты JaCarta WebPass Tool" приведено описание системных требований к компьютеру и описание процедур установки и удаления JaCarta WebPass Tool.
- в разделе 4 "Работа с утилитой JaCarta WebPass Tool" содержится описание основных процедур использования электронных ключей JaCarta WebPass.
- в разделе 5 "Электронные ключи JaCarta WebPass" приведено описание электронных ключей JaCarta WebPass, включая описание внешнего вида, индикации, режимов работы и др.

В конце документа приведен предметный указатель (см. стр. 41).

1.5 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве руководства по установке, настройке и использованию утилиты JaCarta WebPass Tool. Кроме того, документ содержит информацию о порядке работы с электронными ключами JaCarta WebPass, а также описание приложений, установленных на электронных ключах JaCarta WebPass.

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

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

1.7 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, 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 АО "Аладдин Р.Д." без предварительного уведомления.

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

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

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

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

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

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

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

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;

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

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

2. Общие сведения об утилите 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	Последовательность символов, которую необходимо ввести, чтобы администратор мог совершить определенную операцию

3. Установка и удаление утилиты JaCarta WebPass Tool

3.1 Описание пакетов установки

Утилита JaCarta WebPass Tool входит в состав ПО "Единый Клиент JaCarta" (далее – Единый Клиент JaCarta). Утилита не имеет отдельного пакета установки, ее установка выполняется с помощью пакета установки Единого Клиента JaCarta.

Пакеты установки Единого Клиента JaCarta для операционной системы Microsoft Windows имеют следующие представления:

- **JaCartaUnifiedClient_2.13.xxx.xxxx_win-x86_ru-Ru.msi** – пакет установки для 32-разрядных операционных систем;
- **JaCartaUnifiedClient_2.13.xxx.xxxx_win-x64_ru-Ru.msi** – пакет установки для 64-разрядных операционных систем.

3.2 Системные требования

Системные требования к компьютеру, на который устанавливается JaCarta WebPass Tool приведены в таблице 4.

Таблица 4 – Системные требования

Требование	Содержание
Поддерживаемые операционные системы	Microsoft Windows 7 SP1 (32/64-бит): Professional, Enterprise, Ultimate Microsoft Windows 8.1 (32/64-бит): Core, Pro, Enterprise Microsoft Windows 10 (32/64-бит): Home, Professional, Enterprise Microsoft Windows Server 2008 R2 SP1: Standard, Enterprise, Datacenter Microsoft Windows Server 2012: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2012 R2: Foundation, Essentials, Standard, Datacenter Microsoft Windows Server 2016 Microsoft Windows Server 2019
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	Не ниже 1024x768

3.3 Установка утилиты

Если на компьютере уже установлен Единый Клиент JaCarta, то утилита JaCarta WebPass Tool может быть установлена дополнительно из того же пакета установки, из которого был установлен Единый Клиент JaCarta.

Если на компьютере не установлен Единый Клиент JaCarta, то установка утилиты выполняется в процессе установки Единый Клиент JaCarta. Для получения подробной информации об этом обратитесь к разделу 4 "Установка программы" документа "Единый Клиент JaCarta. Руководство администратора".

Для установки утилиты JaCarta WebPass:

1. Запустить стартовое окно мастера установки Единый Клиент JaCarta одним из следующих способов:
   – В меню "Пуск" выбрать "Параметры" → "Приложения и возможности". В открывшемся окне "Приложения и возможности" выбрать в перечне установленных на компьютере приложений Единый Клиент JaCarta и нажать кнопку "Изменить".

   Примечание. *Для реализации этого способа необходимо, чтобы место хранения пакета установки Единый Клиент JaCarta не было изменено с момента его установки.*

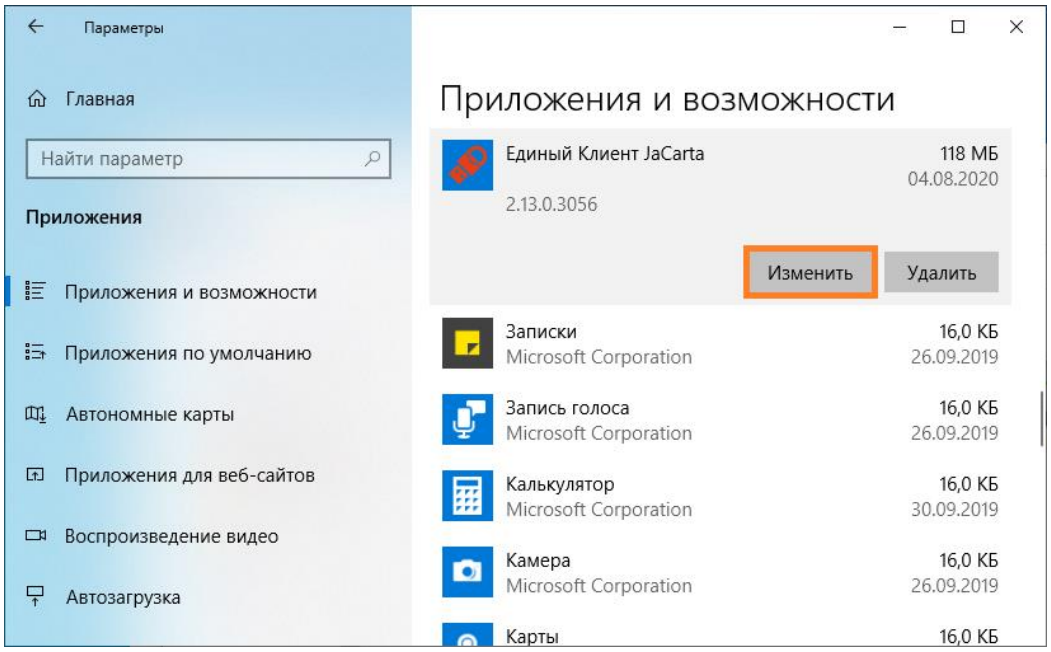


Рисунок 1 – Приложения и возможности. Изменение Единого Клиента JaCarta

   – Запустить файл установки Единый Клиент JaCarta, соответствующий разрядности операционной системе MS Windows (см. п. 3.1 на стр. 9).

2. В открывшемся стартовом окне мастера установки Единый Клиент JaCarta нажать кнопку "Далее".

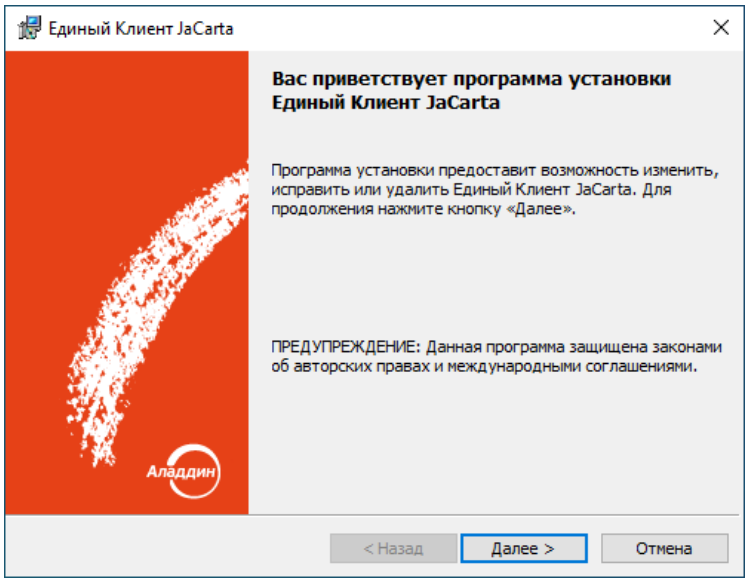


Рисунок 2 – Стартовое окно мастера установки Единый Клиент JaCarta

3. Выбрать в окне "Изменение, исправление или удаление Единый Клиент JaCarta" опцию "Изменить" и нажать кнопку "Далее".

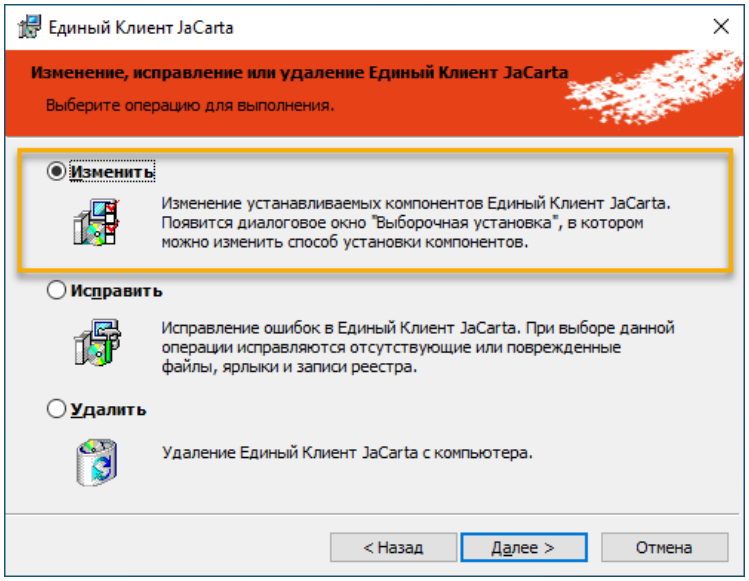


Рисунок 3 – Изменение, исправление или удаление Единый Клиент JaCarta

4. В окне "Выборочная установка" в списке компонентов выбрать "JaCarta WebPass Tool", раскрыть выпадающий список с помощью элемента ▼ и выбрать опцию "Данный компонент и все подкомпоненты будут установлены на локальный жесткий диск". Нажать кнопку "Далее".

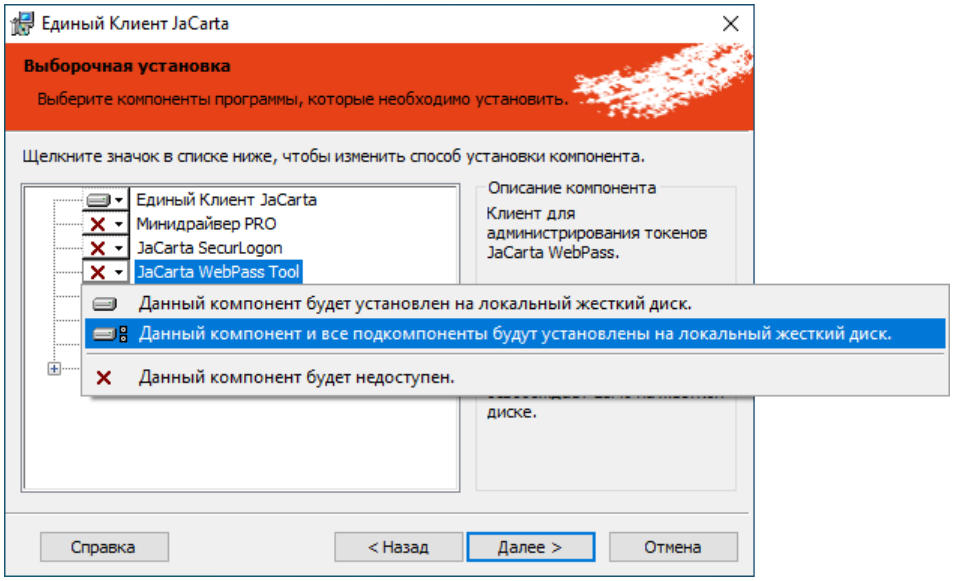


Рисунок 4 – Выбор компонентов программы для установки

5. В окне "Изменение программы" нажать кнопку "Изменить" для подтверждения установки.

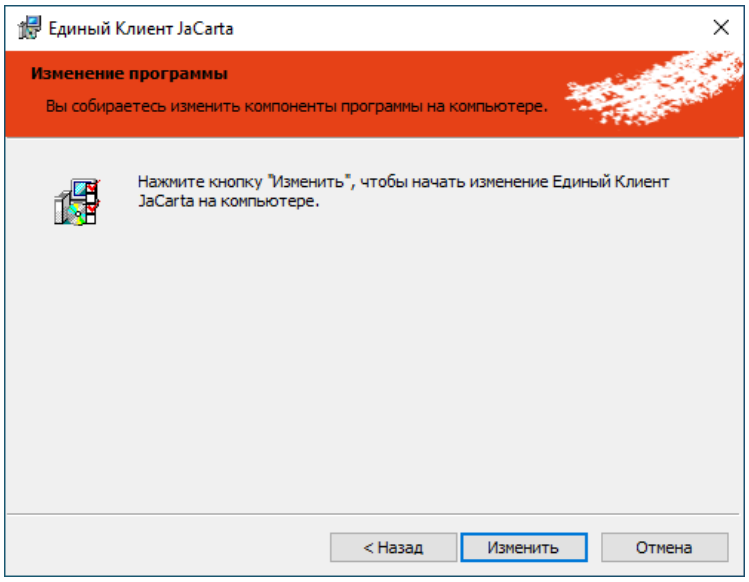


Рисунок 5 – Мастер установки Единый Клиент JaCarta. Окно "Изменение программы"

6. Будет выполняться установка утилиты. По завершении установки будет отображено окно "Программа установки завершена". Нажать кнопку "Готово".

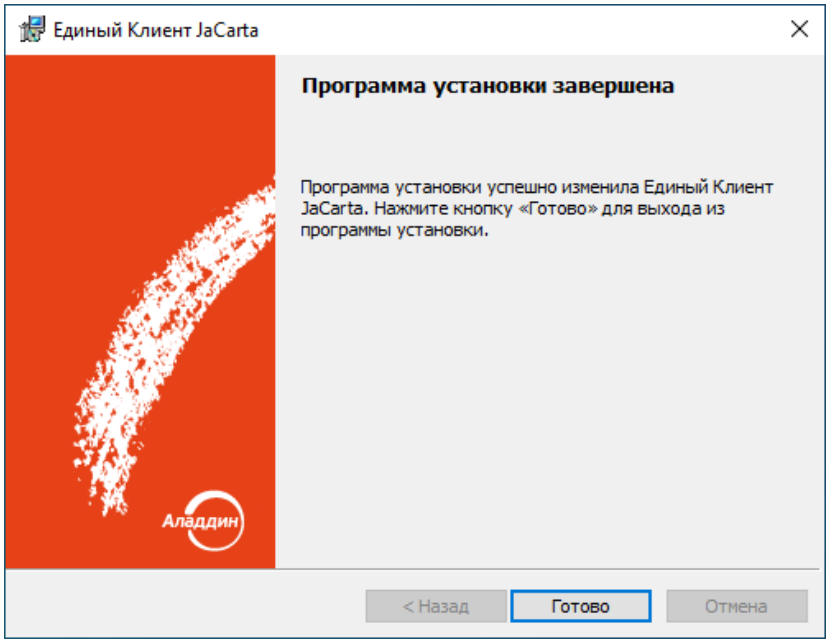


Рисунок 6 – Окно завершения установки Единого Клиента JaCarta

7. После установки утилиты рекомендуется перезагрузить компьютер. Для этого нажать кнопку "Да" в появившемся окне.

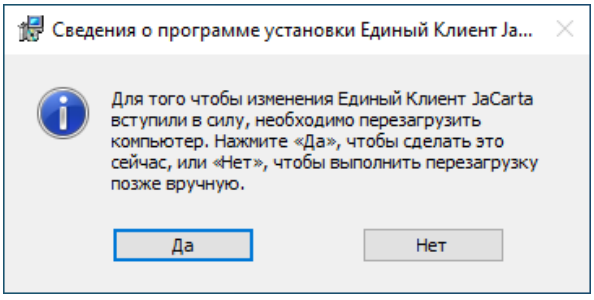


Рисунок 7 – Сообщение о необходимости перезагрузки компьютера

3.4 Удаление утилиты

Для удаления утилиты JaCarta WebPass Tool:

1. Выполните шаги 1-3 процедуры установки утилиты JaCarta WebPass Tool (см. п. 3.3 на стр. 9).
2. Выбрать в перечне установленных компонентов JaCarta WebPass Tool, раскрыть выпадающий список с помощью элемента ▼ и в появившемся меню выбрать пункт "Данный компонент будет недоступен". Нажать кнопку "Далее".

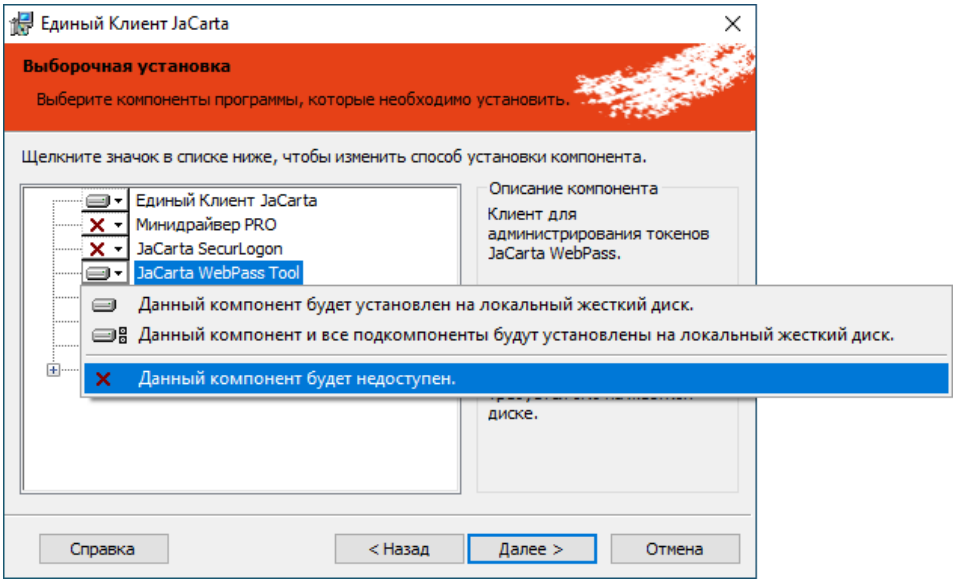


Рисунок 8 – Окно "Выборочная установка" мастера установки Единый Клиент JaCarta

3. В окне "Изменение программы" нажать кнопку "Изменить" для того, чтобы подтвердить удаление компонента.

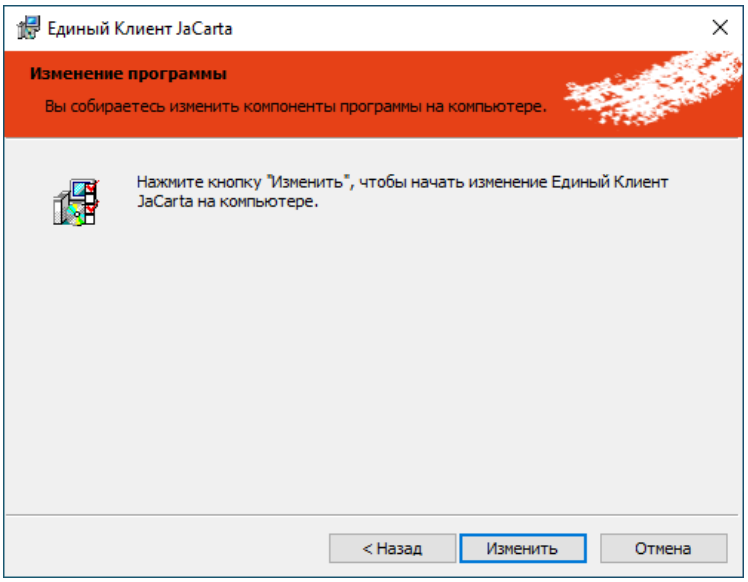


Рисунок 9 – Окно "Изменение программы" мастера установки Единый Клиент JaCarta

4. Будет выполняться удаление компонента. Процесс удаления будет отображаться в окне "Изменение Единый Клиент JaCarta" в поле "Состояние" в виде индикатора.

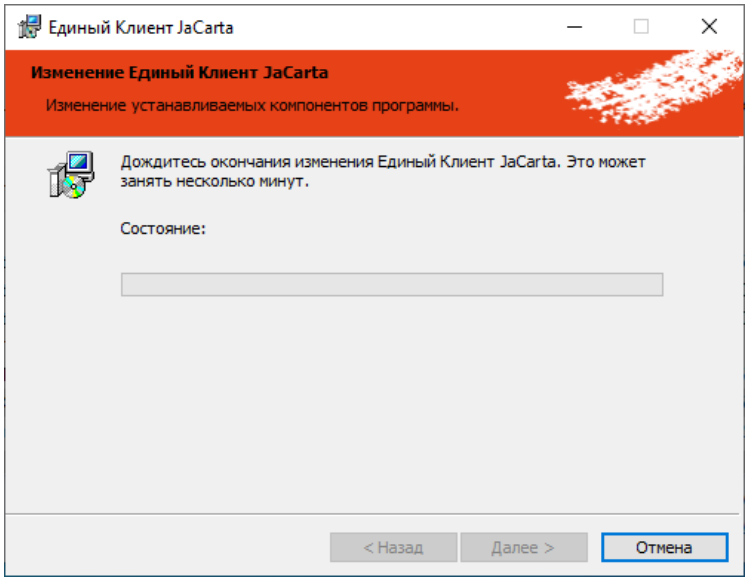


Рисунок 10 – Окно "Дополнительные параметры работы" мастера установки Единый Клиент JaCarta

5. После завершения удаления компоненета JaCarta WebPass Tool будет отображено заключительное окно мастера устновки Единый Клиент JaCarta. Нажать кнопку "Готово".

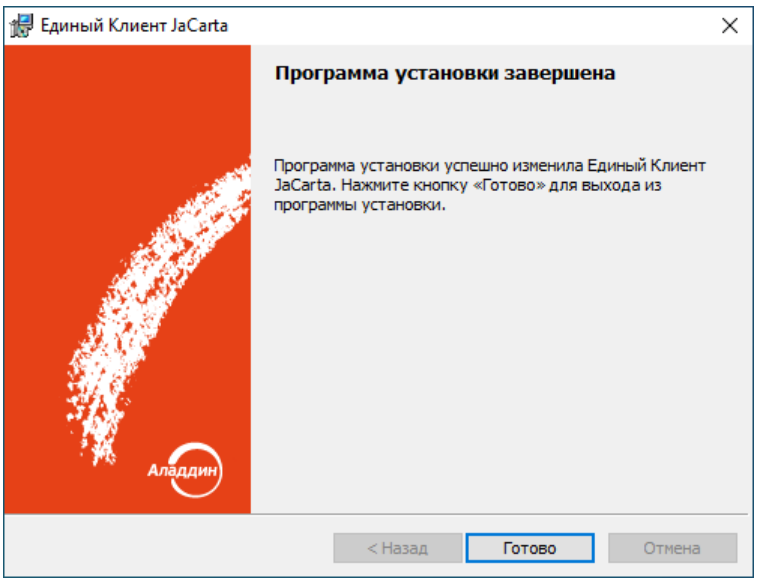


Рисунок 11 – Успешное удаление компонента с помощью мастера установки Единый Клиент JaCarta

6. После удаления утилиты рекомендуется перезагрузить компьютер. Для этого нажать кнопку "Да" в появившемся окне.

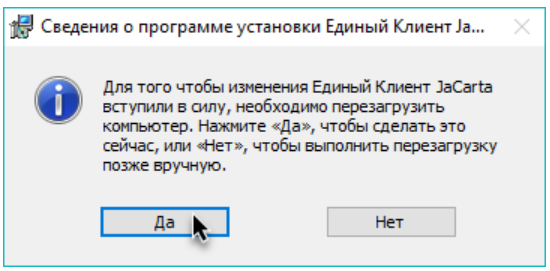


Рисунок 12 – Сообщение о необходимости перезагрузки компьютера

4. Работа с утилитой JaCarta WebPass Tool

4.1 Запуск утилиты

Для запуска утилиты JaCarta WebPass Tool:

1. В меню "Пуск" раскрыть папку "Аладдин Р.Д." и выбрать в ней "JaCarta WebPass Tool".

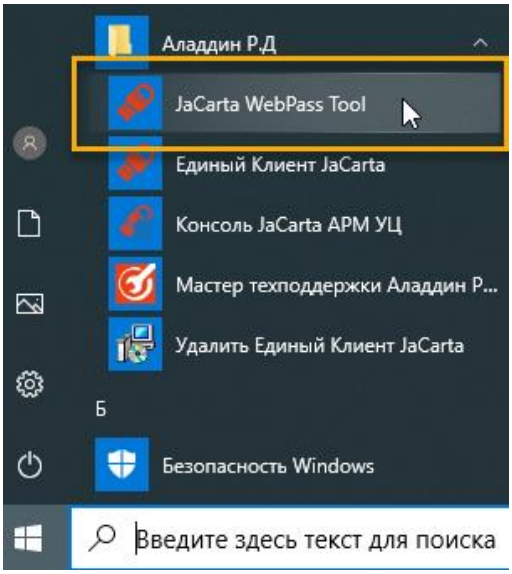


Рисунок 13 – Запуск утилиты JaCarta WebPass Tool

2. Будет выполнен запуск утилиты и отображено основное окно.

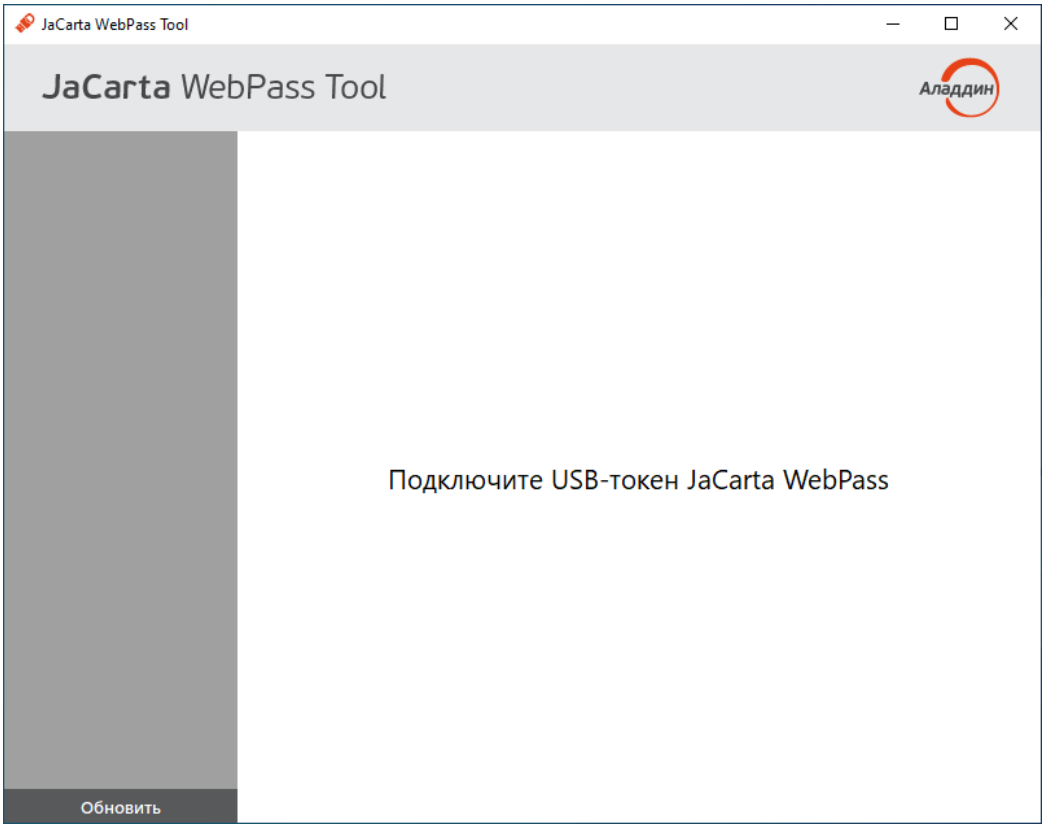


Рисунок 14 – Вид основного окна утилиты JaCarta WebPass Tool (ни один электронный ключ не подключен)

4.2 Просмотр сведений об утилите

Для просмотра сведений об утилите JaCarta WebPass Tool:

1. В основном окне утилиты нажмите логотип компании "Аладдин Р.Д." в верхнем правом углу окна. Будет отображено окно со сведениями об утилите.

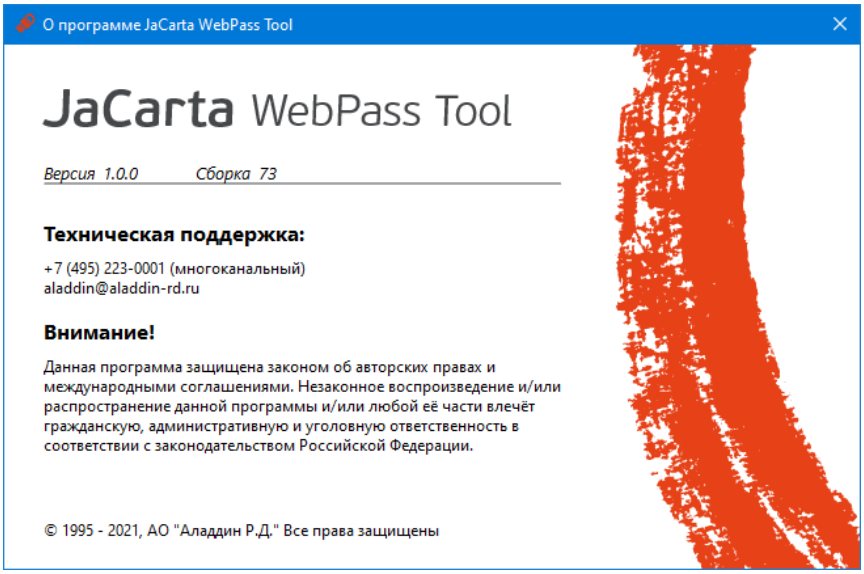


Рисунок 15 – Окно "О программе"

4.3 Обзор пользовательского интерфейса утилиты

Для начала работы с утилитой подключите электронный ключ JaCarta WebPass или JaCarta U2F/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. Будет отображено основное окно утилиты:

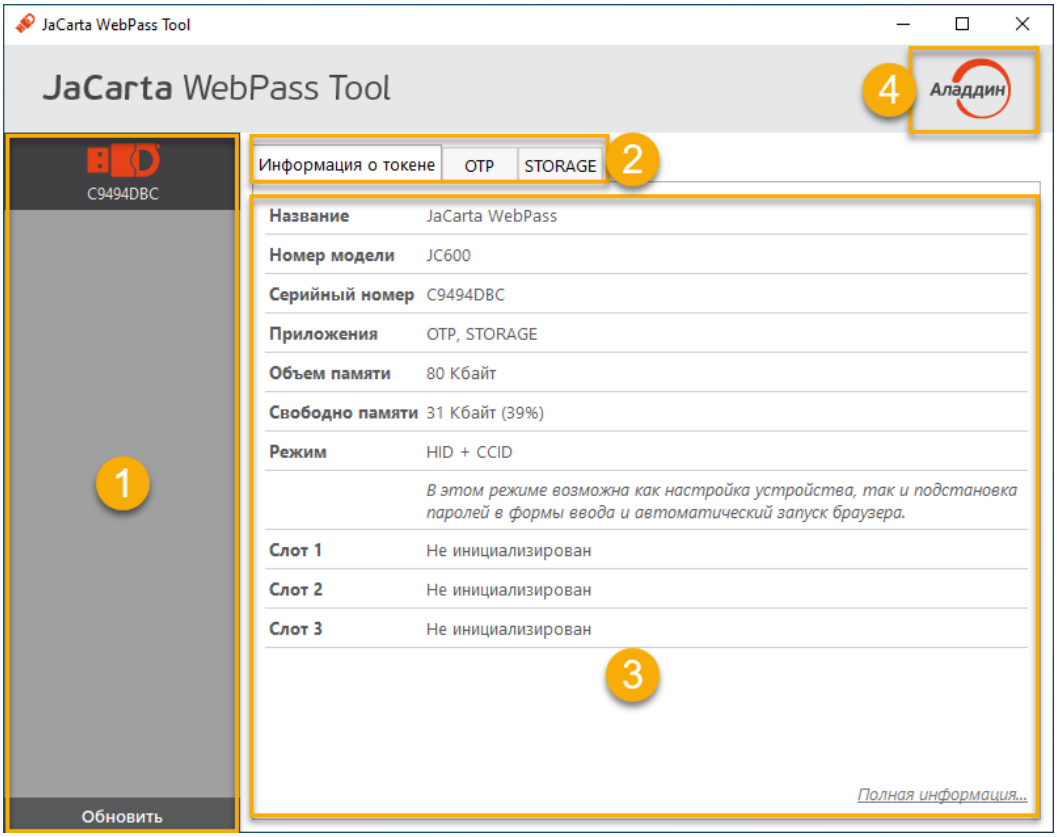


Рисунок 16 – Основное окно утилиты после установления драйверов

Основное окно утилиты содержит следующие области:

1	Область для отображения подсоединённых к компьютеру электронных ключей. Содержит кнопку "Обновить" для повторного поиска и опроса поддерживаемых электронных ключей (обновления списка подключенных устройств)
2	Вкладки для работы с электронным ключом. *Вкладки отображаются только при наличии подсоединенного к USB-порту электронного ключа.* Вкладка **Информация о токене** предназначена для просмотра информации о подсоединенном электронном ключе (модель ключа, установленные приложения, объем памяти, информация об инициализации слотов, количество выполненных нажатий на кнопку электронного ключа, количество подключений электронного ключа к USB-порту и др.). Вкладка является активной по умолчанию. Вкладка **OTP** предоставляет доступ к операциям смены PIN-кода электронного ключа, операциям управления слотами электронного ключа – записи в них одноразового или многоразового пароля либо URL-адреса защищенного ресурса, а также очистки слотов. Вкладка **STORAGE** предоставляет возможность для перехода в Единый Клиент JaCarta для выполнения операций с ключами и сертификатами, хранящимися в памяти электронного ключа
3	Область для отображения содержимого выбранной вкладки
4	Кнопка для вызова окна со сведениями об утилите

4.4 Просмотр информации о подсоединенном электронном ключе

Для просмотра информации о подсоединенном электронном ключе:

1. Подключите электронный ключ JaCarta WebPass или JaCarta U2F/WebPass к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В области слева будет отображен значок электронного ключа и его серийный номер. Информация об электронном ключе будет отображена во вкладке "Информация о токене":

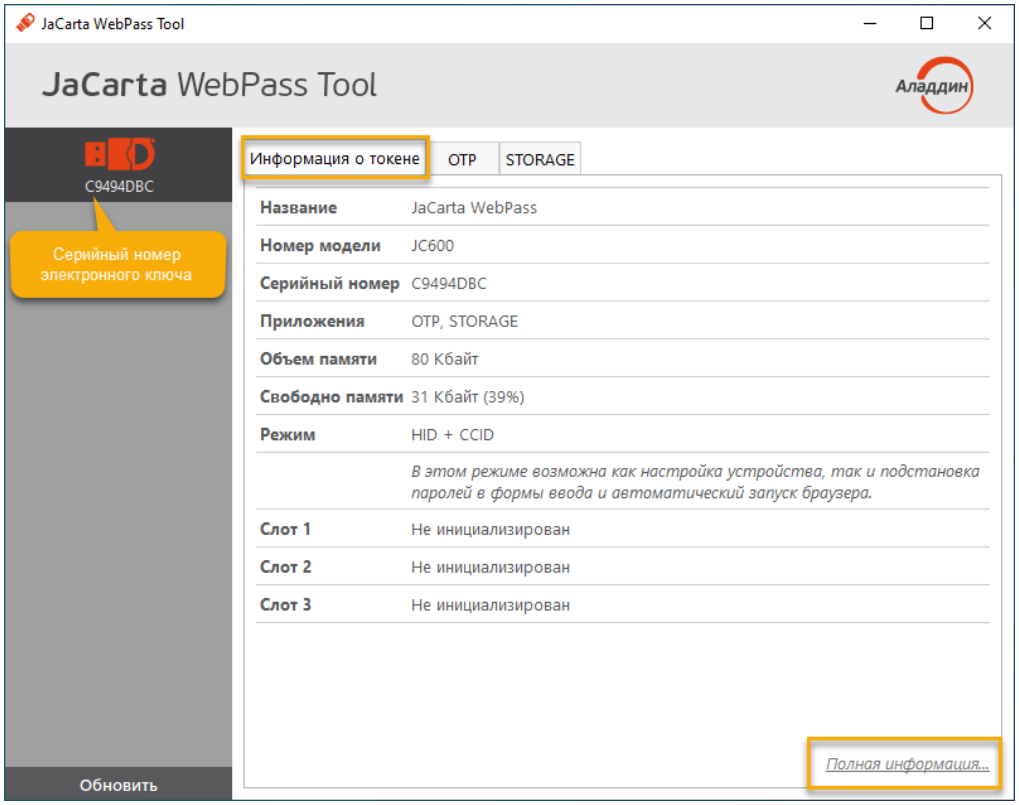


Рисунок 17 – Вкладка "Информация о токене" с подключенным электронным ключом JaCarta WebPass

Описание отображаемых полей на вкладке "Информация о токене" приведено в таблице 5.

Таблица 5 – Вкладка "Информация о токене". Описание параметров

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

2. Нажмите кнопку "*Полная информация...*" для вызова окна с подробными сведениями о выбранном электронном ключе.

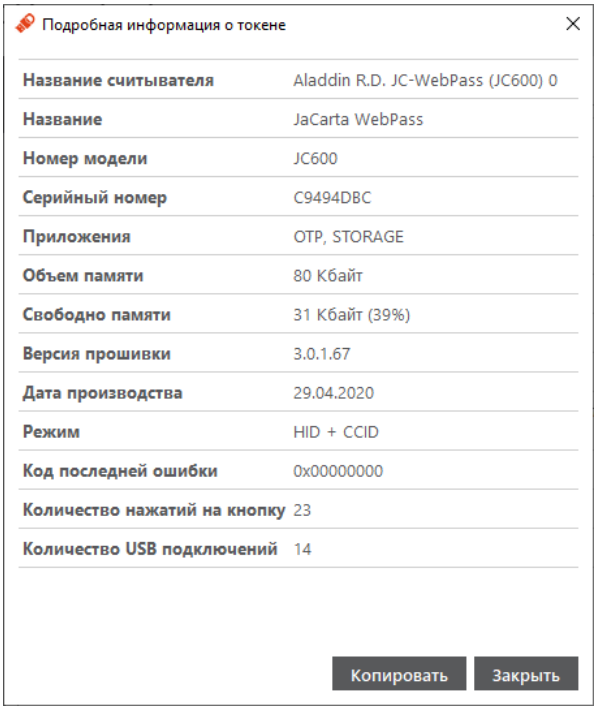


Рисунок 18 – Подробная информация о токене

Описание подробной информации об электронном ключе приведено в таблице 6.

Таблица 6 – Подробная информация о токене. Описание параметров

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

3. Нажмите кнопку "Закрыть" для закрытия окна "Подробная информация о токене".

4.5 Смена PIN-кода электронного ключа

Смена PIN-кода электронного ключа может быть выполнена в любой момент работы с электронным ключом. Количество изменений PIN-кода электронного ключа не ограничено.

Кроме того, необходимо изменить PIN-код электронного ключа, заданный по умолчанию перед началом использования электронного ключа.

Подробнее о PIN-коде электронного ключа см. п. 5.1.3 на стр. 38.

Для смены PIN-кода электронного ключа:

1. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне утилиты перейдите к вкладке "OTP" и нажмите кнопку "Сменить PIN-код". Будет отображено одноименное окно.

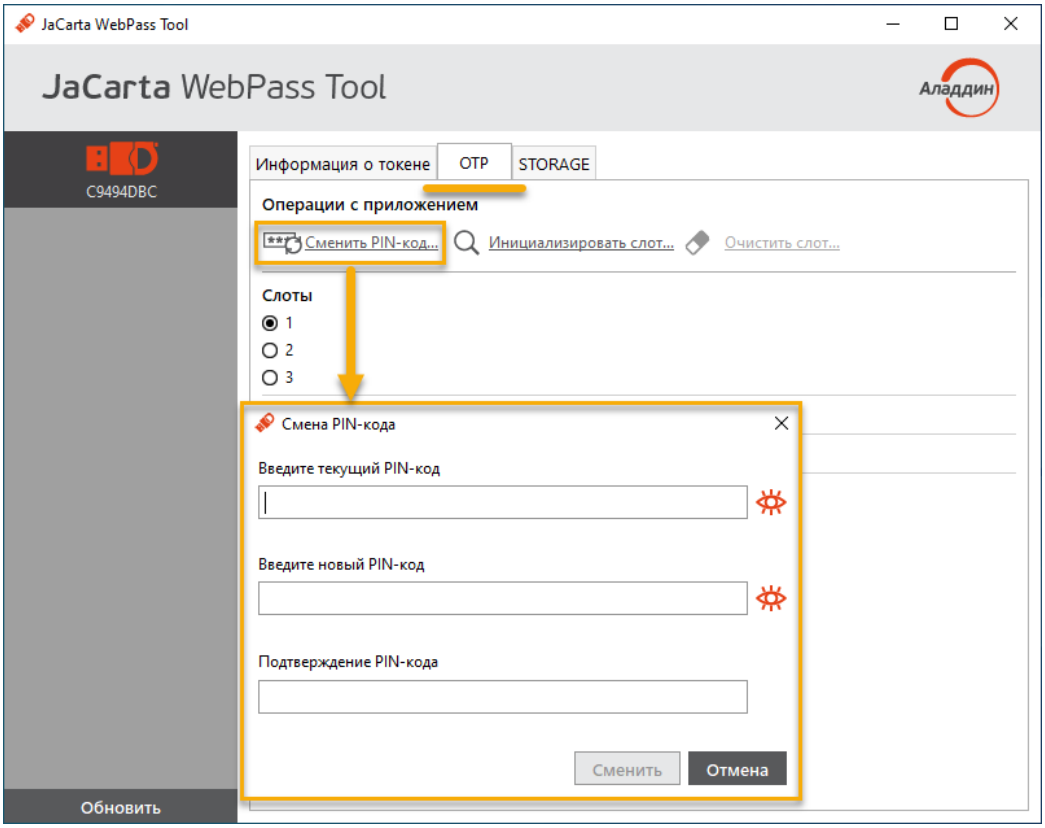


Рисунок 19 – Вызов окна "Смена PIN-кода"

2. В окне "Сменить PIN-код" введите текущий PIN-код, после чего введите новый PIN-код и подтвердите его еще раз, затем нажмите кнопку "Сменить". PIN-код электронного ключа будет изменен. На экране будет отображено окно с информацией об этом.

Рисунок 20 – Сообщение об успешной смене PIN-кода

3. Нажмите кнопку "ОК" для закрытия окна сообщения.

4.6 Просмотр информации о слотах

Для просмотра информации о слоте:

1. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне перейдите к вкладе "OTP" и выберите нужный слот. В нижней части окна будет отображена информация о параметрах инициализации и способе использования слота.

   На рисунке 21 приведен вид вкладки "OTP" по умолчанию (т.е. ни один из слотов не инициализирован) с выбранным слотом 1.

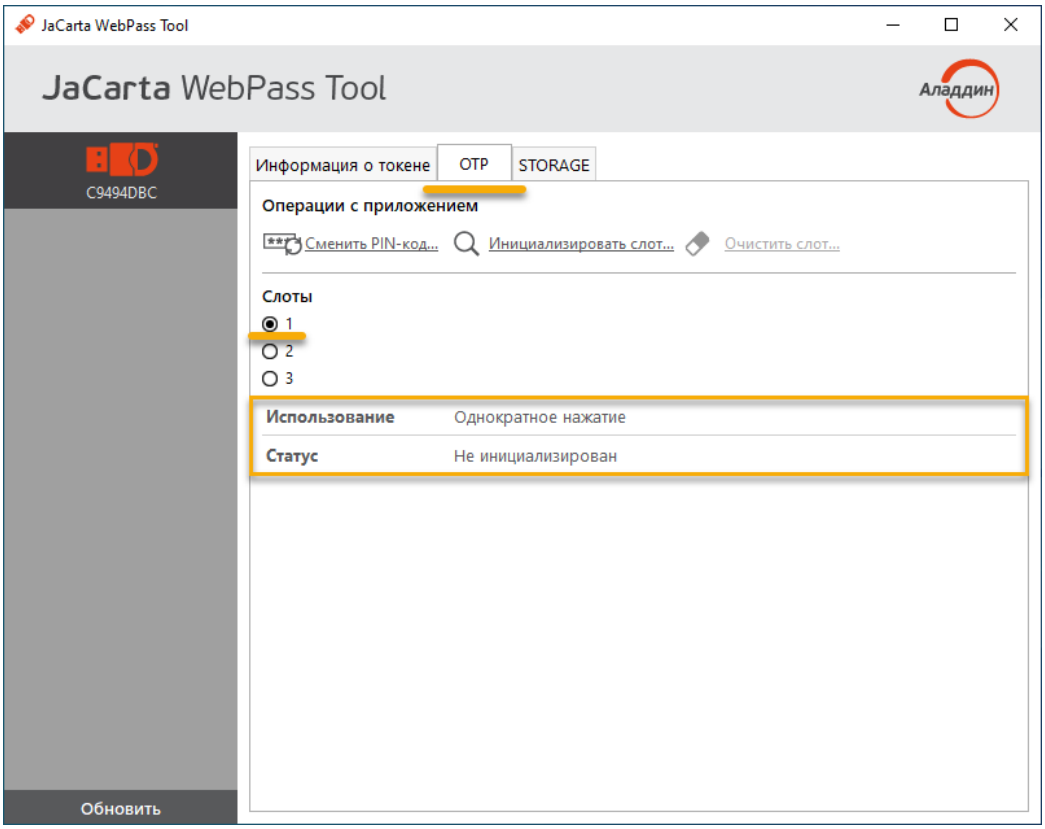


Рисунок 21 – Вкладка "OTP", просмотр информации о слоте 1 (ни один из слотов не инициализирован)

На рисунке 22 приведен вид вкладки "OTP" с инициализированными слотами 1, 2, 3 с выбранным слотом 3.

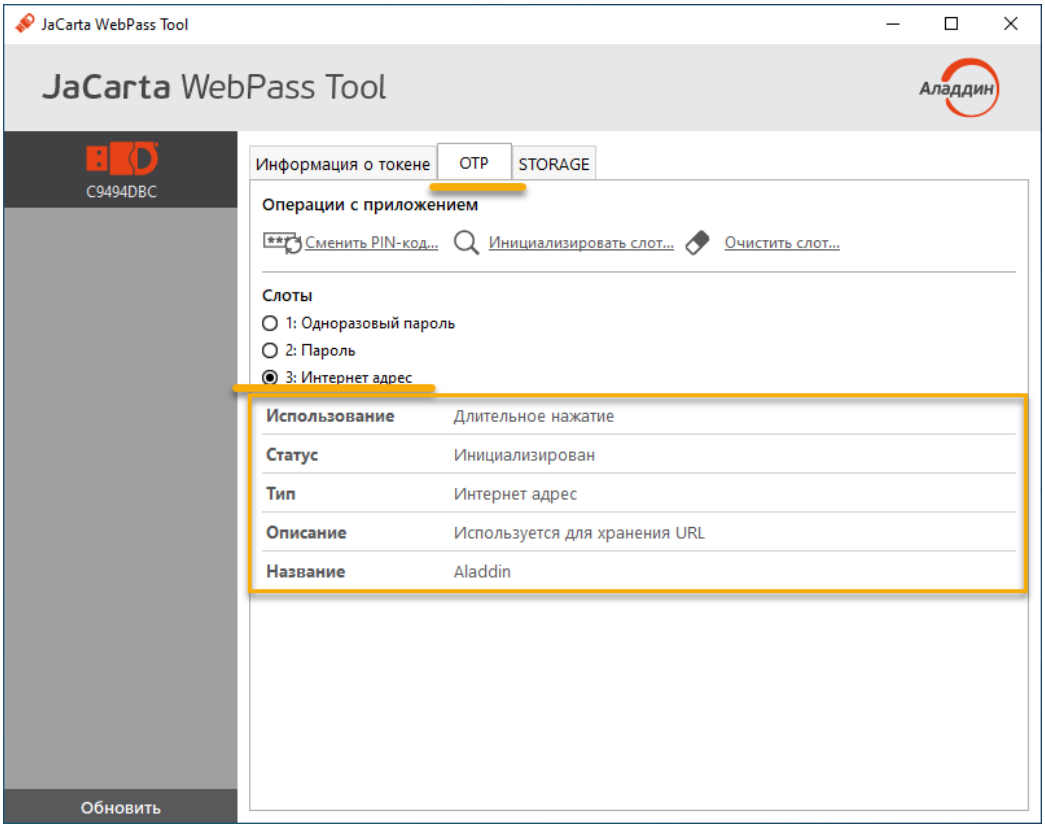
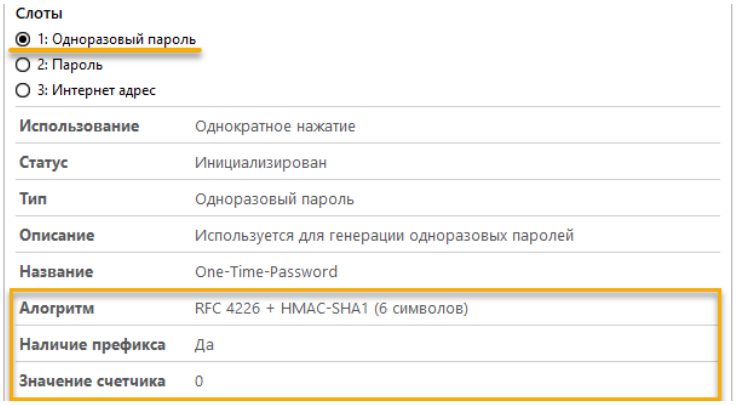
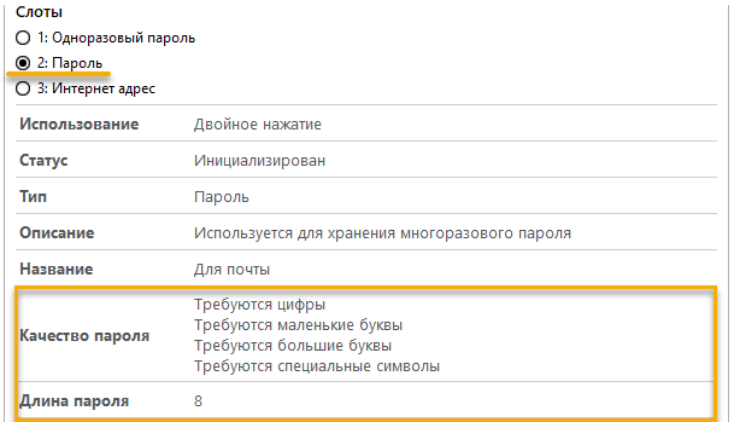


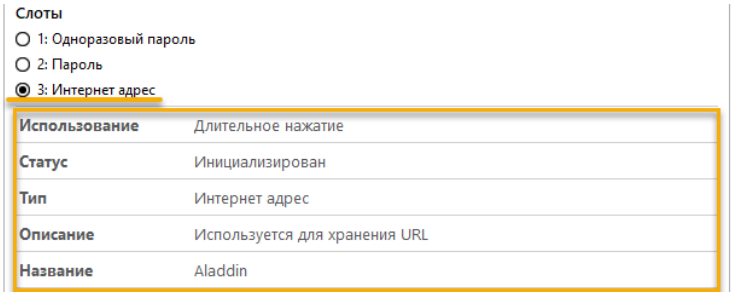
Рисунок 22 – Вкладка "OTP", просмотр информации о слоте 3 (все слоты инициализированы)

В таблице ниже приведено описание полей, в которых отображается информация о слотах.

Таблица 7 – Параметры слота

Элемент интерфейса	**Описание**
Поле "Использование"	Способ нажатия на кнопку, расположенную на корпусе 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"	Содержит значение, соответствующее текущему статусу слота: "Не инициализирован", "Инициализирован", "Заблокирован"
Поля "Тип"	Содержит тип слота, заданный при его инициализации: "Одноразовый пароль" – если в слоте хранится механизм для генерации одноразовых паролей; "Пароль" – если в слоте хранится автоматически сгенерированный многоразовый пароль; "Интернет адрес" – если в слоте хранится URL-адрес для доступа к Web-ресурсу.
Поле "Описание"	Содержит описание типа слота (значение поля формируется автоматически)
Поле "Название"	Содержит имя слота, заданное пользователем при инициализации слота

Элемент интерфейса	Описание
Поля для слота с типом "Одноразовый пароль"	 Поле "Алгоритм" – содержит информацию об алгоритме генерации одноразовых паролей, выбранном при инициализации слота. Поддерживается четыре алгоритма генерации одноразовых паролей (event-based алгоритмы согласно RFC 4226). Поле "Наличие префикса" – содержит признак наличия префикса, подставляемого перед одноразовым паролем. Поле "Значение счетчика" – содержит текущее значение счетчика сгенерированных одноразовых паролей, принимает значение от 0 до 2^{31}
Поля для слота с типом "Пароль"	 Поле "Качество пароля" – содержит параметры качества пароля, заданные 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). Поле "Длина пароля" – содержит значение длины пароля, заданное при инициализации слота

Элемент интерфейса	Описание
Поля для слота с типом "Интернет адрес"	 Поле "Название" – содержит название, указанное пользователем при инициализации слота

4.7 Управление слотами электронного ключа

Утилита JaCarta WebPass Tool позволяет записывать в слот электронного ключа данные для хранения и дальнейшего использования. Эта операция называется ***инициализацией слота***. Инициализация слота выполняется с предъявлением PIN-кода электронного ключа.

Любой слот электронного ключа может быть проинициализирован неограниченное количество раз.

> *Перед первой инициализацией слота необходимо изменить PIN-код электронного ключа по умолчанию.*

Для инициализированного слота электронного ключа доступны операции очистки слота (см. п. 4.7.3 на стр. 32) и повторной инициализации слота. При повторной инициализации данные, записанные в ходе предыдущей инициализации удаляются и заменяются новыми данными.

При инициализации в слот могут быть записаны данные одного из следующих типов:

- одноразовый пароль, который генерируется по выбранному алгоритму (см. п. 4.7.1 на стр. 24);
- многоразовый пароль, соответствующий указанным критериям качества (см. п. 4.7.2 на стр. 29);
- URL-адрес защищенного ресурса (см. п. 4.7.3 на стр. 32).

4.7.1 Инициализация слота типом "Одноразовый пароль"

В ходе выполнения инициализации слота типом "Одноразовый пароль" в слот записывается механизм для генерации одноразовых паролей за указанному алгоритму.

Для инициализации слота типом "Одноразовый пароль":

2. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне перейдите к вкладе "OTP", установите отметку возле того слота, в который необходимо записать одноразовый пароль и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 23 отметка установлена возле пустого слота 1, однако одноразовый пароль может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

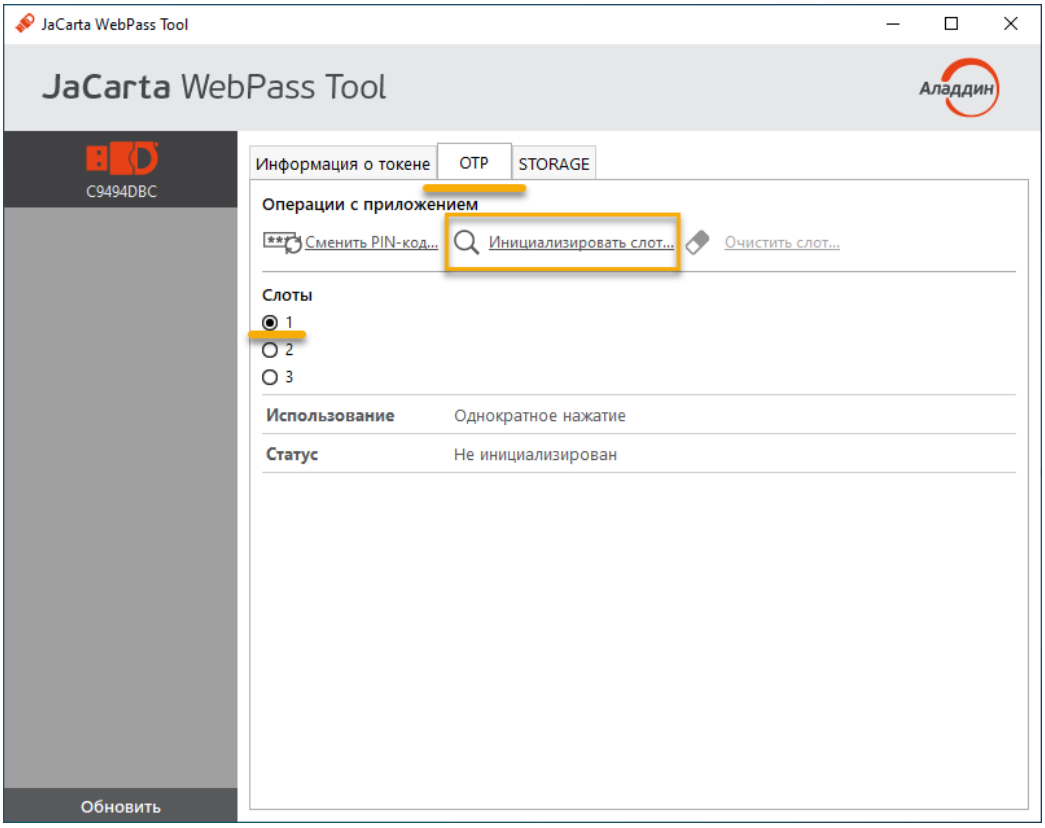


Рисунок 23 – Вкладка "OTP", выбора слота 1 для инициализации"

3. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота <№ слота>". Заполните поля мастера следующим образом (см. рисунок 24):
   - в поле "Тип слота" выберите в раскрывающемся списке значение "Одноразовый пароль";
   - в поле "Название слота" введите название слота. Длина поля не должна превышать 32 символа;
   - в поле "Алгоритм" из раскрывающегося 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;
   - в поле "Префикс" при необходимости укажите префикс – дополнительное постоянное значение, которое будет автоматически подставляться перед значением одноразового пароля. Таким образом, итоговое значение подставляемого пароля будет содержать больше символов, чем значение собственно одноразового пароля. Для ввода префикса:
     - введите нужное значение с клавиатуры (не более 32-х символов);
     - нажмите кнопку S/N для автоматической вставки серийного номера электронного ключа в качестве префикса;
   - выберите опцию "Автоматическая генерация вектора инициализации" или введите последовательность из 20 символов в поле "Вектор инициализации";
   - в поле "Значение счетчика" введите значение счетчика генераций;

– выберите опцию "Сохранить параметры инициализации", для сохранения введенных настроек инициализации для последующих инициализаций других слотов.

Нажмите кнопку "Далее".

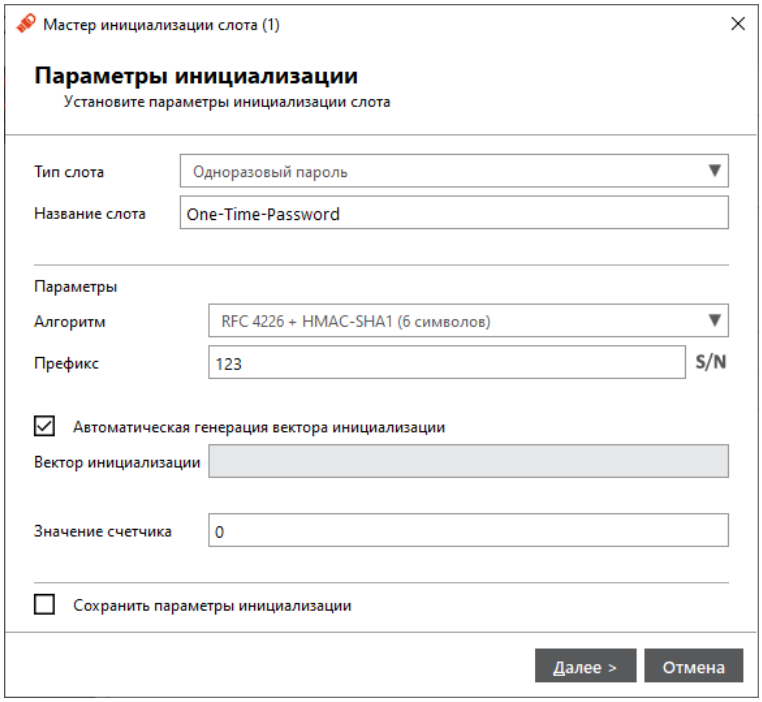


Рисунок 24 - Инициализация слота типом "Одноразовый пароль"

4. В появившемся окне "Сохранение файла конфигурации" (см. рисунок 25) при необходимости укажите формат и имя файла, в который будут сохранены результаты инициализации слота:

Примечание. *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.*

– в поле "Выбрать формат файла" выберите в раскрывающемся списке формат конфигурационного файла из предлагаемых значений: SAM/JMS/JAS;

– в поле "Имя файла" укажите путь для сохранения конфигурационного файла. Для этого нажмите кнопку "Обзор" и выберите место сохранения конфигурационного файла. Если файл не существует и его требуется создать, то введите его имя и нажмите "Сохранить".

Если конфигурационный файл создавать и сохранять не требуется, то установите отметку "Пропустить эту страницу". Нажмите кнопку "Далее".

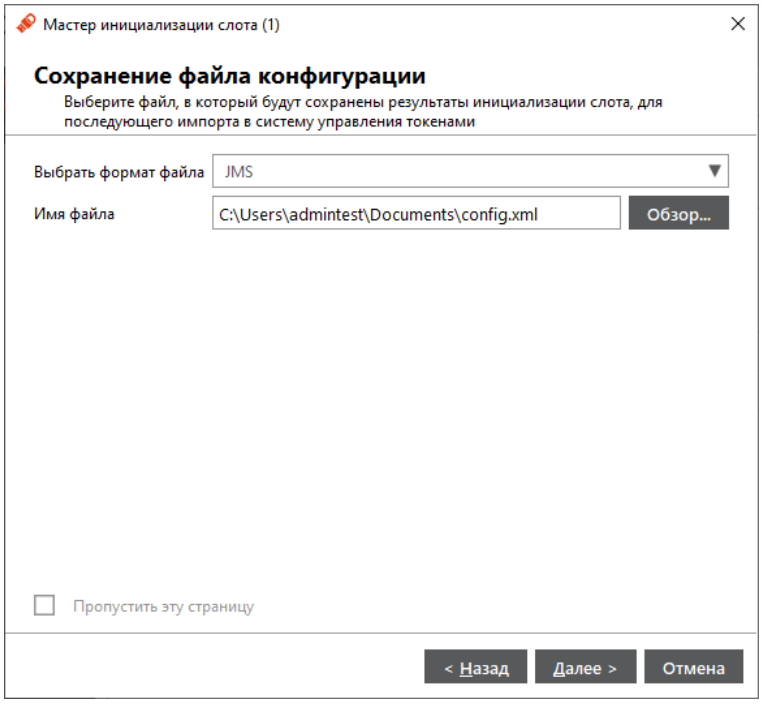


Рисунок 25 - Инициализация слота типом "Одноразовый пароль". Сохранение файла конфигурации

5. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

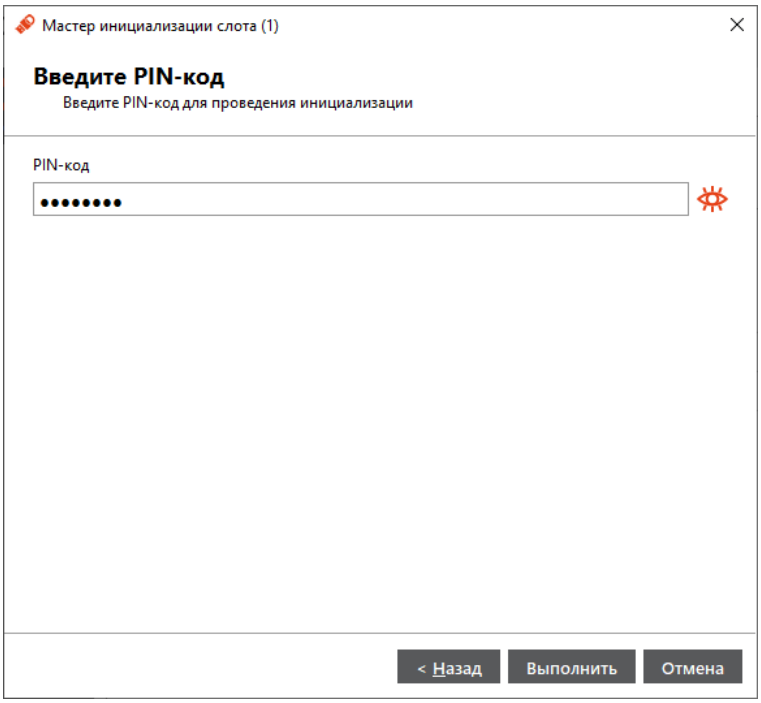


Рисунок 26 – Инициализация слота типом "Одноразовый пароль". Ввод PIN-кода

6. Для перехода в папку с сохраненным конфигурационным файлом установите отметку "Выбрать файлы при помощи программы Проводник". В этом случае, после нажатия кнопки "Завершить" будет открыта папка с сохраненным конфигурационным файлом. Нажмите кнопку "Завершить".

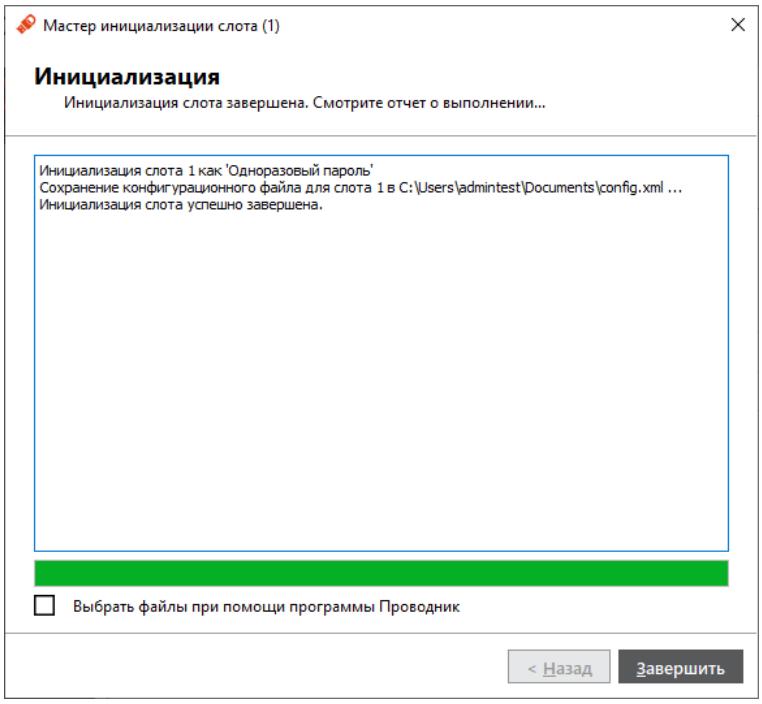


Рисунок 27 – Завершение инициализации слота типом "Одноразовый пароль"

7. Окно мастера инициализиции будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Одноразовый пароль".

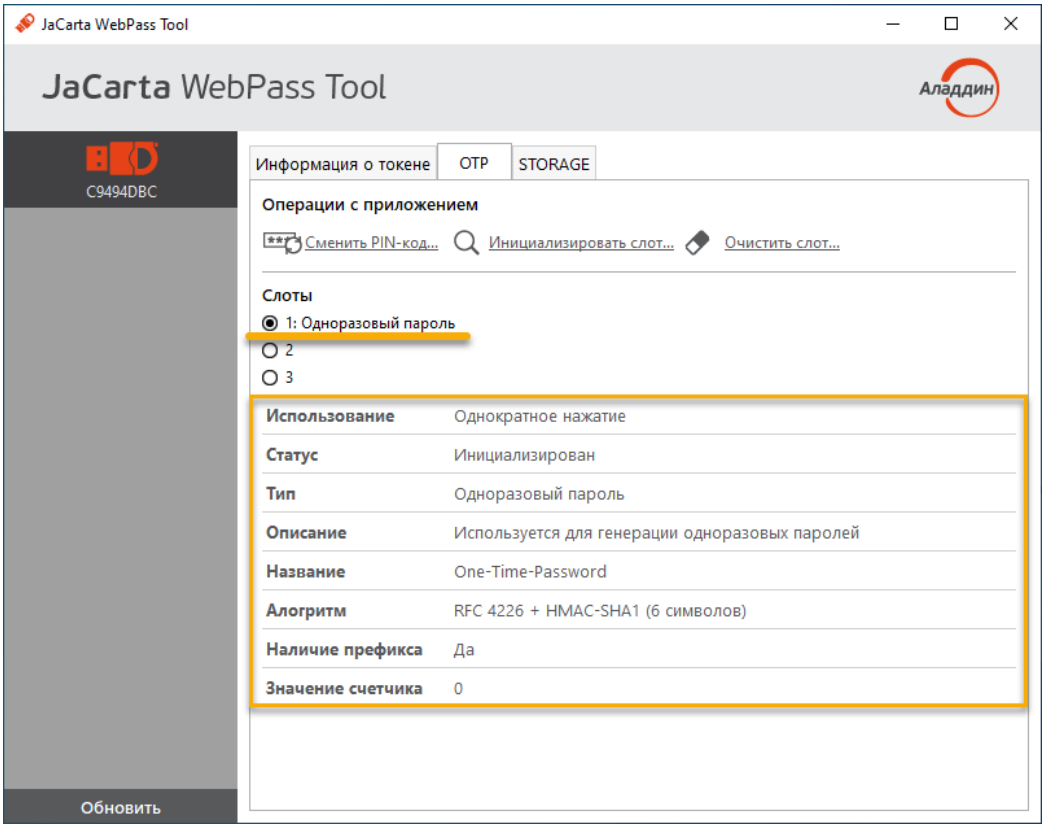


Рисунок 28 – Слот 1 инициализирован типом "Одноразовый пароль"

4.7.2 Инициализация слота типом "Пароль"

В ходе выполнения инициализации слота типом "Пароль" происходит генерация и сохранение в слот многоразового пароля с указанными параметрами качества.

Для инициализации слота типом "Пароль":

1. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне перейдите к вкладе "OTP", установите отметку возле того слота, в который необходимо записать многоразовый пароль и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 29 отметка установлена возле пустого слота 2, однако многоразовый пароль может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

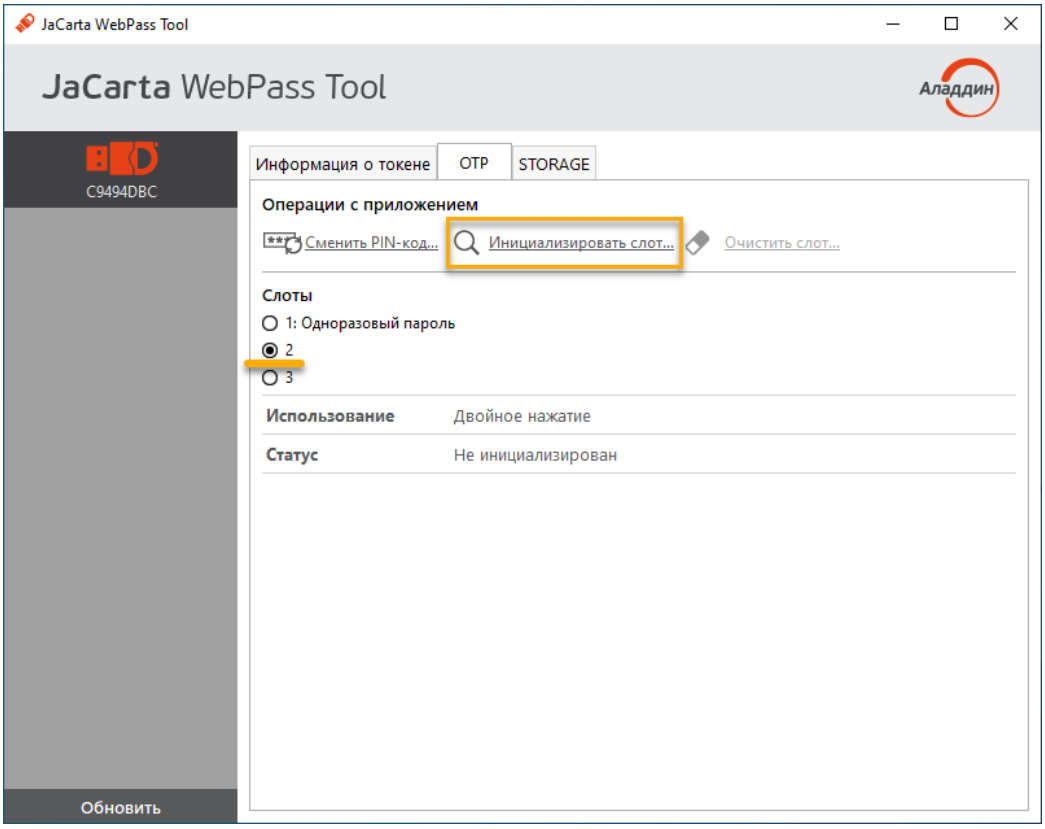


Рисунок 29 – Вкладка "OTP", выбора слота 2 для инициализации"

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота <№ слота>". Заполните поля мастера следующим образом (см. рисунок 30):
   - в поле "Тип слота" выберите значение "Пароль";
   - В поле "Название слота" введите название, например, "Для почты". Длина поля не должна превышать 32 символа;
   - укажите параметры качества, которым должен соответствовать многоразовый пароль:
     - в поле "Длина пароля" установите необходимую длину пароля (по умолчанию длина пароля составляет 4 символа);
     - выберите опцию "Использовать маленькие буквы", если в состав пароля должны входить маленькие буквы;
     - выберите опцию "Использовать большие буквы" если в состав пароля должны входить большие буквы;
     - выберите опцию "Использовать цифры" если в состав пароля должны входить цифры;
     - выберите опцию "Использовать специальные символы", если в состав пароля должны входить специальные символы;
     - выберите опцию "Добавить код клавиши Enter к паролю при нажатии" при необходимости
   - выберите опцию "Сохранить параметры инициализации", если необходимо сохранить настройки инициализации для последующих инициализаций других слотов;

Нажмите кнопку "Далее".

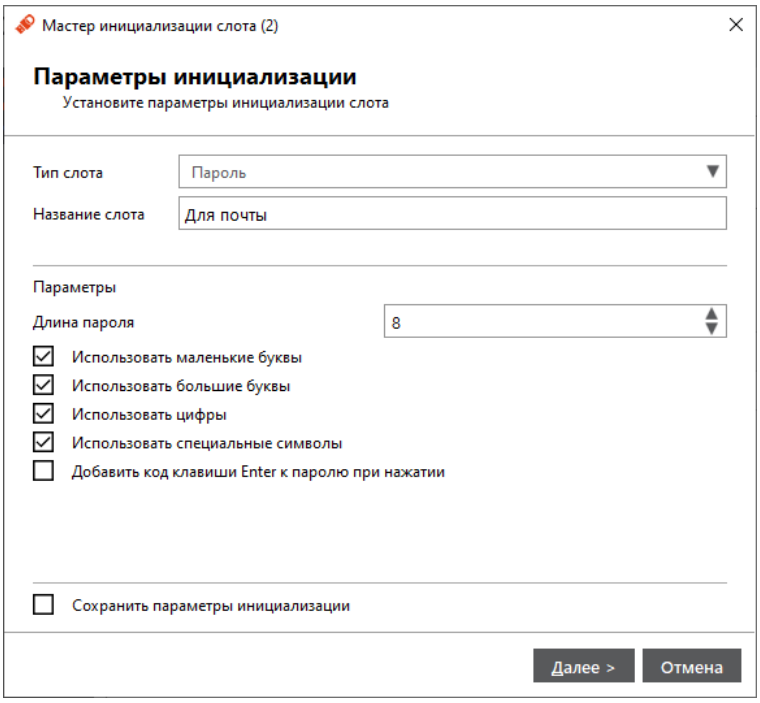


Рисунок 30 – Инициализация слота типом "Пароль". Выбор параметров инициализации

3. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

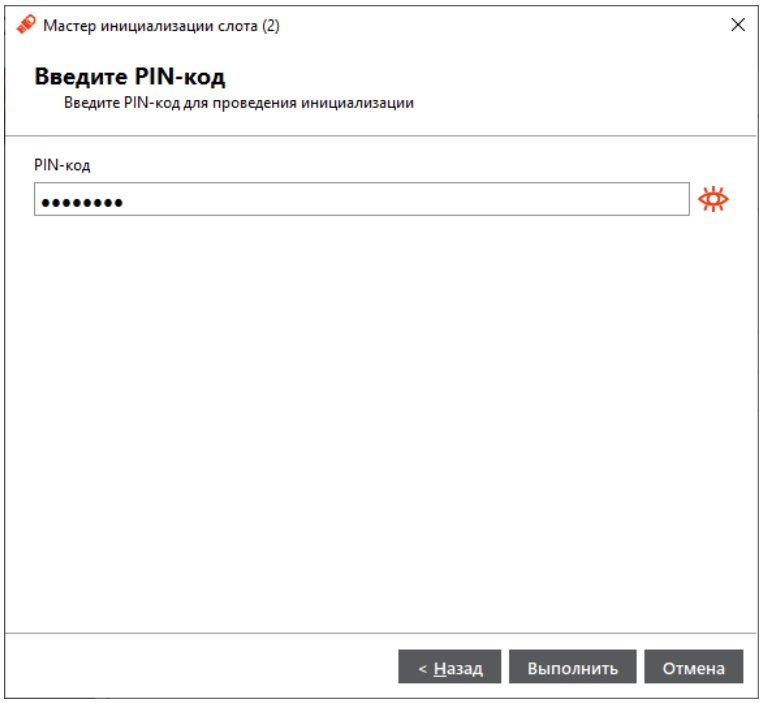


Рисунок 31 - Инициализация слота типом "Пароль". Ввод PIN-кода

4. Будет выполняться генерация и запись многоразового пароля в выбранный слот. По завершении процесса информация об этом будет отображена в окне мастера инициализации. Нажмите кнопку "Завершить".

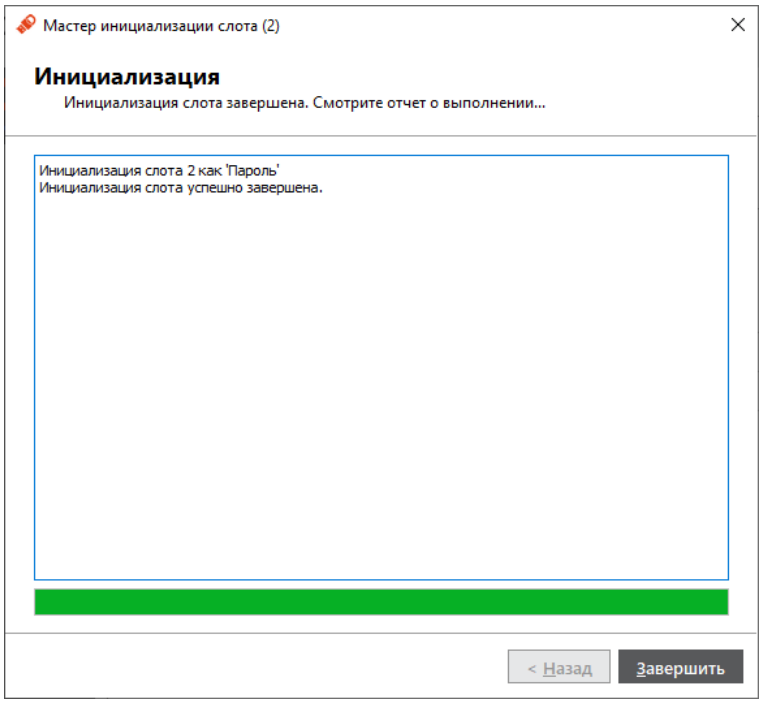


Рисунок 32 – Завершение инициализации слота типом "Пароль"

5. Окно мастера инициализации будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Пароль".

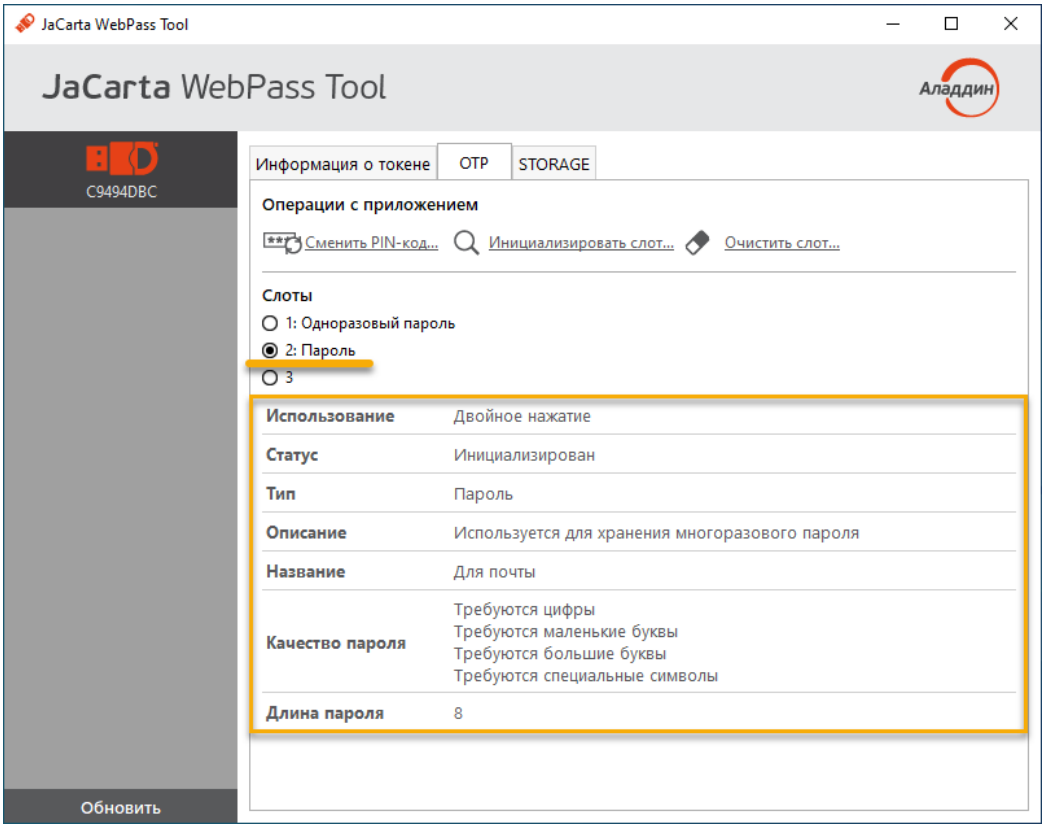


Рисунок 33 – Слот 2 инициализирован типом "Пароль"

4.7.3 Инициализация слота типом "Интернет адрес"

Для записи в слот электронного ключа URL-адреса защищённого ресурса:

1. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне перейдите к вкладе "OTP" и установите отметку возле того слота, в который необходимо записать URL-адрес защищённого ресурса и нажмите кнопку "Инициализировать слот".

   Примечание. *На рисунке 34 отметка установлена возле пустого слота 3, однако URL-адрес может быть записан в любой другой (непустой) слот, при этом данные, которые до этого хранились в слоте будут удалены.*

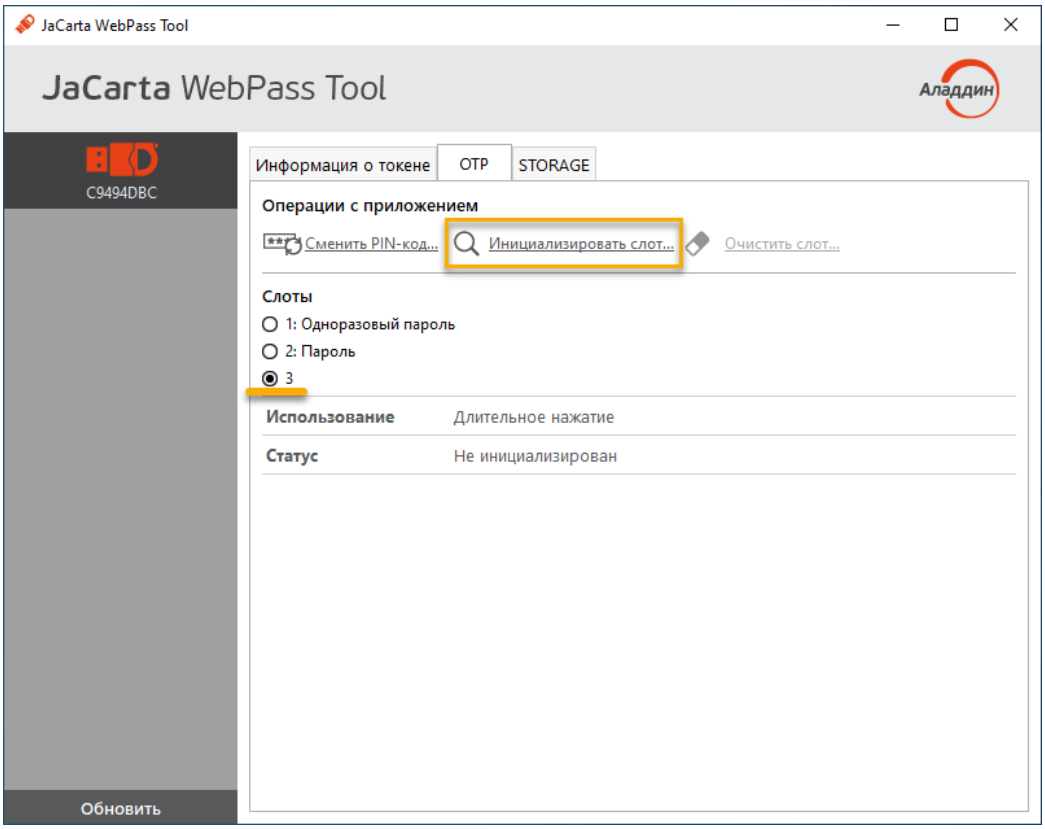


Рисунок 34 – Вкладка "OTP", выбора слота 3 для инициализации

2. Будет открыто стартовое окно мастера инициализации слота "Мастер инициализации слота <№ слота>". Заполните поля мастера следующим образом (см. рисунок 35):
   - в поле "Тип слота" выберите значение "Интернет адрес";
   - в поле "Название слота" введите название, например, Aladdin. Длина поля не должна превышать 32 символа;
   - 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, https://aladdin.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.

Нажмите кнопку "Далее".

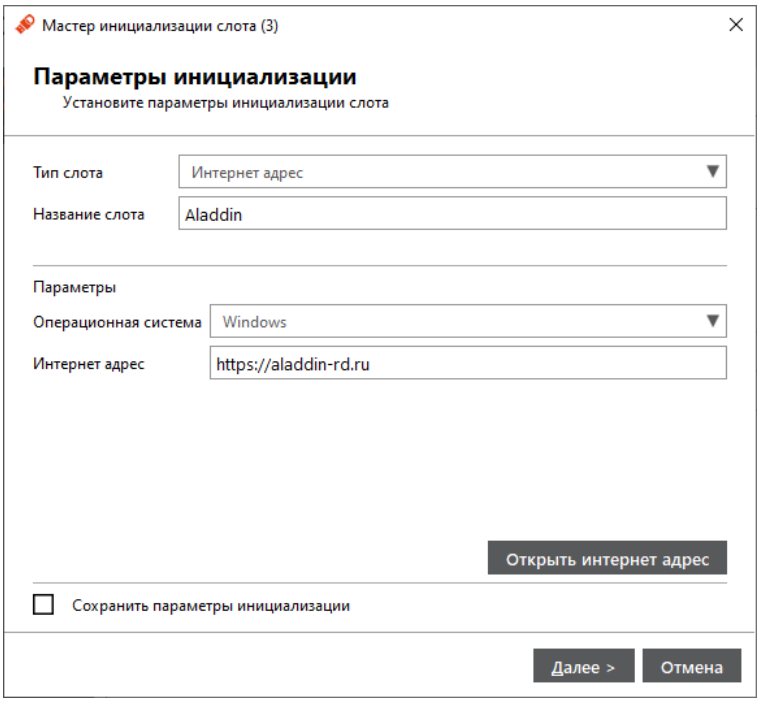


Рисунок 35 – Инициализация слота типом "Интернет адрес". Выбор параметров инициализации

3. В следующем окне мастера инициализации введите PIN-код электронного ключа в одноименное поле, после чего нажмите кнопку "Выполнить" для запуска инициализации.

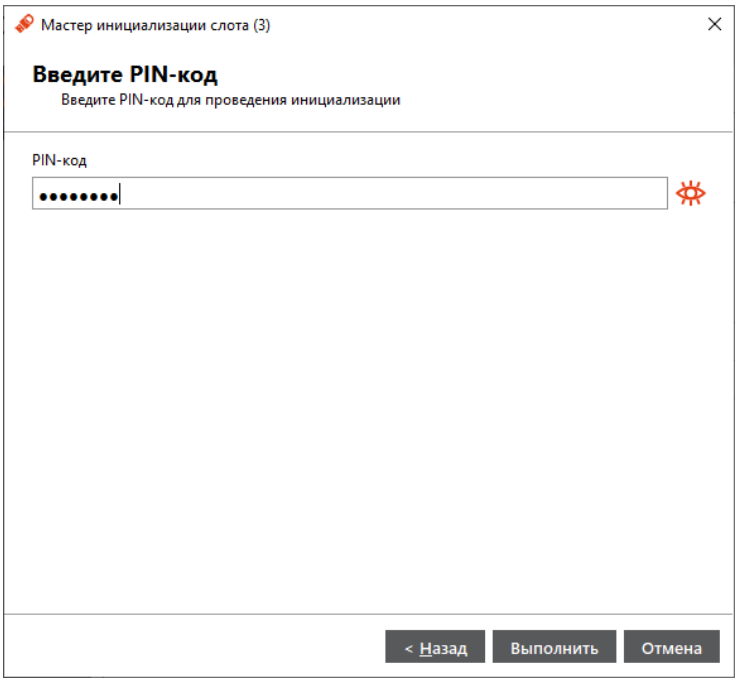


Рисунок 36 – Инициализация слота типом "Интернет адрес". Ввод PIN-кода

4. Будет выполняться запись указанного URL-адреса защищенного ресурса в выбранный слот. По завершении процесса информация об этом будет отображена в окне мастера инициализации. Нажмите кнопку "Завершить".

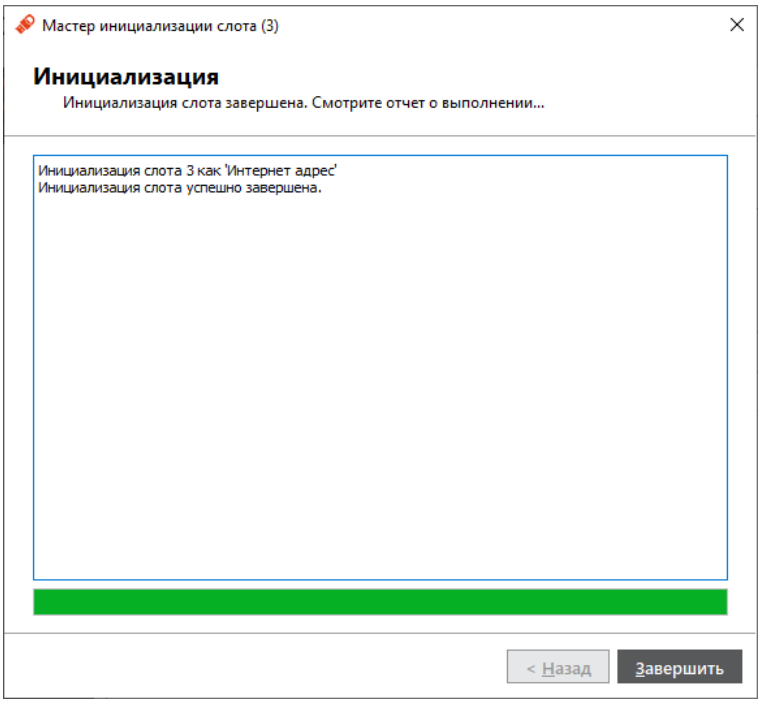


Рисунок 37 – Завершение инициализации слота типом "Интернет адрес"

5. Окно мастера инициализиции будет закрыто. Во вкладке "OTP" будут отображены свойства слота, инициализированного типом "Интернет адрес".

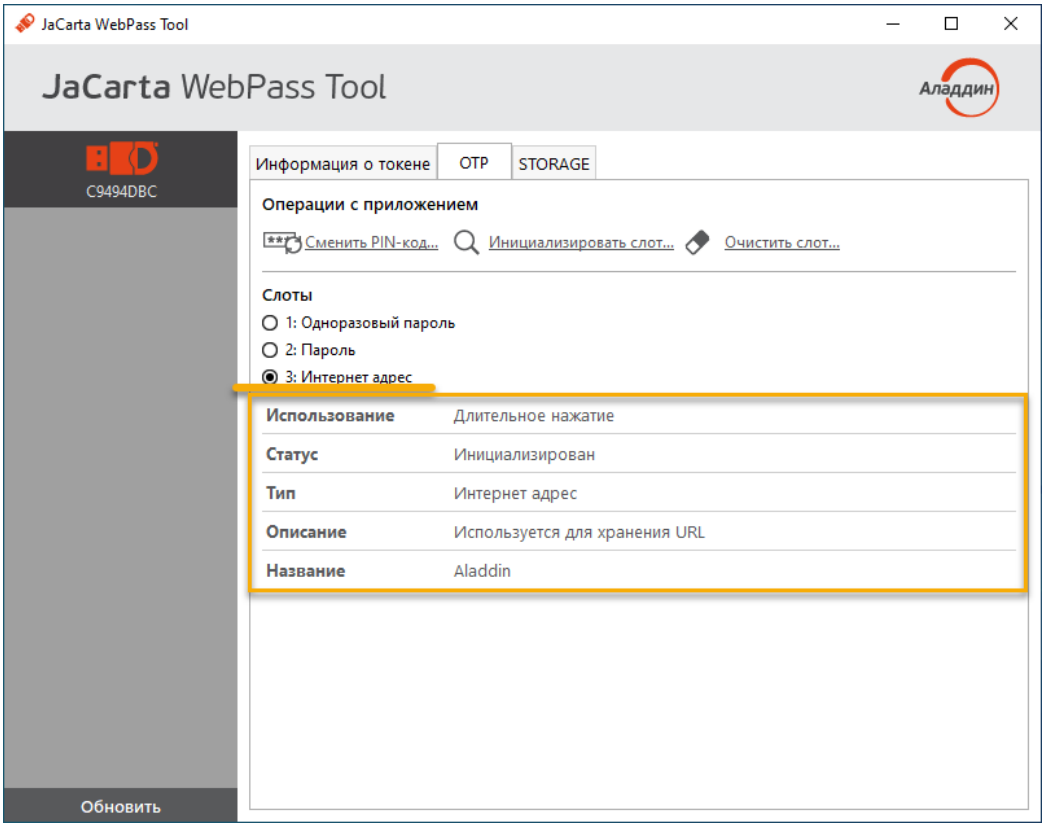


Рисунок 38 – Слот 3 инициализирован типом "Интернет адрес"

4.7.4 Очистка слота

Инициализированный слот электронного ключа может быть очищен, при этом данные, хранящиеся в слоте будут удалены. Для выполнения очистки слота необходимо предъявить PIN-код.

По завершении очистки слот может быть повторно инициализирован любым типом (одноразовый или многоразовый пароль, URL-адрес защищенного ресурса).

Операции очистки слота и его последующая повторная инициализация могут быть выполнены неограниченное количество раз.

Для очистки слота:

1. Подключите электронный ключ к USB-порту и запустите утилиту (см. п. 4.1 на стр. 15). В основном окне перейдите к вкладе "OTP" и выберите слот, который необходимо очистить (на рисунке 39 для примера выбран слот 3 с типом "Интернет адрес"). Нажмите кнопку "Очистить слот". Будет открыто окно "Очистить слот "номер слота"".

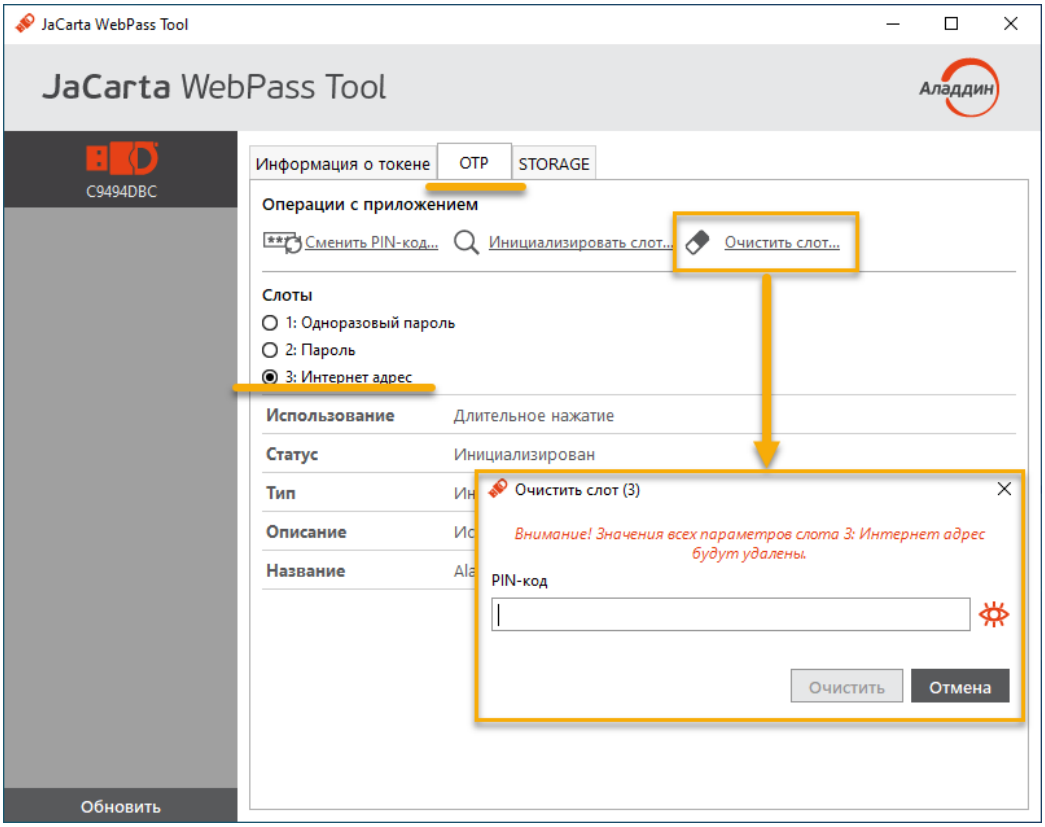


Рисунок 39 – Очистка слота

2. В поле "PIN-код" в окне "Очистить слот "номер слота"" введите PIN-код электронного ключа и нажмите кнопку "Очистить".
3. Будет выполняться очистка слота. По ее завершении данные, хранящиеся в слоте будут удалены. На экране будет отображена информация об этом.

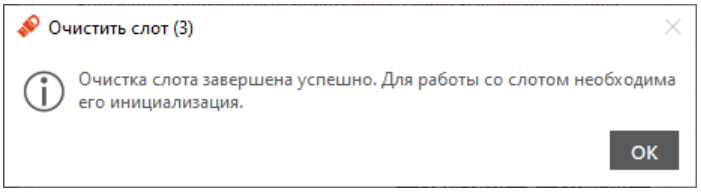


Рисунок 40 - Сообщение о завершении очистки слота

4. Нажмите кнопку "OK" для закрытия окна.

4.7.5 Блокировка слота

Слот блокируется автоматически по достижении счетчиком генерации предельного значения 2^{31}. Для заблокированного слота в поле "Статус" указывается значение "Заблокирован" (см. п. 4.6 на стр. 21).

4.8 Операции с ключевыми контейнерами программных СКЗИ

На электронных ключах JaCarta WebPass реализована возможность хранения ключевых контейнеров программных СКЗИ (КриптоПро CSP и пр.). Операции с ключевыми контейнерами программных СКЗИ выполняются в приложении STORAGE (см. рисунок 41).

Приложение STORAGE является дополнительным приложением. Для работы с электронными ключами JaCarta WebPass переходить на вкладку STORAGE не обязательно.

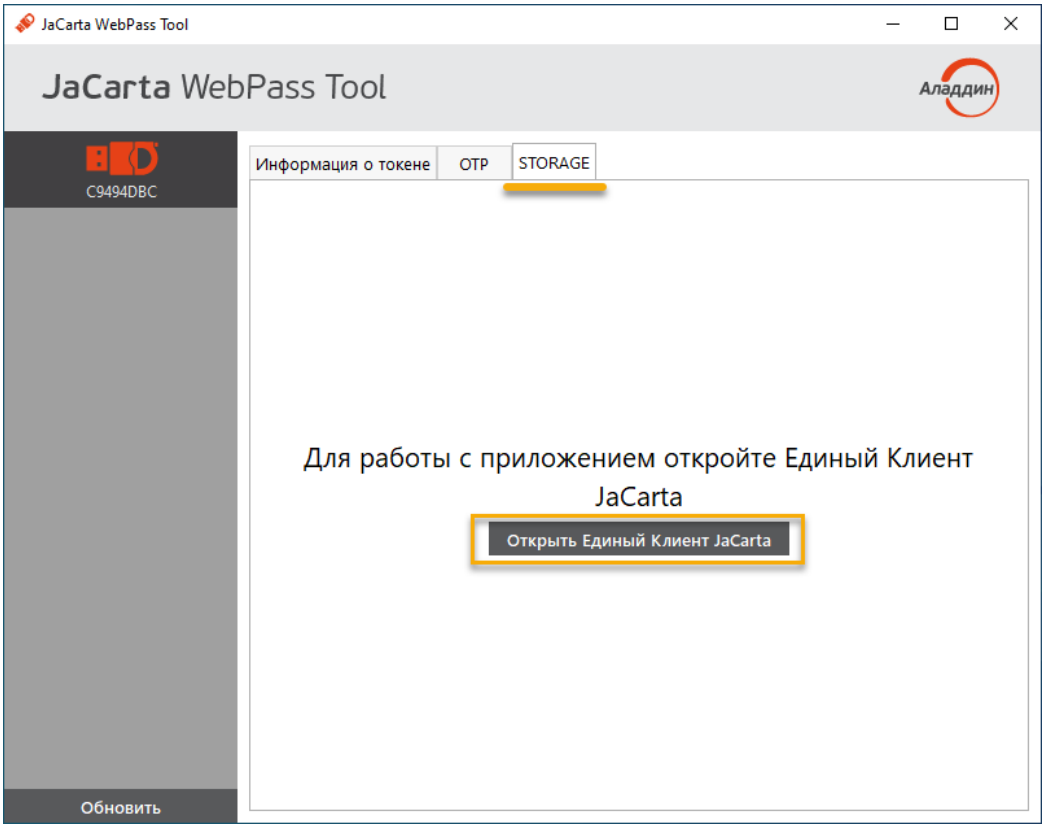


Рисунок 41 - Вкладка "STORAGE"

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

Примечание. *Подробное описание операций в приложении STORAGE приведено в документе "Единый Клиент JaCarta 2.13. Руководство администратора". Подробное описание операций с объектами, хранящимися в памяти электронного ключа приведено в документе "Единый Клиент JaCarta 2.13. Руководство пользователя".*

5. Электронные ключи JaCarta WebPass

5.1 Общие сведения

Внешний вид электронного ключа JaCarta WebPass показан на рисунке 42.

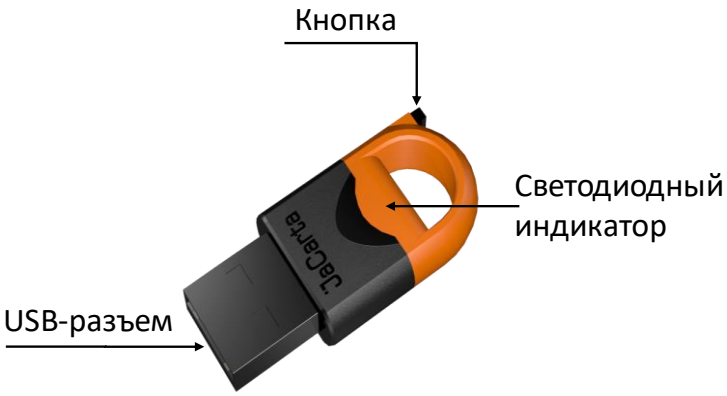


Рисунок 42 – Внешний вид электронного ключа JaCarta WebPass

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 42).

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****!*

5.1.1 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:

5. CCID (Circuit Card Interface Device) – считыватель смарт-карт;
6. 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).

5.1.2 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.

5.1.3 PIN-код

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

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

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

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, общий (одинаковый) для всех трех слотов.

PIN-код используется при выполнении следующих операций:

- смена PIN-кода;
- инициализация слота (запись в слот одноразового или многоразового пароля либо URL-адреса защищенного ресурса);
- очистка слота.

5.2 Регистрация электронного ключа 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).

> *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.

Для регистрации электронного ключа:

1. Подключить электронный ключ к компьютеру и запустить утилиту JaCarta WebPass Tool. (см. п. 4.1 на стр. 15).
2. Сгенерировать файл с расширением *.xml / *.dat с помощью утилиты JaCarta WebPass Tool.

Примечание. *Генерация файла с расширением *.xml / *.dat с помощью утилиты JaCarta WebPass Tool выполняется в процессе инициализации слота типа "Одноразовый пароль" (подробнее см. п. 4.7.1 "*Инициализация слота типом "Одноразовый пароль"*).*

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

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

5.3 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.

5.3.1 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".

5.3.2 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".

5.3.3 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, соответствующем слоту 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

6. Контакты

6.1 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.ru (общий)

Web: https://www.aladdin.ru

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

6.2 Техподдержка

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

Коротко о компании

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

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

Основные направления

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

Лицензии

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

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Система менеджмента качества компании соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)

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