Единый клиент JaCarta

Руководство администратора

Версия: 1.2

Редакция от: 23 ноября 2015 г.

Листов: 97

Аннотация

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

В настоящем Руководстве приведены общие сведения, системные требования, режимы работы, порядок и содержание действий по установке и удалению Единого клиента JaCarta, обзор пользовательского интерфейса, сведения по изменению настроек, инициализации электронных ключей, установке PIN-кода, операциях с объектами в памяти электронных ключей и др.

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

Содержание

1. Общие сведения

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

1.1. Термины и определения

Термины, используемые в настоящем Руководстве приведены в таблице 1.

Таблица 1

Термин	Определение
Пользователь	Конечный пользователь электронного ключа
PIN-код пользователя	PIN-код, предоставляющий доступ к операциям на уровне доступа пользователя
Администратор	Сотрудник, отвечающий за подготовку к работе и техническое обслуживание электронного ключа
PIN-код администратора	PIN-код, предоставляющий доступ к операциям на уровне администратора
Инициализация	Установка основных параметров работы электронного ключа (подготовка к работе)
Приложение	Программное обеспечение, установленное в память электронного ключа. Существуют следующие приложения: • PKI; • PKI/BIO; • ГОСТ; • STORAGE; • ФКН. PIN-код пользователя и PIN-код администратора действуют в рамках приложения. Таким образом, если на электронном ключе установлены два приложения, для каждого из них могут присутствовать свои PIN-код пользователя и PIN-код администратора.

Таблица 1

Внимание!

Не допускайте блокировки PIN-кода администратора на электронных ключах JaCarta. PIN-код администратора, в отличие от PIN-кода пользователя, разблокировать невозможно.

1.2. Режимы работы Единого клиента JaCarta

Единый клиент JaCarta может работать в двух режимах:

1. Режим пользователя – позволяет просматривать краткие сведения о подсоединённых электронных ключах и предоставляет доступ к базовым операциям с электронными ключами.
2. Режим администратора – позволяет просматривать полные сведения о подсоединённых электронных ключах и предоставляет доступ ко всем операциям с электронными ключами.

1.3. Сведения об электронных ключах

1.3.1. Параметры электронных ключей при поставке

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

Таблица 2

Параметры	Модели электронных ключей:				
	eToken PRO **eToken PRO (Java)** **eToken NG-FLASH** **eToken NG-FLASH (Java)** **eToken NG-OTP** **eToken NG-OTP (Java)** **JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin**	**JaCarta PKI** **JaCarta PKI/Flash** **JaCarta PKI/BIO**	**JaCarta ГОСТ/Flash** **JaCarta ГОСТ** **eToken ГОСТ**	**JaCarta LT**	**JaCarta CryptoPro**
Приложение	PKI	PKI и PKI/BIO	ГОСТ	STORAGE	ФКН
PIN-код пользователя по умолчанию	1234567890	11111111	Не установлен	1234567890	Нет
PIN-код администратора по умолчанию	1234567890	00000000	1234567890	1234567890	Нет
Можно инициализировать без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после инициализации)	Да	Да	Да	Нет	Нет
Можно инициализировать без назначения PIN-кода администратора	Да	Нет	Нет	Только при первичной инициализации	Нет
Поведение ключа при разблокировке PIN-кода пользователя[1]	Во время разблокировки администратор задаёт новый PIN-код пользователя		Разблокировка сбрасывает счётчик неверных попыток доступа – PIN-код пользователя при этом остаётся неизменным		Нет
Можно разблокировать PIN-код пользователя в удалённом режиме	Да	Да	Нет	Нет	Нет
Администратор может сменить установленный PIN-код пользователя без инициализации	Да	Да	Нет	Нет	Нет

Таблица 2

[1] *В случае с электронными ключами JaCarta PKI/BIO при разблокировке биометрического доступа пользователь вновь получает возможность аутентифицироваться по ранее сохранённому отпечатку пальца.*

1.3.2. Операции с электронными ключами

Доступные операции с электронными ключами, с указанием нужного режима работы и необходимости аутентификации для совершения операции приведены в таблице 3.

Таблица 3

<table>
<tr><th>Операция</th><th>Приложение</th><th>Режим работы Единого клиента JaCarta</th><th>Аутентификация</th></tr>
<tr><td rowspan="6">Инициализация</td><td>PKI на следующих электронных ключах:
eToken PRO
eToken PRO (Java)
eToken NG-FLASH
eToken NG-FLASH (Java)
eToken NG-OTP
eToken NG-OTP (Java)
JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin
JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin</td><td>Режим администратора</td><td>Не требуется</td></tr>
<tr><td>PKI на следующих электронных ключах:
JaCarta PKI
JaCarta PKI/Flash
JaCarta PKI/ГОСТ</td><td rowspan="3">Режим администратора</td><td rowspan="3">PIN-код администратора</td></tr>
<tr><td>PKI/BIO</td></tr>
<tr><td>ГОСТ</td></tr>
<tr><td>STORAGE</td><td></td><td></td></tr>
<tr><td>ФКН</td><td colspan="2">Недоступно</td></tr>
<tr><td rowspan="5">Установка (смена) PIN-кода пользователя администратором</td><td>PKI</td><td rowspan="2">Режим администратора</td><td rowspan="2">PIN-код администратора</td></tr>
<tr><td>PKI/BIO</td></tr>
<tr><td>ГОСТ</td><td colspan="2" rowspan="3">Недоступно</td></tr>
<tr><td>STORAGE</td></tr>
<tr><td>ФКН</td></tr>
<tr><td rowspan="5">Смена своего PIN-кода пользователем</td><td>PKI</td><td rowspan="4">Режим пользователя</td><td rowspan="4">PIN-код пользователя</td></tr>
<tr><td>PKI/BIO</td></tr>
<tr><td>ГОСТ</td></tr>
<tr><td>STORAGE</td></tr>
<tr><td>ФКН</td><td colspan="2">Недоступно</td></tr>
<tr><td rowspan="4">Смена своего PIN-кода администратором</td><td>PKI</td><td rowspan="4">Режим администратора</td><td rowspan="4">PIN-код администратора</td></tr>
<tr><td>PKI/BIO</td></tr>
<tr><td>ГОСТ</td></tr>
<tr><td>STORAGE</td></tr>
</table>

Операция	Приложение	Режим работы Единого клиента JaCarta	Аутентификация
	ФКН	Недоступно	
Смена отпечатков пальцев	PKI	Недоступно	
	PKI/BIO	Режим администратора	PIN-код администратора
	ГОСТ	Недоступно	
	STORAGE		
	ФКН		
Разблокировка PIN-кода пользователя	PKI	Режим администратора	PIN-код администратора
	PKI/BIO		
	ГОСТ		
	STORAGE		
	ФКН	Недоступно	
Операции с объектами в памяти электронных ключей[2]	PKI	Режим администратора	PIN-код пользователя
	PKI/BIO		
	ГОСТ		
	STORAGE		
	ФКН		
Просмотр кратких сведений о подсоединённом электронном ключе	PKI	Режим пользователя	Не требуется
	PKI/BIO		
	ГОСТ		
	STORAGE		
	ФКН		
Просмотр полных сведений о подсоединённом электронном ключе	PKI	Режим администратора	Не требуется
	PKI/BIO		
	ГОСТ		
	STORAGE		
	ФКН		
Создание запроса на сертификат	PKI	Режим администратора	PIN-код пользователя
	PKI/BIO		
	ГОСТ		
	STORAGE	Недоступно	
	ФКН		

Таблица 3

[2] *В случае с электронными ключами ФКН поддерживаются операции только с контейнерами CryptoPro*

2. Описание пакетов установки

Дистрибутив Единого клиента JaCarta включает пакеты установки, приведенные в таблице 4.

Таблица 4

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 4

3. Системные требования

Внимание! Перед установкой Единого клиента JaCarta убедитесь в том, что компьютер соответствует минимальным требованиям. Системные требования приведены в таблице 5.

Таблица 5

Требование	Содержание
Поддерживаемые операционные системы	Windows XP SP3 (32-бит) Windows XP SP2 (64-бит) Windows Vista SP2 (32/64-бит) Windows 7 SP1 (32/64-бит) Windows 8 (32/64-бит) Windows 8.1 Update 1 (32/64-бит) Windows 10 (32/64-бит) Windows Server 2003 SP2 (32/64-бит) Windows Server 2008 SP2 (32/64-бит) Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2
Поддерживаемые модели электронных ключей	Электронные ключи eToken: • eToken Anywhere • eToken CryptoPro • eToken PRO • eToken PRO (Java) • eToken NG-FLASH • eToken NG-FLASH (Java) • eToken NG-OTP • eToken NG-OTP (Java) • eToken ГОСТ Электронные ключи JaCarta: • JaCarta CryptoPro • JaCarta PKI • JaCarta PKI/Flash • JaCarta PKI/BIO • JaCarta PKI/BIO/ГОСТ • JaCarta PKI/ГОСТ • JaCarta PKI/ГОСТ/Flash • JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin • JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin • JaCarta ГОСТ/Flash • JaCarta ГОСТ • JaCarta LT
Необходимые аппаратные средства	USB-порт (для токенов). Для смарт-карт необходимо наличие подключённого считывателя смарт-карт. Для электронных ключей в форм-факторе microSD можно использовать следующее оборудование: • разъём microSD; • разъём SD через переходник microSD-to-SD; • USB-порт через переходник microSD-to-USB. Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование: • USB-порт через переходник microUSB-to-USB.
Рекомендуемое разрешение экрана	Для корректного отображения интерфейса Единого клиента JaCarta рекомендуется установить разрешение монитора не ниже 1024x768
Дополнительное ПО	Для использования электронных ключей eToken, а так же для использования полной функциональности электронных ключей JaCarta PKI и JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin необходимо, чтобы на

Требование	Содержание
	компьютере был установлен eToken PKI Client 5.1 SP1/SafeNet Authentication Client версии 8.0 SP2 и выше. Для использования электронных ключей eToken CryptoPro и JaCarta CryptoPro необходимо, чтобы на компьютере было установлено Программное обеспечения для работы с СКЗИ КриптоПро ФКН CSP.
ПО, которое необходимо удалить перед установкой Единого клиента JaCarta	Если на компьютере установлено следующее программное обеспечение, удалите его до установки Единого клиента JaCarta: • CCID Fix; • Модуль поддержки для Signal-COM CSP (eToken for Signal-COM CSP); • JC-PROClient; • Модуль поддержки JaCarta BIO для CriptoPro CSP (CryptoPRO BIO); • Athena Micro SD Driver; • Модуль поддержки для CPRO JSP (JaCarta for CryptoPro JCP); • USB eToken Driver.

Таблица 5

4. Установка Единого клиента JaCarta

Внимание! Перед установкой Единого клиента JaCarta убедитесь в том, что компьютер соответствует требованиям, приведенным в таблице 5.

Во избежание возникновения критической системной ошибки не устанавливайте в режиме "silent mode" (в том числе через групповые политики) версию ПО Единый клиент JaCarta 2.6.6.929 поверх версии ПО Единый клиент JaCarta 2.7.0.X и выше. Это может привести к нежелательным последствиям вплоть до возникновения BSOD.

Внимание! ПО Единый клиент JaCarta уже содержит модуль JC-Client, поэтому не рекомендуется устанавливать ПО JC-Client на компьютер с установленным Единым клиентом JaCarta. Отдельная дополнительная установка JC-Client может нарушить настройки Единого клиента JaCarta и вызвать ошибки при последующих установках и удалениях этих приложений.

Чтобы установить Единый клиент JaCarta выполните следующие действия:

1. В зависимости от разрядности операционной системы запустите нужный файл установки (см. раздел 2. Описание пакетов установки).

Если на компьютере не установлен eToken PKI Client/SafeNet Authentication Client, отобразится следующее окно (см. рис. 1).

Предупреждение об отсутствии eToken PKI Client/SafeNet Authentification Client

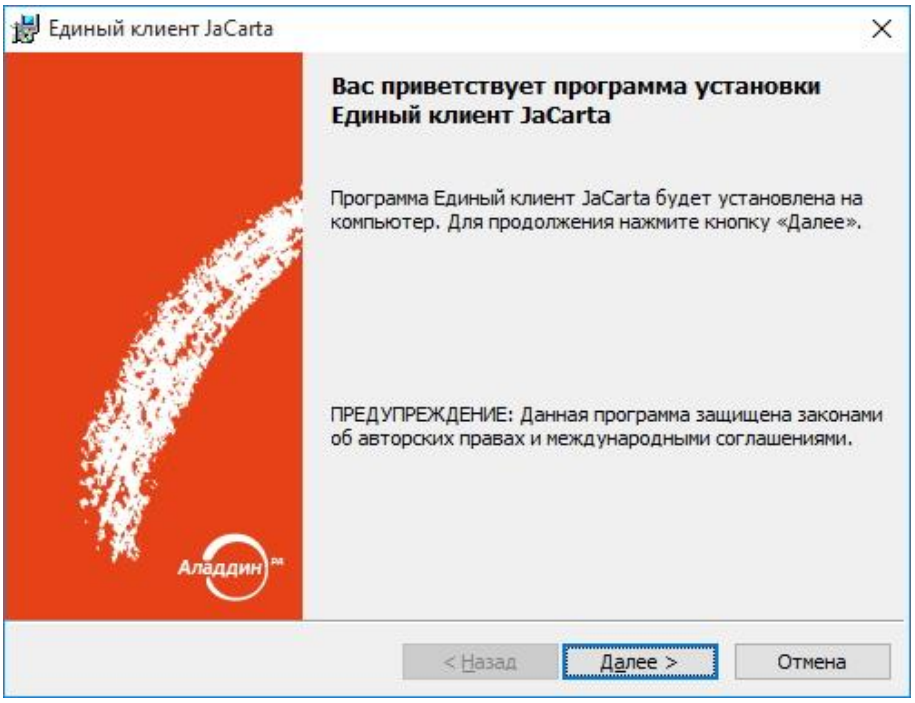

Рисунок 1

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

Окно приветствия мастера установки Единого клиента JaCarta

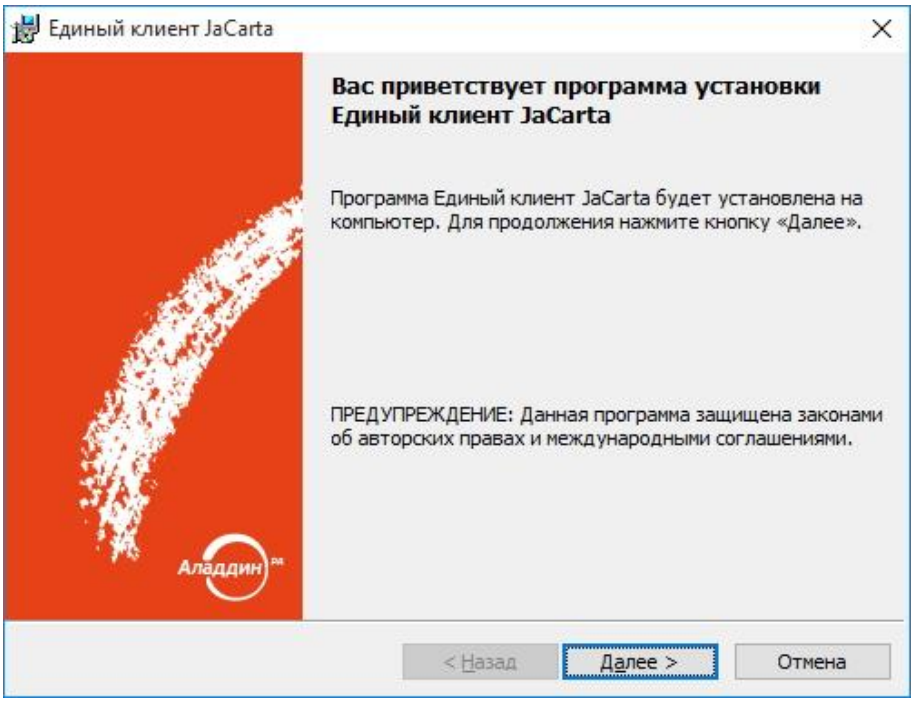

Рисунок 2

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

Окно лицензионного соглашения

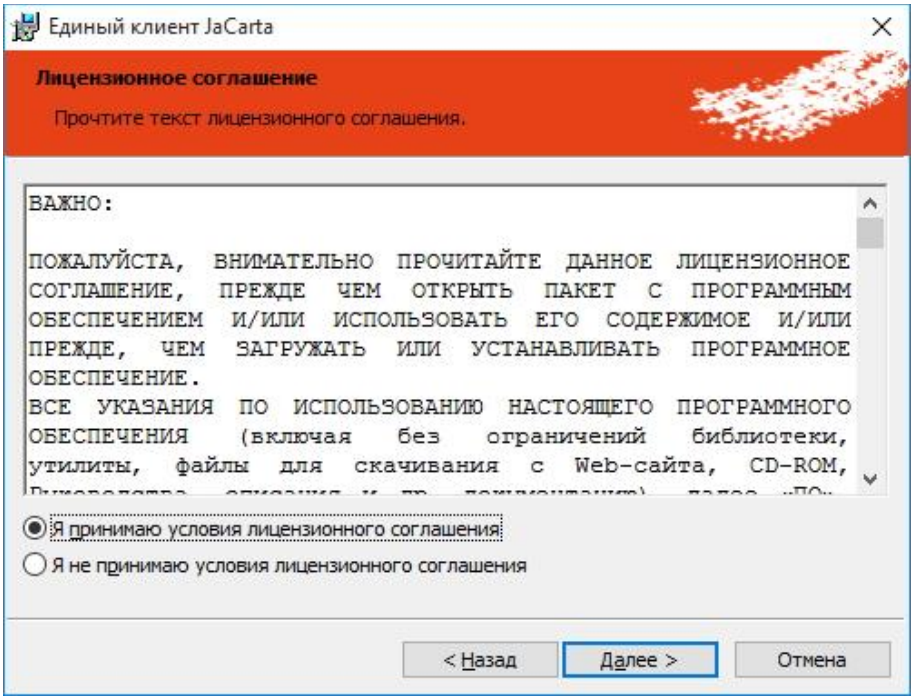

Рисунок 3

4. Прочитайте лицензионное соглашение

4.1. Если вы не согласны с условиями лицензионного соглашения, прекратите установку, нажав **Отмена**.

4.2. Если вы согласны с условиями лицензионного соглашения, выберите пункт **Я принимаю условия лицензионного соглашения** и нажмите **Далее >**. Отобразится следующее окно (см. рис. 4).

Окно выбора пути и вида установки Единого клиента JaCarta

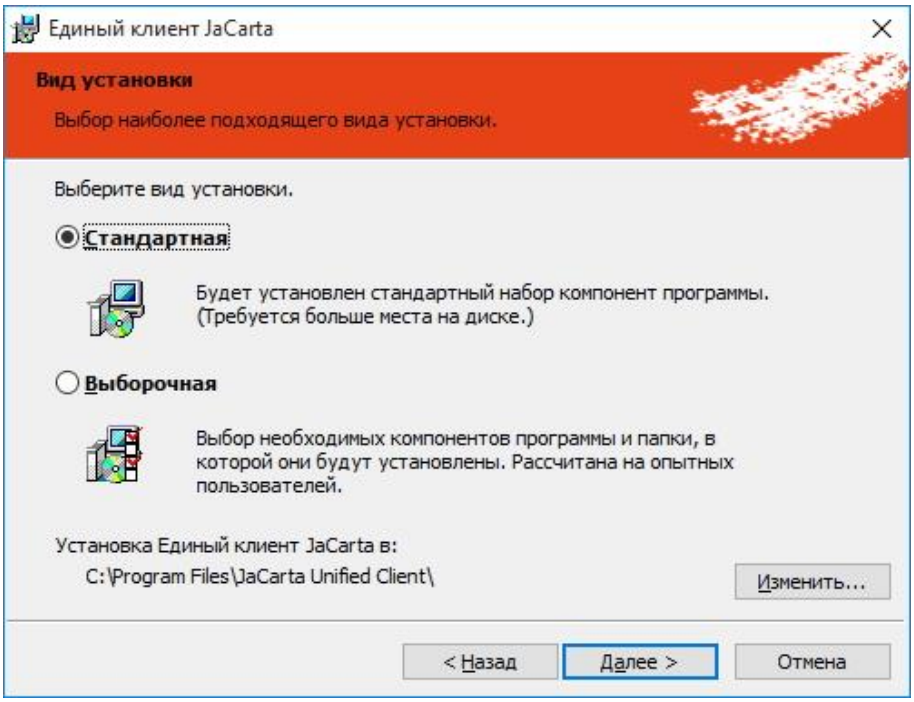

Рисунок 4

5. Выберите вид установки: **Стандартная** или **Выборочная**.
6. При необходимости воспользуйтесь кнопкой **Изменить…**, чтобы изменить путь установки Единого клиента JaCarta.
7. Нажмите **Далее >**. Если был выбран вид установки **Стандартная**, отобразится окно (см. рис. 5). Если был выбран вид установки **Выборочная**, отобразится окно (см. рис. 6 и рис. 7).

Установка стандартного набора компонент Единого клиента JaCarta

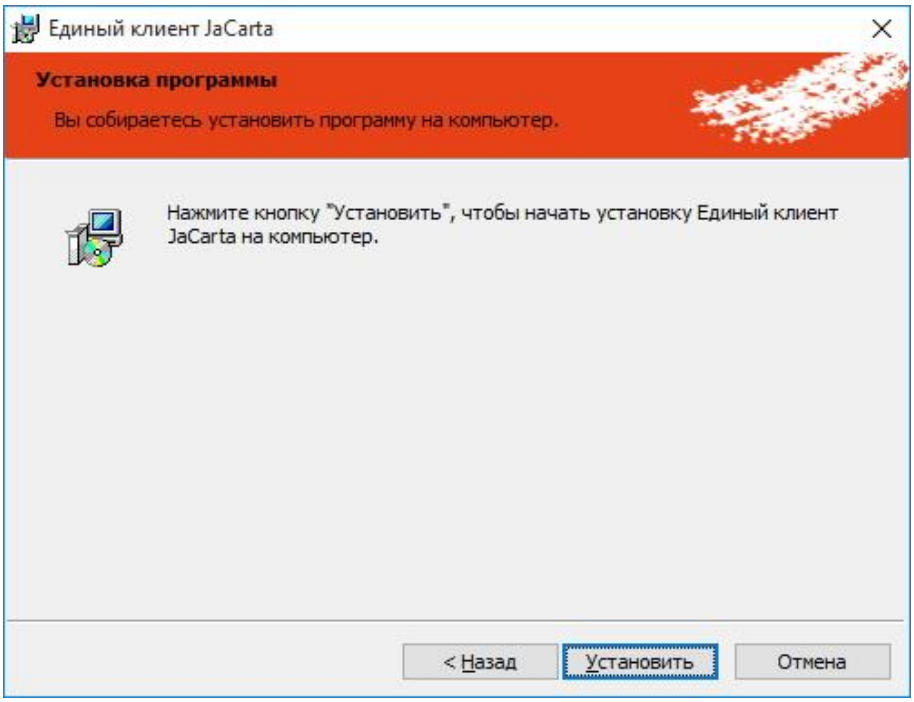

Рисунок 5

Выборочная установка компонент Единого клиента JaCarta

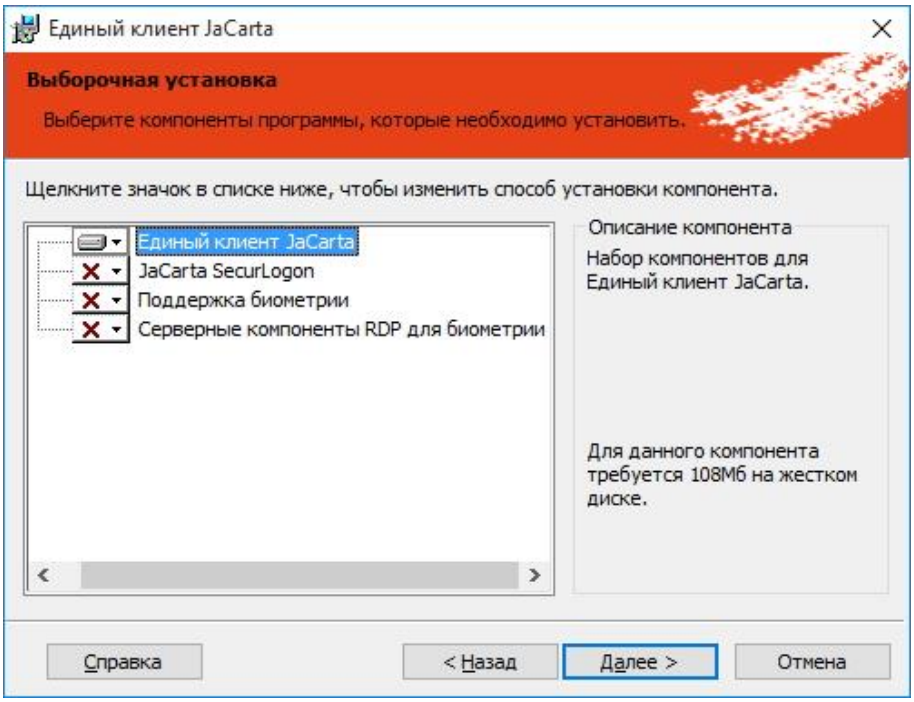

Рисунок 6

Выбор способа автоматического обновления при выборочной установке Единого клиента JaCarta

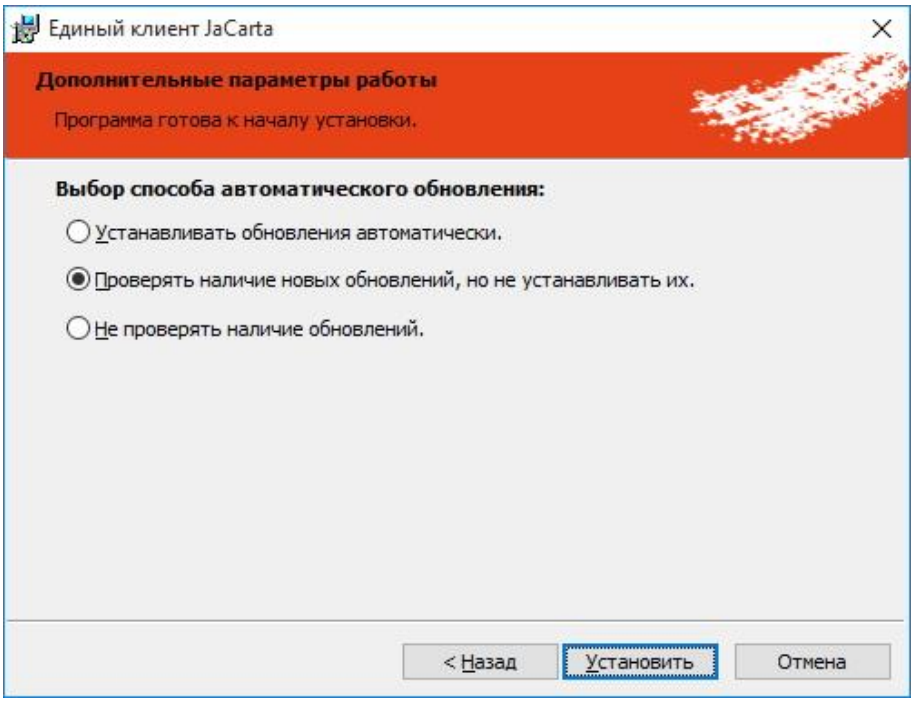

Рисунок 7

8. Нажмите **Установить** и дождитесь окончания установки.

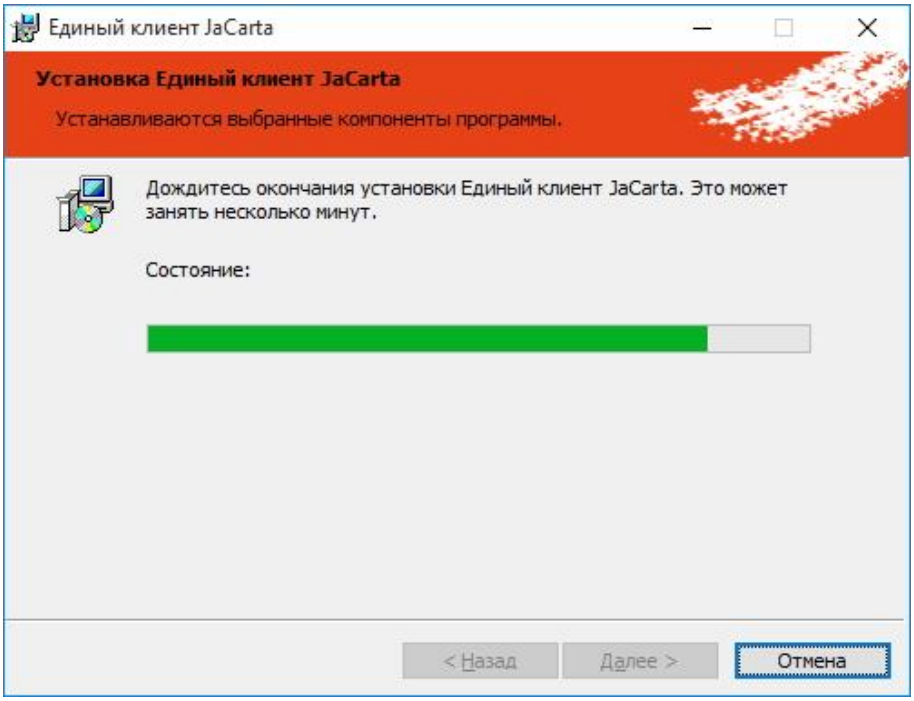

Рисунок 8

9. По завершении установки отобразится следующее окно (см. рис. 9).

Окно завершения установки Единого клиента JaCarta

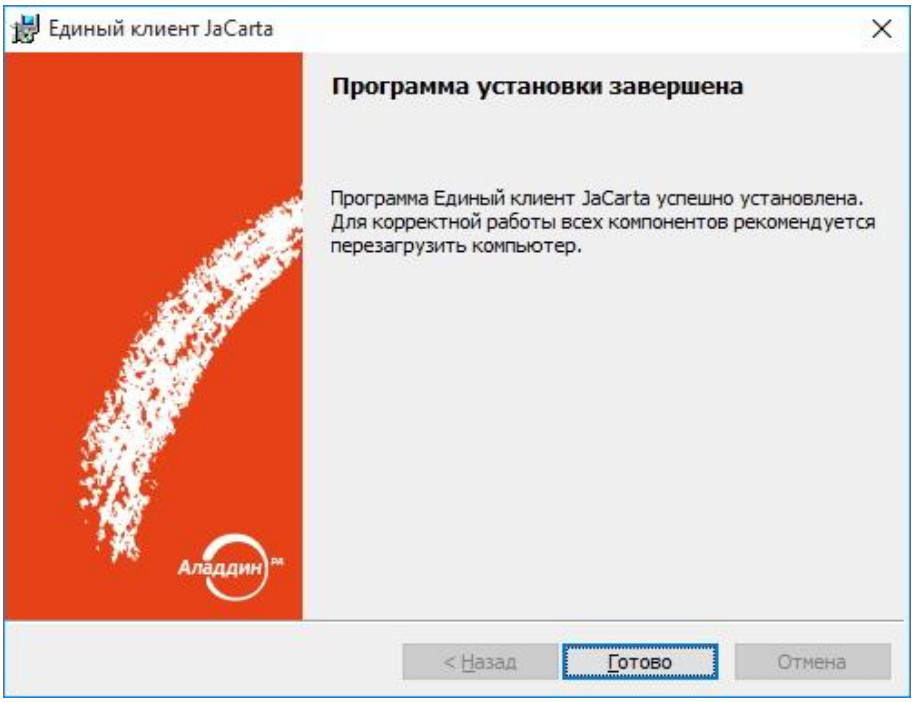

Рисунок 9

10. Нажмите **Готово.**
11. Перезагрузите компьютер, если отобразится соответствующее предупреждение.

Внимание!

Для использования электронных ключей eToken необходимо, чтобы на компьютере был так же установлен eToken PKI Client 5.1 SP1 или SafeNet Authentication Client версии 8.0 SP2 и выше.

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

Особенности установки Единый клиент JaCarta на ОС Windows XP с установленным антивирусом Dr.Web

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

1. Запустить **SpIDer Agent**, нажав значок на панели задач в области уведомлений.
2. Разблокировать **SpIDer Agent** для внесения изменений нажав кнопку (см. рис.10).

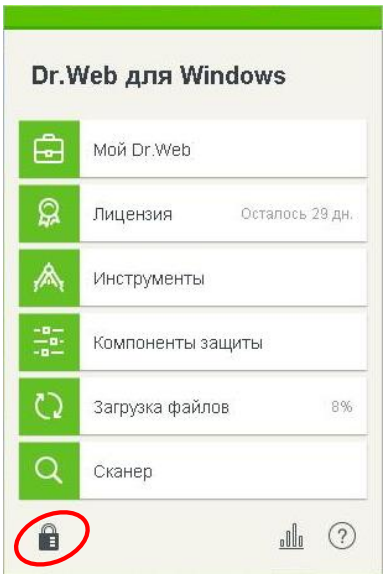

Рисунок 10

3. В появившемся окне нажать значок Настройки (см. рис. 11).

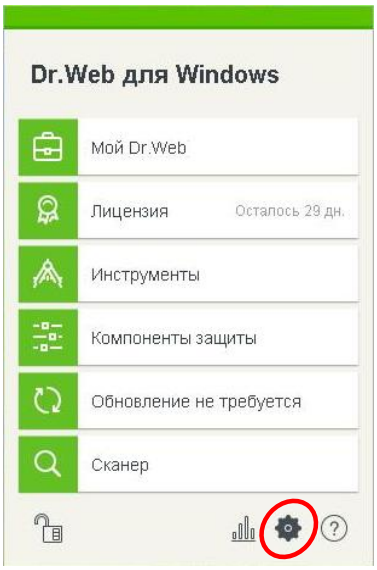

Рисунок 11

4. В появившемся окне выбрать опцию **Компоненты защиты** (см. рис. 12).

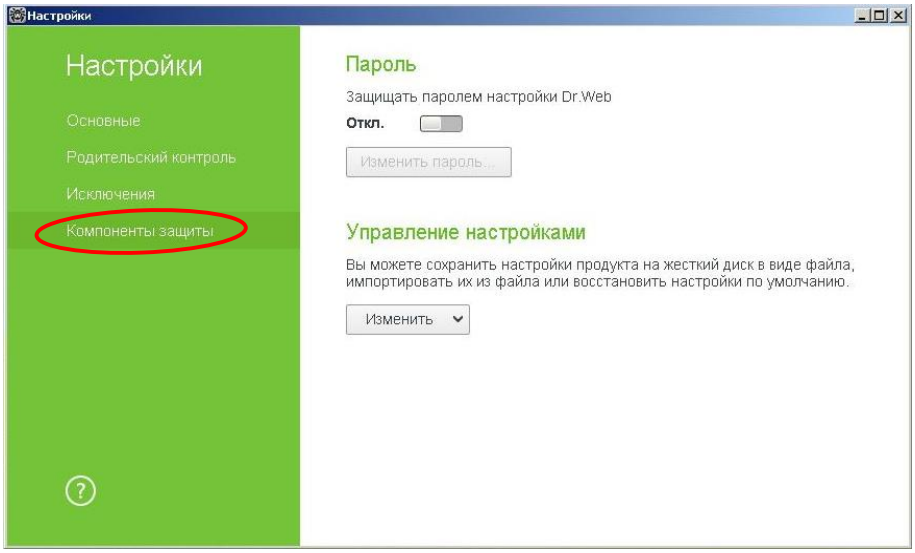

Рисунок 12

5. В появившемся окне выбрать опцию **Превентивная защита** и установить параметр **Разрешать** в соответствии с рисунком 13.

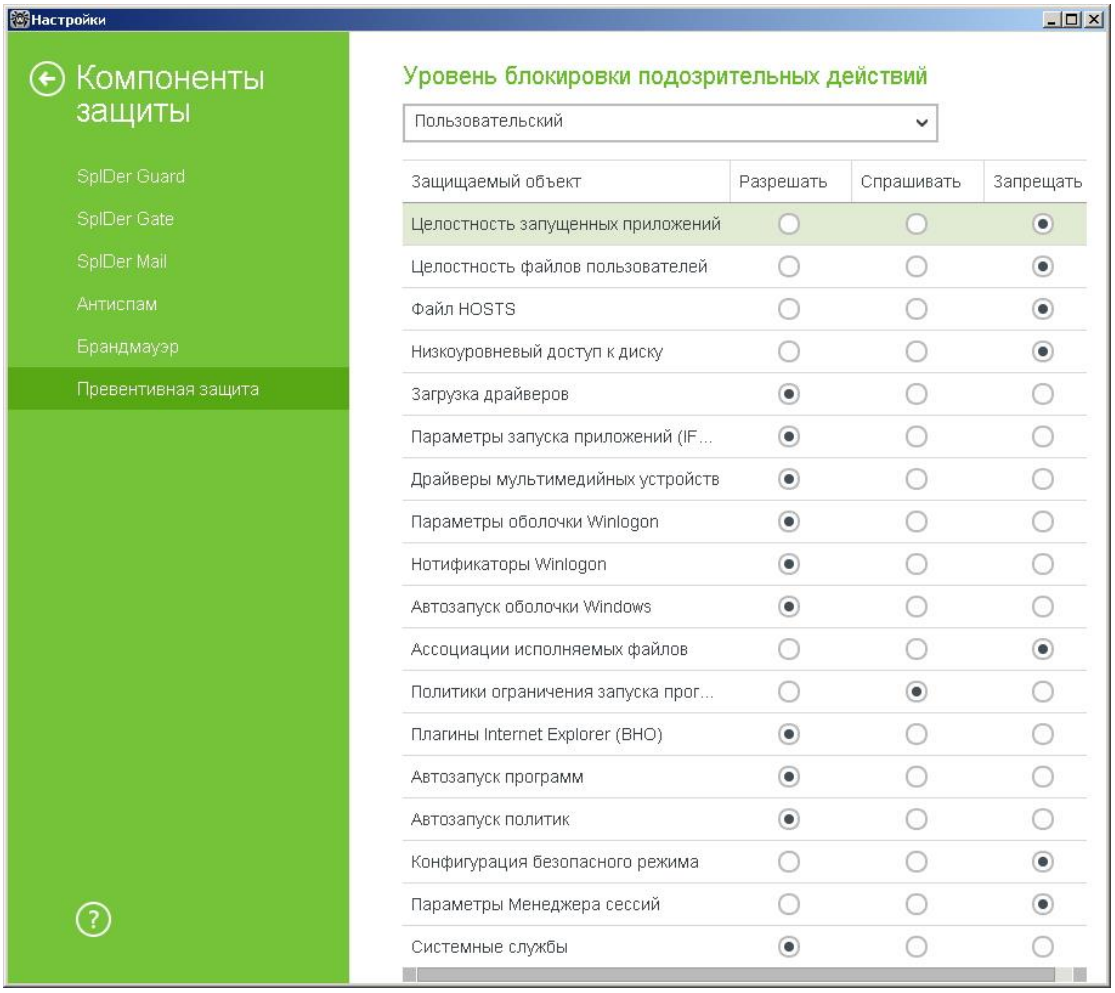

Рисунок 13

6. Закрыть окно **Настройки** и установить ПО Единый клиент JaCarta (подробнее см.раздел 4. Установка Единого клиента JaCarta).

Внимание!

Если при установке ПО Единый клиент JaCarta, будет выбрана опция **Устанавливать обновления автоматически** или опция **Проверять наличие новых обновлений, но не устанавливать их**, то после перезагрузки ОС может появится следующее окно (см. рис. 14).

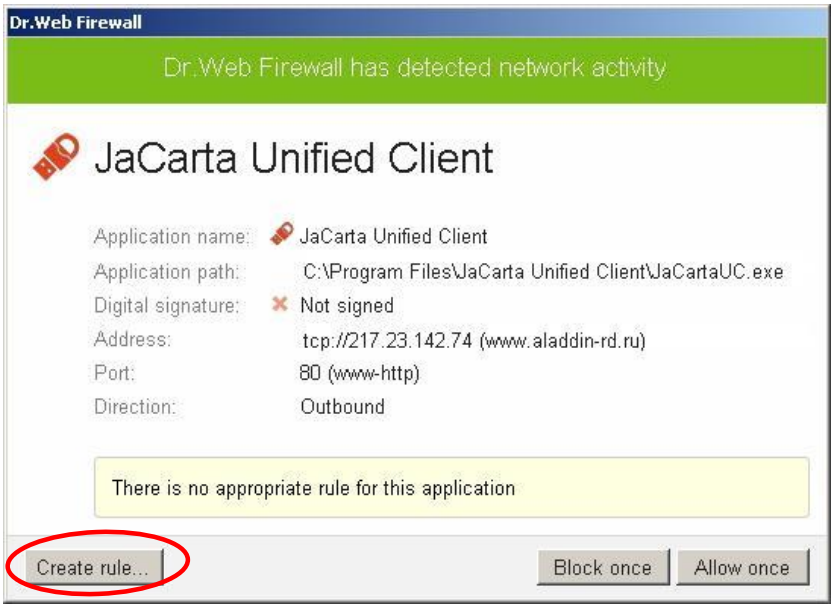

Рисунок 14

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

Для создания правила следует нажать кнопку **Create rule…**

Далее в появившемся окне (см. рис. 15) следует выбрать:
Allow network connections for application on 80,

Allow all network connections

или Create custom rule и нажать **ОК**.

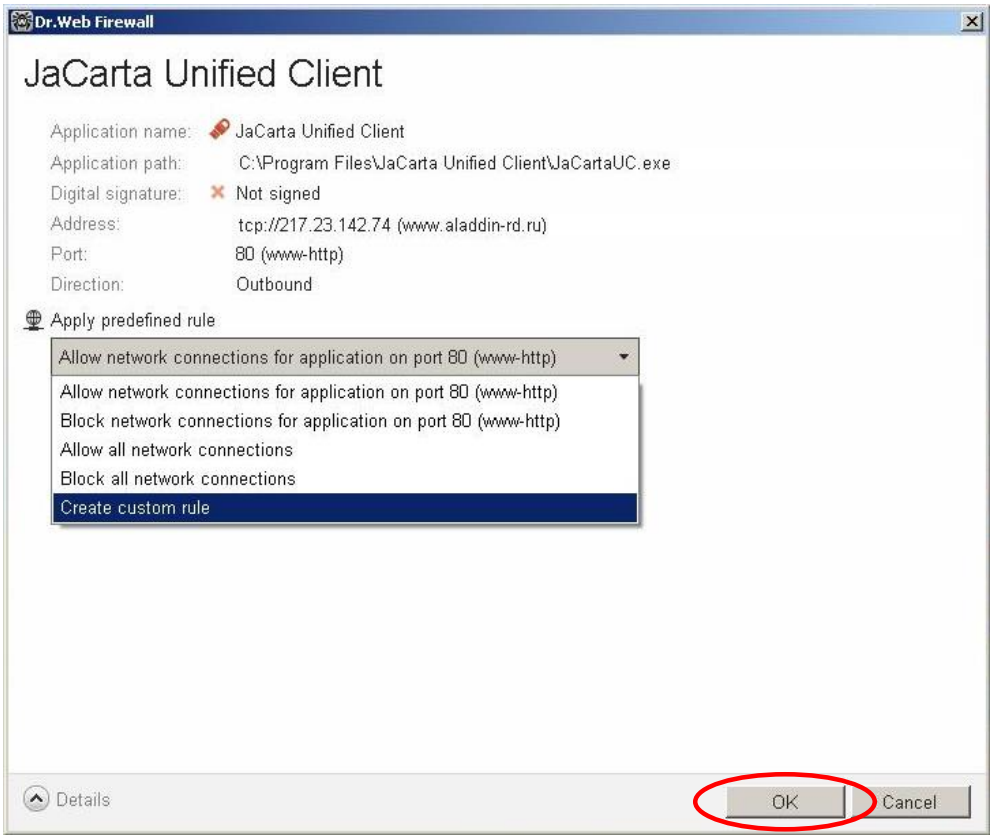

Рисунок 15

В случае, если была выбрана опция **Create custom rule**, должно появиться следующее окно (см. рис. 16), в котором необходимо нажать **OK** для завершения.

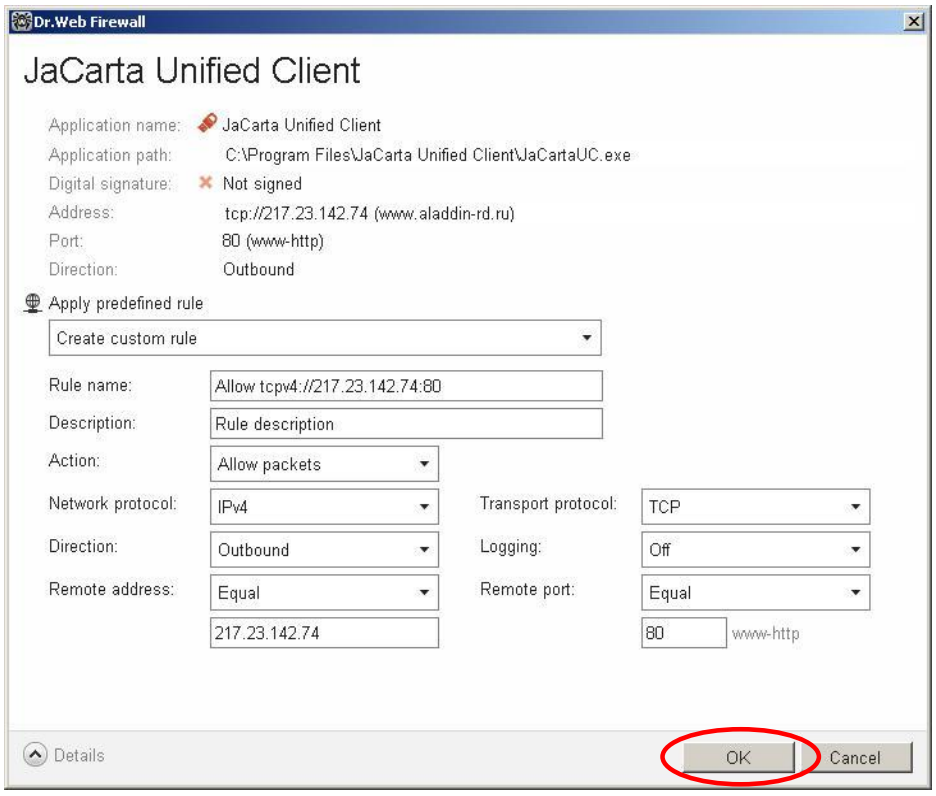

Рисунок 16

Особенности отображения плитки Управление токеном после установки Единый клиент JaCarta

После установки Единого клиента JaCarta, если во время установки был выбран вид установки **Стандартная** или же был выбран вид установки **Выборочная** с установкой компонента JaCarta SecurLogon, то перед моментом входа в ОС будет отображаться плитка Управление токеном (см. рис. 17).

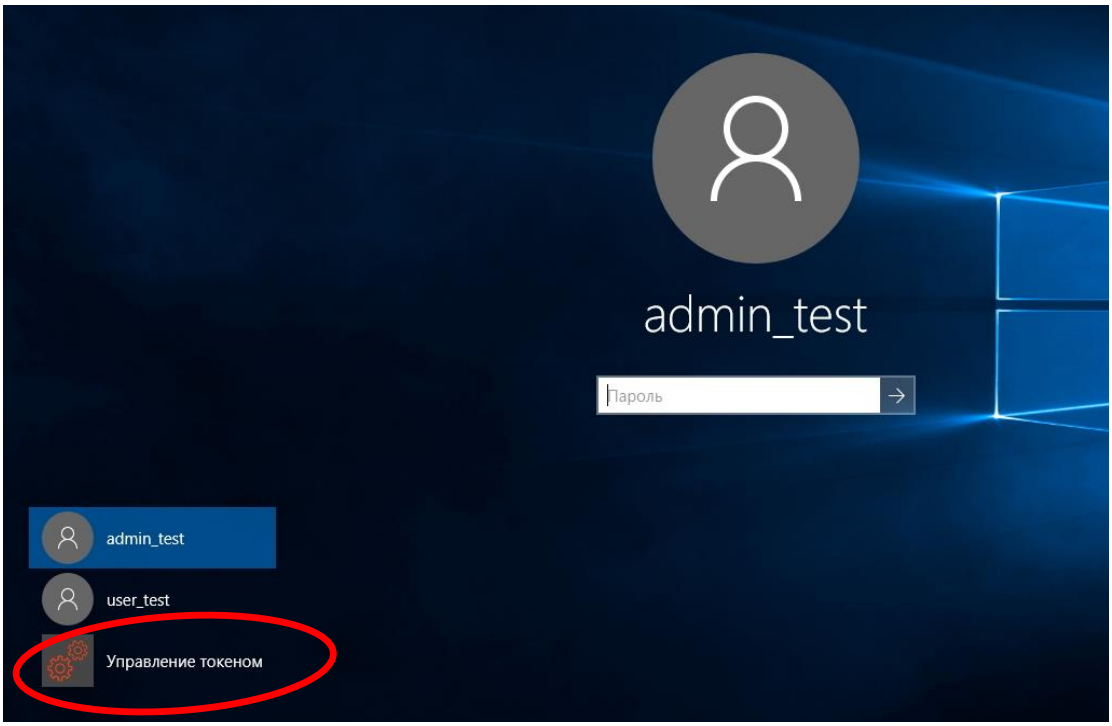

Рисунок 17

Отменить отображение этой плитки можно двумя способами:

1. В случае, если у пользователя есть лицензия на JaCarta SecurLogon необходимо выполнить следующие действия:

1.1. Нажать сочетание клавиш **Win**+**R**, в появившемся окне ввести **gpedit.msc** и нажать **ОК**.

1.2. В появившемся окне зайти в Конфигурация компьютера –> Административные шаблоны –> Компоненты Windows –> JaCarta SecurLogon.

1.3. Выбрать параметр **ShowTokenManageLogonScreen** и установить ему значение **Отключено**.

2. В случае, если у пользователя нет лицензии на JaCarta SecurLogon отменить отображение плитки **Управление токеном** можно только удалив компонент JaCarta SecurLogon. Для этого необходимо зайти в Панель управления –> Программы и компоненты –> Единый клиент JaCarta и выбрать опцию **Изменить**. После чего исключить компонент JaCarta SecurLogon из установленных компонентов.

5. Удаление Единого клиента JaCarta

Чтобы удалить Единый клиент JaCarta, выполните следующие действия:

1. В Панели управления выберите пункт **Программы и компоненты**. Отобразится следующее окно (см. рис. 18).

Окно программы и компоненты

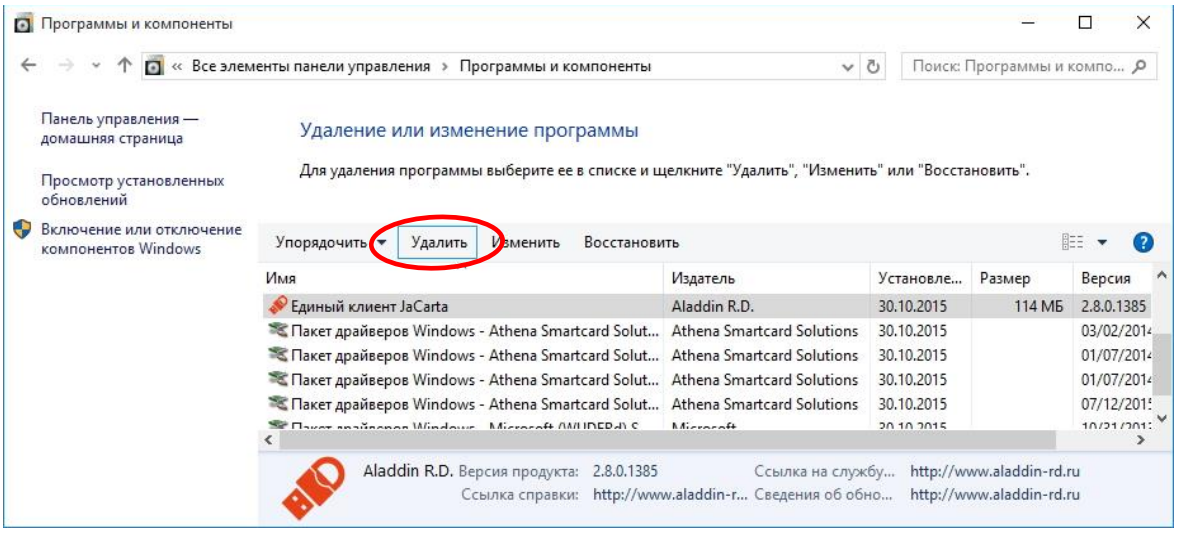

Рисунок 18

2. В списке установленных программы отметьте пункт **Единый клиент JaCarta** и нажмите **Удалить**. Отобразится следующее окно (см. рис. 19).

Окно предупреждения об удалении Единого клиента JaCarta

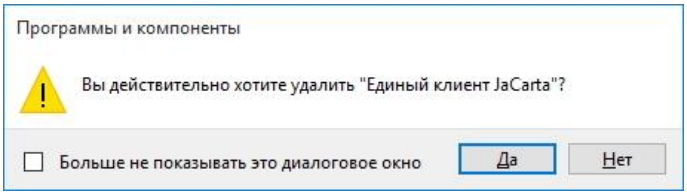

Рисунок 19

3. Нажмите **Да**, чтобы подтвердить операцию. Удаление Единого клиента JaCarta займёт некоторое время.
4. По завершении удаления вы можете закрыть окно **Программы и компоненты**.

6. Обзор пользовательского интерфейса

6.1. Меню быстрого запуска

Меню быстрого запуска Единого клиента JaCarta отображается на панели задач в области уведомлений в виде значка .

Чтобы открыть меню, нажмите на значке правой кнопкой мыши – меню будет иметь следующий вид (см. рис. 20).

Меню быстрого запуска

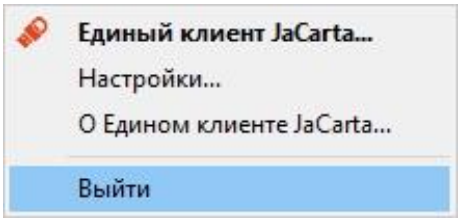

Рисунок 20

Описание пунктов меню быстрого запуска приведено в таблице 6.

Таблица 6

Пункт меню	Описание
Единый клиент JaCarta…	Открывает окно основного интерфейса Единого клиента JaCarta (подробнее см. подраздел 6.2. Основной интерфейс).
Настройки…	Открывает окно, позволяющее редактировать общие настройки Единого клиента JaCarta (подробнее см. раздел 7. Настройка работы Единого клиента JaCarta).
О Едином клиенте JaCarta…	Отображает сведения об установленном экземпляре Единого клиента JaCarta (см. рис. 21).
Выйти	Скрывает значок из области уведомлений на панели задач и осуществляет выход из Единого клиента JaCarta.

Таблица 6

Рисунок 21

6.2. Основной интерфейс

Чтобы открыть основное окно пользовательского интерфейса Единого клиента JaCarta выполните одно из следующих действий:

- Нажмите на значке правой кнопкой мыши и в контекстном меню выберите **Единый клиент JaCarta**.

ИЛИ

- В меню **Пуск** выберите **Все программы > Аладдин Р. Д. > Единый клиент JaCarta.**

Окно будет выглядеть следующим образом (см. рис. 22).

Основное окно пользовательского интерфейса

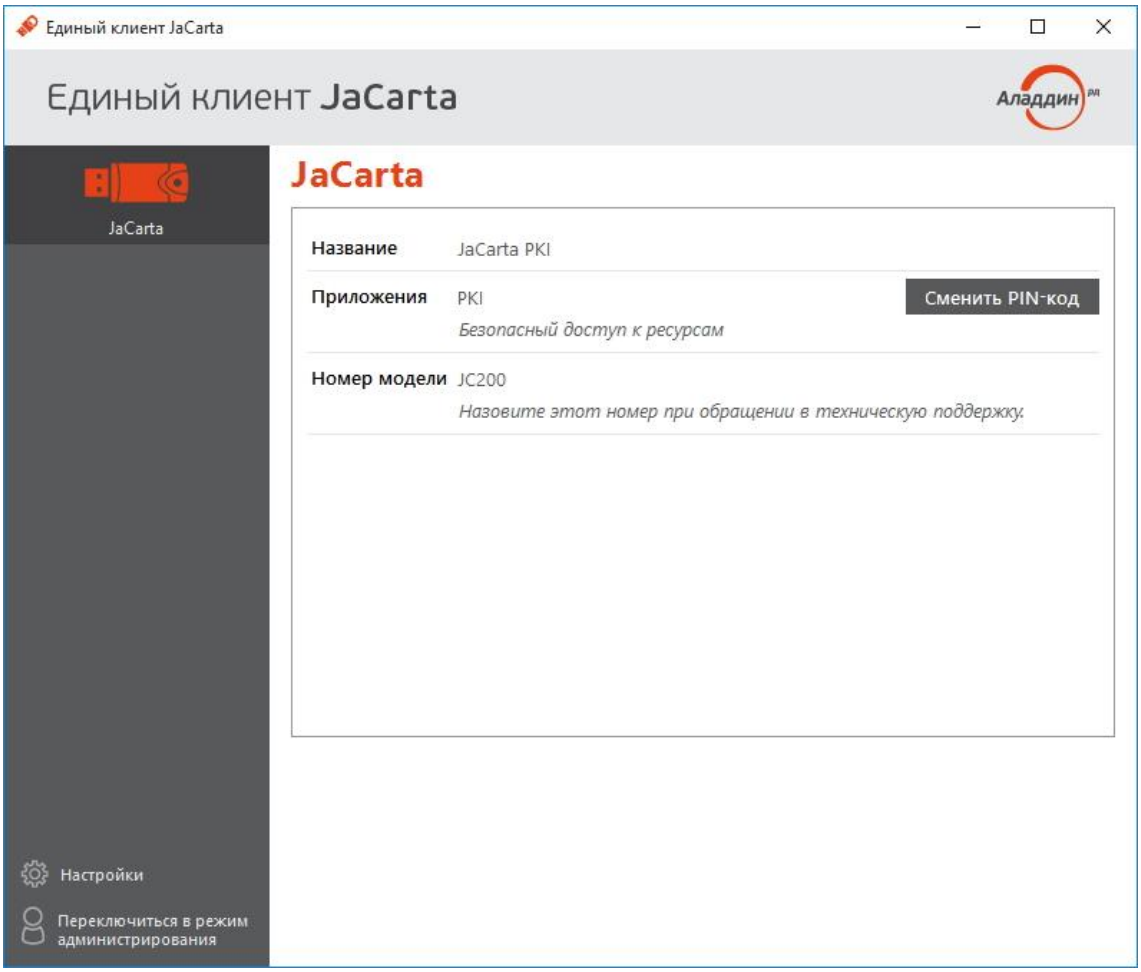

Рисунок 22

В верхней части левой панели отображаются подсоединённые к компьютеру электронные ключи. Значок электронного ключа зависит от типа этого электронного ключа. Виды значков электронных ключей и описание соответствующих им типов приведены в таблице 7.

При нажатии на логотип компании в верхнем правом углу окна – появится окно со сведениями о программе Единый клиент JaCarta (см. рис. 21).

Таблица 7

Изображение	Описание
	MicroUSB токен
	USB токен JaCarta в корпусе nano
	USB токен JaCarta в корпусе mini
	USB токен JaCarta в корпусе XL

Изображение	Описание
	Смарт-карта
	eToken PRO, eToken PRO (Java)
	eToken NG Flash, eToken NG-FLASH (Java)
	eToken NG OTP, eToken NG-OTP (Java)
	Тип электронного ключа не определён
	Электронный ключ в форм-факторе MicroSD
	Электронный ключ находится на стадии определения

Таблица 7

В нижней части левой панели основного окна Единого клиента JaCarta расположены ссылки:

- **Настройки** – отображает окно настроек Единого клиента JaCarta (см. раздел 7. Настройка работы Единого клиента JaCarta);
- **Переключиться в режим администрирования/пользователя** – позволяет переключить Единый клиент JaCarta в режим администратора или в режим пользователя соответственно.

В центральной части окна сверху отображается метка электронного ключа, выбранного в левой панели. Отображение остальных элементов зависит от выбранного режима (см. 6.2.1. Режим пользователя и 6.2.2. Режим администратора).

6.2.1. Режим пользователя

Окно Единого клиента JaCarta в режиме пользователя выглядит следующим образом (см. рис. 23).

Окно в режиме пользователя

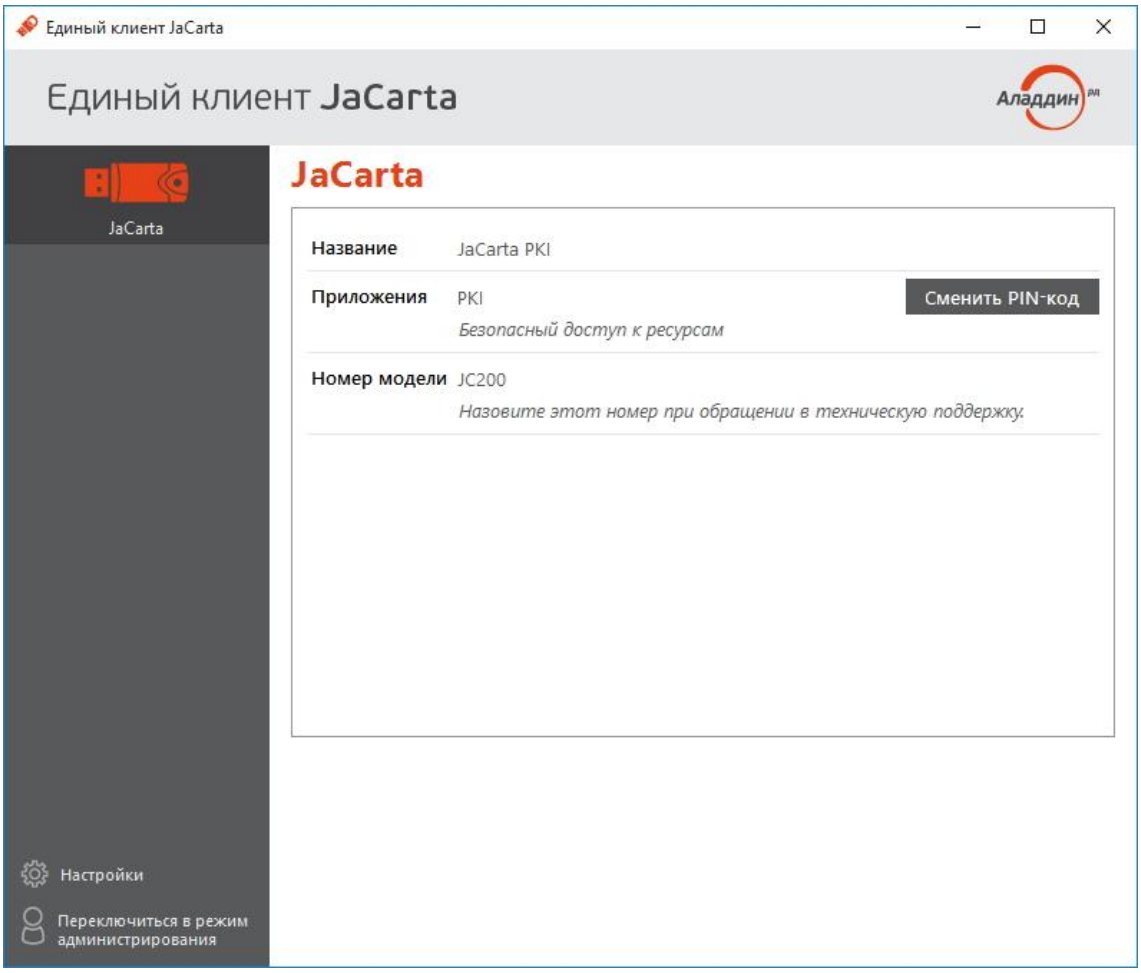

Рисунок 23

Описание интерфейса Единого клиента JaCarta в режиме пользователя приведено в таблице 8.

Таблица 8

Поле	Описание
Название	Название модели выбранного электронного ключа.
Приложения	Список приложений в памяти выбранного электронного ключа. Здесь также расположена кнопка **Сменить PIN-код**, которая позволяет пользователю сменить пароль пользователя выбранного электронного ключа (описание процедуры смены пароля пользователя приведено в документе [Единый клиент JaCarta. Руководство пользователя]).
Номер модели	Номер модели выбранного электронного ключа. В случае возникновения проблем при использовании пользователь должен сообщить этот номер в службу технической поддержки.

Таблица 8

При наличии обновлений для Единого клиента JaCarta ниже отображается уведомление со ссылкой, позволяющей установить это обновление.

6.2.2. Режим администратора

При переходе в режим администратора в основном окне интерфейса Единого клиента JaCarta появляются вкладки. Описание вкладок приведено в таблице 9.

Таблица 9

Вкладка	Описание
Информация о токене	На этой вкладке отображаются общие сведения о выбранном электронном ключе. Чтобы отобразить подробные сведения, нажмите **Полная информация...** (Подробнее см. "Вкладка Информация о токене").
PKI	Вкладка отображается, если на выбранном электронном ключе установлено приложение PKI.
PKI\BIO	Вкладка отображается, если на выбранном электронном ключе установлено приложение PKI/BIO.
ГОСТ	Вкладка отображается, если на выбранном электронном ключе установлено приложение ГОСТ.
STORAGE	Вкладка отображается, если на выбранном электронном ключе установлено приложение STORAGE.
ФКН	Вкладка отображается, если на выбранном электронном ключе установлено приложение ФКН.
SecurLogon	Вкладка отображается, если на выбранном электронном ключе установлено одно из следующих приложений: PKI, PKI/BIO, ГОСТ или STORAGE.

Таблица 9

Вкладка Информация о токене

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

Вкладка Информация о токене

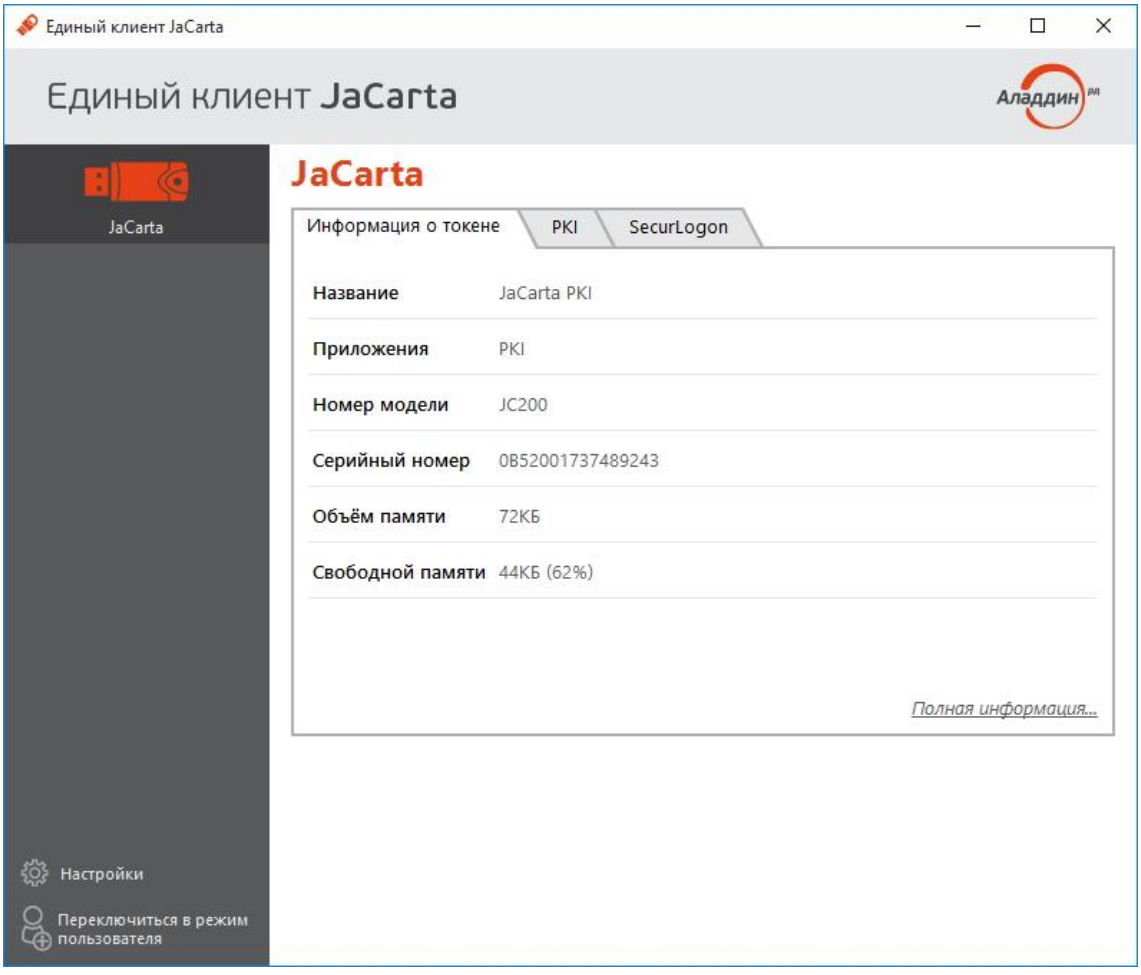

Рисунок 24

Описание отображаемых полей на вкладке **Информация о токене** приведено в таблице 10.

Таблица 10

Поле	Описание
Название	Название модели выбранного электронного ключа
Приложения	Приложения, установленные на выбранном электронном ключе
Номер модели	Номер модели выбранного электронного ключа
Серийный номер	Серийный номер выбранного электронного ключа
Объём памяти	Полный объём памяти выбранного электронного ключа
Свободной памяти	Объём свободной памяти выбранного электронного ключа

Таблица 10

Ниже располагается ссылка **Полная информация…**, нажатие на которую открывает окно с подробными сведениями о выбранном электронном ключе (см. рис. 25).

Подробная информация о токене

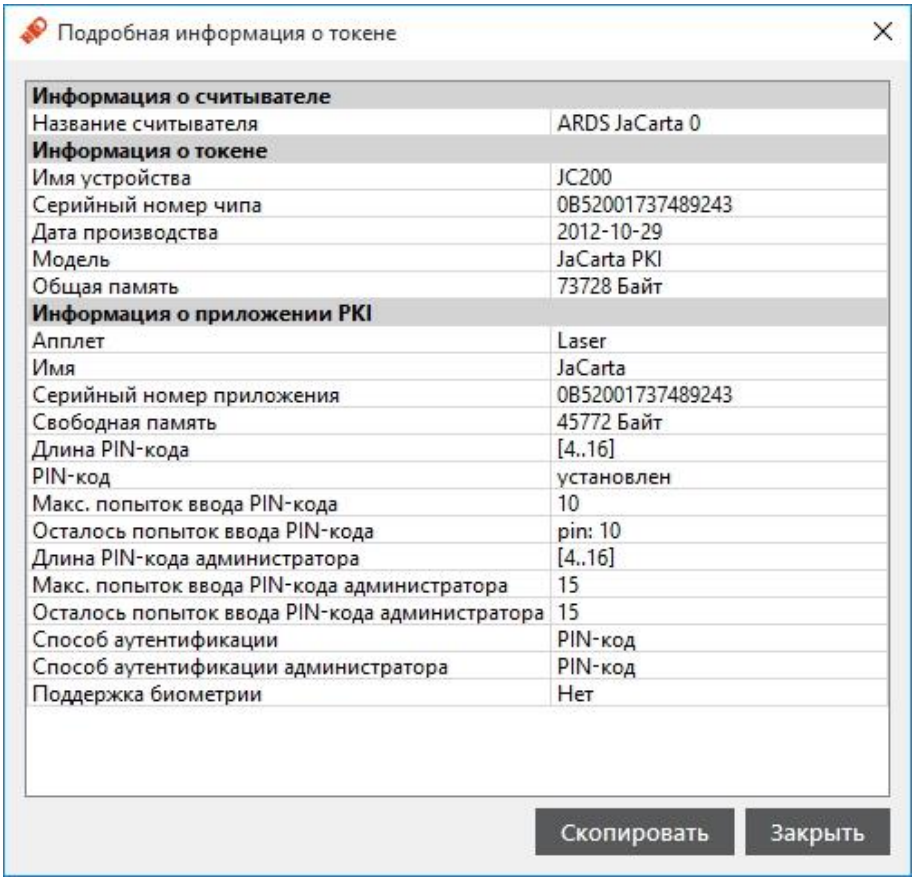

Рисунок 25

Описание предоставляемой информации о токене приведено в таблице 11.

Таблица 11

Секция	Поле	Описание
Информация о считывателе	Название считывателя	Название используемого считывателя
Информация о токене	Имя устройства	Имя выбранного электронного ключа
	Серийный номер чипа	Серийный номер микросхемы выбранного электронного ключа
	Модель	Модель выбранного электронного ключа
	Общая память	Объём памяти выбранного электронного ключа.
Информация о приложении	Апплет	Название используемого апплета выбранного электронного ключа.
	Имя	Метка выбранного электронного ключа.
	Серийный номер приложения	Серийный номер выбранного электронного ключа. В случае с электронными ключами eToken серийный номер может отличаться в зависимости от приложения.
	Свободная память	Объём свободной памяти выбранного электронного ключа.
	Длина PIN-кода	Количество символов PIN-кода пользователя для выбранного приложения.
	PIN-код	Статус PIN-кода пользователя приложения: установлен/не установлен.
	Макс. Попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя.
	Осталось попыток ввода PIN-кода	Число неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода пользователя.
	Длина PIN-кода администратора	Длина PIN-кода администратора выбранного приложения.
	Макс. Попыток ввода PIN-кода администратора	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора.
	Осталось попыток ввода PIN-кода администратора	Число неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода администратора.
	Способ аутентификации	Установленный способ аутентификации для выбранного приложения.
	Способ аутентификации администратора	Установленный способ аутентификации администратора.
	Версия приложения	Версия установленного приложения (только для приложения ГОСТ).
	Количество ключей	Количество секретных ключей в приложении (только для приложения ГОСТ).
	Количество объектов	Количество объектов в приложении (только для приложения ГОСТ).
	Режим предъявления ключа администратора	Установленный режим формы предъявления ключа администратора.

Таблица 11

7. Настройка работы Единого клиента JaCarta

Окно **Настройки** Единого клиента JaCarta можно вызвать двумя способами:

- Нажмите правой кнопкой мыши на значке в области уведомлений и выберите **Настройки**...
- В левом нижнем углу основного окна Единого клиента JaCarta нажмите Настройки. Отобразится следующее окно (см. рис. 26).

Настройки Единого клиента JaCarta на вкладке Основные

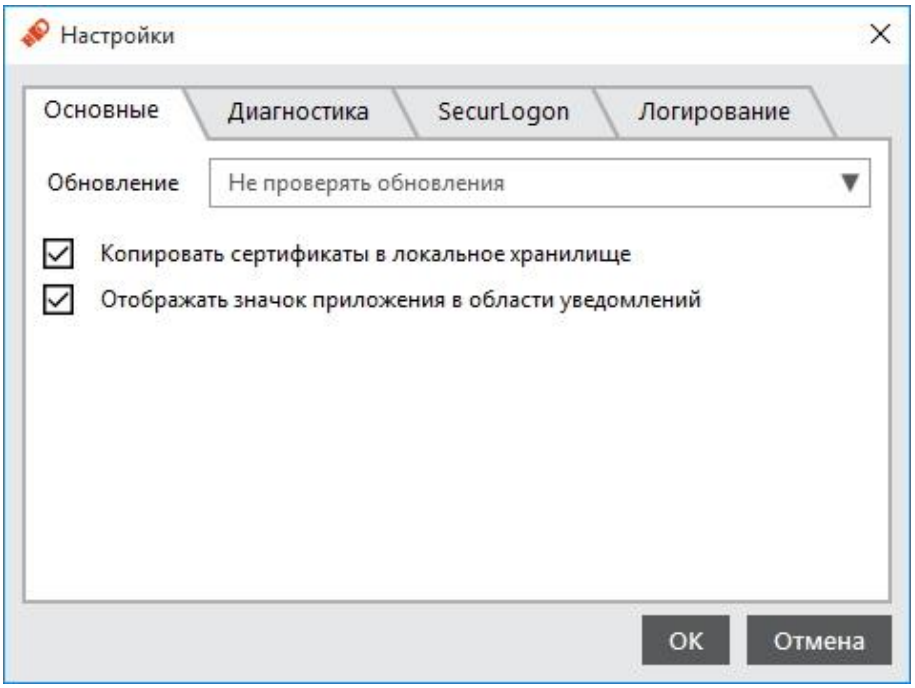

Рисунок 26

Окно Настройки Единого клиента JaCarta содержит три вкладки:

- Основные
- Диагностика
- SecurLogon
- Логирование

Описание настроек на вкладке **Основные** приведено в таблице 12, после изменения настроек следует нажать **OK**, чтобы сохранить изменения.

Таблица 12

Настройка	Описание
Обновление	Список содержит три пункта: • Не проверять обновления - Единый клиент JaCarta не будет проверять наличие обновлений; • Проверять обновления - Единый клиент JaCarta будет проверять наличие обновлений; • Автоматически - при выходе новых обновлений они будут загружены и установлены на компьютер автоматически.
Копировать сертификаты в	Если флажок установлен, сертификаты в памяти подсоединённых электронных ключей будут

Настройка	Описание
локальное хранилище	копироваться в локальное хранилище сертификатов.
Отображать значок приложения в области уведомлений	Определяет, будет ли отображаться значок в области уведомлений.

Таблица 12

Описание окна Настройки на вкладке **Диагностика** (см. рис. 27) приведено в таблице 13, после изменения настроек следует нажать **ОК**, чтобы сохранить изменения.

Окно Настройки Единого клиента JaCarta на вкладке Диагностика

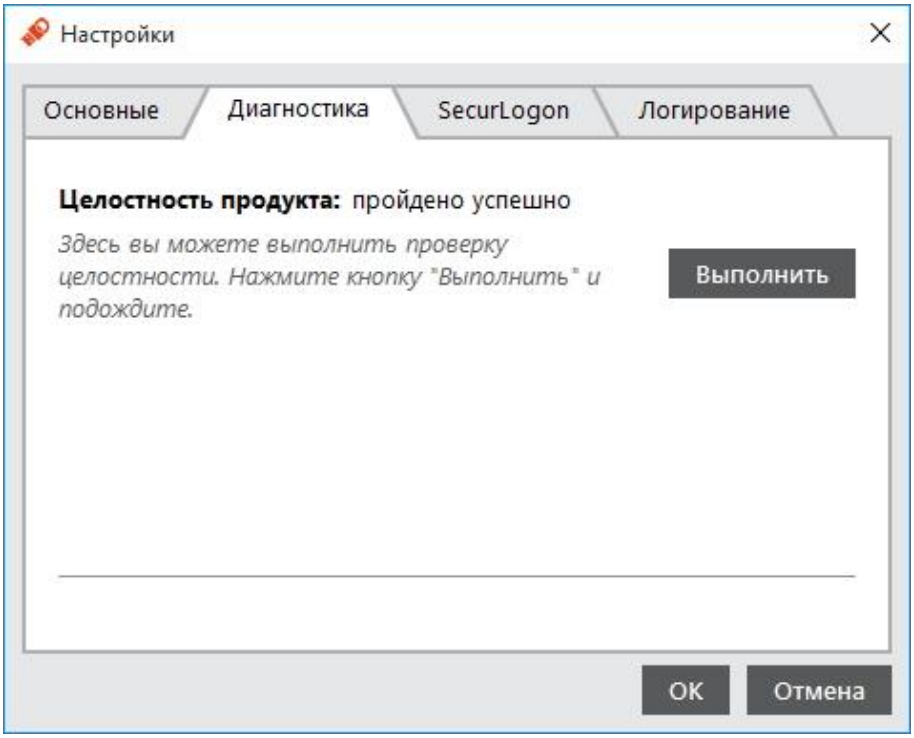

Рисунок 27

Таблица 13

Настройка	Описание
Выполнить	Выполняется проверка целостности Единого клиента JaCarta с последующим отображением результатов проверки.

Таблица 13

Описание окна Настройки на вкладке **SecurLogon** (см. рис. 28) приведено в таблице 14, после изменения настроек следует нажать **ОК**, чтобы сохранить изменения.

Окно Настройки Единого клиента JaCarta на вкладке SecurLogon

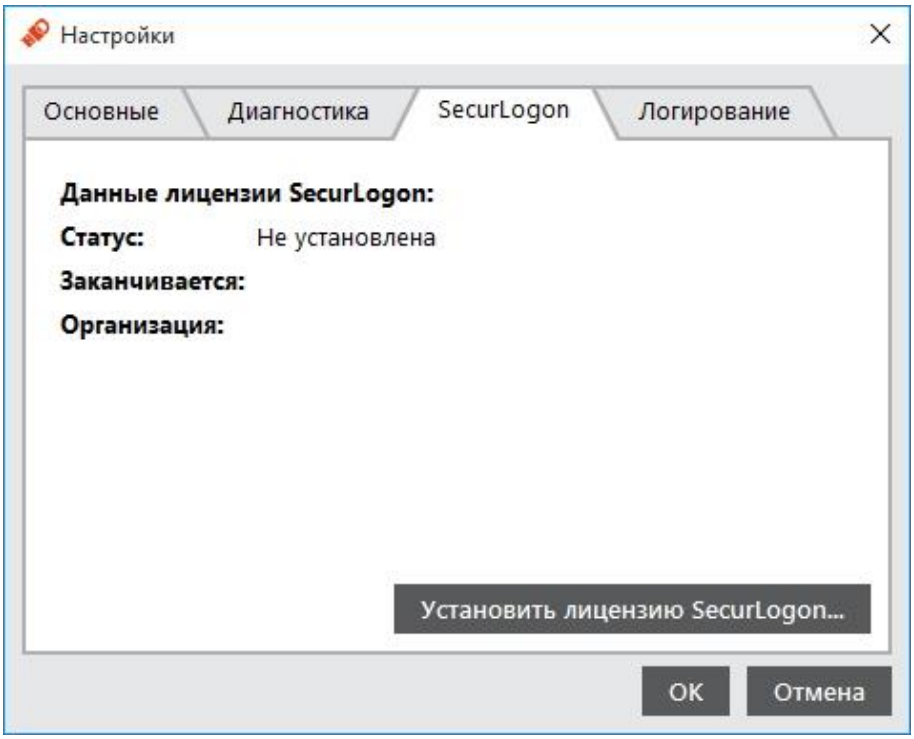

Рисунок 28

Подробнее про работу с продуктом JaCarta Securlogon написано в документе [JaCarta Securlogon Руководство администратора].

Таблица 14

Настройка	Описание
Установить лицензию SecurLogon…	Открывает окно для выбора и установки файла лицензии ПО JaCarta SecurLogon с последующим отображением информации о статусе лицензии.

Таблица 14

Описание окна Настройки на вкладке **Логирование** (см. рис. 29) приведено в таблице 15.

Внимание! На вкладке **Логирование** настройки только отображаются. Изменение настроек на этой вкладке невозможно. Подробнее об изменении настроек логирования см. [Единый клиент JaCarta. Инструкция по сбору диагностической информации].

Окно Настройки Единого клиента JaCarta на вкладке Логирование

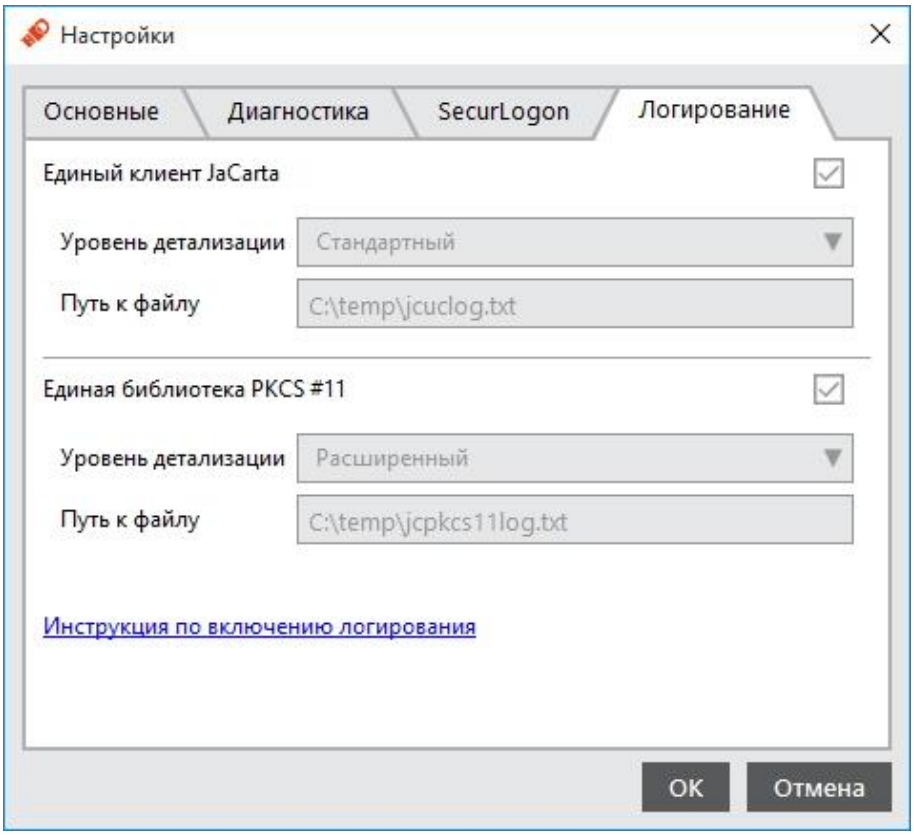

Рисунок 29

Ссылка **Инструкция по включению логирования** открывает статью в базе знаний (http://kbp.aladdin-rd.ru), содержащую порядок действий по сбору диагностической информации.

Таблица 15

Настройка	Описание
Единый клиент JaCarta	Отображает настройки логирования Единого клиента JaCarta. Если логирование выключено, то отображаются следующие настройки логирования: • Чекбокс Включения/Выключения логирования. Если логирование включено, то отображаются следующие настройки логирования: • Уровень детализации логирования (только Стандартный). • Путь к файлу с логами.
Единая библиотека PKCS #11	Отображает настройки логирования Единой библиотеки PKCS #11: Если логирование выключено, то отображаются следующие настройки логирования: • Чекбокс Включения/Выключения логирования. Если логирование включено, то отображаются следующие настройки логирования: • Уровень детализации логирования (Стандартный или Расширенный). • Путь к файлу с логами.

Таблица 15

8. Инициализация электронных ключей

Во время инициализации задаются основные параметры работы электронных ключей. После инициализации электронный ключ следует передать конечному пользователю электронного ключа.

8.1. Приложение PKI (электронные ключи eToken и JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin)

Чтобы подготовить электронный ключ к работе, выполните следующие действия:

1. Запустите Единый клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру, выберите его в левой панели интерфейса Единого клиента JaCarta и в центральной части окна выберите вкладку **PKI**.
3. Нажмите **Инициализировать…**. Отобразится следующее окно (см. рис. 30).

Общие параметры инициализации

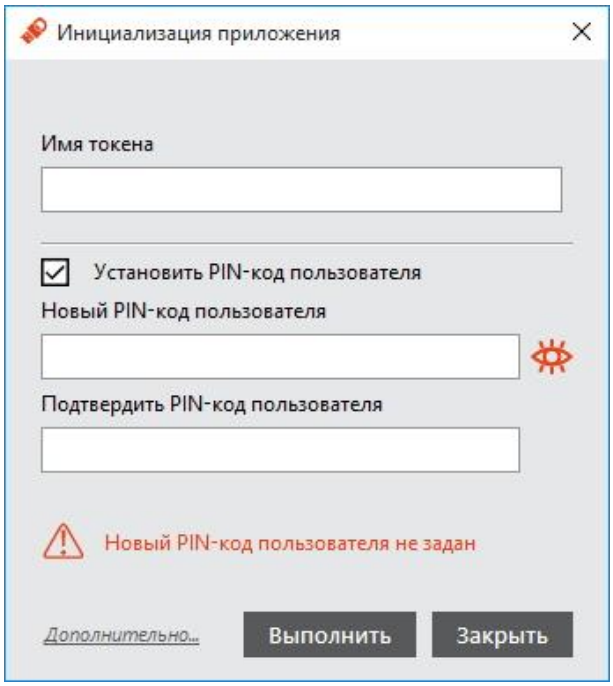

Рисунок 30

4. Выполнить настройку. Описание общих параметров инициализации приведено в таблице 16.

Таблица 16

Поле	Описание
Имя токена	Укажите в этом поле метку электронного ключа (например, имя будущего владельца).

Поле	Описание
Установить PIN-код пользователя	Установите флажок, если хотите задать PIN-код пользователя на этапе инициализации. Если вы снимите флажок, PIN-код пользователя во время инициализации установлен не будет – его можно будет установить позже (для этого потребуется PIN-код администратора).
Новый PIN-код пользователя	Введите значение PIN-кода пользователя (данное поле активно, если установлен флажок **Установить PIN-код пользователя**).

Таблица 16

5. Если вы хотите настроить дополнительные параметры инициализации, нажмите ***Дополнительно…***, в противном случае переходите к шагу 14 настоящей процедуры. После нажатия ***Дополнительно…*** отобразится следующее окно (см. рис. 31).

Окно дополнительных настроек инициализации. Вкладка Параметры.

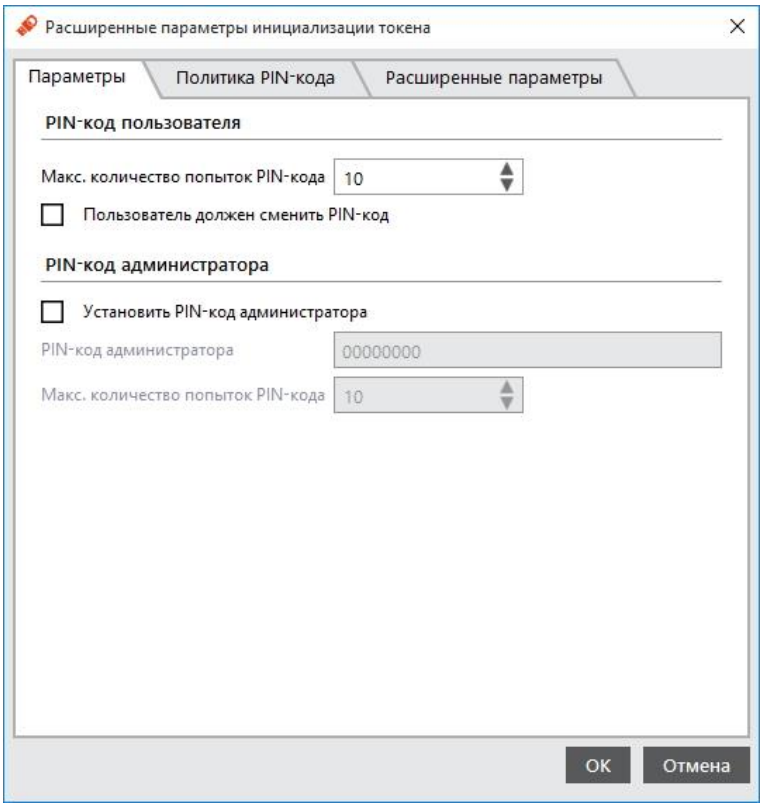

Рисунок 31

6. Выполнить настройку. Описание дополнительных настроек на вкладке **Параметры** приведено в таблице 17.

Таблица 17

Секция	Настройка	Описание
PIN-код пользователя	Макс. Количества попыток	Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована.
	Пользователь должен сменить PIN-код	Если флажок установлен, пользователь должен будет сменить PIN-код пользователя при первом использовании электронного ключа, в противном случае он не сможет продолжить работу с этим электронным ключом.

Секция	Настройка	Описание
PIN-код администратора	Установить PIN-код администратора	Если флажок установлен, в процессе инициализации будет установлен PIN-код администратора.
	PIN-код администратора	Введите значение PIN-кода администратора (поле активно, только если установлен флажок Установить PIN-код администратора).
	Макс. Количество попыток	Максимальное количество неверных последовательных попыток ввода PIN-кода администратора, после которого возможность использования PIN-кода администратора будет заблокирована.

Таблица 17

7. Перейдите на вкладку **Политика PIN-кода**. Окно примет следующий вид (см. рис. 32).

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

Окно дополнительных настроек инициализации. Вкладка Политика PIN-кода.

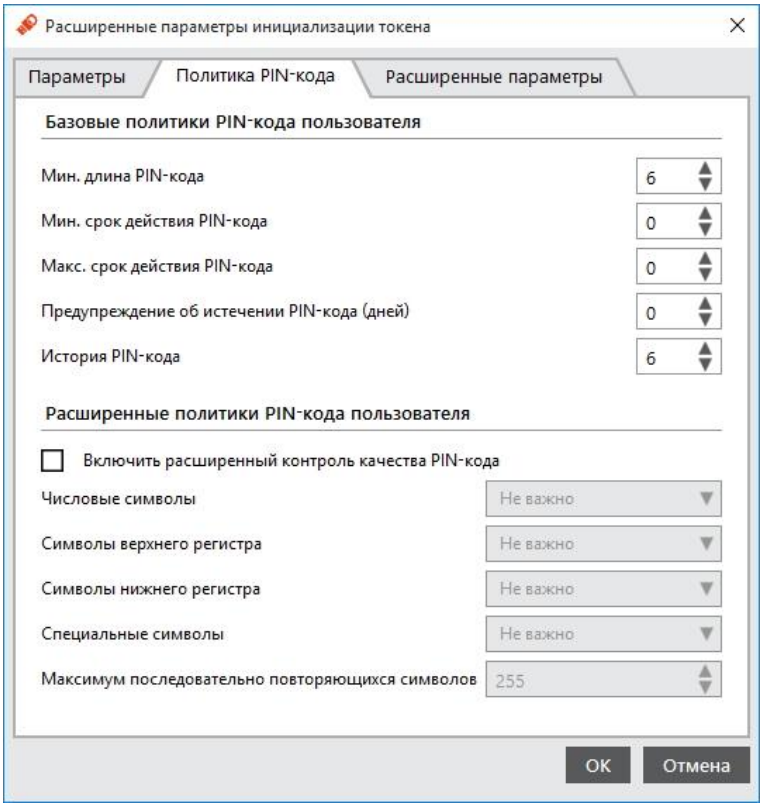

Рисунок 32

8. Выполнить настройку. Описание дополнительных настроек на вкладке Политика PIN-кода приведено в таблице 18.

Таблица 18

Секция	Настройка	Описание
Базовые политики PIN-кода пользователя	Мин. длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде.
	Мин. срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя.
	Макс. срок действия PIN-кода	Максимальный срок (в днях), в течение которого можно использовать PIN-код пользователя.

Секция	Настройка	Описание
	Предупреждение об истечении PIN-кода (дней)	За сколько дней до окончания срока действия PIN-кода пользователя последний будет получать соответствующее уведомление.
	История PIN-кода	Число использовавшихся ранее PIN-кодов пользователя, которые нельзя использовать при назначении нового PIN-кода пользователя. Например, если значение установлено в «3», пользователь не сможет назначить PIN-код пользователя, совпадающий с одним из трёх ранее использованных подряд PIN-кодов.
Расширенные политики PIN-кода пользователя	Включить расширенный контроль качества PIN-кода	Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя.
	Числовые символы	Использование цифр в PIN-коде пользователя. Список содержит три пункта: • Не важно • Запрещено • Обязательно
	Символы верхнего регистра	Использование алфавитных символов верхнего регистра в PIN-коде пользователя. Список содержит три пункта: • Не важно • Запрещено • Обязательно
	Символы нижнего регистра	Использование алфавитных символов нижнего регистра в PIN-коде пользователя. Список содержит три пункта: • Не важно • Запрещено • Обязательно
	Специальные символы	Использование специальных символов в PIN-коде пользователя. Список содержит три пункта: • Не важно • Запрещено • Обязательно
	Максимум последовательно повторяющихся символов	Использование идущих подряд одинаковых символов. Список содержит поле с возможностью выбора значения из диапазона от 0 до 255.

Таблица 18

9. Перейдите на вкладку **Расширенные параметры**. Окно примет следующий вид (см. рис. 33).

Окно дополнительных настроек инициализации. Вкладка Расширенные параметры.

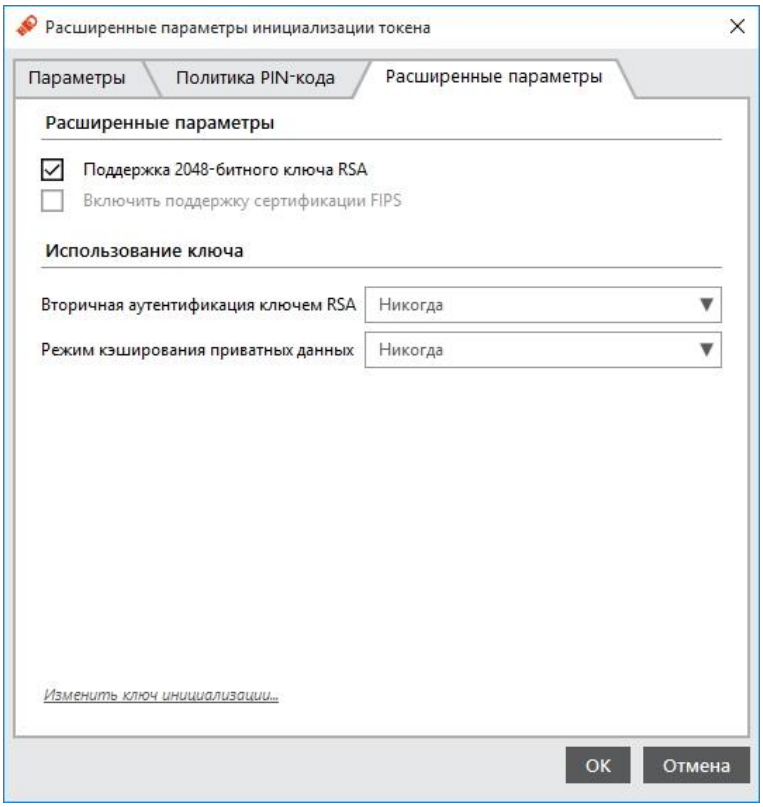

Рисунок 33

10. Выполнить настройку. Описание дополнительных настроек на вкладке Расширенные параметры приведено в таблице 19 .

Таблица 19

Секция	Настройка	Описание
Расширенные параметры	Поддержка 2048-битного ключа RSA	Выберите этот пункт для поддержки 2048-битных ключей RSA. Электронные ключи eToken PRO 32/64k не поддерживают эту опцию.
	Включить поддержку сертификации FIPS	Выберите этот пункт для инициализации устройств в режиме соответствия стандарту FIPS. FIPS (Federal Information Processing Standards) – утвержденный правительством США набор стандартов, направленных на улучшение управления и использования компьютерных и телекоммуникационных систем связи.
Использование ключа	Вторичная аутентификация ключом RSA	Список содержит четыре пункта: Никогда – вторичная аутентификация не производится; **Prompt conditional** (Предлагать по требованию приложения) - в этом режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность; **Prompt always** (Всегда запрашивать у пользователя) – при генерации RSA ключа, каждый раз запрашивается дополнительный пароль RSA для доступа к этому ключу. Однако пользователь может и не задавать дополнительный пароль, при этом генерация ключа продолжится без использования дополнительного пароля RSA; **Mandatory** (Всегда) –при создании ключа RSA вам будет предложено задать дополнительный пароль для доступа к ключу. При нажатии кнопки ОК генерируется ключ, введенный пароль используется в качестве дополнительного пароля RSA для этого ключа.
	Режим кэширования приватных данных	Список содержит три пункта: • **Никогда** – кэширование не производится;

Секция	Настройка	Описание
		• **При входе пользователя** – кэширование производится при входе пользователя, данные сохраняются к кэше до завершения сеанса входа; • **Всегда** – кэширование производится всегда.

Таблица 19

11. Если вы хотите изменить ключ инициализации, нажмите на ссылке ***Изменить ключ инициализации…*** внизу окна. В противном случае переходите к шагу 13 настоящей процедуры. После нажатия ***Изменить ключ инициализации…*** отобразится следующее окно (см. рис. 34).

Параметры ключа инициализации

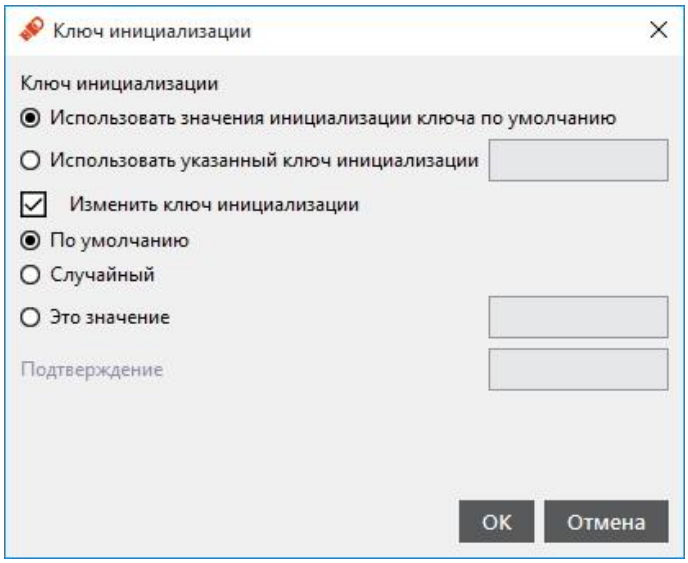

Рисунок 34

Описание настроек в окне Параметры ключа инициализации приведены в таблице 20.

Таблица 20

Настройка	Описание
Ключ инициализации	Использовать значения инициализации ключа по умолчанию – использование стандартного ключа инициализации.
	Использовать указанный ключ инициализации - введите то значение, которое было установлено в поле Это значение.
Изменить ключ инициализации	**По умолчанию** – восстановить значение по умолчанию.
	Случайный – в этом случае повторная инициализация eToken невозможна.
	Это значение – введите новый ключ инициализации и введите подтверждение соответственно.

Таблица 20

1. Нажмите **OK**, чтобы закрыть окно параметров ключа инициализации.
2. Нажмите **OK**, чтобы закрыть окно расширенных параметров инициализации электронного ключа.
3. В окне **Инициализация приложения** (см. рис. 30) нажмите **Выполнить**.
4. Подтвердите свой выбор в отобразившемся окне предупреждения.
5. При успешной инициализации отобразится соответствующее сообщение – нажмите **OK**, чтобы закрыть его.

8.2. Приложение PKI (электронные ключи JaCarta) и PKI/BIO

8.2.1. Настройки инициализации

Чтобы подготовить электронный ключ к работе, выполните следующие действия.

1. Запустите Единый клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру, выберите его в левой панели интерфейса Единого клиента JaCarta и в центральной части окна выберите вкладку **PKI**.
3. Нажмите **Инициализировать**. Отобразится следующее окно (см. рис. 35).

Общие параметры инициализации

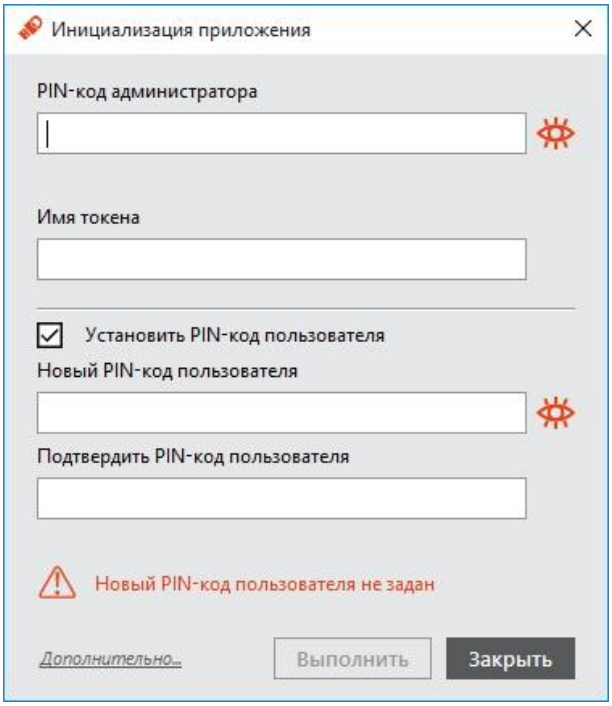

Рисунок 35

4. Выполнить настройку. Описание общих параметров инициализации приведено в таблице 21.

Таблица 21

Поле	Описание
PIN-код администратора	Введите текущий PIN-код администратора (см. 1.3.1. Параметры электронных ключей при поставке).
Имя токена	Введите желаемую метку электронного ключа (например, это могут быть имя и фамилия будущего владельца).
Установить PIN-код пользователя	Установите этот флажок, если хотите задать PIN-код пользователя во время инициализации. Вы можете не задавать PIN-код пользователя, если: • вы используете электронный ключ с приложением PKI/BIO и вы хотите установить для пользователя только биометрическую аутентификацию (подробнее см. дополнительные настройки инициализации в рамках настоящей процедуры); • вы хотите задать PIN-код пользователя позже – в этом случае для последующей установки PIN-кода пользователя необходимо будет предъявить PIN-код администратора.
Новый PIN-код пользователя	Введите новый PIN-код пользователя (поле активно, если установлен флажок **Установить PIN-код пользователя**).

Поле	Описание
Подтверждение PIN-кода	Введите подтверждение нового PIN-кода пользователя (поле активно, если установлен флажок **Установить PIN-код пользователя**).

Таблица 21

5. Если вы хотите настроить дополнительные параметры инициализации, нажмите ***Дополнительно…*** , в противном случае переходите к шагу 13 настоящей процедуры. После нажатия ***Дополнительно…*** отобразится следующее окно (см. рис. 36).

Дополнительные параметры инициализации

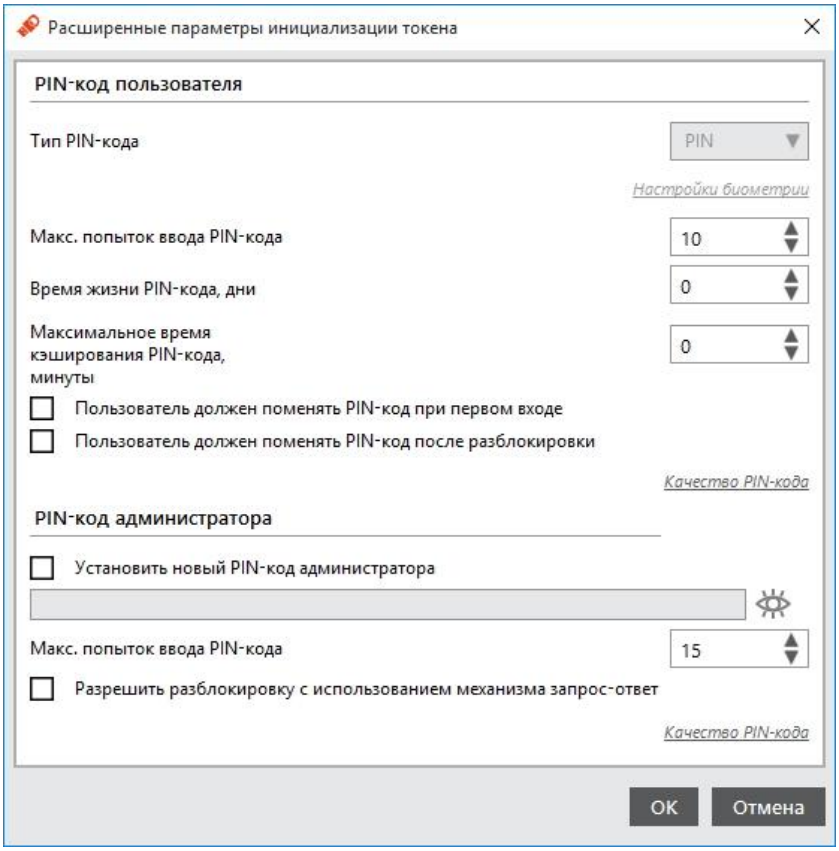

Рисунок 36

6. Выполнить настройку. Описание расширенных параметров инициализации приведено в таблице 22.

Таблица 22

Секция	Настройка	Описание
PIN-код пользователя	Тип PIN-кода	Возможны четыре варианта: • PIN – для аутентификации пользователь должен ввести PIN-код пользователя; • BIO – для аутентификации пользователь должен приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN или BIO – для аутентификации пользователь должен сделать одно из двух: ввести PIN-код пользователя или приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO); • PIN и BIO – для аутентификации пользователь должен как ввести PIN-код пользователя, так и приложить палец к сканеру отпечатков пальцев (только для электронных ключей с приложением PKI/BIO).
	Макс. попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя.

Секция	Настройка	Описание
	Время жизни PIN-кода	Число дней, спустя которое пользователь должен будет сменить PIN-код пользователя.
	Максимальное время кэширования PIN-кода	В течение какого времени (в минутах) PIN-код пользователя будет кэшироваться на компьютере, к которому подсоединён электронный ключ.
	Пользователь должен поменять PIN-код при первом входе	Установка этого флажка обяжет пользователя сменить PIN-код пользователя при первом использовании электронного ключа.
PIN-код администратора	Установить новый PIN-код администратора	Установка этого флажка делает доступным поле для ввода нового PIN-кода администратора и поле для повторного подтверждения этого кода.
	PIN-код администратора	Введите значение нового PIN-кода администратора. Ключ администратора может быть: • значением, соответствующим установленному качеству паролей (см. качество PIN-кода ниже); • ключом 3DES (если установлен флажок **Разрешить разблокировку с использованием механизма запрос-ответ**).
	Макс. попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора.
	Разрешить разблокировку с использованием механизма запрос-ответ	При установке этого флажка после инициализации появляется возможность разблокировать электронный ключ в удалённом режиме, используя механизм «запрос-ответ». Для этого также в поле PIN-код администратора необходимо задать значение ключа 3DES, который будет выполнять функцию PIN-кода администратора.

Таблица 22

7. Задайте настройки качества PIN-кода пользователя и PIN-кода администратора, нажав на соответствующей ссылке ***Качество PIN-кода*** в секции **PIN-код пользователя** и **PIN-код администратора** соответственно (см. рис. 36). Окно настроек качества PIN-кода пользователя выглядит следующим образом (см. рис. 37). Описание настроек качества PIN-кода приведено в таблице 23.

При задании настроек к качеству PIN-кода рекомендуется следующее:

- использовать буквы латинского алфавита (abc…z, ABC…Z), цифры (123…0) и спецсимволы (~!@#...);
- минимальная длина PIN-кода – 6 символов.

8. Нажмите **OK**, чтобы сохранить настройки.

Окно настроек качества PIN-кода пользователя

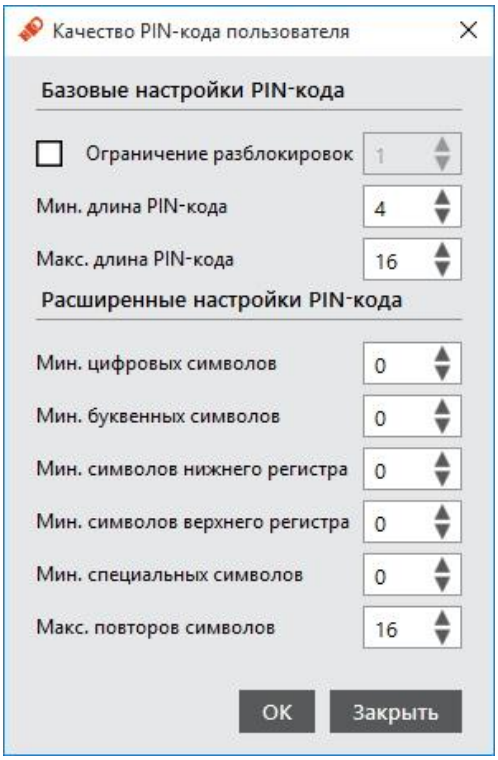

Рисунок 37

Таблица 23

Секция	Настройка	Описание
Базовые настройки PIN-кода	Ограничение разблокировок	Установите флажок и установите количество возможных разблокировок заблокированного PIN-кода.
	Мин. длина PIN-кода	Минимальное число символов в PIN-коде.
	Макс. длина PIN-кода	Максимальное число символов в PIN-коде.
Расширенные настройки PIN-кода	Мин. цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде.
	Мин. буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде.
	Мин. символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде.
	Мин. символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде.
	Мин. специальных символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде.
	Макс. Повторов символов	Определяет максимальное допустимое число одинаковых символов, идущих подряд.

Таблица 23

9. Выполните следующие действия в зависимости от приложения, установленного на электронном ключе:

- PKI – переходите к шагу 12 настоящей процедуры.
- PKI/BIO – если в поле **Тип PIN-кода** выбрано **BIO**, **PIN или BIO** или **PIN и BIO**, нажмите **Настройки биометрии**. После нажатия **Настройки биометрии** отобразится следующее окно (см. рис. 38).

Окно настроек биометрии

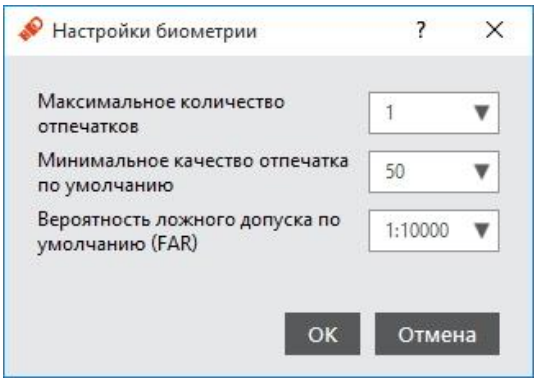

Рисунок 38

10. Выполнить настройку. Описание настроек биометрии приведено в таблице 24.

Таблица 24

Настройка	Описание
Максимальное количество отпечатков	Определяет максимальное количество отпечатков пальцев пользователя, которое можно сохранить в памяти электронного ключа JaCarta (от 1 до 10). В каждом конкретном случае пользователь сможет выбрать, какой отпечаток пальца использовать. Минимальное рекомендуемое значение: 2.
Минимальное качество отпечатка по умолчанию	Определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться.
Вероятность ложного допуска по умолчанию (FAR)	Определяет вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000.

Таблица 24

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

Если вы инициализируете электронный ключ с поддержкой биометрии следует руководствоваться п.п. 8.2.2. Инициализация с биометрическими параметрами.

14. В случае успешной инициализации отобразится соответствующее сообщение – нажмите **OK**, чтобы закрыть его.

Электронный ключ можно передать пользователю.

8.2.2. Инициализация с биометрическими параметрами

Если вы инициализируете электронный ключ с биометрическими настройками, через некоторое время после запуска процесса инициализации отобразится следующее окно (см. рис. 39).

Окно регистрации отпечатков

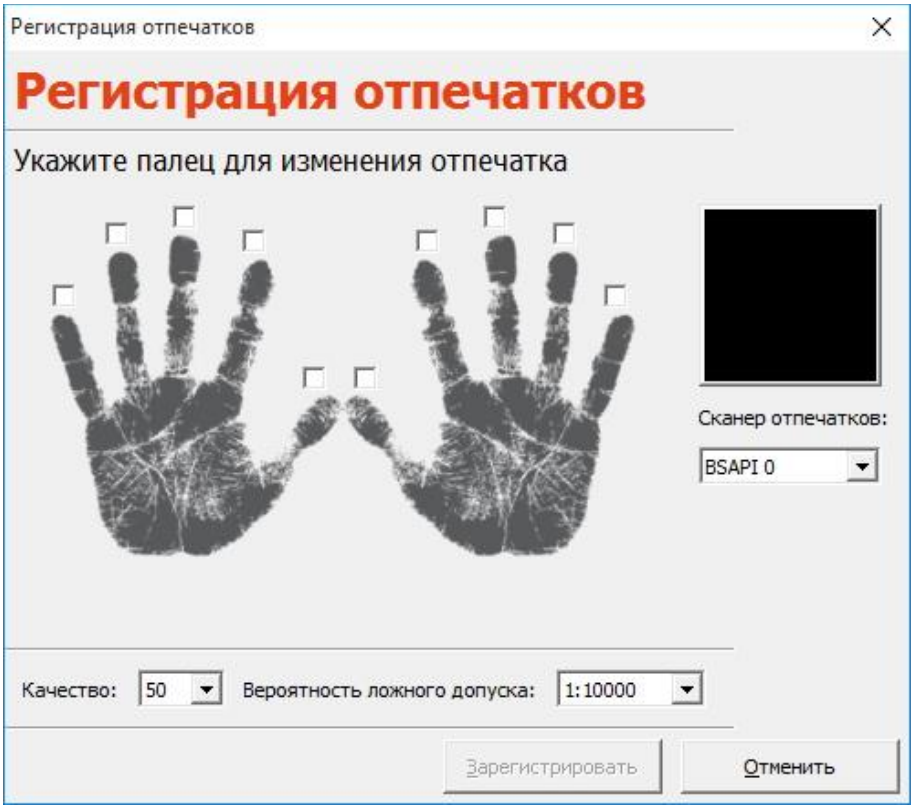

Рисунок 39

1. На схематическом изображении ладоней отметьте палец, который будет отсканирован во время инициализации (см. рис. 40).

Окно выбора пальца для сканирования

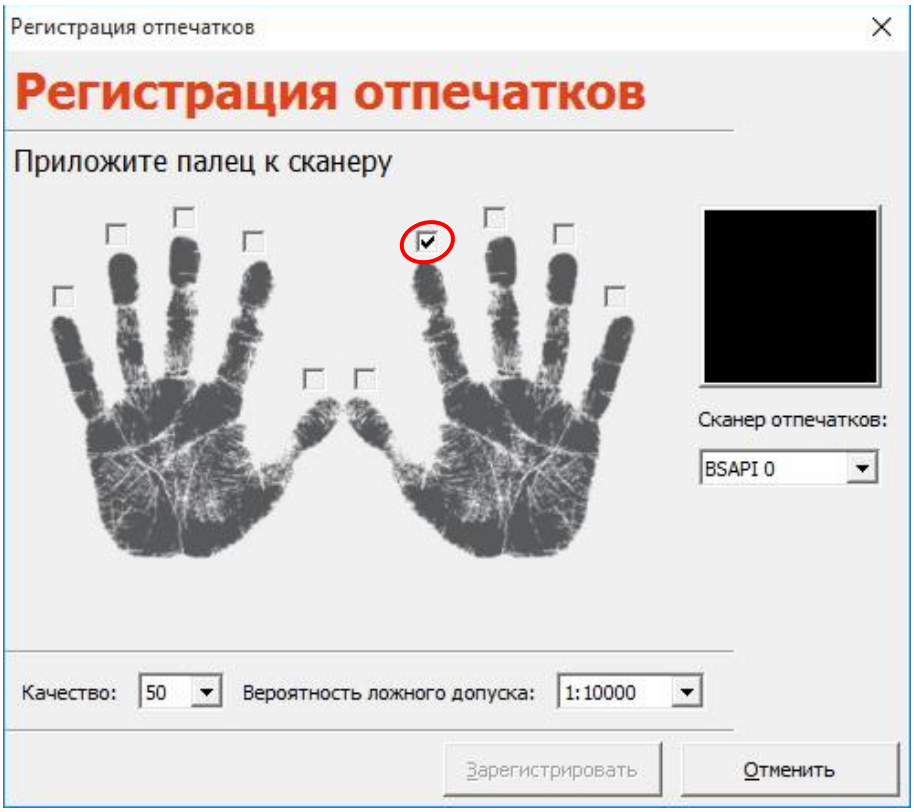

Рисунок 40

2. При необходимости измените дополнительные параметры сканирования. Описание дополнительных параметров сканирования приведено в таблице 25.

Таблица 25

Настройка	Описание
Сканер отпечатков	Используемый сканер отпечатков пальцев.
Качество изображения	Определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться.
Вероятность ложного допуска	Определяет вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000. Рекомендуемое значение: 1:10000.

Таблица 25

3. Будущий владелец электронного ключа должен приложить отмеченный палец к сканеру отпечатков пальцев.

После считывания отпечатка пальца отобразится следующее окно (см. рис. 41).

Результат считывания отпечатка пальца

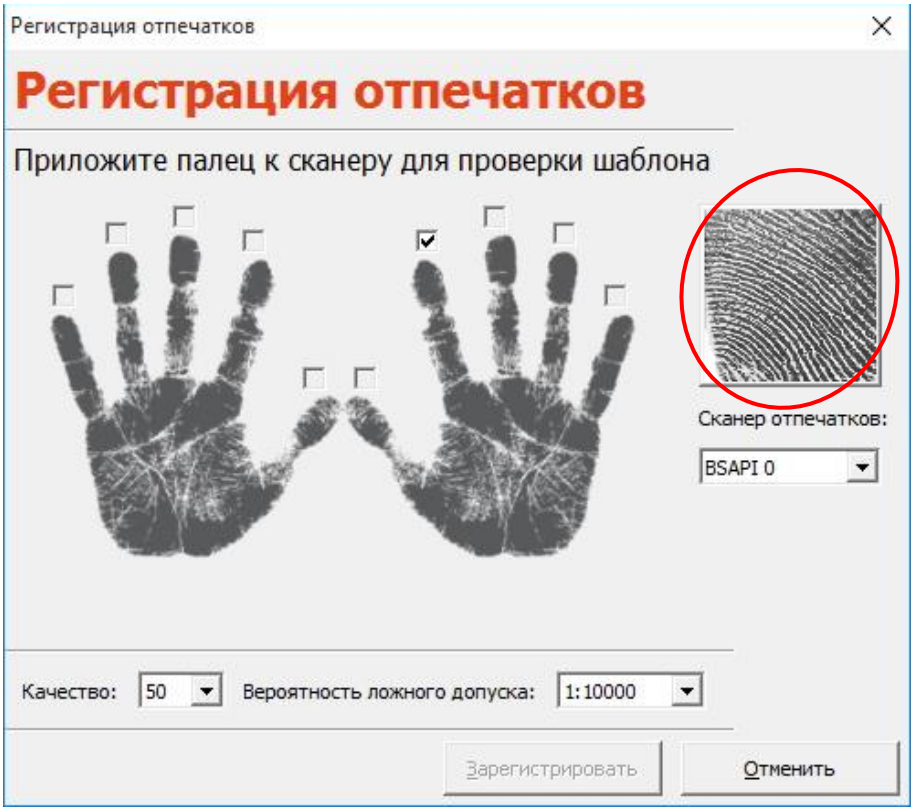

Рисунок 41

4. После того, как приложенный палец будет убран со сканера отпечатков, отобразится следующее окно (см. рис. 42). Нажмите **ОК**.

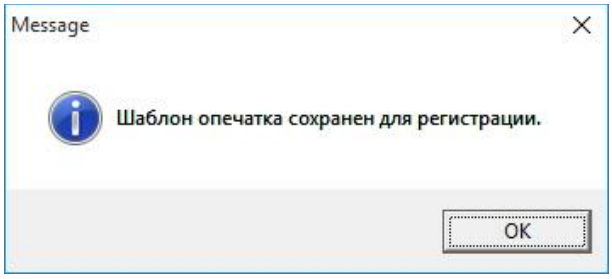

Рисунок 42

В окне регистрации отпечатков станет доступна кнопка **Зарегистрировать** (см. рис. 43).

Окно регистрации отпечатков

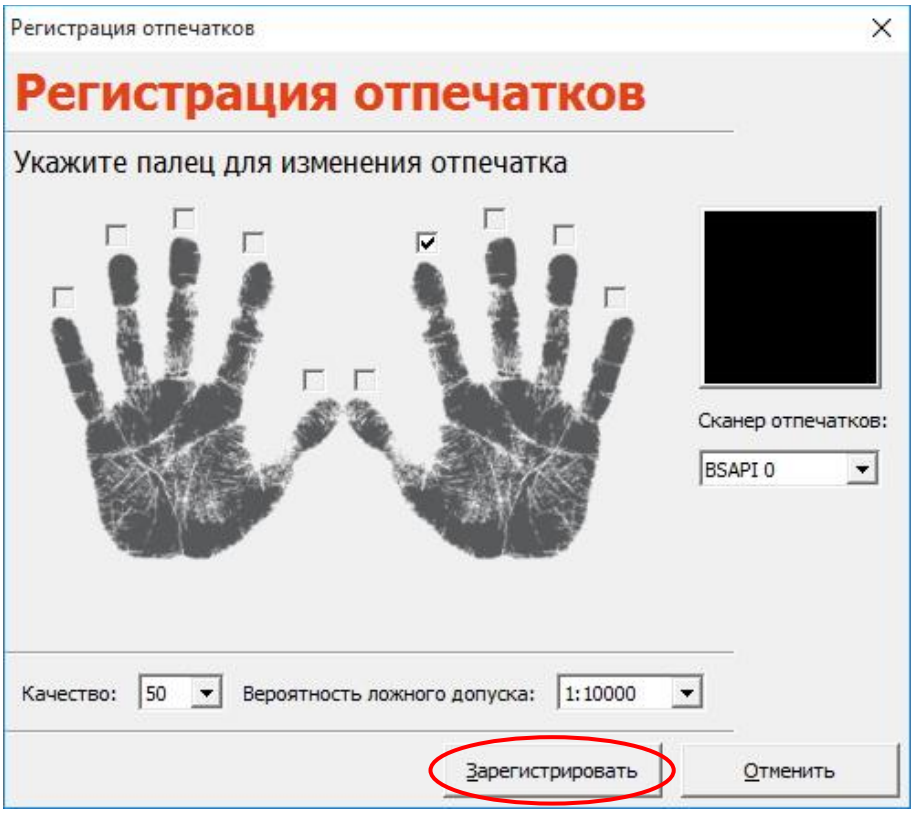

Рисунок 43

5. Нажмите **Зарегистрировать**. В отобразившемся окне (см. рис. 44) нажмите **ОК**.

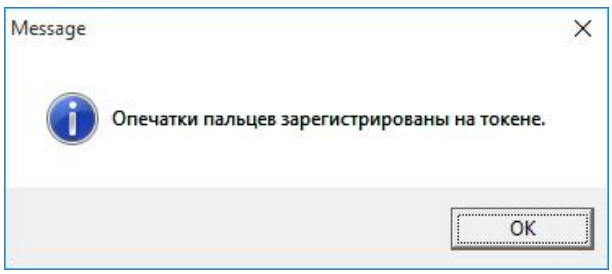

Рисунок 44

6. Если в настройках инициализации было указано, что в памяти электронного ключа нужно сохранить несколько отпечатков пальцев, повторите необходимые шаги настоящей процедуры для сохранения их всех.

7. При успешном завершении инициализации отобразится соответствующее сообщение (см. рис. 45). Нажмите **ОК** для его закрытия.

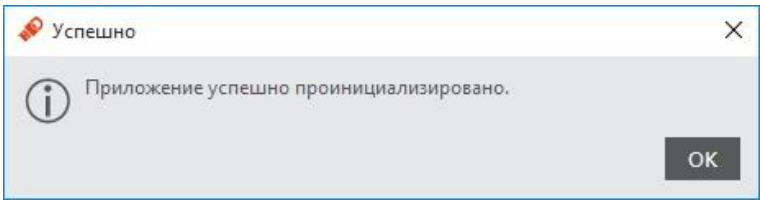

Рисунок 45

Электронный ключ можно передавать пользователю.

8.3. Приложения ГОСТ и STORAGE

Чтобы подготовить электронный ключ к работе, выполните следующие действия:

1. Запустите Единый клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините нужный электронный ключ к компьютеру, выберите его в левой панели интерфейса Единого клиента JaCarta и в центральной части окна в зависимости от того, какое приложение установлено на ключе, выберите вкладку **ГОСТ** или **STORAGE**.
3. Нажмите **Инициализировать**. Отобразится следующее окно (см. рис. 46).

Окно инициализации электронного ключа

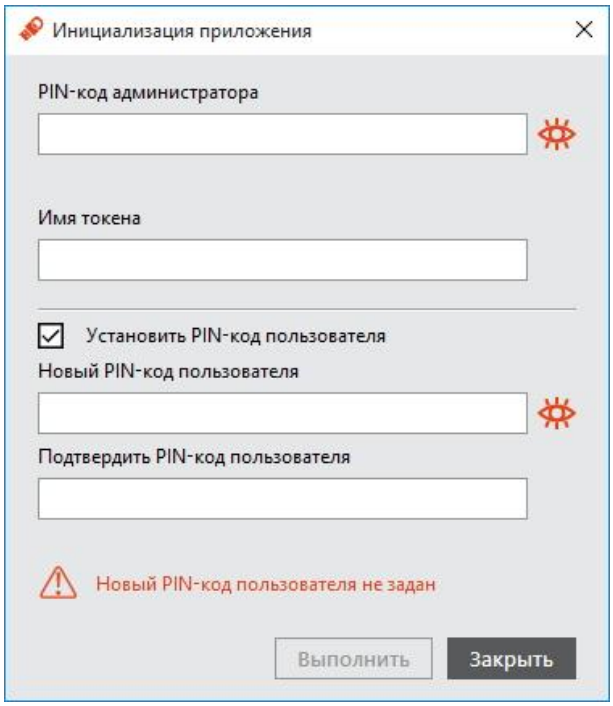

Рисунок 46

4. Выполнить настройку. Описание настроек инициализации электронного ключа приведено в таблице 26.

Таблица 26

Настройка	Описание
PIN-код администратора	Введите в этом поле текущий PIN-код администратора (см. 1.3.1. Параметры электронных ключей при поставке).
Имя токена	Введите значение, которое станет меткой инициализируемого приложения.
Установить PIN-код пользователя	• Если вы инициализируете приложение ГОСТ – установите флажок, если хотите задать PIN-код пользователя на этапе инициализации. Вы также можете снять флажок, если хотите задать PIN-код пользователя позже. • Если вы инициализируете приложение STORAGE - приложение STORAGE не может быть инициализировано без PIN-кода пользователя, поэтому нельзя снять этот флажок.
Новый PIN-код пользователя	Введите новое значение PIN-кода пользователя. (Поле активно, только если установлен флажок **Установить PIN-код пользователя**.)
Подтверждение PIN-кода	Введите подтверждение нового значения PIN-кода пользователя. (Поле активно, только если установлен флажок **Установить PIN-код пользователя**.)

Таблица 26

5. Нажмите **Выполнить** и подтвердите свой выбор в окне с предупреждающим сообщением.
6. При успешной инициализации отобразится соответствующее сообщение – нажмите **ОК**, чтобы закрыть его.

9. Установка (смена) PIN-кода пользователя администратором

Для некоторых приложений администратор может задать PIN-код пользователя, если PIN-код пользователя не был назначен во время инициализации. Также, администратор может сменить текущий PIN-код пользователя. Подробнее см. «1.3.1. Параметры электронных ключей при поставке» и «1.3.2. Операции с электронными ключами».

Для установки или смены PIN-кода пользователя администратором электронного ключа необходимо, чтобы на этом электронном ключе был установлен PIN-код администратора.

Внимание!

После введения неправильного PIN-кода администратора несколько раз подряд электронный ключ блокируется. Не допускайте блокировки PIN-кода администратора на электронных ключах JaCarta. PIN-код администратора, в отличие от PIN-кода пользователя, разблокировать невозможно.

В случае блокировки электронного ключа после неправильного введения PIN-кода администратора электронный ключ разблокировать нельзя. В этом случае можно обратиться в службу техподдержки и переинициализировать электронный ключ, но с потерей всех данных, хранящихся на нем. Данная операция доступна не для всех моделей. Подробности следует уточнять в службе техподдержки.

Заданное количество попыток ввода PIN-кода администратора, а также оставшееся количество попыток можно узнать запустив Единый клиент JaCarta перейдя на вкладку **Информация о токене** и кликнув ссылку **Полная информация…**.

Чтобы сменить PIN-код пользователя, выполните следующие действия:

1. Подсоедините электронный ключ, на котором необходимо установить/сменить PIN-код пользователя к компьютеру, запустите Единый клиент JaCarta и перейдите в режим администратора.
2. В левой панели Единого клиента JaCarta выберите нужный электронный ключ и в центральной части окна выберите вкладку, соответствующую приложению, для которого необходимо назначить (сменить) PIN-код пользователя.
3. Нажмите **Установить PIN-код пользователя**. Отобразится следующее окно (см. рис.47).

Окно установки PIN-кода пользователя

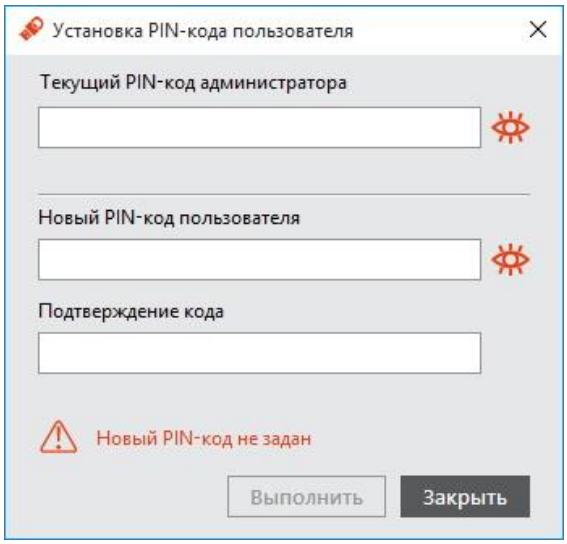

Рисунок 47

4. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора.
5. В полях **Новый PIN-код пользователя** и **Подтверждение PIN-кода** введите новый PIN-код пользователя и подтверждение соответственно.
6. Нажмите **Выполнить**.
7. При успешной установке нового PIN-кода пользователя отобразится соответствующее сообщение, нажмите **ОК**, чтобы закрыть его.

10. Разблокировка PIN-кода пользователя (в присутствии администратора)

Если пользователь превысил максимальное допустимое число последовательных неверных попыток ввода PIN-кода пользователя, то PIN-код пользователя блокируется. Процедура разблокировки PIN-кода пользователя различается в зависимости от приложения, установленного в память электронного ключа:

- PKI и PKI/BIO – после разблокировки администратор должен установить новый PIN-код пользователя.

- ГОСТ и STORAGE – разблокировка обнуляет счётчик неверных попыток доступа, значение PIN-кода пользователя остаётся прежним.

10.1. Приложения PKI и PKI/BIO

Чтобы разблокировать PIN-код пользователя, выполните следующие действия:

1. Подсоедините электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустите Единый клиент JaCarta и перейдите в режим администратора.
3. В левой панели Единого клиента JaCarta выберите нужный электронный ключ и в центральной части в зависимости от установленного в памяти электронного ключа приложения окна выберите вкладку **PKI** или **PKI/BIO**.
4. Если PIN-код пользователя заблокирован, будет отображаться значок **Разблокировать PIN-код пользователя** (см. рис. 48).

Значок разблокировать PIN-код пользователя

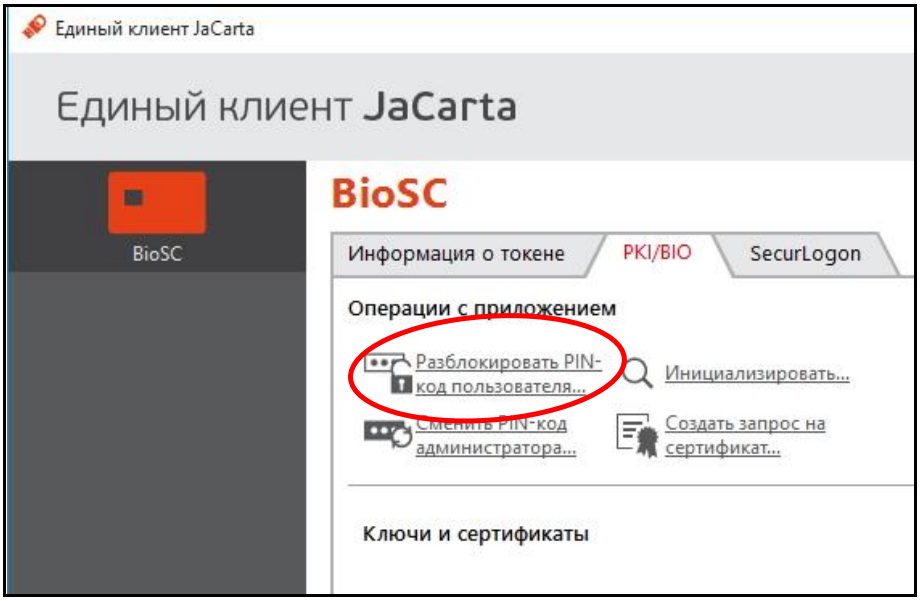

Рисунок 48

5. Нажмите **Разблокировать PIN-код пользователя**. Отобразится следующее окно (см. рис. 49).

Окно разблокировки PIN-кода пользователя

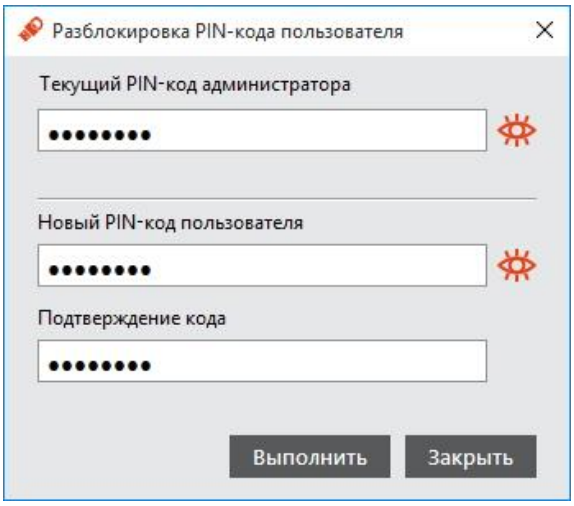

Рисунок 49

6. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора.
7. В полях **Новый PIN-код пользователя** и **Подтверждение PIN-кода** введите новый PIN-код пользователя и подтверждение соответственно, после чего нажмите **Выполнить**.
8. При успешной разблокировке и назначении нового PIN-кода пользователя отобразится соответствующее сообщение (см. рис. 50)– нажмите **ОК**, чтобы закрыть его.

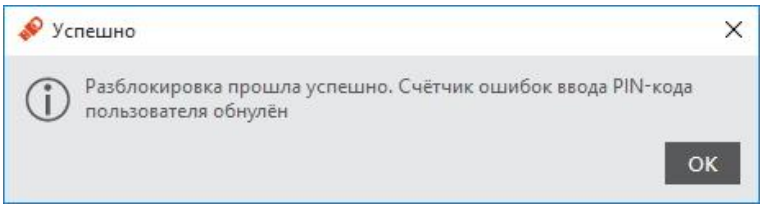

Рисунок 50

После произведенных действий электронный ключ можно передавать пользователю.

10.2. Приложения ГОСТ и STORAGE

Чтобы разблокировать PIN-код пользователя, выполните следующие действия:

1. Подсоедините электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустите Единый клиент JaCarta и перейдите в режим администратора.
3. В левой панели Единого клиента JaCarta выберите нужный электронный ключ и в центральной части в зависимости от установленного в памяти электронного ключа приложения окна выберите вкладку **ГОСТ** или **STORAGE**.

Если PIN-код пользователя заблокирован, будет отображаться значок **Разблокировать PIN-код пользователя** (см. рис. 51).

Значок разблокировки PIN-кода пользователя

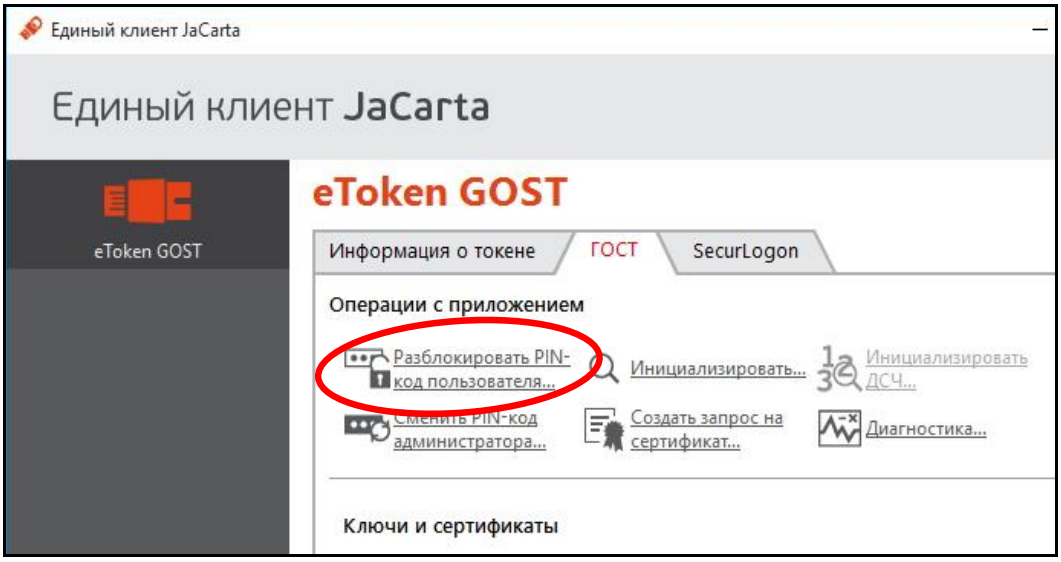

Рисунок 51

4. Нажмите **Разблокировать PIN-код пользователя**. Отобразится следующее окно (см. рис. 52).

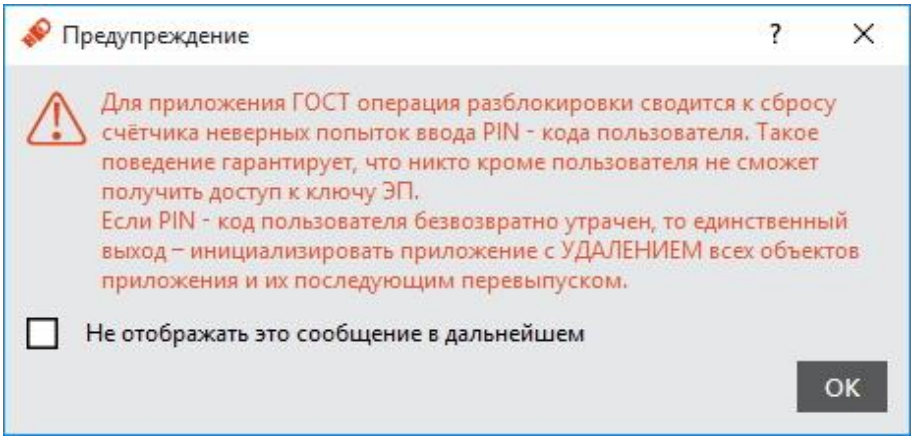

Рисунок 52

5. Нажмите **ОК**. Отобразится следующее окно (см. рис. 53).

Окно разблокировки PIN-кода пользователя

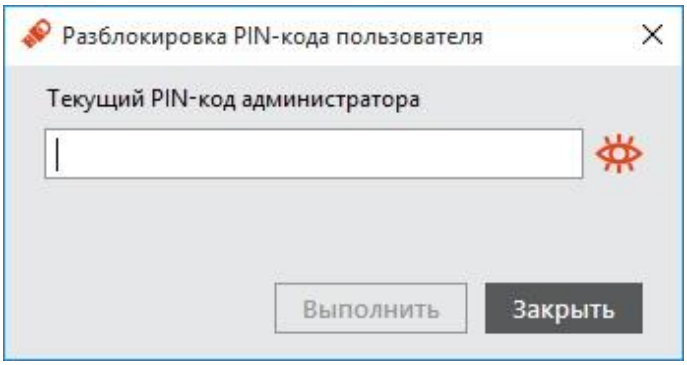

Рисунок 53

6. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора, после чего нажмите **Выполнить**.

При разблокировке PIN-кода пользователя сбрасывается счётчик неверных попыток ввода PIN-кода пользователя, при этом само значение PIN-кода пользователя остаётся неизменным. При необходимости изменить значение PIN-кода пользователя воспользуйтесь процедурой инициализации.

7. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. рис. 54). Нажмите **OK**, чтобы закрыть его.

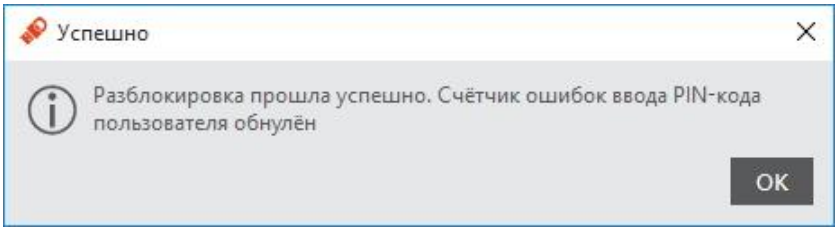

Рисунок 54

11. Разблокировка PIN-кода пользователя (в удалённом режиме)

Разблокировка PIN-кода пользователя в удалённом режиме доступна только для электронных ключей с приложениями PKI и PKI/BIO (подробнее см. 1.3.1. Параметры электронных ключей при поставке).

Для возможности разблокировки электронного ключа в удалённом режиме:

- необходимо, чтобы в организации была установлена система учёта и управления аппаратных средств аутентификации; в настоящем документе для примера будет использоваться система JaCarta Management System (подробнее см. документ [JaCarta Management System. Руководство администратора]);
- необходимо, чтобы электронный ключ, подлежащий разблокированию был зарегистрирован в системе учёта и управления аппаратных средств аутентификации до момента его блокировки;
- если используются электронные ключи eToken и JaCarta PKI с функцией обратной совместимости с продуктами компании Аладдин, необходимо, чтобы они были инициализированы с заданным PIN-кодом администратора;
- если используются электронные ключи JaCarta, необходимо, чтобы в качестве PIN-кода администратора при инициализации был задан ключ 3DES (см. раздел 8. Инициализация электронных ключей).

Чтобы разблокировать PIN-код пользователя в удалённом режиме, выполните следующие действия:

1. Проинструктируйте пользователя (например, по телефону) подключить электронный ключ с заблокированным PIN-кодом пользователя к компьютеру и запустить Единый клиент JaCarta.

Окно Единого клиента JaCarta на экране пользователя будет выглядеть следующим образом (см. рис.55).

Окно с заблокированным PIN-кодом пользователя в режиме пользователя

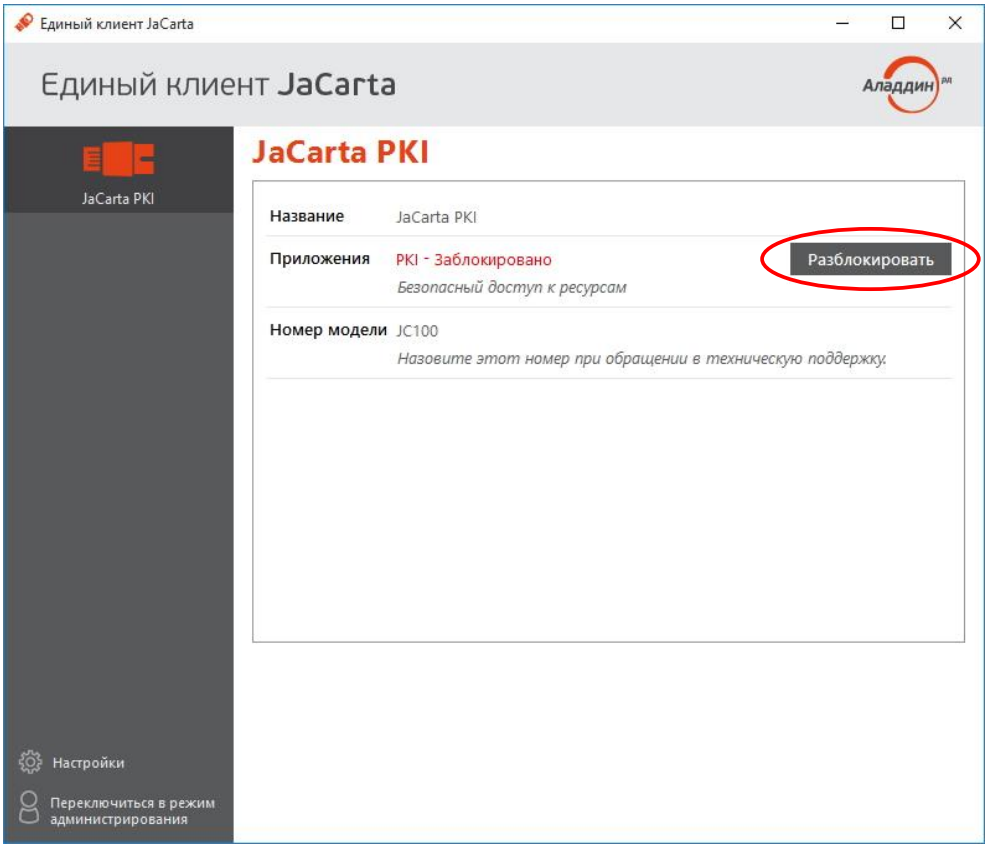

Рисунок 55

2. Пользователь должен нажать **Разблокировать**. На экране пользователя отобразится следующее окно (см. рис.56).

Окно задания нового PIN-кода пользователя

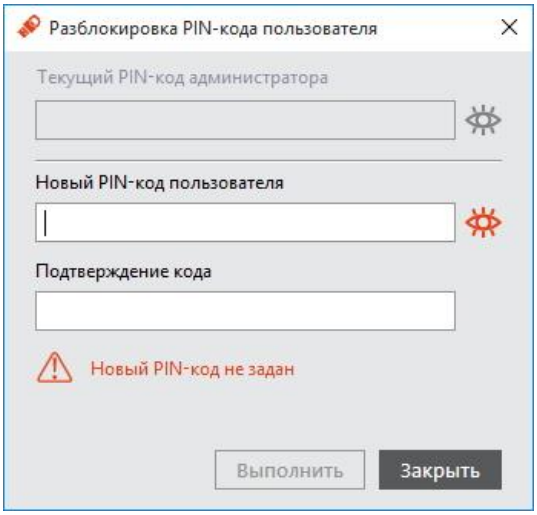

Рисунок 56

3. В полях **Новый PIN-код пользователя** и **Подтверждение PIN-кода** пользователь должен ввести новое значение PIN-кода пользователя и подтверждение соответственно, после чего пользователь должен нажать **Выполнить**. На экране пользователя отобразится следующее окно (см. рис. 57).

Окно запрос/ответ

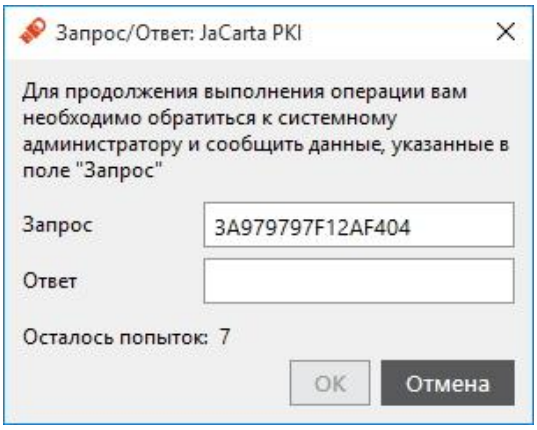

Рисунок 57

4. Пользователь должен продиктовать администратору отображающийся код запроса.
5. Администратор, используя интерфейс Консоли управления JMS должен открыть окно удалённой разблокировки (см. рис. 58).

Окно консоли управления JMS

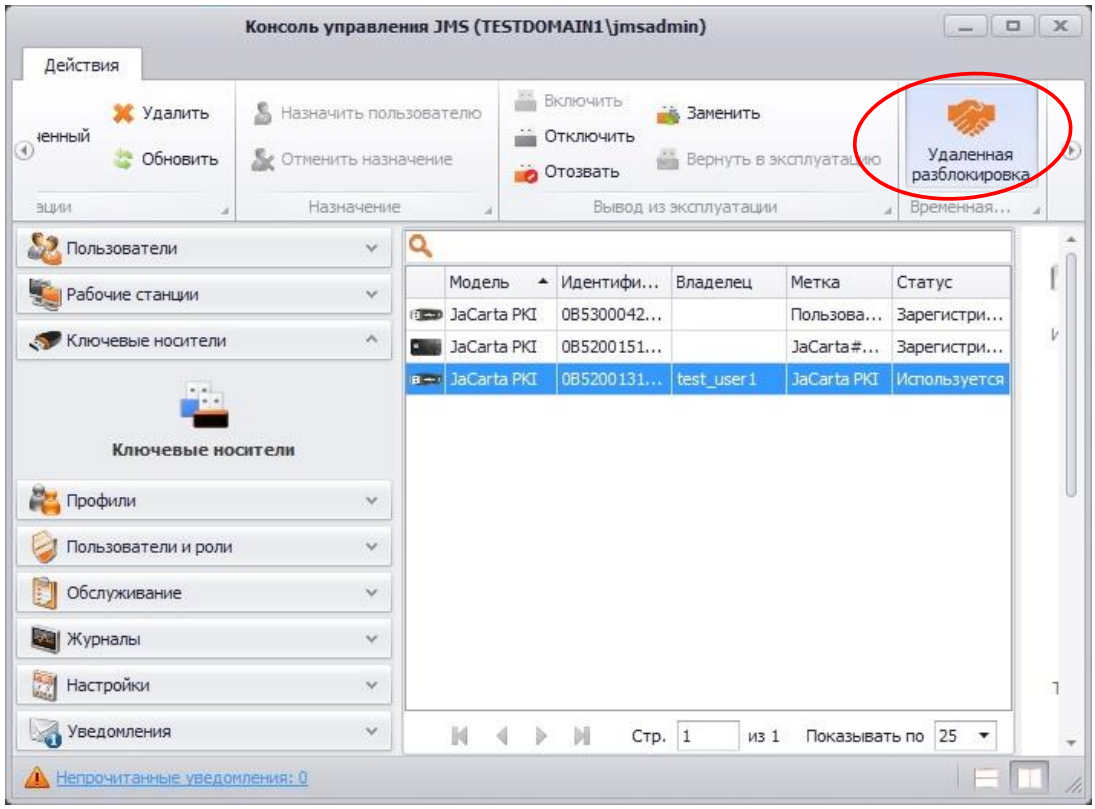

Рисунок 58

Окно удалённой разблокировки будет выглядеть следующим образом (см. рис. 59).

Окно удаленной разблокировки

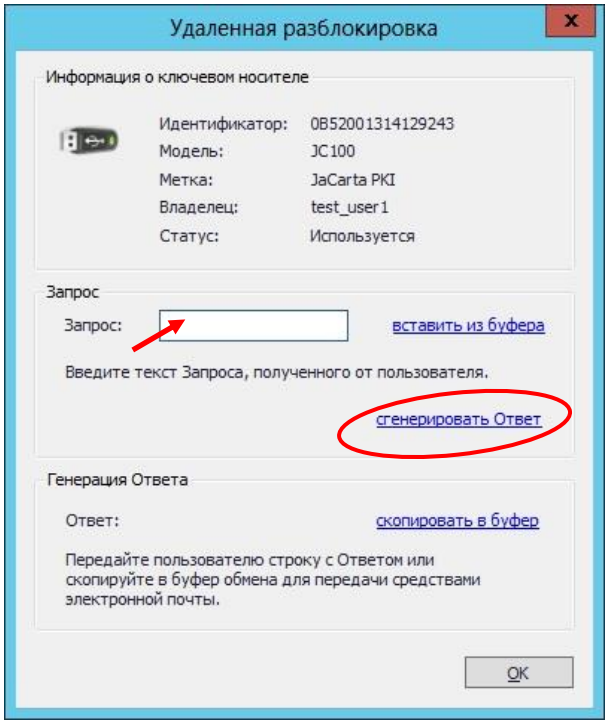

Рисунок 59

6. Администратор должен ввести код запроса, сообщённый пользователем, в поле **Запрос**, после чего нажать **сгенерировать Ответ**.

Код ответа отобразится в соответствующем поле (см. рис. 60).

Окно удаленной разблокировки с кодом ответа

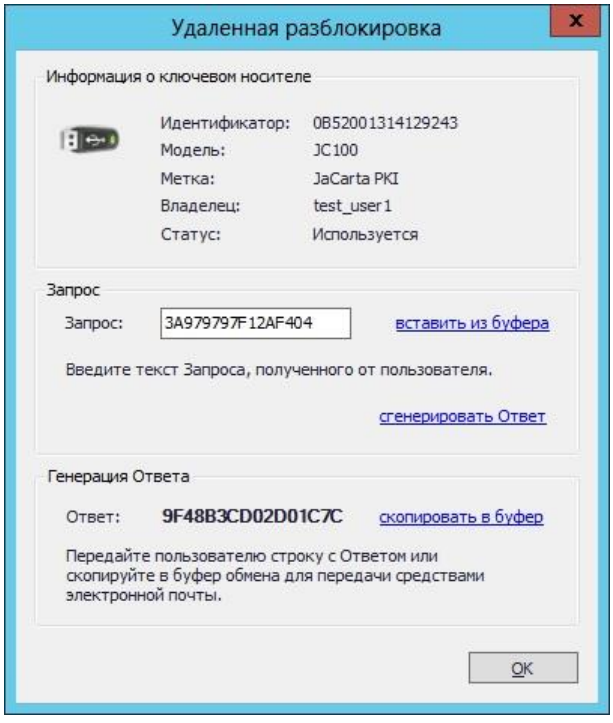

Рисунок 60

7. Администратор должен продиктовать пользователю код ответа.
8. Пользователь должен ввести код ответа в соответствующем поле (см. рис. 61) и подтвердить ввод нажатием кнопки **OK**.

Окно запрос/ответ с введенным кодом ответа

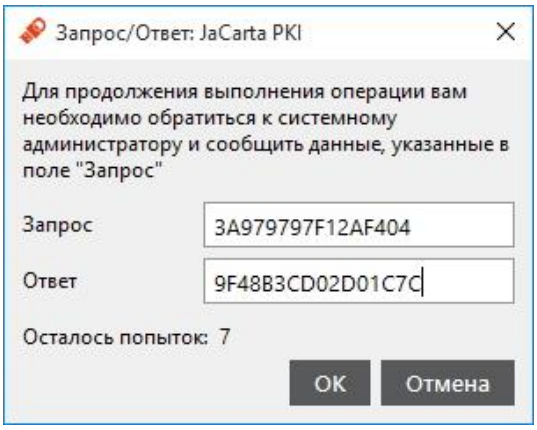

Рисунок 61

Если код ответа был введён верно, на экране пользователя отобразится следующее сообщение (см. рис. 62).

Окно успешно выполненной разблокировки

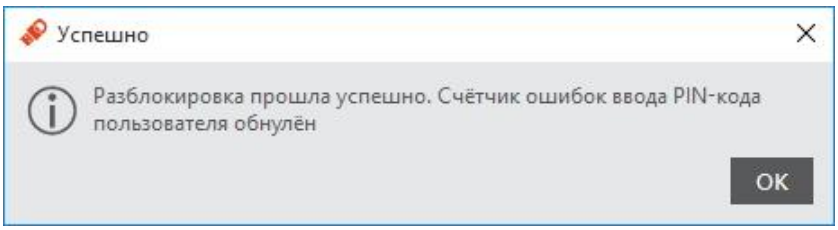

Рисунок 62

12. Смена PIN-кода администратора

PIN-код администратора может быть установлен не во всех приложениях в памяти электронных ключей. Подробнее см. «1.3.1. Параметры электронных ключей при поставке».

Внимание!

После введения неправильного PIN-кода администратора несколько раз подряд электронный ключ блокируется. Не допускайте блокировки PIN-кода администратора на электронных ключах JaCarta. PIN-код администратора, в отличие от PIN-кода пользователя, разблокировать невозможно.

В случае блокировки электронного ключа после неправильного введения PIN-кода администратора электронный ключ разблокировать нельзя. В этом случае можно обратиться в службу техподдержки и переинициализировать электронный ключ, но с потерей всех данных, хранящихся на нем.

Заданное количество попыток ввода PIN-кода администратора, а также оставшееся количество попыток можно узнать запустив Единый клиент JaCarta перейдя на вкладку **Информация о токене** и кликнув ссылку **Полная информация…**.

Чтобы сменить PIN-кода администратора, выполните следующие действия:

1. Подсоедините электронный ключ, на котором необходимо сменить PIN-код администратора, к компьютеру.
2. Запустите Единый клиент JaCarta и перейдите в режим администратора.
3. В левой панели Единого клиента JaCarta выберите нужный электронный ключ и в центральной части окна выберите вкладку, соответствующую приложению, для которого необходимо изменить PIN-код администратора.
4. Нажмите **Сменить PIN-код администратора**. Отобразится следующее окно (см. рис. 63).

Окно смены PIN-кода администратора

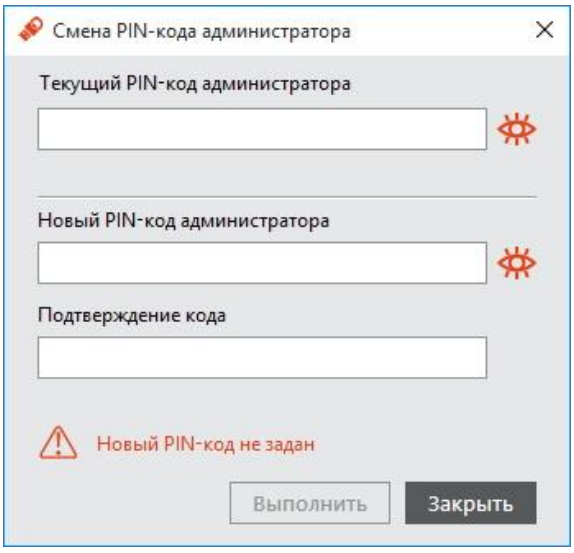

Рисунок 63

5. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора.
6. В полях **Новый PIN-код администратора** и **Подтверждение PIN-кода** введите новый PIN-код администратора и подтверждение соответственно.
7. Нажмите **Выполнить**.
8. При успешной смене PIN-кода отобразится соответствующее сообщение – нажмите **ОК**, чтобы закрыть его.

13. Создание запроса на сертификат

Чтобы создать запрос на сертификат, выполните следующие действия:

1. Подсоедините электронный ключ к компьютеру.
2. Запустите Единый клиент JaCarta, в левой панели Единого клиента JaCarta выберите нужный электронный ключ и перейдите в режим администратора.
3. В центральной части окна выберите вкладку, соответствующую приложению, для которого необходимо создать запрос на сертификат, отобразится следующее окно (см. рис. 64).

Окно Единый клиент JaCarta в режиме администратора на вкладке PKI

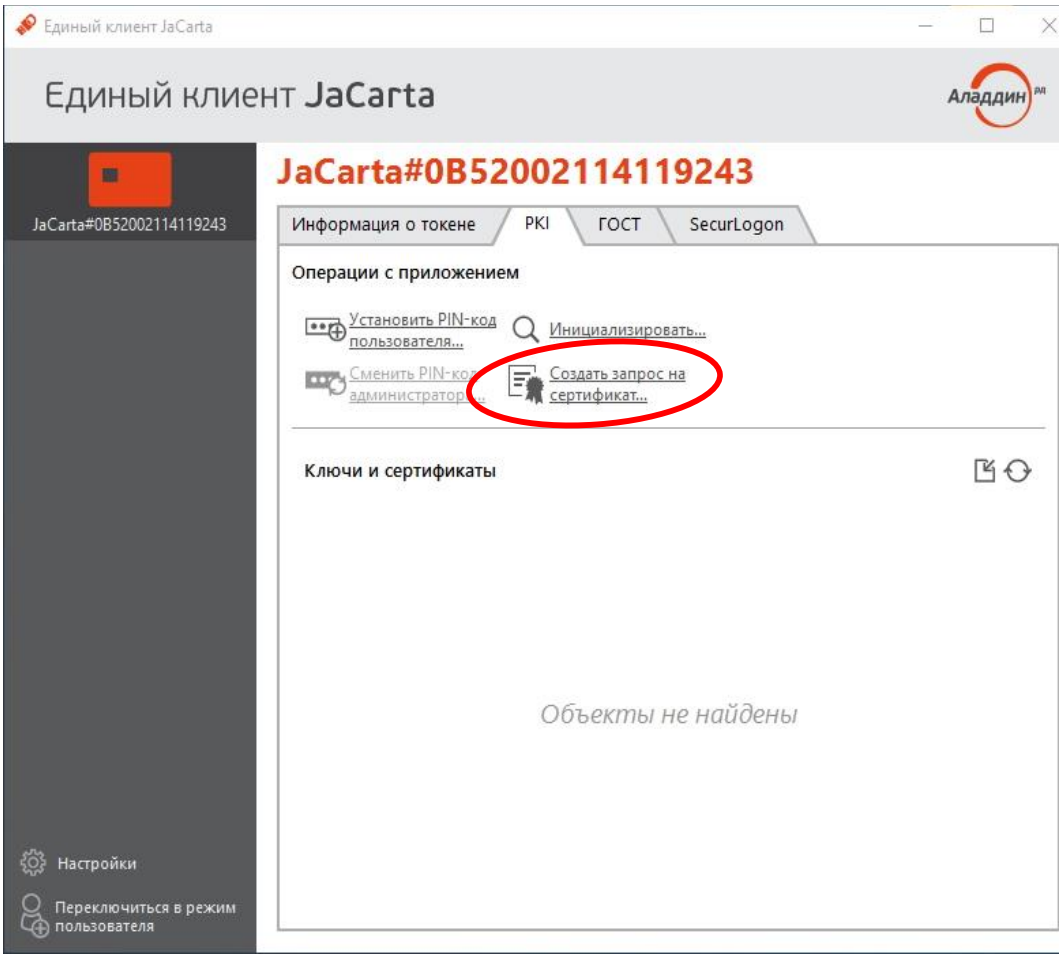

Рисунок 64

4. Нажмите **Создать запрос на сертификат….** Отобразится следующее окно (см. рис. 65).

Окно введите PIN-код пользователя

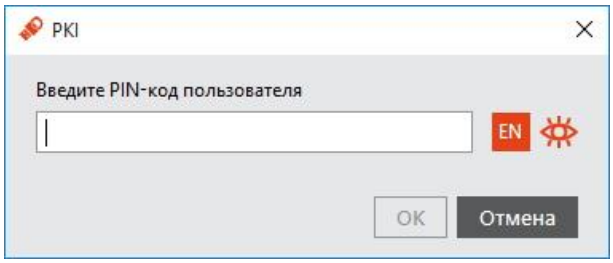

Рисунок 65

5. Введите PIN-код пользователя и нажмите **ОК**. Отобразится следующее окно (см. рис. 66).

Окно создания запроса на сертификат

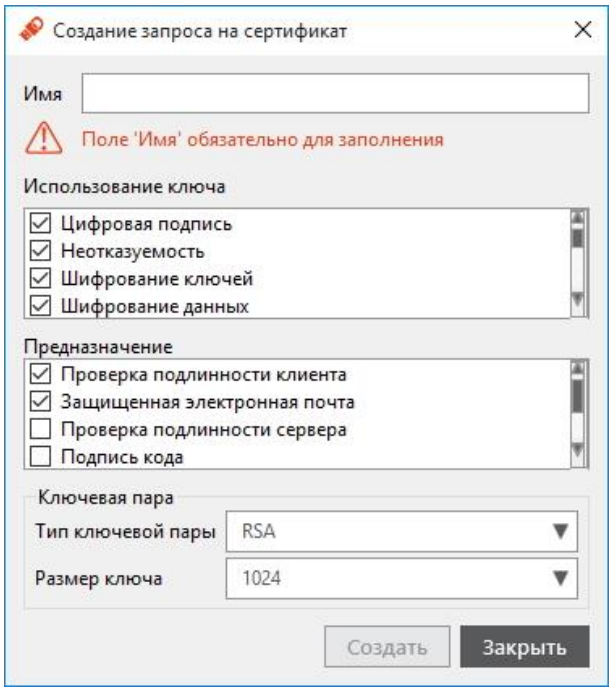

Рисунок 66

6. Введите имя запроса, выберите необходимые опции в поле **Использование ключа**, после чего нажмите кнопку **Создать**. Отобразится следующее окно (см. рис. 67).

Окно сохранения запроса

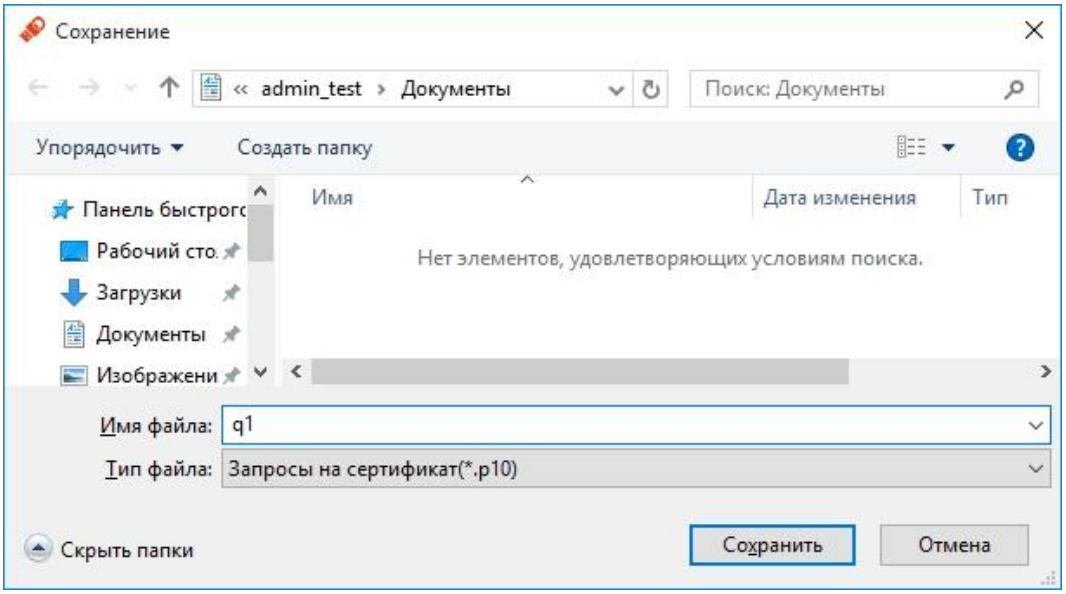

Рисунок 67

7. Введите имя файла для сохранения запроса, выберите формат сохранения из раскрывающегося списка и нажмите **Сохранить**. Отобразится следующее окно (см. рис. 68).

Окно сообщения о созданном запросе на сертификат

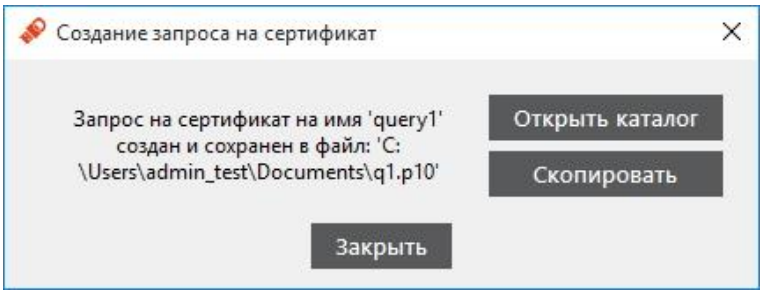

Рисунок 68

8. Если хотите убедиться, что запрос на сертификат сохранен в файл и перейти в каталог с сохраненным запросом на сертификат – нажмите **Открыть каталог** .
9. Если хотите скопировать содержимое запроса в буфер обмена – нажмите **Скопировать**. Запрос копируется в одну строку без тегов.
10. Нажмите **Закрыть** для завершения.

После выпуска сертификата его можно импортировать на токен (подробнее см. документ [*Единый клиент JaCarta. Руководство пользователя*] раздел 5).

14. Операции с объектами в памяти электронных ключей

Для выполнения операций с объектами (ключевыми контейнерами, цифровыми сертификатами) в памяти электронных ключей необходимо предъявлять PIN-код пользователя. Исключение составляют электронные ключи с приложением ФКН.

Сведения об операциях с объектами в памяти электронных ключей приведены в документе [*Единый клиент JaCarta. Руководство пользователя*].

15. Выпуск электронных ключей на примере удостоверяющего центра Microsoft Windows

Процедура выпуска электронного ключа на примере удостоверяющего центра Microsoft Windows предусматривает подготовку шаблонов сертификатов, установку сертификатов и выпуск электронного ключа.

В приведенном ниже описании рассмотрена процедура выпуска электронного ключа с приложением PKI в операционных системах Windows7/Server 2008/Server 2012 с установленными службами Microsoft Windows (AD DS и AD CS).

Процедура включает следующие этапы:

1. Подготовка шаблонов сертификатов:
1.1. Шаблон сертификата **Агент регистрации** – для администратора, который будет отвечать за выпуск электронных ключей.
1.2. Шаблон сертификата **Пользователь со смарт-картой** – сертификаты по этому шаблону будут записываться в память электронных ключей во время выпуска.
2. Установка сертификата **Агент регистрации** в локальное хранилище на компьютере администратора.
3. Выпуск электронного ключа.

15.1. Подготовка шаблонов сертификатов

1. Намите ПУСК =>Администрирование => Центр сертификации. Разверните узел центра сертификации, затем нажмите правой кнопкой мыши на пункте Шаблоны сертификатов и выберите Управление (см. рис. 69).

Окно управления шаблонами сертификатов

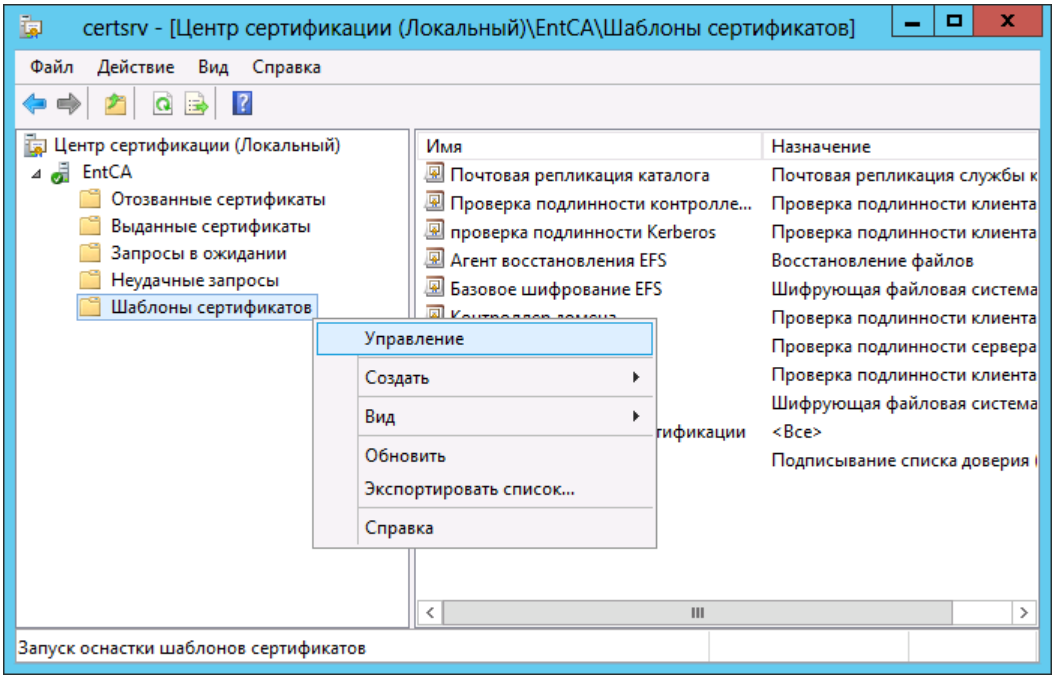

Рисунок 69

Отобразится следующее окно (см. рис. 70).

Окно консоли шаблонов сертификатов

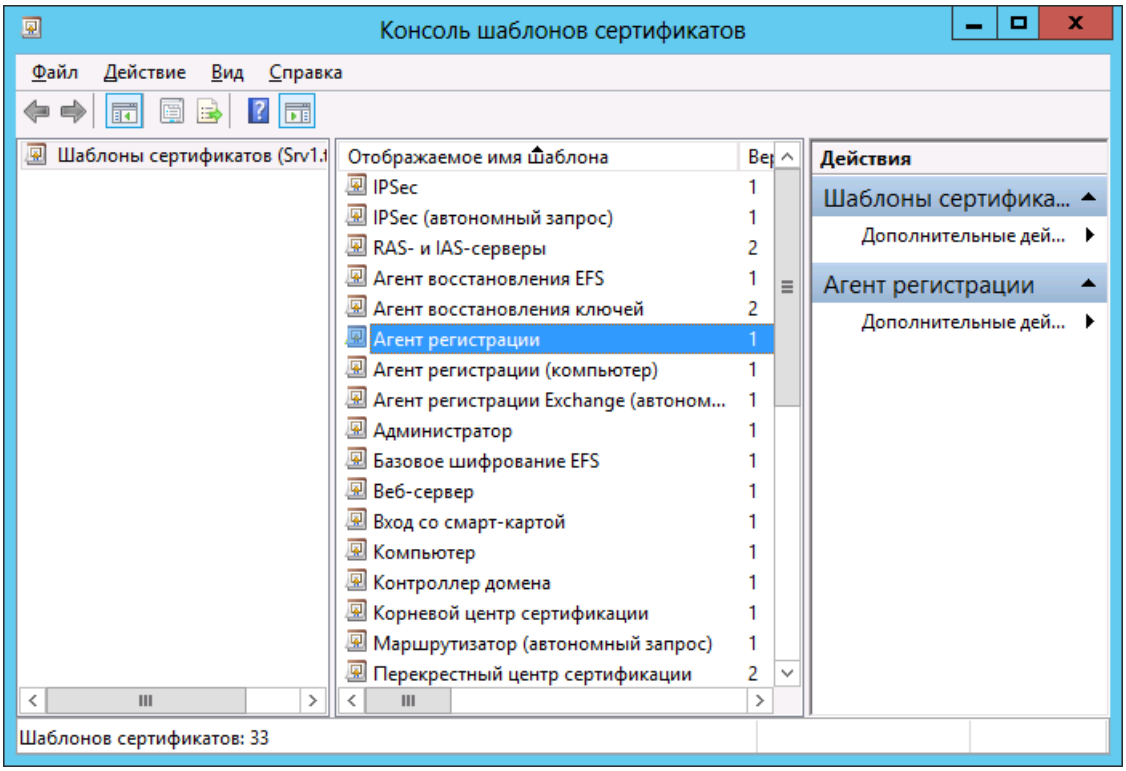

Рисунок 70

2. В зависимости от того, какой шаблон вы хотите создать, нажмите правой кнопкой мыши на соответствующем шаблоне и выберите **Скопировать шаблон**.

Если вы используете Windows Server 2008, отобразится окно, в котором вам будет предложено выбрать версию шаблона сертификата: **Windows Server 2003 Enterprise** или **Windows Server 2008 Enterprise**. Выберите первый пункт (**Windows Server 2003 Enterprise**) и нажмите **OK**.

15.1.1. Подготовка шаблона сертификата для Агента регистрации

1. В отобразившемся окне перейдите на вкладку **Общие**. Окно примет следующий вид (см. рис. 71).
2. В поле **Отображаемое имя шаблона** введите имя создаваемого шаблона, например, **Агент регистрации Единого клиента JaCarta**.
3. Перейдите на вкладку **Безопасность**. Окно примет следующий вид (см. рис. 72).

Окно свойств нового шаблона сертификата. Вкладка Общие.

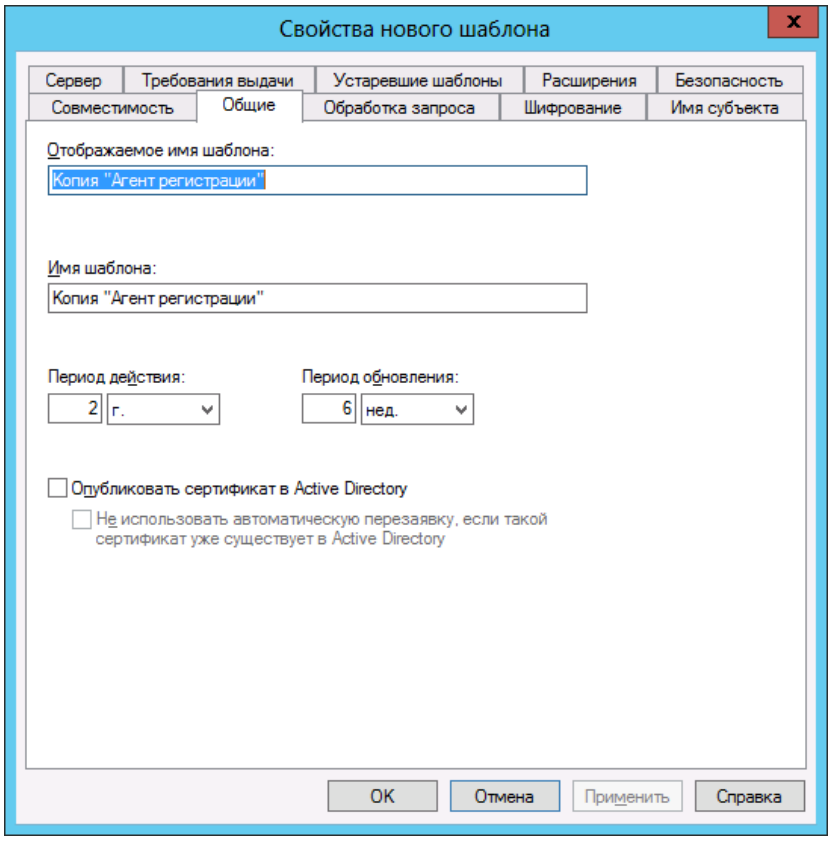

Рисунок 71

Окно свойств нового шаблона сертификата. Вкладка Безопасность.

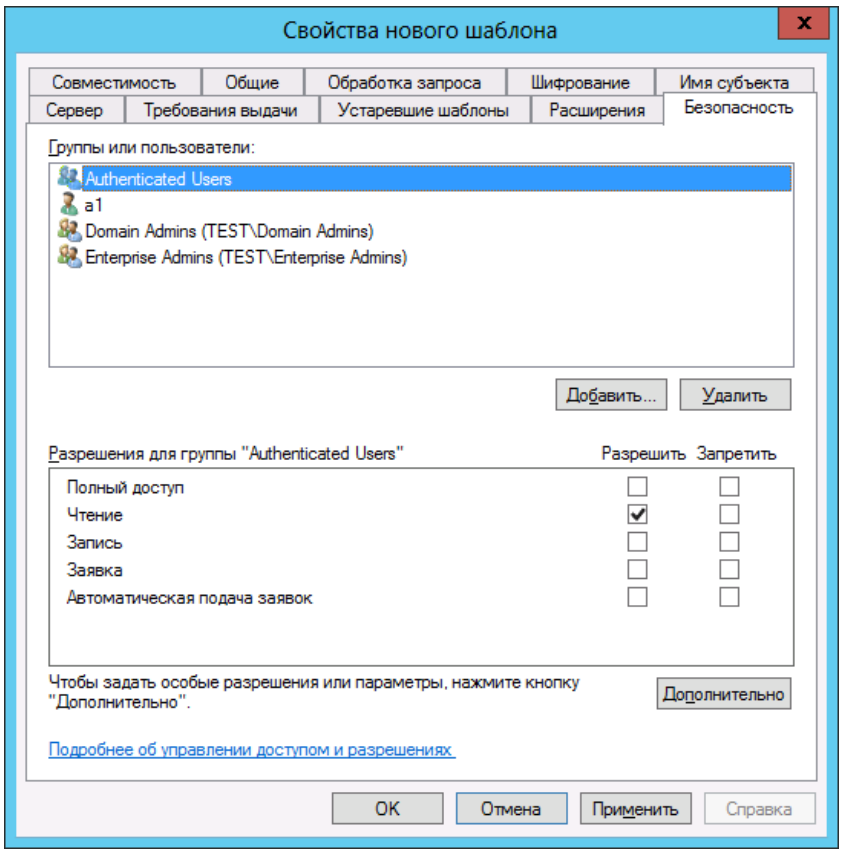

Рисунок 72

15.1.2. Подготовка шаблона сертификата для Пользователя со смарт-картой

Процедура отличается в зависимости от используемой операционной системы:

- ОС Windows Server 2008

или

- ОС Windows Server 2012

Процедура для ОС Windows Server 2008:

1. Перейдите на вкладку **Общие**. Окно примет следующий вид (см. рис. 73).

Окно свойств нового шаблона сертификата. Вкладка Общие.

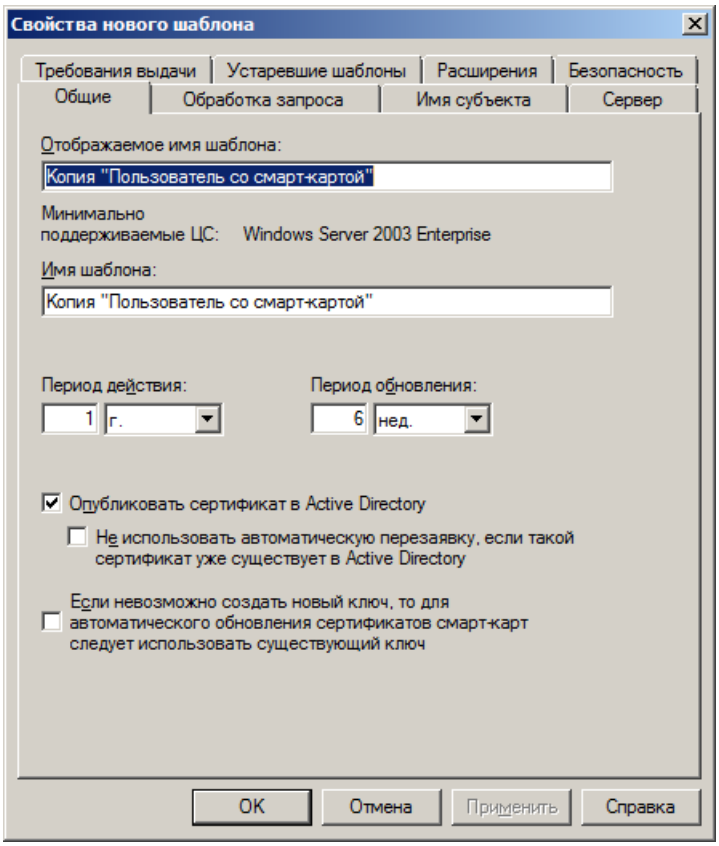

Рисунок 73

2. В поле **Отображаемое имя шаблона** введите имя шаблона сертификата, например, **Пользователь Единого клиента JaCarta**.
3. Перейдите на вкладку **Требования выдачи**. Окно примет следующий вид (см. рис. 74).

Окно свойств нового шаблона сертификата. Вкладка Требования выдачи.

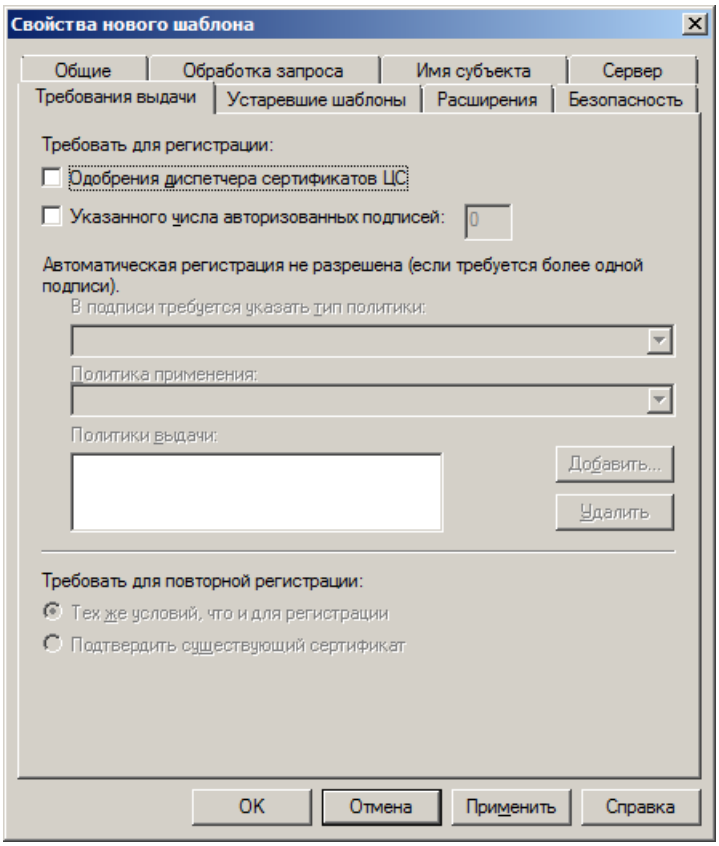

Рисунок 74

4. Выполните следующие настройки:

4.1. Установите флажок **Указанного числа авторизованных подписей**.

4.2. В списке **В подписи требуется указать тип политики** выберите **Политика применения**.

4.3. В списке **Политика применения** выберите **Агент запроса сертификата**. Настройки будут выглядеть следующим образом (см. рис. 75).

Настройки требований выдачи сертификата

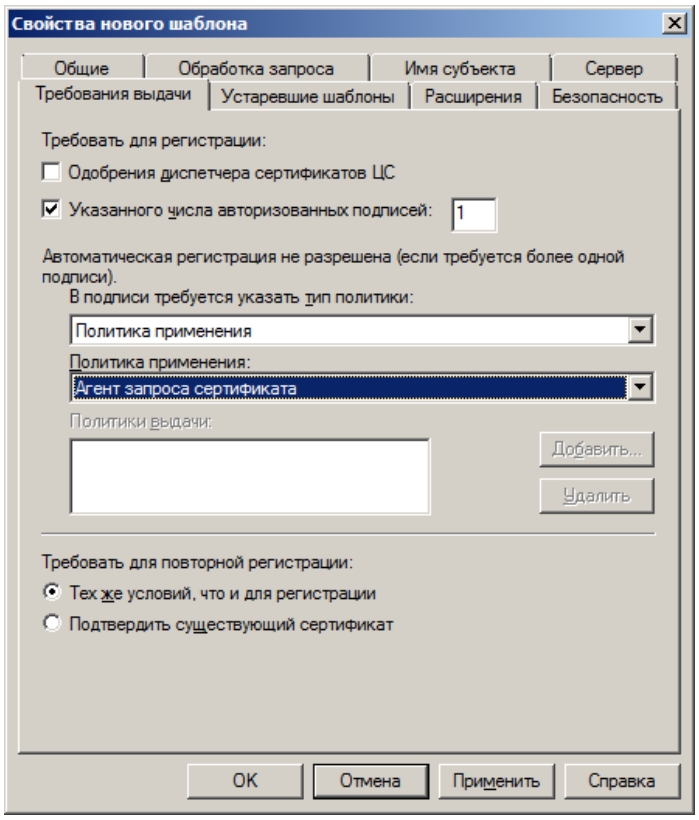

Рисунок 75

5. Перейдите на вкладку **Обработка запроса**. Окно будет выглядеть следующим образом (см. рис. 76).

Окно свойств нового шаблона сертификата. Вкладка Обработка запроса.

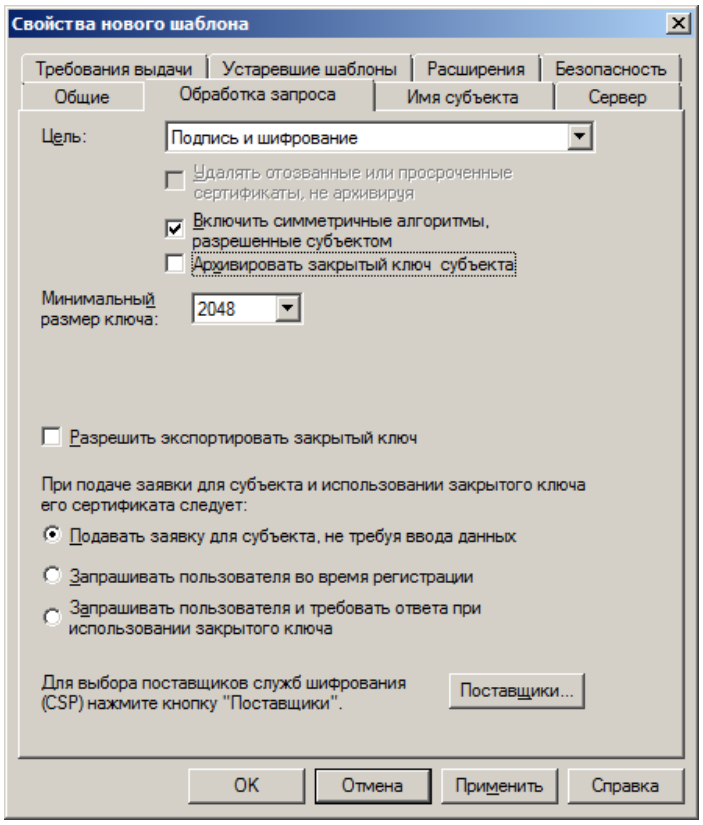

Рисунок 76

6. В поле **Минимальный размер ключа** установите значение не менее 1024.
7. Нажмите **Поставщики**. Отобразится следующее окно (см. рис. 77).

Окно выбора поставщиков

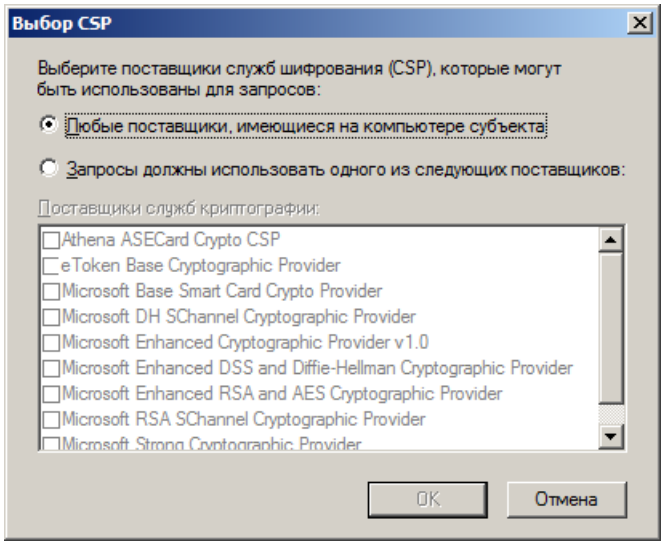

Рисунок 77

8. Выполните следующие настройки:

8.1. Выберите пункт **Запросы должны использовать одного из следующих поставщиков**.

8.2. В списке **Поставщики служб криптографии** отметьте пункт **Microsoft Base Smart Card Crypto Provider**.

9. Последовательно нажмите **ОК**, чтобы закрыть окно поставщиков служб криптографии и сохранить изменения в шаблоне.

Процедура для ОС Windows Server 2012:

1. Перейдите на вкладку Общие. Окно примет следующий вид (см. рис. 78).
2. В поле **Отображаемое имя шаблона** введите имя шаблона сертификата, например, **Пользователь Единого клиента JaCarta**.
3. Перейдите на вкладку **Требования выдачи**. Окно примет следующий вид (см. рис. 79).

Окно свойств нового шаблона сертификата. Вкладка Общие.

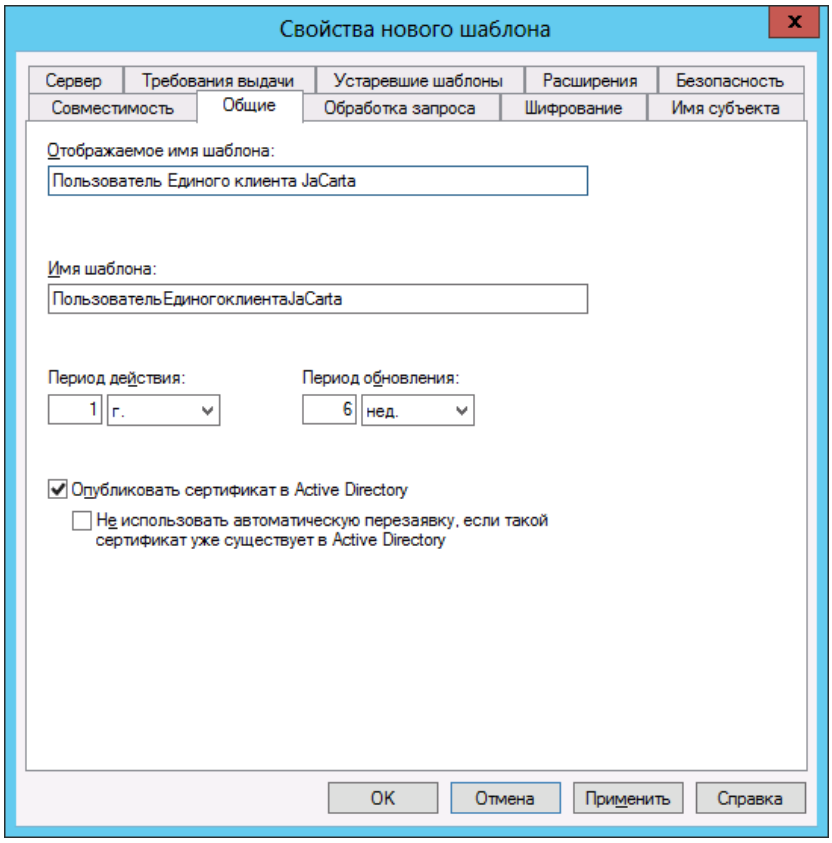

Рисунок 78

Окно свойств нового шаблона сертификата. Вкладка Требования выдачи.

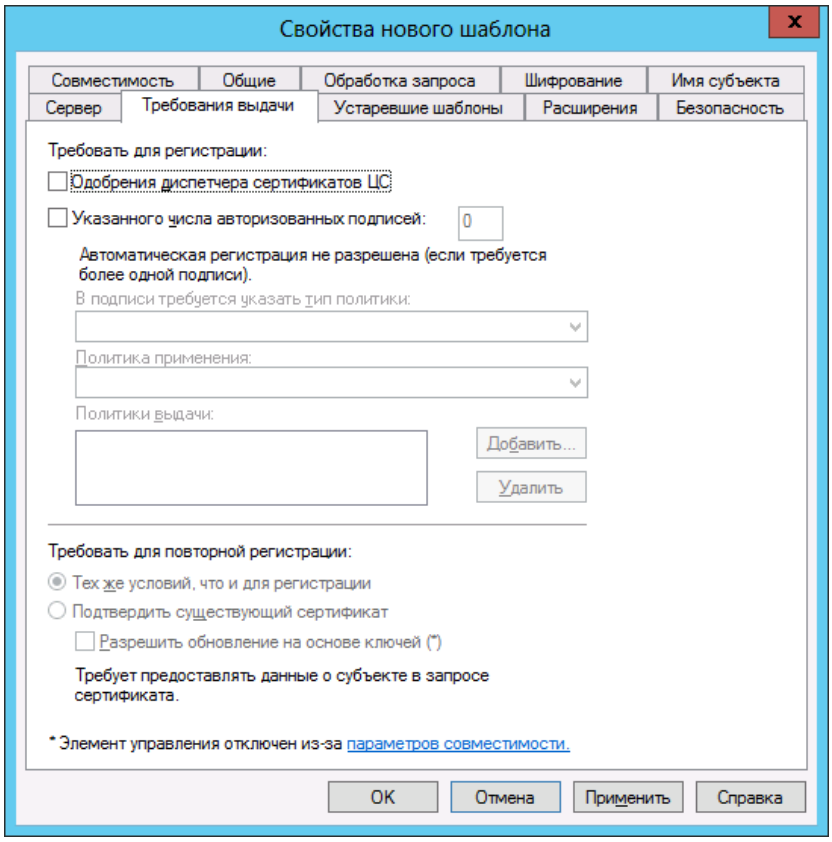

Рисунок 79

4. Выполните следующие настройки:

4.1. Установите флажок **Указанного числа авторизованных подписей**.

4.2. В списке **В подписи требуется указать тип политики** выберите **Политика применения**.

4.3. В списке **Политика применения** выберите **Агент запроса сертификата**. Настройки будут выглядеть следующим образом (см. рис. 80).

Настройки требований выдачи сертификата

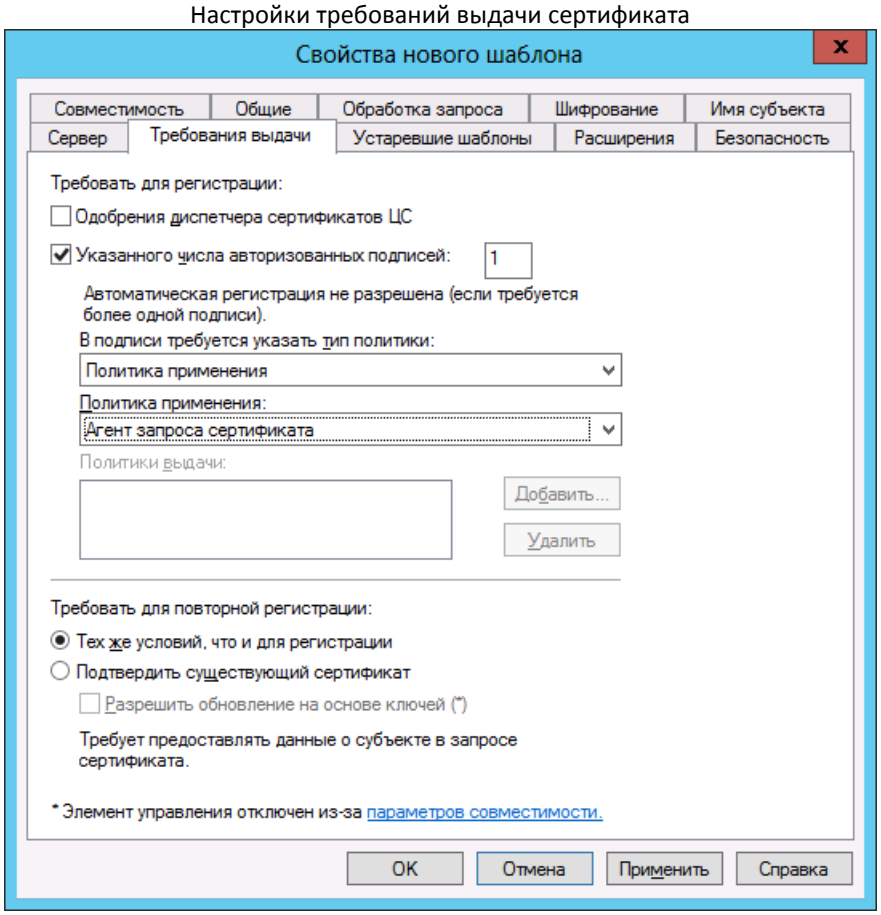

Рисунок 80

5. Перейдите на вкладку **Шифрование**. Окно будет выглядеть следующим образом (см. рис. 81).

6. Выполните следующие настройки:

6.1. В поле **Минимальный размер ключа** установите значение не менее 1024.

6.2. Выберите пункт **В запросах могут использоваться только следующие поставщики**.

6.3. В списке **Поставщики** отметьте пункт **Microsoft Base Smart Card Crypto Provider**.

7. Нажмите **OK**, чтобы сохранить изменения.

Окно свойств нового шаблона сертификата. Вкладка Шифрование.

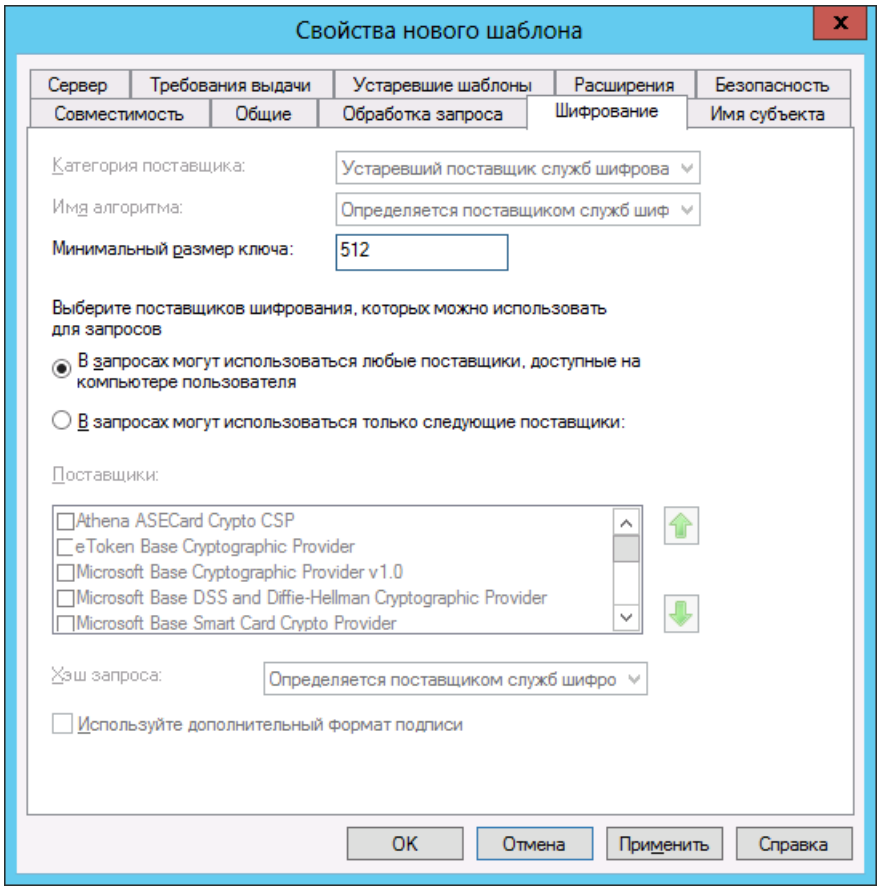

Рисунок 81

15.2. Публикация созданных шаблонов сертификатов

Чтобы опубликовать настроенные шаблоны сертификатов, выполните следующие действия.

1. В консоли управления центра сертификации разверните узел центра сертификации, нажмите правой кнопкой мыши на пункте **Шаблоны сертификатов** и выберите **Создать > Выдаваемый шаблон сертификата** (см. рис. 82). Отобразится следующее окно (см. рис. 83).

Окно публикации выдаваемого шаблона сертификата

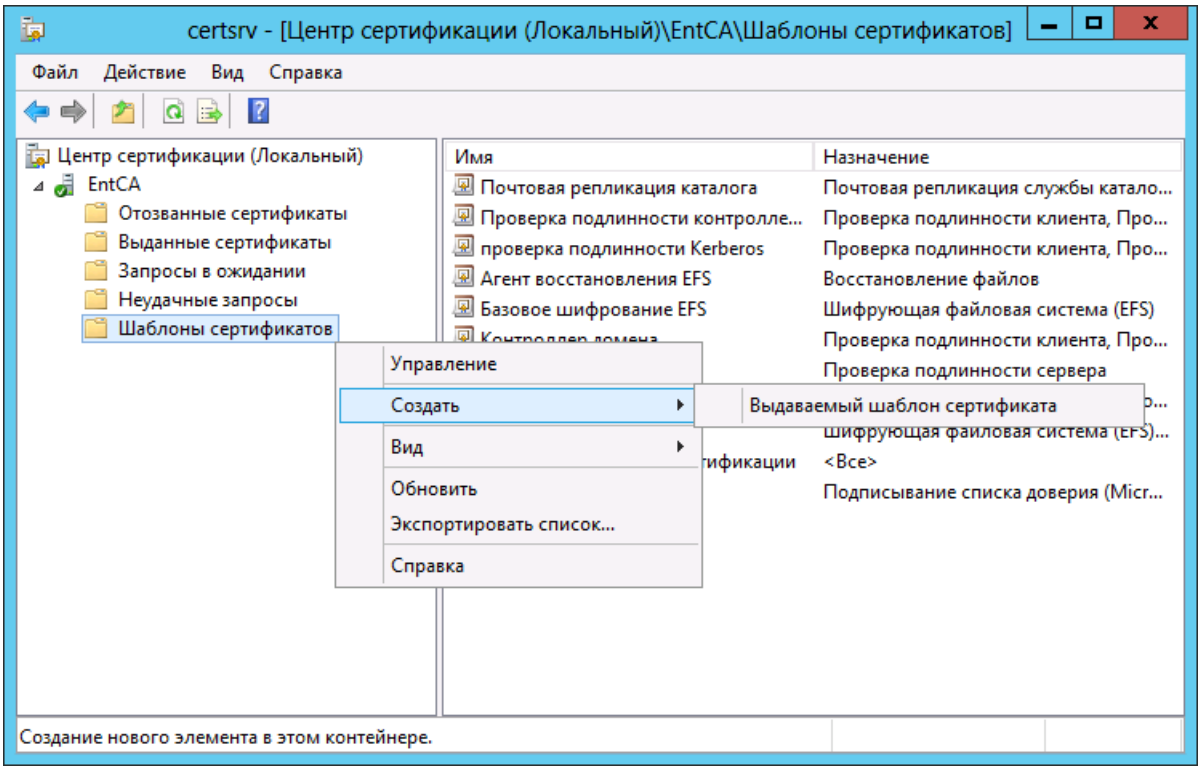

Рисунок 82

Окно списка шаблонов сертификатов

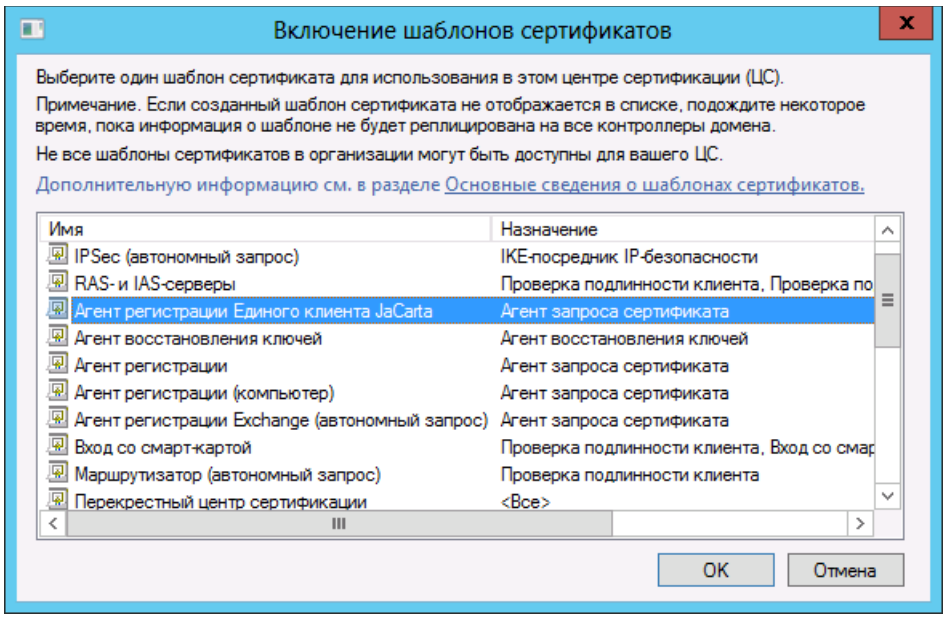

Рисунок 83

2. Отметьте настроенные шаблоны сертификатов и нажмите **OK**. Шаблоны отобразятся в списке выдаваемых шаблонов (см. рис. 84).

Окно с отображенными новыми шаблонами в списке выдаваемых шаблонов

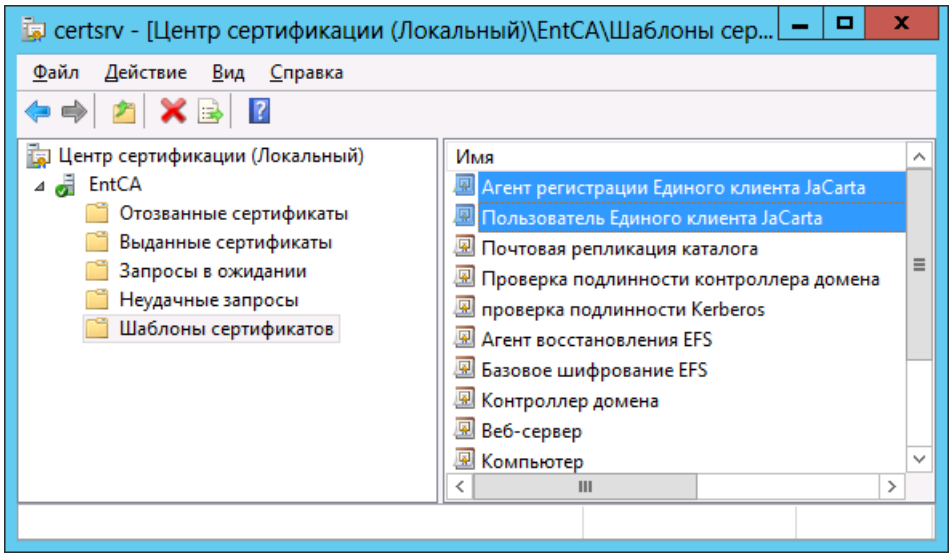

Рисунок 84

15.3. Выпуск сертификата агента регистрации

Чтобы выпустить сертификат агента регистрации, выполните следующие действия на компьютере, который будет станцией выпуска электронных ключей:

1. В окне консоли управления сертификатами пользователя нажмите правой кнопкой мыши на пункте **Личное** и выберите **Все задачи > Запросить новый сертификат** (см. рис. 85). Отобразится следующее окно (см. рис. 86).

Пользователь, от имени которого производится заявка должен иметь разрешения Чтение и Заявка для запрашиваемого сертификата.

Окно запроса сертификата агента регистрации

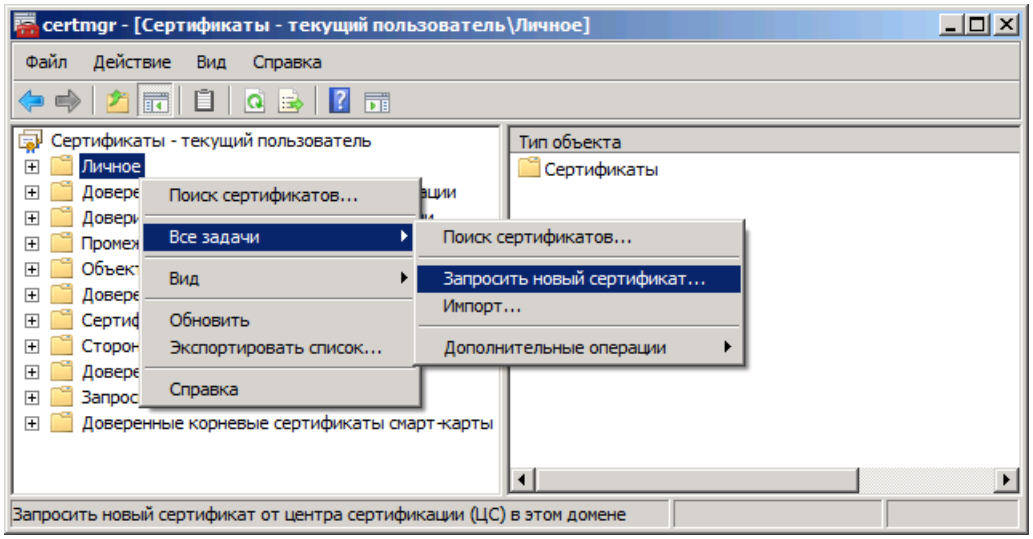

Рисунок 85

Окно мастера приветствия запроса сертификата

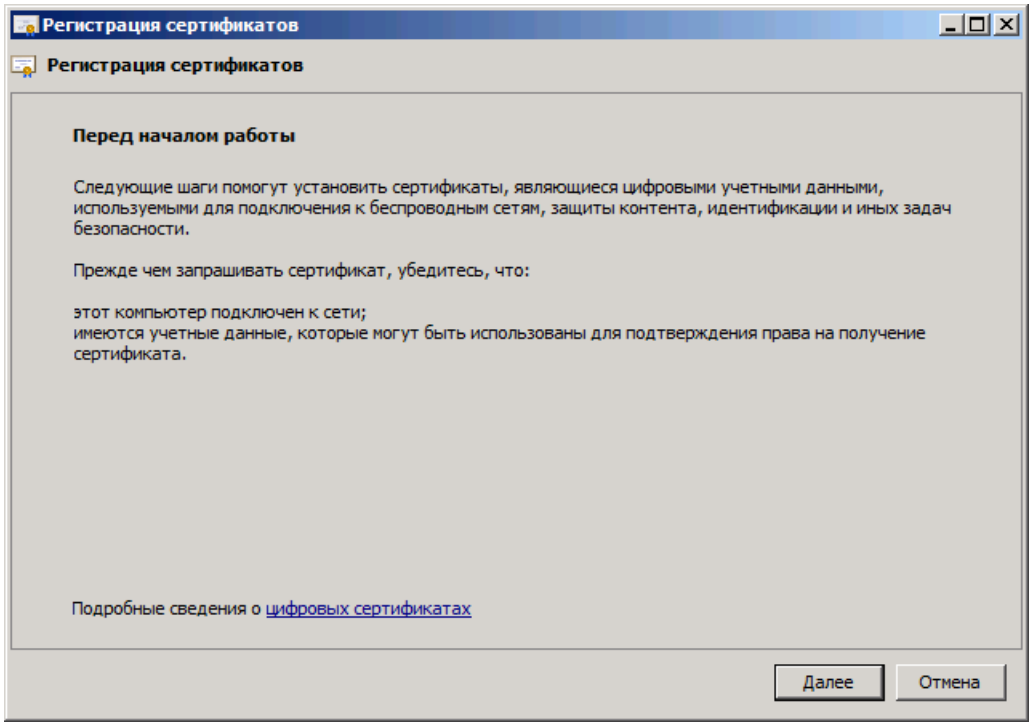

Рисунок 86

2. Нажмите **Далее**. Отобразится следующее окно (см. рис. 87).

Окно выбора политики регистрации сертификатов

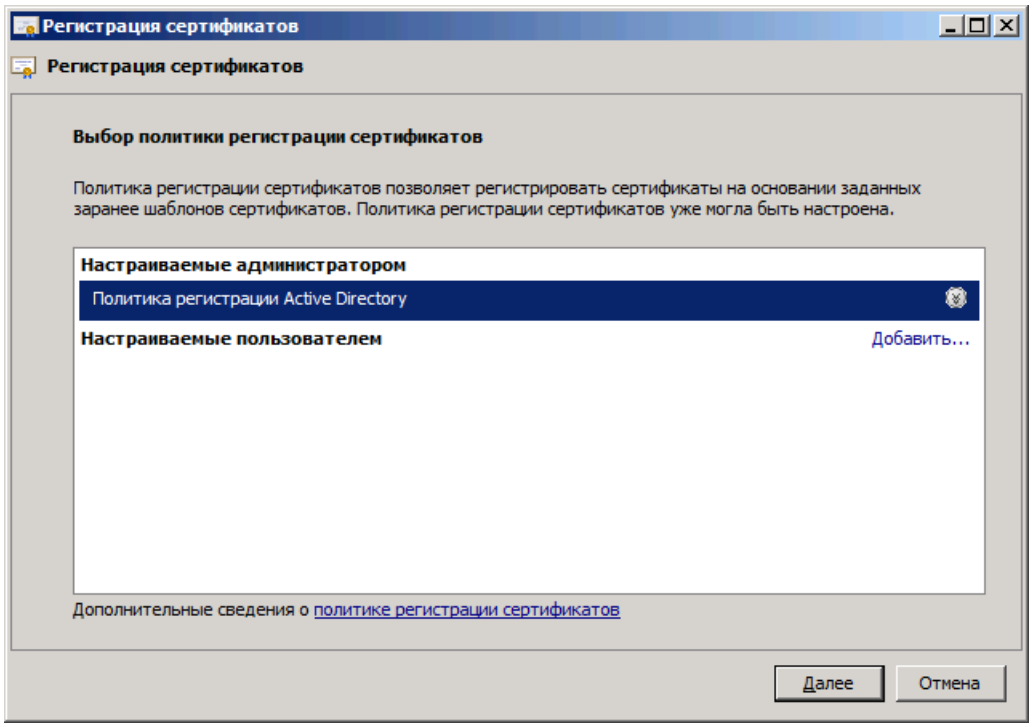

Рисунок 87

3. Нажмите **Далее**. Отобразится следующее окно (см. рис. 88).

Окно выбора шаблона сертификата

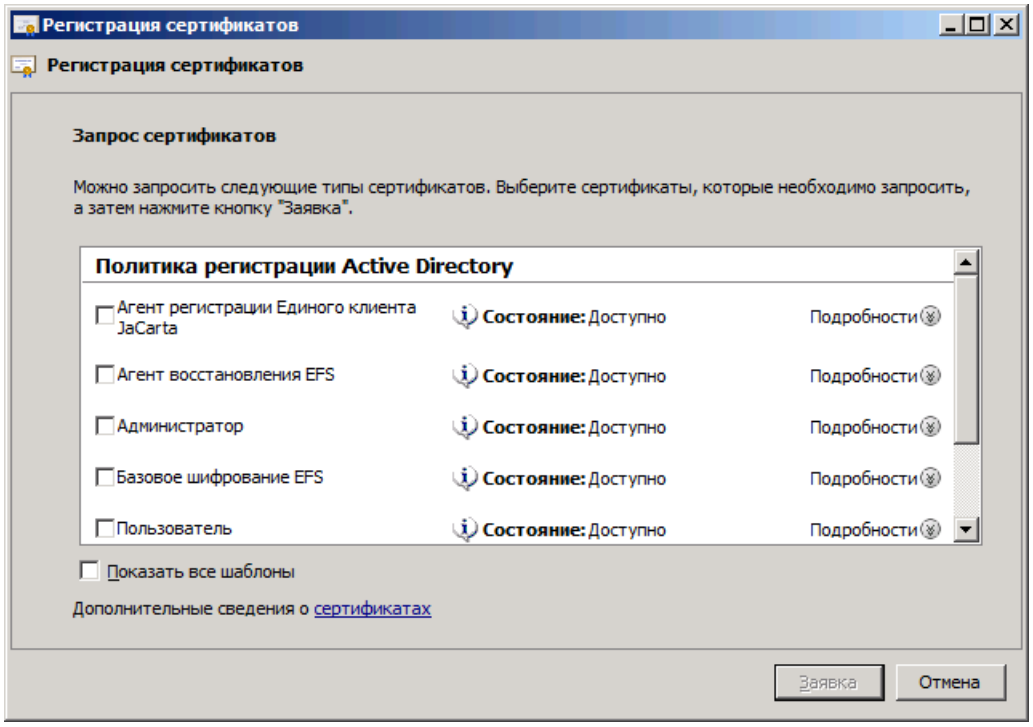

Рисунок 88

4. Отметьте шаблон, по которому будет выдан шаблон, после чего нажмите **Заявка**.
При успешном выпуске отобразится следующее окно (см. рис. 89).

Окно сообщения об успешном выпуске сертификата

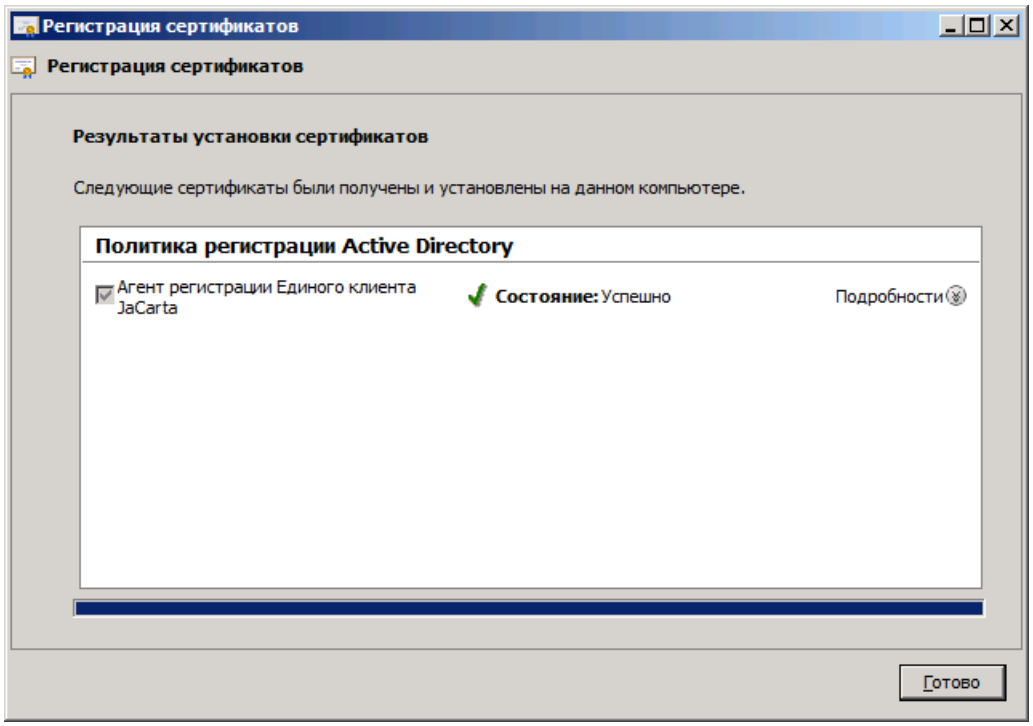

Рисунок 89

5. Нажмите **Готово**, чтобы закрыть окно.
Выпущенный сертификат отобразится в окне консоли управления сертификатами текущего пользователя (см. рис. 90).

Окно сертификата агента запроса сертификатов в личном хранилище сертификатов пользователя

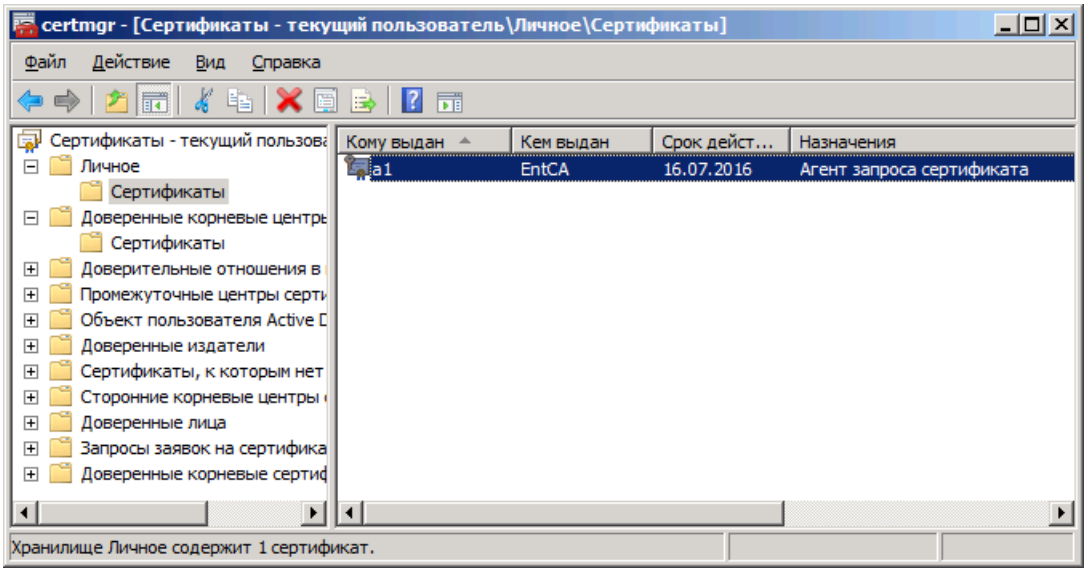

Рисунок 90

15.4. Выпуск электронного ключа с сертификатом пользователя со смарт-картой

Чтобы выпустить электронный ключ на имя пользователя, на компьютере, который является станцией выпуска электронных ключей, выполните следующие действия:

1. В консоли управления сертификатами пользователя нажмите правой кнопкой мыши на пункте **Личное** и выберите **Все задачи > Дополнительные операции > Зарегистрироваться от имени** (см. рис. 91). Отобразится следующее окно (см. рис. 92).

Окно выпуска сертификата от имени пользователя

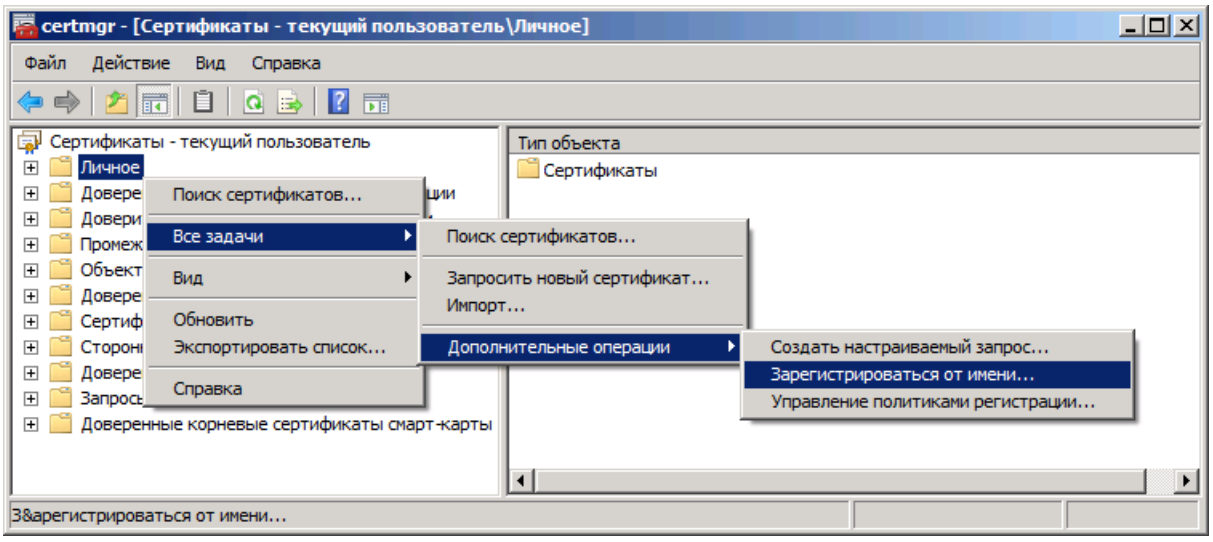

Рисунок 91

Окно приветствия мастера запроса сертификатов

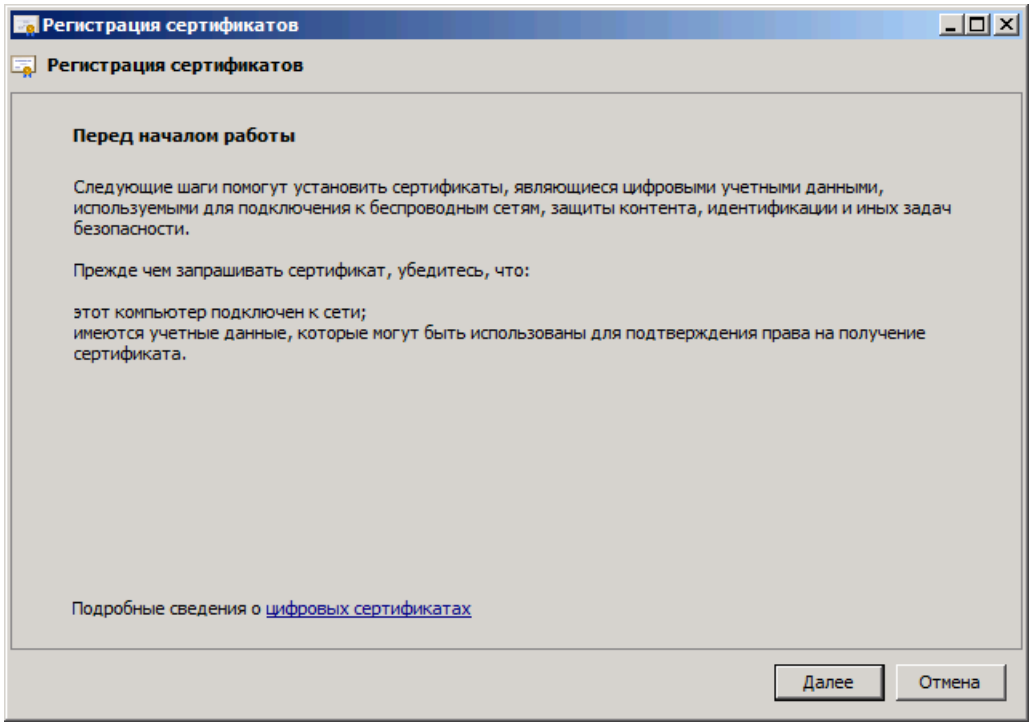

Рисунок 92

2. Нажмите **Далее**. Отобразится следующее окно (см. рис. 93).

Окно выбора политики регистрации сертификатов

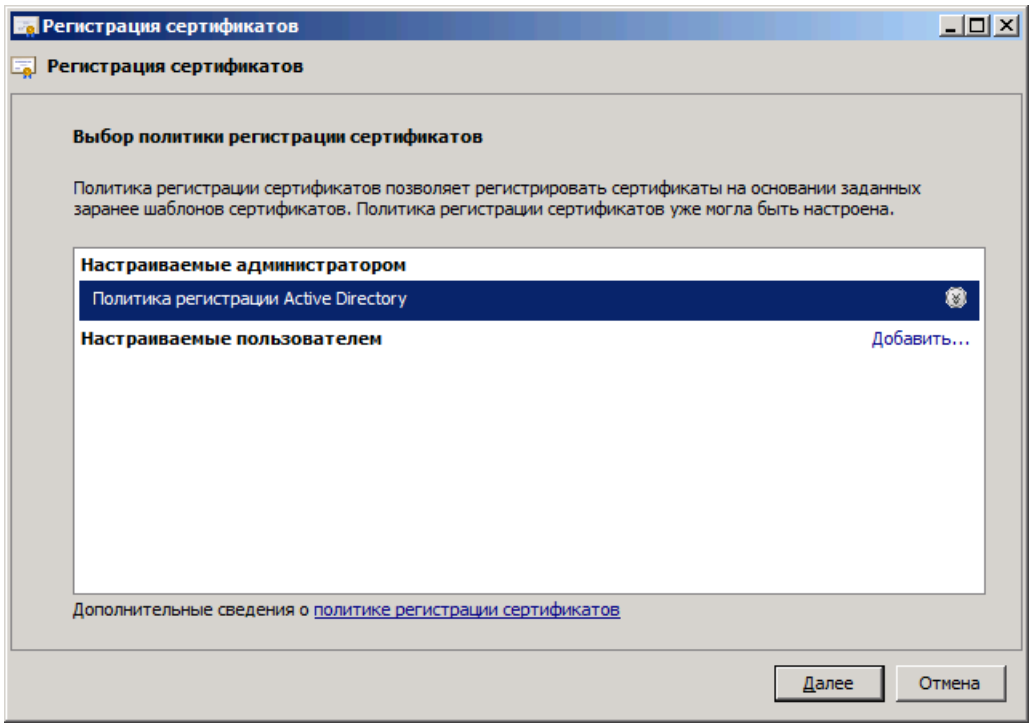

Рисунок 93

3. Нажмите **Далее**. Отобразится следующее окно (см. рис. 94).

Окно выбора сертификата агента регистрации

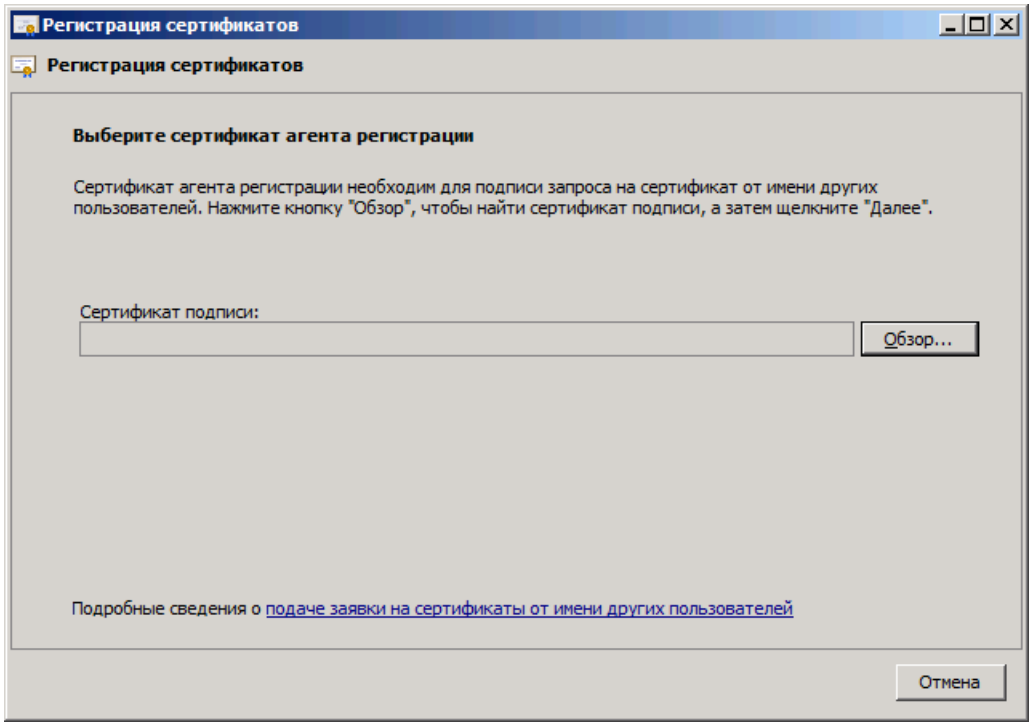

Рисунок 94

4. Воспользуйтесь кнопкой **Обзор**, чтобы выбрать сертификат агента регистрации, установленный в локальное хранилище пользователей на данном компьютере, после чего нажмите **Далее**. Отобразится следующее окно (см. рис. 95).

Окно выбора шаблона сертификата

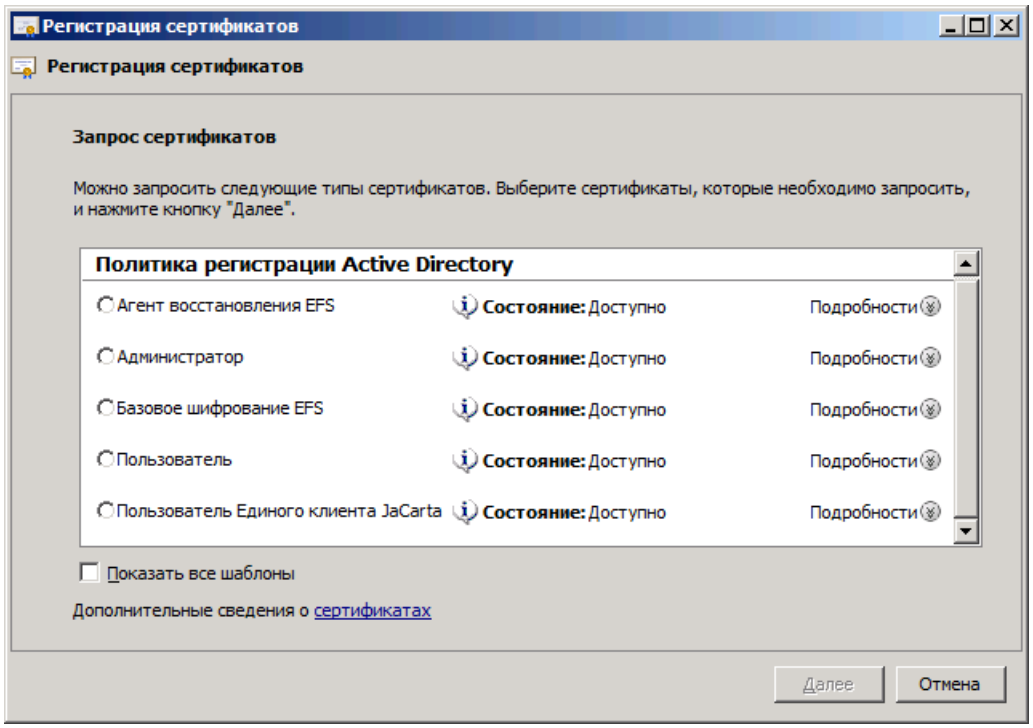

Рисунок 95

5. Отметьте подготовленный для пользователей шаблон, после чего нажмите **Далее**. Отобразится следующее окно (см. рис. 96).

Окно выбора пользователя

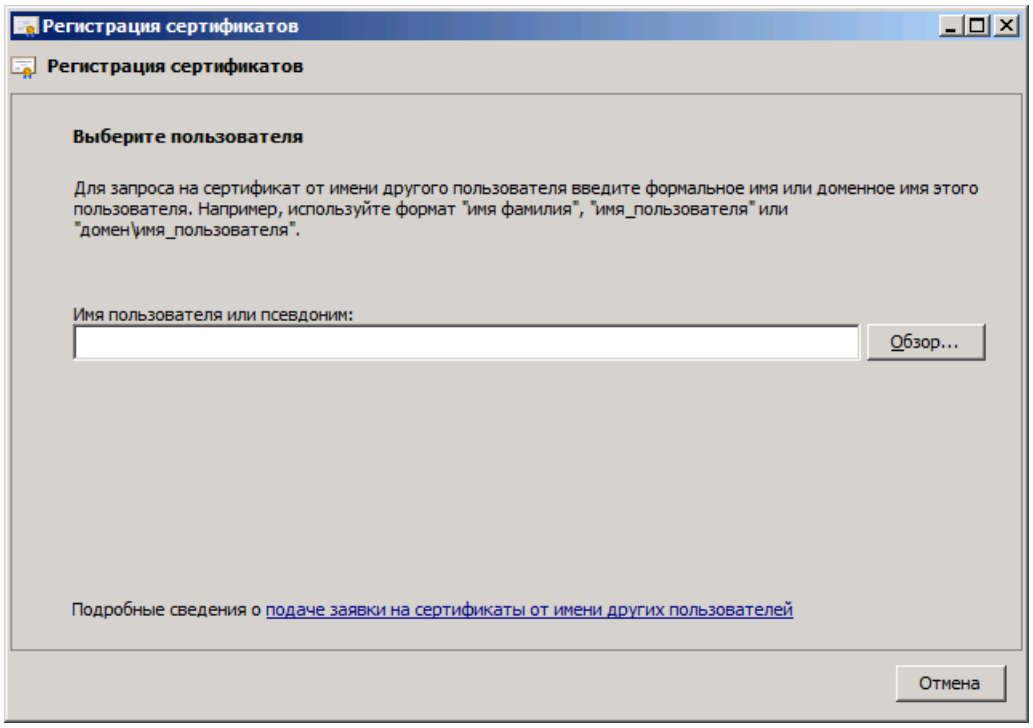

Рисунок 96

6. Воспользуйтесь кнопкой **Обзор**, чтобы выбрать пользователя, на имя которого будет выпущен сертификат и электронный ключ, после чего нажмите **Далее**. Отобразится следующее окно (см. рис. 97).

Окно ввода PIN-кода пользователя

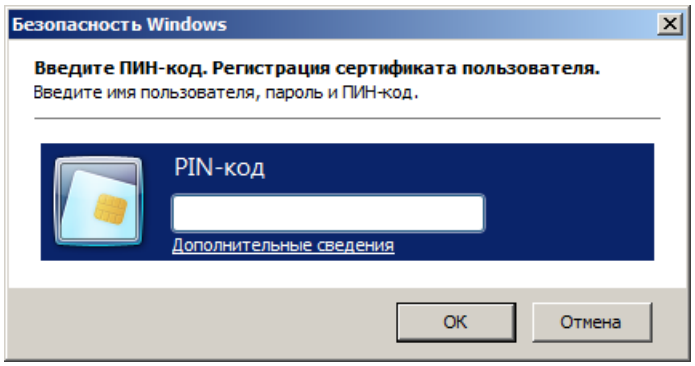

Рисунок 97

7. В поле **PIN-код** введите PIN-код пользователя электронного ключа, после чего нажмите **OK**.

При успешном выпуске отобразится следующее окно (см. рис. 98).

Окно сообщения об успешном выпуске сертификата

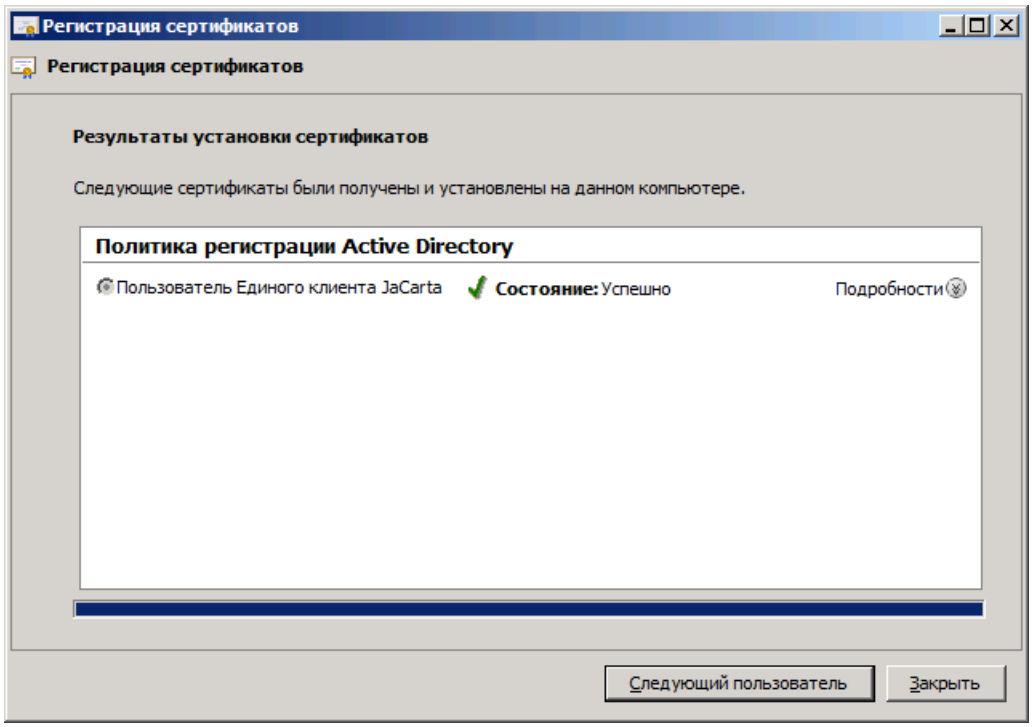

Рисунок 98

8. Нажмите **Закрыть** для завершения процедуры.

16. Мастер техподдержки

В Едином клиенте JaCarta существует возможность сбора диагностической информации об аварийных ситуациях, случившихся у пользователей с последующей отправкой собранной информации в службу технической поддержки компании Aladdin R.D.

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

Внимание! Подробнее о настройках логирования см. раздел 7. Настройка работы Единого клиента JaCarta в описании вкладки Логирование (см. рис. 29 и табл. 15).

Чтобы запустить Мастер техподдержки выполните следующие действия:

1. Нажмите Пуск –> Все программы –> Аладдин Р.Д. –> Мастер техподдержки Аладдин Р.Д. (см. рис. 99).

Запуск Мастера техподдержки

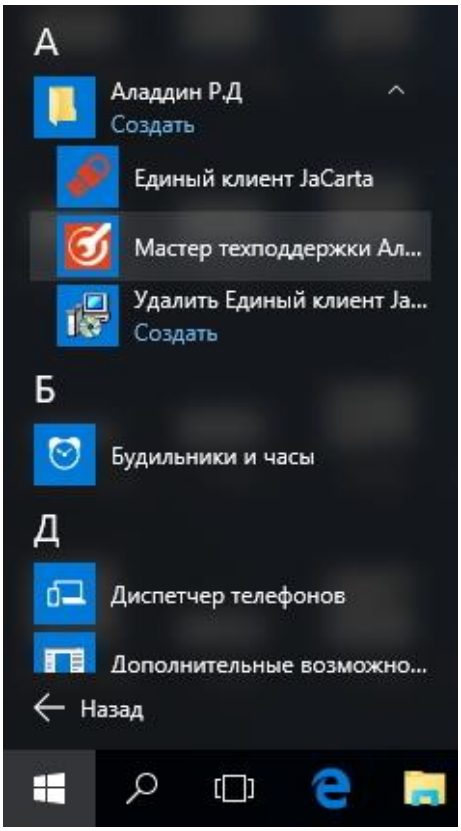

Рисунок 99

2. В появившемся окне (см. рис. 100) нажмите **Далее>**.

Приветствие Мастера техподдержки

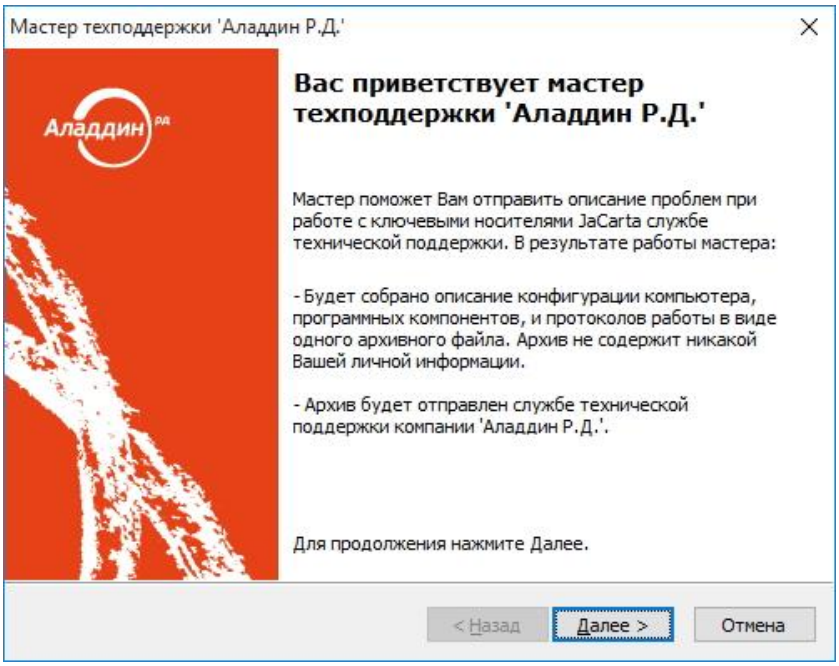

Рисунок 100

3. В появившемся окне (см. рис. 101) для выбора места сохранения файла с диагностической информацией нажмите кнопку **Изменить…** , после чего нажмите **Далее>**.

Окно выбора места расположения для сохранения файла с диагностической информацией

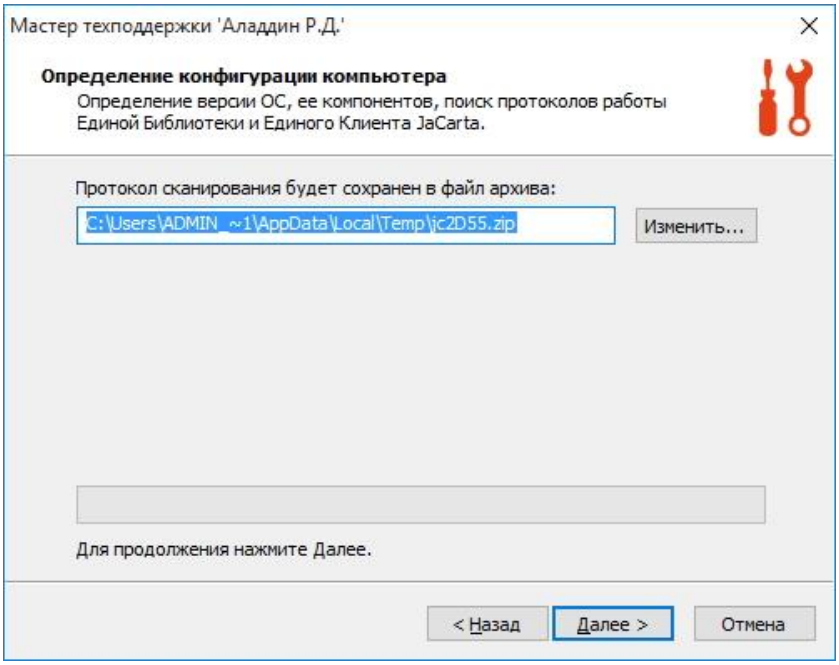

Рисунок 101

Мастер техподдерки начнет процесс сбора диагностической информации (см. рис. 102).

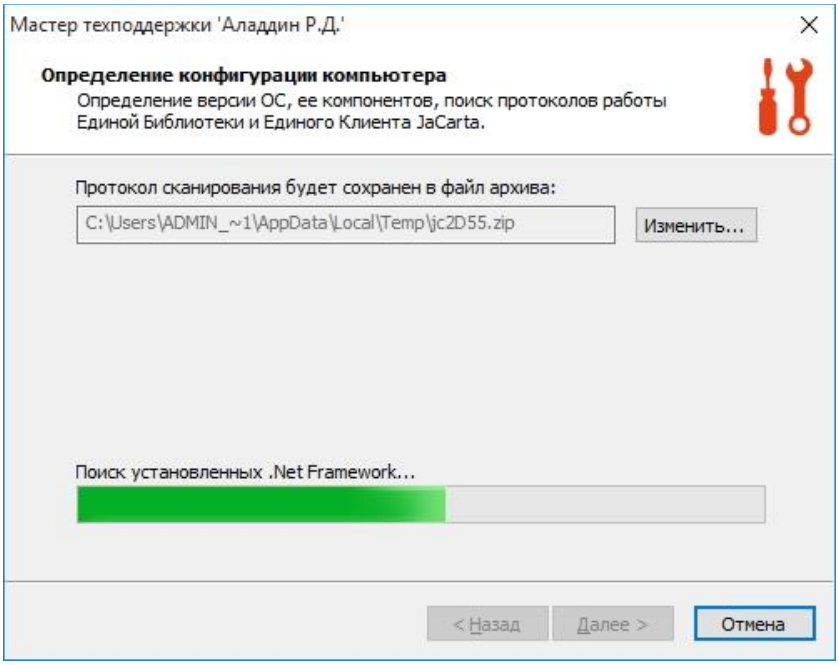

Рисунок 102

4. В появившемся окне (см. рис. 103) заполните поле **Описание проблемы**, а в поле E-mail адрес укажите свой адрес электронной почты, после чего нажмите **Далее>**.

Заполнение обязательных полей

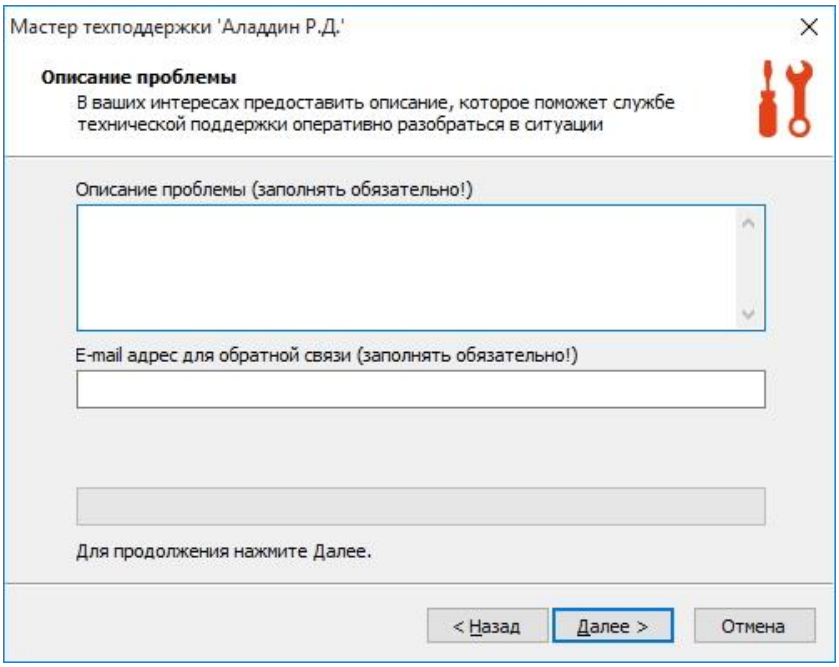

Рисунок 103

5. В появившемся окне (см. рис. 104) выберите способ отправки результатов сбора диагностической информации в службу технической поддержки компании Aladdin R.D., после чего нажмите **Далее>**.

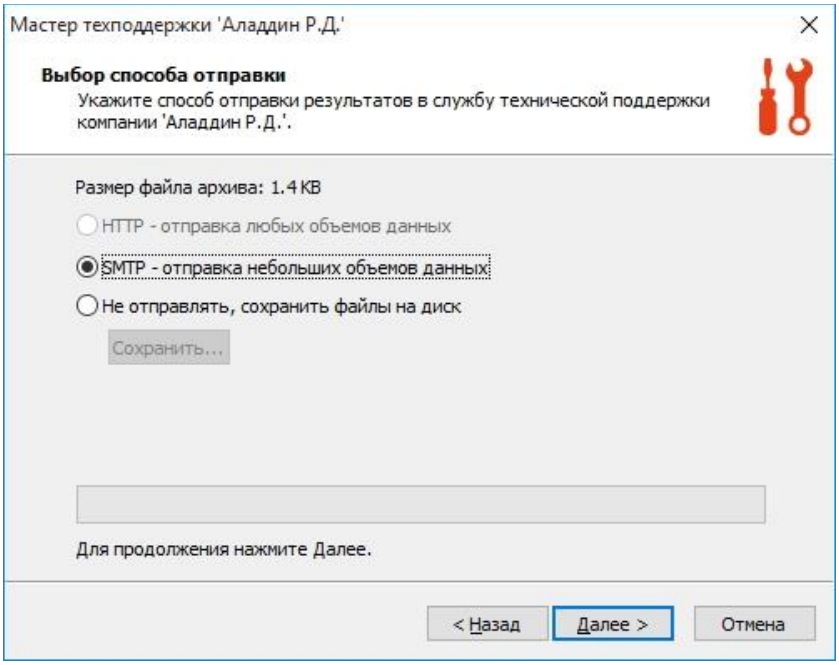

Рисунок 104

5.1. Если был выбран способ **Не отправлять, сохранить файлы на диск** (см. рис. 105), то станет доступной кнопка **Сохранить…**, после нажатия на которую отобразится следующее окно (см. рис. 106).

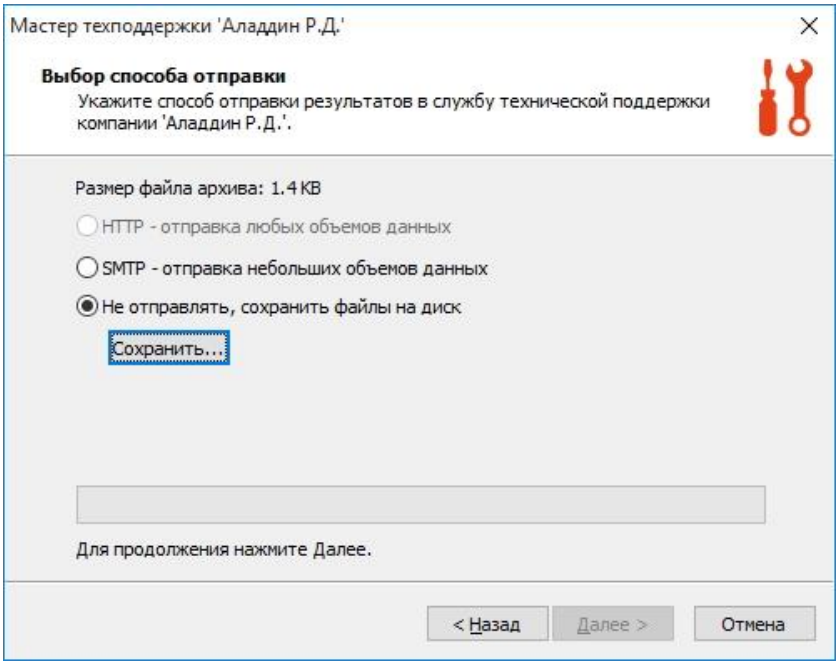

Рисунок 105

Укажите место сохранения, после чего сохраните файл с логами JaCarta, нажав кнопку **Сохранить** (см. рис. 106). Эту же процедуру выполните для сохранения файла Сопроводительного письма (см. рис. 107).

Сохранение архива с логами JaCarta

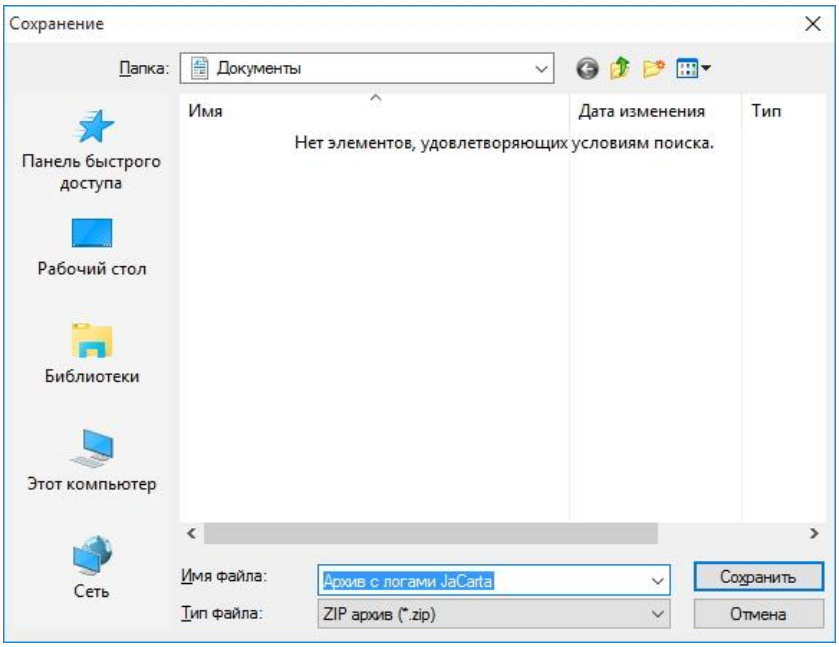

Рисунок 106

Сохранение сопроводительного письма

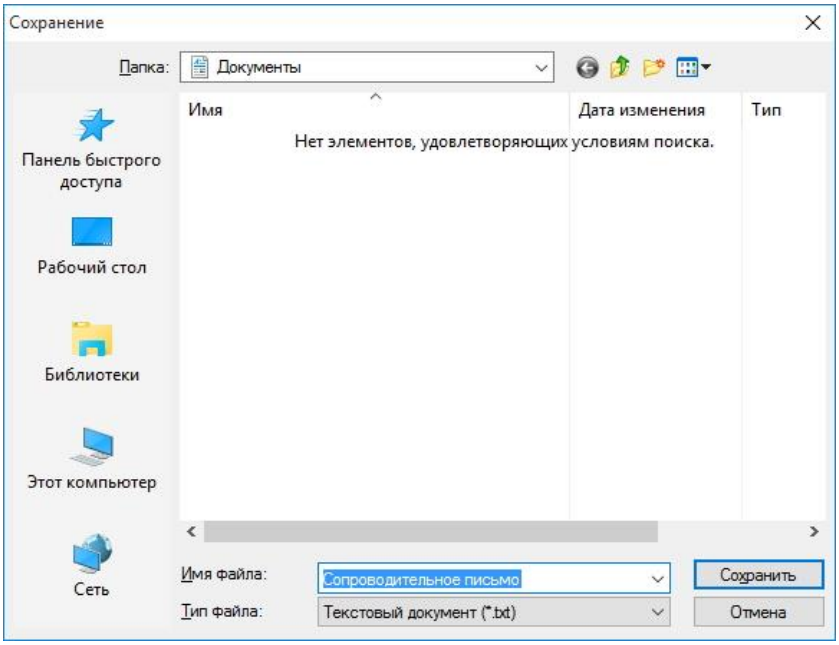

Рисунок 107

5.2. Если был выбран способ отправки: **SMTP – отправка небольших объемов данных**, то после нажатия кнопки **Далее>** отобразится следующее окно (см. рис. 108).

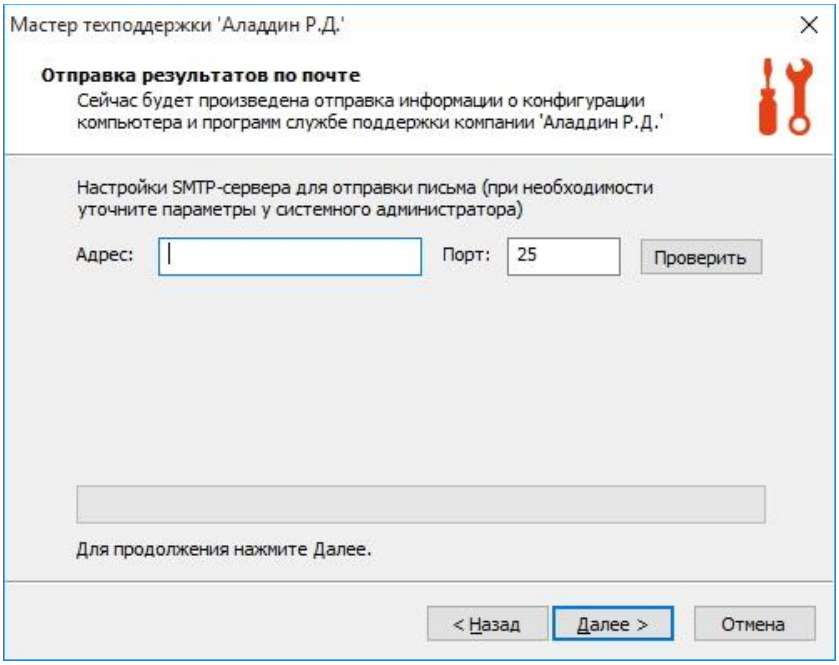

Рисунок 108

В поле **Адрес:** введите адрес SMTP-сервера для отправки письма с диагностической информацией в службу технической поддержки компании Aladdin R.D., после чего в поле **Порт:** укажите номер порта и нажмите кнопку **Проверить** для проверки возможности отправки письма по указанному адресу и порту.

После нажатия кнопки **Далее>** письмо с диагностическими данными будет отправлено указанному адресату.

Сокращения и аббревиатуры

ГОСТ	Государственный стандарт
AD CS	(Active Directory Certificate Services) службы сертификации
AD DS	(Active Directory Domain Services) доменные службы
PIN	(Personal Identification Number) личный опознавательный номер
PKI	(Public Key Infrastructure) инфраструктура открытых ключей
USB	(Universal Serial Bus) универсальная последовательная шина
VPN	(Virtual Private Network) виртуальная частная сеть

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.

Техподдержка

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

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
1.2	Обновлены разделы 1, 3, 4, 6, 7, 11, 13. Добавлен раздел 16.
1.1	*Внесены изменения в раздел 4*
1.0	*Создание документа*

Предметный указатель

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