



Единый Клиент JaCarta

Руководство администратора

Версия: 1.4

Редакция от: 29 марта 2018 г.

Листов: 102

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 Microsoft Windows и Интернет.

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

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

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

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

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

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

© 1995-2017, ЗАО "Аладдин Р.Д." Все права защищены.

Содержание

Аннотация	2
1. Общие сведения	5
1.1. Термины и определения	5
1.2. Режимы работы Единого Клиента JaCarta	5
1.3. Сведения об электронных ключах	6
2. Описание пакетов установки	11
3. Системные требования	12
4. Установка Единого Клиента JaCarta	14
4.1. Обязательные меры предосторожности	14
4.2. Установка с помощью программы мастера установки	14
4.3. Особенности установки Единый Клиент JaCarta на ОС Microsoft Windows XP с установленным антивирусом Dr.Web	20
4.4. Особенности отображения плитки Управление токеном после установки Единый Клиент JaCarta	24
4.5. Установка в режиме командной строки	26
5. Удаление Единого Клиента JaCarta	29
6. Изменение Единого Клиента JaCarta	31
7. Обзор пользовательского интерфейса	32
7.1. Меню быстрого запуска	32
7.2. Основной интерфейс	34
8. Настройка работы Единый Клиент JaCarta	40
9. Инициализация электронных ключей	44
9.1. Приложение PKI (электронные ключи eToken, JaCarta PRO и JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin)	44
9.2. Приложение PKI (электронные ключи JaCarta) и PKI/BIO	50
9.3. Приложения ГОСТ и STORAGE	58
9.4. Приложение ГОСТ с апплетом Криптотокен 2	59
10. Установка (смена) PIN-кода пользователя администратором	61
11. Смена PIN-кода подписи	63
12. Разблокировка PIN-кода пользователя (в присутствии администратора)	64
12.1. Приложения PKI и PKI/BIO	64
12.2. Приложение ГОСТ с апплетом Криптотокен и приложение STORAGE	65
12.3. Приложение ГОСТ с апплетом Криптотокен 2	67
13. Разблокировка PIN-кода пользователя (в удалённом режиме)	69
14. Смена PIN-кода администратора	74
15. Создание запроса на сертификат	76
16. Операции с объектами в памяти электронных ключей	79
16.1. Отображение списка объектов	79
16.2. Импорт объектов	81
16.3. Экспорт объектов	83
16.4. Удаление объектов	84
16.5. Отображение информации об объекте	84

16.6. Повторная инициализация датчика случайных чисел (приложение ГОСТ)	85
16.7. Диагностика электронного ключа (приложение ГОСТ)	86
17. Операции, производимые с помощью утилиты JaCarta APM УЦ	87
18. Синхронизация паролей электронного ключа и учетной записи домена Windows	88
19. Мастер техподдержки	92
Сокращения и аббревиатуры	100
Контакты, техническая поддержка	101
Регистрация изменений	102
Предметный указатель	103

1. Общие сведения

Единый Клиент JaCarta представляет собой программное обеспечение, обеспечивающее работу с электронными ключами JaCarta/eToken в операционных системах семейства Microsoft 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 от имени пользователя
Администратор	Сотрудник, отвечающий за подготовку к работе и техническое обслуживание электронного ключа
PIN-код администратора	PIN-код, предоставляющий доступ к операциям от имени администратора
PUK-код	PUK-код, позволяющий разблокировать PIN-код пользователя после его блокировки
Инициализация	Установка основных параметров работы электронного ключа (подготовка к работе)
Приложение	<p>Программное обеспечение, установленное в память электронного ключа. Существуют следующие приложения:</p> <ul style="list-style-type: none">•PKI;•PKI/BIO;•ГОСТ;•STORAGE;•ФКН. <p>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.</p>

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 (Java) eToken Anywhere eToken NG-FLASH (Java) eToken NG-OTP (Java) JaCarta PRO JaCarta PKI с функцией обратной совместимости JaCarta-2 PRO/ГОСТ	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO JaCarta-2 PKI/ГОСТ JaCarta-2 PKI/BIO/ГОСТ	JaCarta ГОСТ/Flash JaCarta ГОСТ eToken ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ JaCarta-2 PRO/ГОСТ JaCarta-2 PKI/BIO/ГОСТ	JaCarta LT	JaCarta CryptoPro	JaCarta WebPass JaCarta U2F/Web Pass
Приложение	PKI	PKI и PKI/BIO	ГОСТ	ГОСТ	STORAGE	ФКН	OTP, STORAGE
PIN-код пользователя по умолчанию	1234567890	11111111	Не установлен	1234567890	1234567890	Нет	Нет
PUK-код для разблокирования	Нет			Да	Нет		
PIN-код администратора по умолчанию	1234567890	00000000	1234567890	Нет ¹	1234567890	Нет	Нет
Можно инициализировать без назначения PIN-кода пользователя (администратор может назначить PIN-код пользователя после инициализации)	Да	Да	Да	Да	Нет	Нет	Да
Можно инициализировать без назначения PIN-кода администратора	Да	Нет	Нет	Нет	Только при первичной инициализации	Нет	Да
Поведение ключа при разблокировке PIN-кода пользователя ²	Во время разблокировки администратор задаёт новый PIN-код пользователя		Разблокировка сбрасывает счётчик неверных попыток доступа – PIN-код пользователя при этом остаётся неизменным			Нет	Нет
Можно разблокировать PIN-код пользователя в удалённом режиме	Да	Да	Нет	Да	Нет	Нет	Нет
Администратор может сменить установленный PIN-код пользователя без инициализации	Да	Да	Нет	Нет	Нет	Нет	Нет

¹Административные операции с JaCarta-2 ГОСТ выполняются с помощью АРМа администратора безопасности JaCarta-2 ГОСТ (СКЗИ "Криптотокен 2 ЭП", исполнение 13).

² В случае с электронными ключами JaCarta PKI/BIO при разблокировке биометрического доступа пользователь вновь получает возможность аутентифицироваться по ранее сохранённому отпечатку пальца.

Таблица 2

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

Операция	Приложение	Режим работы Единого Клиента JaCarta	Аутентификация
Инициализация	PKI на следующих электронных ключах: <ul style="list-style-type: none"> •eToken PRO (Java) •eToken Anywhere •eToken NG-FLASH (Java) •eToken NG-OTP (Java) •JaCarta PRO •JaCarta PRO/ГОСТ •JaCarta-2 PRO/ГОСТ •JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin •JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin 	Режим администратора	Не требуется
	PKI на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta PKI •JaCarta PKI/Flash •JaCarta PKI/ГОСТ •JaCarta-2 PKI/ГОСТ •JaCarta-2 PKI/БИО/ГОСТ 	Режим администратора	PIN-код администратора
	PKI/БИО		
	ГОСТ на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta PRO/ГОСТ •JaCarta ГОСТ/Flash •JaCarta ГОСТ •JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin •eToken ГОСТ 		
	STORAGE	Режим администратора (инициализация возможна только от имени пользователя)	PIN-код пользователя
	ГОСТ на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta-2 PKI/ГОСТ •JaCarta-2 ГОСТ •JaCarta-2 PRO/ГОСТ •JaCarta-2 PKI/БИО/ГОСТ 		
	ФКН	Недоступно	

Операция	Приложение	Режим работы Единого Клиента JaCarta	Аутентификация
Установка (смена) PIN-кода пользователя администратором	PKI на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta PKI •JaCarta PKI/Flash •JaCarta PKI/ГОСТ •JaCarta-2 PKI/ГОСТ •JaCarta-2 PKI/БИО/ГОСТ 	Режим администратора	PIN-код администратора
	PKI/БИО		
	PKI на следующих электронных ключах: <ul style="list-style-type: none"> •eToken PRO (Java) •eToken Anywhere •eToken NG-FLASH (Java) •eToken NG-OTP (Java) •JaCarta PRO •JaCarta PRO/ГОСТ •JaCarta-2 PRO/ГОСТ •JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin •JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin 	Недоступно, если PIN-код уже установлен	
	ГОСТ		
	STORAGE	Недоступно	
	ФКН		
Смена своего PIN-кода пользователем	PKI	Режим пользователя	PIN-код пользователя
	PKI/БИО		
	ГОСТ		
	STORAGE		
	ФКН	Недоступно	
Смена своего PIN-кода администратором	PKI	Режим администратора	PIN-код администратора
	PKI/БИО		
	ГОСТ на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta PRO/ГОСТ •JaCarta ГОСТ/Flash •JaCarta ГОСТ •JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin 		
	eToken ГОСТ		
	STORAGE		
	ГОСТ на следующих электронных ключах: <ul style="list-style-type: none"> •JaCarta-2 PKI/ГОСТ •JaCarta-2 ГОСТ •JaCarta-2 PRO/ГОСТ 	Недоступно	

Операция	Приложение	Режим работы Единого Клиента JaCarta	Аутентификация
	●JaCarta-2 PKI/БИО/ГОСТ		
	ФКН	Недоступно	
Установка (смена) своего PIN-кода подписи пользователем	PKI	Недоступно	
	PKI/БИО		
	ГОСТ на следующих электронных ключах: ●JaCarta-2 PKI/ГОСТ ●JaCarta-2 ГОСТ ●JaCarta-2 PRO/ГОСТ ●JaCarta-2 PKI/БИО/ГОСТ	Режим пользователя	PIN-код пользователя
	ГОСТ на следующих электронных ключах: ●JaCarta PRO/ГОСТ ●JaCarta ГОСТ/Flash ●JaCarta ГОСТ ●JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin ●eToken ГОСТ	Недоступно	
	STORAGE		
	ФКН		
Смена отпечатков пальцев	PKI	Недоступно	
	PKI/БИО	Режим администратора	PIN-код администратора
	ГОСТ		
	STORAGE	Недоступно	
	ФКН		
Разблокировка PIN-кода пользователя	PKI	Режим администратора/Режим пользователя	Возможно 2 варианта: ●с помощью PIN-код администратора; ●с помощью механизма запрос-ответ.
	PKI/БИО	Режим администратора/Режим пользователя	
	ГОСТ на следующих электронных ключах: ●JaCarta PRO/ГОСТ ●JaCarta ГОСТ/Flash ●JaCarta ГОСТ ●JaCarta PKI/ГОСТ с функцией обратной совместимости с продуктами компании Aladdin ●eToken ГОСТ	Режим администратора	
	STORAGE		
	ГОСТ на следующих электронных ключах: ●JaCarta-2 PKI/ГОСТ ●JaCarta-2 ГОСТ ●JaCarta-2 PRO/ГОСТ JaCarta-2 PKI/БИО/ГОСТ	Режим администратора/Режим пользователя	Возможно 3 варианта: ●с помощью PUK-кода; ●по заданному в настройках токена счетчику времени; ●с помощью механизма запрос-ответ.

Операция	Приложение	Режим работы Единого Клиента JaCarta	Аутентификация
	ФКН	Недоступно	
Операции с объектами в памяти электронных ключей ³	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

³ В случае с электронными ключами ФКН поддерживаются операции только с контейнерами CryptoPro

2. Описание пакетов установки

Дистрибутив Единый Клиент 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	Microsoft Windows XP SP3 (32-бит) Microsoft Windows XP SP2 (64-бит) Microsoft Windows Vista SP2 (32/64-бит) Microsoft Windows 7 SP1 (32/64-бит) Microsoft Windows 8 (32/64-бит) Microsoft Windows 8.1 Update 1 (32/64-бит) Microsoft Windows 10 (32/64-бит) Microsoft Windows Server 2003 SP2 (32/64-бит) Microsoft Windows Server 2008 SP2 (32/64-бит) Microsoft Windows Server 2008 R2 SP1 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016
Поддерживаемые модели электронных ключей	Электронные ключи eToken: <ul style="list-style-type: none"> •eToken PRO (Java) •eToken Anywhere •eToken NG-FLASH (Java) •eToken NG-OTP (Java) •eToken ГОСТ •eToken CryptoPro Электронные ключи JaCarta: <ul style="list-style-type: none"> •JaCarta PKI •JaCarta PKI/Flash •JaCarta PKI/BIO •JaCarta PKI/BIO/ГОСТ •JaCarta PKI/ГОСТ •JaCarta-2 PKI/ГОСТ •JaCarta-2 PKI/BIO/ГОСТ •JaCarta PKI/ГОСТ/Flash •JaCarta PRO •JaCarta PRO/ГОСТ •JaCarta-2 PRO/ГОСТ •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-2 ГОСТ •JaCarta CryptoPro •JaCarta LT •JaCarta WebPass •JaCarta U2F/WebPass •JaCarta U2F
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:

Требование	Содержание
	<ul style="list-style-type: none"> •разъём microSD; •разъём SD через переходник microSD-to-SD; •USB-порт через переходник microSD-to-USB. <p>Для электронных ключей в форм-факторе microUSB можно использовать следующее оборудование:</p> <ul style="list-style-type: none"> •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 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	<p>Если на компьютере установлено одно из перечисленных ниже программных обеспечений, его необходимо удалить до установки Единого Клиента JaCarta:</p> <p>CCID Fix; Модуль поддержки для Signal-COM CSP (eToken for Signal-COM CSP); JC-PROClient; Модуль поддержки JaCarta BIO для CryptoPro CSP (CryptoPRO BIO); Athena Micro SD Driver; Модуль поддержки для CPRO JSP (JaCarta for CryptoPro JCP); •USB eToken Driver.</p>

Таблица 5

4. Установка Единого Клиента JaCarta

4.1. Обязательные меры предосторожности



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



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.



Внимание! Перед удалением или обновлением Единого Клиента JaCarta обязательно убедитесь в том, что на вашем компьютере настроена хотя бы одна учетная запись, которая позволяет входить с административными полномочиями при помощи логина и пароля, то есть без использования токенов и смарт-карт.



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

4.1.1. Особенности работы с JaCarta microSD

При работе с JaCarta microSD на планшетах, оснащенных ОС Microsoft Windows 8.x, могут возникнуть проблемы при переходе в энергосберегающий режим и обратно. Рекомендуется использовать JaCarta microUSB-токен вместо JaCarta microSD на планшетах с ОС Microsoft Windows 8.x и выше.

4.1.2. Особенности установки и работы совместно с JMS

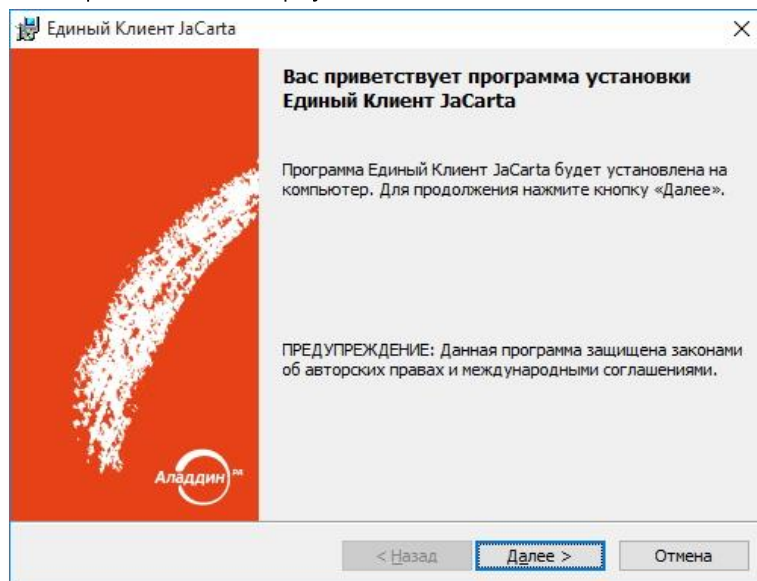
- Единый Клиент JaCarta 2.11 совместим с JMS 3.1.
- Единый Клиент JaCarta 2.9 совместим с JMS 2.2 и 2.3.
- Единый Клиент JaCarta 2.8 рекомендуется использовать с более ранними версиями JMS.
- Единый Клиент JaCarta 2.7 не рекомендуется использовать совместно с JMS.

4.2. Установка с помощью программы мастера установки

Чтобы установить Единый Клиент JaCarta выполните следующие действия:

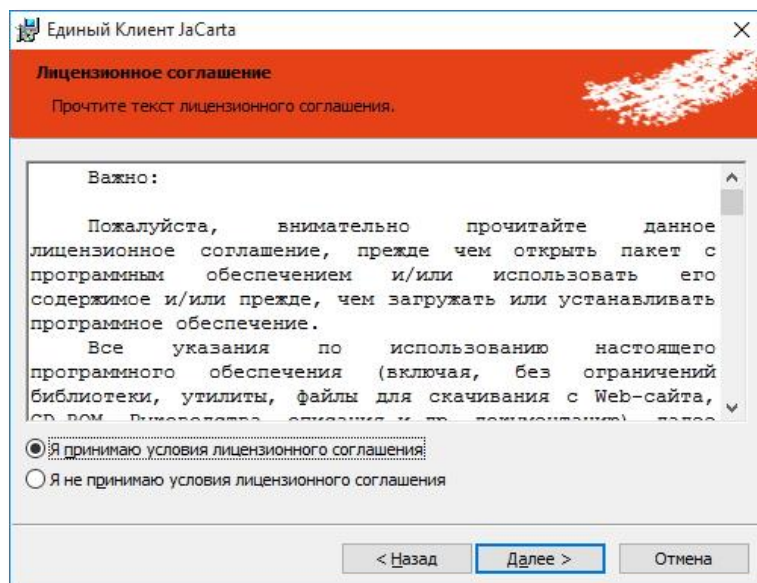
1. В зависимости от разрядности операционной системы запустите нужный файл установки (см. раздел "2. Описание пакетов установки"). Отобразится окно установки Единый Клиент Ja Carta (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 1 - Окно приветствия мастера установки Единого Клиента JaCarta



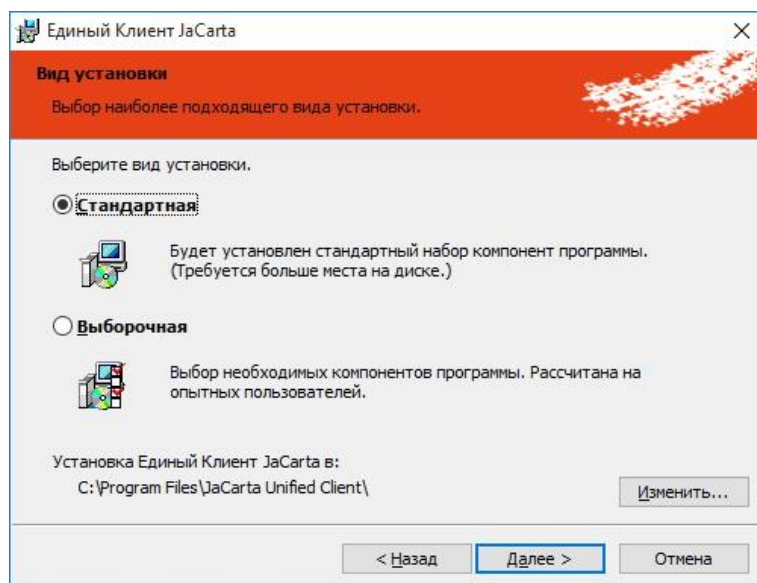
2. Нажмите **Далее >**. Будет осуществлен переход к окну **Лицензионное соглашение** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 2 - Окно Лицензионного соглашения



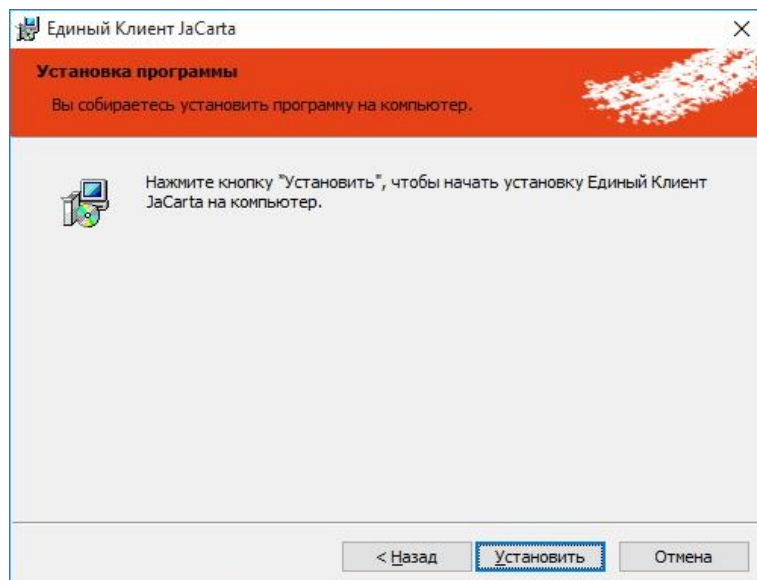
3. Ознакомьтесь с Лицензионным соглашением
 - 3.1. Если вы согласны с условиями Лицензионного соглашения, выберите пункт **Я принимаю условия Лицензионного соглашения** и нажмите **Далее >**. Отобразится окно **Вид установки** (см. Рис. **Ошибка! Источник ссылки не найден.**).
 - 3.2. Если вы не согласны с условиями Лицензионного соглашения, прекратите установку, нажав **Отмена**.

Рисунок 3 - Окно выбора пути и вида установки Единого Клиента JaCarta



4. Выберите вид установки: **Стандартная** или **Выборочная**.
5. При необходимости воспользуйтесь кнопкой **Изменить...**, чтобы изменить путь установки Единого Клиента JaCarta.
6. Нажмите **Далее >**. Если был выбран вид установки **Стандартная**, отобразится окно **Установка программы** (см. Рис. **Ошибка! Источник ссылки не найден.**). Если был выбран вид установки **Выборочная**, отобразится окно (см. Рис. **Ошибка! Источник ссылки не найден.** и Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 4 - Установка стандартного набора компонент Единого Клиента JaCarta



При **Стандартной** установке будут установлены следующие компоненты:

- Единый Клиент JaCarta;
- Управление токеном;
- Поддержка биометрии;
- Серверные компоненты RDP для биометрии;
- Установка Athena CSP в качестве криптопровайдера по умолчанию.

При **Выборочной** установке возможен выбор из следующего набора компонентов:

- JaCarta SecurLogon;
- JaCarta WebPass Tool;

- JaCarta APM УЦ;
- Управление токеном;
- Поддержка биометрии;
- Серверные компоненты RDP для биометрии;
- Установка Athena CSP в качестве криптопровайдера по умолчанию;
- Драйверы:
 - Поддержка работы устаревших моделей JaCarta в продуктах VMware;
 - Поддержка JaCarta PKI с обратной совместимостью;
 - Поддержка JaCarta Secure MicroSD;
 - Поддержка eToken PRO 32K/64K (USB eToken Driver).



Примечание – Компонент Единый Клиент JaCarta является обязательным и устанавливается всегда (независимо от выбранного типа установки).

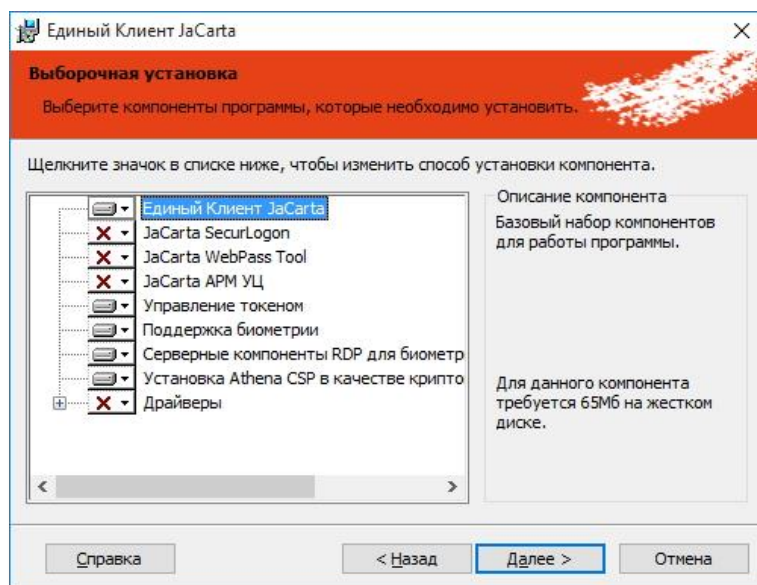
Описание компонентов см. в Таблице 6.

Таблица 6

Название компонента	Описание
JaCarta SecurLogon	Для обеспечения двухфакторной аутентификации с использованием электронных ключей JaCarta и eToken в ОС Microsoft Windows
JaCarta WebPass Tool	Для возможности администрирования токенов JaCarta WebPass
JaCarta APM УЦ	Позволяет генерировать ключевые пары с использованием встроенных криптографических возможностей электронных ключей JaCarta ГОСТ и eToken ГОСТ, а также формировать запросы к удостоверяющему центру на получение сертификата открытого ключа и записывать полученные сертификаты в память электронного ключа
Управление токеном	Для возможности выполнять операции с токеном до входа пользователя в систему
Поддержка биометрии	Добавляет возможность использования биометрических считывателей и электронных ключей JaCarta BIO
Серверные компоненты RDP для биометрии	Позволяет подключаться к данному компьютеру через удаленный рабочий стол с использованием электронных ключей JaCarta PKI/BIO и биометрических данных
Установка Athena CSP в качестве криптопровайдера по умолчанию	Для использования Athena CSP криптопровайдером по умолчанию. В противном случае (в случае отмены установки этого компонента) криптопровайдером по умолчанию будет Microsoft Base Smart Card CSP.
Драйверы – Поддержка работы устаревших моделей JaCarta в продуктах VMware	Для возможности использования токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware
Драйверы – Поддержка JaCarta PKI с обратной совместимостью	Для возможности использования токенов JaCarta PKI с обратной совместимостью
Драйверы – Поддержка JaCarta Secure MicroSD	Для возможности использования токенов JaCarta в форм-факторе Secure MicroSD
Драйверы – Поддержка eToken PRO 32K/64K (USB eToken Driver)	Для возможности использования устаревших моделей eToken PRO 32K/64K

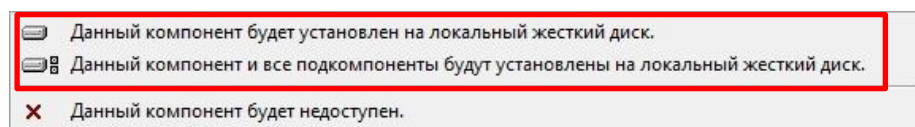
Таблица 6

Рисунок 5 - Выборочная установка компонент Единого Клиента JaCarta



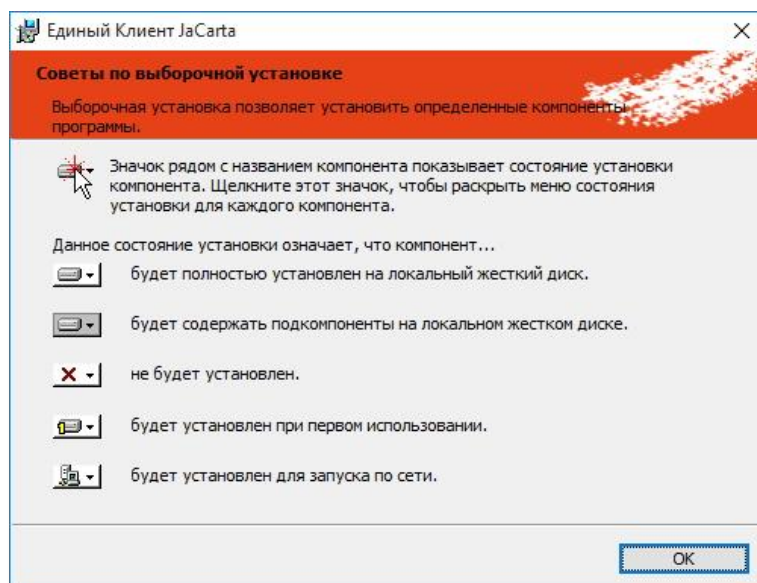
7. Для установки требуемого компонента в окне **Выборочная установка** в строке с названием требуемого компонента нажмите на значок и в выпадающем списке (см. Рис. **Ошибка! Источник ссылки не найден.**) выберите необходимую опцию установки.

Рисунок 6 - Опции установки



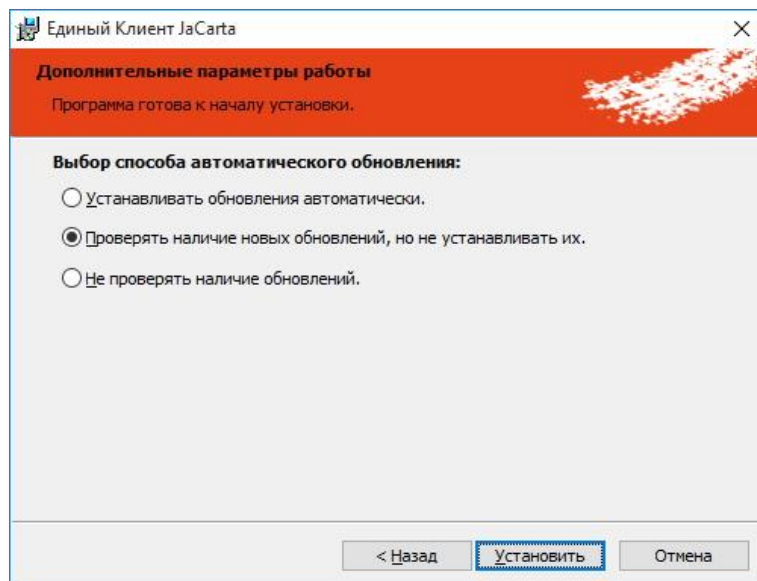
При нажатии на кнопку **Справка** будет открыто окно **Советы по выборочной установке**, содержащее подробное описание состояний установки компонентов (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 7 - Советы по выборочной установке



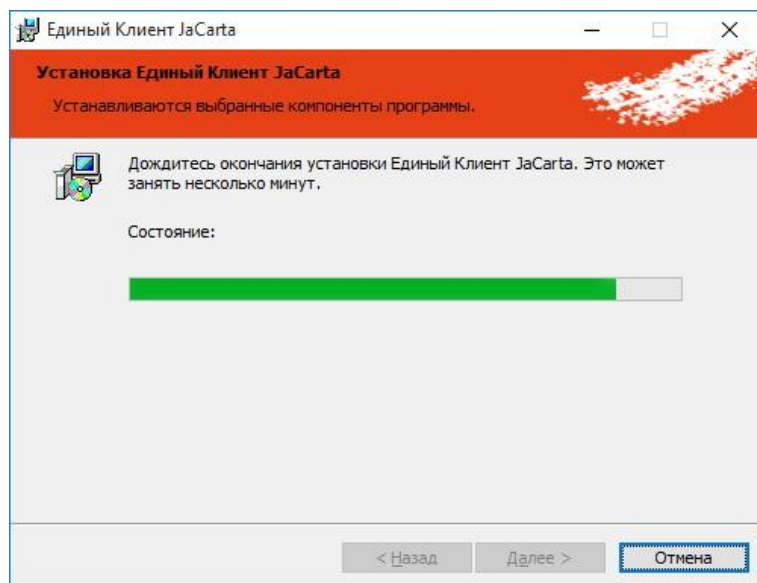
После выбора требуемых компонентов нажмите **Далее**. Отобразится окно **Дополнительные параметры работы** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 8 - Выбор способа автоматического обновления



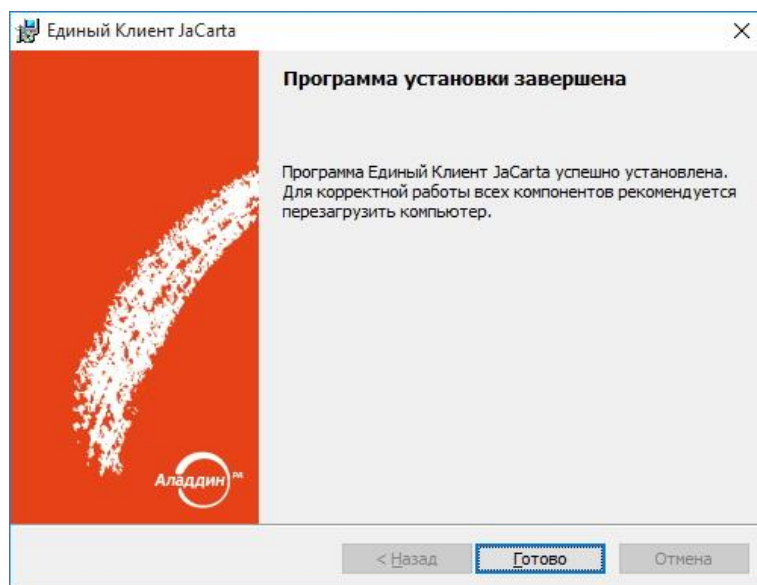
8. Нажмите **Установить** и дождитесь окончания установки (см. Рисунок 9).

Рисунок 9 - Установка Единый Клиент JaCarta



9. После завершения установки отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 10 - Окно завершения установки Единого Клиента JaCarta



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

**Внимание!**

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

4.3. Особенности установки Единый Клиент JaCarta на ОС Microsoft Windows XP с установленным антивирусом Dr.Web

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



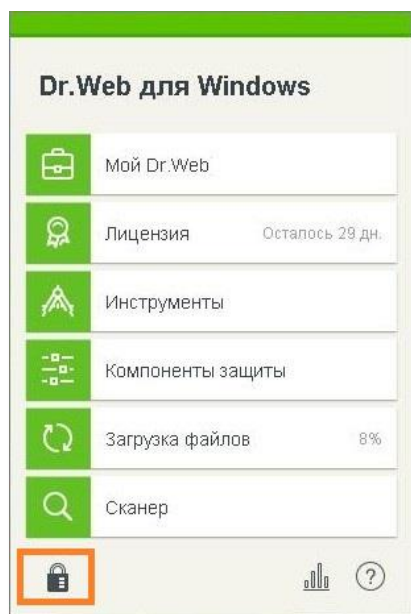
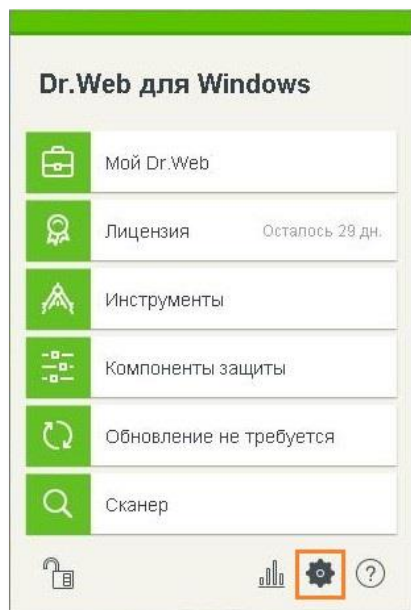
1. Запустить **SpIDer Agent**, нажав значок  на панели задач в области уведомлений.
2. Разблокировать **SpIDer Agent**. Для внесения изменений нажать кнопку  (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 11 - Разблокирование элементов управления



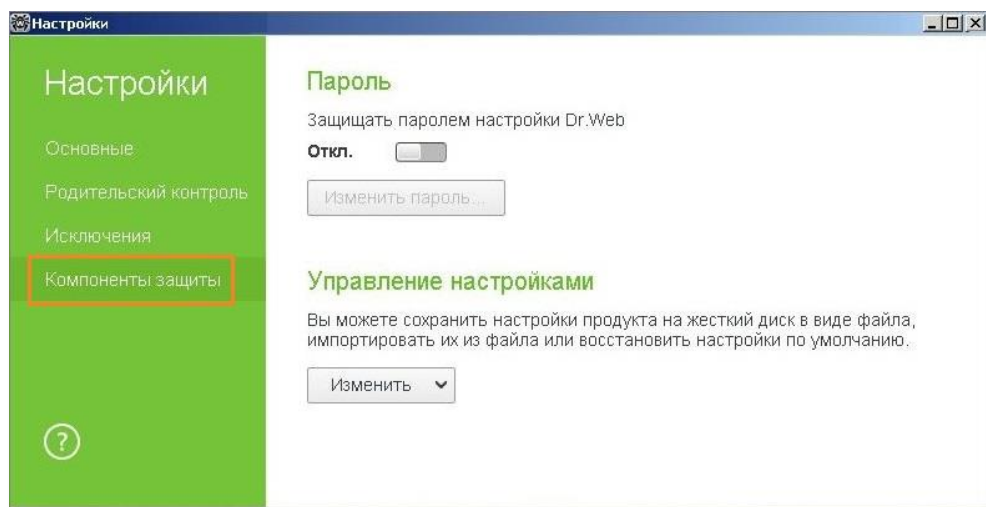
3. Нажать появившуюся кнопку  **Настройки** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 12 - Элемент управления Настройки



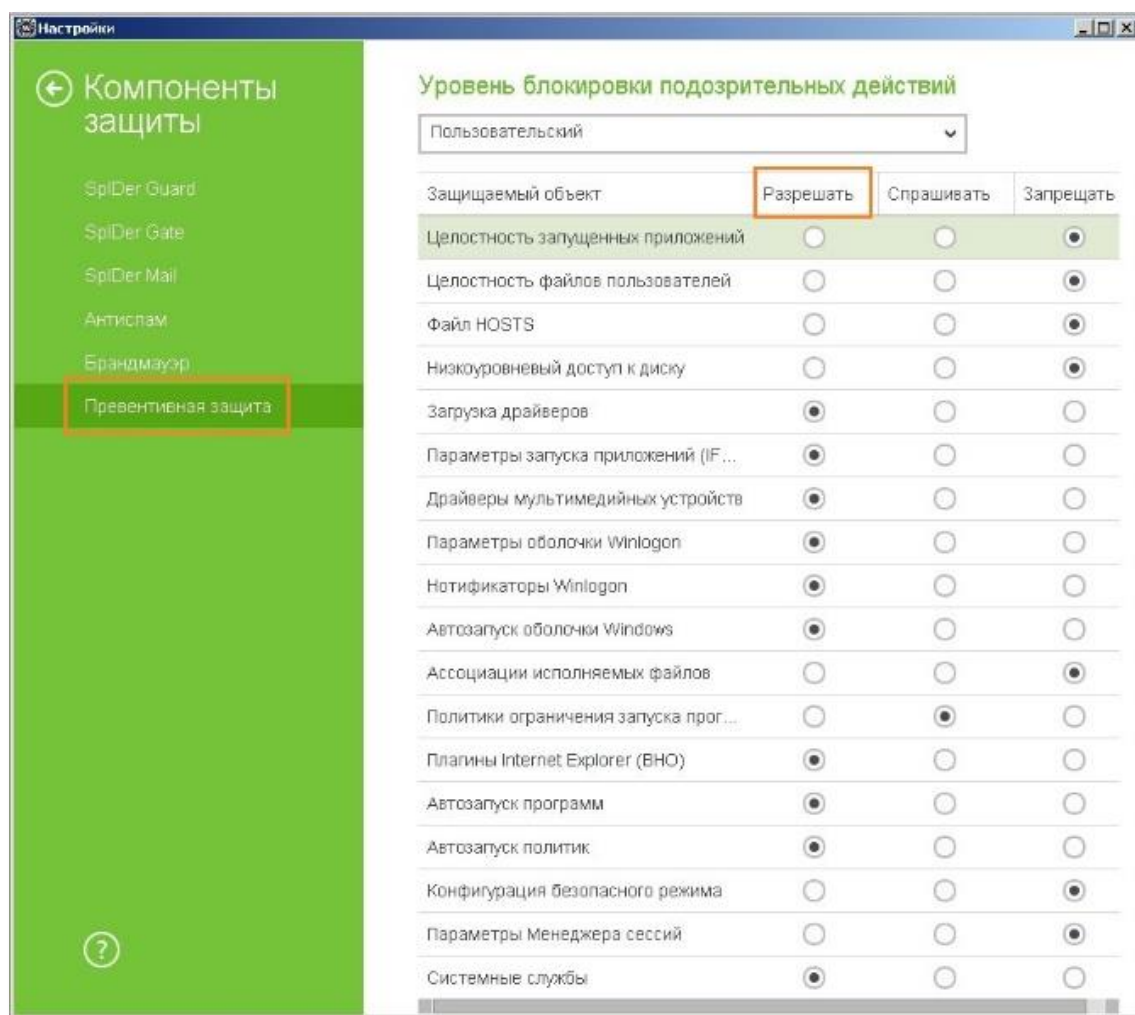
4. В окне **Настройки** выбрать опцию **Компоненты защиты** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 13 - Окно Настройки



5. В окне **Компоненты защиты** выбрать опцию **Превентивная защита** и установить для объектов параметр **Разрешать** в соответствии с Рисунком **Ошибка! Источник ссылки не найден.**

Рисунок 14 - Окно Компоненты защиты



6. Закрыть окно **Настройки** и установить ПО Единый Клиент JaCarta (подробнее см.раздел "4. Установка Единого Клиента JaCarta").


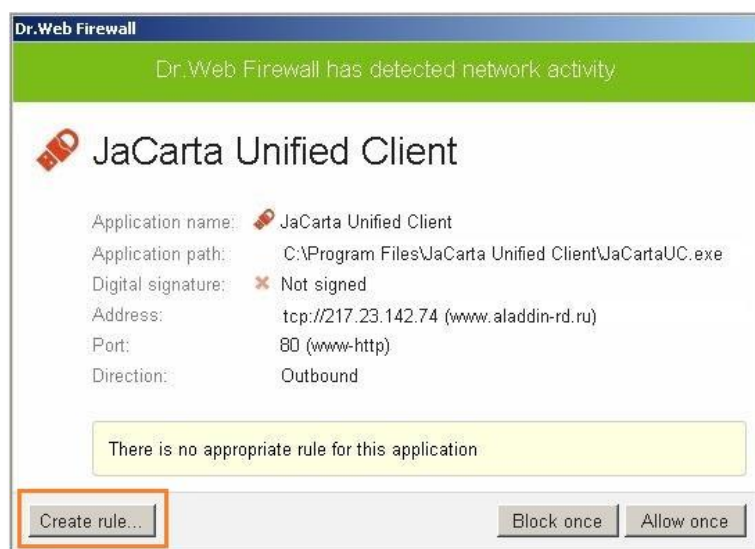
 **Внимание!** Если при установке ПО Единый Клиент JaCarta будет выбрана опция **Устанавливать обновления автоматически** или опция **Проверять наличие новых обновлений, но не устанавливать их**, то после перезагрузки ОС может появиться следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

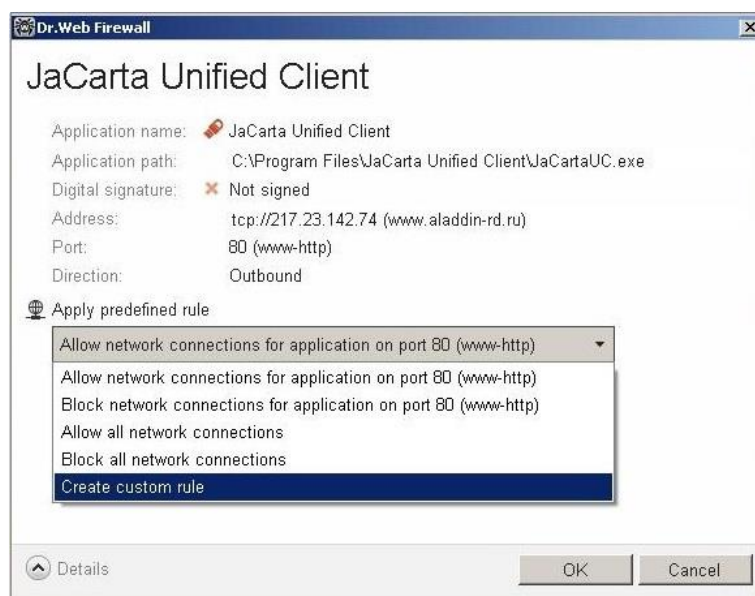
Рисунок 15 – Информационное окно антивируса Dr.Web



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.

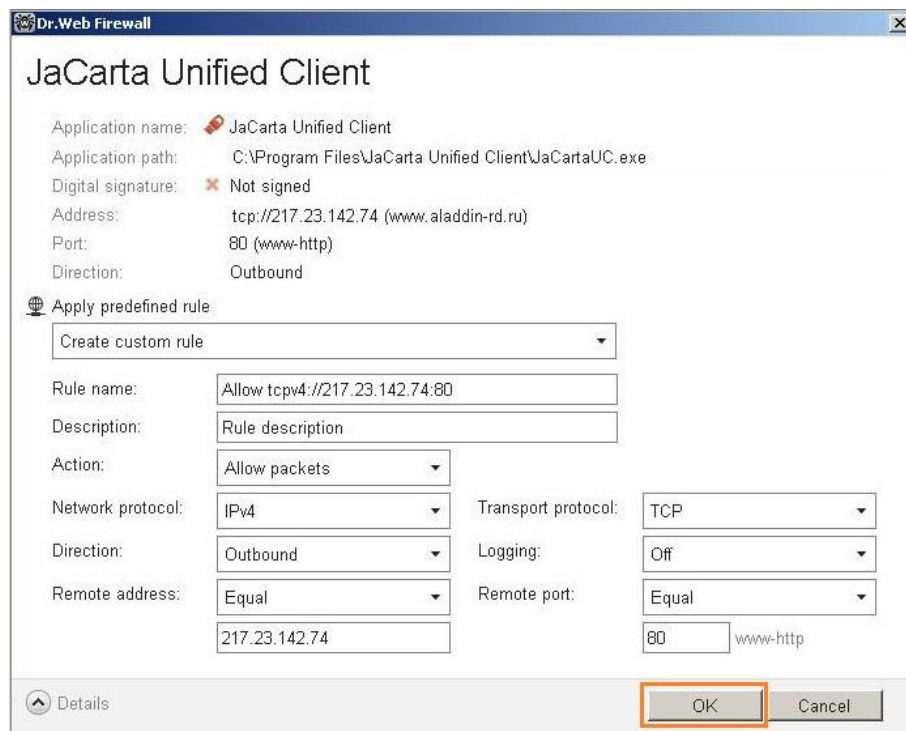
Для создания правила следует нажать кнопку **Create rule...** Далее в появившемся окне (см. Рис. **Ошибка! Источник ссылки не найден.**) необходимо раскрыть выпадающий список и выбрать одно из значений: **Allow network connections for application on 80**, **Allow all network connections** или **Create custom rule**. После нажать **OK**.

Рисунок 16 - Выбор правила



В случае, если была выбрана опция **Create custom rule**, будет отображено следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**), в котором необходимо нажать **OK** для завершения.

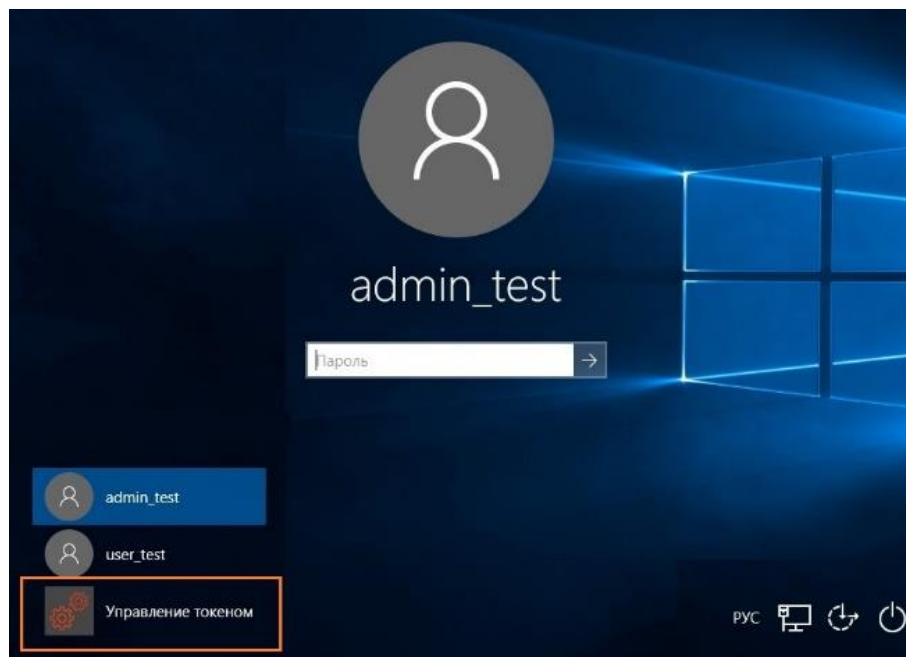
Рисунок 17 - Завершение настройки правила



4.4. Особенности отображения плитки Управление токеном после установки Единый Клиент JaCarta

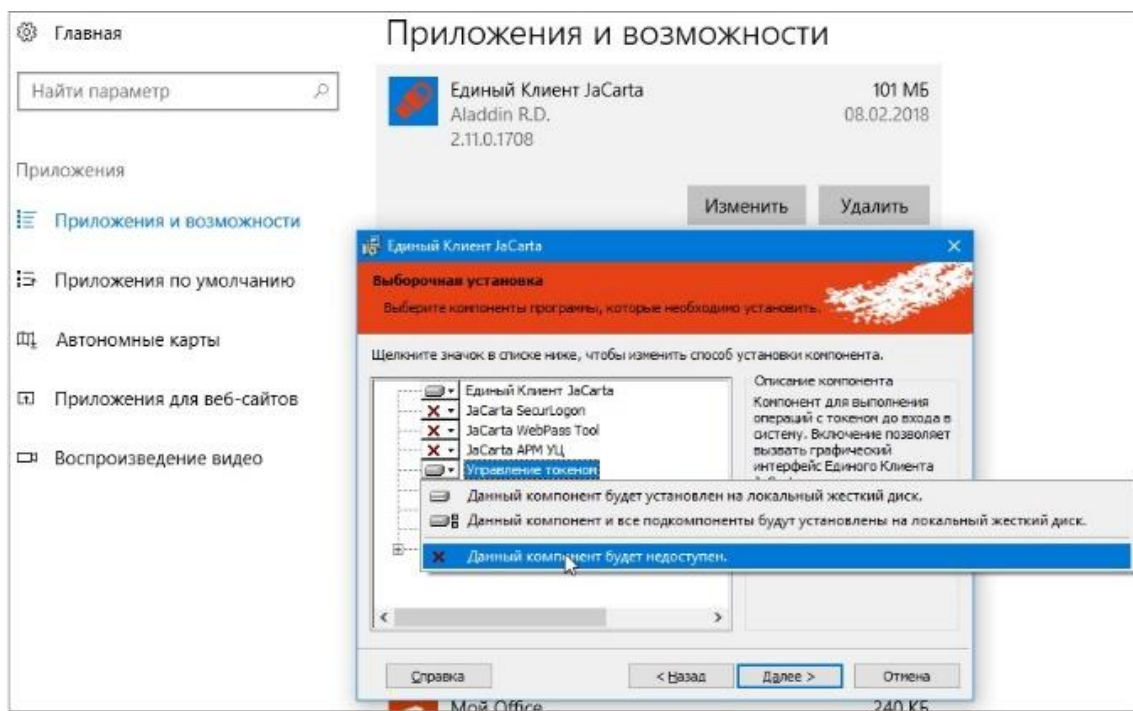
После завершения установки Единый клиент JaCarta и перехода в экран блокировки Windows, будет отображен элемент управления **Управление токеном**. Он появляется в случае, если в ходе установки был выбраны один из следующих видов: **Стандартная** или **Выборочная** с компонентом **Управление токеном**. (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 18 - Элемент управления на экране блокировки Windows



Скрыть отображение данного элемента управления можно с помощью удаления компонента **Управление токеном**. Для этого необходимо последовательно выбрать **Панель управления, Программы и компоненты, Единый Клиент JaCarta** и нажать кнопку **Изменить**. После чего исключить компонент **Управление токеном** из установленных компонентов (см. Рисунок 19).

Рисунок 19 - Исключение компонента "Управление токеном"



4.5. Установка в режиме командной строки

Другой вариант установки ПО Единый клиент JaCarta осуществляется с помощью командной строки, где в качестве параметров возможно указать необходимые для установки компоненты. В этом случае используется стандартный синтаксис Windows Installer:

```
msiexec /i JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi
```

где **JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi** – это пакет установки для 32-битных платформ Microsoft Windows.



Примечание – Для 64-битных платформ используйте пакет установки **JaCartaUnifiedClient_x.x.xx.xxx_win-x64_ru-Ru.msi**.

Чтобы установить Единый Клиент JaCarta в режиме командной строки, выполните следующие действия:

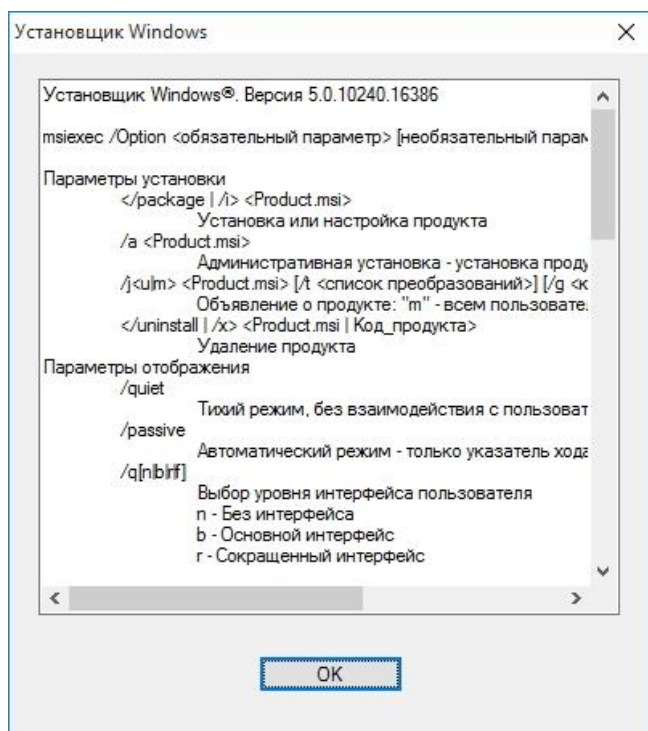
1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Выберите последовательно **Пуск, Все программы, Стандартные, Командная строка**.
4. Если вы выполняете установку в ОС Microsoft Windows Vista/7/8.1 Update 1/10/Server 2008/2012, у компонента **Командная строка** вызвать контекстное меню и выбрать пункт **Запуск от имени Администратора**.
5. Введите в командной строке **msiexec** с необходимыми параметрами.

4.5.1. Справка по Windows Installer

Встроенная справка Windows Installer предназначена для предоставления полного перечня возможных параметров, которые можно использовать при установке ПО Единый Клиент JaCarta. Для ее вызова выполните следующие действия.

1. Нажмите **Пуск**, затем **Выполнить**.
2. В поле **Открыть** введите **msiexec** и нажмите **ОК**.
На экране появится окно со списком параметров Windows Installer (см. Рисунок 20).

Рисунок 20 - Окно программы Windows Installer



4.5.2. Установка параметров в режиме командной строки

При установке в режиме командной строки существует возможность задавать особые параметры и их значения кроме тех, которые определены по умолчанию.

Чтобы установить параметры установки, используйте следующий формат:

```
msiexec /i JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi ПАРАМЕТР=ЗНАЧЕНИЕ
ПАРАМЕТР=ЗНАЧЕНИЕ /qb
```

Список параметров установки Единый Клиент JaCarta в режиме командной строки представлен в Таблице 7.

Таблица 7

Параметр	Описание
INSTALL_JC_CLIENT	Установка JC-Client 6.40
INSTALL_BIO	Установка поддержки биометрии (0 или 1).
INSTALL_SECURLOGON	Установка компонента SecurLogon (0 или 1).
INSTALL_GINA	Установка GINA для биометрии (Microsoft Windows XP) (0 или 1).
INSTALL_CRYPTOPRO_JCP	Установка поддержки для CPRO JCP (0 или 1). Даже если задано значение = 1, то установка будет возможна только при наличии установленного CPRO JCP и JRE.
INSTALL_CRYPTOPRO_CSP	Установка поддержки для CPRO CSP (0 или 1). Даже если задано значение = 1, то установка будет возможна только при наличии установленного CPRO CSP.
INSTALL_SIGNALCOM_CSP	Установка поддержки для SCOM CSP (0 или 1). Даже если задано значение = 1, то установка будет возможна только при наличии установленного SCOM CSP.
INSTALL_BIO_RDP	Установка компонентов RDP для биометрии (0 или 1).
INSTALL_BIO_CITRIX	Установка клиентских компонентов Citrix для биометрии (0 или 1). Даже если задано значение = 1, то установка будет возможна только при наличии установленного Citrix-client.

Параметр	Описание
INSTALL_CCID_FIX	Установка драйвера поддержки работы с устаревшими моделями токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware (0 или 1).
INSTALL_JCPRO_CLIENT	Установка драйвера поддержки работы с моделями токенов JaCarta PKI с обратной совместимостью (0 или 1).
INSTALL_MICROSD_SC_READER	Установка драйвера поддержки работы с моделями токенов JaCarta в форм-факторе Secure MicroSD (0 или 1).
INSTALL_USB_ETOKEN_DRIVER	Установка драйвера для eToken PRO 32K/64K (0 или 1).
INSTALL_ASEDRIVE	Установка драйвера для возможности работы с устаревшими моделями смарт-карт ридеров Athena (0 или 1).
INSTALL_JACARTA_CCID_DRIVER	Установка драйвера для возможности использования JaCarta на Windows 8.1 x64 (0 или 1).
INSTALL_ATHENA_CSP	Установка криптопровайдера Athena CSP (0 или 1).
INSTALL_DEF_ATHENA_CSP	Установка Athena CSP в качестве криптопровайдера по умолчанию (0 или 1)
INSTALL_JCWEBPASS	Установка утилиты JaCarta WebPass Tool (0 или 1).
INSTALL_TOKEN_MNG	Установка компонента Управление токеном (0 или 1).
INSTALL_CA_MANAGER	Установка утилиты APM УЦ (0 или 1).
UPDATE_UC	Задание настройки автоматического обновления Единого Клиента JaCarta (от 0 до 2: 0 – не проверять обновления; 1 – проверять обновления, но не устанавливать их; 2 – устанавливать обновления автоматически).
INSTALL_CERTS	Сертификаты для проверки подписи драйверов
INSTALL_MSVC80_CRT	Runtime от MS Visual Studio 2005 (для корректной работы частей от JC-Client)
INSTALL_MSVC90_CRT	Runtime от MS Visual Studio 2008 (для корректной работы JaCarta APM УЦ)
INSTALL_DIFXAPI	Difxapi.dll для работы custom actions исправляющих установку драйверов

Таблица 7

4.5.3. Пример комбинации параметров

При установке Единый Клиент JaCarta в режиме командной строки параметры установки можно комбинировать в одной команде, например:

```
msiexec.exe /i "<путь к файлу установки>\JaCartaUnifiedClient_2.9.1.1545_win-
x64_ru-Ru.msi" INSTALL_CCID_FIX=0 INSTALL_JCPRO_CLIENT=0
INSTALL_MICROSD_SC_READER=0
```

В данном примере будет выполнена установка со следующими параметрами:

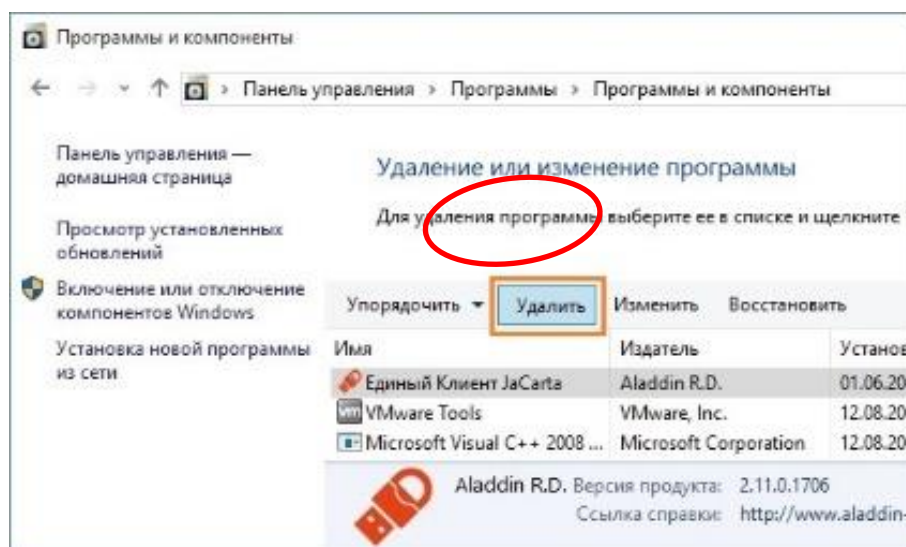
- INSTALL_CCID_FIX=0 - не устанавливать драйвер поддержки работы с устаревшими моделями токенов JaCarta (выпуск до 2014 года включительно) в инфраструктуре VMware;
- INSTALL_JCPRO_CLIENT=0 - не устанавливать драйвер поддержки работы с моделями токенов JaCarta PKI с обратной совместимостью;
- INSTALL_MICROSD_SC_READER=0 - не устанавливать драйвер поддержки работы с моделями токенов JaCarta в форм-факторе Secure MicroSD.

5. Удаление Единого Клиента JaCarta

Для удаления Единый Клиент JaCarta выполните следующие действия:

1. В **Панели управления** выберите пункт **Программы и компоненты**. Отобразится следующее окно (см. Рисунок 21).

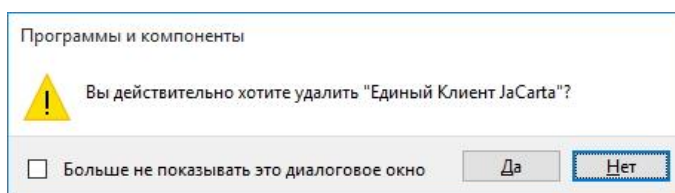
Рисунок 21 - Окно программы и компоненты – Удаление



2. В списке установленных программы отметьте пункт **Единый Клиент JaCarta** и нажмите **Удалить**. Отобразится следующее окно (см. Рисунок 22).

Окно предупреждения об удалении Единого Клиента JaCarta

Рисунок 22 - Окно предупреждения об удалении Единого Клиента JaCarta



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

Для удаления Единый Клиент JaCarta из командной строки, выполните следующие действия:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Запустите интерпретатор командной строки от имени администратора.
4. Выполните команду **msiexec** в следующем формате:

```
msiexec /x JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi
```

где JaCartaUnifiedClient_x.x.xx.xxx_win-x86_ru-Ru.msi – имя установочного файла Единый Клиент JaCarta для 32-битной платформы.

Для 64-битной платформы замените это имя на JaCartaUnifiedClient_x.x.xx.xxx_win-x64_ru-Ru.msi. Чтобы выполнить удаление в полуавтоматическом режиме, то есть без необходимости подтверждения действий, добавьте в конце строки параметр /q.

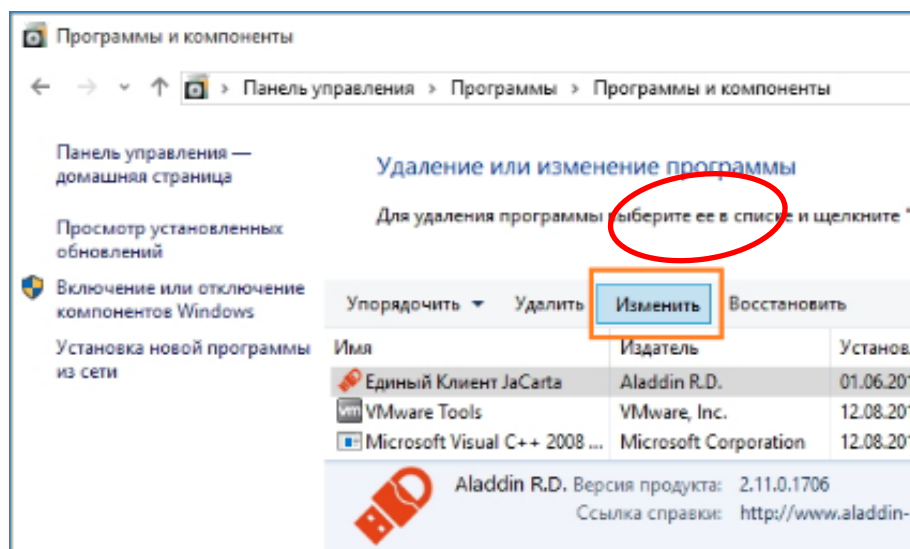
5. После того как Единый Клиент JaCarta будет удален, перезагрузите компьютер.

6. Изменение Единого Клиента JaCarta

Для изменения перечень установленных компонентов Единый Клиент JaCarta выполните следующие действия:

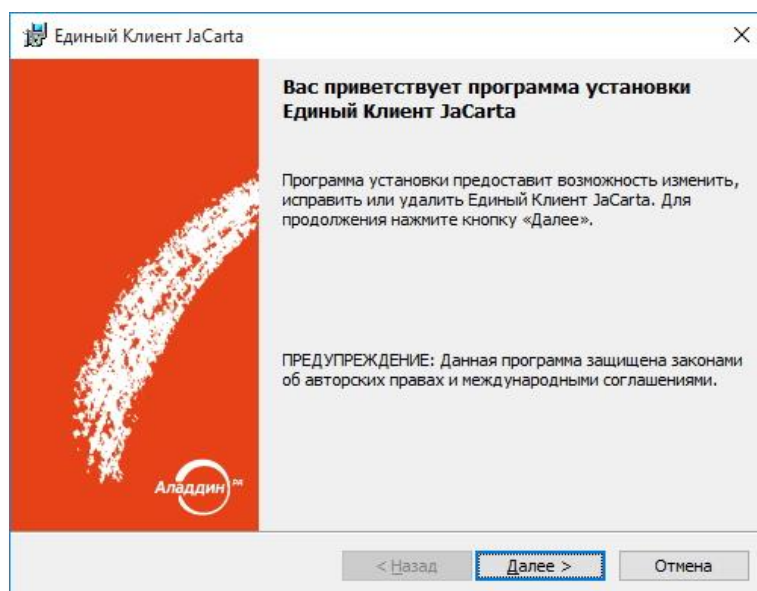
1. В **Панели управления** выберите пункт **Программы и компоненты**. Отобразится следующее окно (см. Рисунок 23).

Рисунок 23 - Окно программы и компоненты – Изменение



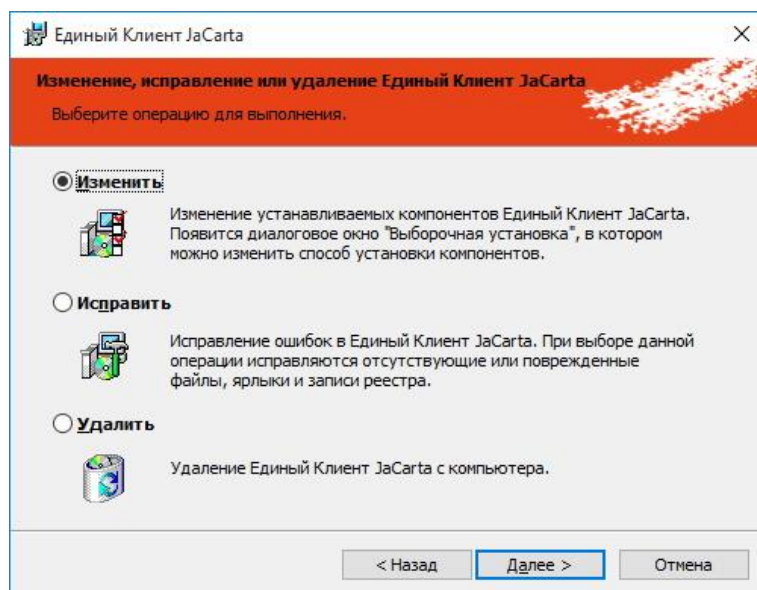
2. В списке установленных программ выбрать пункт **Единый Клиент JaCarta** и нажать **Изменить**. Отобразится следующее окно (см. Рисунок 24).

Рисунок 24 - Окно приветствия программы установки Единый Клиент JaCarta



3. В окне (см. Рисунок 24) нажмите **Далее** и в появившемся окне (см. Рис. **Ошибка! Источник ссылки не найден.**) выберите опцию **Изменить**. Нажмите **Далее**, после чего появится диалоговое окно **Выборочная установка компонентов Единый клиент JaCarta** (см. Рис. **Ошибка! Источник ссылки не найден.**), в котором возможно изменить перечень установленных компонентов Единый Клиент JaCarta.

Рисунок 25 - Окно выбора операций Единый Клиент JaCarta



Если необходимо добавить отсутствующие или исправить поврежденные файлы, ярлыки и записи реестра Единый Клиент JaCarta, то следует выбрать опцию **Исправить** и нажать **Далее**.

7. Обзор пользовательского интерфейса

7.1. Меню быстрого запуска


Для отображения **Меню быстрого запуска** Единый Клиент JaCarta служит элемент управления . Он расположен на **Панели задач** в группе, которая становится доступной по раскрытию элемента управления **Отображать скрытые значки** (см. Рисунок 26).

Рисунок 26 - Элемент управления "Отображать скрытые значки"




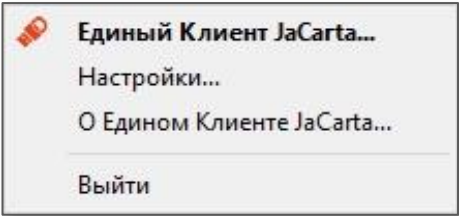
Доступ к **Меню быстрого запуска** Единого Клиента JaCarta осуществляется с помощью нажатия правой кнопкой мыши по элементу  (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 27 - Меню быстрого запуска



Описание пунктов меню быстрого запуска приведено в Таблице 8.

Таблица 8



Пункт меню	Описание
Единый Клиент JaCarta...	Открывает окно основного интерфейса Единого Клиента JaCarta (подробнее см. подраздел "7.2. Основной интерфейс").
Настройки...	Открывает окно, позволяющее редактировать общие настройки Единого Клиента JaCarta (подробнее см. раздел "8. Настройка работы Единый Клиент JaCarta").
О Едином Клиенте JaCarta...	Отображает сведения об установленном экземпляре Единого Клиента JaCarta (см. Рис. Ошибка! Источник ссылки не найден.).
Сменить PIN - код и пароль домена...	Открывает окно для смены PIN-кода и пароля домена.  Эта опция появляется в Меню быстрого запуска после введения имени домена для синхронизации паролей. Ввод имени домена выполняется через реестр. Подробнее см. раздел "18. Синхронизация паролей электронного ключа и учетной записи домена Windows".
Выйти	Скрывает значок  из области уведомлений на панели задач и осуществляет выход из Единого Клиента JaCarta.


Таблица 8

Рисунок 28 - Информационное окно "О программе"



7.2. Основной интерфейс

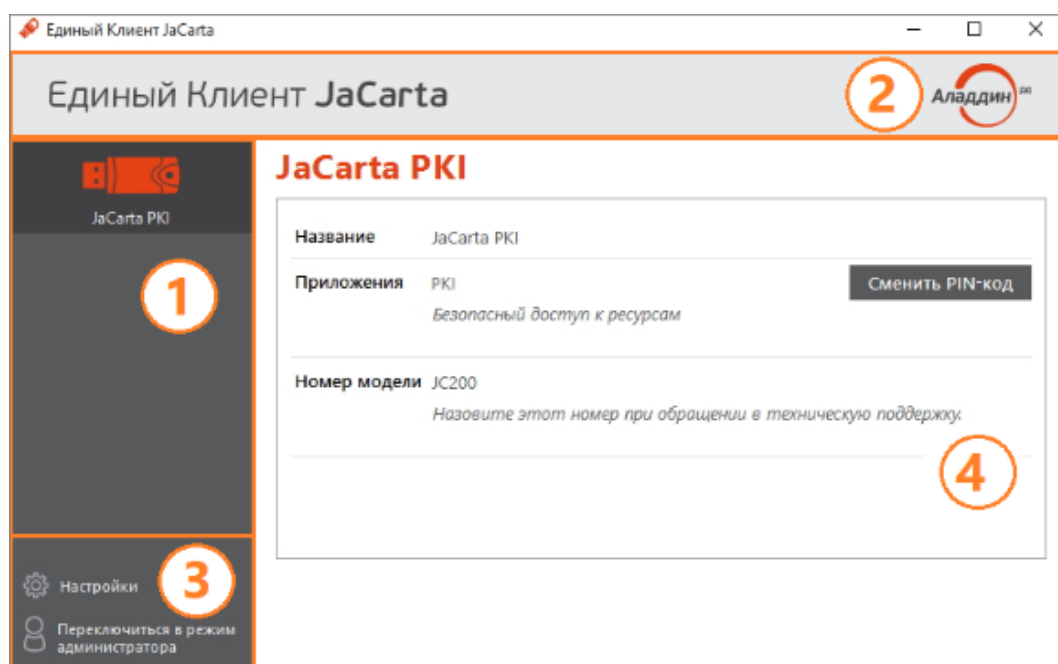
Чтобы открыть основное окно пользовательского интерфейса Единого Клиента JaCarta выполните одно из следующих действий:

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

или

- В меню **Пуск** последовательно выберите **Все программы, Аладдин Р. Д., Единый Клиент JaCarta**.

Рисунок 29 - Основное окно пользовательского интерфейса



Основное окно содержит следующие настройки:

- 1 - Перечень электронных ключей, подключенных к компьютеру. Обозначение электронного ключа зависит от его типа. Перечень обозначений и описание электронных ключей приведены в Таблице 9;
- 2 - При нажатии на логотип компании в верхнем правом углу окна – появится окно со сведениями о программе Единый Клиент JaCarta (см. Рис. **Ошибка! Источник ссылки не найден.**);
- 3 - Элементы управления, позволяющие перейти к следующим настройкам:
 - **Настройки** – после нажатия будет открыто окно настроек Единого Клиента JaCarta (см. раздел "8. Настройка работы Единый Клиент JaCarta");
 - **Переключиться в режим администратора/пользователя** – позволяет переключить Единый Клиент JaCarta в режим администратора или в режим пользователя соответственно;
- 4 - Отображения настроек выбранного электронного ключа из перечня доступных.

Таблица 9













Изображение	Описание
	MicroUSB-токен
	USB-токен JaCarta в корпусе nano
	USB-токен JaCarta в корпусе nano с кнопкой
	USB-токен JaCarta в корпусе mini
	USB-токен JaCarta в корпусе XL
	Смарт-карта
	eToken PRO (Java)
	eToken NG-FLASH (Java)
	eToken NG-OTP (Java)
	Тип электронного ключа не определён
	Электронный ключ в форм-факторе Secure MicroSD
	Электронный ключ находится на стадии определения

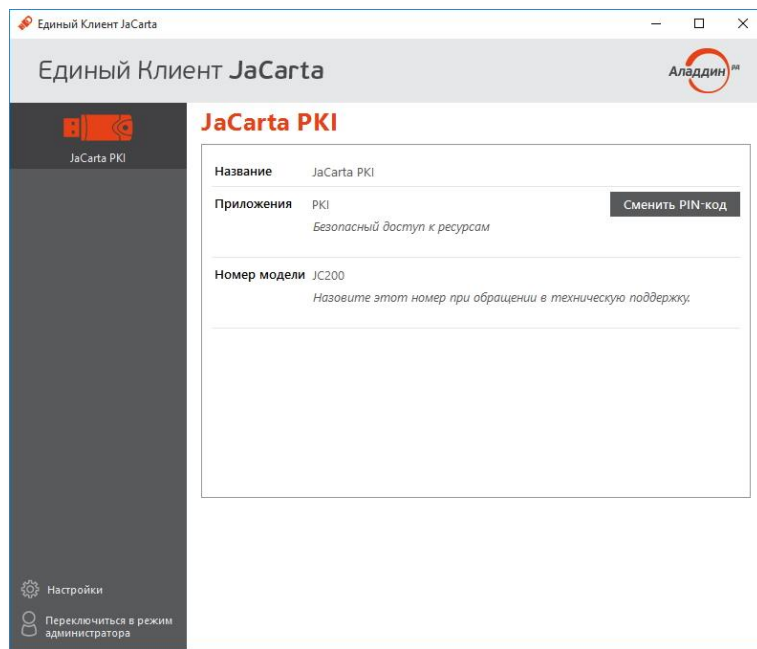
Таблица 9

7.2.1. Режим пользователя

Окно ПК Единый Клиента JaCarta в режиме пользователя выглядит следующим образом (см. Рис. **Ошибка! Источник ссылки не найден.**).

Окно в режиме пользователя

Рисунок 30 - Окно в режиме пользователя



Описание интерфейса Единый Клиент JaCarta в режиме пользователя приведено в Таблице 10.

Таблица 10

Поле	Описание
Название	Название модели выбранного электронного ключа.
Приложения	Список приложений, установленных в памяти выбранного электронного ключа. Кнопка Сменить PIN-код - Сменить PIN-код позволяет сменить PIN-код пользователя (описание процедуры смены PIN-кода 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 10

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

7.2.2. Режим администратора

Переход из режима пользователя в режим администратора осуществляется с помощью

нажатия на кнопку **Переключиться в режим администратора** - **Переключиться в режим администратора**. При переходе в режим администратора в основном окне интерфейса Единый Клиент JaCarta появляются вкладки. Описание вкладок приведено в Таблице 11.

Таблица 11

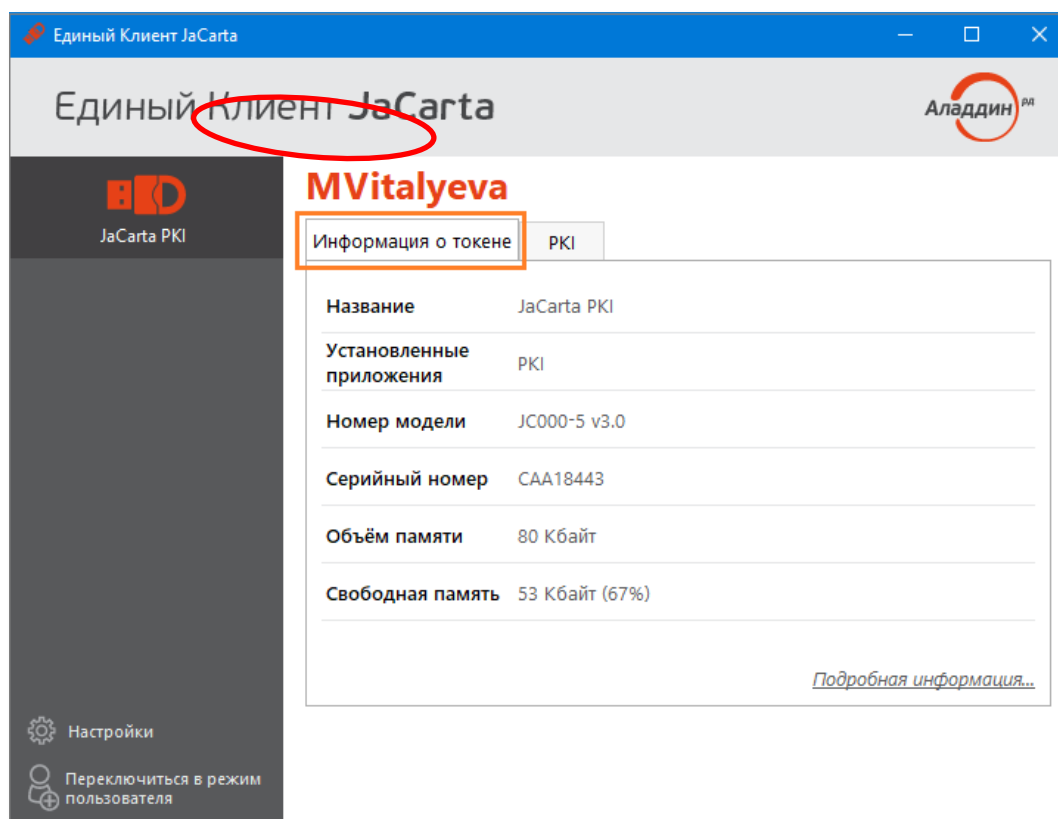
Вкладка	Описание
Информация о токене	На этой вкладке отображаются общие сведения о выбранном электронном ключе. Чтобы отобразить

Вкладка	Описание
	подробные сведения, нажмите Подробная информация... (Подробнее см. "Ошибка! Источник ссылки не найден.")
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 выбранный электронный ключ поддерживает хранение профилей SecurLogon

Таблица 11

Вкладка **Информация о токене** имеет следующий вид (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 31 - Вкладка Информация о токене



Описание отображаемых полей на вкладке **Информация о токене** приведено в Таблице 12.

Таблица 12

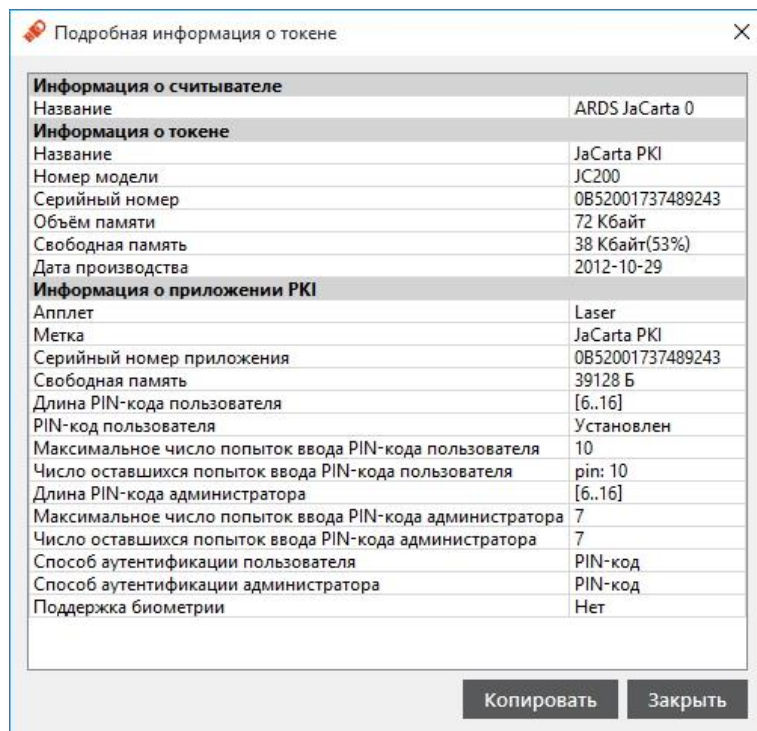
Поле	Описание
Название	Название модели выбранного электронного ключа
Установленные приложения	Приложения, установленные на выбранном электронном ключе
Номер модели	Номер модели выбранного электронного ключа
Серийный номер	Серийный номер выбранного электронного ключа
Объём памяти	Полный объём памяти выбранного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

Поле	Описание
Свободная память	Объём свободной памяти выбранного электронного ключа

Таблица 12

Ниже располагается ссылка [Подробная информация...](#), нажатие на которую открывает окно с подробными сведениями о выбранном электронном ключе (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 32 - Подробная информация о токене



Описание предоставляемой информации о токене приведено в Таблице 13.

Таблица 13


Секция	Поле	Описание
Информация о считывателе	Название	Название используемого считывателя
Информация о токене	Название	Имя выбранного электронного ключа
	Номер модели	Модель выбранного электронного ключа
	Серийный номер	Серийный номер микросхемы выбранного электронного ключа
	Объём памяти	Общий объём памяти выбранного электронного ключа
	Свободная память	Объём свободной памяти выбранного электронного ключа
	Дата производства	Дата производства выбранного электронного ключа
Информация о приложении	Апплет	Название используемого апплета выбранного электронного ключа
	Метка	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

Секция	Поле	Описание
	Длина PIN-кода пользователя	Количество символов PIN-кода пользователя для выбранного приложения
	PIN-код пользователя	Статус PIN-кода пользователя приложения: установлен/не установлен
	Максимальное число попыток ввода PIN-кода пользователя	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя
	Число оставшихся попыток ввода PIN-кода пользователя	Число неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода пользователя
	Длина PIN-кода администратора	Длина PIN-кода администратора выбранного приложения
	Максимальное число попыток ввода PIN-кода администратора	Максимально допустимое число неверных последовательных попыток ввода PIN-кода администратора
	Число оставшихся попыток ввода PIN-кода администратора	Число неверных попыток ввода PIN-кода пользователя до блокировки возможности использования PIN-кода администратора
	Способ аутентификации пользователя	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
	Поддержка биометрии	Статус поддержки биометрии (Да/Нет)

Таблица 13

8. Настройка работы Единый Клиент JaCarta

Окно **Настройки** (см. Рис. **Ошибка! Источник ссылки не найден.**) Единого Клиента JaCarta можно вызвать двумя способами:

- С помощью нажатия правой кнопкой мыши на значке  в области уведомлений и выбора пункта **Настройки...**;
- В левом нижнем углу основного окна Единого Клиента JaCarta нажать кнопку **Настройки** -

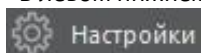
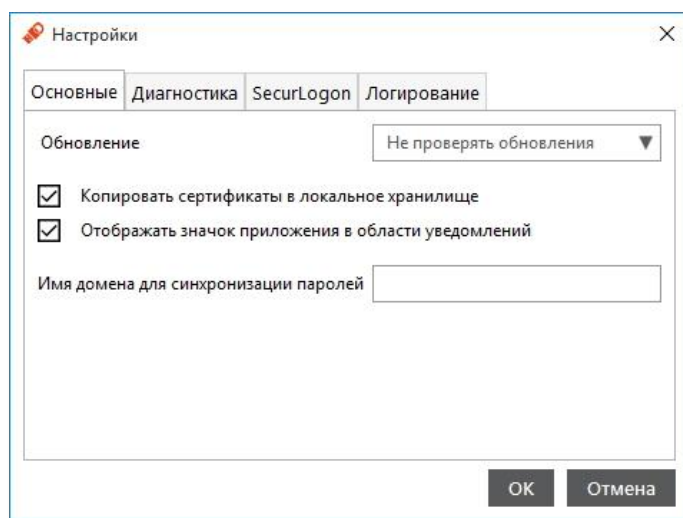


Рисунок 33 - Настройки Единого Клиента JaCarta на вкладке Основные




Окно **Настройки** содержит четыре вкладки:

- Основные;
- Диагностика;
- SecurLogon;
- Логирование.

Описание настроек на вкладке **Основные** приведено в Таблице 14. После изменения настроек следует нажать **ОК**, чтобы сохранить изменения.

Таблица 14

Настройка	Описание
Обновление	<p>Выпадающий список содержит три пункта:</p> <ul style="list-style-type: none"> • 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 локальное хранилище	Если флажок установлен, сертификаты в памяти подсоединённых электронных ключей будут копироваться в локальное хранилище сертификатов.
Отображать значок приложения в области уведомлений	<p>Определяет, будет ли отображаться значок  в области уведомлений.</p>

Настройка	Описание
уведомлений	
Имя домена для синхронизации паролей	Содержит поле для отображения имени домена Windows, в котором зарегистрирована учетная запись пользователя. После ввода имени домена становится доступной кнопка смены PIN-кода и пароля домена (см. Рис. Ошибка! Источник ссылки не найден.). Описание процедуры смены PIN-кода и пароля домена приведено в разделе "18. Синхронизация паролей электронного ключа и учетной записи домена Windows".

Таблица 14

Описание окна Настройки на вкладке **Диагностика** (см. Рис. **Ошибка! Источник ссылки не найден.**) приведено в Таблице 15, после изменения настроек следует нажать **ОК**, чтобы сохранить изменения.

Рисунок 34 - вкладка Диагностика

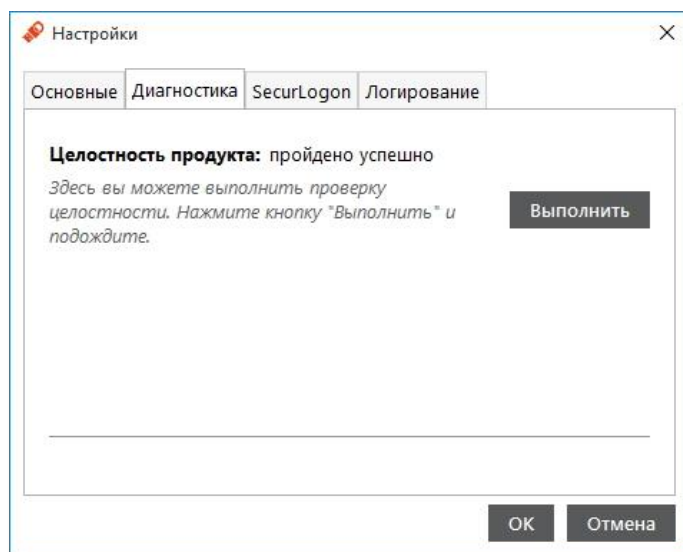


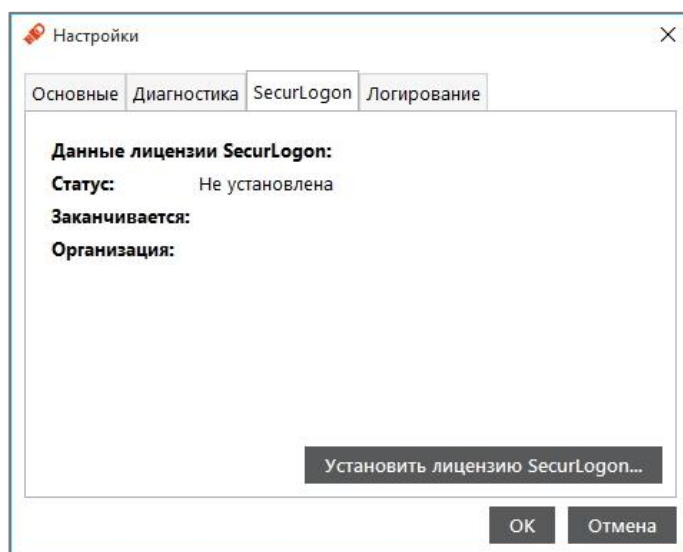
Таблица 15

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

Таблица 15

Описание окна Настройки на вкладке **SecurLogon** (см. Рис. **Ошибка! Источник ссылки не найден.**) приведено в Таблице 16, после изменения настроек следует нажать **ОК**, чтобы сохранить изменения.

Рисунок 35 - вкладка SecurLogon



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

Таблица 16

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

Таблица 16

Описание окна Настройки на вкладке **Логирование** (см. Рис. **Ошибка! Источник ссылки не найден.**) приведено в Таблице 17.



Внимание! Подробнее об изменении настроек логирования через редактор реестра см. документ [Единый Клиент JaCarta. Инструкция по сбору диагностической информации]. Подробные сведения о включении и настройках логирования так же изложены в базе знаний: <http://kbp.aladdin-rd.ru/index.php?View=entry&EntryID=95>

Рисунок 36 - вкладка Логирование

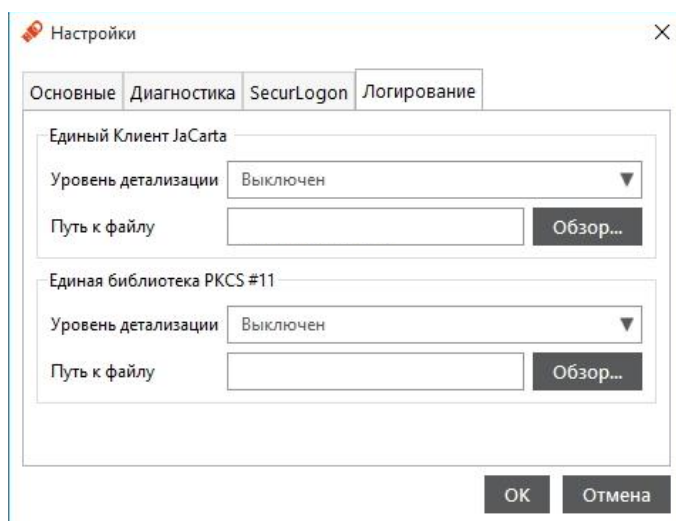


Таблица 17

Элемент интерфейса	Описание
Сегмент Единый Клиент JaCarta	<p>Отображает настройки логирования Единого Клиента JaCarta:</p> <ul style="list-style-type: none"> • Уровень детализации – для выбора опций: Выключен / Стандартный. • Поле Путь к файлу – для отображения пути к файлу с логами. • Кнопка Обзор... – для указания места расположения файла с логами.
Сегмент Единая библиотека PKCS #11	<p>Отображает настройки логирования Единой библиотеки PKCS #11:</p> <ul style="list-style-type: none"> • Уровень детализации – для выбора опций: Выключен / Стандартный / Расширенный. • Поле Путь к файлу – для отображения пути к файлу с логами. • Кнопка Обзор... – для указания места расположения файла с логами.

Таблица 17

9. Инициализация электронных ключей



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

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

Чтобы подготовить электронный ключ к работе, выполните следующие действия:


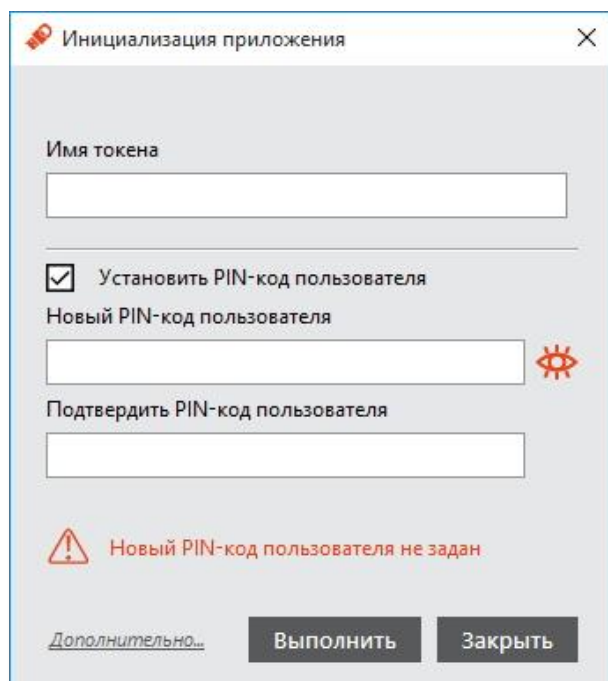
1. Запустите Единый Клиент JaCarta и переключитесь в режим администратора.
2. Подсоедините электронный ключ к компьютеру. Если вставлен один ключ, то его настройки в центральной части окна будут отображены по умолчанию. В случае присоединения нескольких электронных ключей, необходимо выбрать один токен и перейти к его настройкам. Единого Клиента JaCarta и
3. Перейти на вкладку PKI, если она не будет выбрана автоматически..
4. Нажмите **Инициализировать...** -  [Инициализировать...](#). Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 37 - Общие параметры инициализации



5. Выполнить настройку. Описание общих параметров инициализации приведено в Таблице 18.

Таблица 18

Поле	Описание
Имя токена	Укажите в этом поле название 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 потребуются PIN-код администратора).
Новый PIN-код пользователя	Введите значение PIN-кода пользователя (данное поле активно, если установлен флажок Установить PIN-код пользователя).

Таблица 18

6. Если вы хотите настроить дополнительные параметры инициализации, нажмите **Дополнительно...**, в противном случае переходите к шагу 15 настоящей процедуры. После нажатия **Дополнительно...** отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 38 - Окно дополнительных настроек инициализации. Вкладка Параметры

7. Выполнить настройку. Описание дополнительных настроек на вкладке **Параметры** приведено в Таблице 19.

Таблица 19

Секция	Настройка	Описание
PIN-код пользователя	Максимальное число попыток PIN-кода	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.
PIN-код	Установить PIN-код	Если флажок установлен, в процессе инициализации будет установлен PIN-код

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

Таблица 19

8. Перейдите на вкладку **Политика PIN-кода**. Окно примет следующий вид (см. Рис. **Ошибка! Источник ссылки не найден.**).



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

Рисунок 39 - Окно дополнительных настроек инициализации. Вкладка Политика PIN-кода

9. Выполнить настройку. Описание дополнительных настроек на вкладке Политика PIN-кода приведено в Таблице 20.

Таблица 20

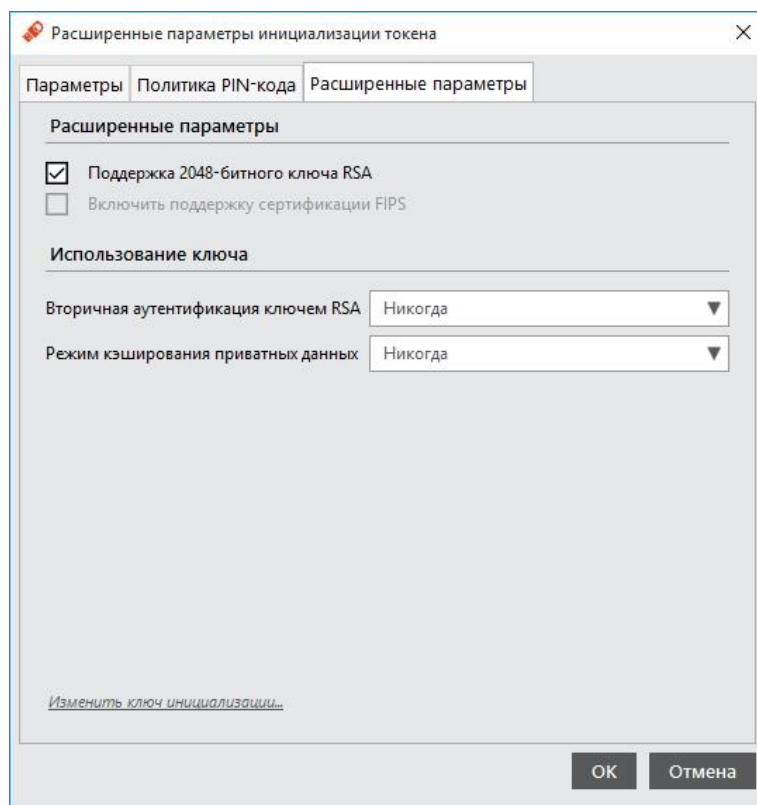
Секция	Настройка	Описание
Базовые политики PIN-кода пользователя	Минимальная длина PIN-кода	Минимальное количество символов, которые можно использовать в PIN-коде.
	Минимальный срок действия PIN-кода	Минимальный срок (в днях), в течение которого можно использовать PIN-код пользователя.
	Максимальный срок действия PIN-кода	Максимальный срок (в днях), в течение которого можно использовать PIN-код пользователя.
	Предупреждение об истечении PIN-кода (дней)	За сколько дней до окончания срока действия PIN-кода пользователя автоматически будет отправлено соответствующее уведомление.

Секция	Настройка	Описание
	История PIN-кода	Число использовавшихся ранее PIN-кодов пользователя, которые нельзя использовать при назначении нового PIN-кода пользователя. Например, если установлено значение «3», невозможно будет назначить PIN-код пользователя, совпадающий с одним из трёх ранее использованных.
Расширенные политики PIN-кода пользователя	Включить расширенный контроль качества PIN-кода	Установка флажка позволяет выполнить тонкую настройку качества PIN-кодов пользователя.
	Числовые символы	Выпадающий список содержит варианты использования цифр в PIN-коде пользователя: <ul style="list-style-type: none"> • Не важно • Запрещено • Обязательно
	Символы верхнего регистра	Выпадающий список содержит варианты использования алфавитных символов верхнего регистра в PIN-коде пользователя: <ul style="list-style-type: none"> • Не важно • Запрещено • Обязательно
	Символы нижнего регистра	<ul style="list-style-type: none"> • Выпадающий список содержит варианты использования алфавитных символов нижнего регистра в PIN-коде пользователя: Не важно • Запрещено • Обязательно
	Специальные символы	<ul style="list-style-type: none"> • Выпадающий список содержит варианты использования специальных символов в PIN-коде пользователя: 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 20


10. Перейдите на вкладку **Расширенные параметры**. Окно примет следующий вид (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 40 - Окно дополнительных настроек инициализации. Вкладка Расширенные параметры



11. Выполнить настройку. Описание дополнительных настроек на вкладке Расширенные параметры приведено в Таблице 21 .

Таблица 21

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; Предлагать по требованию приложения (Prompt conditional) - в этом режиме приложения могут запрашивать пароль для ключа RSA, если в них предусмотрена такая возможность; Всегда запрашивать у пользователя (Prompt always) – 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; Всегда (Mandatory) –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; • При входе пользователя – кэширование производится при входе

Секция	Настройка	Описание
		пользователя, данные сохраняются в кэше до завершения сеанса входа; • Всегда – кэширование производится всегда.

Таблица 21

12. Если вы хотите изменить ключ инициализации, нажмите на ссылке **Изменить ключ инициализации...** внизу окна. В противном случае переходите к шагу 14 настоящей процедуры. После нажатия **Изменить ключ инициализации...** отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 41 - Параметры ключа инициализации

Описание настроек в окне Параметры ключа инициализации приведены в Таблице 22.

Таблица 22

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 22

13. Нажмите **ОК**, чтобы закрыть окно параметров ключа инициализации.
14. Нажмите **ОК**, чтобы закрыть окно расширенных параметров инициализации электронного ключа.
15. В окне **Инициализация приложения** (см. Рис. **Ошибка! Источник ссылки не найден.**) нажмите **Выполнить**.
16. Подтвердите свой выбор в отобразившемся окне предупреждения.
17. При успешной инициализации отобразится соответствующее сообщение – нажмите **ОК**, чтобы закрыть его.

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

9.2.1. 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 42 - Общие параметры инициализации

4. Выполнить настройку. Описание общих параметров инициализации приведено в Таблице 23.

Таблица 23

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: <ul style="list-style-type: none">•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.

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

Таблица 23

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. **Ошибка! Источник ссылки не найден.**).

Рисунок 43 - Дополнительные параметры инициализации

6. Выполнить настройку. Описание расширенных параметров инициализации приведено в Таблице 24.

Таблица 24

Секция	Настройка	Описание
PIN-код пользователя	Тип PIN-кода	<p>Возможны четыре варианта:</p> <ul style="list-style-type: none"> •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).

Секция	Настройка	Описание
	Максимальное число попыток ввода PIN-кода	Максимально допустимое число неверных последовательных попыток ввода PIN-кода пользователя.
	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	При установке флажка пользователю будет необходимо сменить PIN-код при первом использовании электронного ключа
	Пользователь должен поменять PIN-код после разблокировки	При установке флажка пользователю будет необходимо сменить PIN-код после разблокировки электронного ключа.
PIN-код администратора	Установить новый PIN-код администратора	Установка этого флажка делает доступными поля для ввода нового PIN-кода администратора и для повторного подтверждения этого кода.
	PIN-код администратора	Введите значение нового PIN-кода администратора. Ключ администратора может быть: <ul style="list-style-type: none"> • значением, соответствующим установленному качеству паролей (см. качество PIN-кода ниже); • ключом 3DES (если установлен флажок Разрешить разблокировку с использованием механизма запрос-ответ).
	Максимальное число 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 24

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. **Ошибка! Источник ссылки не найден.**). Окно настроек качества PIN-кода пользователя выглядит следующим образом (см. Рис. **Ошибка! Источник ссылки не найден.**). Описание настроек качества PIN-кода приведено в Таблице 25.



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 **ОК**, чтобы сохранить настройки.

Рисунок 44 - Окно настроек качества PIN-кода пользователя



Таблица 25

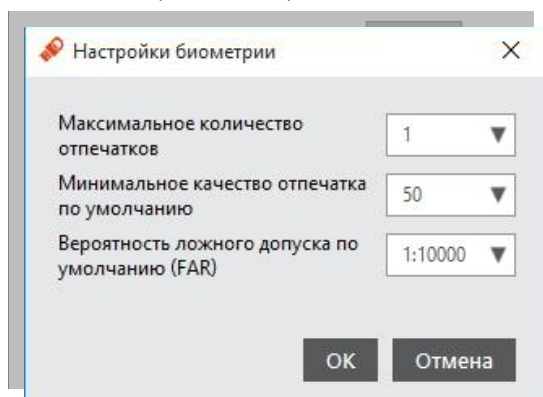
Секция	Настройка	Описание
Базовые настройки PIN-кода	Ограничение разблокировок	Установите флажок и задайте количество возможных разблокировок заблокированного PIN-кода
	Минимальная длина PIN-кода	Минимальное число символов в PIN-коде
	Максимальная длина PIN-кода	Максимальное число символов в PIN-коде
Расширенные настройки PIN-кода	Минимальное число цифровых символов	Определяет, сколько цифровых символов необходимо использовать в PIN-коде
	Минимальное число буквенных символов	Определяет, сколько буквенных символов необходимо использовать в PIN-коде
	Минимальное число символов нижнего регистра	Определяет, сколько буквенных символов в нижнем регистре необходимо использовать в PIN-коде
	Минимальное число символов верхнего регистра	Определяет, сколько буквенных символов в верхнем регистре необходимо использовать в PIN-коде
	Минимальное число специальных символов	Определяет, сколько специальных (не алфавитно-цифровых) символов необходимо использовать в PIN-коде
	Максимальное число повторов символов	Определяет число повторяющихся символов в любом месте PIN-кода

Таблица 25

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

- PKI – переходите к шагу 13 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 45 - Окно настроек биометрии



10. Выполнить настройку. Описание настроек биометрии приведено в Таблице 26.

Таблица 26

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 26

11. Нажмите **ОК**, чтобы сохранить изменения настроек биометрии.
12. Нажмите **ОК**, 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. 9.2.2. Инициализация с биометрическими параметрами.

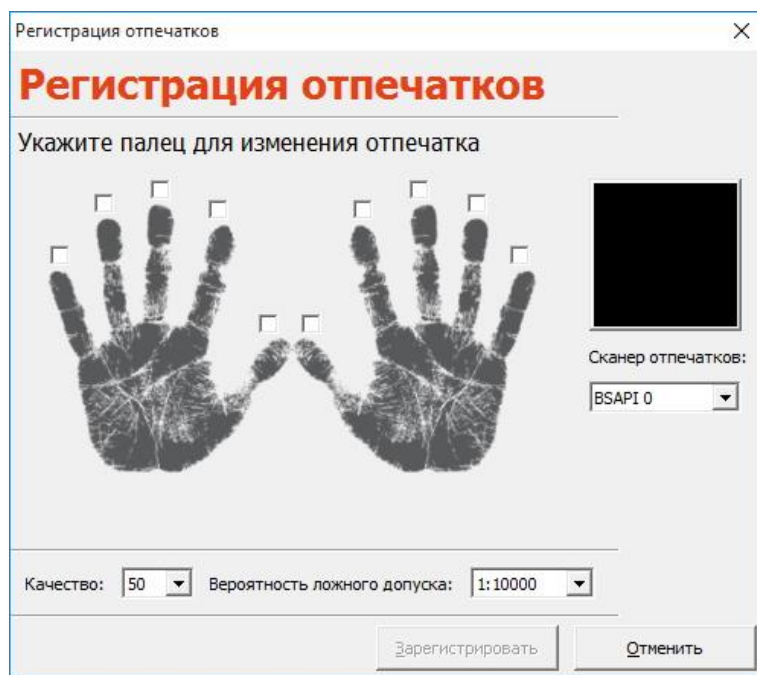
14. В случае успешной инициализации отобразится соответствующее сообщение – нажмите **ОК**, чтобы закрыть его.

Электронный ключ можно передать пользователю.

9.2.2. Инициализация с биометрическими параметрами

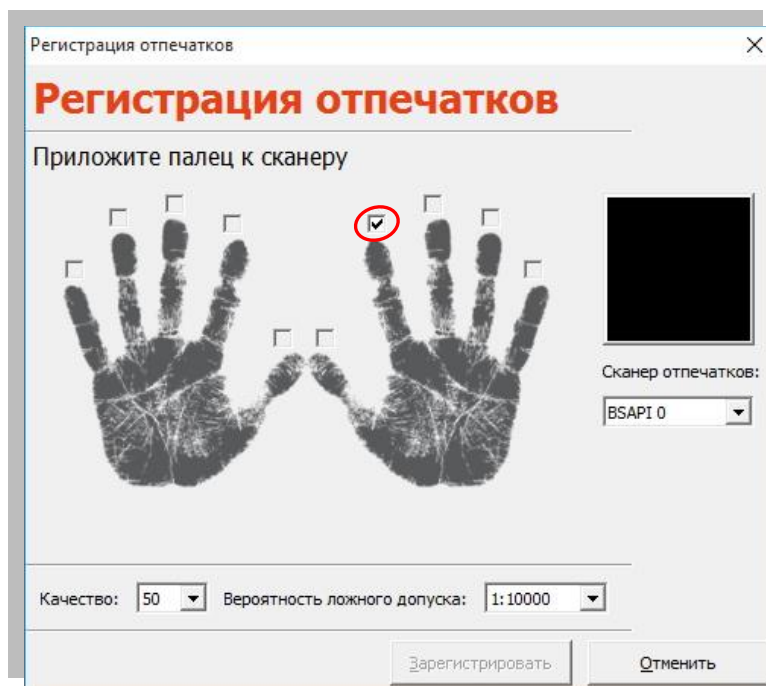
Если вы инициализируете электронный ключ с биометрическими настройками, через некоторое время после запуска процесса инициализации отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 46 - Окно регистрации отпечатков



1. На схематическом изображении ладоней отметьте палец, который будет отсканирован во время инициализации (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 47 - Окно выбора пальца для сканирования



2. При необходимости измените дополнительные параметры сканирования. Описание дополнительных параметров сканирования приведено в Таблице 27.

Таблица 27

Настройка	Описание
Сканер отпечатков	Используемый сканер отпечатков пальцев.
Качество изображения	Определяет граничное значение качества изображения. Если качество изображения ниже данного

Настройка	Описание
	значения, сохранение отпечатков пальцев пользователя не будет производиться.
Вероятность ложного допуска	<p>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.</p> <p>Рекомендуемое значение: 1:10000.</p>

Таблица 27

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

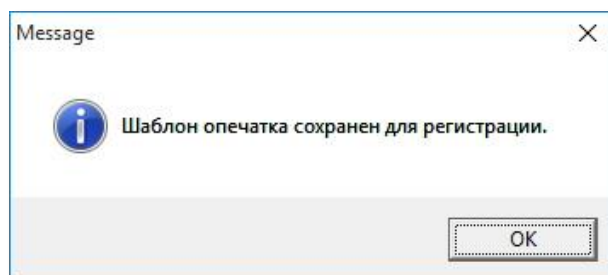
После считывания отпечатка пальца отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 48 - Результат считывания отпечатка пальца



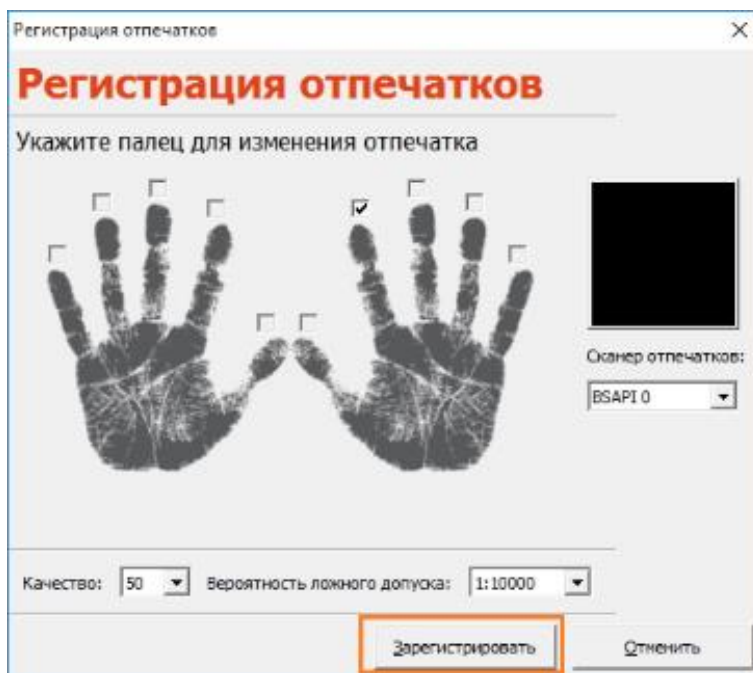
- После того, как приложенный палец будет убран со сканера отпечатков, отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**). Нажмите **ОК**.

Рисунок 49 - Информационное сообщение о сохранении шаблона отпечатка



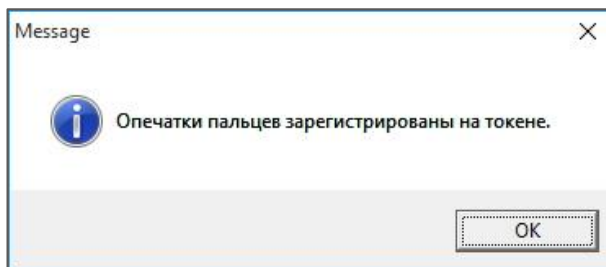
В окне регистрации отпечатков станет доступна кнопка **Зарегистрировать** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 50 - Окно регистрации отпечатков



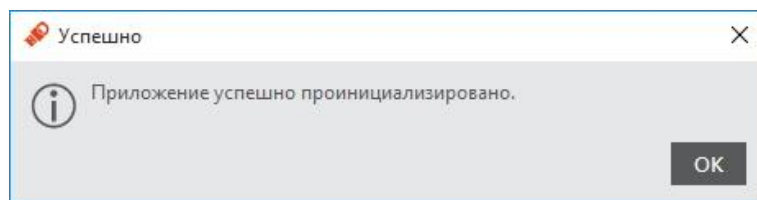
5. Нажмите **Зарегистрировать**. В отобразившемся окне (см. Рис. **Ошибка! Источник ссылки не найден.**) нажмите **ОК**.

Рисунок 51 - Информационное сообщение о регистрации отпечатков пальцев



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. **Ошибка! Источник ссылки не найден.**). Нажмите **ОК** для его закрытия.

Рисунок 52 - Сообщение об успешной инициализации



Инициализация завершена. Электронный ключ можно передавать пользователю.

9.3. 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 53 - Окно инициализации электронного ключа

4. Выполнить настройку. Описание настроек инициализации электронного ключа приведено в Таблице 28.

Таблица 28

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 название инициализируемого приложения.
Установить PIN-код пользователя	<ul style="list-style-type: none"> •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 .)
Подтвердить PIN-код пользователя	Введите подтверждение нового значения PIN-кода пользователя. (Поле активно, только если установлен флажок Установить PIN-код пользователя .)

Таблица 28

5. Нажмите **Выполнить** и подтвердите свой выбор в окне с предупреждающим сообщением.

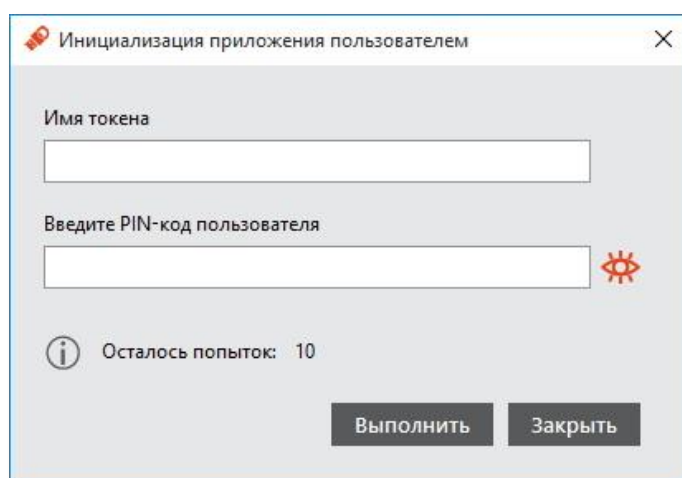
- При успешной инициализации отобразится соответствующее сообщение – нажмите **ОК**, чтобы закрыть его.

9.4. Приложение ГОСТ с апплетом Криптотокен 2

Чтобы подготовить электронный ключ к работе, выполните следующие действия:

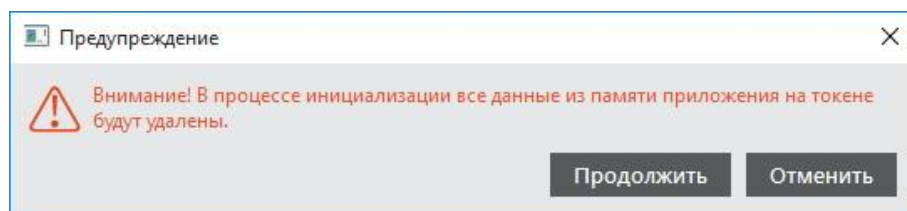
- Запустите Единый клиент JaCarta и переключитесь в режим администратора.
- Подсоедините нужный электронный ключ к компьютеру, выберите его в левой панели интерфейса Единого клиента JaCarta и в центральной части окна вкладку **ГОСТ**.
- Нажмите **Инициализировать пользователем....** Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 54 - Окно инициализации приложения пользователем



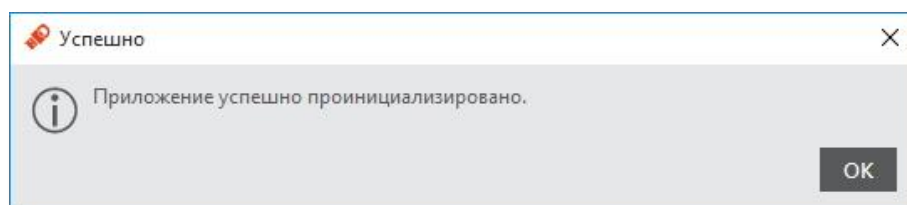
- Заполните поля **Имя токена** и **Введите PIN-код пользователя**, после чего нажмите **Выполнить**.
- В появившемся окне (см. Рис. **Ошибка! Источник ссылки не найден.**) нажмите **Продолжить**.

Рисунок 55 - Предупреждение об удалении всех данных с токена



- В появившемся окне (см. Рис. **Ошибка! Источник ссылки не найден.**) нажмите **ОК** для завершения.

Рисунок 56 - Сообщение об успешной инициализации



10. Установка (смена) PIN-кода пользователя администратором

Для некоторых приложений администратор может задать PIN-код пользователя, если он 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».



PIN-код пользователя имеет свой срок действия. За 7 дней до окончания срока действия PIN-кода пользователь получает уведомление о необходимости смены PIN-кода. Информационные сообщения будут приходить каждый день до окончания срока действия PIN-кода, пока он не будет изменен.



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.

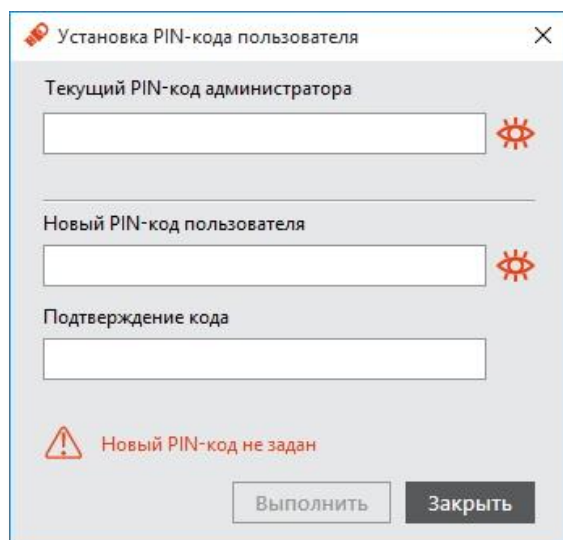


Заданное количество попыток ввода PIN-кода администратора, а также оставшееся количество попыток можно узнать, запустив Единый Клиент JaCarta перейдя на вкладку **Информация о токене** и кликнув ссылку [Подробная информация...](#).

Чтобы сменить PIN-код пользователя, выполните следующие действия:

1. Подсоедините электронный ключ. На нем 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 57 - Окно установки PIN-кода пользователя



Установка PIN-кода пользователя

Текущий PIN-код администратора

Новый PIN-код пользователя

Подтверждение кода

Новый PIN-код не задан

Выполнить Закрыть

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.

11. Смена PIN-кода подписи

Для выполнения операции смены PIN-кода подписи необходимо ввести PIN-код пользователя и текущий PIN-код подписи.

Сведения об операции смены PIN-кода подписи приведены в документе [Единый Клиент JaCarta. Руководство пользователя].

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

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

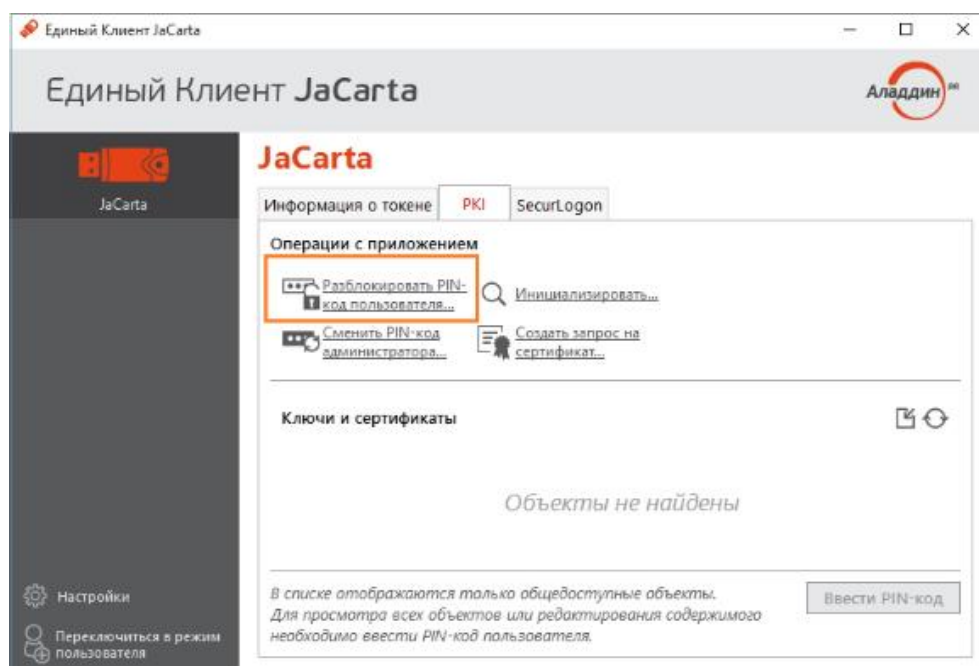
- PKI и PKI/BIO – после разблокировки администратор должен установить новый PIN-код пользователя.
- ГОСТ и STORAGE – разблокировка обнуляет счётчик неверных попыток доступа, значение PIN-кода пользователя остаётся прежним.

12.1. Приложения PKI и PKI/BIO

Чтобы разблокировать PIN-код пользователя, выполните следующие действия:

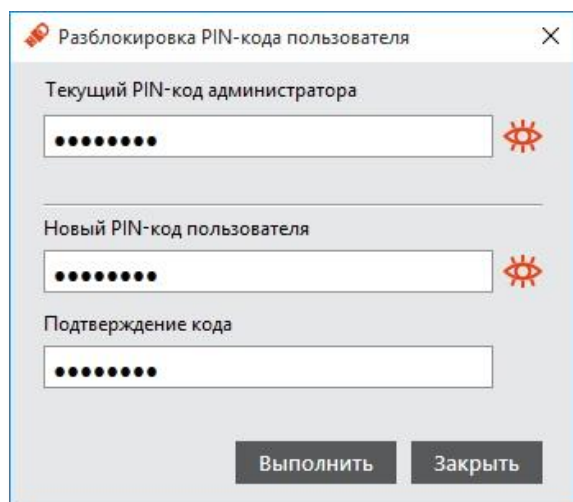
1. Подсоедините электронный ключ, на котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Запустите Единый Клиент JaCarta и перейдите в режим администратора.
3. В левой панели Единого Клиента JaCarta выберите нужный электронный ключ и в центральной части в зависимости от установленного 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 58 - Значок разблокировать PIN-код пользователя



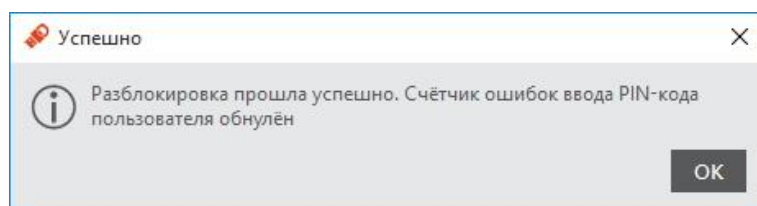
5. Нажмите **Разблокировать PIN-код пользователя**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 59 - Окно разблокировки PIN-кода пользователя



6. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора.
7. В полях **Новый PIN-код пользователя** и **Подтверждение PIN-кода** введите новые 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. **Ошибка! Источник ссылки не найден.**) – нажмите **ОК**, чтобы закрыть его.

Рисунок 60 - Информационное сообщение при успешной разблокировке PIN-кода пользователя



После произведенных действий электронный ключ можно передавать пользователю.

12.2. Приложение ГОСТ с апплетом Криптотокен и приложение STORAGE

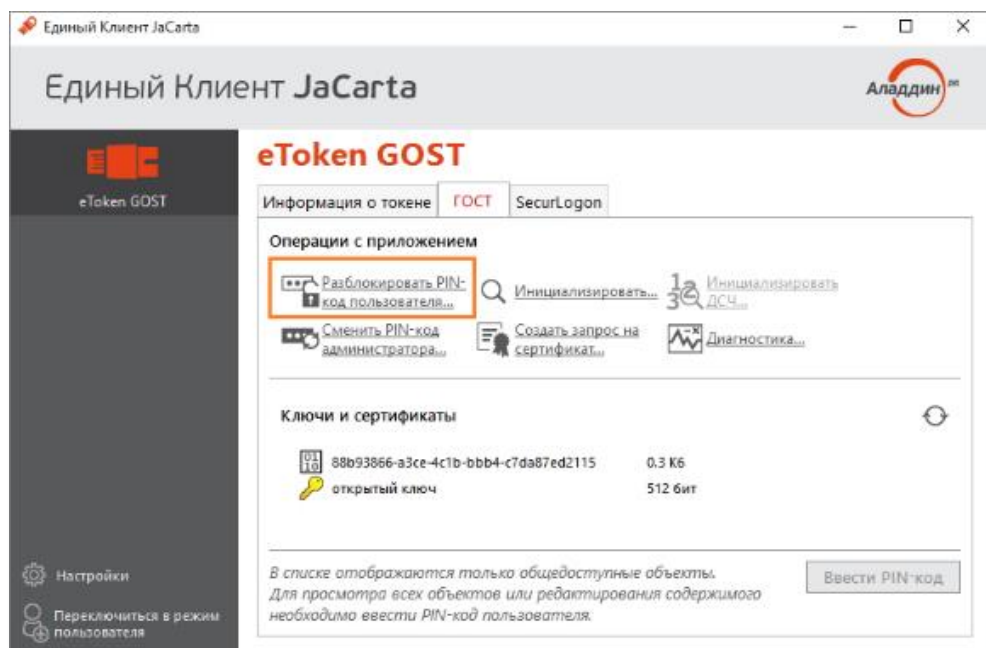
Чтобы разблокировать PIN-код пользователя, выполните следующие действия:

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. **Ошибка! Источник ссылки не найден.**).

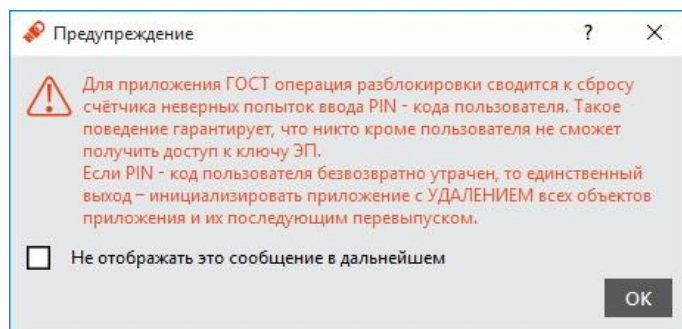
Значок разблокировки PIN-кода пользователя

Рисунок 61 - Значок разблокировки PIN-кода пользователя



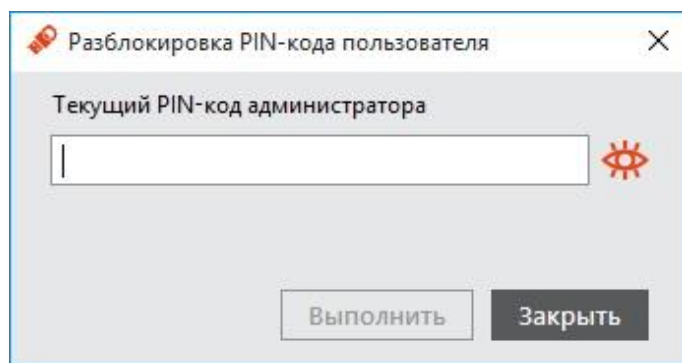
4. Нажмите **Разблокировать PIN-код пользователя**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 62 - Информационное окно с предупреждением



5. Нажмите **ОК**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 63 - Окно разблокировки PIN-кода пользователя



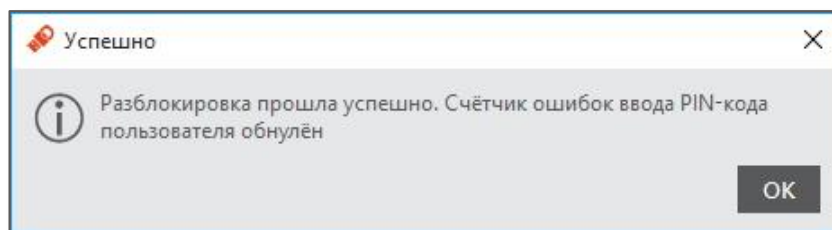
6. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора, после чего нажмите **Выполнить**.



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. В этом случае все данные с ключа будут удалены.

7. При успешной разблокировке PIN-кода пользователя отобразится соответствующее сообщение (см. Рис. **Ошибка! Источник ссылки не найден.**). Нажмите **ОК**, чтобы закрыть его.

Рисунок 64 - Информационное сообщение об успешной разблокировке



12.3. Приложение ГОСТ с апплетом Криптотокен 2



Примечание – Чтобы разблокировать PIN-код пользователя, электронный ключ с апплетом Криптотокен 2 должен быть проинициализирован с заданным PUK-кодом.

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**.



Если PIN-код пользователя заблокирован, название вкладки **ГОСТ** будет написано красными буквами, а в сегменте **Операции с приложением** значок **Разблокировать...** станет доступным для использования (см. Рис. **Ошибка! Источник ссылки не найден.**).

- Нажмите **Разблокировать...** Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 65 - Вкладка ГОСТ

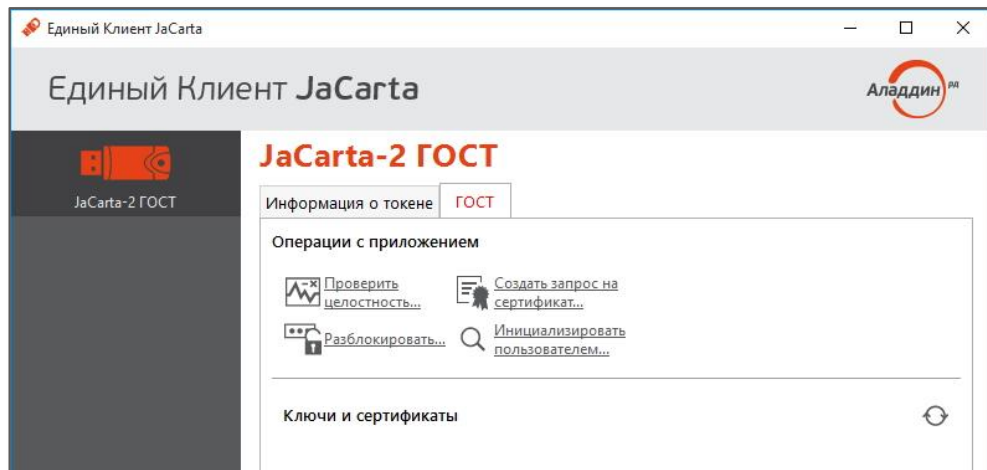
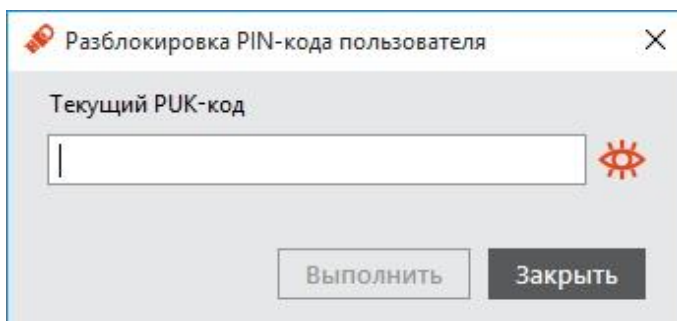
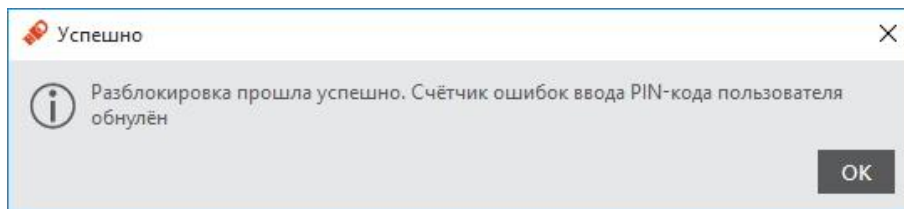


Рисунок 66 - Окно разблокировки PIN-кода пользователя



- В поле **Текущий PUK-код** введите текущий PUK-код, после чего нажмите **Выполнить**.
- При успешной разблокировке отобразится соответствующее сообщение (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 67 - Информационное сообщение об успешной разблокировке



- Нажмите **ОК** для завершения.

13. 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, а также с приложением ГОСТ на следующих электронных ключах: JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta-2 PRO/ГОСТ и JaCarta-2 PKI/BIO/ГОСТ (подробнее см. 1.3.1. Параметры электронных ключей при поставке).

Для возможности разблокировки электронного ключа в удалённом режиме:

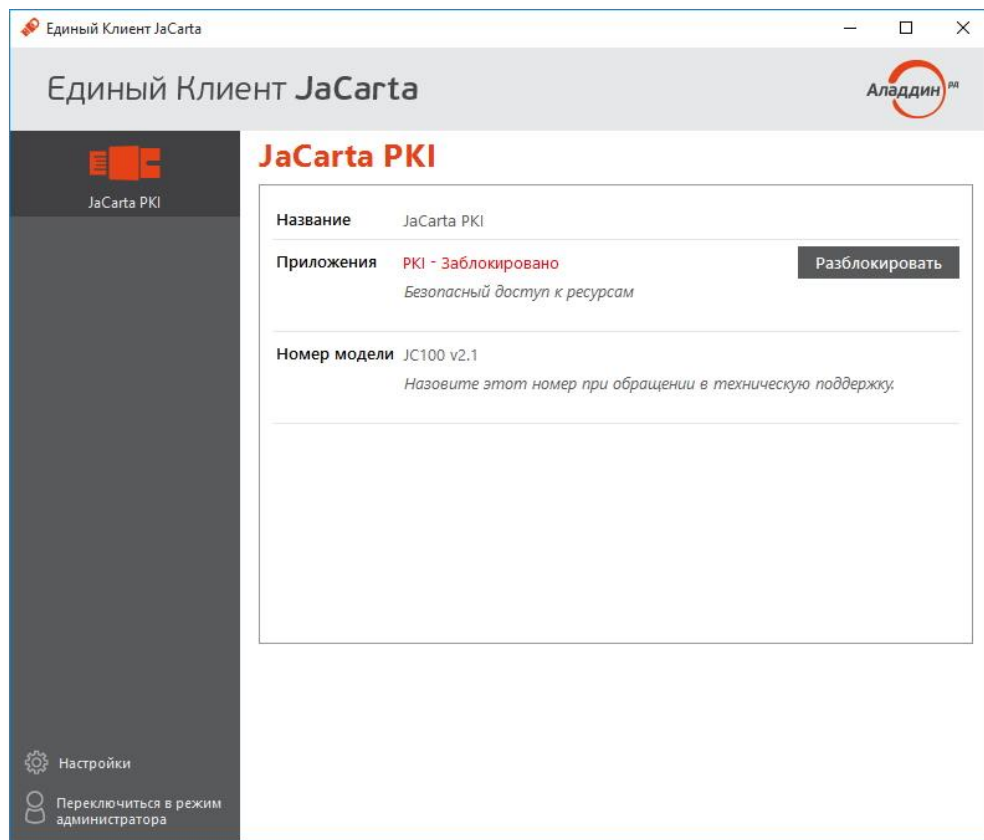
- необходимо, чтобы в организации была установлена система учёта и управления аппаратных средств аутентификации; в настоящем документе для примера будет использоваться система JaCarta Management System (подробнее см. документ [JaCarta Management System. Руководство администратора]);
- необходимо, чтобы 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 "9. 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.

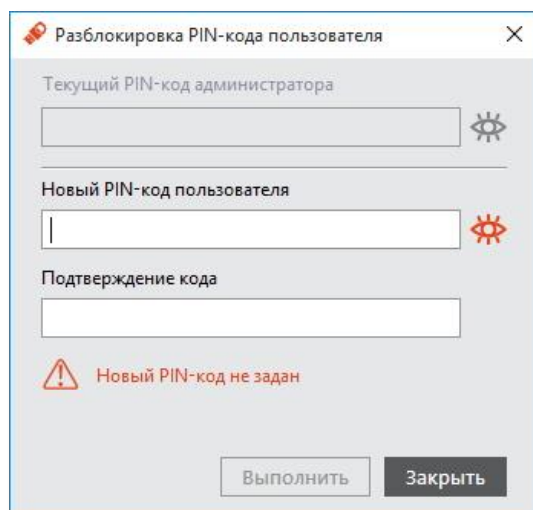
Окно Единого Клиента JaCarta на экране пользователя будет выглядеть следующим образом (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 68 - Окно с заблокированным PIN-кодом пользователя в режиме пользователя



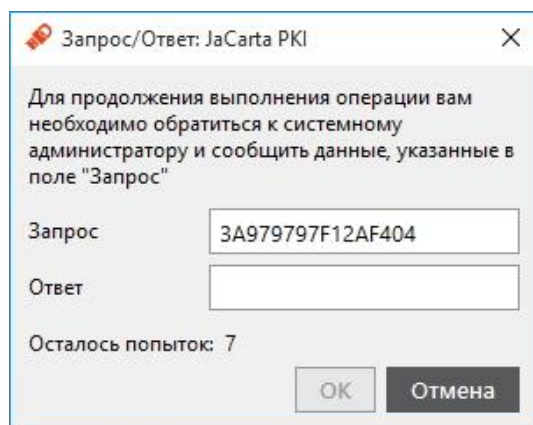
2. Пользователь должен нажать **Разблокировать**. На экране пользователя отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 69 - Окно задания нового PIN-кода пользователя



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. **Ошибка! Источник ссылки не найден.**).

Рисунок 70 - Окно запрос/ответ



Запрос/Ответ: JaCarta PKI

Для продолжения выполнения операции вам необходимо обратиться к системному администратору и сообщить данные, указанные в поле "Запрос"

Запрос: 3A979797F12AF404

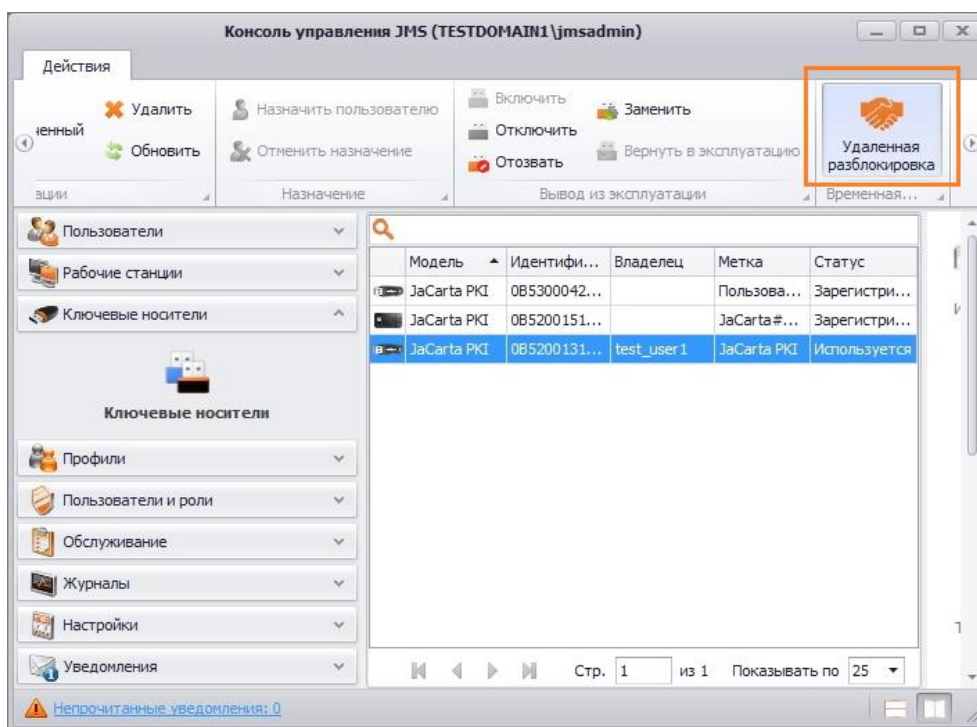
Ответ:

Осталось попыток: 7

OK Отмена

4. Пользователь должен продиктовать администратору отображающийся код запроса.
5. Администратор, используя интерфейс Консоли управления JMS должен открыть окно удалённой разблокировки (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 71 - Окно консоли управления JMS



Окно удалённой разблокировки будет выглядеть следующим образом (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 72 - Окно удаленной разблокировки

Удаленная разблокировка

Информация о ключевом носителе

Идентификатор: 0B52001314129243
Модель: JC100
Метка: JaCarta PKI
Владелец: test_user1
Статус: Используется

Запрос

Запрос:

[вставить из буфера](#)

Введите текст Запроса, полученного от пользователя.

[сгенерировать Ответ](#)

Генерация Ответа

Ответ: [скопировать в буфер](#)

Передайте пользователю строку с Ответом или скопируйте в буфер обмена для передачи средствами электронной почты.

ОК

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

Код ответа отобразится в соответствующем поле - **Ответ** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 73 - Окно удаленной разблокировки с кодом ответа

Удаленная разблокировка

Информация о ключевом носителе

Идентификатор: 0B52001314129243
Модель: JC100
Метка: JaCarta PKI
Владелец: test_user1
Статус: Используется

Запрос

Запрос: 3A979797F12AF404

[вставить из буфера](#)

Введите текст Запроса, полученного от пользователя.

[сгенерировать Ответ](#)

Генерация Ответа

Ответ: 9F48B3CD02D01C7C [скопировать в буфер](#)

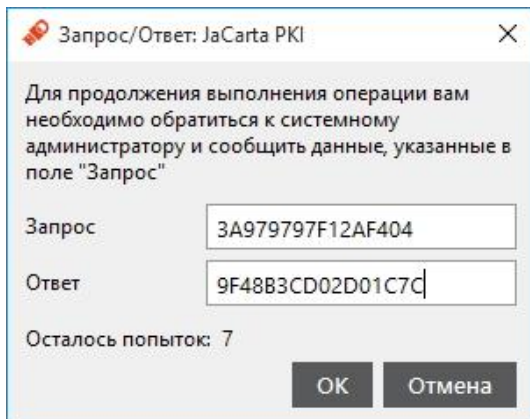
Передайте пользователю строку с Ответом или скопируйте в буфер обмена для передачи средствами электронной почты.

ОК

7. Администратор должен продиктовать пользователю код ответа.

8. Пользователь должен ввести код ответа в соответствующем поле (см. Рис. **Ошибка! Источник ссылки не найден.**) и подтвердить ввод нажатием кнопки **ОК**.

Рисунок 74 - Окно запрос/ответ с введенным кодом ответа



Запрос/Ответ: JaCarta PKI

Для продолжения выполнения операции вам необходимо обратиться к системному администратору и сообщить данные, указанные в поле "Запрос"

Запрос: 3A979797F12AF404

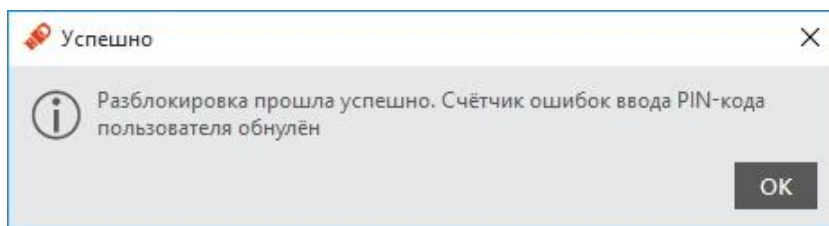
Ответ: 9F48B3CD02D01C7C

Осталось попыток: 7

ОК Отмена

Если код ответа был введен верно, на экране пользователя отобразится следующее сообщение (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 75 - Окно успешно выполненной разблокировки



Успешно

Разблокировка прошла успешно. Счётчик ошибок ввода PIN-кода пользователя обнулён

ОК

14. 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 Подробная 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. **Ошибка! Источник ссылки не найден.**).

Рисунок 76 - Окно смены PIN-кода администратора

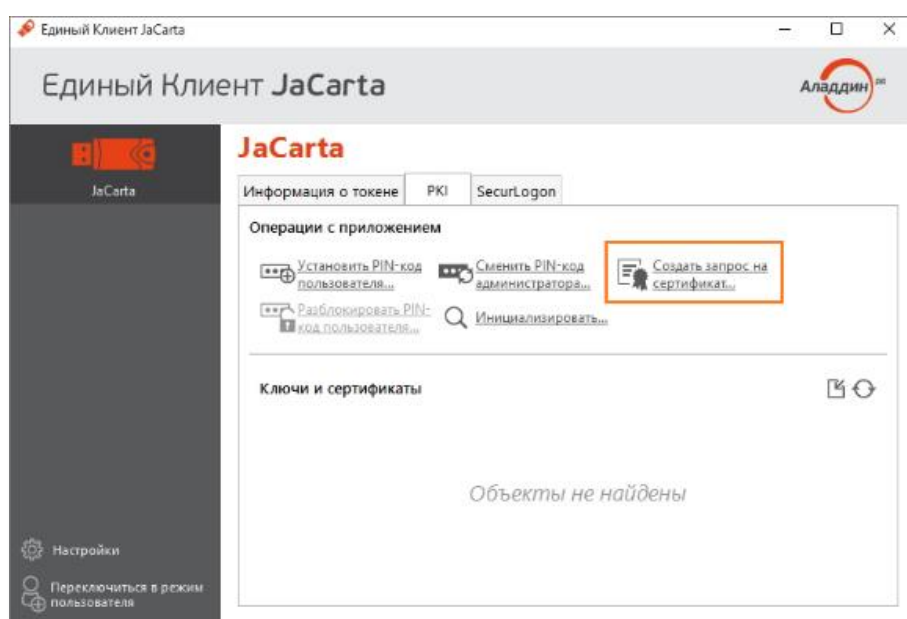
5. В поле **Текущий PIN-код администратора** введите текущий PIN-код администратора.
6. В полях **Новый PIN-код администратора** и **Подтверждение PIN-кода** введите новый PIN-код администратора и подтверждение соответственно.
7. Нажмите **Выполнить**.
8. При успешной смене PIN-кода отобразится соответствующее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

15. Создание запроса на сертификат

Чтобы создать запрос на сертификат, выполните следующие действия:

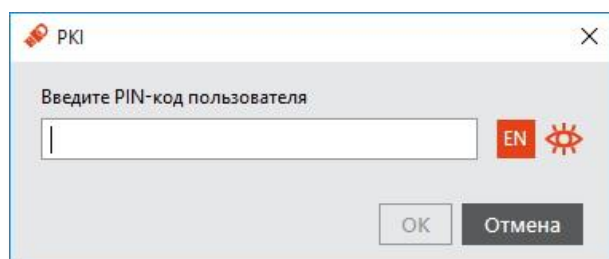
1. Подсоедините электронный ключ к компьютеру.
2. Запустите Единый Клиент JaCarta, в левой панели Единого Клиента JaCarta выберите нужный электронный ключ и перейдите в режим администратора.
3. В центральной части окна выберите вкладку, соответствующую приложению, для которого необходимо создать запрос на сертификат, отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 77 - Окно Единый Клиент JaCarta в режиме администратора на вкладке PKI



4. Нажмите **Создать запрос на сертификат....** Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 78 - Окно введите PIN-код пользователя



5. Введите PIN-код пользователя и нажмите **ОК**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

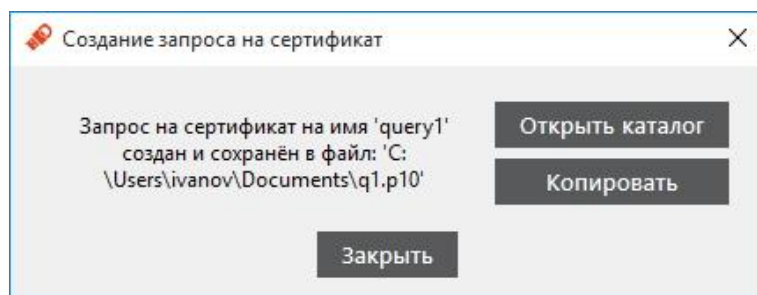
Рисунок 79 - Окно создания запроса на сертификат

6. Введите имя запроса, выберите необходимые опции в поле **Использование ключа**, после чего нажмите кнопку **Создать**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 80 - Окно сохранения запроса

7. Введите имя файла для сохранения запроса, выберите формат сохранения из раскрывающегося списка и нажмите **Сохранить**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 81 - Окно сообщения о созданном запросе на сертификат



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



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

16. 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.

В настоящем документе операции с объектами описаны на примере сертификатов в приложении PKI.

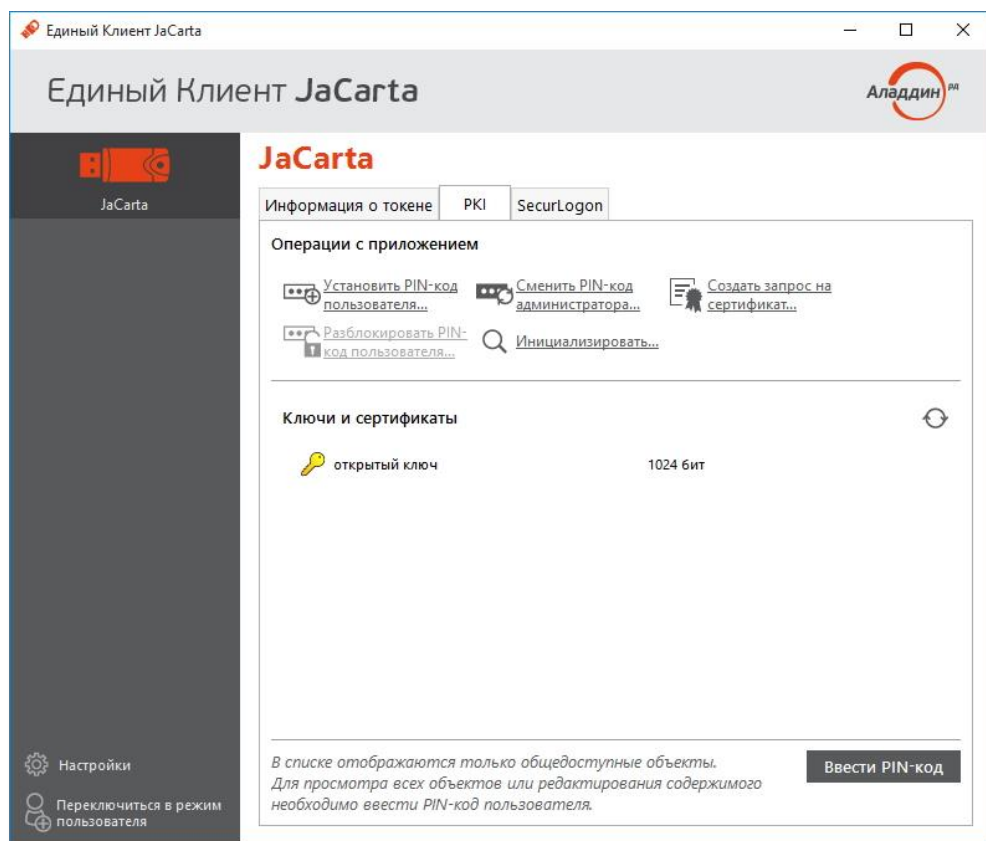
Сведения об операциях с объектами в памяти электронных ключей приведены так же в документе [Единый Клиент JaCarta. Руководство пользователя].

16.1. Отображение списка объектов

Чтобы просмотреть список объектов, выполните следующие действия:

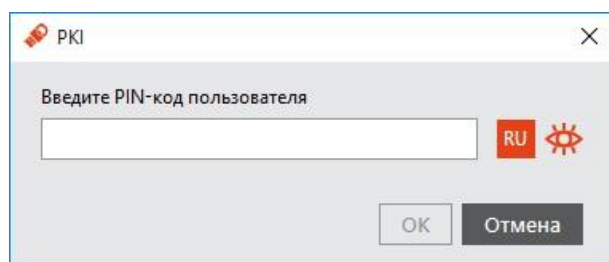
1. Подсоедините электронный ключ к компьютеру и запустите Единый Клиент JaCarta.
2. Если к компьютеру подсоединено несколько электронных ключей, в левой части интерфейса Единого Клиента JaCarta выберите нужный.
3. Если Единый Клиент JaCarta работает в режиме пользователя, переключитесь в режим администратора.
4. В центральной части окна выберите вкладку приложения, объекты которого вы хотите отобразить. В окне Единого Клиента JaCarta отобразится список общедоступных объектов в памяти электронного ключа (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 82 - Окно со списком общедоступных объектов в поле Ключи и сертификаты



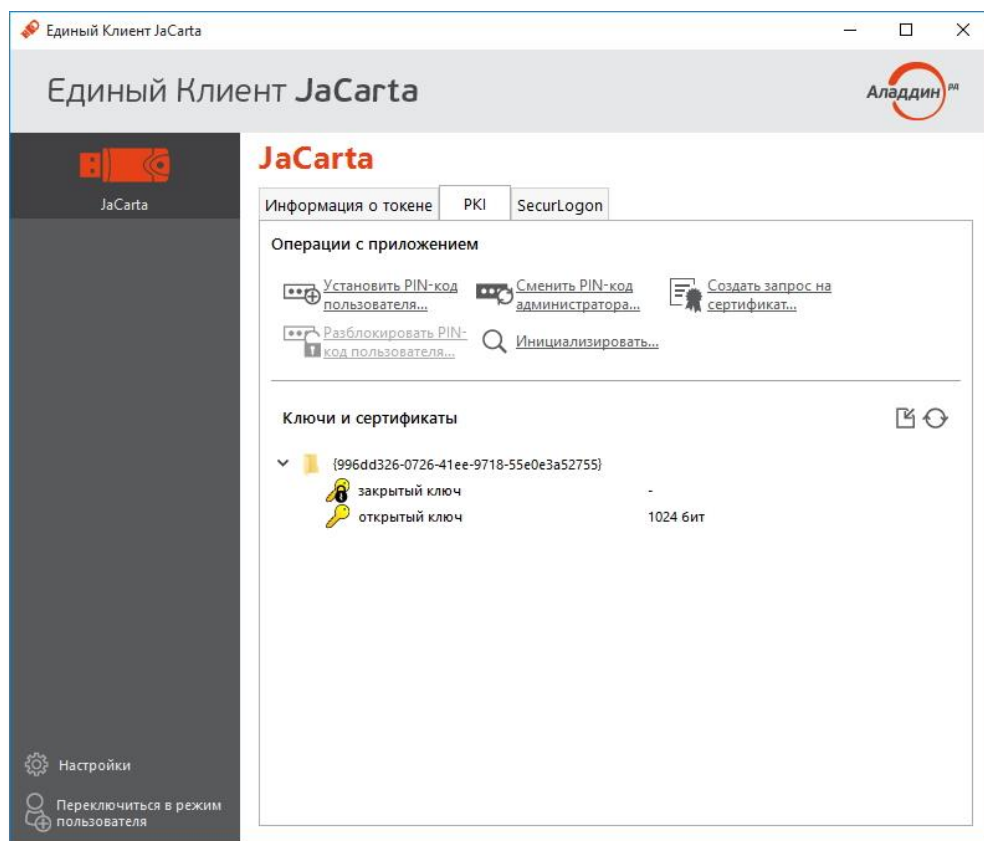
5. Чтобы отобразить полный список объектов в памяти электронного ключа, нажмите кнопку **Ввести PIN-код**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 83 - Окно ввода PIN-кода пользователя



6. Введите PIN-код пользователя в соответствующее поле, после чего нажмите **ОК**.
В окне Единый Клиент JaCarta отобразится полный список объектов выбранного приложения (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 84 - Окно с полным списком объектов



16.2. Импорт объектов

Чтобы импортировать объект в приложение, выполните следующие действия:


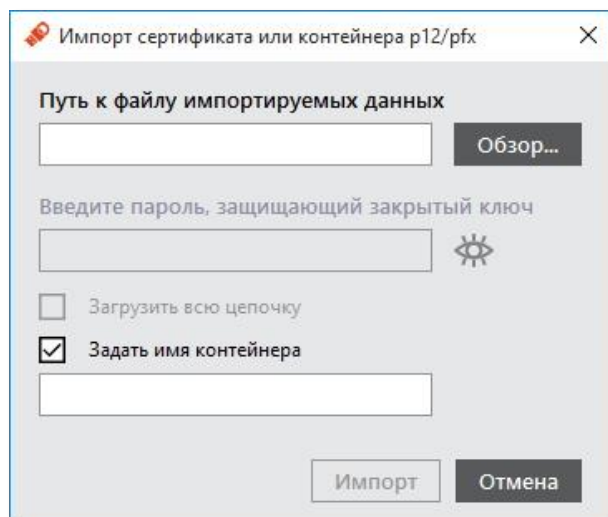
1. Выполните действия из подраздела "16.1. Отображение списка объектов".
2. Выполните одно из следующих действий:
 - нажмите правой кнопкой мыши в секции **Ключи и сертификаты** и в контекстном меню выберите **Импорт**;
 - нажмите на значке . Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 85 - Окно импорт сертификата



3. Выполните необходимые действия в соответствии с Таблицей 29.

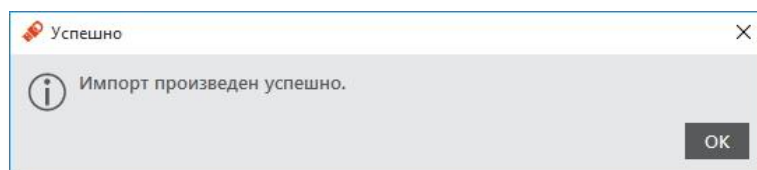
Таблица 29

Настройка	Описание
Путь к файлу импортируемых данных	Воспользуйтесь кнопкой Обзор... , чтобы указать путь к импортируемому сертификату.
Введите пароль, защищающий закрытый ключ	Поле становится активным, если импортируемый сертификат содержит защищённый паролем закрытый ключ.
Загрузить всю цепочку	Флажок становится активным, если импортируемый сертификат содержит цепочку сертификатов более высокого уровня. Установите этот флажок, если хотите загрузить всю цепочку сертификатов.
Задать имя контейнера	Установите флажок, если хотите вручную задать имя контейнера, в который будет импортирован сертификат. В противном случае имя контейнера будет сгенерировано автоматически.

Таблица 29

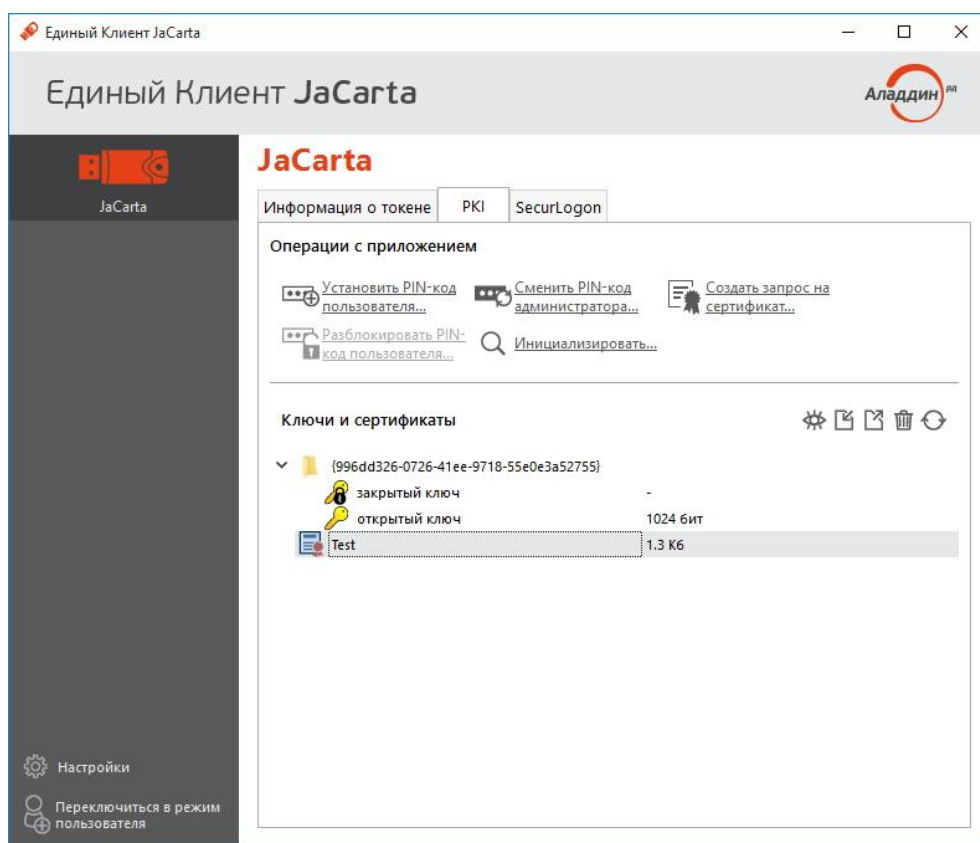
4. Нажмите **Импорт**. При успешном завершении операции отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 86 - Информационное сообщение об успешном импорте сертификата




5. Нажмите **ОК**.
Импортированные объекты отобразятся в секции **Ключи и сертификаты** (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 87 - Окно с отображением импортированных объектов



16.3. Экспорт объектов

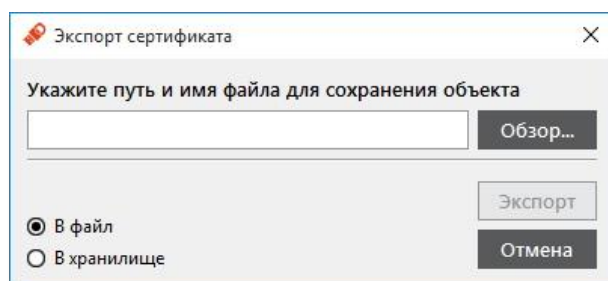
Чтобы экспортировать объект из приложения, выполните следующие действия:

1. Выполните действия из подраздела "16.1. Отображение списка объектов".
2. Выполните одно из следующих действий:
 - нажмите правой кнопкой мыши на объекте, который вы хотите экспортировать и выберите **Экспорт**;
 - выберите объект для экспорта, после чего нажмите на значке .

Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Окно экспорт сертификата

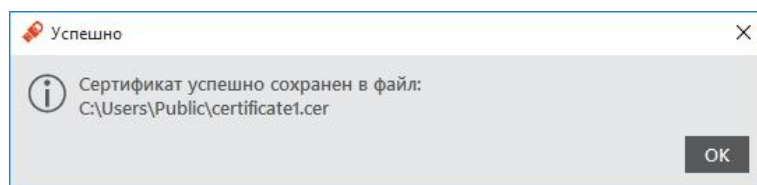
Рисунок 88 - Окно экспорт сертификата



3. Выберите, куда вы хотите экспортировать сертификат:
 - **В файл** – в этом случае воспользуйтесь кнопкой **Обзор**, чтобы указать путь сохранения экспортируемого сертификата;
 - **В хранилище** – сертификат будет экспортирован в личное хранилище сертификатов на компьютере (переходите к следующему шагу процедуры).

4. Нажмите **Экспорт**. В случае успешного завершения операции отобразится соответствующее сообщение (см. Рис. **Ошибка! Источник ссылки не найден.**).


Рисунок 89 – Информационное сообщение об успешном экспорте сертификата



5. Нажмите **ОК** для завершения процедуры.

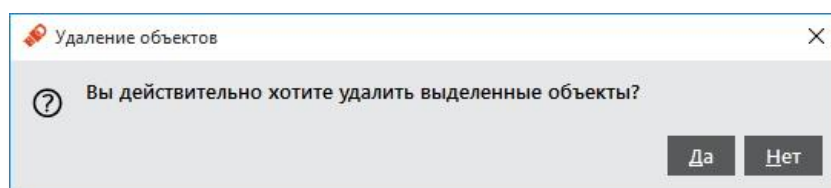
16.4. Удаление объектов

Чтобы удалить объект, выполните следующие действия:

1. Выполните действия из подраздела "16.1. Отображение списка объектов".
2. Выполните одно из следующих действий:
 - Нажмите правой кнопкой мыши на объекте, который хотите удалить, и выберите **Удалить**;
 - Выберите объект, который хотите удалить, после чего нажмите на значке .

Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).
Окно удаления объектов


Рисунок 90 - Окно удаления объектов



3. Нажмите **Да** для подтверждения.

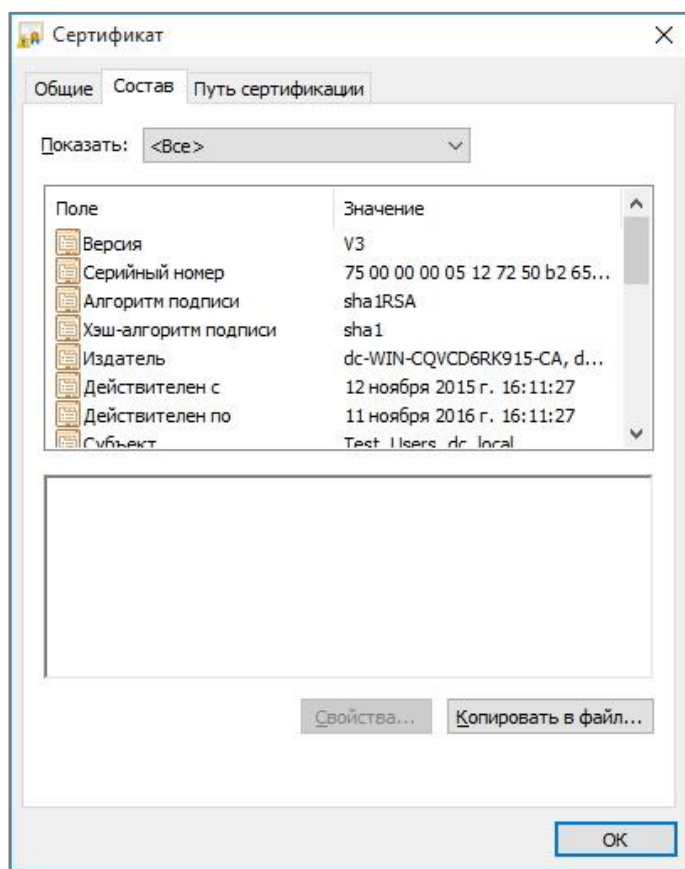
16.5. Отображение информации об объекте

Чтобы просмотреть информацию об объекте, выполните следующие действия:

1. Выполните действия из подраздела "16.1. Отображение списка объектов".
2. Выполните одно из следующих действий:
 - нажмите правой кнопкой мыши на объекте, информацию о котором хотите просмотреть, и выберите **Просмотр**;
 - выберите объект, информацию о котором хотите просмотреть, после чего нажмите на значке .

Отобразится окно, содержащее сведения об объекте (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 91 - Окно свойств сертификата

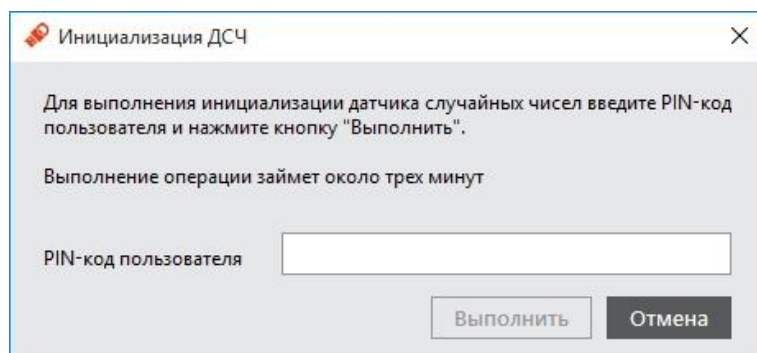


16.6. Повторная инициализация датчика случайных чисел (приложение ГОСТ)

Данную процедуру рекомендуется производить не реже, чем раз в три года (36 месяцев). Чтобы повторно инициализировать датчик случайных чисел, выполните следующие действия:

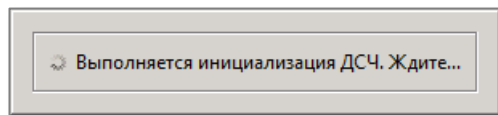
1. Подсоедините электронный ключ к компьютеру, запустите Единый Клиент JaCarta и перейдите в режим администратора.
2. Выберите вкладку **ГОСТ**.
3. Нажмите **Инициализировать ДСЧ**. Отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 92 - Окно ввода PIN-кода пользователя



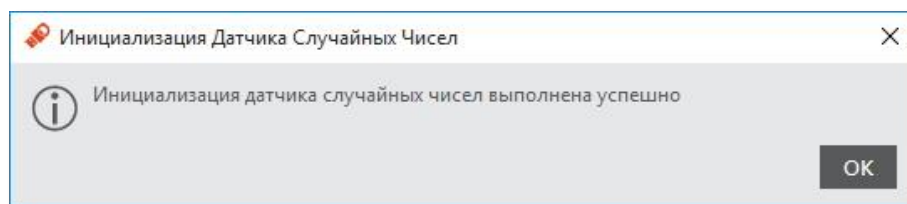
4. Введите PIN-код пользователя и нажмите **Выполнить**. Процесс займёт некоторое время (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 93 - Процесс инициализации датчика случайных чисел



При успешном завершении отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 94 - Сообщение об успешной инициализации датчика случайных чисел



5. Нажмите **ОК**, чтобы завершить процедуру.

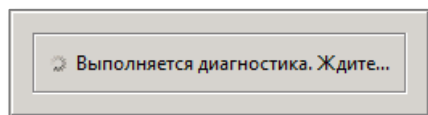
16.7. Диагностика электронного ключа (приложение ГОСТ)

Диагностика выполняется в случае выявления каких-либо неисправностей в работе приложения (ГОСТ).

Для диагностики приложения выполните следующие действия:

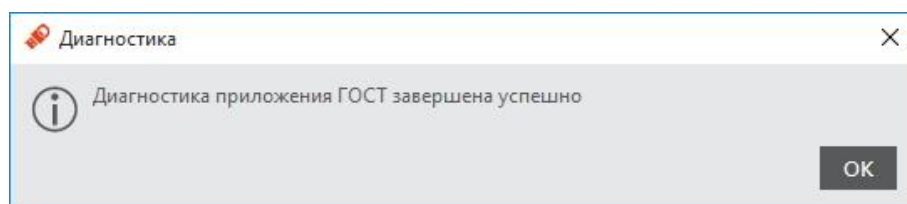
1. Подсоедините электронный ключ к компьютеру, запустите Единый Клиент JaCarta и переключитесь в режим администратора.
2. Перейдите на вкладку **ГОСТ**.
3. Нажмите **Диагностика**. Процесс займёт некоторое время (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 95 - Процесс выполнения диагностики



При успешном завершении отобразится следующее окно (см. Рис. **Ошибка! Источник ссылки не найден.**).

Рисунок 96 - Сообщение об успешном завершении диагностики



4. Нажмите **ОК** для завершения процедуры.

17. Операции, производимые с помощью утилиты JaCarta АРМ УЦ

С помощью утилиты АРМ УЦ возможно осуществлять следующие действия:

- Генерировать ключевые пары с использованием встроенных криптографических возможностей электронных ключей JaCarta ГОСТ и eToken ГОСТ;
- Формировать запросы к удостоверяющему центру на получение сертификата открытого ключа;
- Производить запись полученных сертификатов в память электронных ключей JaCarta ГОСТ и eToken ГОСТ.

Подробные сведения об операциях, производимых с помощью утилиты АРМ УЦ приведены в документе [АРМ УЦ. Руководство администратора].

18. Синхронизация паролей электронного ключа и учетной записи домена Windows



Единый Клиент JaCarta позволяет проводить синхронизацию PIN-кода электронного ключа с паролем учетной записи пользователя, который запрашивается при входе в домен Windows. Пароль учетной записи пользователя (пароль домена) синхронизируется с PIN-кодом электронного ключа и, при последующих изменениях PIN-кода электронного ключа, пароль учетной записи пользователя (доменный пароль) вводить не требуется.

В случае рассинхронизации паролей или смены администратором AD пароля учетной записи пользователя (доменного пароля) необходимо произвести повторную синхронизацию паролей.



В случаях, когда пароль не соответствует требованиям к качеству одной из политик синхронизация невозможна.



Синхронизация PIN-кода электронного ключа с паролем учетной записи пользователя возможна только для приложений PKI (в том числе с апплетом PRO) и PKI/BIO.

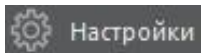
Для того, чтобы синхронизировать PIN-код пользователя и пароль учетной записи домена Windows необходимо выполнить следующие действия:

1. Зайдите в редактор реестра с правами администратора.
2. В разделе HKEY_LOCAL_MACHINE/SOFTWARE/AladdinRD/JCUC/SyncPin создайте строковый параметр с именем Domain и задайте ему значение имени домена.



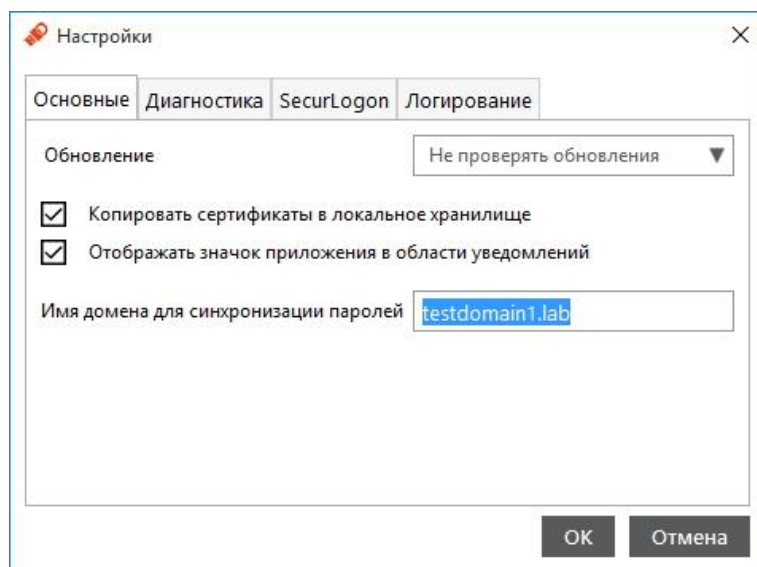
Если раздела **SyncPin** нет, то необходимо создать по указанному адресу раздел с указанным именем.

3. В левом нижнем углу основного окна Единого Клиента JaCarta нажмите **Настройки** -



На вкладке **Основные** в поле **Имя домена для синхронизации паролей** (см.Рисунок 97) должно отображаться введенное ранее в редакторе реестра (см. п.2) имя домена. Нажмите **ОК**.

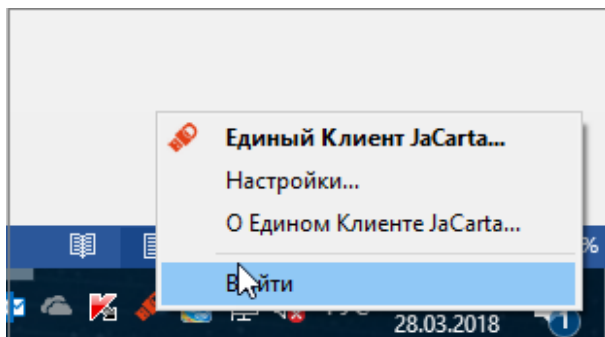
Рисунок 97 - Окно Настройки. Вкладка Основные



4. Закройте окно Единый Клиент JaCarta.

5. На панели задач в области уведомлений нажмите на стрелку, открывающую панель запущенных программ (см.Рисунок 98).

Рисунок 98 - Выход из Единый Клиент JaCarta




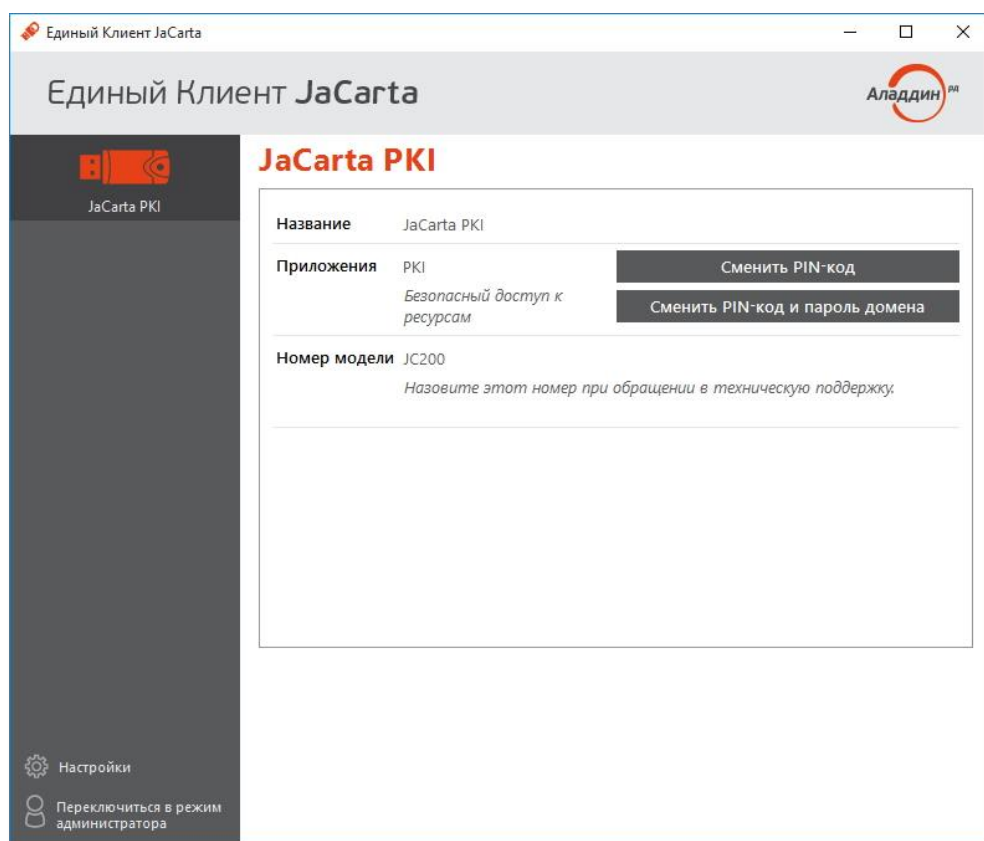
6. Нажмите правой кнопкой мыши на значке  и в появившемся контекстном меню (см.Рисунок 98) выберите **Выйти**.
7. Нажмите последовательно **ПУСК, Все приложения, Аладдин Р.Д., Единый Клиент JaCarta**. В окне Единый Клиент JaCarta в режиме пользователя будет доступна кнопка **Сменить PIN-код и пароль домена** (см. Рисунок 99).

Рисунок 99 - Окно Единого Клиента JaCarta в режиме пользователя




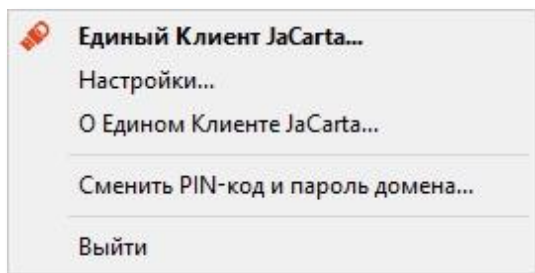
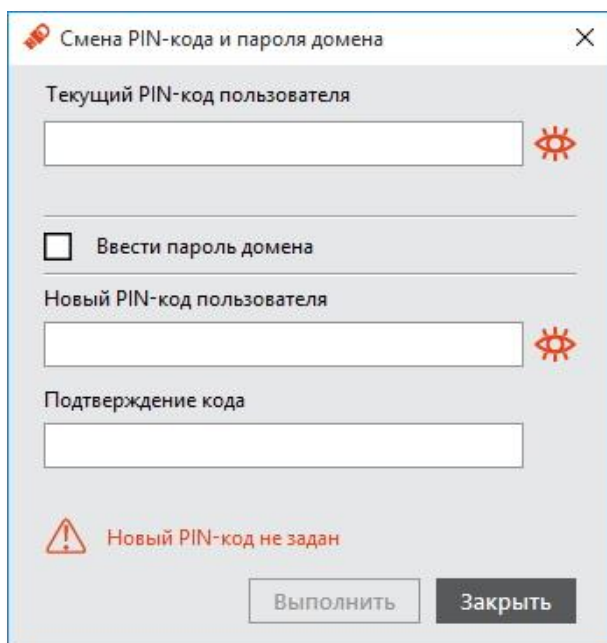
Примечание – Опция **Сменить PIN-код и пароль домена** появится и в **Меню быстрого запуска** (см. Рисунок 100), которое можно запустить на панели задач в области уведомлений нажав правой кнопкой мыши на значок .

Рисунок 100 - Меню быстрого запуска



8. Нажмите кнопку **Сменить PIN-код и пароль домена**. Появится окно (см.Рисунок 101).

Рисунок 101 - Окно смены PIN-кода и пароля домена

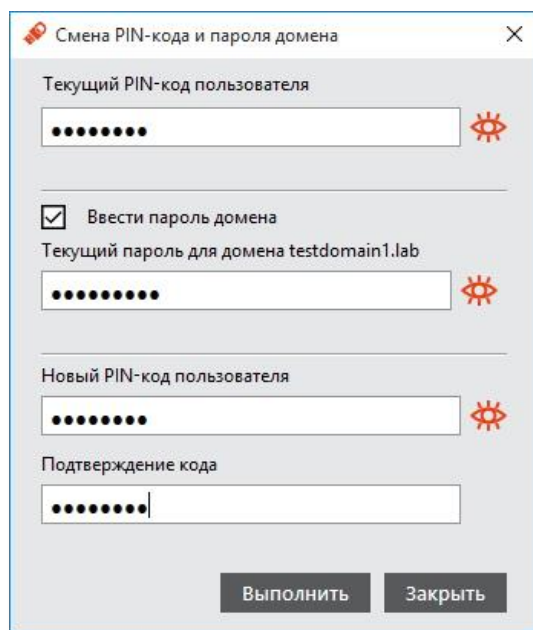


9. Введите текущий PIN-код пользователя, после чего введите новый PIN-код пользователя и повторно подтвердите его.
10. При выборе опции **Ввести пароль домена** в диалоговом окне добавится поле для ввода пароля домена (см.Рисунок 102).



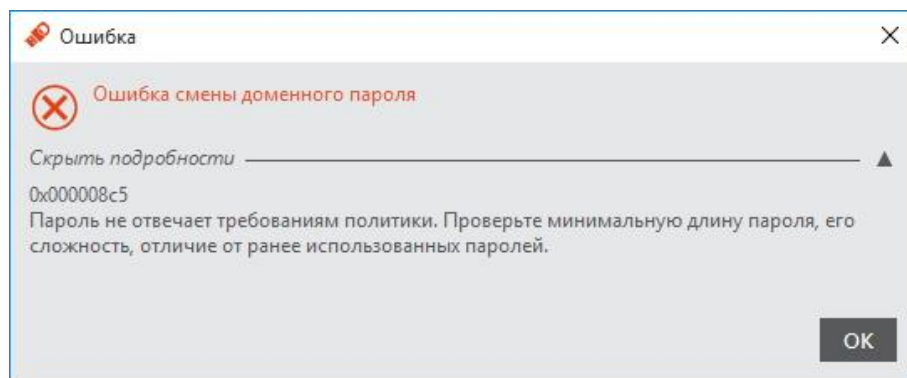
Пароль домена следует вводить только при первой синхронизации или в случае рассинхронизации. При смене только одного PIN-кода пользователя пароль домена вводить не обязательно.

Рисунок 102 - Окно смены PIN-кода и пароля домена



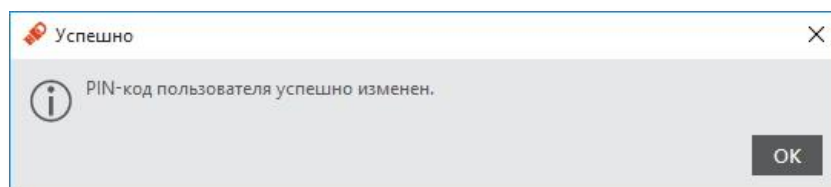
11. Введите текущий пароль домена, после чего введите новый PIN-код пользователя и повторно подтвердите его.
12. Нажмите **Выполнить**.
В случае, если введенный пароль пользователя не отвечает требованиям к качеству пароля, появится окно (см.Рисунок 103).

Рисунок 103 - Окно сообщения об ошибке смены пароля



При успешной смене появится окно (см. Рисунок 104).

Рисунок 104 - Окно сообщения об успешной смене пароля



19. 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 Аладдин Р.Д.

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

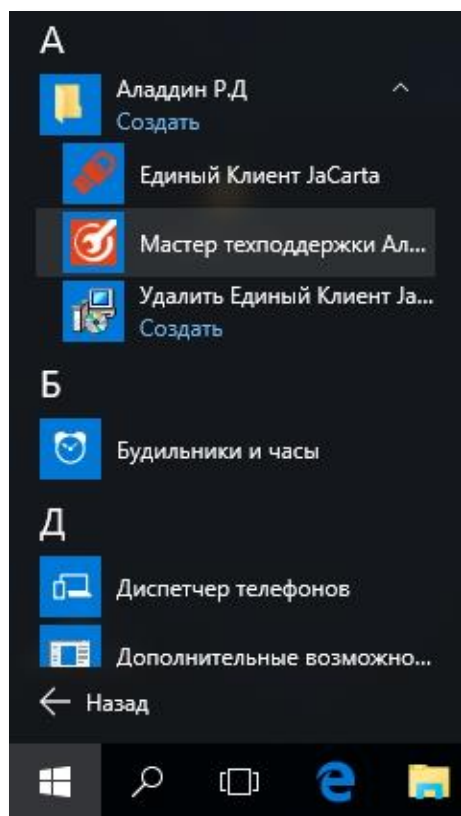


Внимание! Подробнее о настройках логирования см. раздел "8. Настройка работы Единый Клиент JaCarta" в описании вкладки Логирование (см. Рис. **Ошибка! Источник ссылки не найден.** и табл. 17).

Чтобы запустить Мастер техподдержки выполните следующие действия:

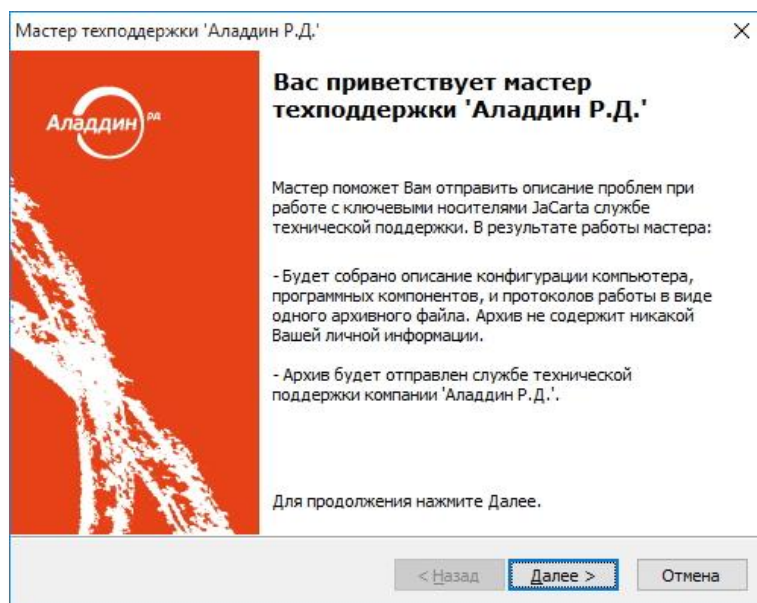
1. Выберите последовательно **Пуск, Все программы, Аладдин Р.Д., Мастер техподдержки Аладдин Р.Д.** (см. Рисунок 105).

Рисунок 105 - Запуск Мастера техподдержки



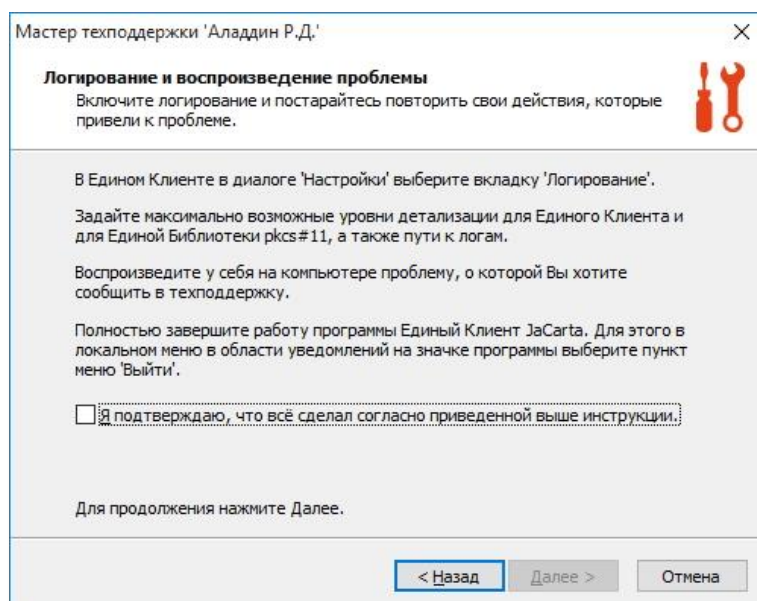
2. В появившемся окне (см. Рисунок 106) нажмите **Далее>**.

Рисунок 106 - Окно приветствия Мастера техподдержки



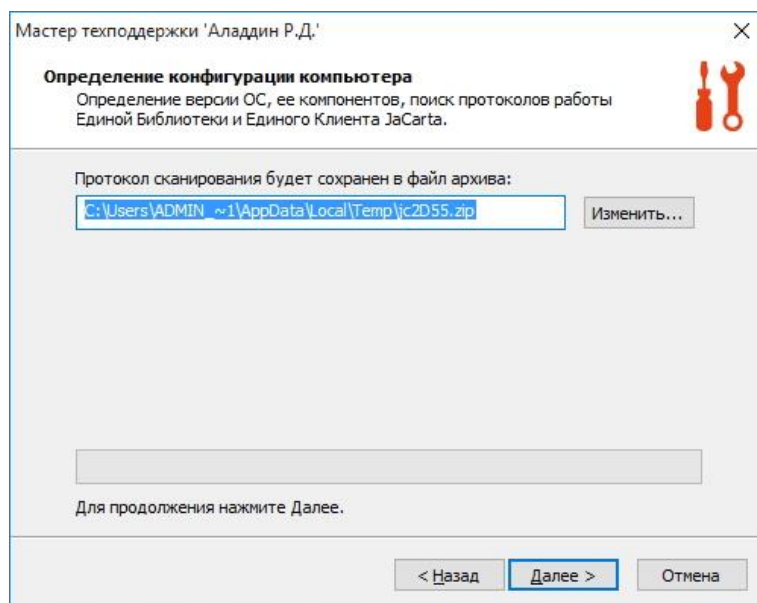
3. В появившемся окне (см. Рисунок 107) прочитайте и выполните все перечисленные в этом окне действия, затем выберите опцию **Я подтверждаю, что все сделал согласно приведенной выше инструкции**, после чего нажмите **Далее>**.

Рисунок 107 - Окно Мастера техподдержки. Логирование и воспроизведение проблем



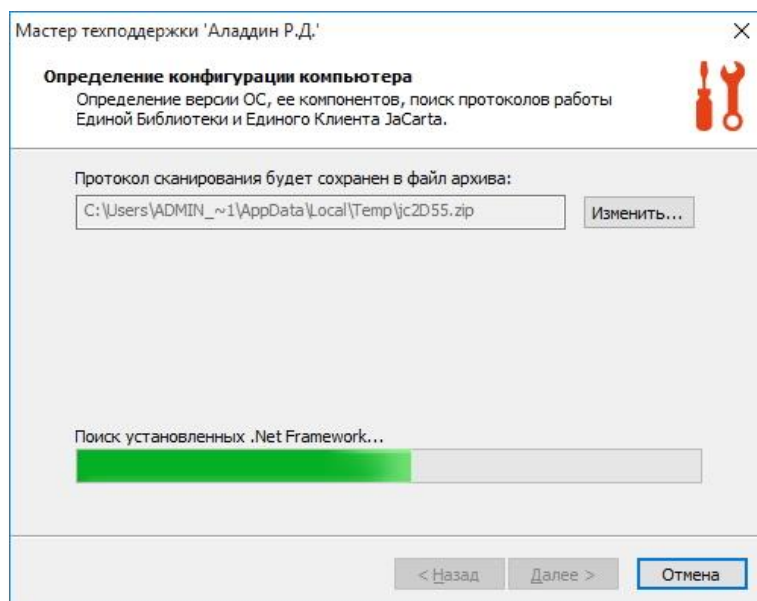
4. В появившемся окне (см. Рисунок 108) если вы хотите изменить место сохранения файла с диагностической информацией – нажмите кнопку **Изменить...**, укажите место сохранения, после чего нажмите **Сохранить**. Если вы не хотите изменять место сохранения файла с диагностической информацией, то оставьте место сохранения, указанное по умолчанию.
5. Нажмите **Далее>**.

Рисунок 108 - Мастер техподдержки. Выбор директории для сохранения файла



Мастер техподдержки начнет процесс сбора диагностической информации (см. Рисунок 109). Дождитесь окончания.

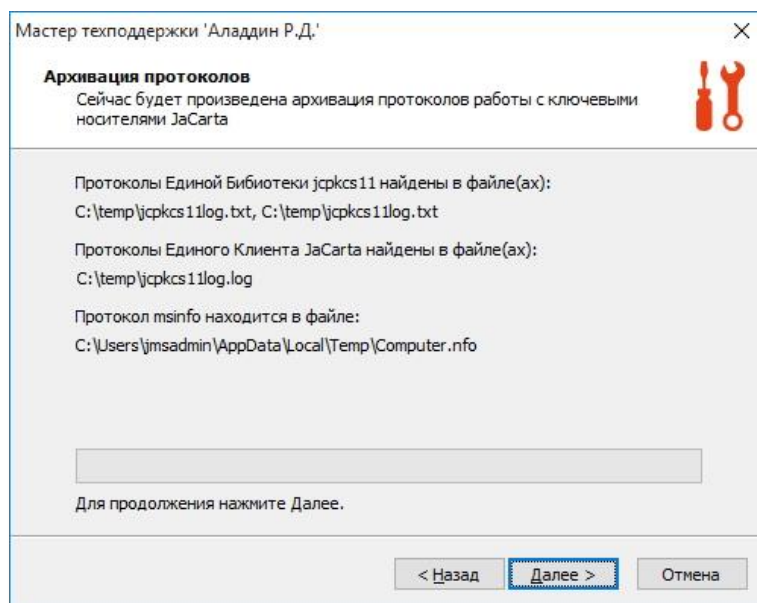
Рисунок 109 - Мастер техподдержки. Процесс сбора диагностической информации



В появившемся окне (см. Рисунок 110) будут указаны созданные файлы логирования.

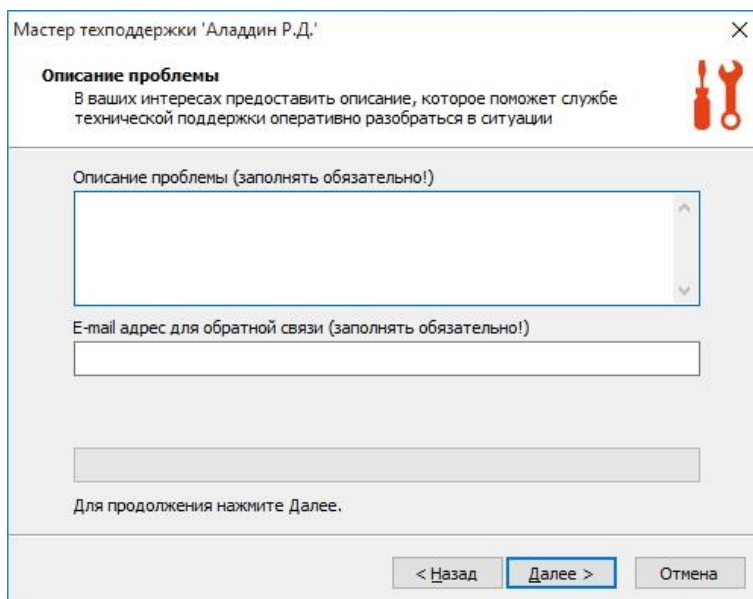
6. Нажмите **Далее>**.

Рисунок 110 - Мастер техподдержки. Перечень созданных файлов



7. В появившемся окне (см. Рисунок 111) заполните поле **Описание проблемы**, а в поле **E-mail адрес для обратной связи** укажите свой адрес электронной почты, после чего нажмите **Далее>**.

Рисунок 111 - Мастер техподдержки. Заполнение обязательных полей



8. В появившемся окне (см. Рисунок 112) выберите способ отправки результатов сбора диагностической информации в службу технической поддержки компании Аладдин Р.Д., после чего нажмите **Далее>**.

Рисунок 112 - Мастер техподдержки. Выбор способа отправки

Мастер техподдержки 'Аладдин Р.Д.'

Выбор способа отправки
Укажите способ отправки результатов в службу технической поддержки компании 'Аладдин Р.Д.'.

Размер файла архива: 1.4 KB

☐ HTTP - отправка любых объемов данных

☒ SMTP - отправка небольших объемов данных

☐ Не отправлять, сохранить файлы на диск

Сохранить...

Для продолжения нажмите Далее.

< Назад Далее > Отмена

Если был выбран способ **Не отправлять, сохранить файлы на диск** (см. Рисунок 113), то станет доступной кнопка **Сохранить...**, после нажатия на которую отобразится следующее окно (см. Рисунок 114 Рисунок 113 - Мастер техподдержки. Выбор сохранения на диск

Мастер техподдержки 'Аладдин Р.Д.'

Выбор способа отправки
Укажите способ отправки результатов в службу технической поддержки компании 'Аладдин Р.Д.'.

Размер файла архива: 1.4 KB

☐ HTTP - отправка любых объемов данных

☐ SMTP - отправка небольших объемов данных

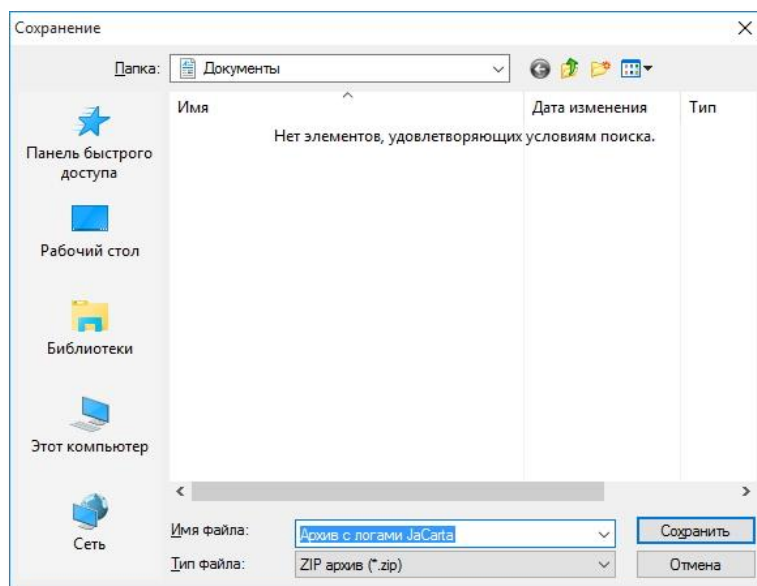
☒ Не отправлять, сохранить файлы на диск

Сохранить...

Для продолжения нажмите Далее.

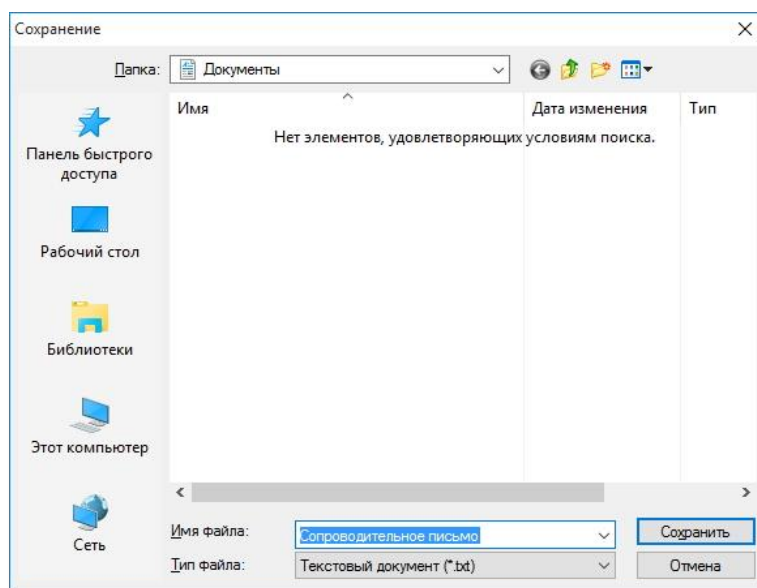
< Назад Далее > Отмена

Рисунок 114 - Сохранение архива с логами JaCarta



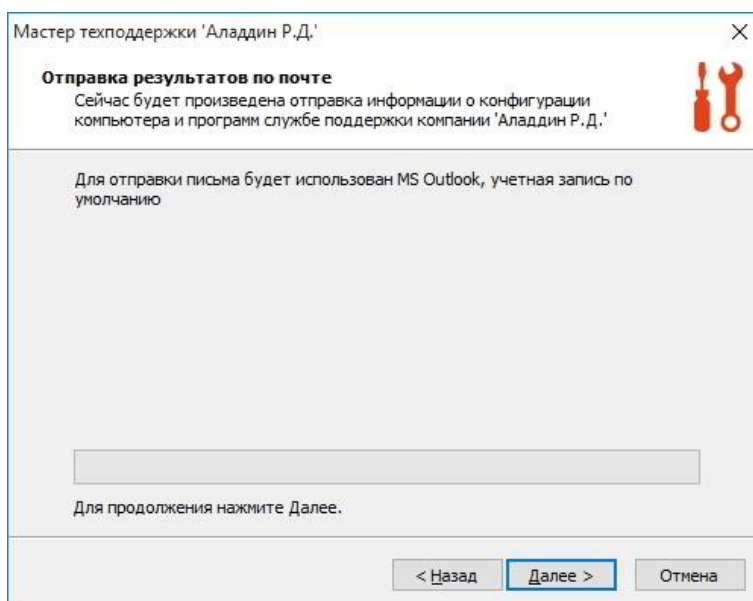
- 8.1.1. Укажите место сохранения файла с логами JaCarta и нажмите кнопку **Сохранить** (см. Рисунок 114).
- 8.1.2. Эту же процедуру выполните для сохранения файла Сопроводительного письма (см. Рисунок 115).

Рисунок 115 - Сохранение сопроводительного письма



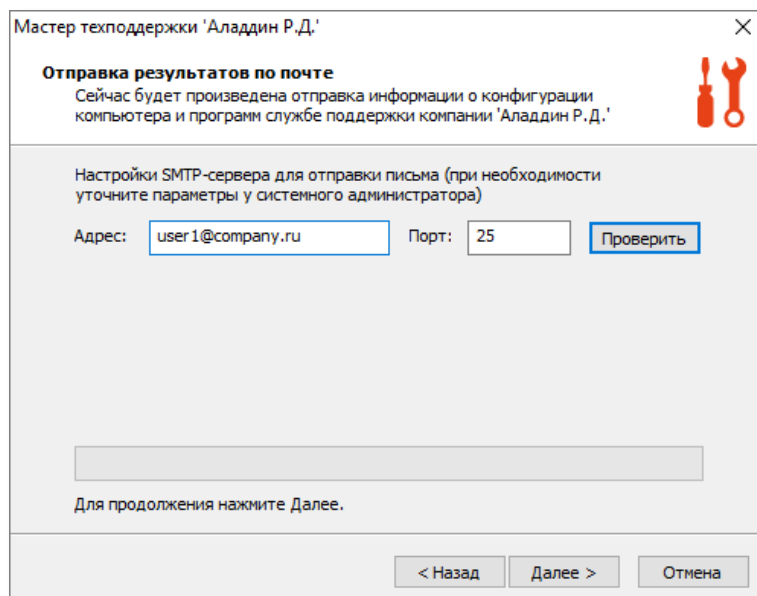
- 8.2. Если был выбран способ отправки: **SMTP – отправка небольших объемов данных**, то после нажатия кнопки **Далее>** (при условии, что на компьютере установлена и настроена программа MS Outlook) отобразится следующее окно (см. Рисунок 116).

Рисунок 116 - Мастер техподдержки. Отправка результатов по электронной почте MS Outlook



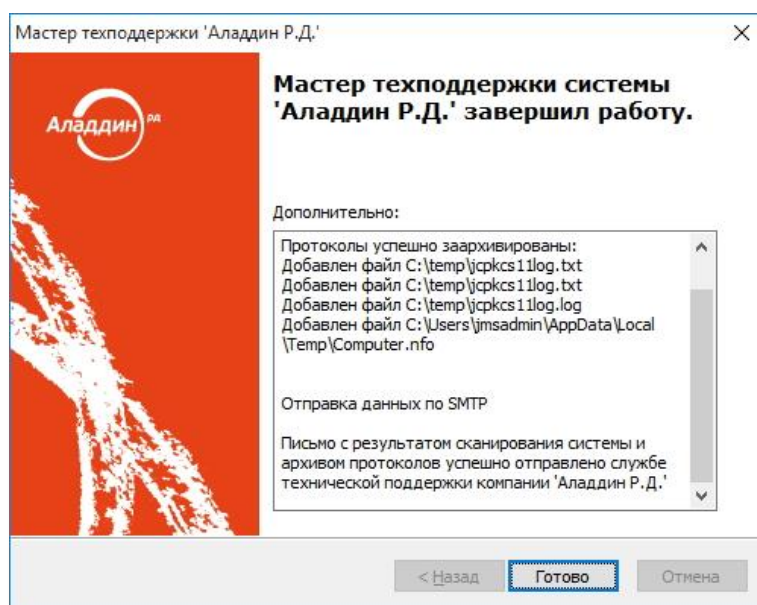
Если на компьютере не установлен почтовый клиент MS Outlook, необходимо заполнить поля **Адрес** и **Порт** данными (см. Рисунок 117). Убедиться в их корректности можно с помощью кнопки **Проверить**.

Рисунок 117 - Мастер техподдержки. Отправка результатов по электронной почте



- 8.2.1. Нажмите **Далее>**
Письмо-запрос технической поддержки с Вашими диагностическими данными будет отправлено по адресу support.jc@aladdin-rd.ru.
- 8.2.2. В появившемся окне (см. Рисунок 118) нажмите **Готово**.

Рисунок 118 - Мастер техподдержки. Завершение работы



Сокращения и аббревиатуры

APM	Автоматизированное рабочее место
ГОСТ	Государственный стандарт
УЦ	Удостоверяющий центр
AD CS	(Active Directory Certificate Services) службы сертификации
AD DS	(Active Directory Domain Services) доменные службы
JMS	JaCarta Management System
ОТР	(One Time Password) одноразовый пароль
PIN	(Personal Identification Number) личный опознавательный номер
PKI	(Public Key Infrastructure) инфраструктура открытых ключей
PUK	(Personal Unblocking Key) персональный код разблокировки
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.

Техническая поддержка

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

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

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

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

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

Выходные дни: суббота и воскресенье.

Телефон: (495) 223-0001 (многоканальный)

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

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

Регистрация изменений

Версия	Изменения
1.3	Добавлены комбинированные модели JaCarta-2, актуализированы разделы и скриншоты, связанные с этим добавлением, исправлены неточности и ошибки
1.2	Актуализирован раздел Мастер техподдержки и скриншоты других разделов
1.1	Добавлен раздел 6 и описание операций с объектами, актуализированы скриншоты
1.0	Создание документа

Предметный указатель

Р

PIN, 117
PIN-код администратора, 5
PIN-код пользователя, 5
PKI, 117

У

USB, 117

В

VPN, 117

А

Агент регистрации, 84
Администратор, 5

Г

ГОСТ, 117

Д

Датчик случайных чисел, 82
Дистрибутив Единого клиента JaCarta, 10

З

Запросить новый сертификат, 96

И

Импортировать объект в приложение, 78
Инициализация, 5
Инициализация с биометрическими параметрами, 53
Инициализация электронных ключей, 43
Информация о токене, 36

Л

Лицензионное соглашение, 14

М

Меню быстрого запуска, 30

О

Операции с электронными ключами, 7
Основное окно пользовательского интерфейса, 33

П

Параметры ключа инициализации, 47
Параметры электронных ключей при поставке, 6
полный список объектов, 77
Пользователь, 5
Пользователь со смарт-картой, 84
Приложение, 5

Р

Разблокировка PIN-кода пользователя, 67
Режим администратора, 5
Режим пользователя, 5

С

Системные требования, 11, 13
Смена PIN-кода администратора, 72
список объектов, 76

У

Удалить объект, 81

Ш

Шаблоны сертификатов, 84

Э

Экспортировать объект из приложения, 80



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

© 1995-2017, ЗАО "Аладдин Р.Д." Все права защищены.

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