



# JaCarta WebPass Tool

---

## Руководство по использованию

Версия документа: 1.5

Редакция от: 4 мая 2017 г.

Листов: 44

## Аннотация

Данное Руководство по использованию (далее – Руководство) предназначено для персонала, осуществляющего установку, эксплуатацию и настройку приложения JaCarta WebPass Tool, входящего в состав программного комплекса Единый Клиент JaCarta.

Приложение JaCarta WebPass Tool предназначено для настройки электронных ключей JaCarta WebPass (JC600) и JaCarta U2F/WebPass (JC603).

В настоящем Руководстве приведены общие сведения, системные требования, режимы работы, краткий обзор пользовательского интерфейса, описание вкладок, порядок работы с электронными ключами JaCarta WebPass и др.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО «Аладдин Р. Д.». Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

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 компанией «Аладдин Р. Д.» без предварительного уведомления. 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 компания «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО «Аладдин Р. Д.».

Владельцем товарных знаков Apple, iPad, iPhone, macOS, OS X является корпорация Apple Inc. Владельцем товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владельцем товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

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

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО «Аладдин Р. Д.» обязательны.

© ЗАО «Аладдин Р. Д.», 1995–2017. Все права защищены.

# Содержание

<b>1. Общие сведения</b>	<b>4</b>
1.1. Термины и определения	4
1.2. Дополнительная документация	4
<b>2. Системные требования</b>	<b>5</b>
<b>3. Описание электронных ключей JaCarta WebPass</b>	<b>6</b>
3.1. Общие сведения	6
3.2. Режимы работы	7
3.3. Световая индикация рабочих состояний	7
3.4. PIN-код администратора	7
3.4.1. Назначение и случаи использования PIN-кода администратора	7
3.4.2. Настройки PIN-кода по умолчанию	8
<b>4. Установка и удаление утилиты JaCarta WebPass Tool</b>	<b>9</b>
4.1. Описание пакетов установки	9
4.2. Установка утилиты	9
4.3. Удаление утилиты	14
<b>5. Запуск утилиты JaCarta WebPass Tool и обзор пользовательского интерфейса</b>	<b>18</b>
5.1. Запуск утилиты	18
5.2. Описание вкладок	21
5.2.1. Вкладка Информация о токене	21
5.2.2. Вкладка OTP	23
5.2.3. Вкладка STORAGE	24
5.3. Операции, выполняемые в приложении OTP	25
5.3.1. Смена PIN-кода администратора	25
5.3.2. Инициализация слотов	26
5.3.3. Очистка слотов	36
<b>6. Порядок работы с электронными ключами JaCarta WebPass</b>	<b>38</b>
6.1. Регистрация токена JaCarta WebPass	38
6.2. Использование токена JaCarta WebPass	39
6.2.1. Автоматическая подстановка одноразового пароля	39
6.2.2. Автоматическая подстановка многоразового пароля	40
6.2.3. Переход на Web-страницу защищённого ресурса	40
<b>Сокращения и аббревиатуры</b>	<b>41</b>
<b>Контакты, техническая поддержка</b>	<b>42</b>
<b>Регистрация изменений</b>	<b>43</b>

# 1. Общие сведения

JaCarta WebPass Tool представляет собой отдельное приложение (далее – утилита), входящее в состав программного комплекса 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 многозначного (постоянного) пароля с возможностью вставки этого пароля в экранные формы ввода, а также запуска Web-браузера и автоматического перехода по сохраненному в токене адресу Web-ресурса.

## 1.1. Термины и определения

Термины, используемые в настоящем Руководстве, приведены в таблице 1.

Таблица 1


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: <ul style="list-style-type: none"><li>• OTP;</li><li>• STORAGE;</li><li>• U2F *.</li></ul>  *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.
Токен	Аппаратное устройство в форм-факторе USB-токена, карты microSD, со стандартными встроенными операционной системой (ОС) и программным обеспечением (ПО).
Электронный ключ	Смарт-карта или токен.
PIN-код администратора	Последовательность символов, которую необходимо ввести, чтобы администратор мог совершить определенную операцию. Подробное описание см. в разделе PIN-код администратора.

Таблица 1

## 1.2. Дополнительная документация

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.

## 2. Системные требования

### Таблица 2

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

Таблица 2

## 3. Описание электронных ключей JaCarta WebPass

### 3.1. Общие сведения

Внешний вид электронного ключа JaCarta WebPass показан на рисунке 1.

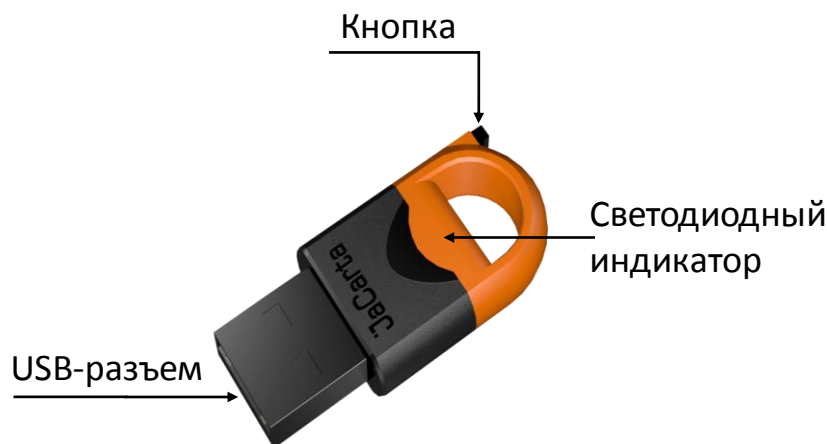


Рисунок 1

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 токена JaCarta WebPass).

Внутри корпуса электронного ключа расположен светодиодный индикатор, отражающий различные режимы работы (подробнее см. Режимы работы и Световая индикация рабочих состояний).

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).



**Внимание!** 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**



Внимание! 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 токена. 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 таблице 3.

Таблица 3

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

Таблица 3

### 4.2. Установка утилиты

Чтобы установить Утилиту JaCarta WebPass Tool выполните следующие действия:

1. В зависимости от разрядности операционной системы запустите нужный файл установки (см. раздел 4.1 Описание пакетов установки). Отобразится следующее окно (см. рис. 2).

Окно приветствия мастера установки Единого Клиента JaCarta

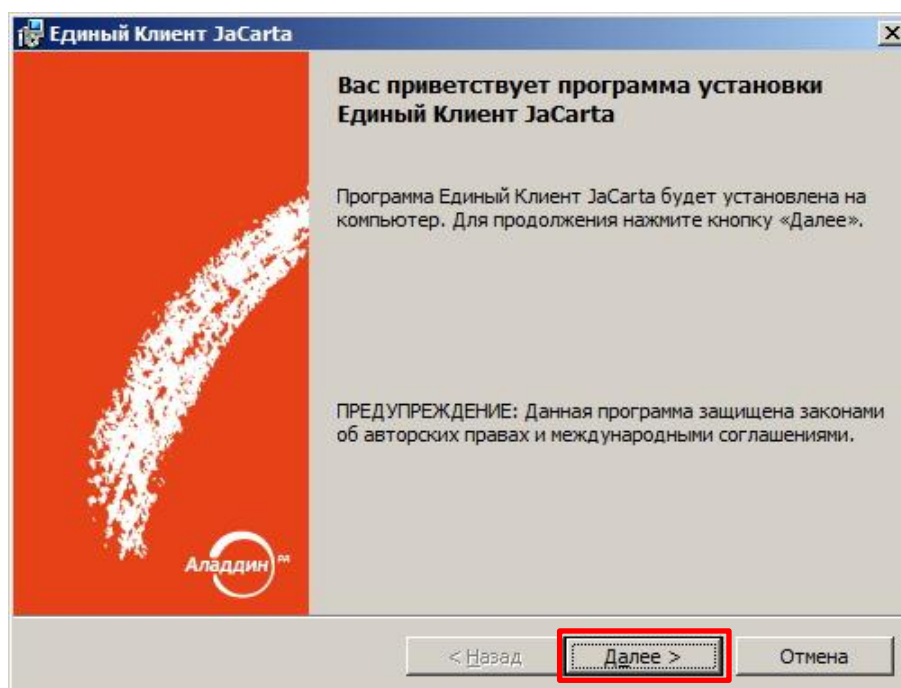


Рисунок 2

2. Нажмите **Далее >**. Отобразится следующее окно (см. рис. 3).

## Окно лицензионного соглашения

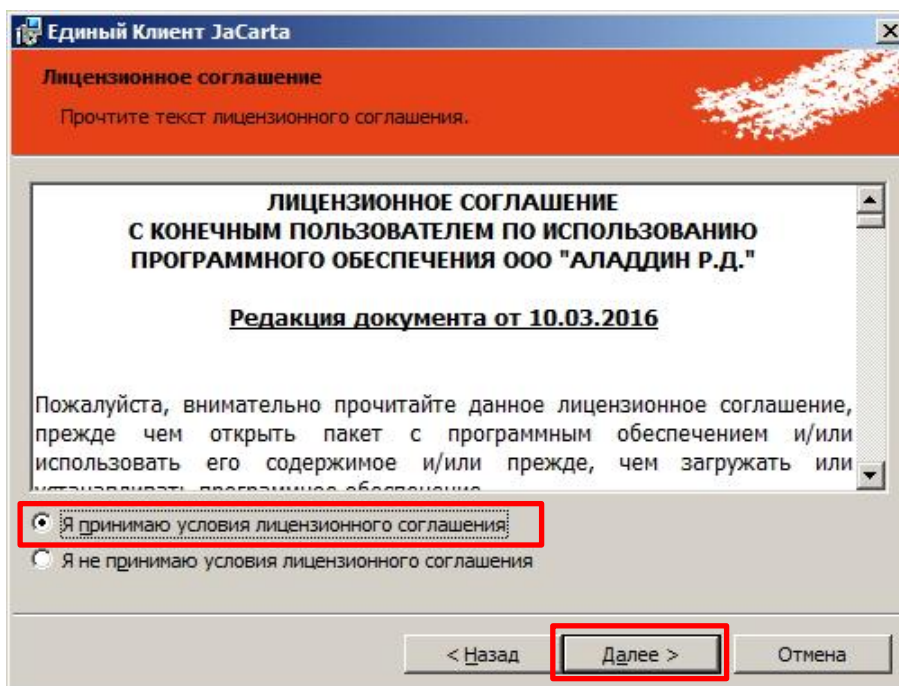


Рисунок 3

## 3. Прочитайте лицензионное соглашение

- 3.1. Если вы не согласны с условиями лицензионного соглашения, прекратите установку, нажав **Отмена**.
- 3.2. Если вы согласны с условиями лицензионного соглашения, выберите пункт **Я принимаю условия лицензионного соглашения** и нажмите **Далее >**.

4. В появившемся окне выберите вид установки: **Выборочная** (см. рис. 4).

## Окно выбора пути и вида установки Единого Клиента JaCarta

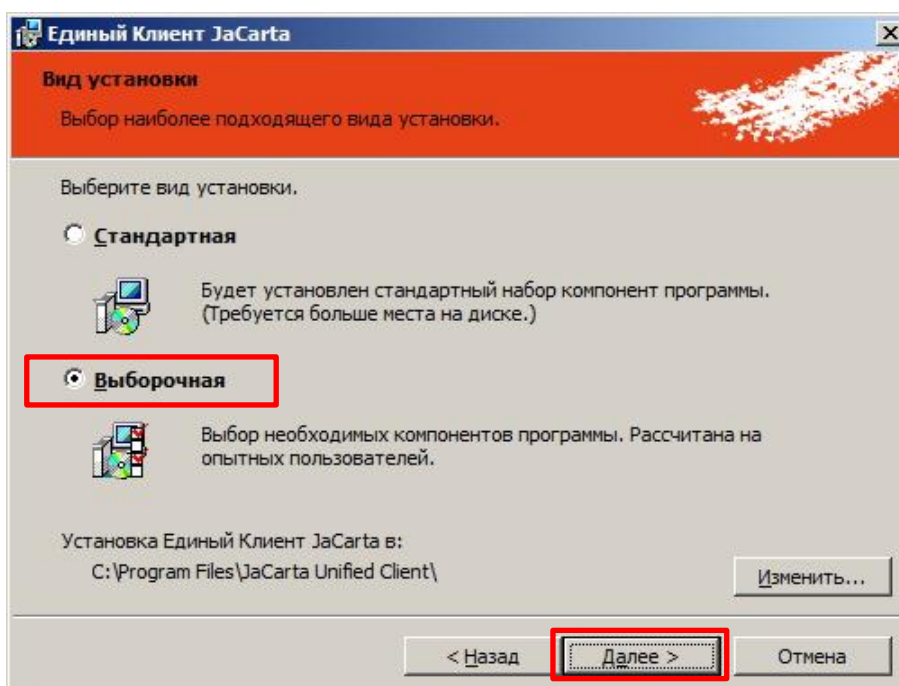



Рисунок 4

- При необходимости воспользуйтесь кнопкой **Изменить...**, чтобы изменить путь установки Единого Клиента JaCarta.
- Нажмите **Далее** > отобразится окно (см. рис. 5).

 Подробное описание компонентов Единого Клиента JaCarta представлено в документе [Единый Клиент JaCarta. Руководство администратора]. Для установки утилиты JaCarta WebPass Tool достаточно выбрать установку двух компонентов: Единый клиент JaCarta и JaCarta WebPass Tool.

Выборочная установка компонент Единого Клиента JaCarta

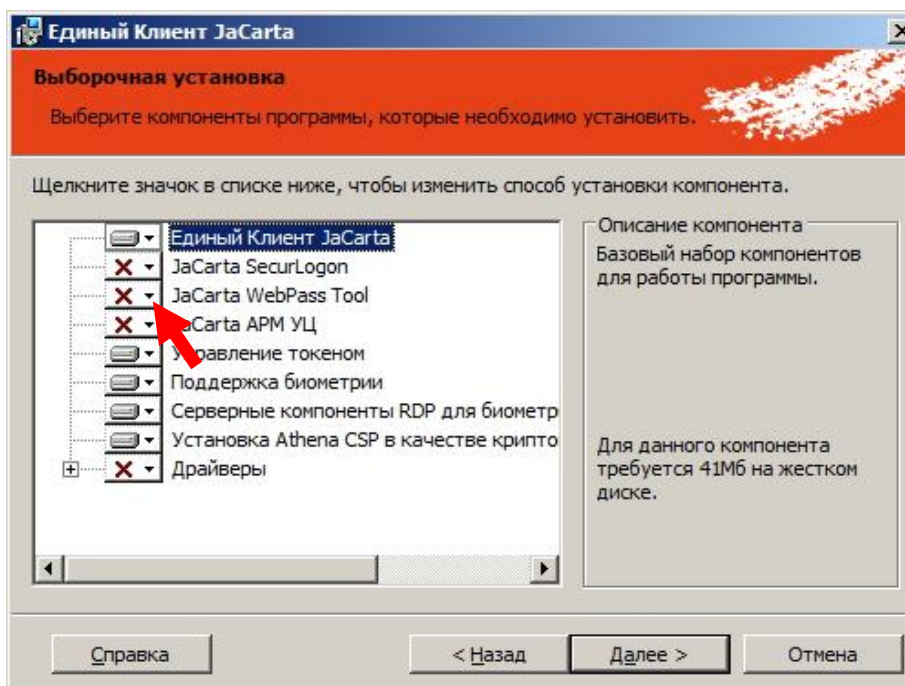



Рисунок 5

- Для установки компонента JaCarta WebPass Tool в списке компонентов строке с названием JaCarta WebPassTool нажмите на значок  и в появившемся контекстном меню (см. рис. 6) выберите необходимую опцию установки.

Опции установки

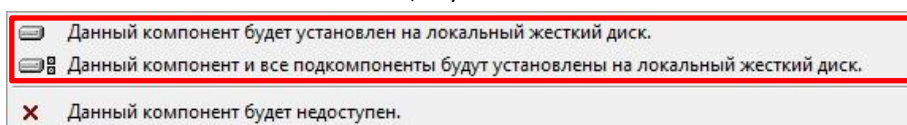


Рисунок 6

После выбора для установки компонента JaCarta WebPass Tool окно выборочной установки будет выглядеть следующим образом (см. рис. 7).

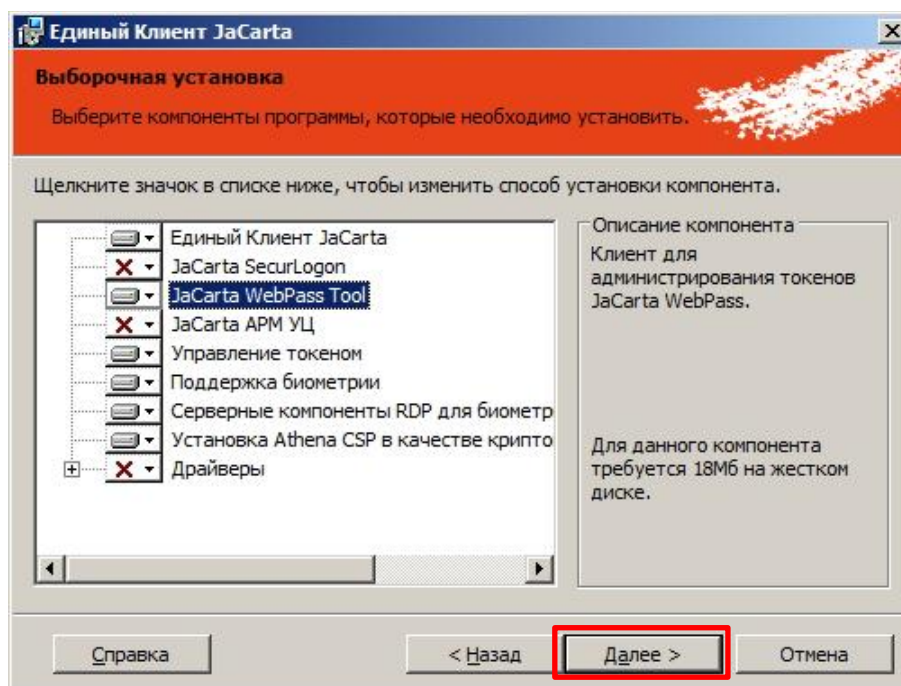


Рисунок 7

8. Нажмите **Далее >** отобразится окно (см. рис. 8).

Выбор способа автоматического обновления при выборочной установке Единого Клиента JaCarta

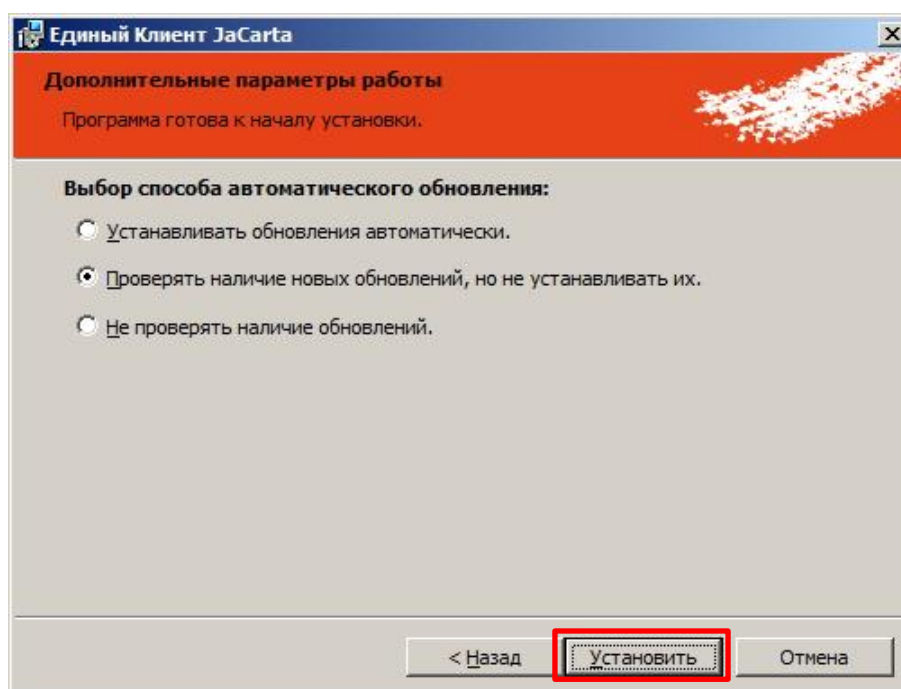


Рисунок 8

9. Выберите способ автоматического обновления, нажмите **Установить** и дождитесь окончания установки.

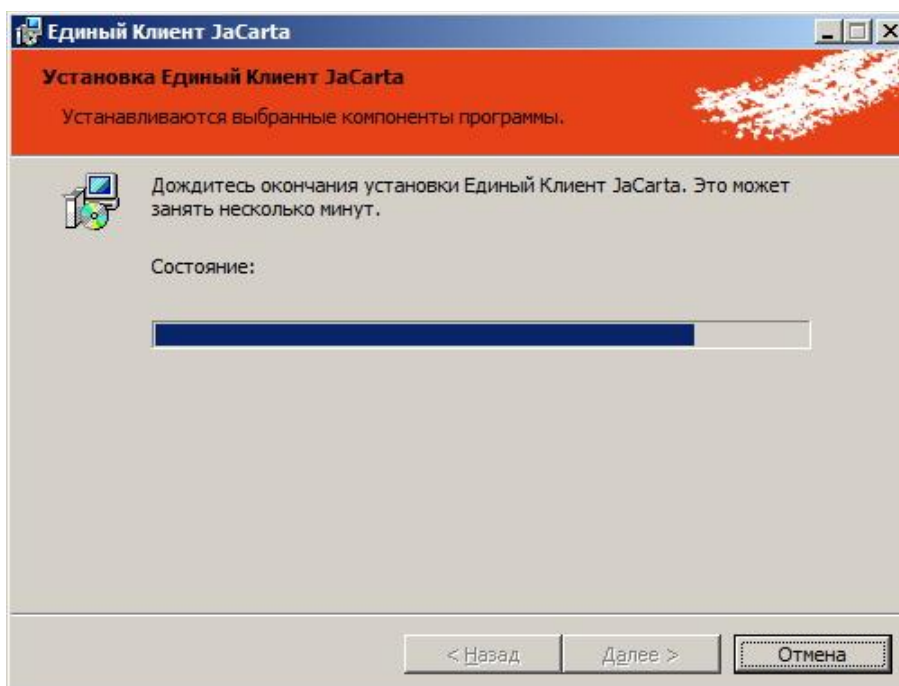


Рисунок 9

10. По завершении установки отобразится следующее окно (см. рис. 10).

Окно завершения установки Единого Клиента JaCarta

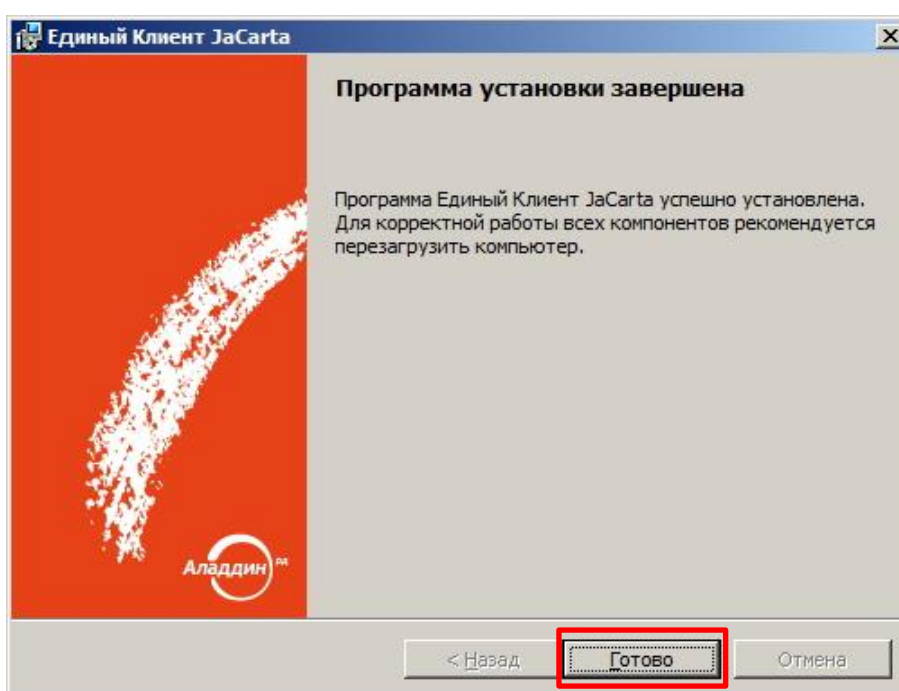


Рисунок 10

11. Нажмите **Готово**.

12. Перезагрузите компьютер, если отобразится соответствующее предупреждение.

Более подробные сведения об установке и удалению Единого Клиента JaCarta см. в документе [Единый Клиент JaCarta. Руководство администратора].



## 4.3. Удаление утилиты

Для того, чтобы удалить утилиту JaCarta WebPass выполните следующие действия:

1. Нажмите **Пуск** → **Панель управления** → **Программы и компоненты**.
2. В появившемся окне найдите и выделите строку с программой **Единый Клиент JaCarta** и на панели инструментов нажмите **Изменить** (см. рис. 11).

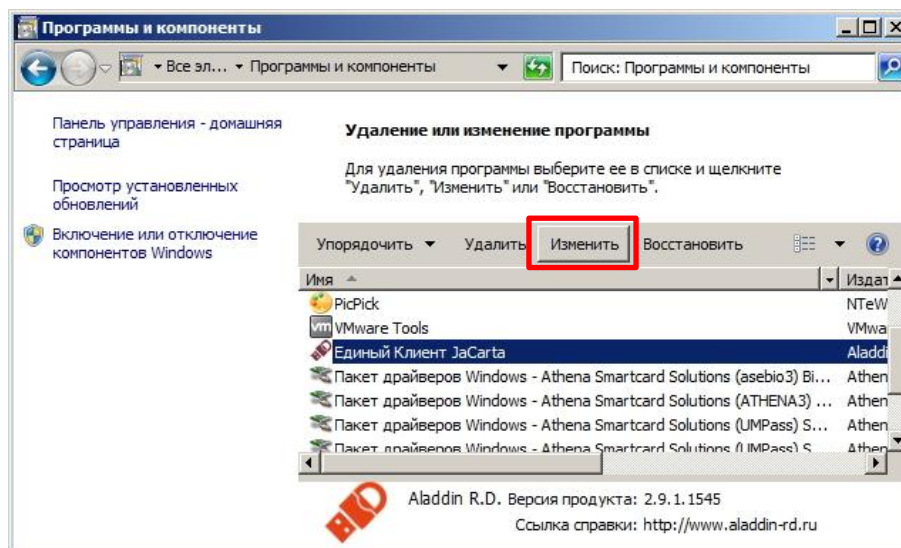


Рисунок 11

3. В появившемся окне (см. рис. 12) нажмите **Далее**.

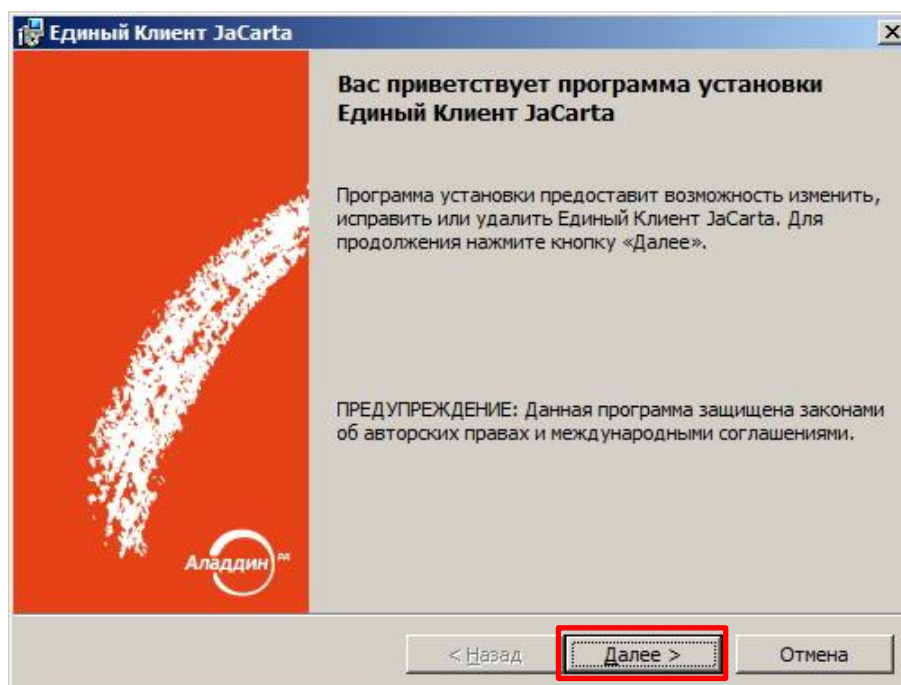


Рисунок 12

4. В появившемся окне (см. рис. 13) выберите опцию **Изменить** и нажмите **Далее**.

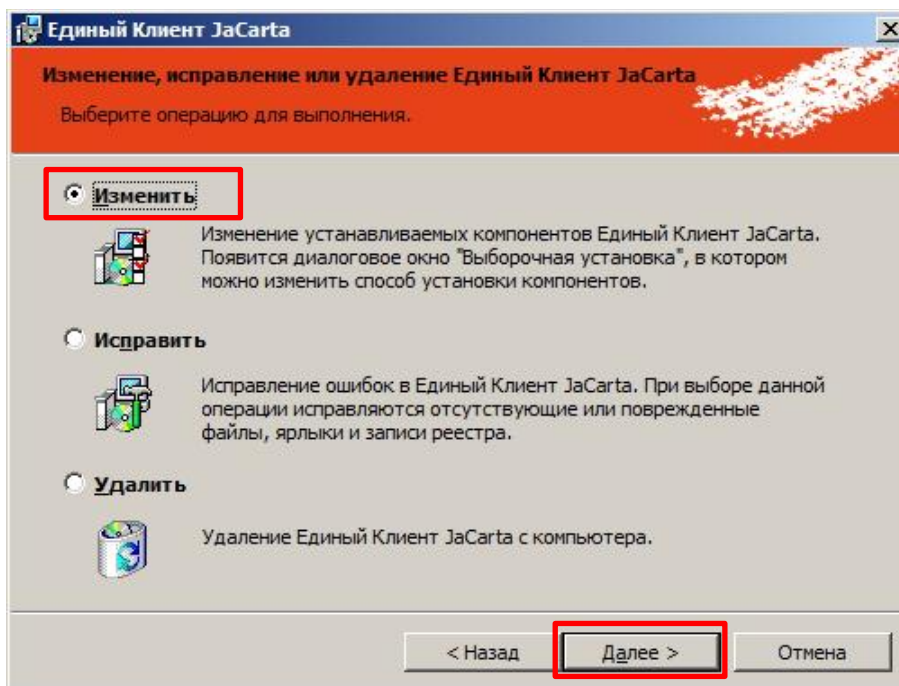



Рисунок 13

5. Для удаления компонента JaCarta WebPass Tool в списке компонентов строке с названием **JaCarta WebPassTool** нажмите на значок  (см. рис. 14) и в появившемся контекстном меню (см. рис. 15) выберите необходимую опцию установки.

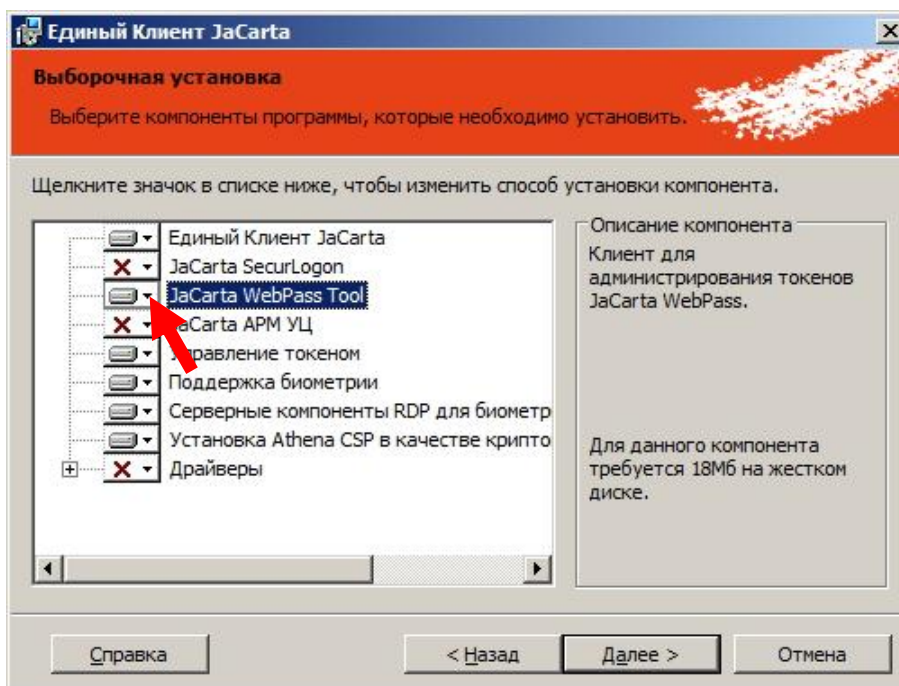


Рисунок 14

#### Опции установки

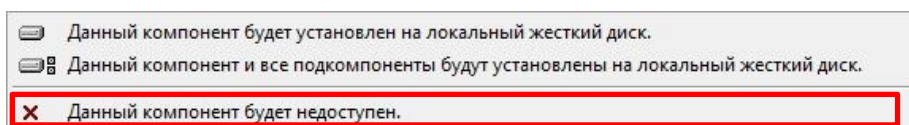


Рисунок 15

После выбора для удаления компонента JaCarta WebPass Tool окно выборочной установки будет выглядеть следующим образом (см. рис. 16).

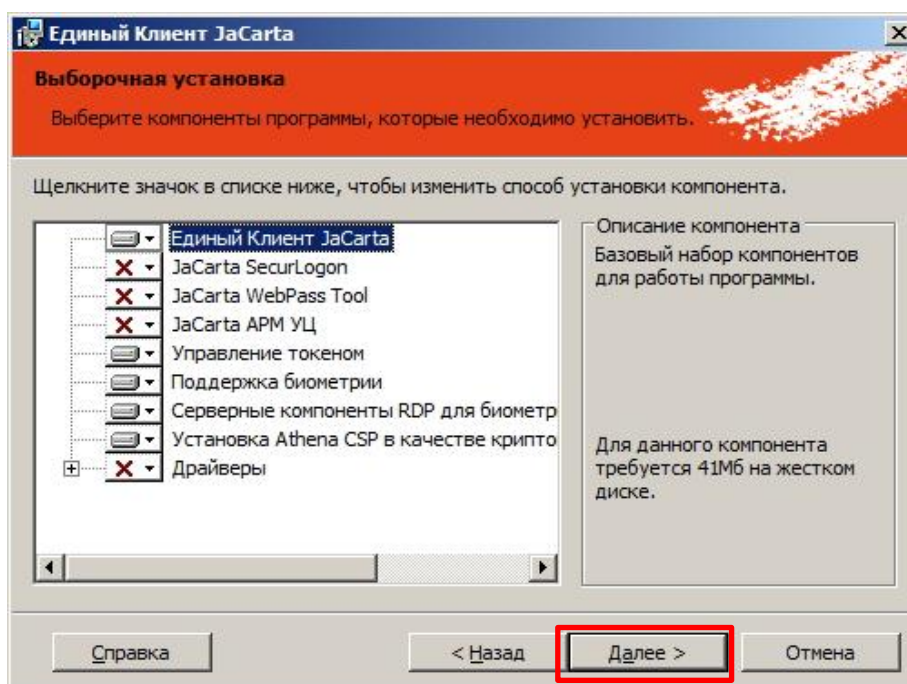


Рисунок 16

6. Нажмите **Далее** и в появившемся окне (см. рис. 17) выберите способ автоматического обновления, нажмите **Изменить** и дождитесь окончания удаления компонента.

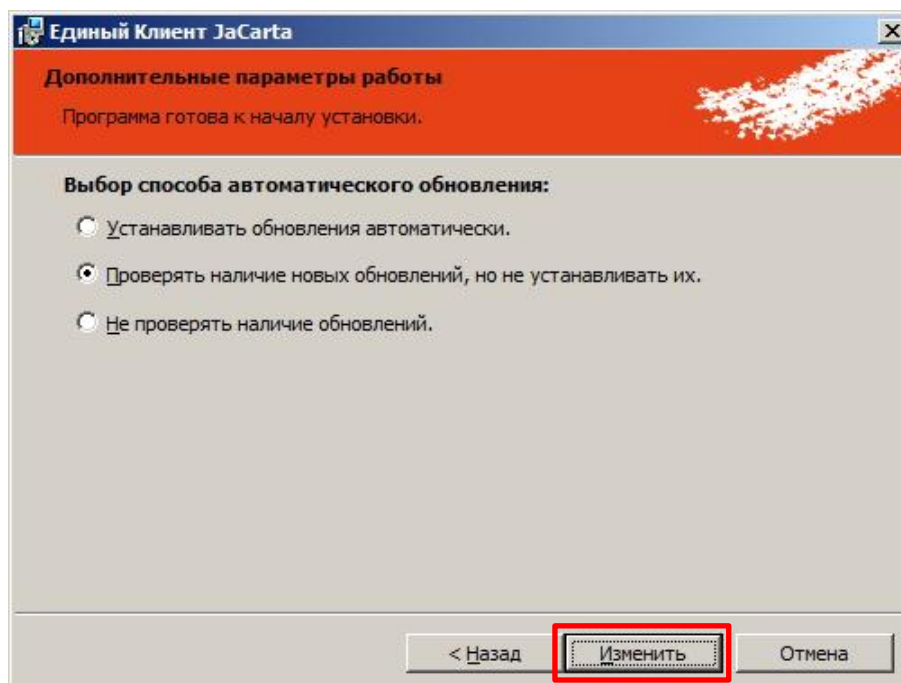


Рисунок 17

После завершения внесения изменений программой установки отобразится следующее окно (см. рис. 18).

7. Нажмите **Готово**.



8. Перезагрузите компьютер, если отобразится соответствующее предупреждение.

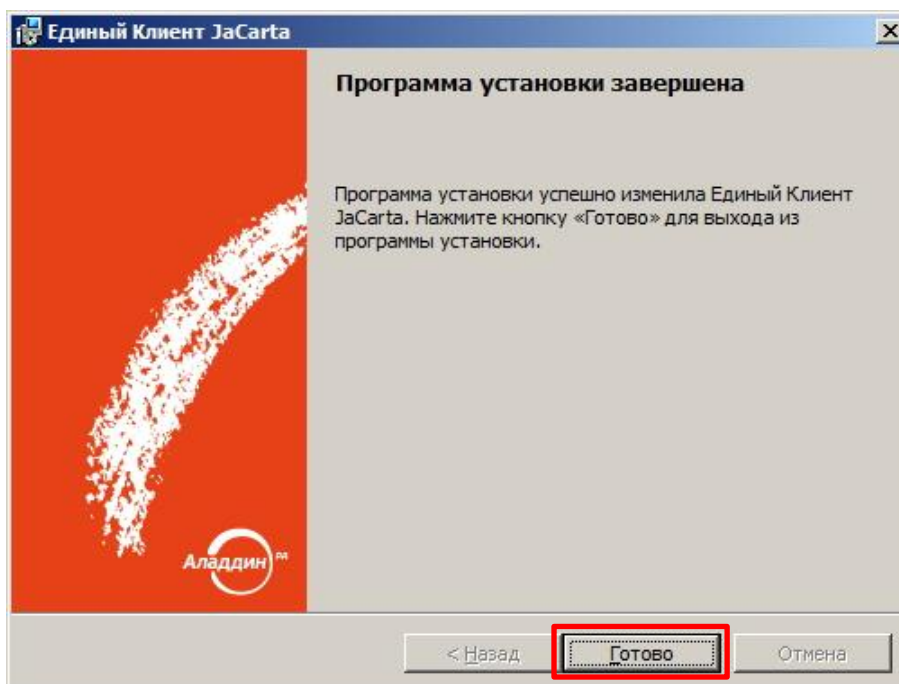


Рисунок 18

Более подробные сведения об установке и удалению Единого Клиента JaCarta см. в документе [Единый Клиент JaCarta. Руководство администратора].

## 5. Запуск утилиты JaCarta WebPass Tool и обзор пользовательского интерфейса

---

### 5.1. Запуск утилиты

Чтобы запустить утилиту JaCarta WebPass Tool нажмите **Пуск**, выберите **Все программы -> Аладдин Р. Д. -> JaCarta WebPass Tool** (см. рис. 19).

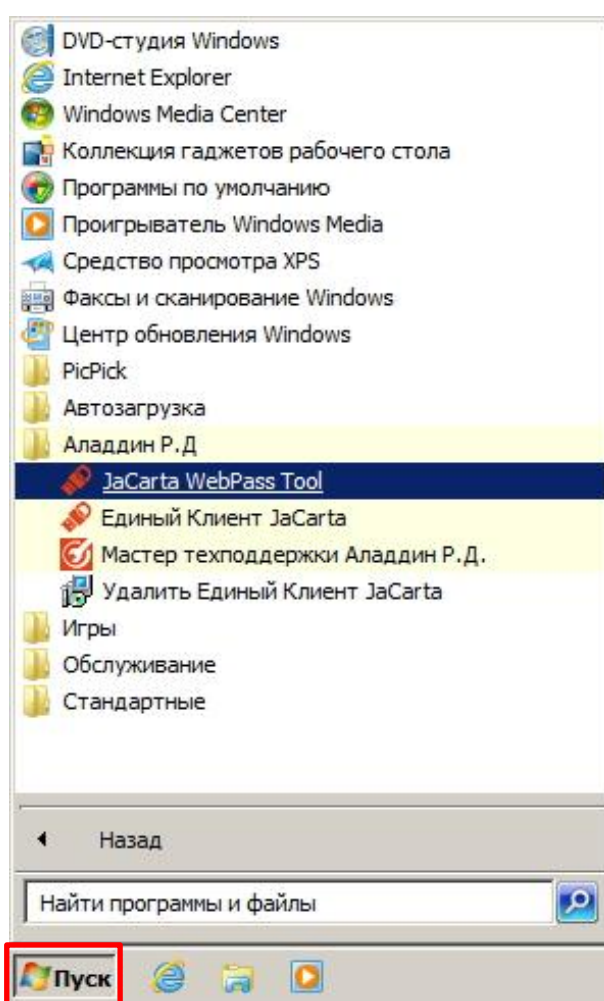


Рисунок 19

После запуска утилиты JaCarta WebPass Tool окно основного интерфейса будет выглядеть следующим образом (см. рис. 20).

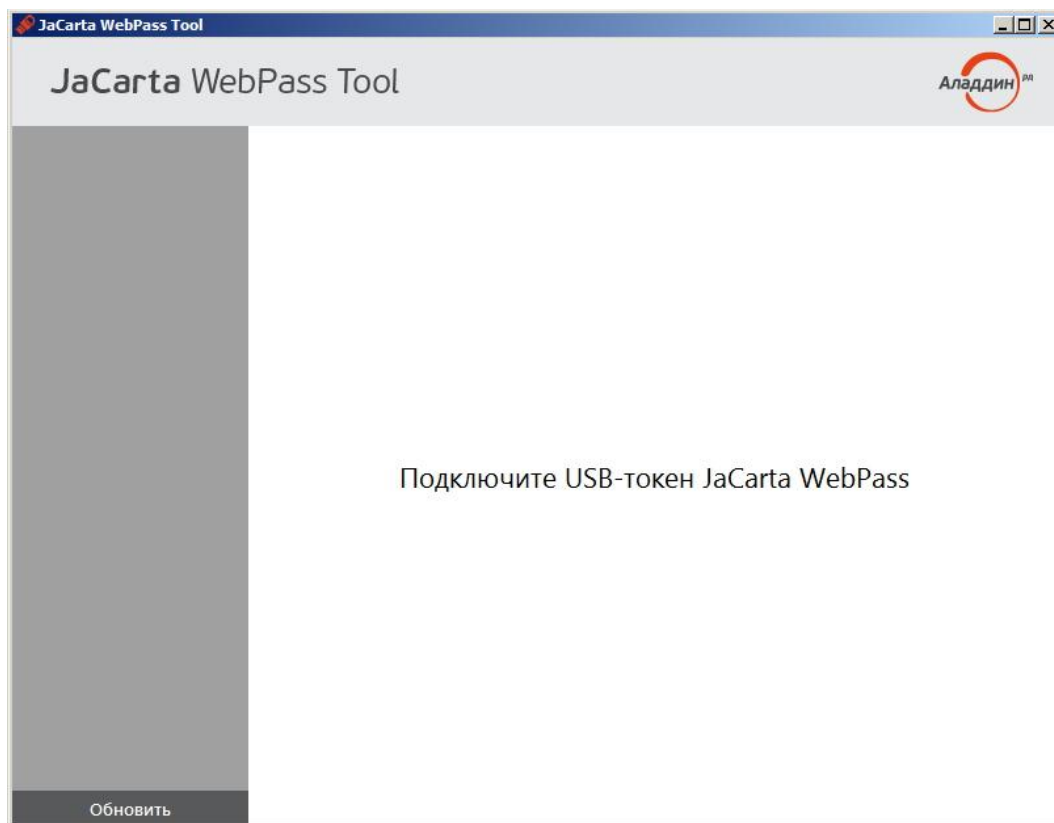


Рисунок 20



 При нажатии на логотип компании Аладдин в верхнем правом углу окна – появится окно со сведениями об утилите JaCarta WebPass Tool (см. рис. 21).



Рисунок 21

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 (см. рис. 22). 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.

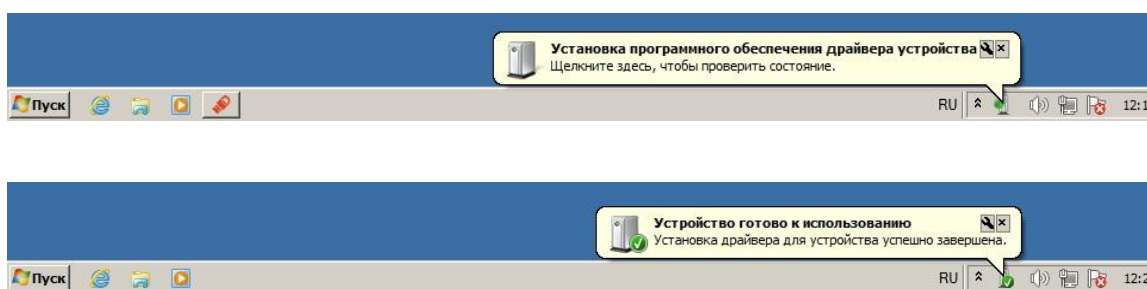



Рисунок 22

 **Примечание** – 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 (см. рис. 23).

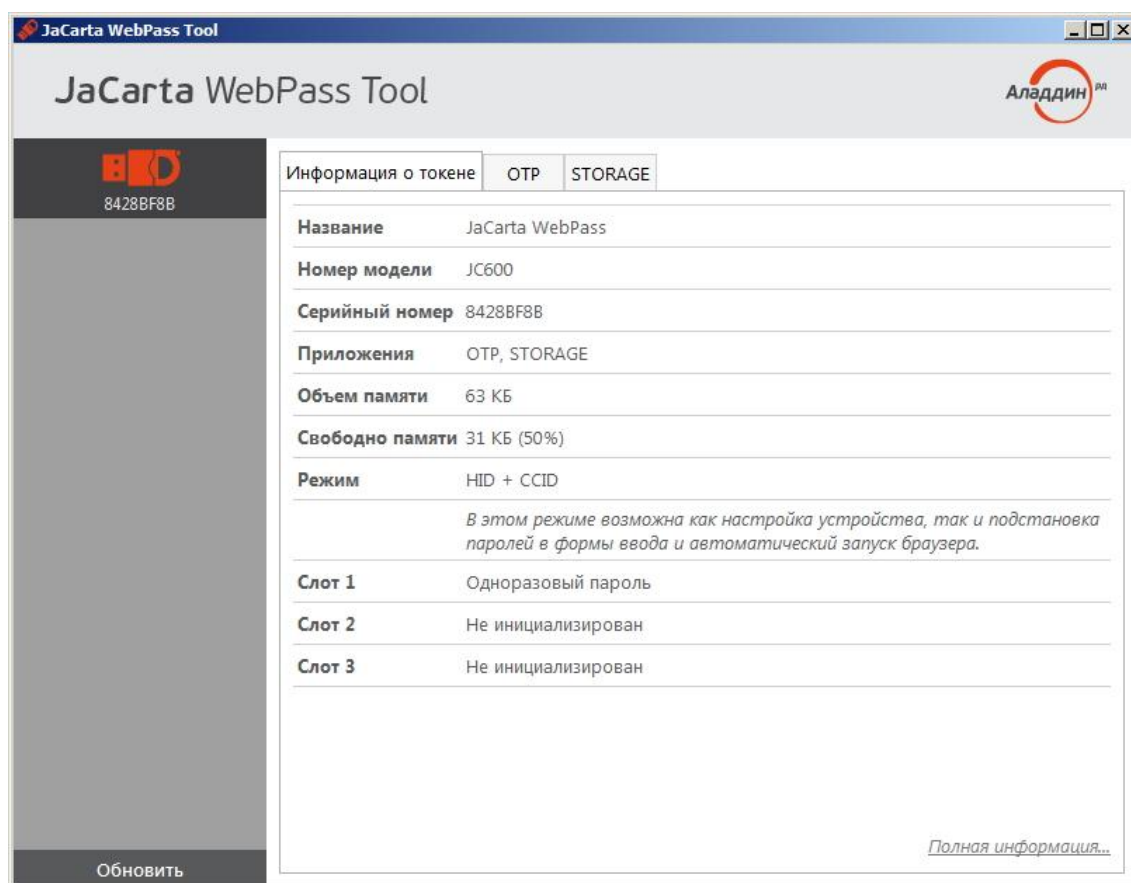


Рисунок 23

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 4.

## Таблица 4

Вкладка	Описание
Информация о токене	На этой вкладке отображаются общие сведения о выбранном электронном ключе. Чтобы отобразить подробные сведения, нажмите <a href="#">Полная информация...</a> (Подробнее см. "Вкладка Информация о токене").
ОТР	На этой вкладке отображаются кнопки операций, выполняемых в приложении ОТР, 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

Таблица 4

## 5.2. Описание вкладок

### 5.2.1. Вкладка Информация о токене

Вкладка **Информация о токене** имеет следующий вид (см. рис. 24).

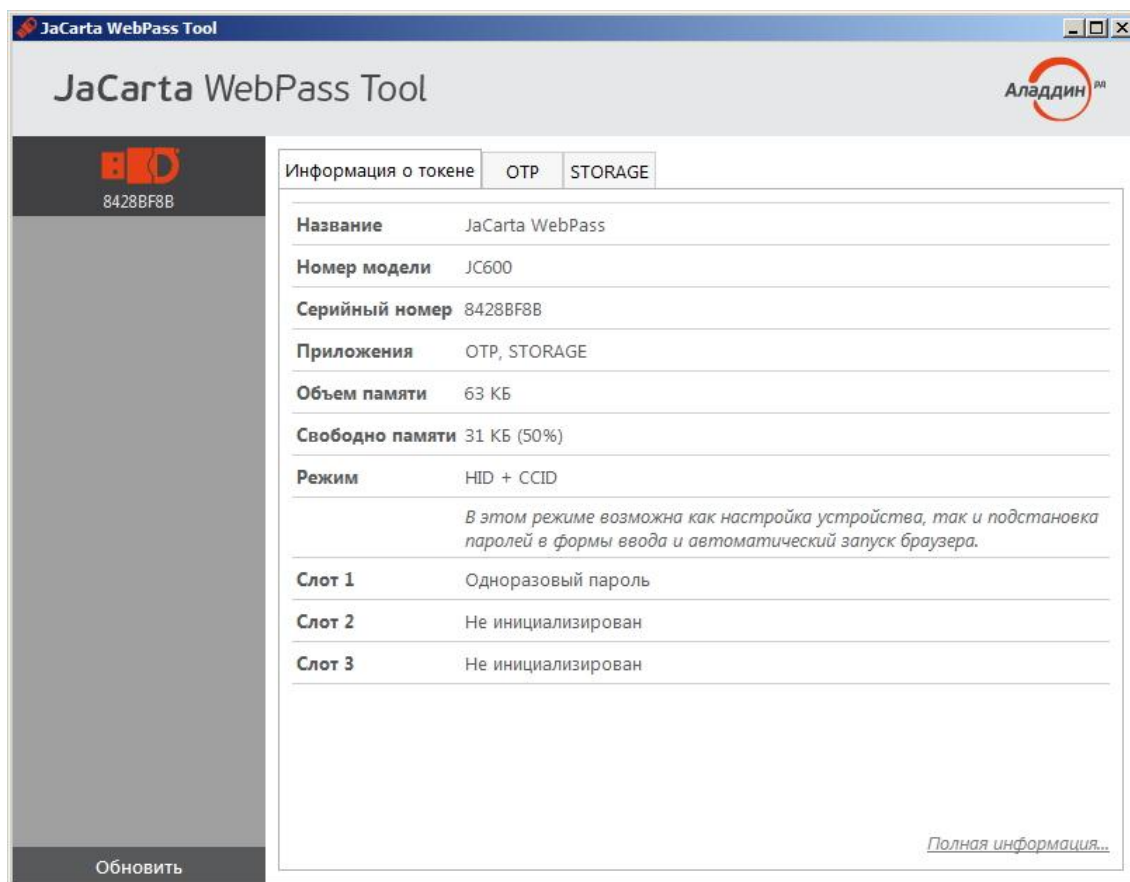


Рисунок 24

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

## Таблица 5

Поле	Описание
Название	Название модели выбранного электронного ключа
Номер модели	Номер модели выбранного электронного ключа


Поле	Описание
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 объем памяти выбранного электронного ключа
Свободно памяти	Объем 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

Таблица 5

В нижнем правом углу вкладки располагается ссылка **Полная информация...**, нажатие на которую открывает окно с подробными сведениями о выбранном электронном ключе (см. рис. 25).



Рисунок 25

Описание предоставляемой информации об электронном ключе приведено в таблице 6.

## Таблица 6

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

Поле	Описание
Приложения	Приложения, установленные на выбранном электронном ключе
Объем памяти	Объем памяти выбранного электронного ключа
Свободно памяти	Объем 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

Таблица 6

## 5.2.2. Вкладка OTP

Вкладка **OTP** имеет следующий вид (см. рис. 26).

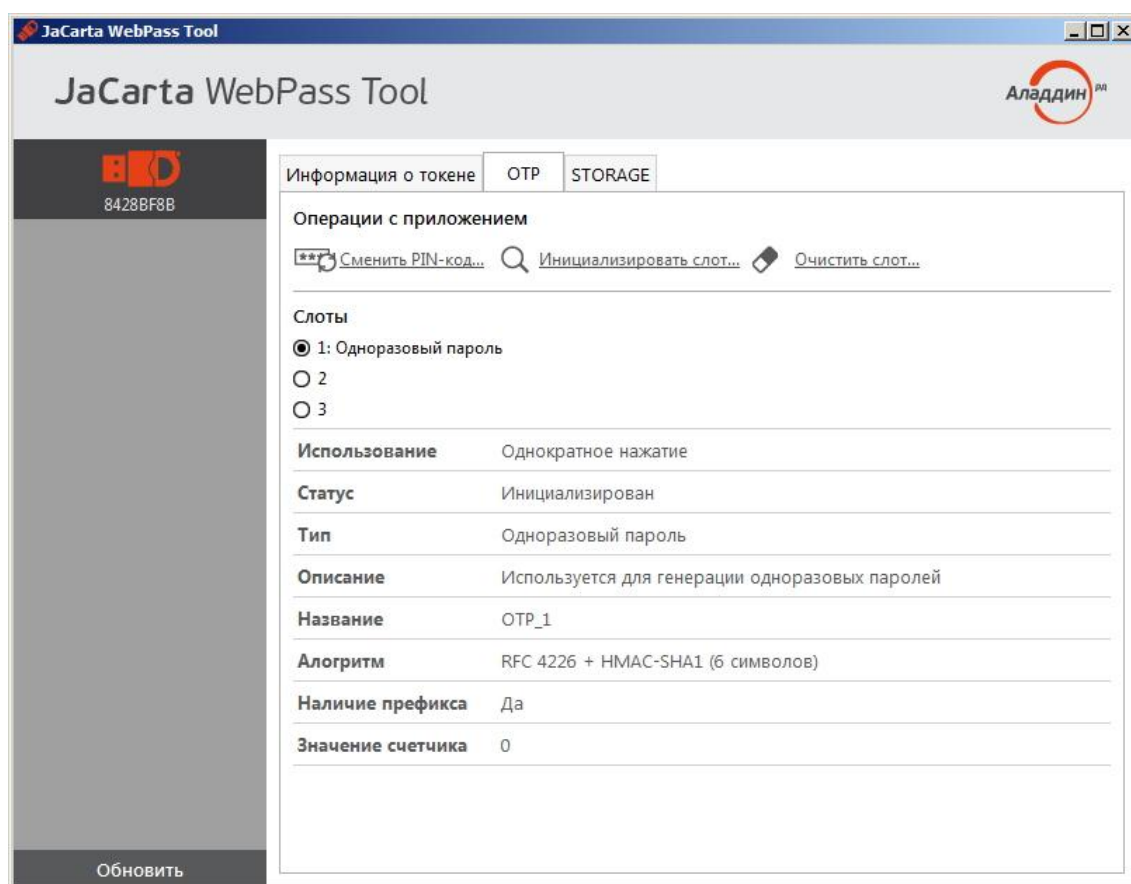



Рисунок 26

Описание отображаемых элементов на вкладке **OTP** приведено в таблице 7.

 В зависимости от типа выбираемого слота (Одноразовый пароль/Интернет адрес/Пароль) и его статуса (Инициализирован/Не инициализирован), некоторые поля, описанные в таблице 7, могут отображаться, либо не отображаться на вкладке **OTP**.



## Таблица 7





Элемент интерфейса	Описание
Сегмент <b>Операции с приложением</b>	<p>В сегменте расположены три кнопки:</p> <ul style="list-style-type: none"> <li> – для смены PIN-кода электронного ключа (подробнее см. подраздел 7.2 Смена PIN-кода администратора);</li> <li> – для запуска мастера инициализации слота электронного ключа (подробнее см. раздел 7. Инициализация слотов);</li> <li> – для очистки заданных при инициализации настроек слота электронного ключа (подробнее см. раздел 9. Очистка слотов).</li> </ul>
Сегмент <b>Слоты:</b>	<p>В сегменте расположены три чек бокса для выбора одного из трех слотов: <b>1</b>, <b>2</b> или <b>3</b>. После выбора слота ниже отображается информация о его характеристиках.</p>
Поле <b>Использование</b>	<p>Способ нажатия на кнопку электронного ключа для использования выбранного слота:</p> <ul style="list-style-type: none"> <li>Слот №1 – однократное нажатие на кнопку;</li> <li>Слот №2 – двойное нажатие на кнопку;</li> <li>Слот №3 – длительное нажатие на кнопку (2-3 секунды).</li> </ul>
Поле <b>Статус</b>	Информация об инициализации выбранного слота или его блокировании.
Поле <b>Тип</b>	<p>Тип выбранного слота (Одноразовый пароль/Интернет адрес/Пароль):</p> <ul style="list-style-type: none"> <li>Одноразовый пароль – слот для генерации одноразовых паролей;</li> <li>Интернет адрес – слот для хранения адреса Web-ресурса;</li> <li>Пароль – слот для генерации и хранения многозначного пароля настраиваемого уровня сложности.</li> </ul>
Поле <b>Описание</b>	Описание предназначения выбранного слота.
Поле <b>Название</b>	Название выбранного слота. Например, тип слота и номер (максимум 32 символа).
Поле <b>Алгоритм</b>	<p>Алгоритм вычисления одноразового пароля.</p> <p> Поддерживаются четыре алгоритма генерации одноразовых паролей (event-based алгоритмы согласно RFC 4226).</p>
Поле <b>Наличие префикса</b>	Сведения о наличии префикса в пароле (Да/Нет).
Поле <b>Значение счетчика</b>	Текущее значение счетчика генераций (число от 0 до $2^{31}$ ).
Поле <b>Критерии качества паролей</b>	<p>Критерии качества паролей, указанные при инициализации слота:</p> <ul style="list-style-type: none"> <li>длина пароля (количество символов от 4 до 160);</li> <li>использовать в пароле английские буквы нижнего регистра (да/нет);</li> <li>использовать в пароле английские буквы верхнего регистра (да/нет);</li> <li>использовать в пароле цифры (да/нет);</li> <li>использовать в пароле спецсимволы (да/нет).</li> </ul>

Таблица 7

### 5.2.3. Вкладка STORAGE



На токенах 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 следующий вид (см. рис. 27).

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).

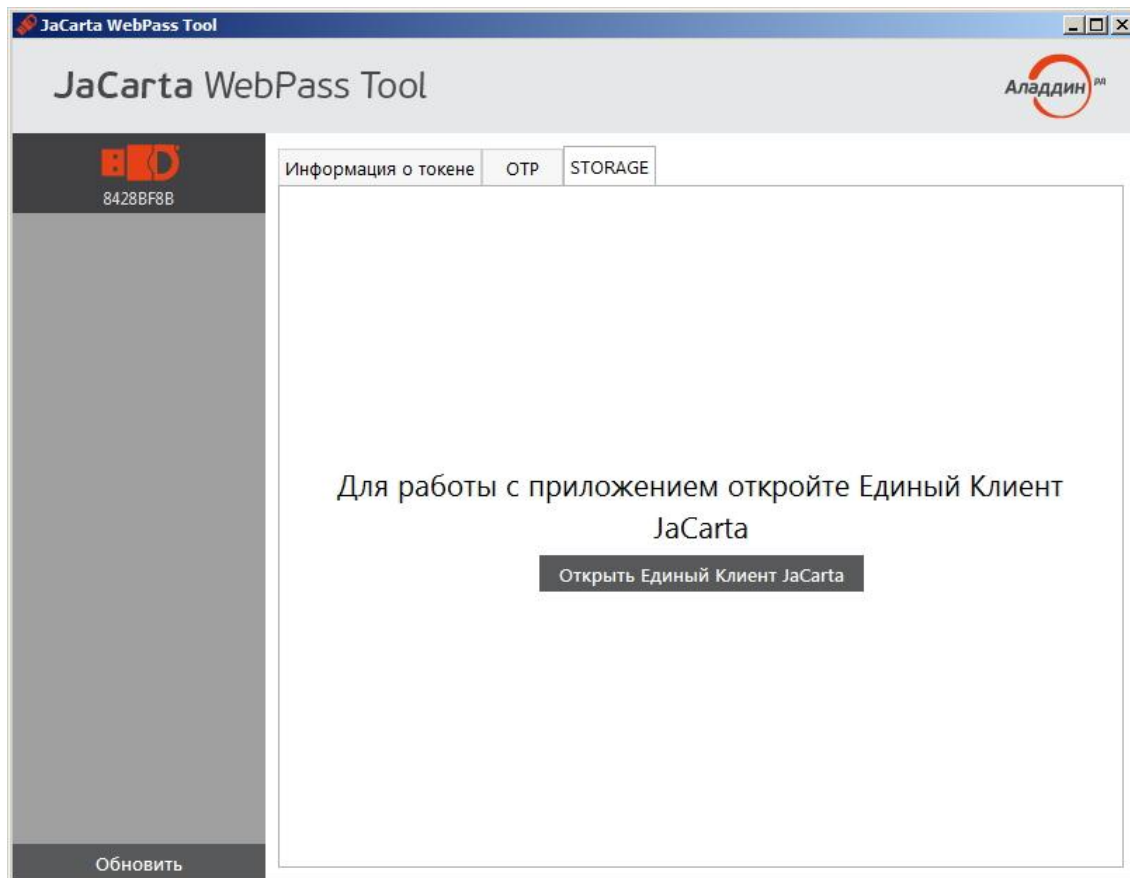


Рисунок 27

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

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

## 5.3. Операции, выполняемые в приложении ОТР

### 5.3.1. Смена PIN-кода администратора

Чтобы сменить PIN-код перейдите на вкладку **ОТР** и нажмите



В появившемся окне (см. рис. 28) введите текущий PIN-код администратора, после чего введите новый PIN-код администратора и подтвердите его еще раз, затем нажмите кнопку **Сменить**.

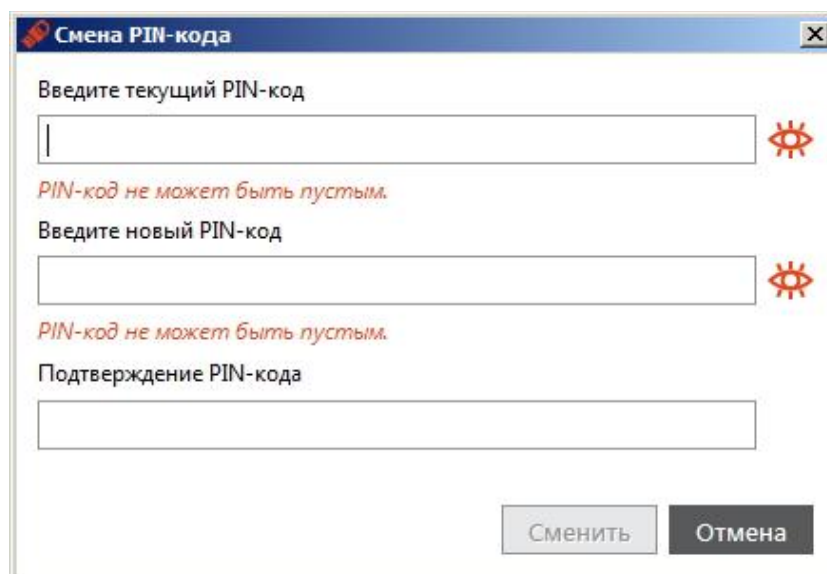


Рисунок 28

### 5.3.2. Инициализация слотов


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

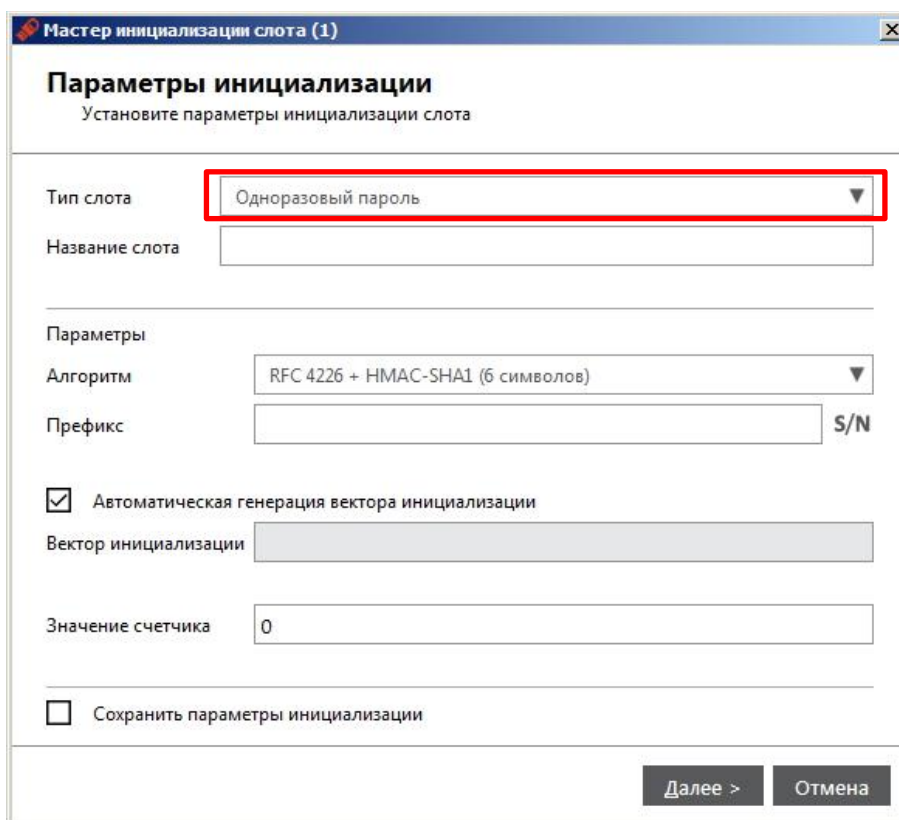


Внимание! Инициализацию слота должен производить администратор. В процессе инициализации слота предыдущие значения параметров слота (если они ранее были записаны в слот) **УДАЛЯЮТСЯ!**

#### 5.3.2.1. Инициализация слота Одноразовый пароль

Для инициализации слота типа **Одноразовый пароль** выполните следующие действия:

1. На вкладке **ОТР** выберите слот, который необходимо инициализировать;
2. Нажмите кнопку  **Инициализировать слот...**;
3. В появившемся окне (см. рис. 29) в поле **Тип слота** выберите: **Одноразовый пароль**;



**Мастер инициализации слота (1)**

**Параметры инициализации**  
Установите параметры инициализации слота

Тип слота: **Одноразовый пароль**

Название слота:

Параметры

Алгоритм: RFC 4226 + HMAC-SHA1 (6 символов)

Префикс:  S/N

☒ Автоматическая генерация вектора инициализации

Вектор инициализации:

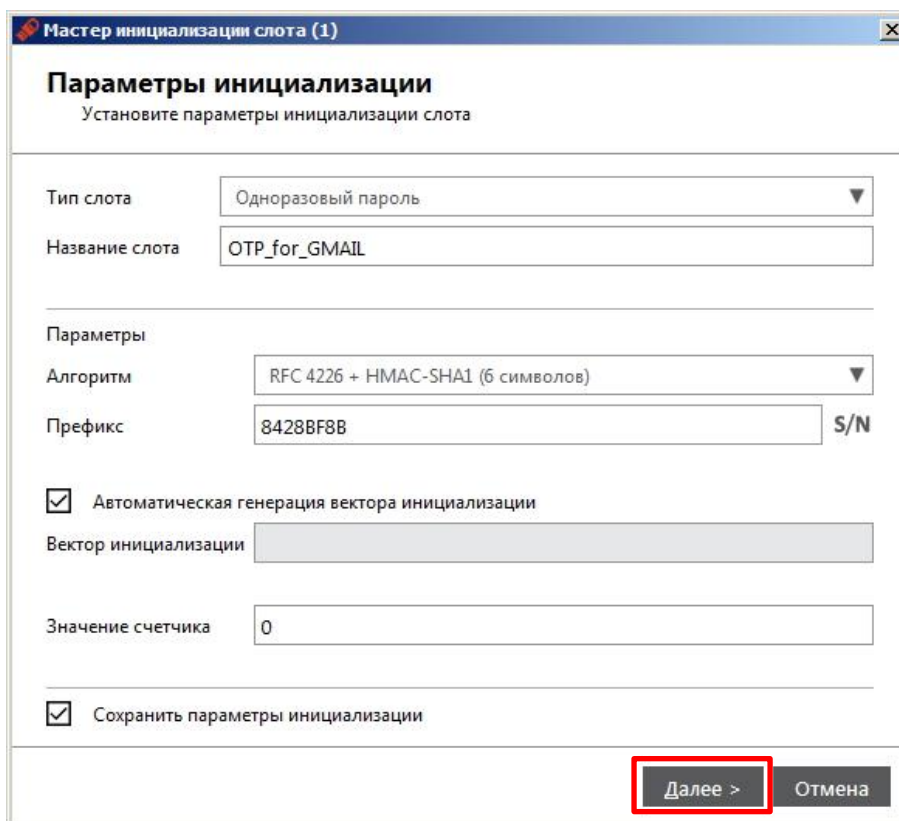
Значение счетчика:

☐ Сохранить параметры инициализации

**Далее >** **Отмена**

Рисунок 29

4. В поле **Название слота** введите название (например: OTP\_1 или любой другой, см. рис. 30);



**Мастер инициализации слота (1)**

**Параметры инициализации**  
Установите параметры инициализации слота

Тип слота: **Одноразовый пароль**

Название слота: **OTP\_for\_GMAIL**

Параметры

Алгоритм: RFC 4226 + HMAC-SHA1 (6 символов)

Префикс: **8428BF8B** S/N

☒ Автоматическая генерация вектора инициализации

Вектор инициализации:


Значение счетчика:


☒ Сохранить параметры инициализации

**Далее >** **Отмена**


Рисунок 30

5. 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;
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. рис. 31) 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 токена 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**;

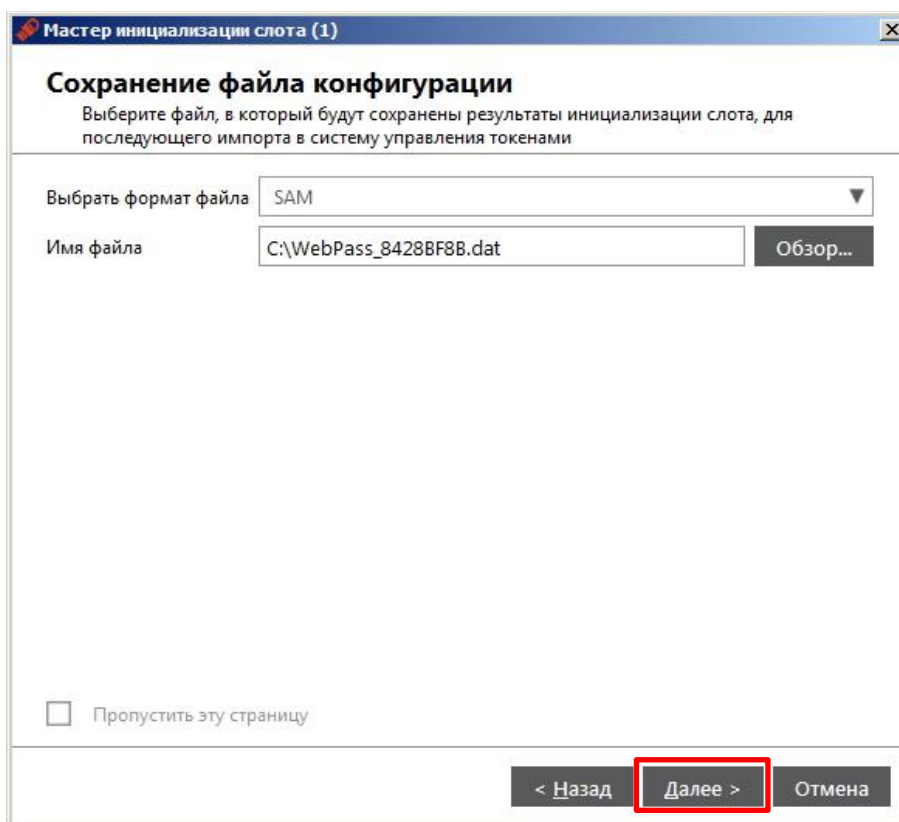


Рисунок 31

12. Если конфигурационный файл создавать и сохранять не требуется, то выберите опцию **Пропустить эту страницу**;
13. Нажмите **Далее >**;
14. В появившемся окне (см. рис. 32) введите **PIN-код** администратора (дополнительную информацию см. в разделе PIN-код администратора), после чего нажмите кнопку **Выполнить**;

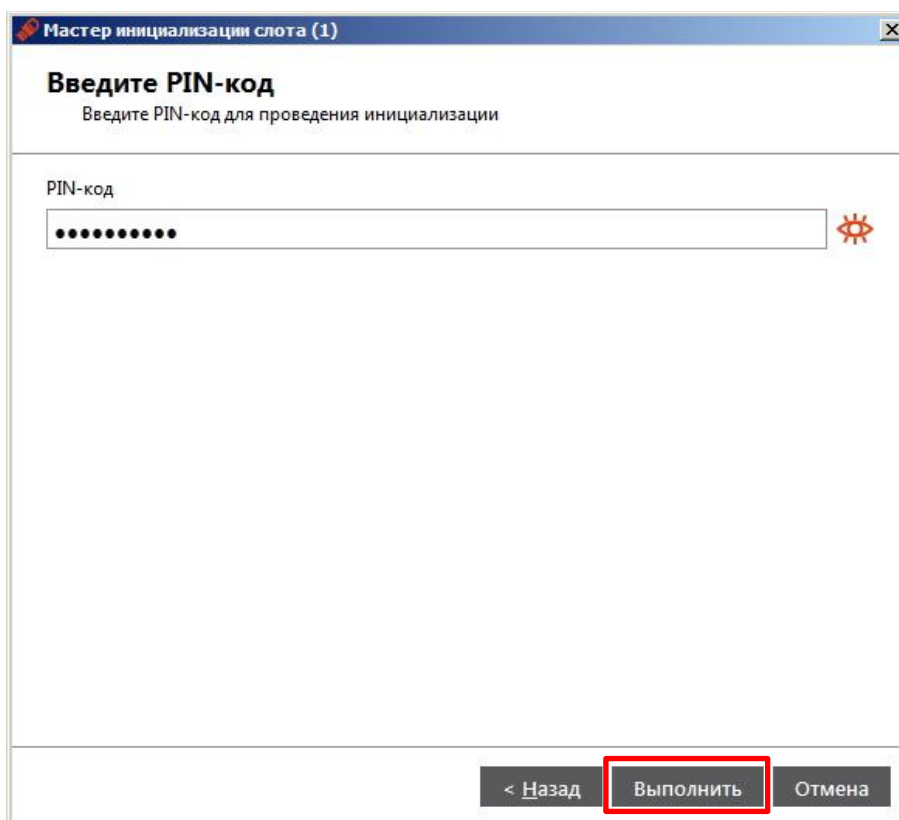


Рисунок 32

15. Для перехода в папку с сохраненным конфигурационным файлом выберите опцию **Выбрать файлы при помощи программы проводник** (см. рис. 33) тогда после нажатия кнопки **Завершить** откроется папка с сохраненным конфигурационным файлом;

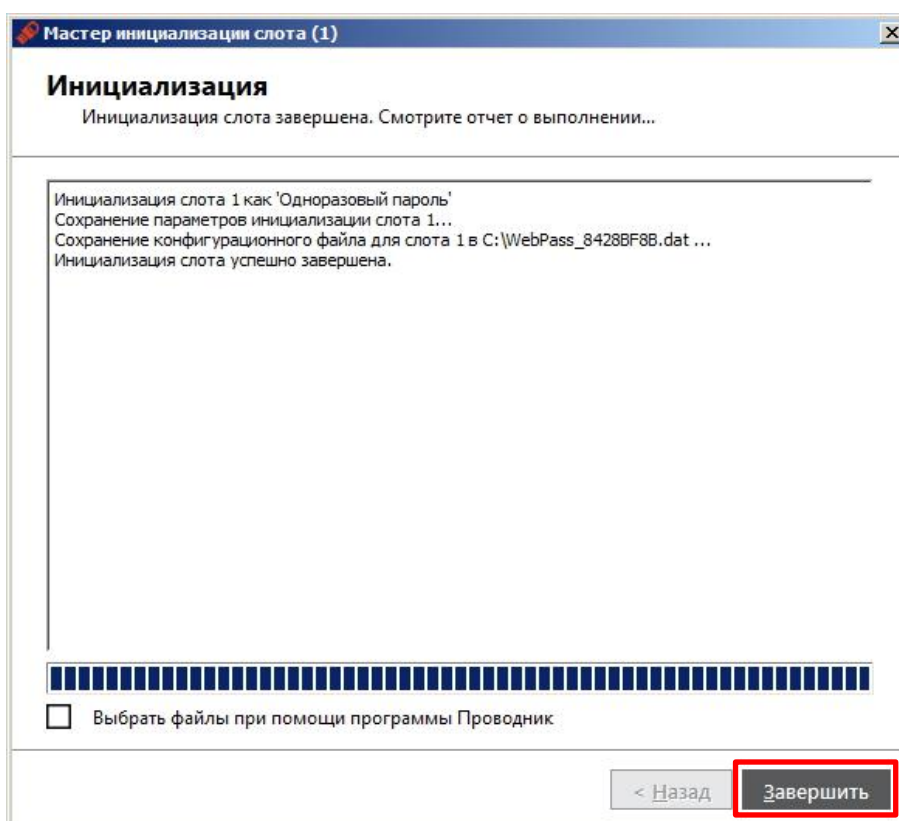



Рисунок 33

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 **ОТР** выберите слот, который необходимо инициализировать;
2. Нажмите кнопку  **Инициализировать слот...**;
3. В появившемся окне (см. рис. 34) в поле **Тип слота** выберите: **Интернет адрес**;

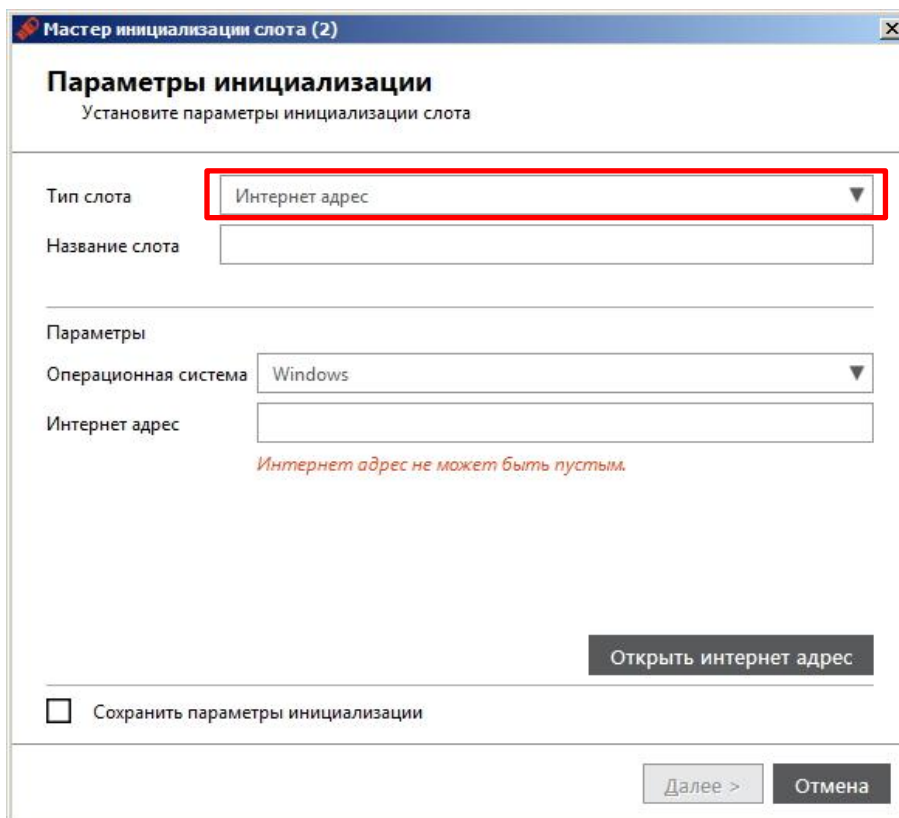


Рисунок 34

4. В поле **Название слота** введите название (например: URL\_1 или любой другой, см. рис. 35);
5. В поле **Операционная система** выберите тип операционной системы: Windows/Mac OS/Linux;
6. 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**.

7. Выберите опцию **Сохранить параметры инициализации** (если необходимо сохранить настройки инициализации для последующих инициализаций данного слота);



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

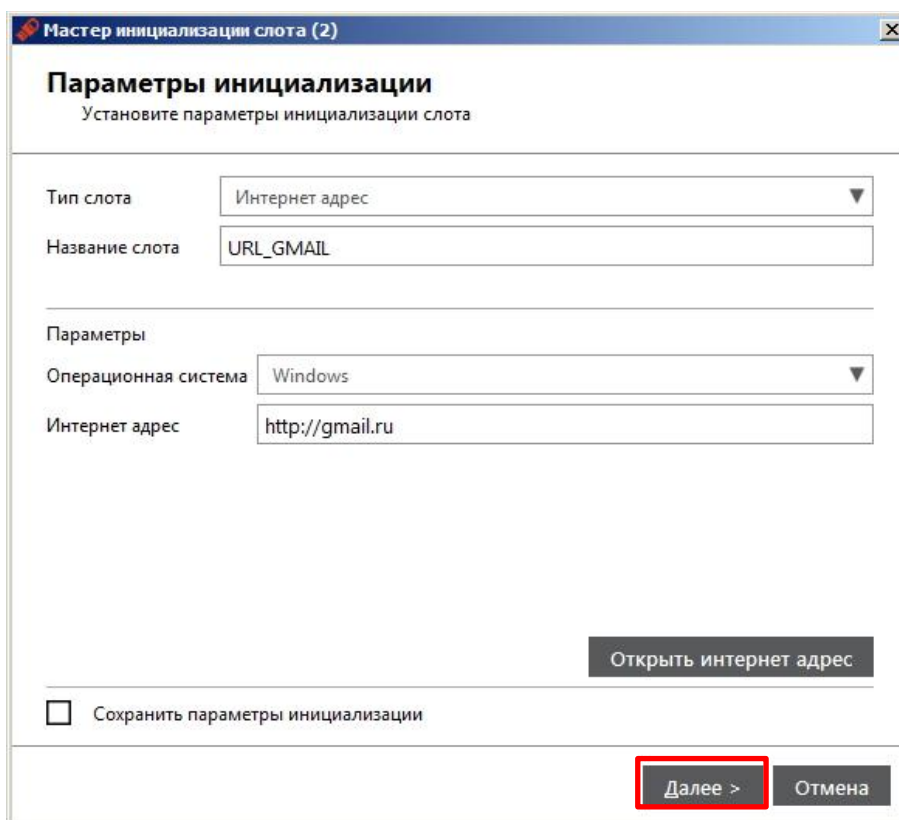


Рисунок 35

8. Нажмите **Далее >** и в появившемся окне (см. рис. 36) введите **PIN-код** администратора (дополнительную информацию см. в разделе PIN-код администратора), после чего нажмите кнопку **Выполнить**.

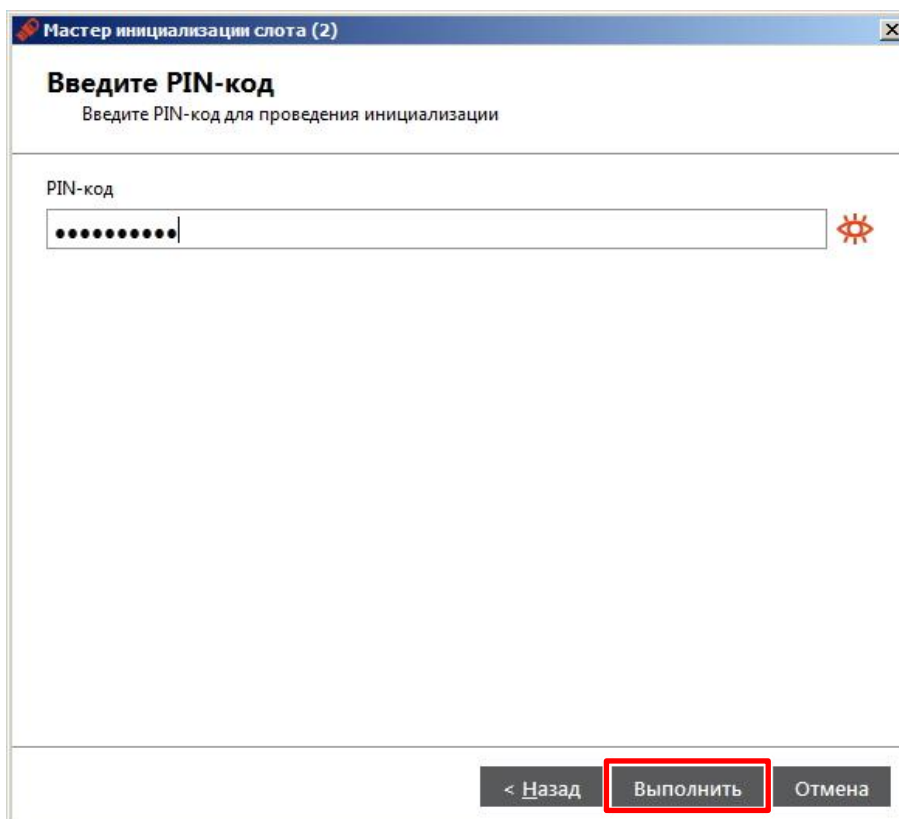


Рисунок 36



9. В появившемся окне (см. рис. 37) нажмите **Завершить**.

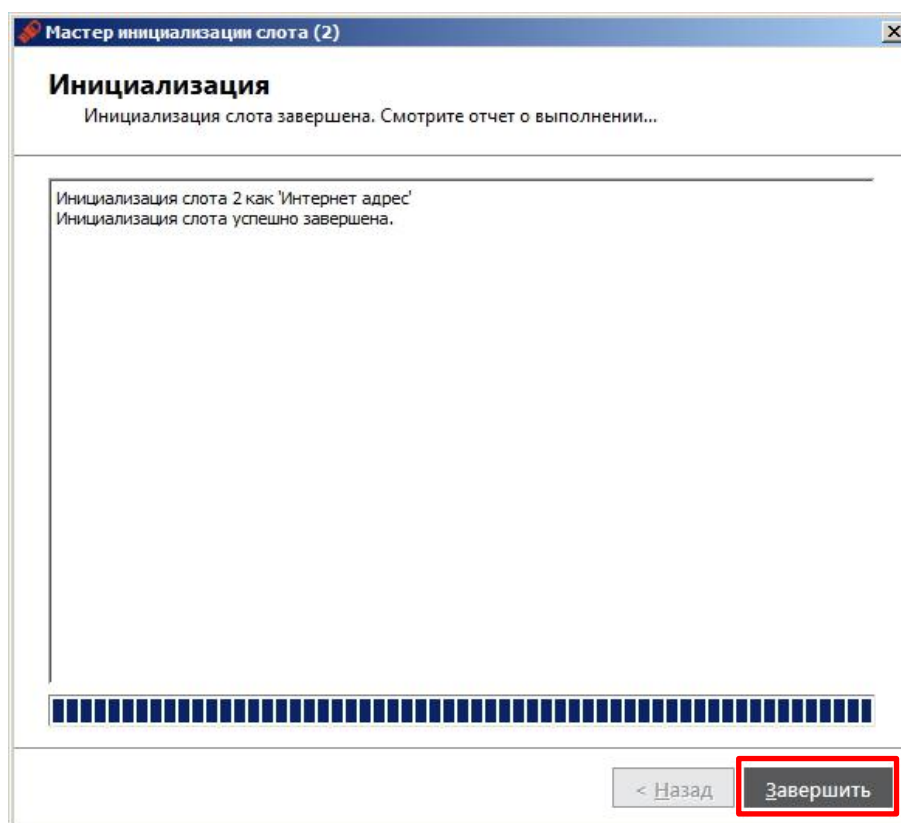

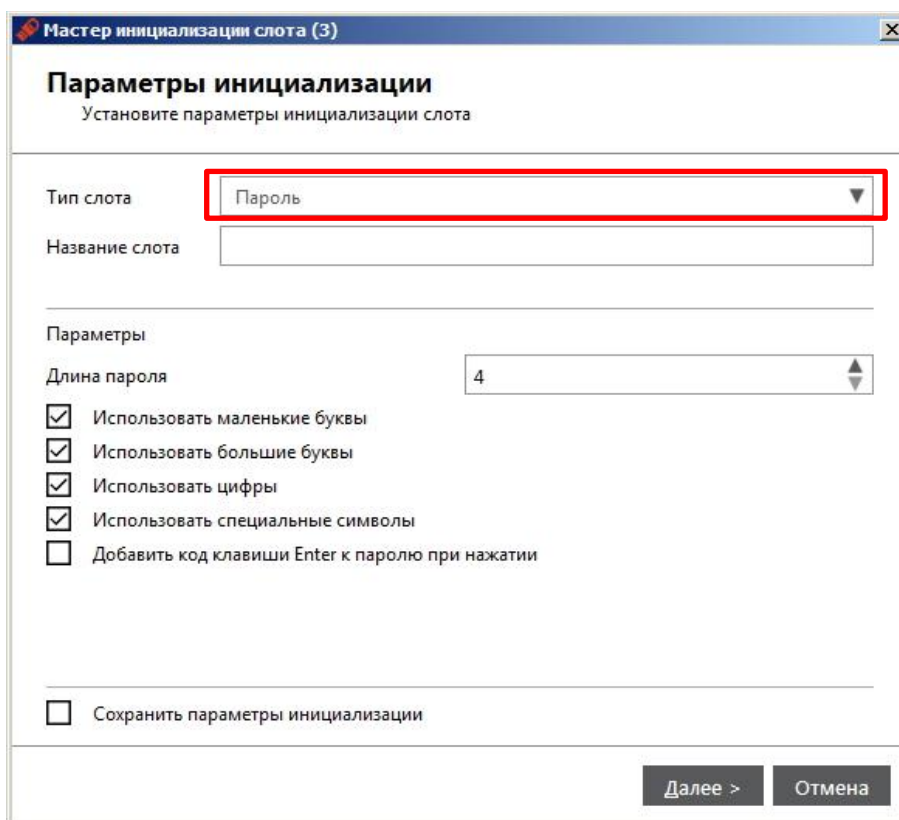


Рисунок 37

### 5.3.2.3. Инициализация слота Пароль

Для инициализации слота типа **Пароль** выполните следующие действия:

1. На вкладке **ОТР** выберите слот, который необходимо инициализировать;
2. Нажмите кнопку  **Инициализировать слот...**;
3. В появившемся окне (см. рис. 38) в поле **Тип слота** выберите: **Пароль**;
4. В поле **Название слота** введите название (например: PASS\_1 или любой другой, см. рис. 39);



**Мастер инициализации слота (3)**

**Параметры инициализации**  
Установите параметры инициализации слота

Тип слота: Пароль

Название слота:

Параметры

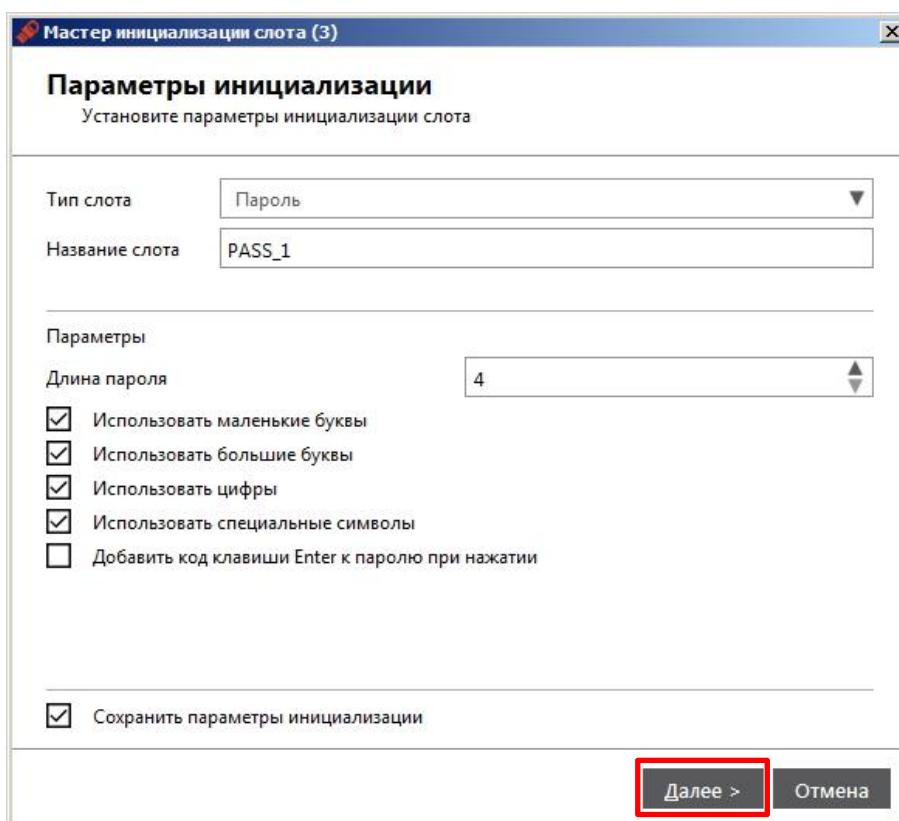
Длина пароля:

- ☒ Использовать маленькие буквы
- ☒ Использовать большие буквы
- ☒ Использовать цифры
- ☒ Использовать специальные символы
- ☐ Добавить код клавиши Enter к паролю при нажатии

☐ Сохранить параметры инициализации

Далее > Отмена

Рисунок 38



**Мастер инициализации слота (3)**

**Параметры инициализации**  
Установите параметры инициализации слота

Тип слота:

Название слота:

Параметры

Длина пароля:

- ☒ Использовать маленькие буквы
- ☒ Использовать большие буквы
- ☒ Использовать цифры
- ☒ Использовать специальные символы
- ☐ Добавить код клавиши Enter к паролю при нажатии

☒ Сохранить параметры инициализации

Далее > Отмена

Рисунок 39

5. 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**;
6. 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.

7. Нажмите **Далее >** и в появившемся окне (см. рис. 40) введите **PIN-код** (дополнительную информацию см. в разделе 7 PIN-код), после чего нажмите кнопку **Выполнить**.

Рисунок 40

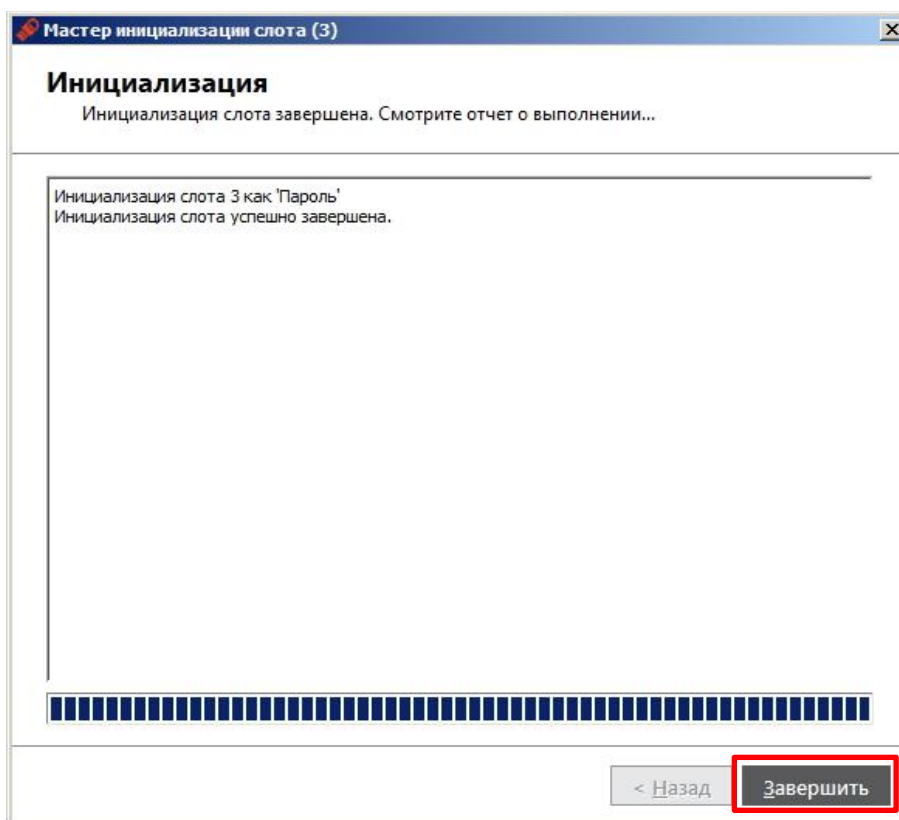



Рисунок 41

8. В появившемся окне (см. рис. 41) нажмите **Завершить**.

### 5.3.3. Очистка слотов

Для очистки слота выполните следующие действия:

1. На вкладке **ОТР** выберите слот, который необходимо очистить;
2. Нажмите кнопку  **Очистить слот...** ;
3. В появившемся окне (см. рис. 42) введите **PIN-код** (дополнительную информацию см. в разделе 7 PIN-код), после чего нажмите кнопку **Очистить**;
4. В появившемся окне (см. рис. 43) нажмите **ОК** для завершения.

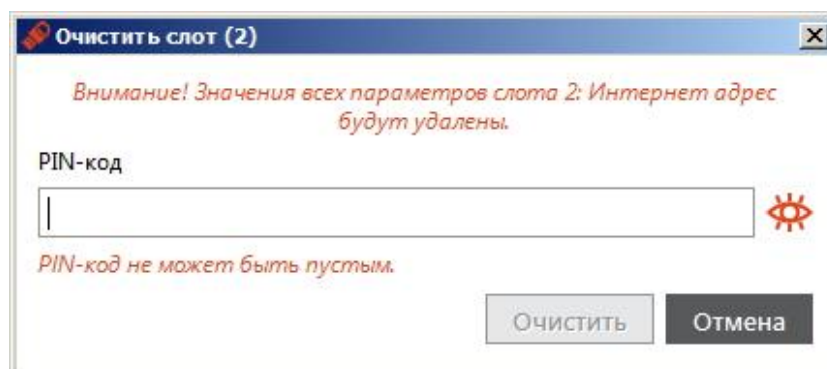


Рисунок 42

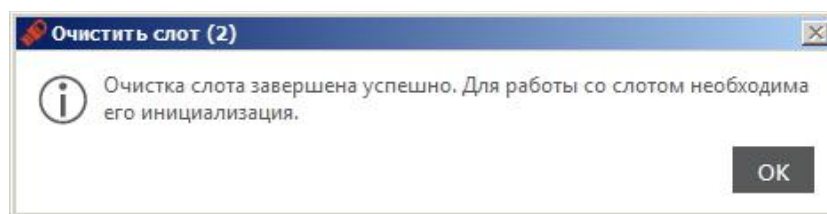


Рисунок 43

## 6. Порядок работы с электронными ключами JaCarta WebPass

---

Перед использованием токена 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 токена JaCarta WebPass



#### Внимание!

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



Для регистрации токена 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 токена JaCarta WebPass

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

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

- слот №1;
- слот №2;
- слот №3.

Каждый из трех слотов токена 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 токена 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 токеном 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: Неслота – 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 токена 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 токена 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.



# Сокращения и аббревиатуры

---

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

# Контакты, техническая поддержка

---

## Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 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](mailto:aladdin@aladdin-rd.ru) (общий).

Web: [www.aladdin-rd.ru](http://www.aladdin-rd.ru)

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

## Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

**[www.aladdin-rd.ru/support/index.php](http://www.aladdin-rd.ru/support/index.php)**

Для оперативного решения вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

# Регистрация изменений

---

Версия	Изменения
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	JS-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.



---

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12  
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14  
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011  
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00073 от 20.08.13  
Microsoft Silver OEM Hardware Partner, Apple Developer, Oracle Gold Partner

© ЗАО «Аладдин Р. Д.», 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) Web: [www.aladdin-rd.ru](http://www.aladdin-rd.ru)