



JaCarta АРМ УЦ

Руководство администратора

Версия документа: 1.1

Редакция от: 4 мая 2017 г.

Листов: 59

Аннотация

Данное Руководство администратора (далее – Руководство) предназначено для персонала, осуществляющего установку, эксплуатацию и настройку программного обеспечения JaCarta АРМ УЦ.

В настоящем Руководстве приведены общие сведения, системные требования, режимы работы, порядок и содержание действий по установке и удалению JaCarta АРМ УЦ, сведения по изменению настроек, созданию запроса на сертификат и осуществления записи сертификата на токен.

Руководство рассчитано на пользователей, обладающих начальными навыками работы на компьютере, знакомых с работой в операционной системе Windows и сети Интернет.

Вопросы или пожелания по содержанию настоящего документа направляйте по адресу:

techwriters@aladdin-rd.ru.

Будем благодарны за конструктивные замечания и ответим на возникшие вопросы. За технической поддержкой обращайтесь на веб-сайт ЗАО «Аладдин Р.Д.» по адресу:

<http://www.aladdin-rd.ru/support>.

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, Mac OS, 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

1. ОБЩИЕ СВЕДЕНИЯ	4
1.1. Описание пакетов установки	4
1.2. Системные требования	4
1.3. Поддерживаемые модели электронных ключей	5
2. УСТАНОВКА	6
3. УДАЛЕНИЕ	11
4. НАСТРОЙКА	15
4.1. Режимы работы	15
4.2. Настройка JaCarta АРМ УЦ для создания запросов в автономном режиме	15
4.3. Настройка для создания запросов в автоматическом режиме	22
4.3.1. Создание соединения с Центром Регистрации	22
4.3.2. Настройка параметров соединения с Центром Регистрации	26
5. ВЫПУСК СЕРТИФИКАТА	33
5.1. Выпуск сертификата в автономном режиме	33
5.1.1. Создание запроса на сертификат	33
5.1.2. Запись сертификата в память электронного ключа	40
5.2. Выпуск сертификата в автоматическом режиме	44
5.2.1. Создание запроса на сертификат	44
5.2.2. Запись сертификата в память электронного ключа	51
5.3. Обновление сертификата для существующего пользователя	53
Контакты, техническая поддержка	57
Регистрация изменений	58

1. ОБЩИЕ СВЕДЕНИЯ

JaCarta APM УЦ представляет собой компонент программного комплекса Единый Клиент JaCarta. JaCarta APM УЦ позволяет генерировать ключевые пары с использованием встроенных криптографических возможностей электронных ключей JaCarta ГОСТ и eToken ГОСТ, а также формировать запросы к удостоверяющему центру на получение сертификата открытого ключа и записывать полученные сертификаты в память электронного ключа.

1.1. Описание пакетов установки

JaCarta APM УЦ входит в состав программного комплекса Единый Клиент JaCarta и не имеет отдельного пакета установки. Установка JaCarta APM УЦ происходит с помощью дистрибутива Единого Клиента JaCarta. Дистрибутив Единого Клиента JaCarta включает пакеты установки, приведенные в Таблице 1.

Таблица 1

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 1

1.2. Системные требования



Внимание! Перед установкой JaCarta APM УЦ убедитесь в том, что компьютер соответствует минимальным требованиям. Системные требования приведены в Таблице 2.

Таблица 2

Требование	Содержание
Поддерживаемые операционные системы	<ul style="list-style-type: none">• Microsoft Windows 8.1 Update 1 (32/64-бит)• Microsoft Windows 8 (32/64-бит)• Microsoft Windows 7 SP1 (32/64-бит)• Microsoft Windows XP SP3 (32-бит)• Microsoft Windows XP SP2 (64-бит)• Microsoft Windows Server 2012 (64-бит)• Microsoft Windows Server 2008 R2 SP1 (64-бит)• Microsoft Windows Server 2003 SP2 (32-бит)
Поддерживаемые модели электронных ключей	<ul style="list-style-type: none">• JaCarta ГОСТ• JaCarta ГОСТ/Flash• JaCarta PKI/ГОСТ• JaCarta PKI/ГОСТ/Flash• eToken ГОСТ
Поддерживаемые УЦ	<ul style="list-style-type: none">• Автономный режим:<ul style="list-style-type: none">• Любой УЦ, поддерживающий PKCS #10 запросы• Автоматический режим:<ul style="list-style-type: none">• КриптоПро УЦ 1.5
Необходимые аппаратные средства	<p>USB-порт (для токенов). Для смарт-карт необходимо наличие подключённого считывателя смарт-карт. Для электронных ключей в форм-факторе microSD можно использовать следующее оборудование:</p> <ul style="list-style-type: none">• Разъём microSD• Разъём SD через переходник microSD-to-SD• USB-порт через переходник microSD-to-USB

Требование	Содержание
	Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование: <ul style="list-style-type: none">• USB-порт через переходник microUSB-to-USB
Рекомендуемое разрешение экрана	Для корректного отображения интерфейса JaCarta АРМ УЦ рекомендуется установить разрешение монитора не ниже 1024x768 (минимальное разрешение: 800 x 600)
Дополнительное ПО	<ul style="list-style-type: none">• Microsoft .NET.Framework 3.5• КриптоПро CSP версии 3.6/3.6 R2 и выше• Единый Клиент JaCarta версии 2.8 и выше
Другие требования	Для работы в автоматическом режиме (режиме online) необходимо: <ul style="list-style-type: none">• Доступ к УЦ КриптоПРО• Установленные сертификаты:<ul style="list-style-type: none">• Корневой сертификат УЦ КриптоПРО (Доверенные корневые центры сертификации)• Сертификат Оператора и/или Администратора, который будет использован для аутентификации в Центре Регистрации (Личное хранилище сертификатов)

Таблица 2

1.3.Поддерживаемые модели электронных ключей

1. JaCarta ГОСТ, JaCarta ГОСТ/Flash, JaCarta PKI/ГОСТ, JaCarta PKI/ГОСТ/Flash, eToken ГОСТ.
2. Модели электронных ключей, поддерживаемые КриптоПро CSP версии 3.6/3.6 R2 и выше.

2. УСТАНОВКА



Внимание! Перед установкой JaCarta АРМ УЦ убедитесь в том, что компьютер соответствует требованиям, приведенным в Таблице 2.

Чтобы установить JaCarta АРМ УЦ выполните следующие действия:

1. Запустите файл установки (см. п. 1.1). Отобразится следующее окно (см. Рис. 1).
Окно приветствия мастера установки Единого Клиента JaCarta

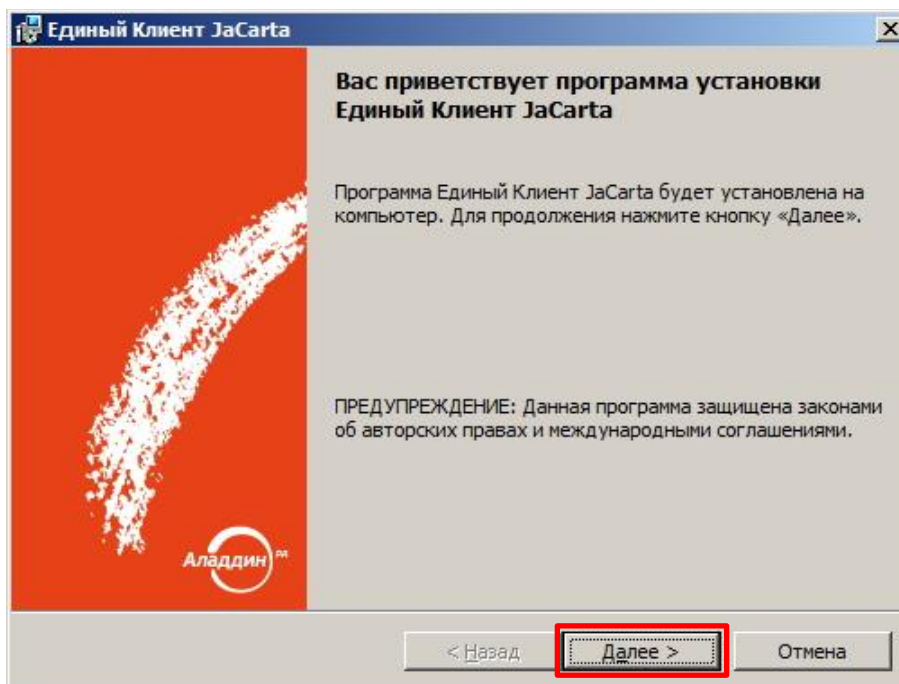


Рисунок 1

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

Окно лицензионного соглашения

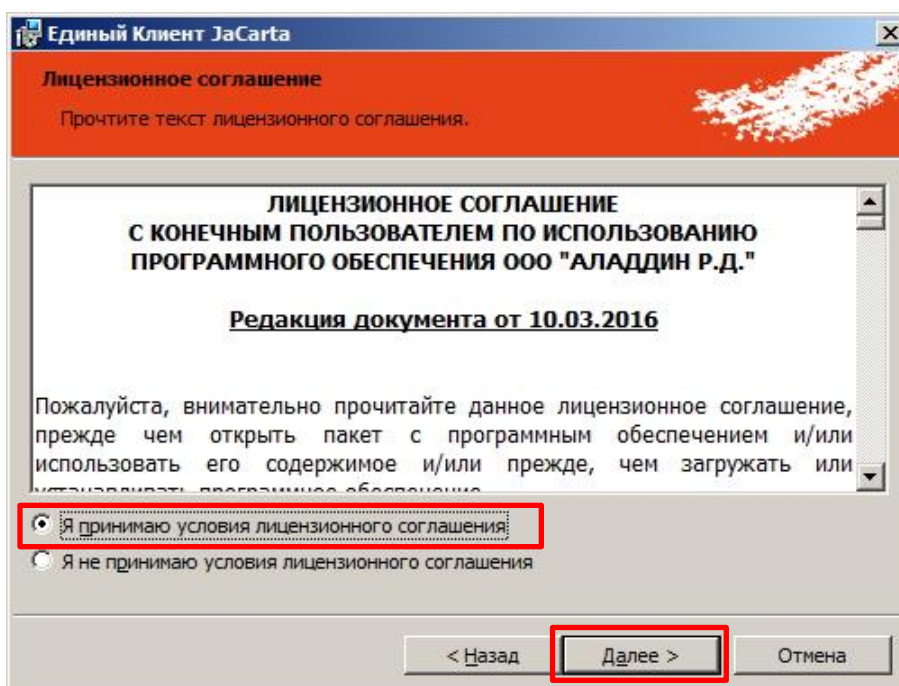


Рисунок 2

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. 3).

Окно выбора пути и вида установки Единого Клиента JaCarta

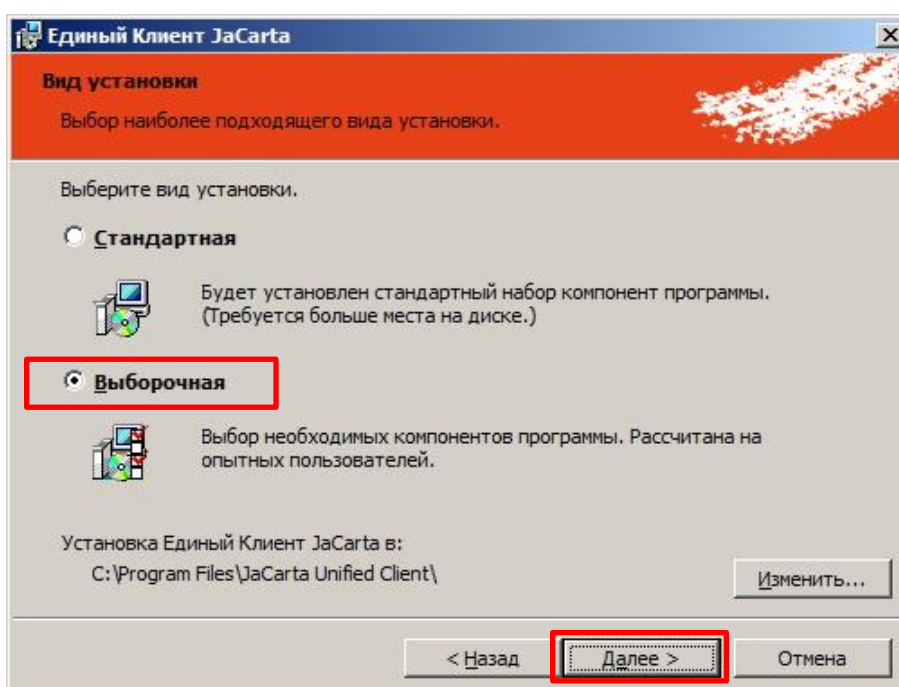



Рисунок 3

5. При необходимости воспользуйтесь кнопкой **Изменить...**, чтобы изменить путь установки Единого Клиента JaCarta.
6. Нажмите **Далее >** отобразится окно (см. Рис. 4).

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

Выборочная установка компонент Единого Клиента JaCarta

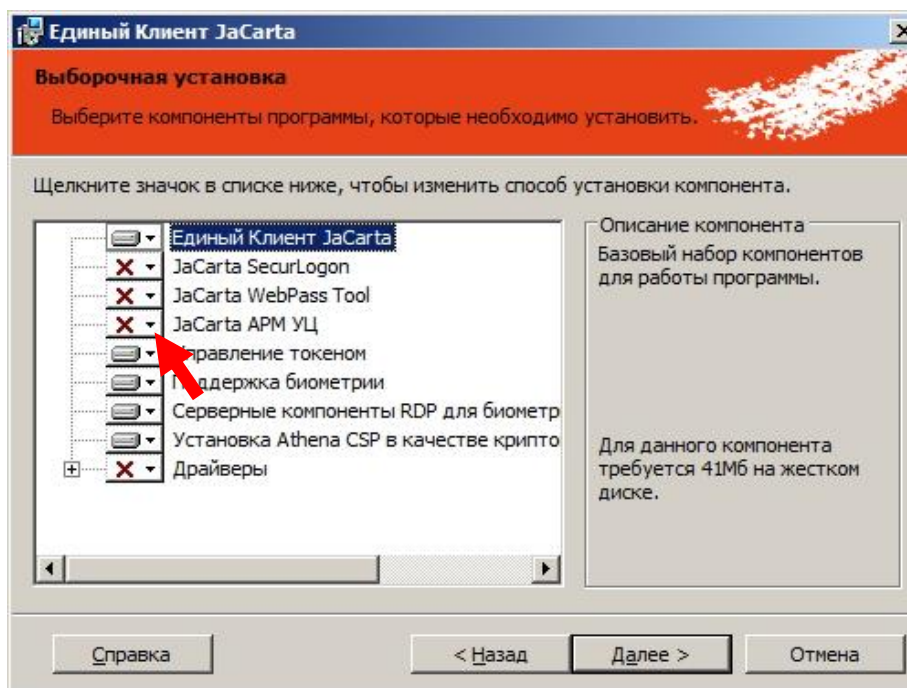



Рисунок 4

7. Для установки компонента JaCarta APM УЦ в списке компонентов строке с названием JaCarta APM УЦ нажмите на значок  и в появившемся контекстном меню (см. Рис. 5) выберите необходимую опцию установки.

Опции установки

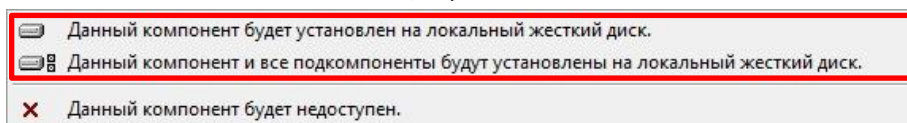


Рисунок 5

После выбора для установки компонента JaCarta APM УЦ окно выборочной установки будет выглядеть следующим образом (см. Рис. 6).

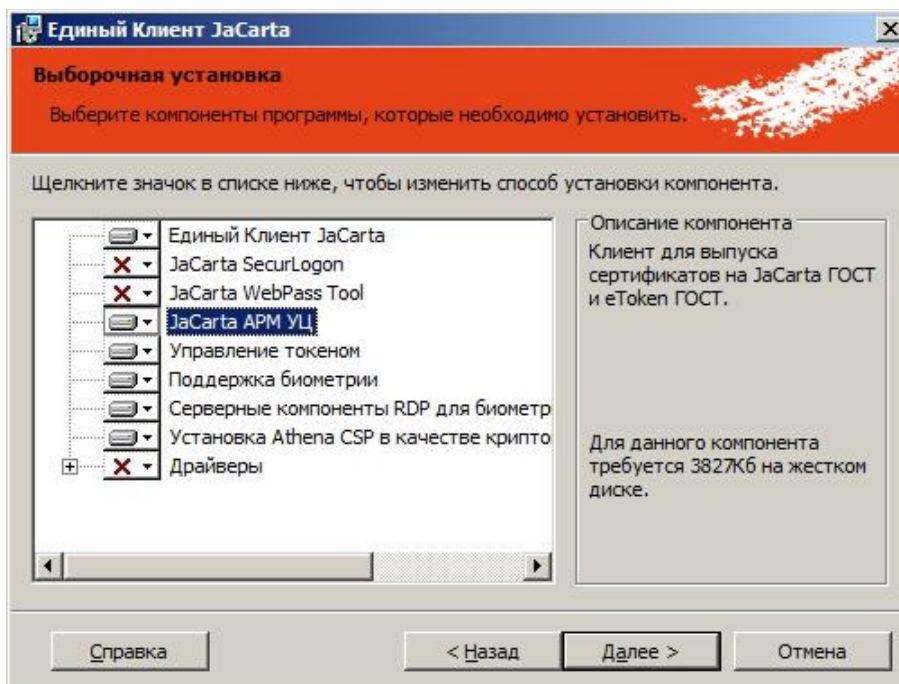


Рисунок 6

8. Нажмите **Далее >** отобразится окно (см. Рис. 7).

Выбор способа автоматического обновления при выборочной установке Единого Клиента JaCarta

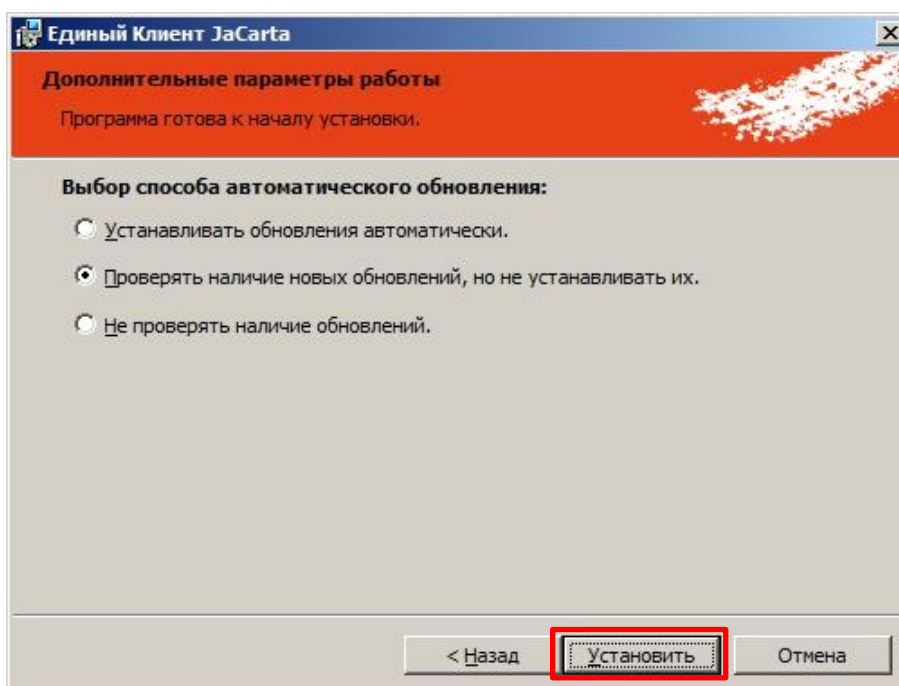


Рисунок 7

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

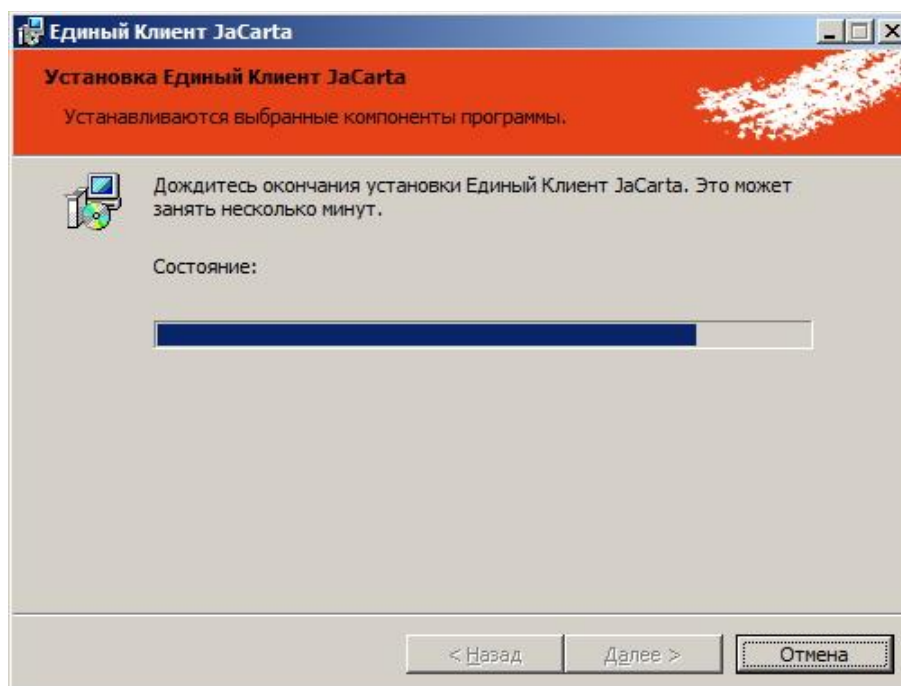


Рисунок 8

10. По завершении установки отобразится следующее окно (см. Рис. 9).

Окно завершения установки Единого Клиента JaCarta

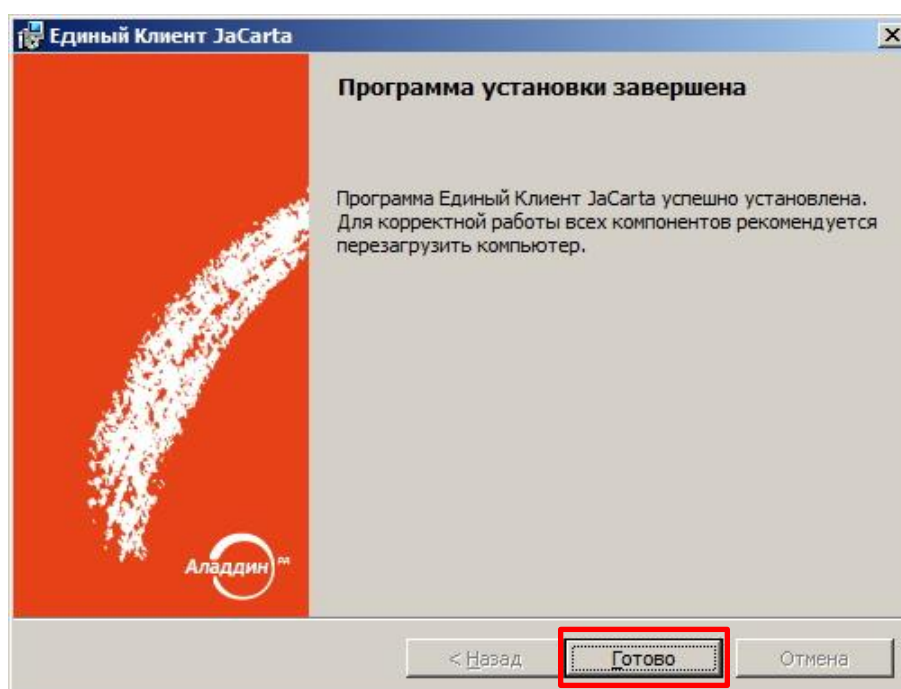


Рисунок 9

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].

3. УДАЛЕНИЕ

Для того, чтобы удалить компонент JaCarta АРМ УЦ 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. 10).

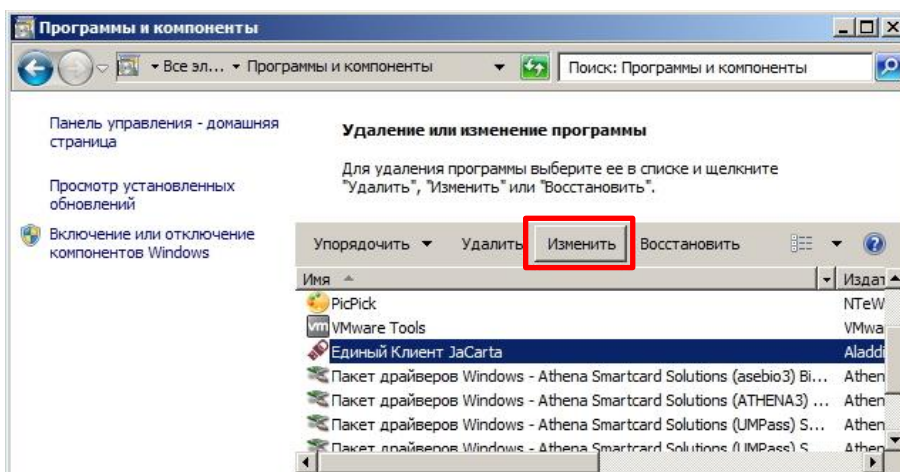


Рисунок 10

3. В появившемся окне (см. Рис. 11) нажмите **Далее**.

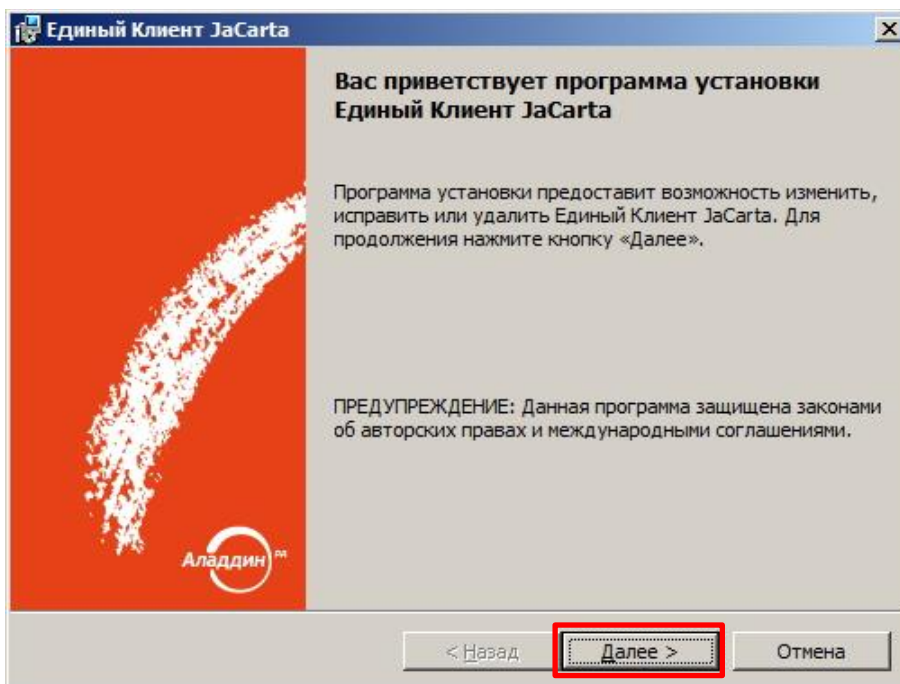


Рисунок 11

4. В появившемся окне (см. Рис. 12) выберите опцию **Изменить** и нажмите **Далее**.

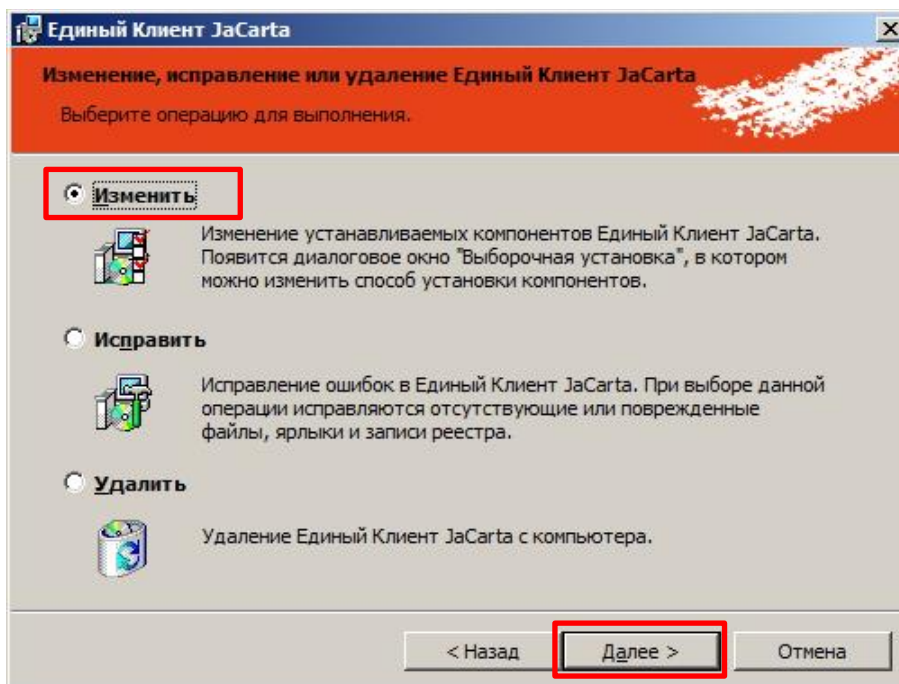



Рисунок 12

5. Для удаления компонента JaCarta WebPass Tool в списке компонентов строке с названием **JaCarta WebPassTool** нажмите на значок  (см. Рис. 13) и в появившемся контекстном меню (см. Рис. 14) выберите необходимую опцию установки.

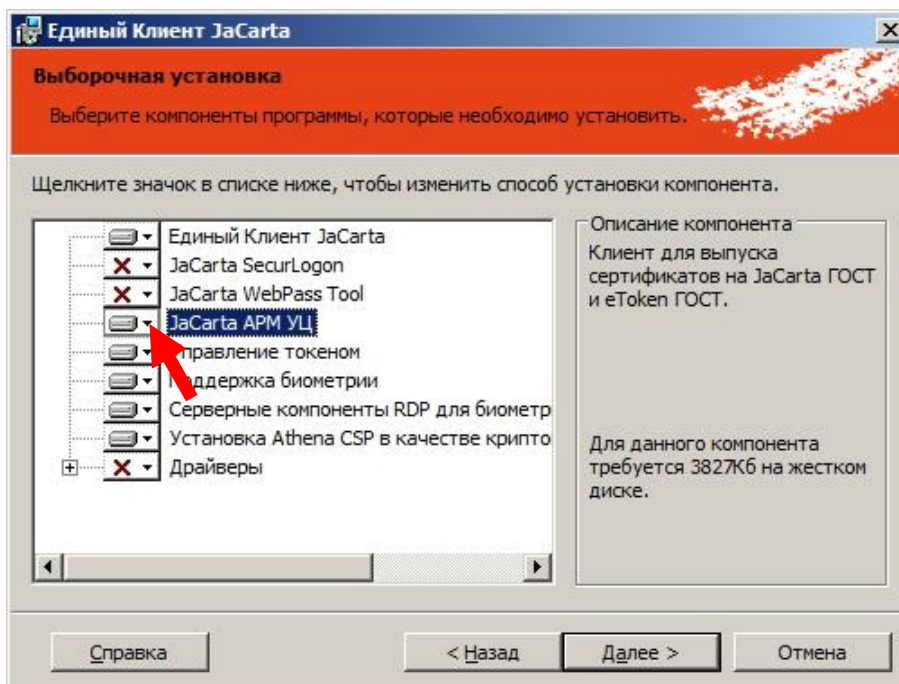


Рисунок 13

Опции установки

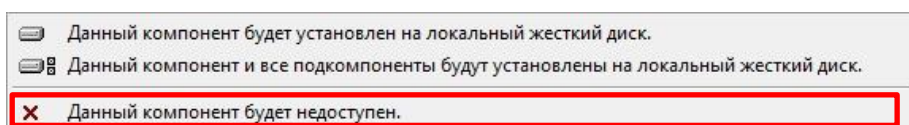


Рисунок 14

После выбора для удаления компонента JaCarta WebPass Tool окно выборочной установки будет выглядеть следующим образом (см. Рис. 15).

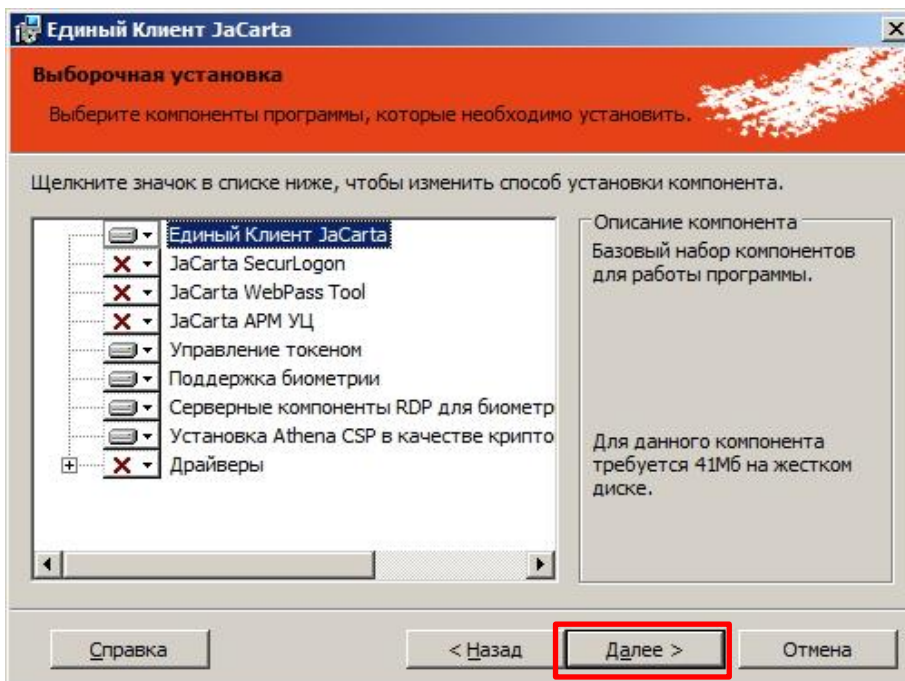


Рисунок 15

6. Нажмите **Далее** и в появившемся окне (см. Рис. 16) выберите способ автоматического обновления, нажмите **Изменить** и дождитесь окончания удаления компонента.

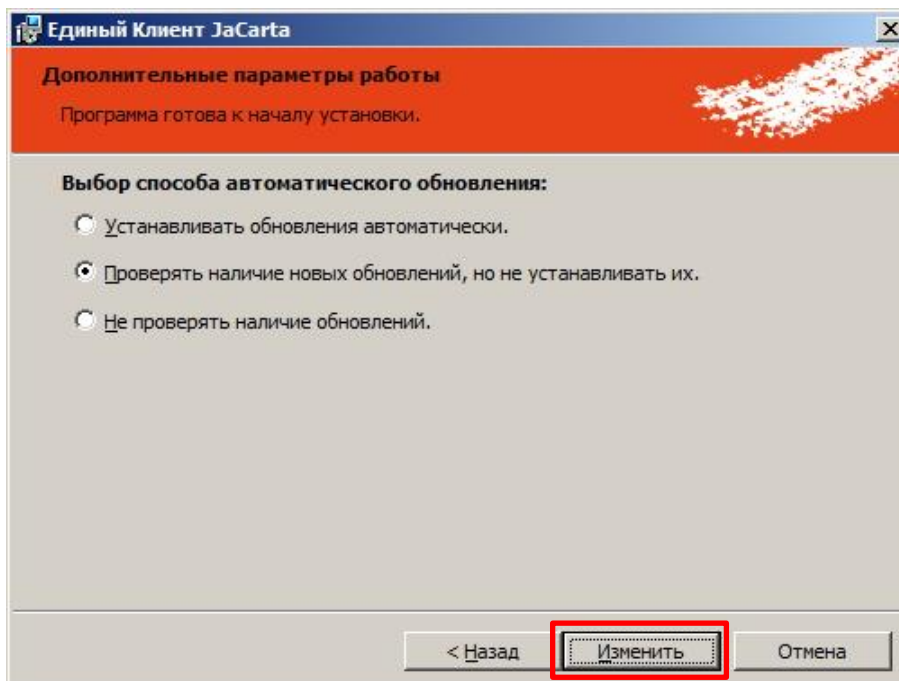


Рисунок 16

После завершения внесения изменений программой установки отобразится следующее окно (см. Рис. 17).

7. Нажмите **Готово**.

8. Перезагрузите компьютер, если отобразится соответствующее предупреждение.

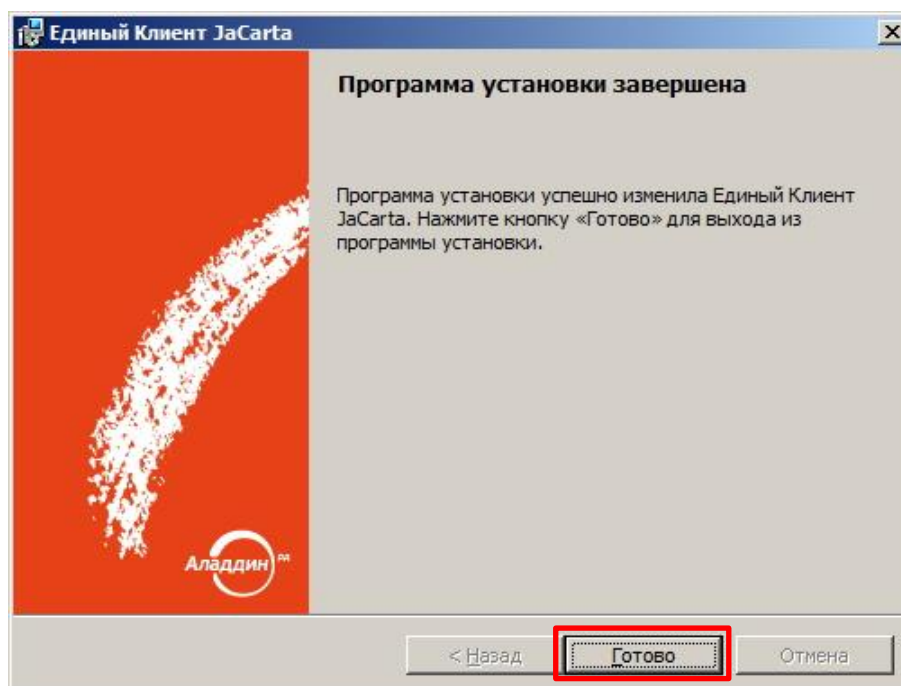


Рисунок 17

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

4. НАСТРОЙКА

4.1. Режимы работы

JaCarta APM УЦ позволяет создавать запросы и записывать сертификаты в память электронных ключей как в автономном, так и в автоматическом режиме.

Автономный режим (режим **offline**) не требует связи с центром регистрации (ЦР) и предназначен для создания запроса на сертификат в случаях отсутствия соединения с ЦР. В этом случае запрос сохраняется на носитель информации (или отправляется в ЦР по электронной почте), доставляется в ЦР для выпуска сертификата, после чего выпущенный сертификат на носителе информации (либо по электронной почте) доставляется пользователю для записи на токен.

Автоматический режим (режим **online**) предусматривает создание соединения с ЦР, создание запроса на сертификат, регистрация запроса в ЦР и получение пользователем готового сертификата.

4.2. Настройка JaCarta APM УЦ для создания запросов в автономном режиме

Чтобы настроить параметры выпуска сертификатов в автономном режиме, выполните следующие действия.

1. Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ (см. Рис. 18).

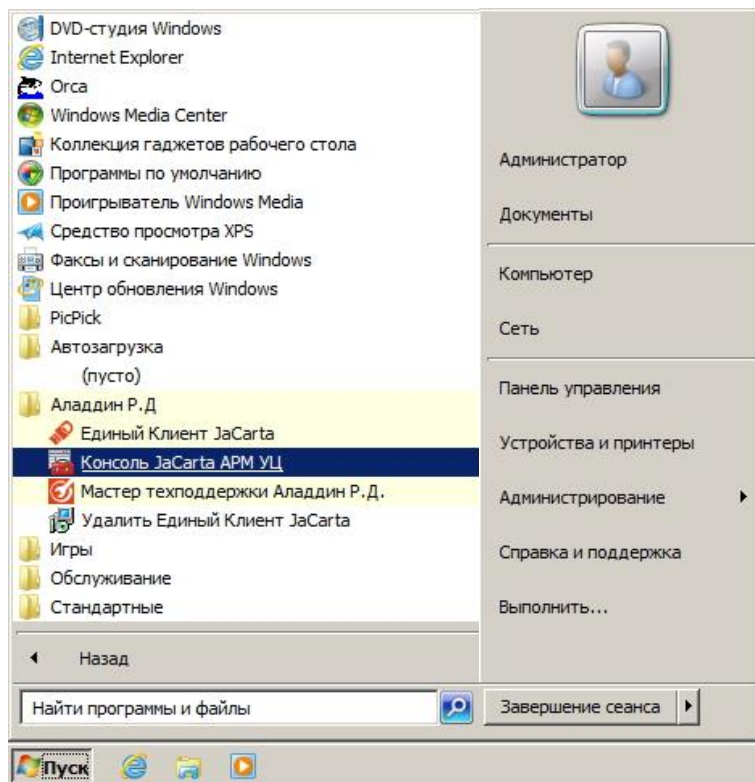


Рисунок 18

2. Отобразится следующее окно (см. Рис. 19). Дождитесь добавления оснастки.

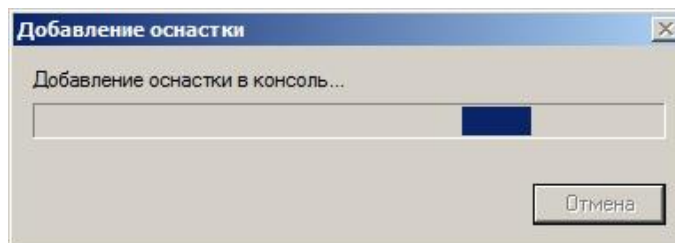


Рисунок 19

3. Для редактирования параметров выпуска запросов на сертификат и записи сертификатов на токен в левой панели отобразившегося окна щелкните правой кнопкой на **JaCarta APM УЦ** и в появившемся контекстном меню выберите опцию **Свойства**. (см. Рис. 20).

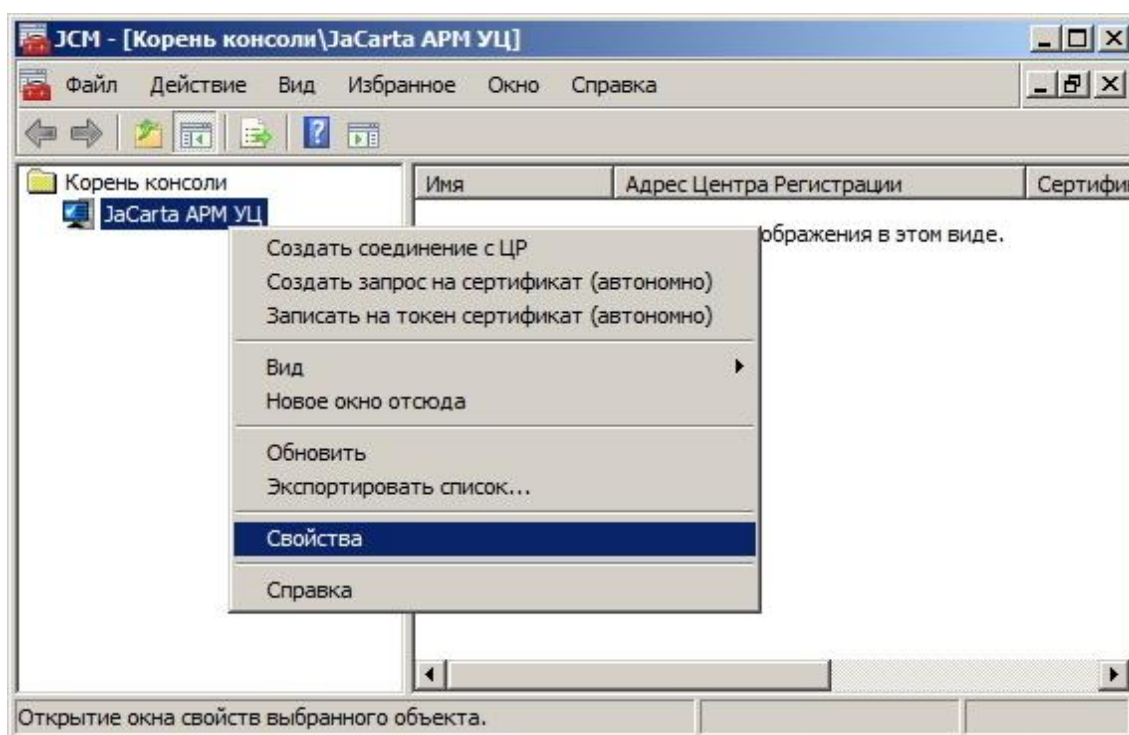


Рисунок 20

В появившемся окне (см. Рис. 21) на вкладке **Шаблоны запроса** имеется возможность настройки параметров каждого из шаблонов запроса на сертификат, а также редактирования содержимого шаблонов запроса на сертификат.

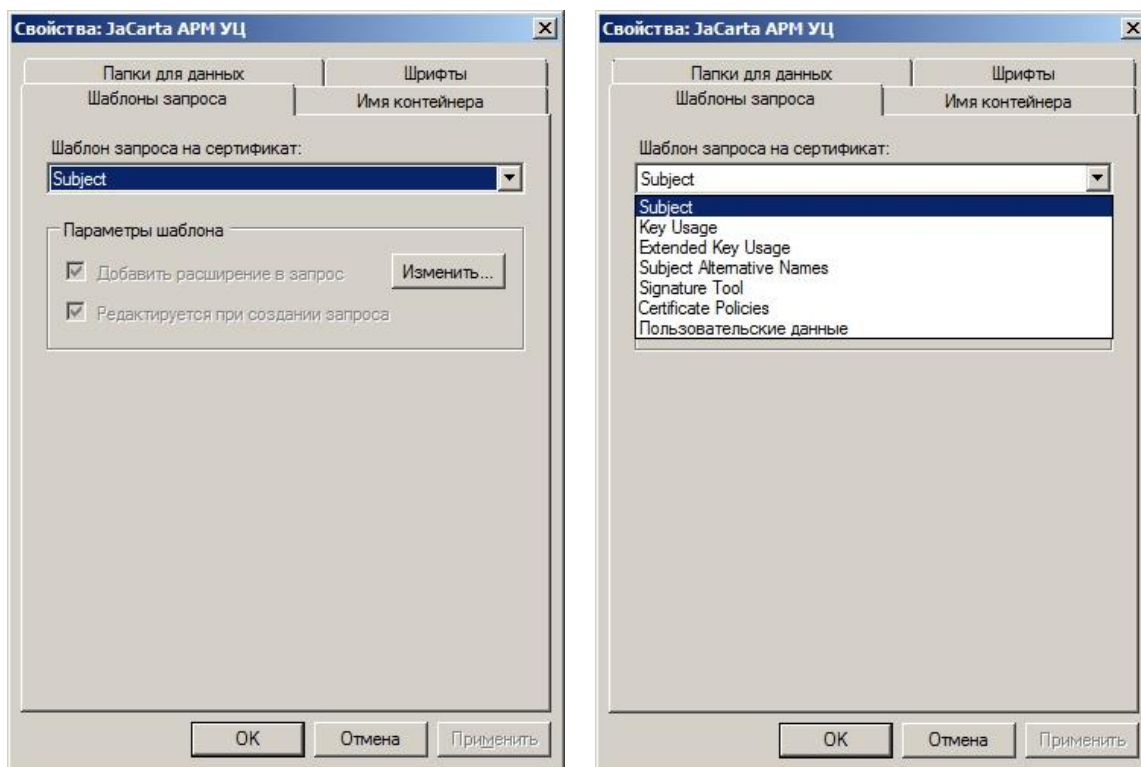


Рисунок 21

4. Выполните необходимые настройки, руководствуясь Таблицей 3.

Таблица 3

Элемент интерфейса	Настройки / Описание
Элемент Шаблон запроса на сертификат :	<p>Содержит раскрывающийся список из следующих шаблонов:</p> <ul style="list-style-type: none"> • Subject (расширение "Субъект"). • Key Usage (расширение "Использование ключа"). • Extended Key Usage (расширение "Улучшенный ключ"). • Subject Alternative Names (расширение "Альтернативные имена субъекта"). • Signature Tool (расширение "Название средства ЭП"). • Certificate Policies (расширение "Политики сертификата"). <p> Содержимое всех этих шаблонов может быть использовано при создании запроса на сертификат. В целях автоматизации действий пользователя и удобства при создании запроса на сертификат – шаблоны могут быть настроены (подробнее см. описание секции Параметры шаблона ниже).</p> <ul style="list-style-type: none"> • Пользовательские данные (расширение "Данные пользователя"). <p> Шаблон "Пользовательские данные" (см. Рис. 22) служит для задания дополнительных полей, которые не входят в запрос и сертификат, а нужны, например, для сохранения в БД согласно регламенту УЦ.</p>
Секция Параметры шаблона :	<p>Содержит:</p> <ul style="list-style-type: none"> • кнопку Изменить... – запускает Редактор шаблона, который позволяет отобразить и изменить поля выбранного шаблона запроса, а также установить отображаемые в полях шаблона значения по умолчанию; <p> При нажатии на кнопку Изменить... запускается Редактор шаблона, в котором можно просмотреть и изменить набор атрибутов, отображаемых в дальнейшем при запуске мастера составления запроса, а так же установить значения атрибутов, которые будут отображаться по умолчанию. Пример использования редактора шаблона показан на Рисунке 23.</p>

Элемент интерфейса	Настройки / Описание
	<ul style="list-style-type: none"> чекбокс Добавить расширение в запрос – добавляет данное расширение в запрос; чекбокс Редактируется при создании запроса – позволяет редактировать поля шаблона непосредственно при создании запроса.

Таблица 3

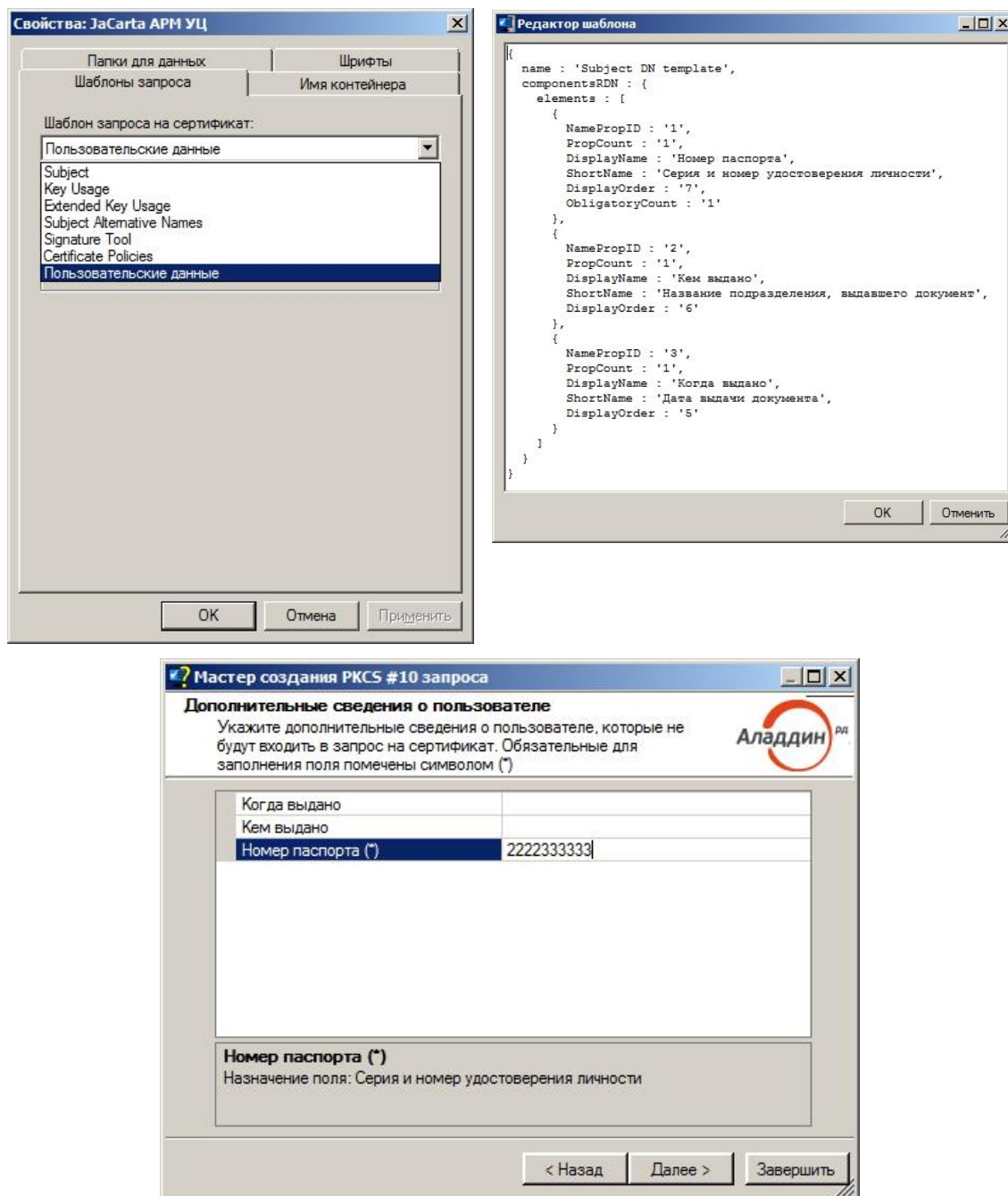


Рисунок 22

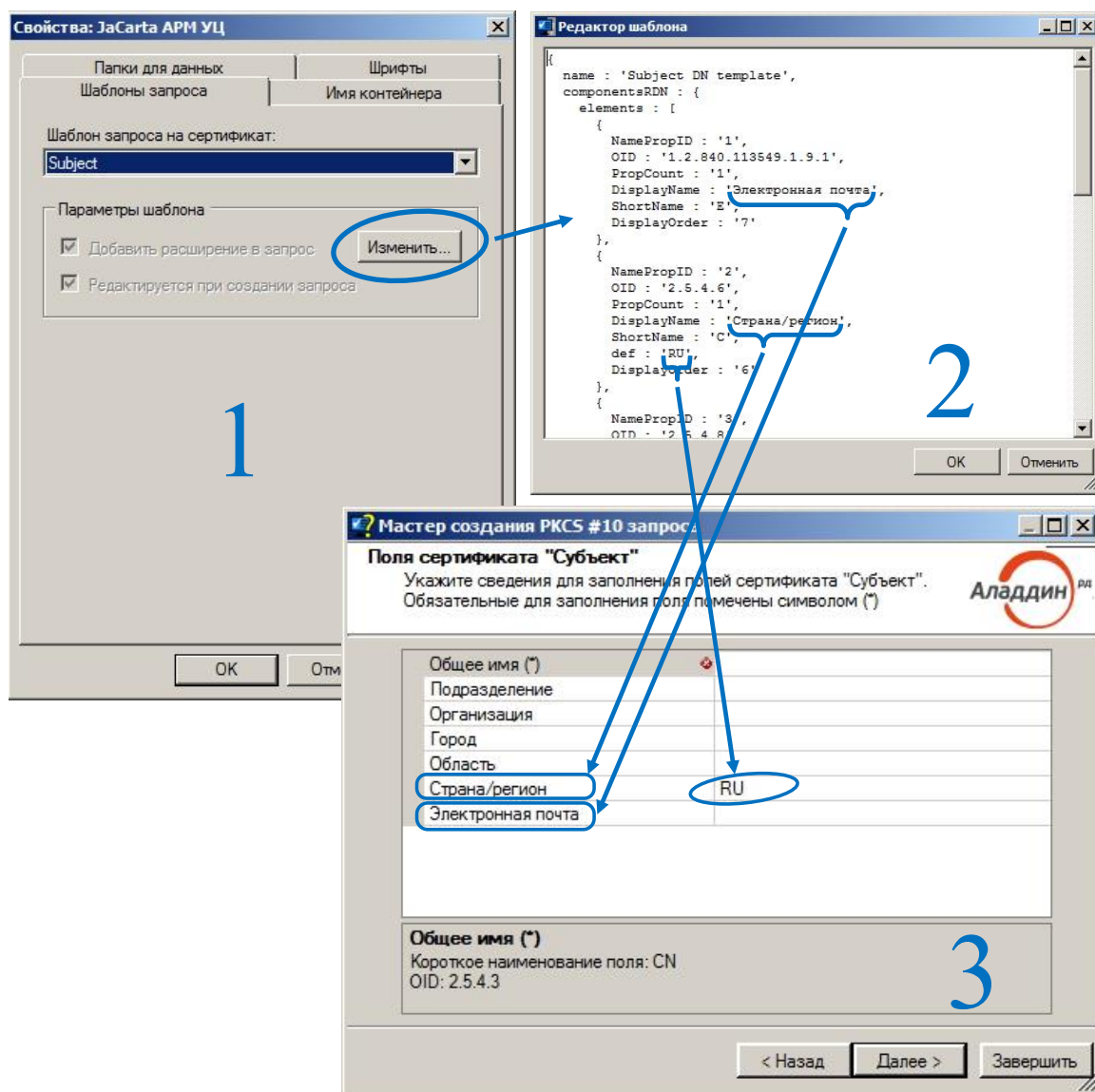


Рисунок 23



Примечание – шаблон для запроса на сертификат хранится в формате JSON. Для каждого параметра в шаблоне должно быть указано:

- NamePropID – номер параметра;
- OID – объектный идентификатор параметра;
- PropCount – количество значений параметра;
- DisplayName – отображаемое в диалоге имя параметра;
- ShortName – короткое имя параметра;
- Def – значение по умолчанию;
- DisplayOrder – номер, задающий порядок отображения параметров в диалогах.

5. Выберите вкладку **Имя контейнера**. Окно примет следующий вид (см. Рис. 24).

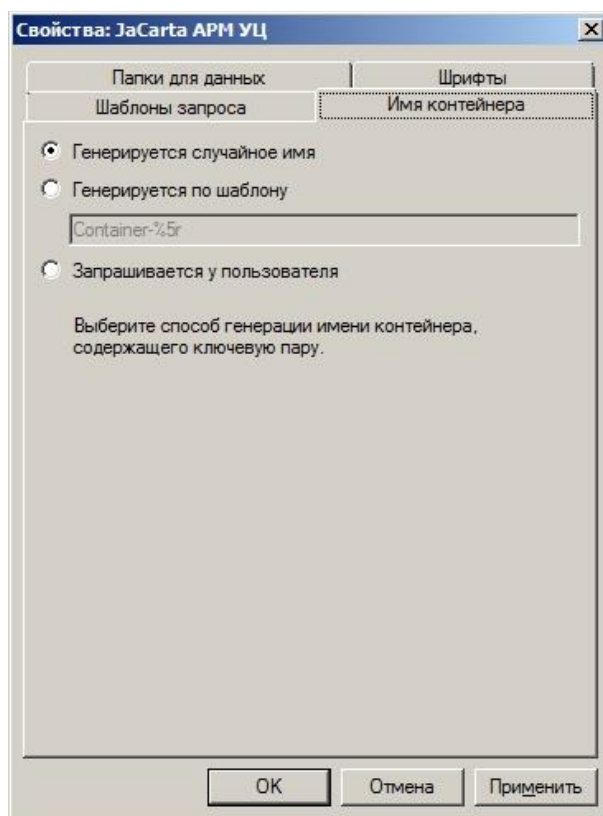


Рисунок 24



Примечание – В случае, если необходимо, чтобы имя Контейнера для хранения запроса было задано пользователем, следует выбрать опцию **Генерируется по шаблону** (см. Рис. 25) и задать имя контейнера.

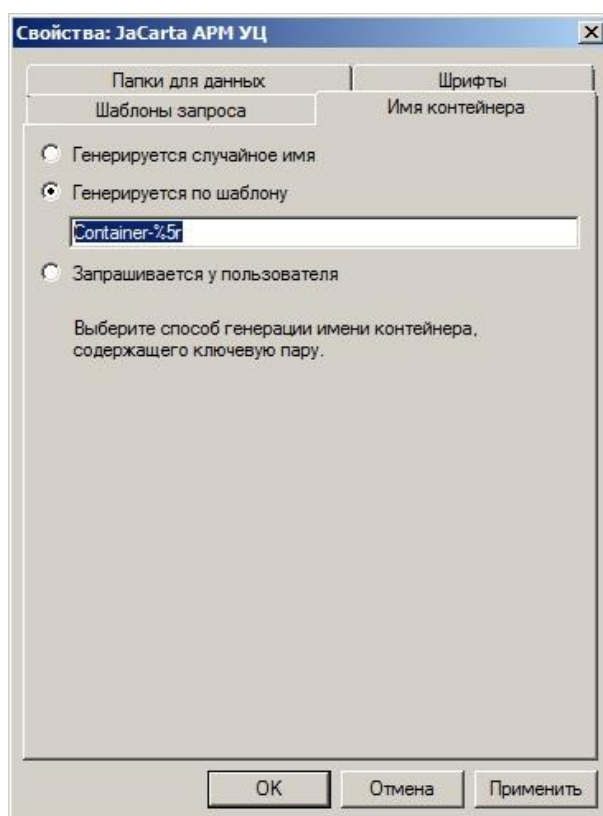


Рисунок 25

6. Настройки вкладки **Имя контейнера** описаны в Таблице 4.

Таблица 4

Настройка	Описание
Генерируется случайное имя	В процессе создания контейнера генерируется случайное значение, которое используется в качестве имени этого контейнера.
Генерируется по шаблону	Позволяет задать шаблон имени контейнера, по которому будет автоматически сформировано имя контейнера. Примеры шаблонов: {TokenSN, 0, 5} – подстрока из первых пяти символов серийного номера токена; {TokenSN, 4, 4} – подстрока из четырех символов, начиная с 4-ого (zero based) символа, серийного номера токена; {TokenSN, 0, -1} – строка с серийным номером токена; {RND, 0, 5} – строка из пяти случайных символов; {RND, 5, 5} – строка из пяти случайных символов; {RND, 0, -1} – строка из 32 случайных символов; {GUID, 0, -1} – уникальный идентификатор; {\{GUID, 0, -1\}} – уникальный идентификатор, заключенный в фигурные скобки; {2.5.4.3, 0, 5} – первые 5 символов значения атрибута с OID = 2.5.4.3.
Запрашивается у пользователя	При создании контейнера пользователь должен самостоятельно ввести имя для этого контейнера.

Таблица 4

7. Выберите вкладку **Папки для данных**. Окно примет следующий вид (см. Рис. 26).

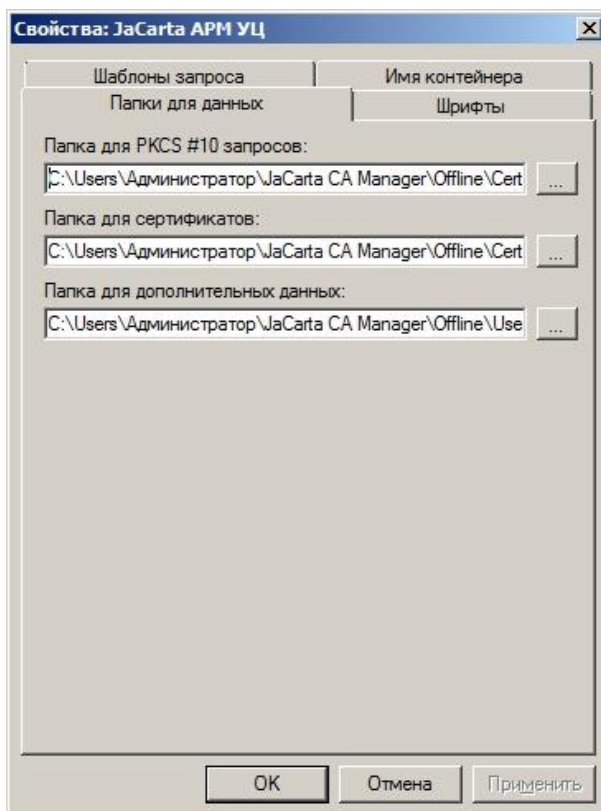


Рисунок 26

8. Заполните поля, руководствуясь Таблицей 5.

Таблица 5

Поле	Описание
Папка для PKCS #10 запросов	Папка, в которую будут сохраняться запросы на сертификаты.
Папка для дополнительных данных	Папка, в которую будут сохраняться дополнительные данные о пользователе, введенные в процессе создания запроса сертификата. Данные будут сохранены в формате XML.
Папка для сертификатов	Папка, в которую следует сохранять сертификаты, которые будут записаны в память электронного ключа.

Таблица 5

- Нажмите **ОК** (либо **Применить**), чтобы сохранить сделанные изменения и закрыть окно настроек.

4.3. Настройка для создания запросов в автоматическом режиме

4.3.1. Создание соединения с Центром Регистрации

Чтобы создать соединение с Центром Регистрации, выполните следующие действия.

- Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ
- В левой панели отобразившегося окна щелкните правой кнопкой на пункте **JaCarta APM УЦ** и выберите **Создать соединение с ЦР** (см. Рис. 27).

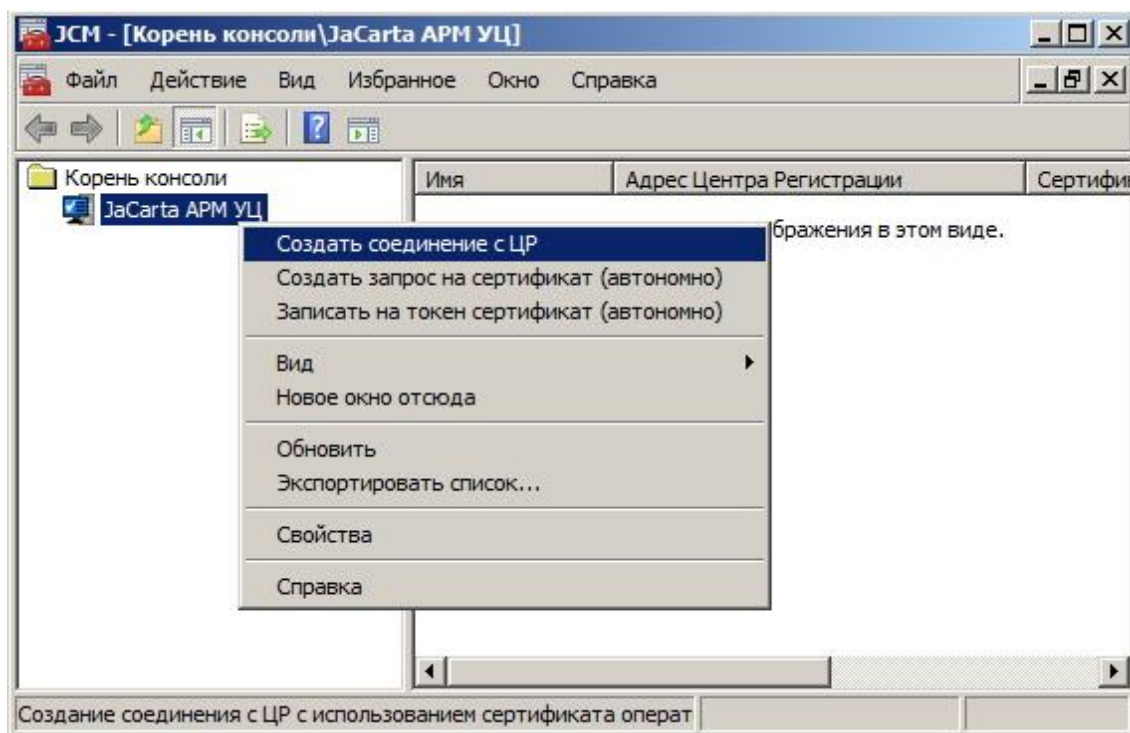


Рисунок 27

- В появившемся окне нажмите **Далее>** (см. Рис. 28).

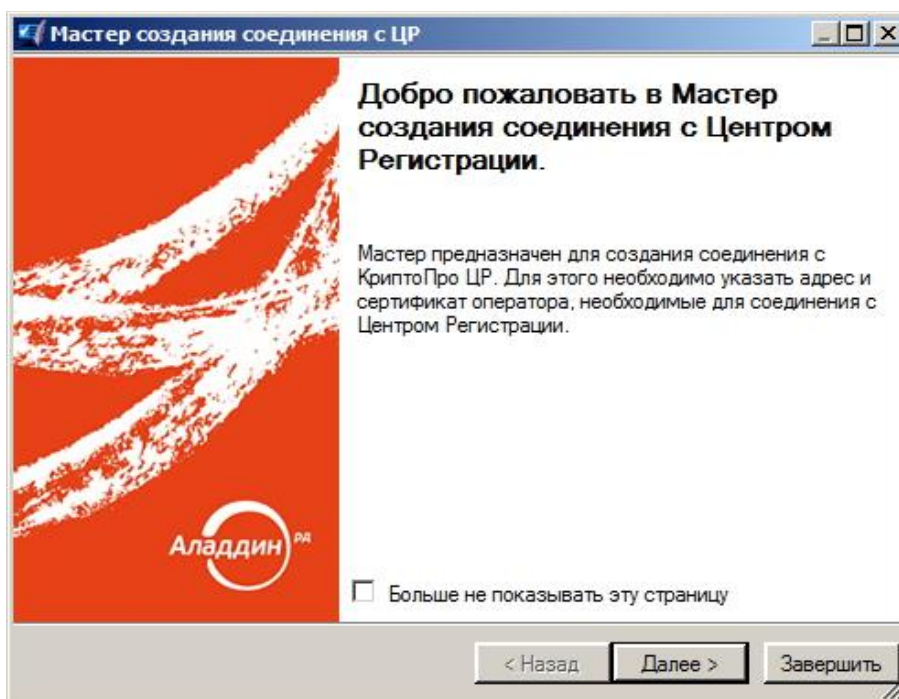


Рисунок 28

4. В появившемся окне введите адрес веб-сервиса Центра Регистрации и нажмите **Далее>** (см. Рис. 29).

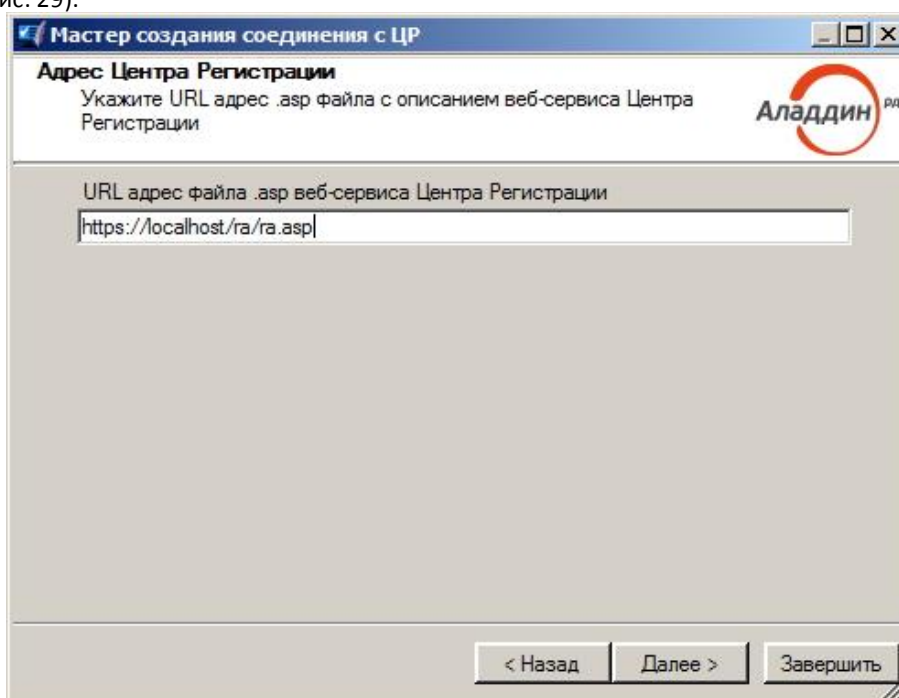


Рисунок 29



Внимание! Доменное имя веб-сервиса должно соответствовать доменному имени сервиса, указанному в сертификате администратора/оператора. Обращение к ЦР по IP-адресу недопустимо. (см. пример на Рис. 30).

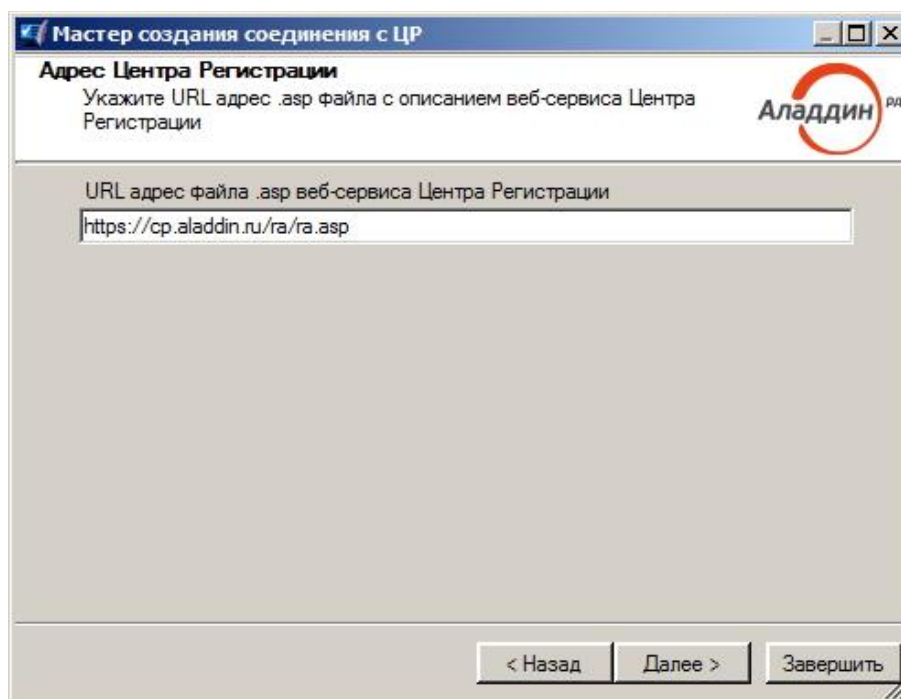


Рисунок 30

5. В появившемся окне нажмите кнопку **Выбрать сертификат**, чтобы выбрать сертификат администратора или оператора ЦР из личного хранилища сертификатов (см. Рис. 31).

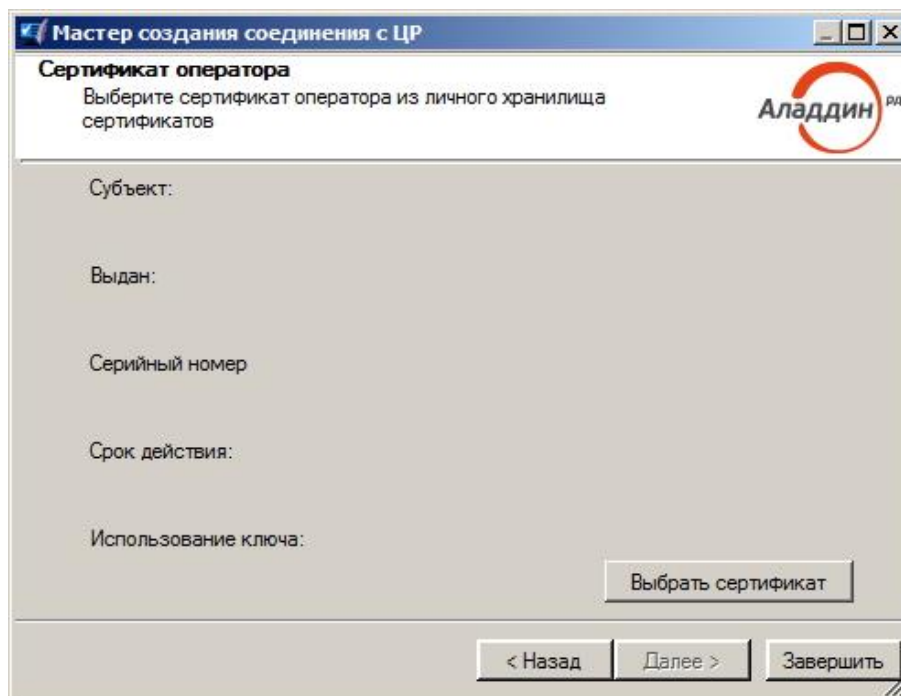


Рисунок 31

6. В следующем окне нажмите **Выбрать сертификат** и в появившемся окне (см. Рис. 32) выберите сертификат администратора или оператора ЦР и нажмите **ОК**.

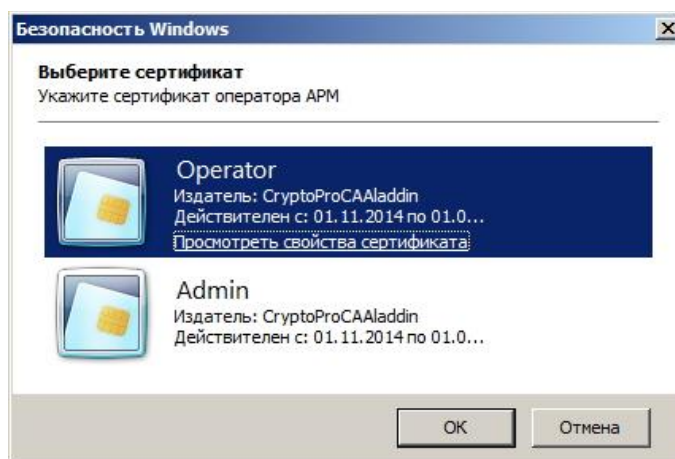


Рисунок 32

7. В появившемся окне нажмите **Далее>** (см. Рис. 33).

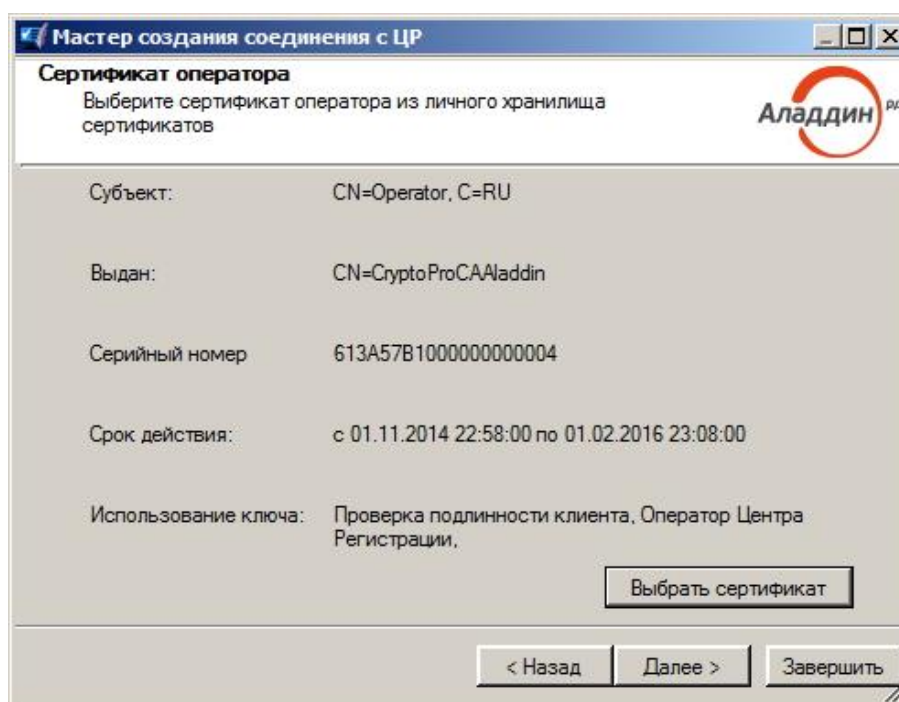


Рисунок 33

8. В появившемся окне нажмите **Завершить** (см. Рис. 34).

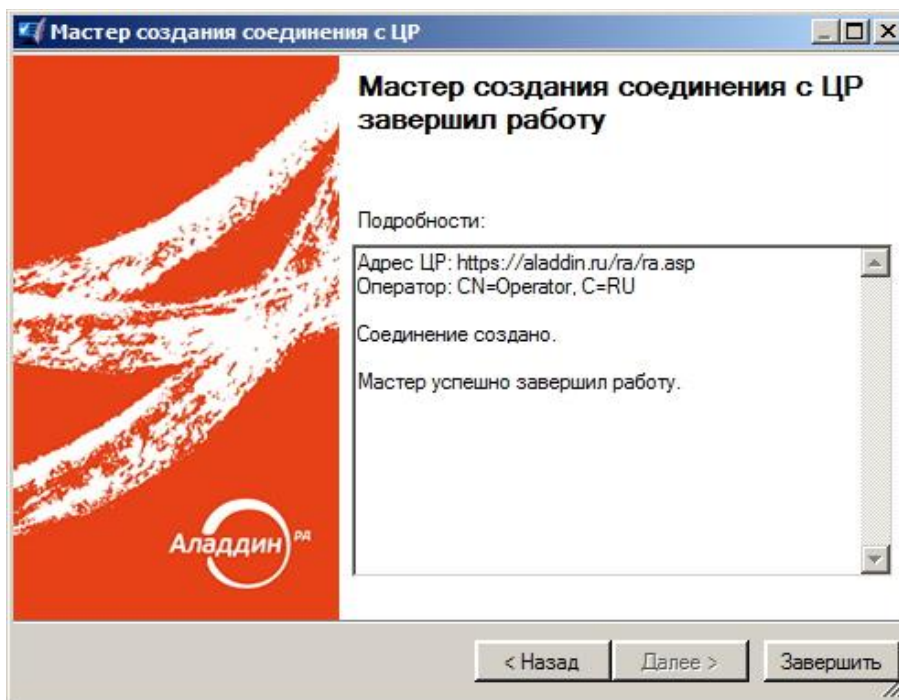


Рисунок 34

После соединения с ЦР меню Центра регистрации отобразится в левой панели консоли JaCarta APM УЦ (см. Рис. 35).

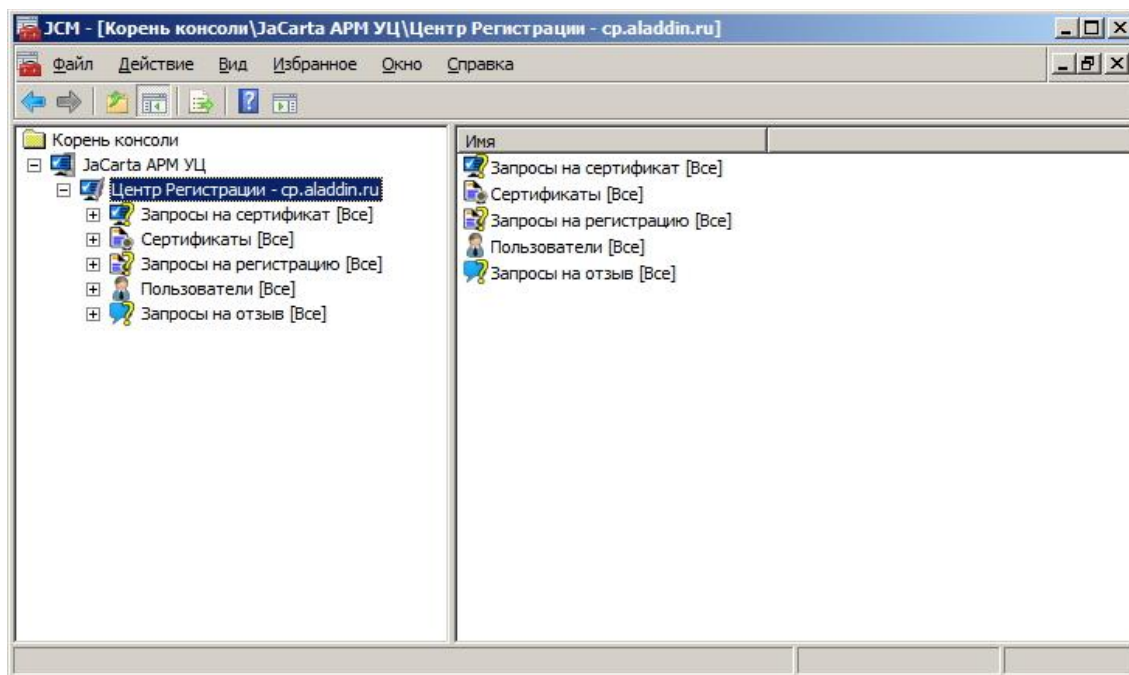


Рисунок 35

4.3.2. Настройка параметров соединения с Центром Регистрации

После того как соединение с ЦР создано, необходимо настроить параметры соединения с ЦР. Для этого выполните следующие действия:

1. Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ.

- В левой панели отобразившегося окна щелкните правой кнопкой на пункте Центр Регистрации и выберите **Свойства** (см. Рис. 36).

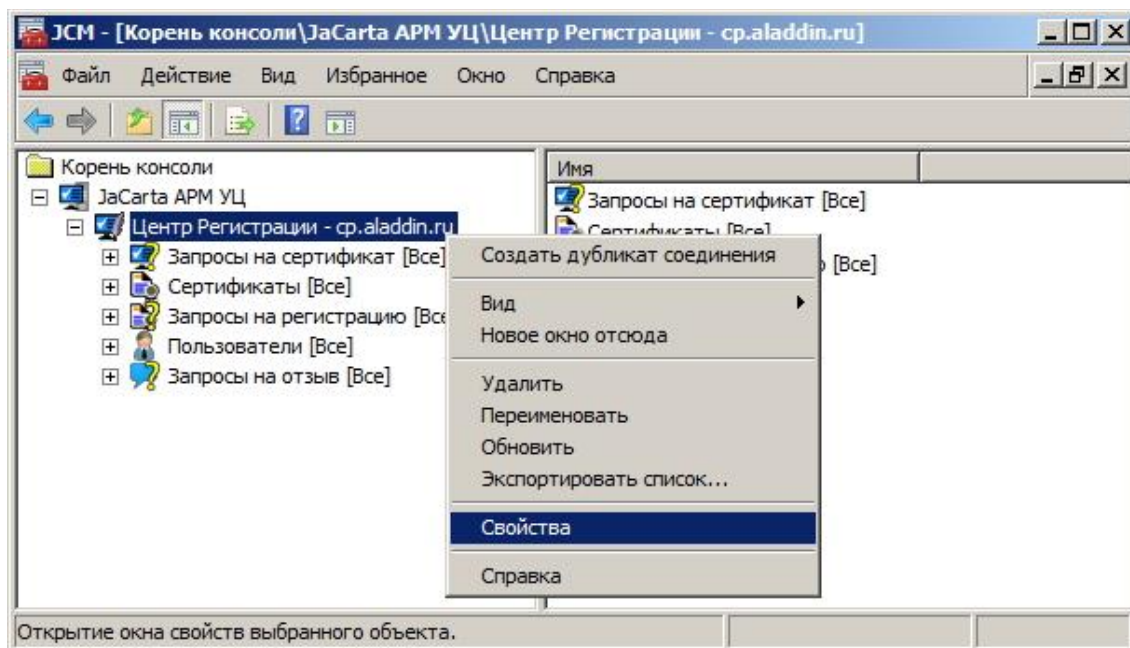


Рисунок 36

В появившемся окне (см. Рис. 37) на вкладке **Шаблоны запроса** имеется возможность настройки параметров каждого из шаблонов запроса на сертификат, а также редактирования содержимого шаблонов запроса на сертификат.

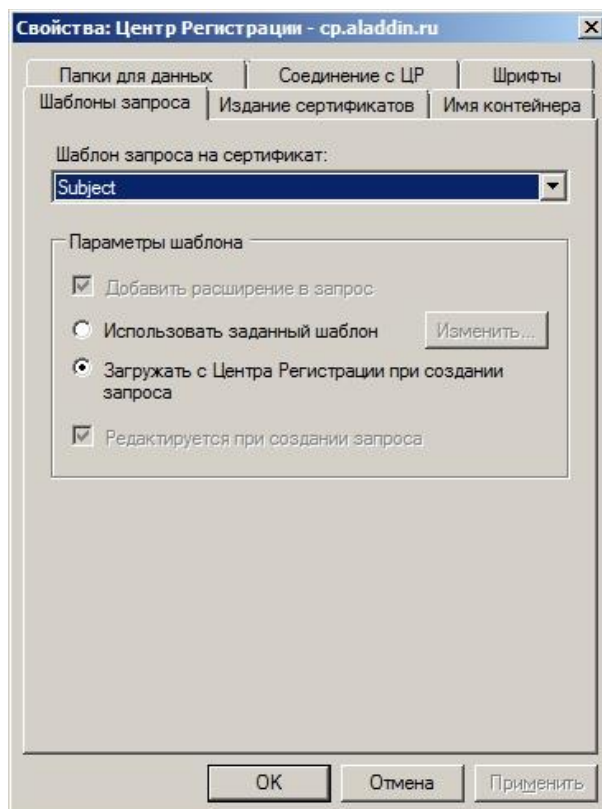


Рисунок 37

3. Выполните необходимые настройки, руководствуясь Таблицей 6.

Таблица 6




Элемент интерфейса	Настройки / Описание
Элемент Шаблон запроса на сертификат :	<p>Содержит раскрывающийся список из следующих шаблонов:</p> <ul style="list-style-type: none"> • Subject (расширение "Субъект"). • Key Usage (расширение "Использование ключа"). • Extended Key Usage (расширение "Улучшенный ключ"). • Subject Alternative Names (расширение "Альтернативные имена субъекта"). • Signature Tool (расширение "Название средства ЭП"). • Certificate Policies (расширение "Политики сертификата"). <p> Содержимое всех этих шаблонов может быть использовано при создании запроса на сертификат. В целях автоматизации действий пользователя и удобства при создании запроса на сертификат – шаблоны могут быть настроены (подробнее см. описание секции Параметры шаблона ниже).</p> <ul style="list-style-type: none"> • Пользовательские данные (расширение "Данные пользователя"). <p> Шаблон "Пользовательские данные" (см. Рис.22) служит для задания дополнительных полей, которые не входят в запрос и сертификат, а нужны, например, для сохранения в БД согласно регламенту УЦ.</p>
Секция Параметры шаблона :	<p>Содержит:</p> <ul style="list-style-type: none"> • кнопку Изменить... – запускает Редактор шаблона, который позволяет отобразить и изменить поля выбранного шаблона запроса, а также установить отображаемые в полях шаблона значения по умолчанию; • чекбокс Добавить расширение в запрос – добавляет данное расширение в запрос; • радиокнопку Использовать заданный шаблон – позволяет выбрать данную опцию; • радиокнопку Загружать с Центра Регистрации при создании запроса – загружает выбранный шаблон запроса на сертификат из Центра Регистрации; <p> Радиокнопка Загружать с Центра Регистрации при создании запроса включена по умолчанию т.к. рекомендуется использовать эту опцию.</p> <ul style="list-style-type: none"> • чекбокс Редактируется при создании запроса – позволяет редактировать значения полей запроса на сертификат.

Таблица 6

4. Выберите вкладку **Издание сертификатов** (см. Рис. 38) и установите флажок **Издавать сертификат в ЦР, используя АРМ**.

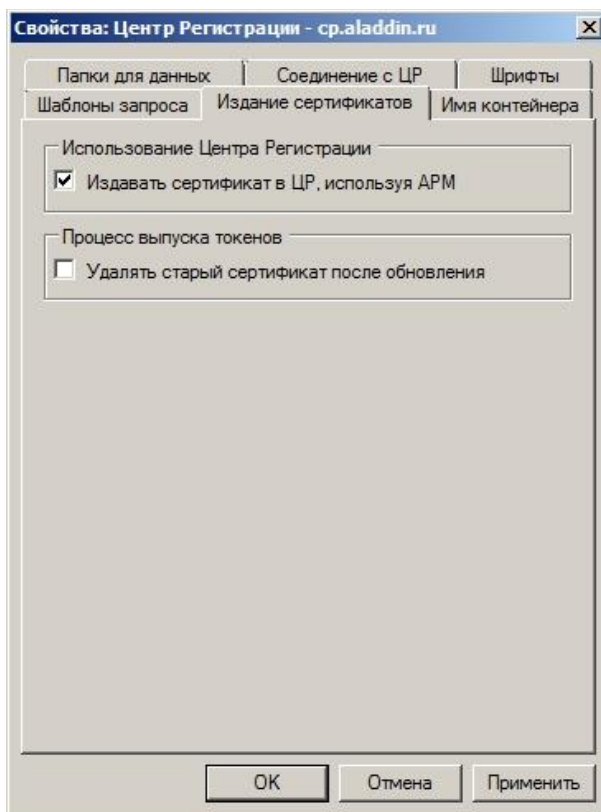


Рисунок 38

**Примечания:**

1 – Опция **Использование Центра Регистрации** отвечает за автоматический выпуск сертификата в ЦР при создании запроса оператором, если это позволяет политика. Если не использовать эту опцию, то необходимо после регистрации запроса в ЦР вручную подтвердить его с помощью АРМ Администратора ЦР КриптоПро.

2 – Опция **Процесс выпуска токенов** отвечает за удаление/сохранение старого сертификата после обновления. Если не использовать эту опцию, то после обновления старый сертификат будет сохранен на токене вместе с новым сертификатом.

5. Выберите вкладку **Имя контейнера**. Окно примет следующий вид (см. Рис. 39).

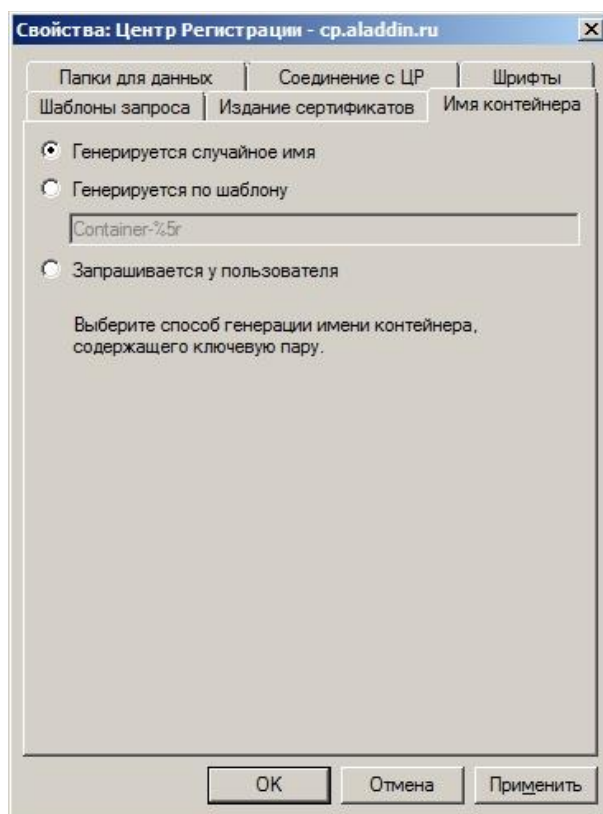


Рисунок 39



Примечание – В случае, если необходимо, чтобы имя Контейнера для хранения запроса было задано пользователем, следует выбрать опцию **Генерируется по шаблону** и задать имя контейнера.

6. Параметры формирования имени контейнера на вкладке **Имя контейнера**, описаны в Таблице 7.

Таблица 7

Настройка	Описание
Генерируется случайное имя	В процесс создания контейнера генерируется случайное значение, которое используется в качестве имени этого контейнера.
Генерируется по шаблону	<p>Позволяет задать шаблон имени контейнера, по которому будет автоматически сформировано имя контейнера.</p> <p>Примеры шаблонов:</p> <ul style="list-style-type: none"> {TokenSN, 0, 5} – подстрока из первых пяти символов серийного номера токена; {TokenSN, 4, 4} – подстрока из четырех символов, начиная с 4-ого (zero based) символа, серийного номера токена; {TokenSN, 0, -1} – строка с серийным номером токена; {RND, 0, 5} – строка из пяти случайных символов; {RND, 5, 5} – строка из пяти случайных символов; {RND, 0, -1} – строка из 32 случайных символов; {GUID, 0, -1} – уникальный идентификатор; {\{GUID, 0, -1}\} – уникальный идентификатор, заключенный в фигурные скобки; {2.5.4.3, 0, 5} – первые 5 символов значения атрибута с OID = 2.5.4.3.
Запрашивается у пользователя	При создании контейнера пользователь должен ввести самостоятельно имя для этого контейнера.

Таблица 7

7. Выберите вкладку **Папки для данных**. Окно примет следующий вид (см. Рис. 40).

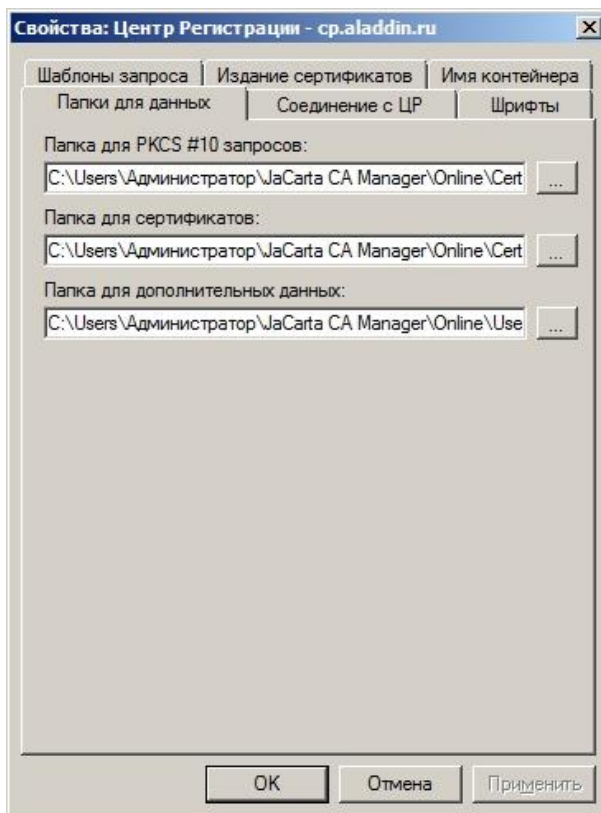


Рисунок 40

8. При необходимости заполните нужные поля, руководствуясь приведенной ниже Таблицей 8.



Примечание: Настройки на данной вкладке необходимы, если вы хотите сохранить копии запросов и сертификатов при автоматическом выпуске.

Таблица 8

Поле	Описание
Папка для PKCS #10 запросов	Папка, в которую будут сохраняться запросы на сертификаты.
Папка для дополнительных данных	Папка, в которую будут сохраняться дополнительные данные о пользователе, введенные в процессе создания запроса сертификата. Данные будут сохранены в формате XML.
Папка для сертификатов	Папка, в которую будут сохраняться копии сертификатов пришедшие из ЦР и записанные на токен.

Таблица 8

9. Выберите вкладку **Соединение с ЦР**. Окно примет следующий вид (см. Рис. 41).

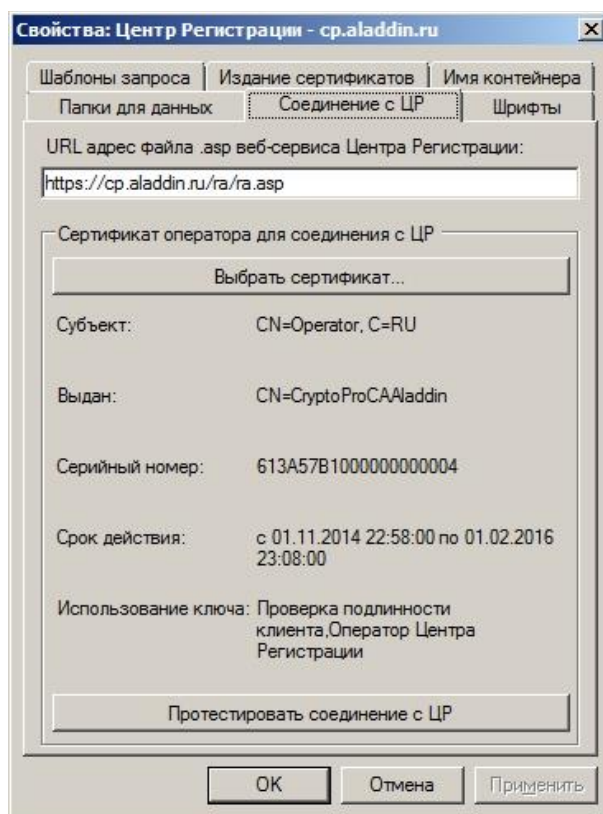


Рисунок 41

На этой вкладке можно изменить настройки соединения с ЦР, выбрать другой сертификат и протестировать соединение с ЦР.

10. Нажмите **ОК**.

5. ВЫПУСК СЕРТИФИКАТА

5.1.Выпуск сертификата в автономном режиме



Внимание! Для создания запроса на сертификат в автономном режиме не требуется создание соединения с ЦР.

5.1.1. Создание запроса на сертификат

Чтобы создать запрос на сертификат, выполните следующие действия:

1. Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ.
2. В левой панели отобразившегося окна щелкните правой кнопкой на пункте JaCarta APM УЦ и выберите **Создать запрос на сертификат** (см. Рис. 42).

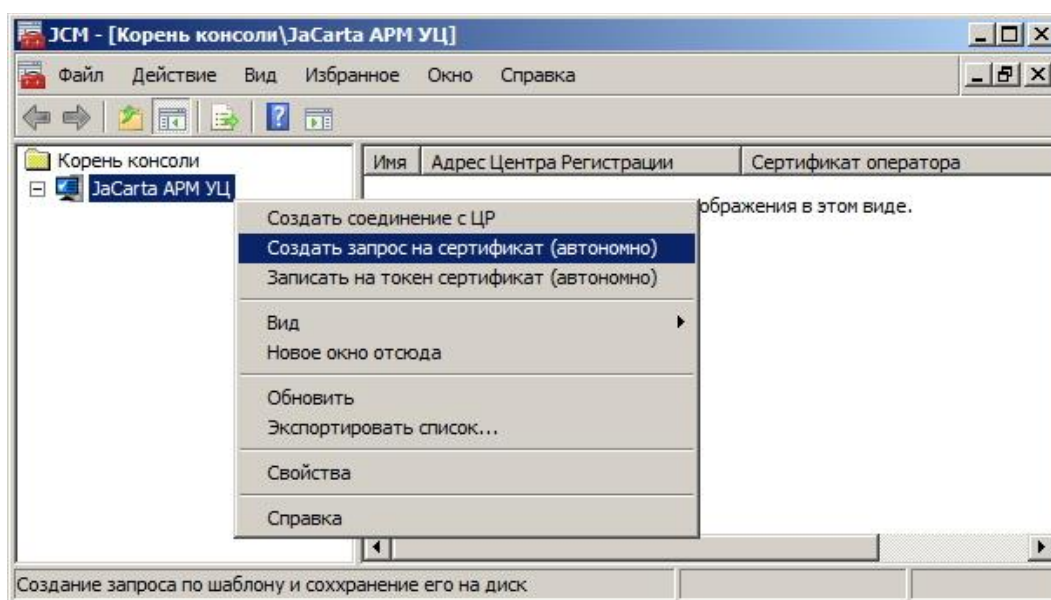


Рисунок 42

Отобразится окно мастера создания запроса (см. Рис. 43).

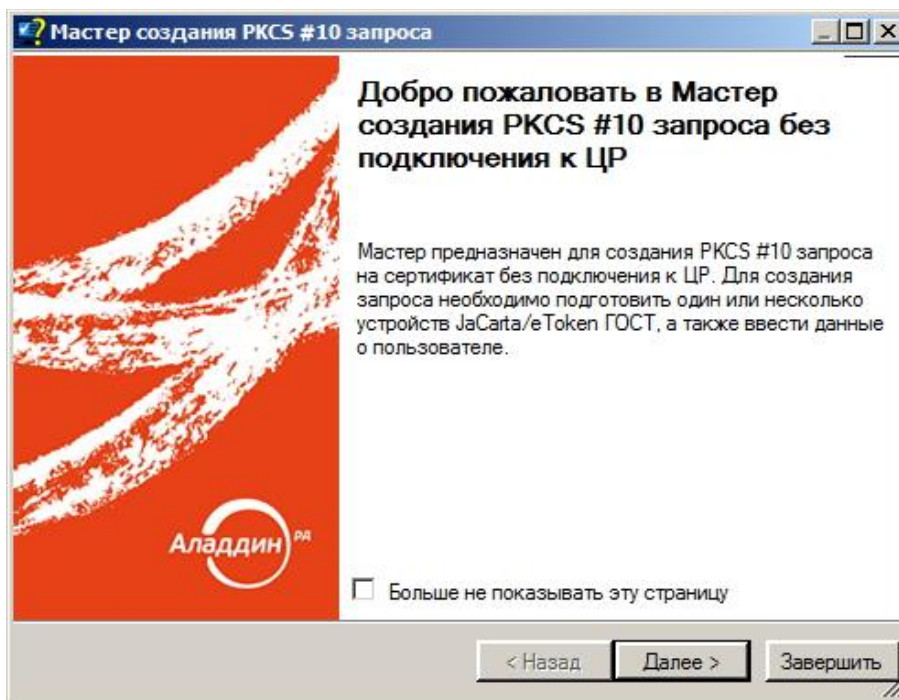


Рисунок 43

3. Нажмите **Далее>**. Отобразится следующее окно (см. Рис. 44).

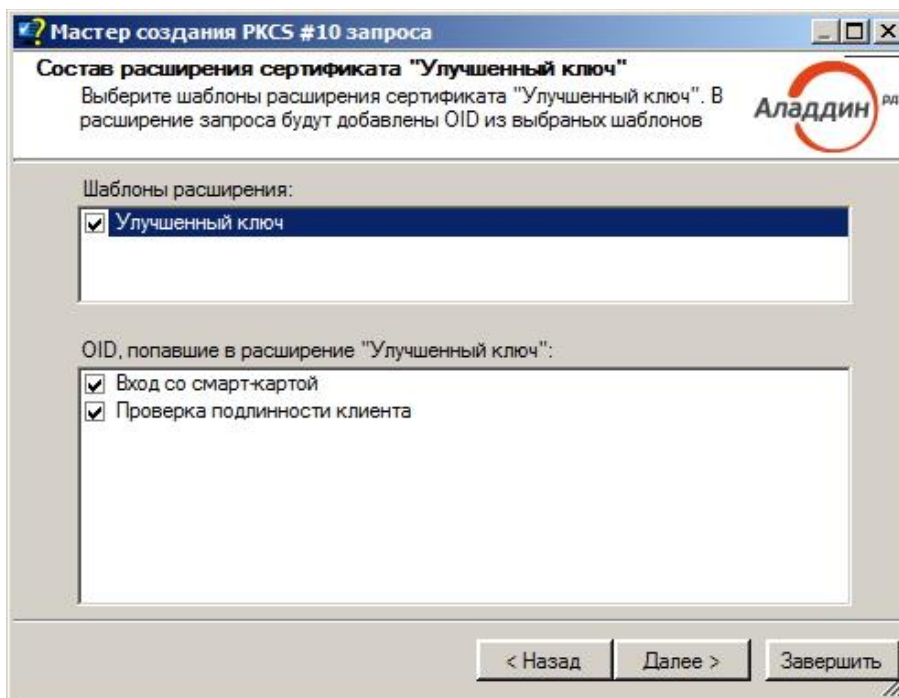


Рисунок 44

4. Выберите шаблоны расширения сертификата.
При выборе шаблона расширения в поле ниже отобразятся включенные в него объектные идентификаторы. Установите необходимые флажки и нажмите **Далее>**. Отобразится следующее окно (см. Рис. 45).

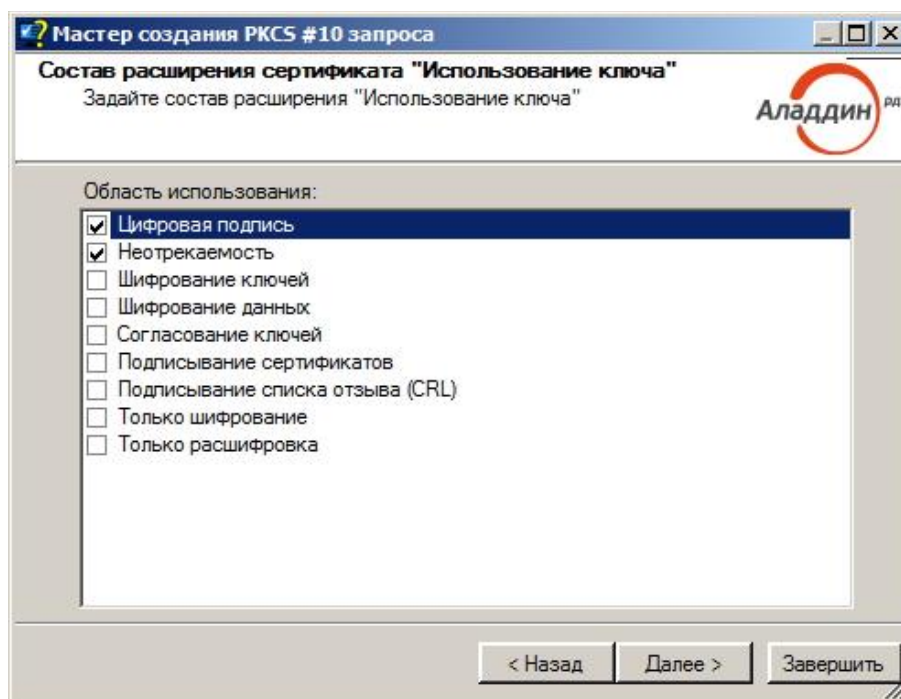


Рисунок 45

5. Задайте область использования ключа, установив соответствующие флажки, и нажмите **Далее>**. Отобразится следующее окно (см. Рис. 46).

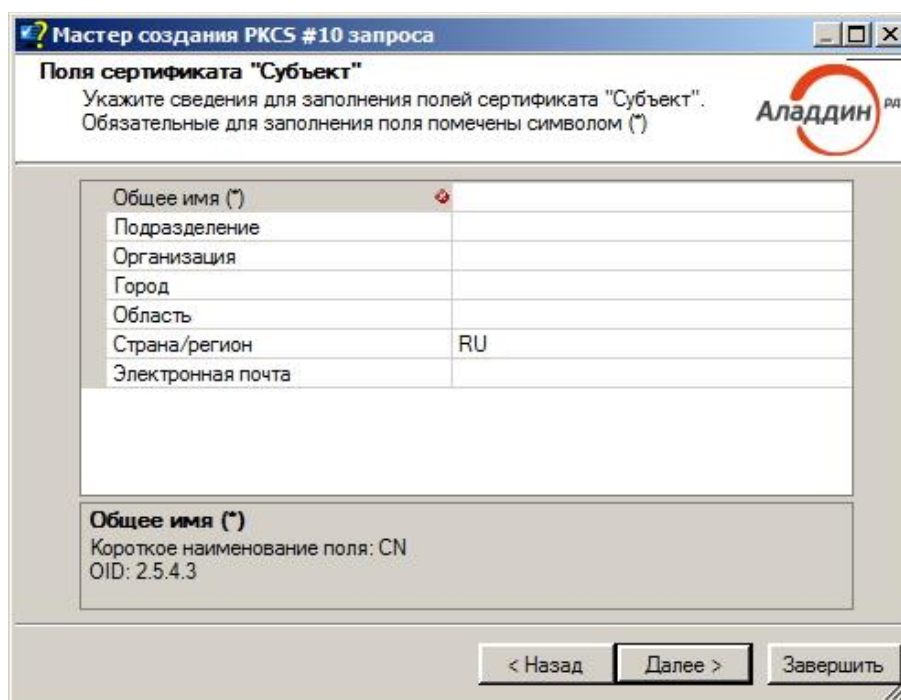



Рисунок 46

6. В появившемся окне (см. Рис. 47) введите данные, которые будут включены в поля сертификата "Субъект" (обязательные поля отмечены символом (*) и значком ) и нажмите **Далее>**.

Общее имя (*)	Фамилия Инициалы
Подразделение	
Организация	
Город	
Область	
Страна/регион	RU
Электронная почта	

Общее имя (*)
Короткое наименование поля: CN
OID: 2.5.4.3

< Назад Далее > Завершить

Рисунок 47

7. В появившемся окне (см. Рис. 48) введите данные для заполнения расширения "Дополнительное имя субъекта" и нажмите **Далее>**.

Фамилия	
Бизнес-категория	
Название подразделения	
Название организации	ОАО "Организация"
Адрес e-mail	
Адрес URL	http://www.some-site.ru
Почтовый адрес	129226, Москва, ул. Докукина
Дополнительное описание	Система защищенной электронной почты
Имя участника	

Почтовый адрес
Наименование поля: physicalDeliveryOfficeName
OID: 2.5.4.19

< Назад Далее > Завершить


Рисунок 48

8. В появившемся окне (см. Рис. 49) нажмите **Далее>**.

Рисунок 49

9. В случае, если электронный ключ не подсоединен к компьютеру, отобразится следующее окно (см. Рис. 50).

Рисунок 50

 **Примечание** – Значение PIN-кода в окне по умолчанию: 1234567890. Если на токене установлен другой PIN-код, то следует ввести его.

10. Подсоедините электронный ключ к компьютеру. Нажмите **Далее>** (см. Рис. 51).

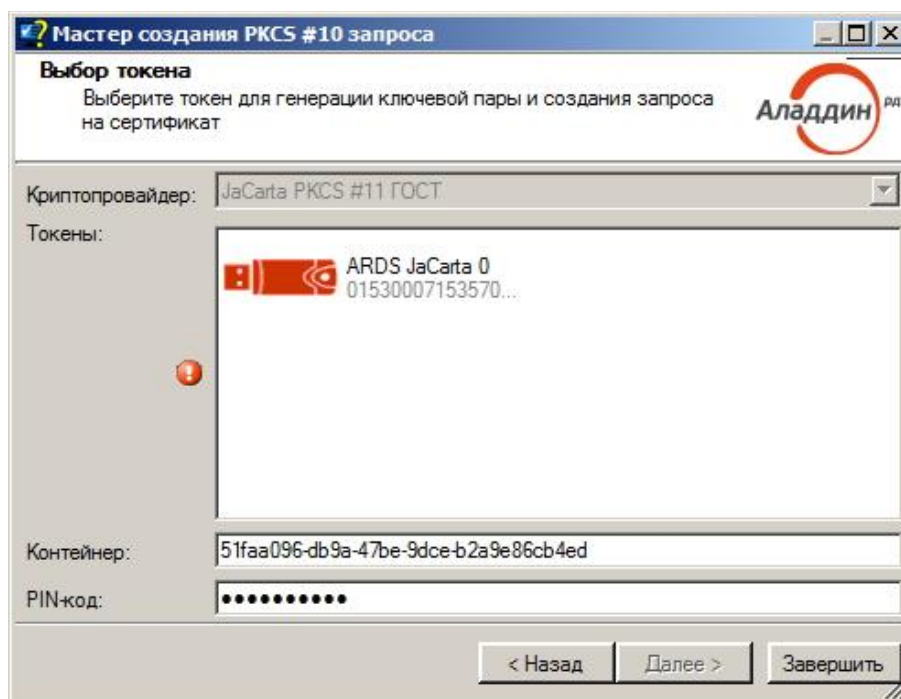


Рисунок 51

Появится окно генерации запроса на сертификат (см. Рис. 52). В памяти электронного ключа контейнер будет создан автоматически.

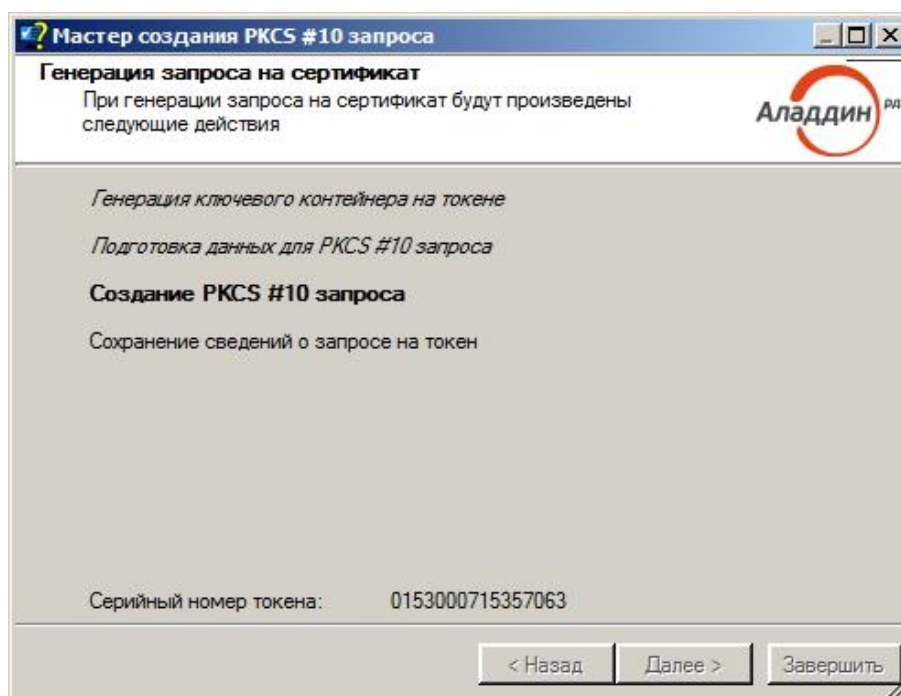


Рисунок 52

После создания запроса и формирования контейнера в памяти электронного ключа, появится отчет о работе Мастера (см. Рис. 53).

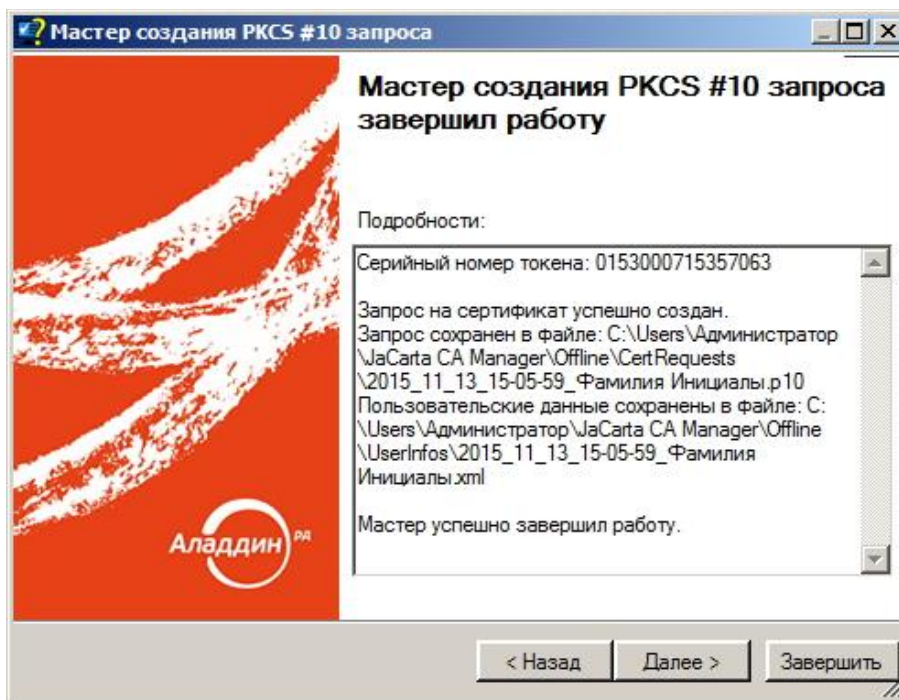



Рисунок 53

11. Закройте окно программы мастера, нажав **Завершить**.

 **Примечание** – При нажатии кнопки **< Назад**, будет осуществлен переход на начальную страницу с сохранением ранее введенных данных. При нажатии кнопки **Далее >**, будет осуществлен переход на начальную страницу с очисткой ранее введенных данных.

Убедиться в том, что запрос на сертификат записан на токен можно, запустив ПО Единый Клиент JaCarta (см. Рис. 54)

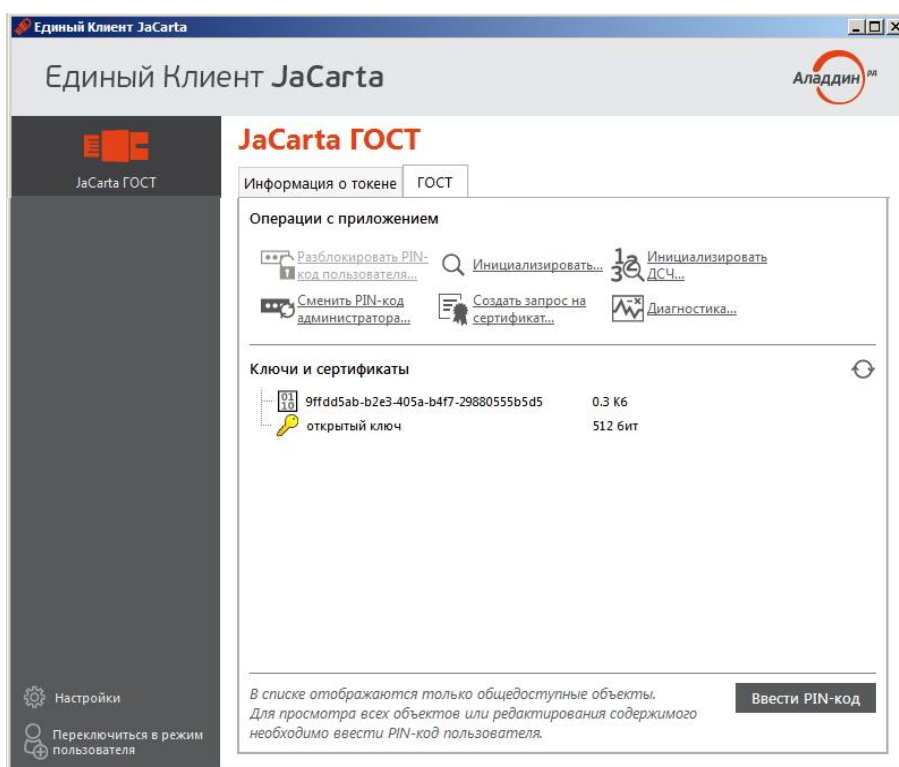


Рисунок 54

Созданный запрос на сертификат появится в заданной в настройках папке (см. Таблицу 5 в разделе “Настройка JaCarta APM УЦ для создания запросов в автономном режиме”).

Убедиться в том, что запрос на сертификат записан в заданную папку можно, перейдя по указанному в настройках адресу (см. Рис. 55).

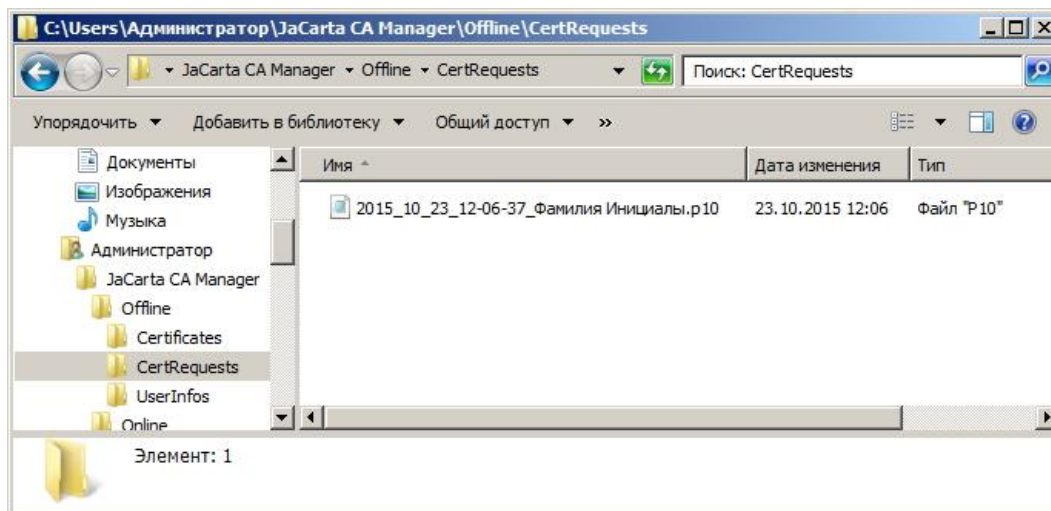


Рисунок 55

12. Далее необходимо отправить файл запроса в Центр Регистрации КриптоПРО УЦ, где Администратором с помощью ПО АРМ администратора Центра Регистрации будет выполнен ряд операций для осуществления выпуска сертификата.



Примечание – Для автономного режима отправлять файл запроса можно в любой Центр Регистрации. Для автоматического режима - только в Центр Регистрации КриптоПРО УЦ.

13. После выпуска сертификата в ЦР файл сертификата сохраняется на носитель и отправляется пользователю (либо отправляется по электронной почте) для записи сертификата на электронный ключ.
14. После получения пользователем файла сертификата его необходимо поместить в папку, предназначенную для записи сертификатов (см. процедуру в разделе “Настройка JaCarta APM УЦ для создания запросов в автономном режиме”).
15. После этого следует записать сертификат в память электронного ключа (см. раздел 5.1.2 “Запись сертификата в память электронного ключа” ниже).

5.1.2. Запись сертификата в память электронного ключа

Чтобы записать выпущенный сертификат в память электронного ключа, выполните следующие действия:

1. Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ.
2. В левой панели отобразившегося окна щелкните правой кнопкой на пункте **JaCarta APM УЦ** и выберите **Записать на токен сертификат** (см. Рис. 56).

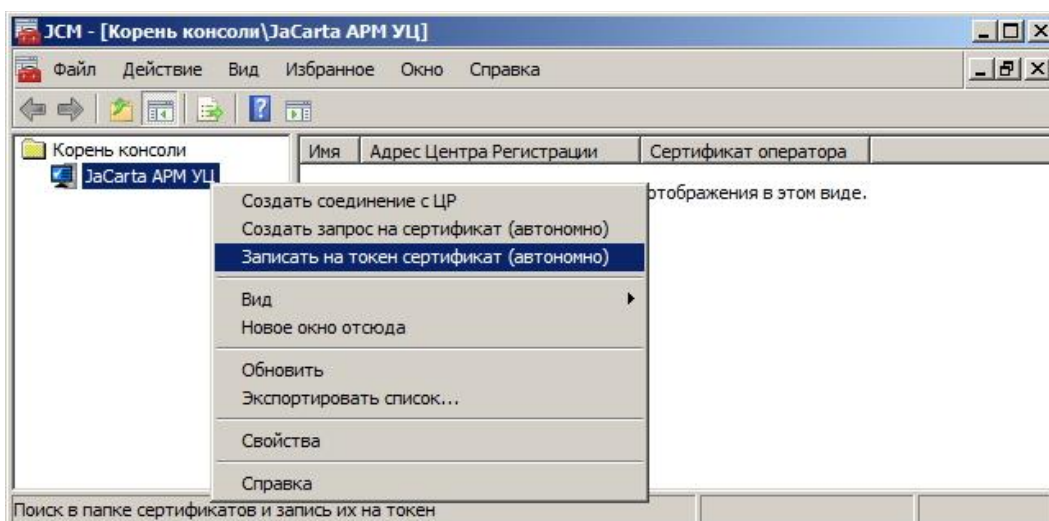


Рисунок 56

3. Отобразится окно программы-мастера записи сертификатов (см. Рис. 57). Нажмите **Далее>**.

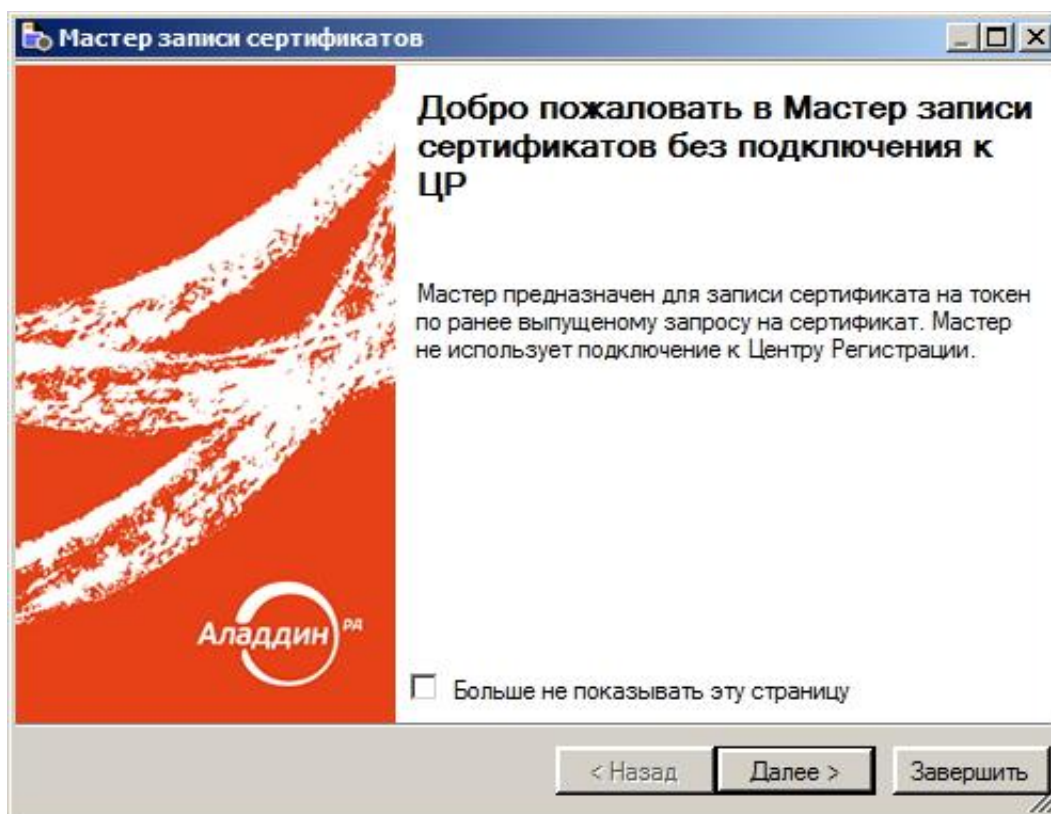


Рисунок 57

4. В появившемся окне нажмите **Далее>** (см. Рис. 58).

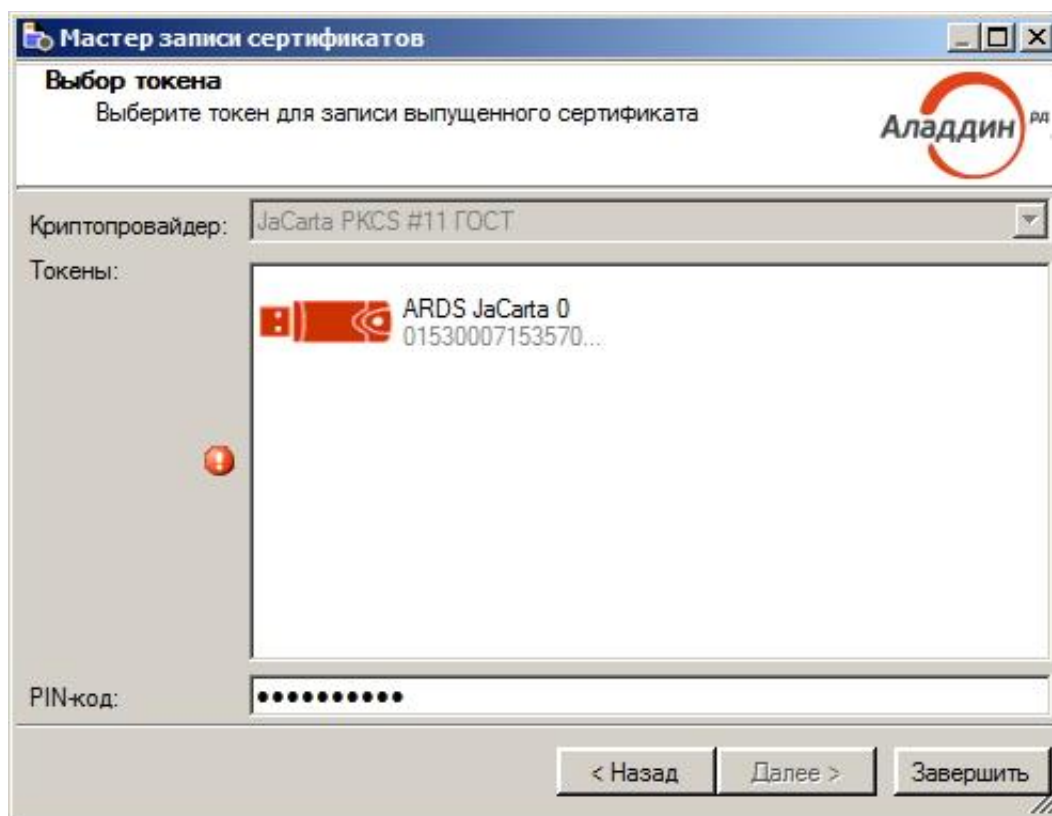


Рисунок 58

5. Выделите электронный ключ, затем введите PIN-код пользователя электронного ключа и нажмите **Далее>**.



Примечание – Значение PIN-кода в окне по умолчанию: 1234567890. Если на токене установлен другой PIN-код, то следует ввести его.

Сертификат будет записан в память электронного ключа автоматически (см. Рис. 59).

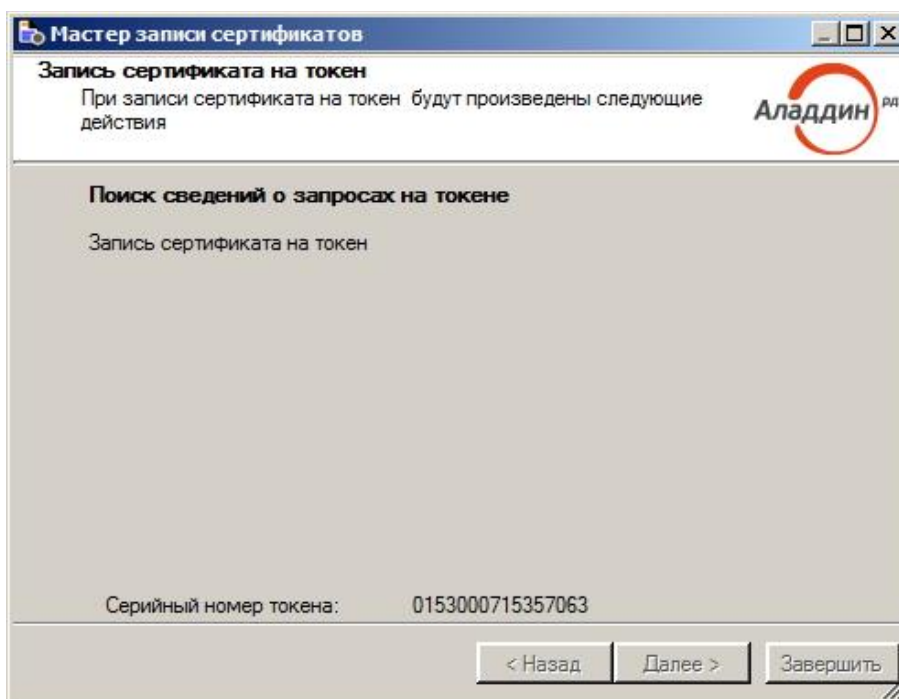


Рисунок 59

6. После записи сертификата в память электронного ключа закройте окно программы мастера, нажав **Завершить** (см. Рис. 60).

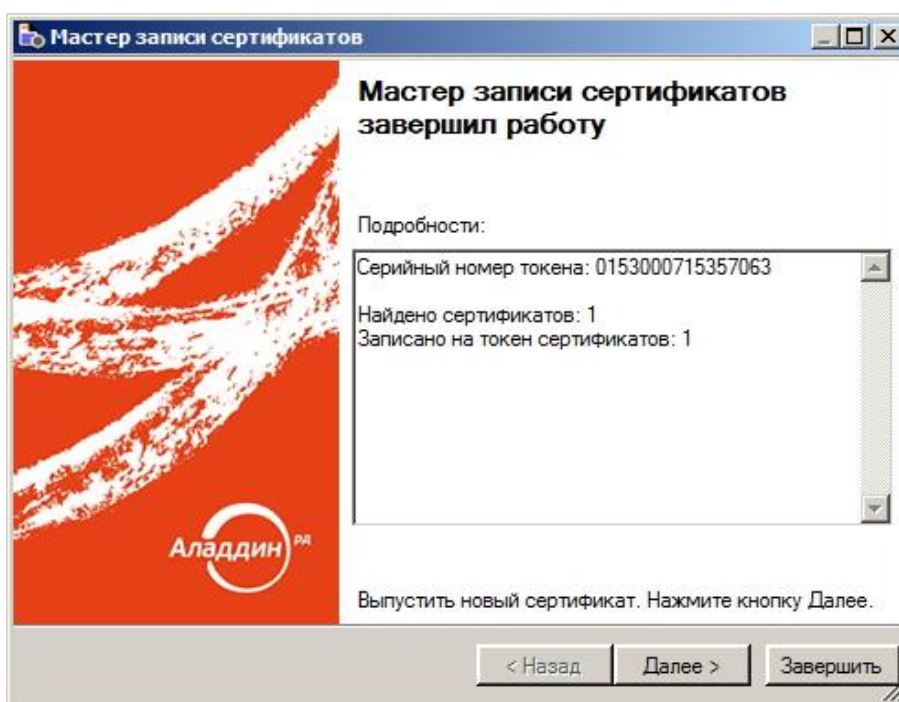


Рисунок 60



Примечание – При нажатии кнопки **Далее >**, Мастер выпуска сертификатов будет запущен заново с очисткой ранее введенных данных.

Убедиться в том, что сертификат записан на токен можно, запустив ПО Единый Клиент JaCarta (см. Рис. 61)

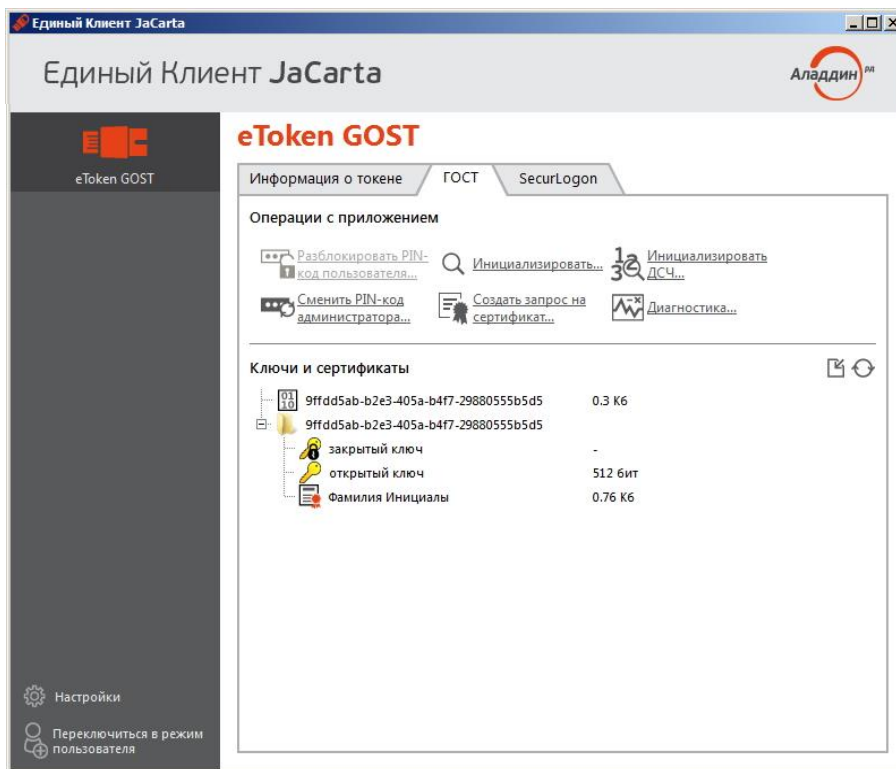




Рисунок 61

5.2. Выпуск сертификата в автоматическом режиме

 **Внимание!** Для создания запроса на сертификат в автоматическом режиме требуется создание соединения с ЦР (см. п. 4.3.1).

 **Примечание** – При регистрации запроса на несуществующего пользователя, он будет автоматически создан, если у Администратора/Оператора есть соответствующие права.

5.2.1. Создание запроса на сертификат

Чтобы запросить сертификат в автоматическом режиме, выполните следующие действия:

1. Нажмите Пуск → Все программы → Аладдин Р.Д. → Консоль JaCarta APM УЦ.
2. Создайте соединение с Центром Регистрации (см. п. 4.3.1).
3. Нажмите Запросы на сертификат → Создать запрос на новый сертификат (см. Рис. 62).

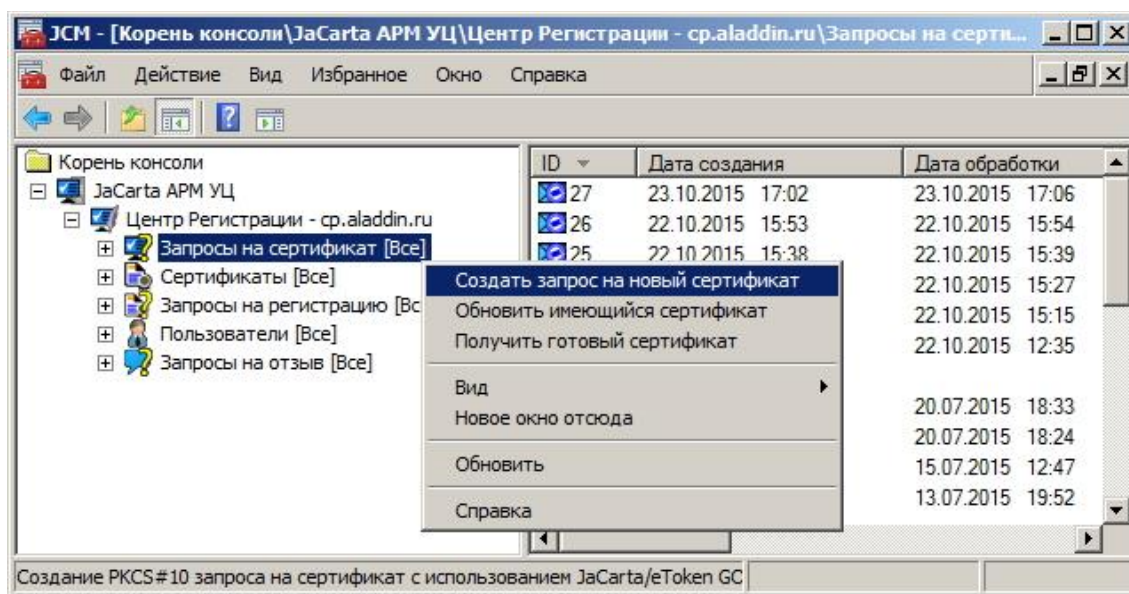


Рисунок 62

4. В появившемся окне нажмите **Далее>** (см. Рис. 63)

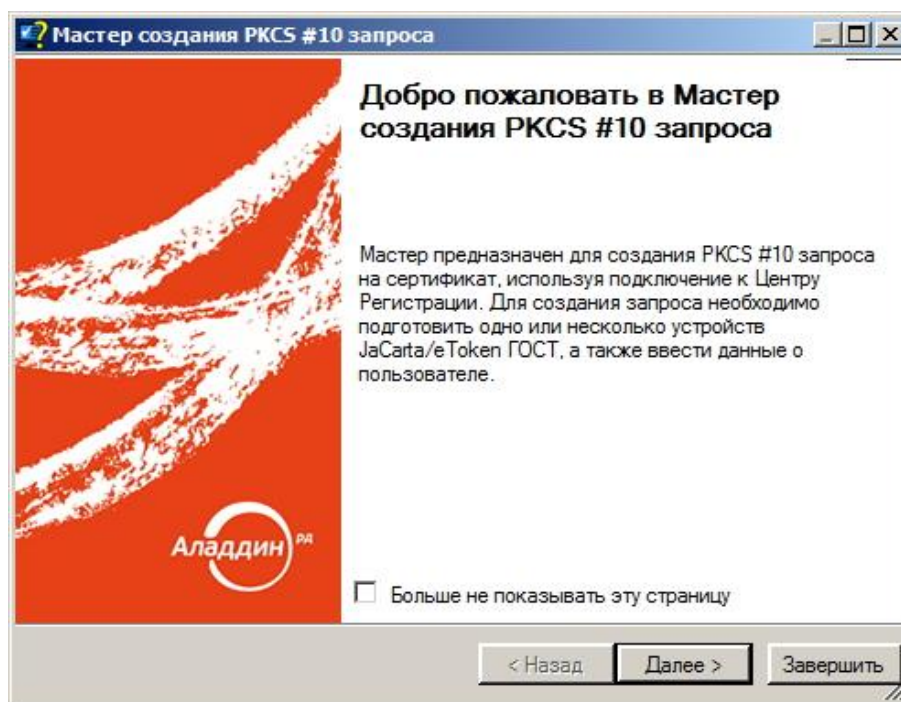


Рисунок 63

5. Выберите требуемый шаблон расширения и нажмите **Далее>** (см. Рис. 64)

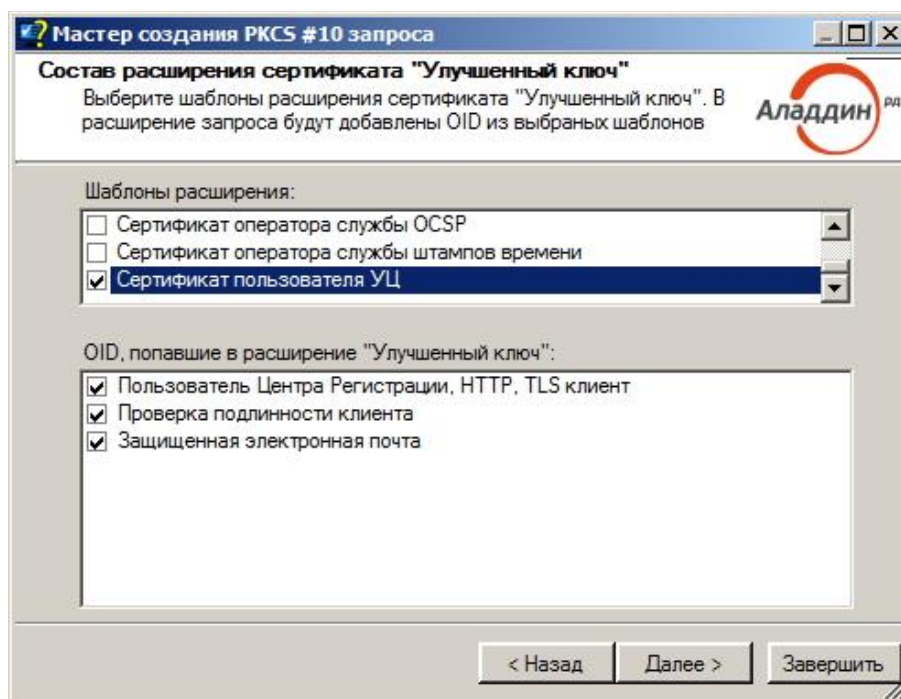


Рисунок 64

6. В появившемся окне выберите область использования и нажмите **Далее>** (см. Рис. 65).

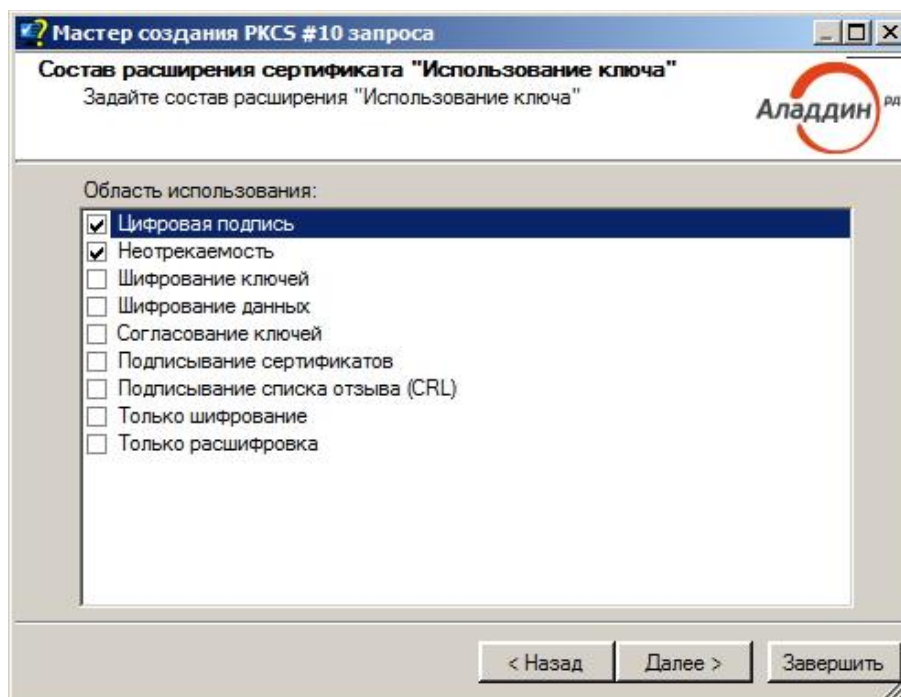


Рисунок 65

7. В появившемся окне заполните поля и нажмите **Далее>** (см. Рис. 66).

Фамилия	
Имя	
Должность/звание	
Адрес	
Общее имя (*)	Инициалы Фамилия
Подразделение	
Организация	
Город	
Область	
Страна/регион	
Электронная почта	

Общее имя (*)
Короткое наименование поля: CN
OID: 2.5.4.3

< Назад Далее > Завершить

Рисунок 66

8. В появившемся окне заполните поля и нажмите **Далее>** (см. Рис. 67).

Фамилия	
Бизнес-категория	
Название подразделения	
Название организации	ОАО "Организация"
Адрес e-mail	
Адрес URL	http://www.some-site.ru
Почтовый адрес	Москва, ул. Докукина
Дополнительное описание	Система защищенной электронной почты
Имя участника	

Название организации
Наименование поля: organizationName
OID: 2.5.4.10

< Назад Далее > Завершить

Рисунок 67

9. В появившемся окне заполните поля и нажмите **Далее>** (см. Рис. 68).

Мастер создания PKCS #10 запроса

Дополнительные сведения о пользователе
Укажите дополнительные сведения о пользователе, которые не будут входить в запрос на сертификат. Обязательные для заполнения поля помечены символом (*)

Аладдин РД

Когда выдано	
Кем выдано	
Номер паспорта (*)	2222333333

Номер паспорта (*)
Назначение поля: Серия и номер удостоверения личности

< Назад Далее > Завершить

Рисунок 68

10. В появившемся окне нажмите **Далее>** (см. Рис. 69).

Мастер создания PKCS #10 запроса

Данные пользователя
Проверьте корректность введенных данных.

Аладдин РД

Дополнительная информация

Номер паспорта (*)	2222333333
--------------------	------------

Компоненты поля запроса "Субъект"

Общее имя (*)	Инициалы Фамилия
---------------	------------------

Компоненты расширения "Альтернативное имя субъекта"

Название организации	ОАО "Организация"
Адрес URL	http://www.some-site.ru
Почтовый адрес	Москва, ул. Докукина
Дополнительное описание	Система защищенной электронной почты

Компоненты расширения "Использование ключа"

Цифровая подпись	Присутствует
Неотрекаемость	Присутствует

Компоненты расширения "Улучшенный ключ"

Пользователь Центра Регистрации	1.2.643.2.2.34.6
Проверка подлинности клиента	1.3.6.1.5.5.7.3.2

< Назад Далее > Завершить

Рисунок 69

11. В появившемся окне (см. Рис. 70) выделите электронный ключ, затем введите PIN-код пользователя электронного ключа и нажмите **Далее>**.



Примечание – Значение PIN-кода в окне по умолчанию: 1234567890. Если на токене установлен другой PIN-код, то следует ввести его.

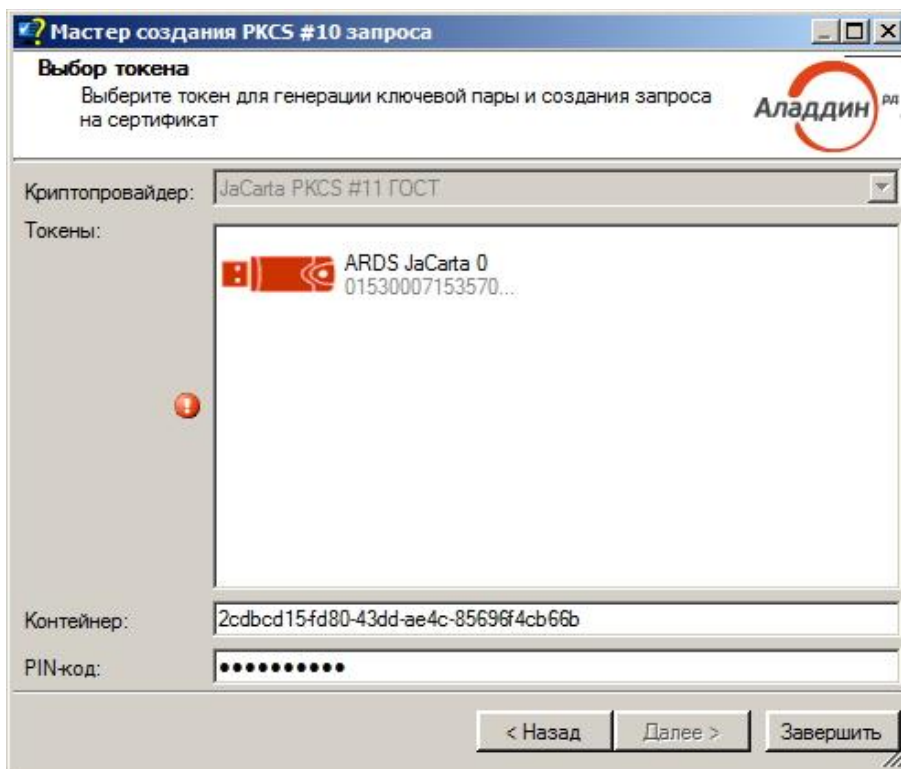


Рисунок 70

Появится окно создания запроса на сертификат (см. Рис. 71)

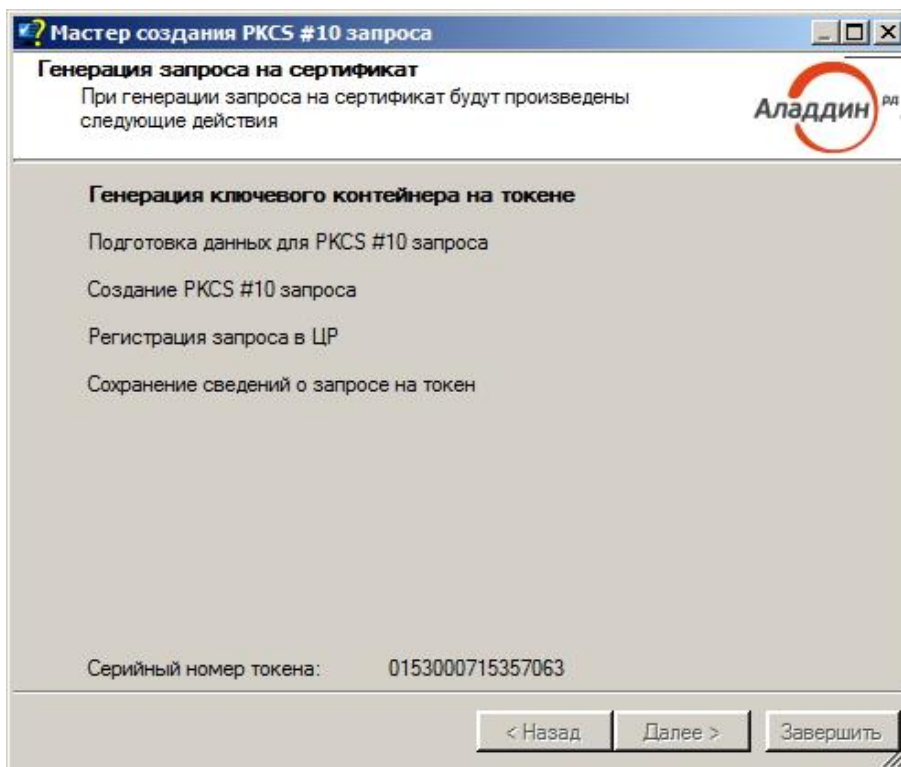


Рисунок 71

После создания запроса и формирования контейнера в памяти электронного ключа, появится сообщение о сохранении запроса в папке Online-запросов на компьютере, а также сохранении файла с расширением *.xml, содержащего пользовательские данные, не вошедшие в запрос (см. Рис. 72). Закройте окно программы мастера, нажав **Завершить**.

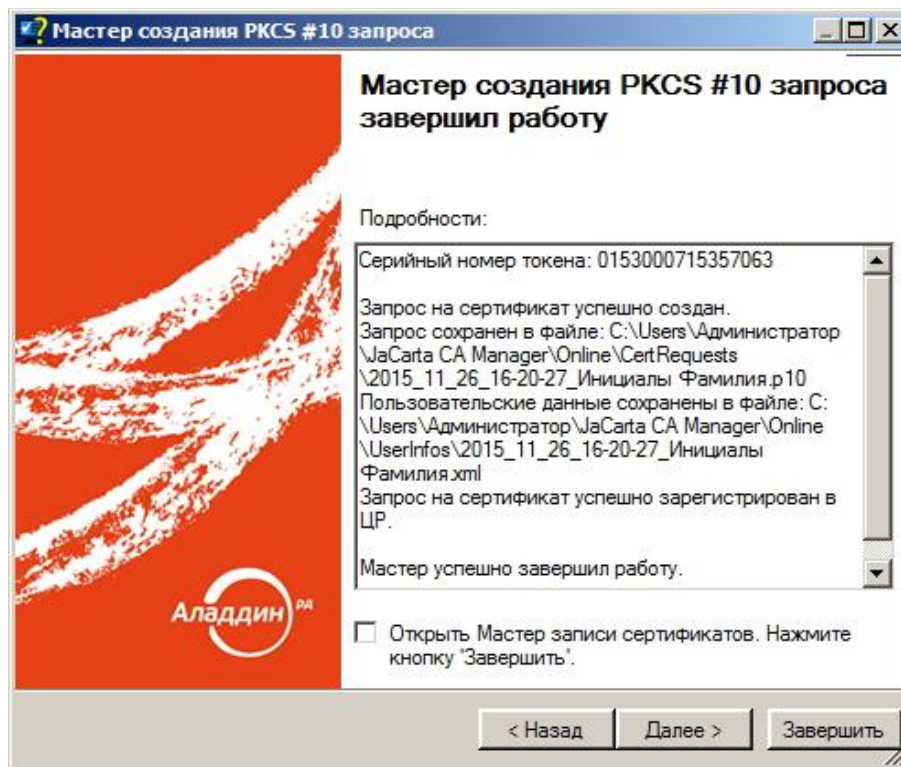



Рисунок 72

 **Примечание** – При выборе опции **Открыть Мастер записи сертификатов. Нажмите кнопку Завершить**, после нажатия на кнопку **Завершить** будет запущен Мастер записи сертификатов.

12. Перейдите в окно Запросы на сертификат и убедитесь, что запрос отправлен в ЦР (см. Рис. 73).

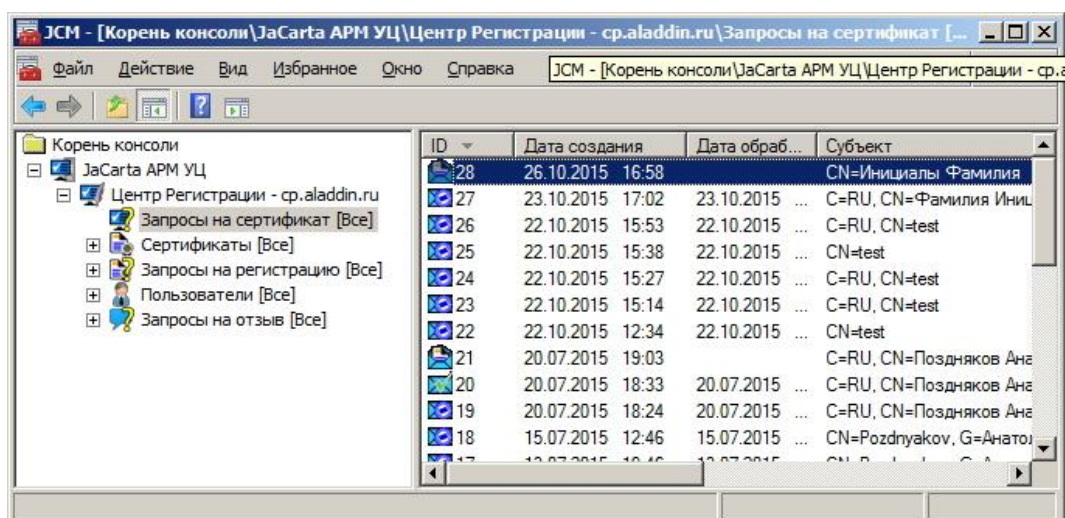


Рисунок 73



Примечание – После того, как в Центре Регистрации запрос на сертификат будет принят, значок запроса (см. Рис. 73 для запроса ID 28) изменится на другой (см. Рис. 74 для запроса ID 28). После этого станет возможным получение и запись сертификата по отправленному запросу.

5.2.2. Запись сертификата в память электронного ключа

Чтобы записать сертификат в память электронного ключа в автоматическом режиме выполните следующие действия:

1. Нажмите правой кнопкой мыши на Запросы на сертификат и из появившегося контекстного меню выберите **Получить готовый сертификат** (см. Рис. 74).

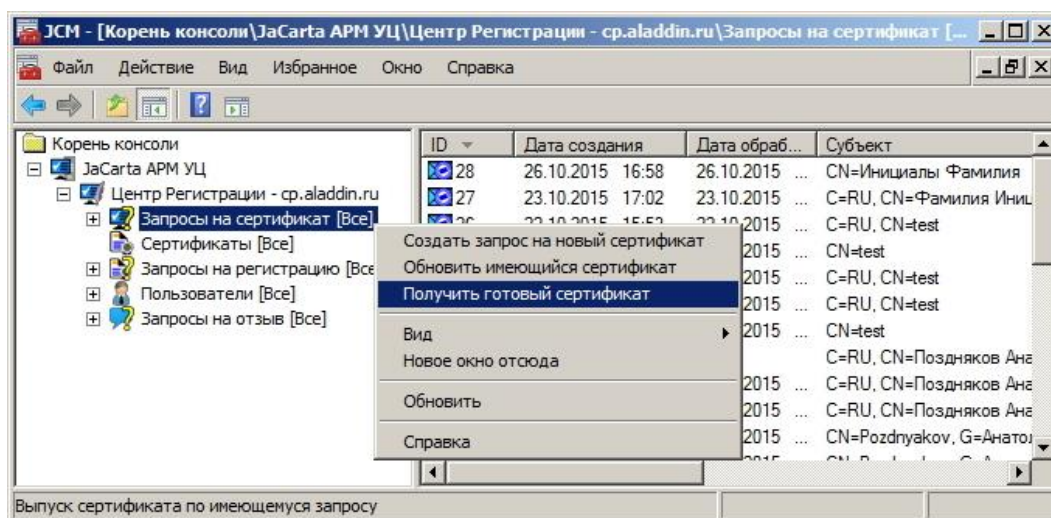


Рисунок 74

2. В появившемся окне нажмите **Далее>** (см. Рис. 75).

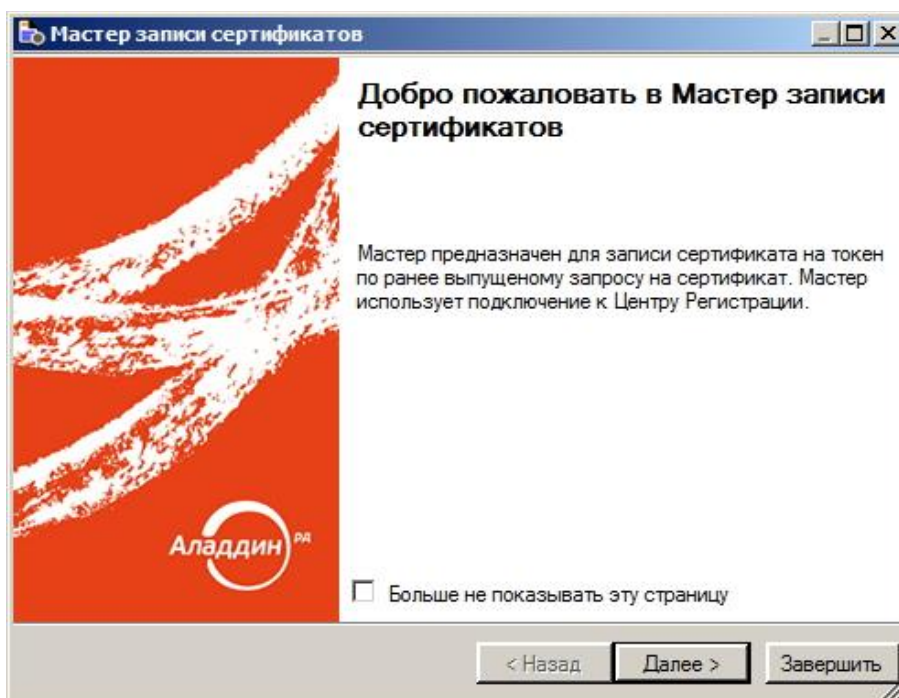



Рисунок 75

3. В появившемся окне введите PIN-код и нажмите **Далее** (см. Рис. 76).

 **Примечание** – Значение PIN-кода в окне по умолчанию: 1234567890. Если на токене установлен другой PIN-код, то следует ввести его.

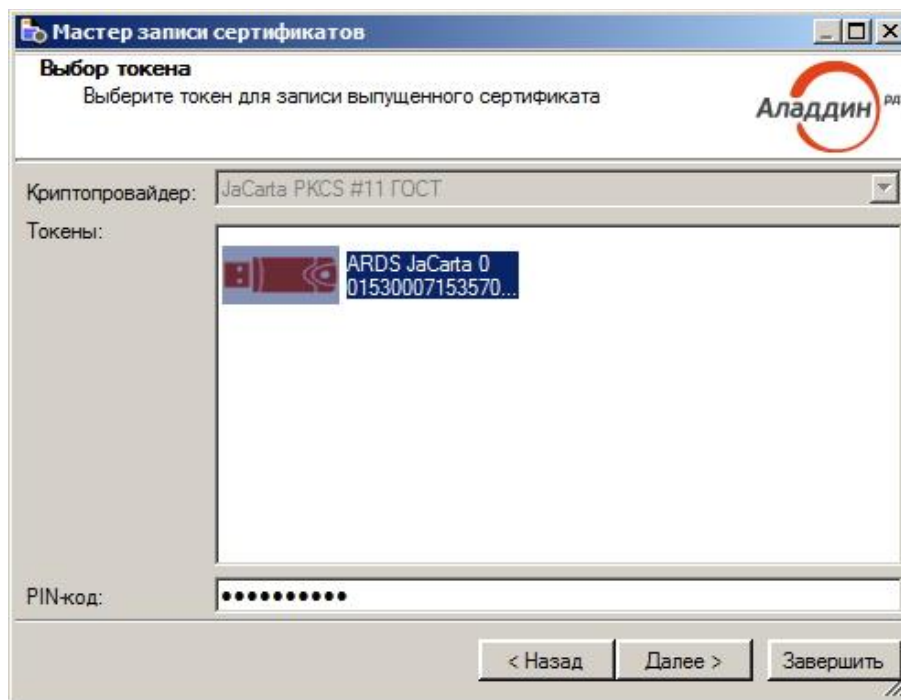


Рисунок 76

Появится окно записи сертификата на токен (см. Рис. 77). Дождитесь окончания записи.

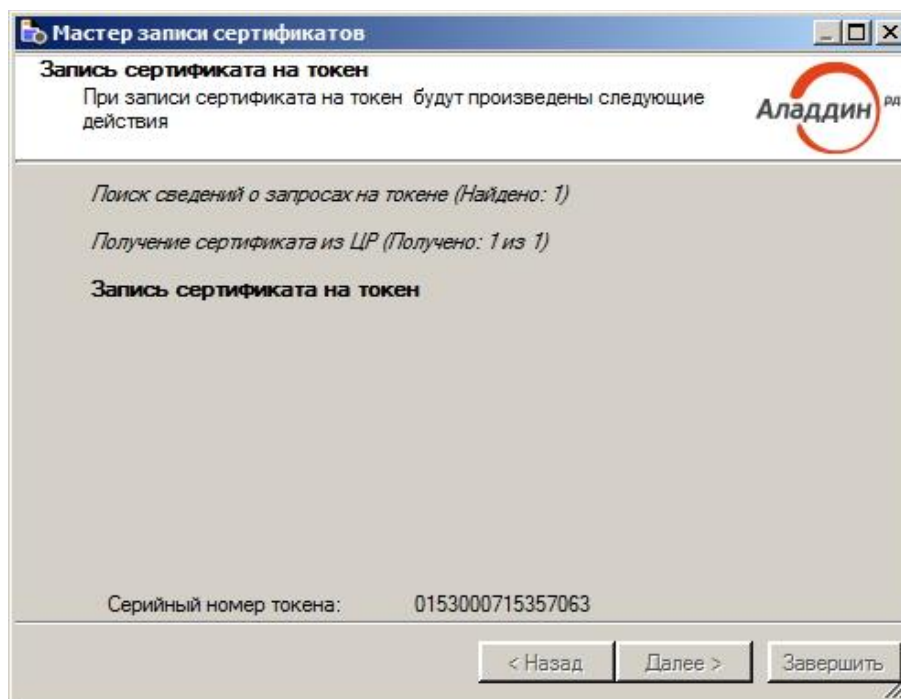


Рисунок 77

4. В появившемся окне нажмите **Завершить** (см. Рис. 78).

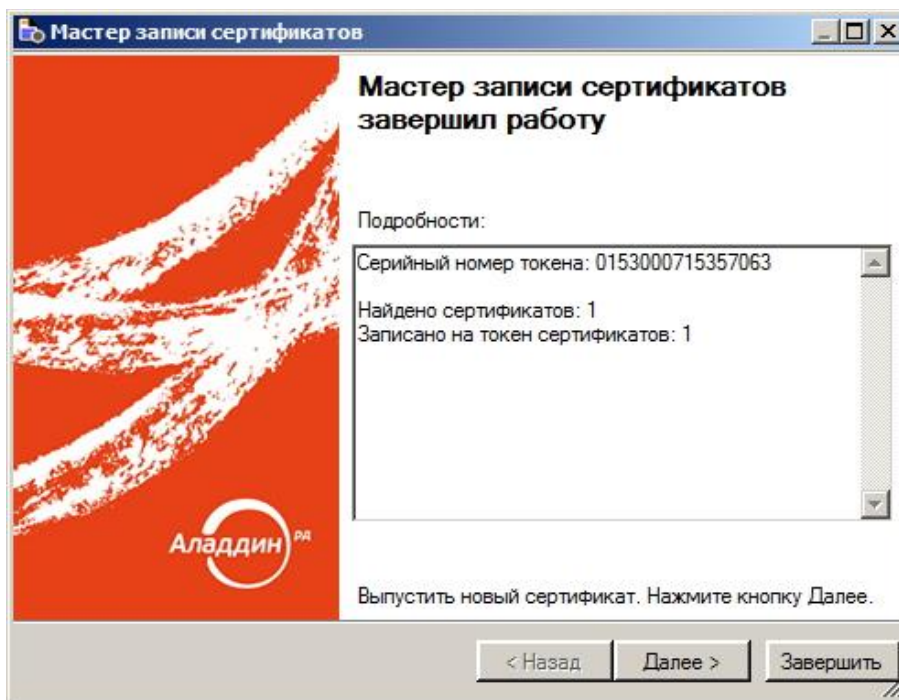


Рисунок 78

5.3. Обновление сертификата для существующего пользователя

Для обновления сертификата существующего пользователя выполните следующие действия:

1. Нажмите правой кнопкой мыши на Запросы на сертификат и из появившегося контекстного меню выберите **Обновить имеющийся сертификат** (см. Рис. 79).

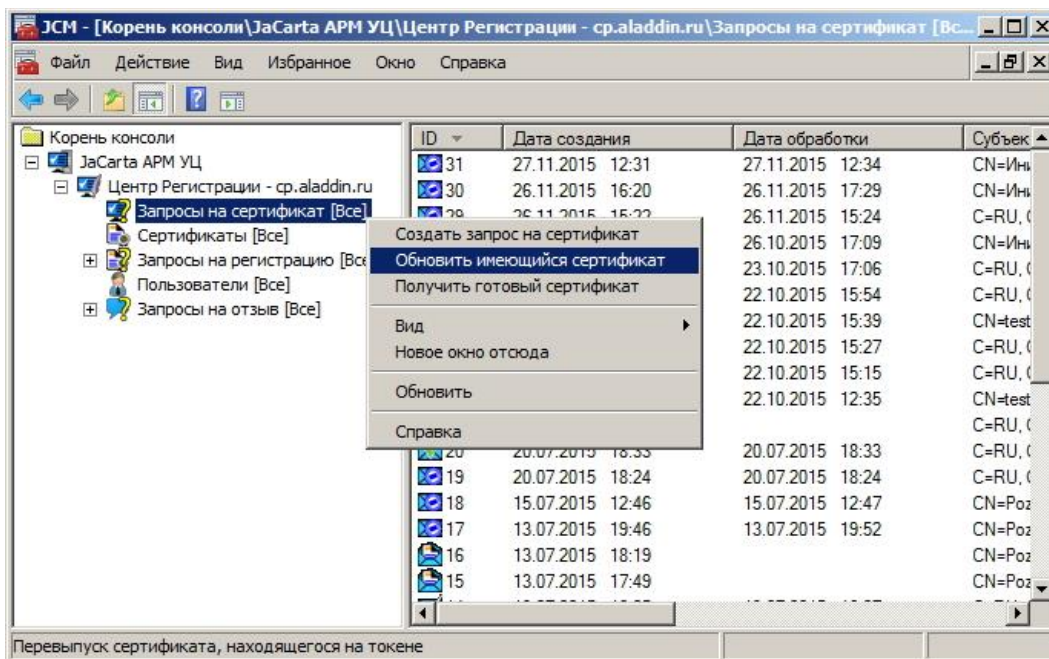


Рисунок 79

2. В появившемся окне нажмите **Далее>** (см. Рис. 80).

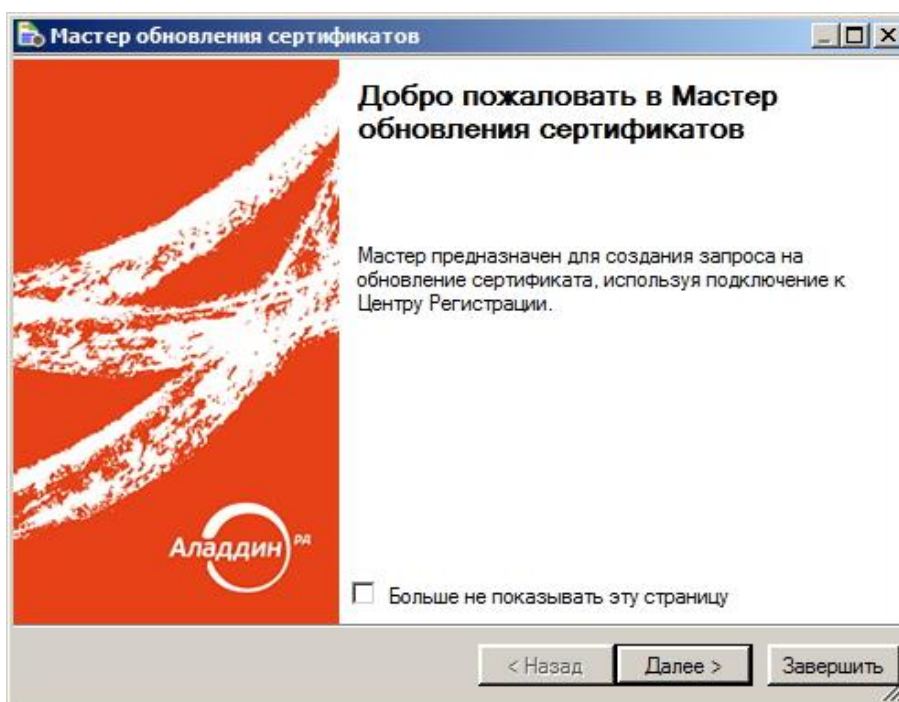


Рисунок 80

3. В появившемся окне (см. Рис. 81) выберите сертификат, который следует обновить на токене и нажмите **Далее>**.

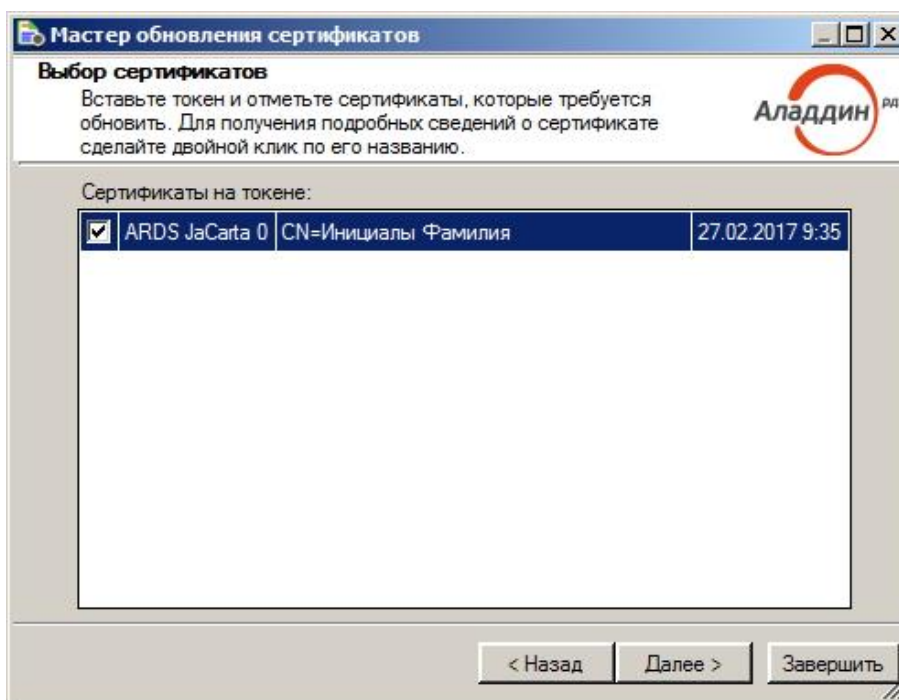


Рисунок 81

4. В появившемся окне (см. Рис. 82) введите PIN-код и нажмите **ОК**.

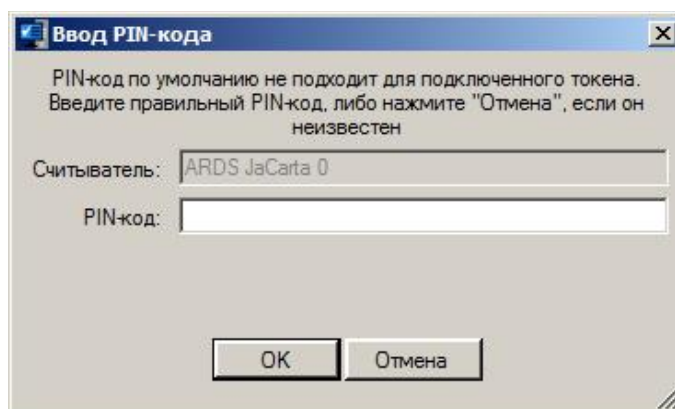


Рисунок 82

5. В появившемся окне (см. Рис. 83) будут выполнены необходимые действия.

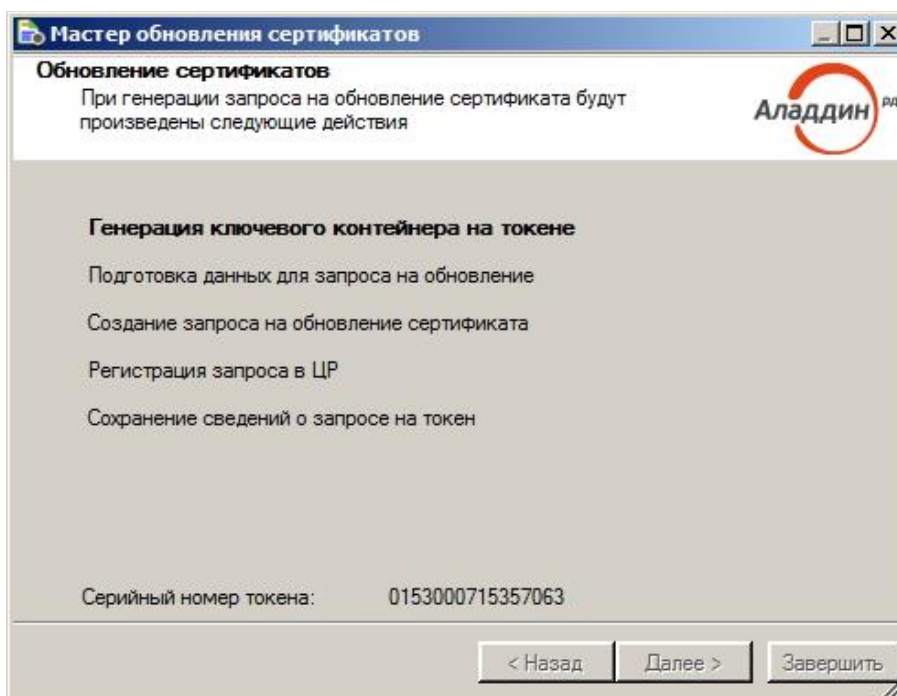


Рисунок 83

6. После окончания (см. Рис.84) генерации запроса на обновление в появившемся окне нажмите **Завершить**.

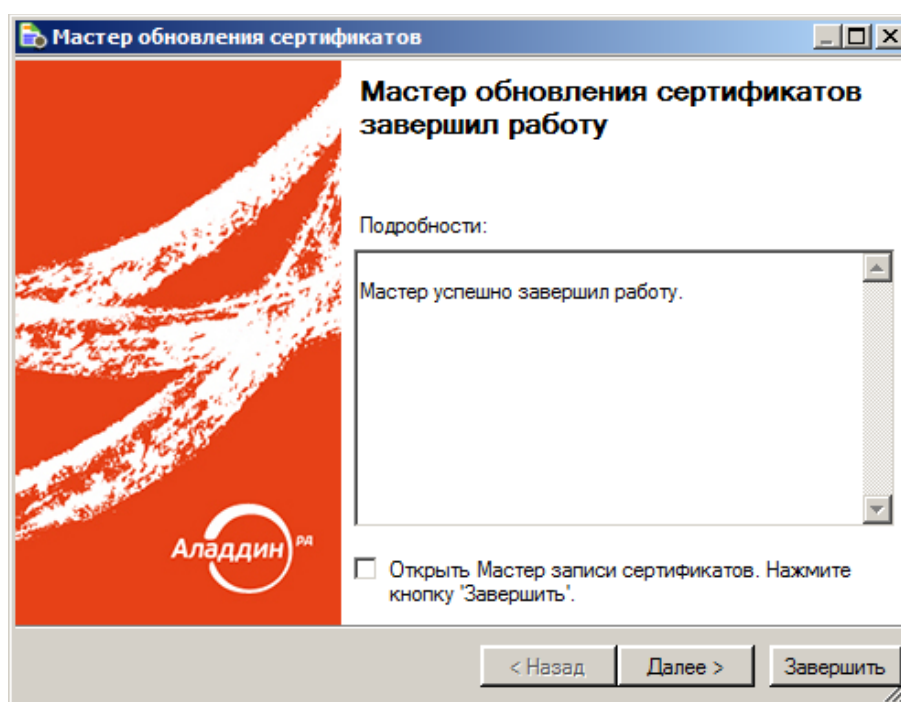


Рисунок 84

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 (общий)

Web: www.aladdin-rd.ru

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

Техническая поддержка

Подробные правила оказания технической поддержки описаны на сайте компании "Аладдин Р.Д.":

<https://www.aladdin-rd.ru/support/rules/>

Оказание базовой технической поддержки осуществляется только через форму заявки, размещённую в разделе "Создание нового обращения" на сайте компании.

Оказание помощи по телефону без заключенного договора расширенной технической поддержки доступно в экстренных случаях (полная неработоспособность системы из-за проблем с USB-токенами и смарт-картами).

Время работы Службы технической поддержки - с 10:00 до 19:00 (по московскому времени), кроме выходных и праздничных дней.

Выходные дни: суббота и воскресенье.

Телефон: (495) 223-0001 (многоканальный)

Компания "Аладдин Р.Д." оказывает базовую техническую поддержку по всем выпускаемым продуктам по текущей и, как правило, по предшествующей версиям. Базовая техническая поддержка входит в стоимость всех поставляемых продуктов, по умолчанию, на 1 год.

В случае возникновения вопросов по установке или использованию продукта рекомендуется обратиться к разделам сайта компании "Аладдин Р.Д.": Часто задаваемые вопросы (FAQ) и База знаний.

Регистрация изменений

Версия	Изменения
1.1	Замена скриншотов для ПО Единый Клиент Ja Carta версии 2.11.
1.0	<i>Создание документа</i>



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/МСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer

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

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