



Утверждён

RU.АЛДЕ.02.13.029-01 34 01-ЛУ

Средство криптографической защиты информации

# АРМ администратора безопасности JaCarta

Программа администрирования

Руководство оператора

RU.АЛДЕ.02.13.029-01 34 01

Листов 92

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

## Аннотация

Настоящий документ содержит сведения, необходимые для эксплуатации Программы администрирования (ПА), функционирующей в составе средства криптографической защиты информации «АРМ администратора безопасности JaCarta» (СКЗИ «АРМ АБ JaCarta»), применяемого администратором безопасности СКЗИ «Криптотокен 2 ЭП» в составе изделий JaCarta ГОСТ и JaCarta-2 ГОСТ.

# Содержание

Авторские права, товарные знаки, ограничения .....	7
Лицензионное соглашение .....	8
<b>Термины и определения .....</b>	<b>10</b>
<b>Сокращения и обозначения.....</b>	<b>11</b>
<b>1. Назначение программы .....</b>	<b>12</b>
<b>2. Условия выполнения программы.....</b>	<b>13</b>
<b>3. Назначение файлов программы .....</b>	<b>14</b>
<b>4. Установка и настройка .....</b>	<b>15</b>
4.1 Установка .....	15
4.2 Настройка Information Property List .....	15
4.2.1 Условия необходимости настройки Information Property List.....	15
4.2.2 Виды устройств, сведения о которых должны содержаться в Information Property List .....	15
4.2.3 Порядок настройки Information Property List .....	15
<b>5. Выполнение программы .....</b>	<b>17</b>
5.1 Начало работы.....	17
5.2 Работа с файлом базы данных.....	21
5.3 Смена пароля сброса изделия JaCarta Admin к заводским настройкам .....	22
5.4 Настройка ПУК-кода изделия JaCarta Admin .....	23
5.5 Смена пароля администратора изделия JaCarta Admin.....	23
5.5.1 Смена установленного на производстве пароля администратора изделия JaCarta Admin .....	23
5.5.2 Смена пароля администратора изделия JaCarta Admin, установленного администратором ранее.....	24
5.5.3 Сброс счётчика последовательных неудачных попыток ввода пароля администратора изделия JaCarta Admin при смене этого пароля .....	25
5.6 Генерация ключа администрирования .....	25
5.7 Генерация ключа базы данных.....	25
5.8 Выбор ключа базы данных по умолчанию.....	26
5.9 Генерация ключа для НМАС.....	27
5.10 Импорт ключа для НМАС.....	28
5.11 Экспорт ключа для НМАС .....	30
5.12 Администрирование изделий JaCarta-2 ГОСТ .....	32
5.13 Ввод изделий JaCarta-2 ГОСТ в эксплуатацию .....	34
5.14 Генерация последовательности для удалённой разблокировки изделия JaCarta-2 ГОСТ .....	34
5.15 Работа с файлами в базе данных .....	35
5.15.1 Загрузка файла в базу данных .....	35
5.15.2 Удаление файла из базы данных .....	36
5.16 Сброс изделия JaCarta-2 ГОСТ к заводским настройкам .....	36
5.17 Блокировка изделия JaCarta Admin.....	36
5.18 Разблокировка изделия JaCarta Admin.....	37
5.19 Сброс изделия JaCarta Admin к заводским настройкам .....	38
5.20 Завершение работы.....	39
5.21 Резервирование данных .....	39
5.22 Удаление программы.....	39
<b>6. Подготовка сценариев АРМ АБ .....</b>	<b>40</b>
6.1 Структура файла сценария .....	40
6.2 Заголовок сценария .....	40
6.3 Операции администрирования изделий JaCarta-2 ГОСТ .....	41

6.4	Создание файла сценария .....	50
6.5	Проверка синтаксиса сценария .....	52
6.6	Редактирование сценария .....	52
6.7	Удаление сценария .....	52
6.8	Создание шаблона сценария .....	53
6.9	Загрузка шаблона сценария .....	53
6.10	Автоматическая загрузка шаблонов сценариев .....	54
<b>7.</b>	<b>Журналы .....</b>	<b>55</b>
7.1	Журнал операций с изделием JaCarta-2 ГОСТ .....	55
7.2	Журнал выполненных сценариев .....	57
7.3	Журнал ошибок .....	58
7.4	Журнал операций с изделием JaCarta Admin .....	58
<b>8.</b>	<b>Сообщения оператору .....</b>	<b>60</b>
8.1	Сообщения строки состояния .....	60
8.2	Сообщения в диалоговых окнах .....	61
8.3	Сообщения, запрашивающие данные или выбор пользователя .....	73
8.4	Сообщения в журналах .....	76
8.4.1	Сообщения в журнале операций с изделием JaCarta Admin .....	76
8.4.2	Сообщения в журналах ошибок, выполненных сценариев и операций с изделием JaCarta-2 ГОСТ .....	78
8.5	Информация о контроле целостности .....	84
	<b>Приложение 1. Файловая система изделия .....</b>	<b>85</b>
	<b>Приложение 2. Примеры сценариев операций .....</b>	<b>87</b>
	Сценарий сброса к заводским настройкам .....	87
	Сценарий смены ключа администратора безопасности и инициализации изделия JaCarta-2 ГОСТ .....	87
	<b>Контакты .....</b>	<b>88</b>
	Офис (общие вопросы) .....	88
	Техподдержка .....	88
	<b>Ресурсы .....</b>	<b>89</b>
	Список литературы .....	89
	Предметный указатель .....	90
	<b>Таблицы</b>	
	Таблица 1 – Назначение файлов ПА .....	14
	Таблица 2 – Сообщения строки состояния ПА .....	60
	Таблица 3 – Сообщения диалоговых окон ПА .....	62
	Таблица 4 – Сообщения, запрашивающие данные или выбор пользователя .....	73
	Таблица 5 – Сообщения в журнале операций с изделием JaCarta Admin .....	76
	Таблица 6 – Сообщения <ExecuteActionsList> в журнале ошибок ПА .....	78
	Таблица 7 – Сообщения <ExecuteActionsList> в журнале операций с изделием JaCarta-2 ГОСТ .....	79
	Таблица 8 – Сообщения операций в журнале ошибок ПА .....	79
	Таблица 9 – Возможные варианты содержания поля <Описания действия> .....	80
	Таблица 10 – Возможные варианты содержания поля <Название APDU-команды> .....	81
	Таблица 11 – Сообщения операций в журнале операций с изделием JaCarta-2 ГОСТ .....	83
	<b>Таблицы приложения 1</b>	
	Таблица 1 – Права доступа к файлам и папкам (двухбайтовое слово) .....	85

## Рисунки

Рисунок 1 – Окно ПА с информацией об оставшихся попытках ввода пароля .....	17
Рисунок 2 – Окно ввода пароля изделия JaCarta Admin .....	18
Рисунок 3 – Окно ПА с отображением процесса аутентификации.....	18
Рисунок 4 – Окно предупреждения о необходимости обновления внутреннего состояния ДСЧ.....	18
Рисунок 5 – Окно биологического ДСЧ .....	19
Рисунок 6 – Окно биологического ДСЧ .....	19
Рисунок 7 – Окно сообщения о создании новой базы данных.....	20
Рисунок 8 – Окно сообщения об установке ключа БД по умолчанию .....	20
Рисунок 9 – Окно предложения генерации нового ключа БД.....	20
Рисунок 10 – Учётные данные сгенерированного ключа базы данных .....	21
Рисунок 11 – Окно запуска ПА с параметром -dbpath .....	21
Рисунок 12 – Окно сообщения о выборе ключа БД.....	22
Рисунок 13 – Окно смены пароля сброса изделия JaCarta Admin к заводским настройкам .....	22
Рисунок 14 – Окно сообщения об успешной смене пароля сброса изделия JaCarta Admin к заводским настройкам .....	22
Рисунок 15 – Окно ввода PUK-кода изделия JaCarta Admin .....	23
Рисунок 16 – Окно сообщения об успешной смене PUK-кода изделия JaCarta Admin.....	23
Рисунок 17 – Окно с информацией о необходимости смены пароля администратора изделия JaCarta Admin .....	23
Рисунок 18 – Окно ввода нового значения пароля администратора .....	24
Рисунок 19 – Окно сообщения об успешной смене пароля администратора .....	24
Рисунок 20 – Вкладка «Ключи администрирования».....	25
Рисунок 21 – Вкладка «Ключи базы данных» .....	26
Рисунок 22 – Вкладка «Ключи для НМАС» .....	27
Рисунок 23 – Окно ввода назначения ключа для НМАС.....	27
Рисунок 24 – Окно с автоматически созданным при генерации ключа для НМАС файлом сценария .....	28
Рисунок 25 – Окно с информацией о назначении сгенерированного ключа для НМАС.....	28
Рисунок 26 – Окно выбора файла ключа для НМАС.....	29
Рисунок 27 – Окно ввода пароля ключевого контейнера при импорте ключа .....	29
Рисунок 28 – Окно ввода назначения импортируемого ключа для НМАС.....	29
Рисунок 29 – Окно сообщения об успешном импорте ключа для НМАС.....	30
Рисунок 30 – Окно ввода пароля создаваемого ключевого контейнера.....	30
Рисунок 31 – Окно ввода имени файла экспортируемого ключевого контейнера .....	31
Рисунок 32 – Окно сообщения об успешном экспорте ключа для НМАС.....	31
Рисунок 33 – Вкладка JaCarta-2 GOST основного окна программы .....	32
Рисунок 34 – Выбор сценария.....	33
Рисунок 35 – Успешное завершение применения сценария.....	33
Рисунок 36 – Неудачное завершение применения сценария .....	34
Рисунок 37 – Окно генерации последовательности для удалённой разблокировки .....	35
Рисунок 38 – Окно со сгенерированной последовательностью для удалённой разблокировки .....	35
Рисунок 39 – Вкладка «Файлы» .....	36
Рисунок 40 – Окно сообщения о блокировке изделия JaCarta Admin .....	37

Рисунок 41 – Окно ввода PUK-кода .....	37
Рисунок 42 – Окно сообщения об успешной разблокировке изделия JaCarta Admin .....	37
Рисунок 43 – Окно ввода пароля сброса изделия JaCarta Admin к заводским настройкам .....	38
Рисунок 44 – Окно подтверждения сброса изделия JaCarta Admin к заводским настройкам .....	38
Рисунок 45 – Окно информирования о завершении сброса изделия JaCarta Admin к заводским настройкам.....	38
Рисунок 46 – Окно перечня файлов сценариев .....	50
Рисунок 47 – Окно сценария.....	51
Рисунок 48 – Окно сообщения об успешном завершении проверки синтаксиса .....	51
Рисунок 49 – Окно ввода имени файла сценария.....	51
Рисунок 50 – Окно подтверждения удаления файла .....	53
Рисунок 51 – Окно выбора сценария .....	53
Рисунок 52 – Окно запуска ПА с автоматической загрузкой сценариев .....	54
Рисунок 53 – Отображение журнала операций с изделием JaCarta-2 ГОСТ .....	56
Рисунок 54 – Отображение журнала выполненных сценариев.....	57
Рисунок 55 – Отображение журнала ошибок.....	58
Рисунок 56 – Отображение журнала операций с изделием JaCarta Admin .....	59
Рисунок 57 – Окно ошибки .....	61
Рисунок 58 – Окно предупреждения .....	61
Рисунок 59 – Информационное окно.....	61

## Авторские права, товарные знаки, ограничения

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 АО «Аладдин Р. Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р. Д.» обязательны.

Владельцем зарегистрированных товарных знаков «Аладдин», Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, «Крипто БД», логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р. Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

### Ограничение ответственности

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

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

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

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

### Государственное регулирование и экспортный контроль

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

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

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

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

## Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые акционерным обществом «Аладдин Р. Д.» (или любым его дочерним предприятием – каждое из них далее упоминается как «Компания»), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на ваш компьютер и/или используя данное программное обеспечение иным способом, вы принимаете данное соглашение и соглашаетесь с его условиями.

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

Настоящее лицензионное соглашение (далее «Соглашение») является договором, заключенным между вами (физическим или юридическим лицом) – конечным пользователем (далее «Пользователь») – и Компанией относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

### Права и собственность

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

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

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

### Лицензия

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

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

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

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

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

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

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

### Требования к использованию

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

### Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;
- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

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

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

- дизайна (графики, расположения элементов оформления и т.п.);
- всех иных элементов, в том числе изображений, фонограмм, текстов.

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

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

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

### Обслуживание и поддержка

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

### Ограниченная гарантия

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

### Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов



или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

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

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

#### **Ограничение возмещения**

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

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

- возместить стоимость, выплаченную вами за ПО.

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

#### **Исключение косвенных убытков**

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

#### **Ограничение ответственности**

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

#### **Прекращение действия соглашения**

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

После прекращения действия данного Лицензионного соглашения:

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

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

#### **Применимое законодательство**

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

Государственное регулирование и экспортный контроль

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

#### **Разное**

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

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

## Термины и определения

В настоящем руководстве применяются следующие термины с соответствующими определениями:

**JaCarta ГОСТ** – старые модели изделий, в составе которых функционируют компоненты СКЗИ «Криптотокен 2 ЭП». За исключением особо и явно оговорённых случаев, все утверждения настоящего документа, относящиеся к изделиям JaCarta-2 ГОСТ, в полной мере применимы к изделиям JaCarta ГОСТ.

**JaCarta-2 ГОСТ** – новые модели изделий, в составе которых функционируют компоненты СКЗИ «Криптотокен 2 ЭП».

**Апплет** – исполняемый программный модуль изделия JaCarta Admin или изделия JaCarta-2 ГОСТ.

**АРМ-апплет** – исполняемый программный модуль изделия JaCarta Admin.

**Ключ администратора безопасности** – 32-байтовая последовательность, используемая для аутентификации администратора безопасности в изделии JaCarta-2 ГОСТ.

**Ключ администрирования** – ключ, используемый для генерации ключей АБ.

**Ключ базы данных** – ключ, используемый при работе с базой данных СКЗИ «АРМ АБ JaCarta».

**Ключ, хранящийся в памяти изделия JaCarta Admin** – ключ администрирования, ключ базы данных или ключ для HMAC.

**Краткий идентификатор ключа, хранящегося в памяти изделия JaCarta Admin** – 2-байтовый порядковый номер ключа, хранящегося в памяти изделия JaCarta Admin.

**Краткий серийный номер** – уникальный машиночитаемый идентификатор изделия, до 16 символов.

**Полный идентификатор ключа, хранящегося в памяти изделия JaCarta Admin** – конкатенация: полный серийный номер изделия JaCarta Admin (8 Б) || краткий идентификатор ключа, хранящегося в памяти изделия JaCarta Admin (2 Б).

**Полный серийный номер** – уникальный машиночитаемый идентификатор изделия, 16 символов.

**ЭВМ АРМ АБ** – электронная вычислительная машина, предназначенная для функционирования ПА.

## Сокращения и обозначения

В настоящем руководстве применяются следующие сокращения и обозначения:

**АБ** – администратор безопасности.

**АРМ АБ** – автоматизированное рабочее место администратора безопасности.

**ДСЧ** – датчик случайных чисел.

**ПА** – программа администрирования СКЗИ «АРМ АБ JaCarta».

**ПДСЧ** – программный датчик случайных чисел.

**СКЗИ** – средство криптографической защиты информации.

**УКЦ** – утилита контроля целостности.

## 1. Назначение программы

Программа администрирования (ПА) средства криптографической защиты информации (СКЗИ) «АРМ АБ JaCarta» предназначена для обеспечения пользовательского интерфейса администратора безопасности (АБ) СКЗИ «Криптотокен 2 ЭП» в составе изделий JaCarta ГОСТ и JaCarta-2 ГОСТ.

## 2. Условия выполнения программы

Для выполнения ПА необходимы:

- ЭВМ аппаратной архитектуры IA-32 или x86-64, к которой подключаются изделия JaCarta-2 ГОСТ и JaCarta Admin (далее – ЭВМ АРМ АБ);
- операционная система Windows (7, 8.1, 10) или Linux (Astra Linux Special Edition релиз Смоленск 1.6, Альт 8 СП; РЕД ОС 7.1 МУРОМ, Ubuntu 18.04 LTS);
- изделие JaCarta Admin;
- свободное место на жёстком диске ЭВМ АРМ АБ в объёме, достаточном для исполняемого файла ПА БД ПА<sup>1</sup>.

Кроме того, в ОС Linux должны быть установлены пакеты pcscd, libpcslite и libccid.

---

<sup>1</sup> Перед началом эксплуатации СКЗИ АРМ АБ JaCarta достаточно 1 МБ свободного места. По мере роста объёма информации в БД ПА в процессе эксплуатации потребность в дисковом пространстве возрастает.

### 3. Назначение файлов программы

Назначение файлов ПА приведено в таблице 1.

Таблица 1 – Назначение файлов ПА

Имя файла	Назначение	ОС	Примечание
jcadmin.exe	Исполняемый файл ПА	Windows	Входит в дистрибутив
jcadmin	Исполняемый файл ПА	Linux	Входит в дистрибутив
ct2.db	Файл БД	Windows и Linux	Создаётся автоматически при первом запуске ПА

## 4. Установка и настройка

### 4.1 Установка

Дистрибутив СКЗИ «АРМ АБ JaCarta» представляет собой файл-архив.

Для установки ПА:

- создайте на жёстком диске ЭВМ АРМ АБ папку;
- извлеките в созданную папку файлы из архива.

### 4.2 Настройка Information Property List

#### 4.2.1 Условия необходимости настройки Information Property List

Установленная ПА обычно готова к работе без дополнительной настройки. Но если в ОС Linux ПА не обнаруживает изделие JaCarta Admin и/или JaCarta-2 ГОСТ, может потребоваться настройка Information Property List.

#### 4.2.2 Виды устройств, сведения о которых должны содержаться в Information Property List

Для полноценной работы с изделиями JaCarta Admin и JaCarta-2 ГОСТ Information Property List должен включать сведения:

- обо всех применяемых USB-токенах JaCarta Admin и JaCarta-2 ГОСТ;
- обо всех USB-считывателях, к которым подключаются смарт-карты JaCarta Admin и JaCarta-2 ГОСТ.

#### 4.2.3 Порядок настройки Information Property List

Для каждой модели устройств, виды которых указаны выше, выполните следующее:

##### 1. Определите VID и PID.

Для изделий АО «Аладдин Р. Д.» VID=24DC.

Различные модели USB-токенов JaCarta имеют различные PID.

USB-токен JaCarta Admin и некоторые другие USB-токены JaCarta имеют PID=0101.

Способы определения VID и PID любых USB-устройств:

- использование входящей в состав ОС Linux утилиты `lsusb` либо её аналогов;
- обращение в службу технической поддержки фирмы-производителя изделия.

*При использовании утилиты `lsusb`:*

##### 1. Подключите к ЭВМ устройства, которые не определяются в ПА.

##### 2. Запустите утилиту `lsusb` с правами суперпользователя:

```
$ sudo lsusb
```

*Утилита `lsusb` выводит сведения обо всех подключенных USB-устройствах в формате:*

```
Bus <номер USB-шины> Device <номер устройства>: ID <VID>:<PID> <Название устройства>
```

##### 3. Если ПА не отображает устройства АО «Аладдин Р. Д.», найдите все строки с VID=24dc и определите по ним PID.

*Для считывателей смарт-карт сторонних производителей опирайтесь на отображаемые утилитой названия устройств либо на информацию из службы технической поддержки производителя считывателя.*

##### 2. Откройте с правами суперпользователя файл Information Property List.

Этот файл можно найти с помощью встроенной утилиты *find*. Признаком файла *Information Property List* является наличием в его имени строки `Info.plist` либо `Info.plist`. Имя файла может совпадать с одной из указанных выше строк, либо иметь какой-нибудь префикс. Пример имени файла *Information Property List* с префиксом: `libccid_Info.plist`.

Файл *Information Property List* может быть не единственным. В случае наличия нескольких файлов *Information Property List* выполните описанные в настоящем документе действия по отношению к каждому из них.

*Information Property List* содержит списки `ifdVendorID`, `ifdProductID` и `ifdFriendlyName`. Каждому из отображаемых в системе видов USB-устройств соответствует номер строки в каждом из списков, т.е.:

- первому виду устройств соответствует первый элемент списка `ifdVendorID`, первый элемент списка `ifdProductID` и первый из элементов списка `ifdFriendlyName`;
- второму виду устройств соответствует второй элемент списка `ifdVendorID`, второй элемент списка `ifdProductID`, и второй из элементов списка `ifdFriendlyName` и т. д.

При использовании комбинированных устройств, которые могут применяться в качестве изделий JaCarta-2 ГОСТ, выполняйте настройку *Information Property List* в соответствии с документацией программного обеспечения, поставляемого вместе с комбинированными устройствами.

3. Для каждого из устройств, не учтённого в *Information Property List*:
  - 1.1. Добавьте в конец списка `ifdVendorID` идентификатор производителя изделия.  
Для изделий АО «Аладдин Р. Д.»: `<string>0x24DC</string>`
  - 1.2. Добавьте в конец списка `ifdProductID` идентификатор модели изделия.  
Для USB-токенов *JaCarta Admin*: `<string>0x0101</string>`
  - 1.3. Добавьте в конец списка `ifdFriendlyName` такое имя, по которому вам удобнее идентифицировать данную модель изделия.  
Для USB-токенов *JaCarta Admin*: `<string>ARDS JaCarta</string>`
4. Сохраните изменённый файл *Information Property List*.
5. Перезагрузите компьютер.



## 5. Выполнение программы

### 5.1 Начало работы

*ПА не поддерживает работу с двумя и более изделиями JaCarta Admin. Перед началом работы убедитесь, что к ЭВМ АРМ АБ не подключены изделия JaCarta Admin. Не подключайте к ЭВМ АРМ АБ более одного изделия JaCarta Admin.*

*Не запускайте более одного экземпляра ПА.*

Для начала работы с ПА:

- подключите изделие JaCarta Admin к ЭВМ АРМ АБ<sup>1</sup>;
- запустите с жёсткого диска ЭВМ АРМ АБ исполняемый файл ПА;
- ознакомьтесь с информацией об оставшихся попытках ввода неверного пароля и PUK-кода подряд (рисунок 1) в основном окне программы;

*При исчерпании попыток изделие JaCarta Admin будет заблокировано. Для возобновления работы потребуется выполнить разблокировку (см. «Разблокировка изделия JaCarta Admin», с. 37) или сброс к заводским настройкам (см. «Сброс изделия JaCarta Admin к заводским настройкам», с. 38).*

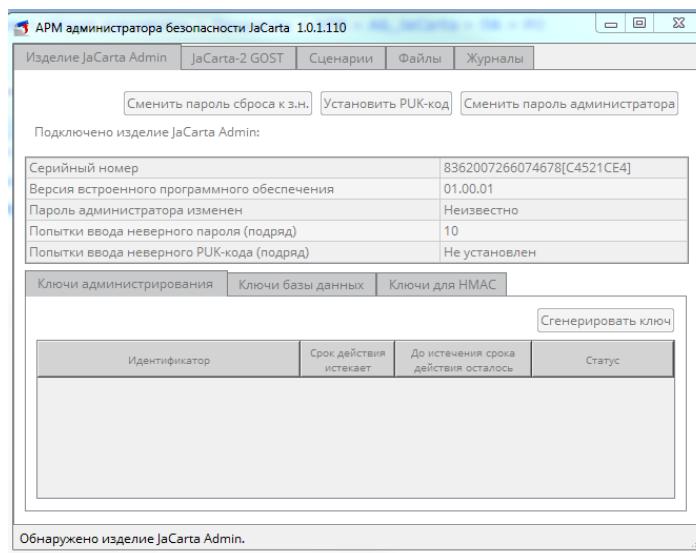


Рисунок 1 – Окно ПА с информацией об оставшихся попытках ввода пароля

- введите пароль администратора изделия JaCarta Admin (рисунок 2);

*На новых изделиях JaCarta Admin пароль администратора имеет значение 1234567890.*

<sup>1</sup> Возможно появление сообщения ОС о том, что не удалось найти драйвер смарт-карты. Окно данного сообщения следует закрыть, а работу с ПА – продолжить.

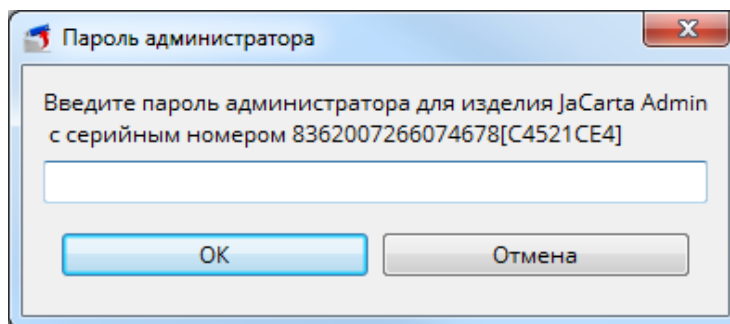


Рисунок 2 – Окно ввода пароля изделия JaCarta Admin

- дождитесь завершения процесса аутентификации, который может занять несколько минут (рисунок 3);

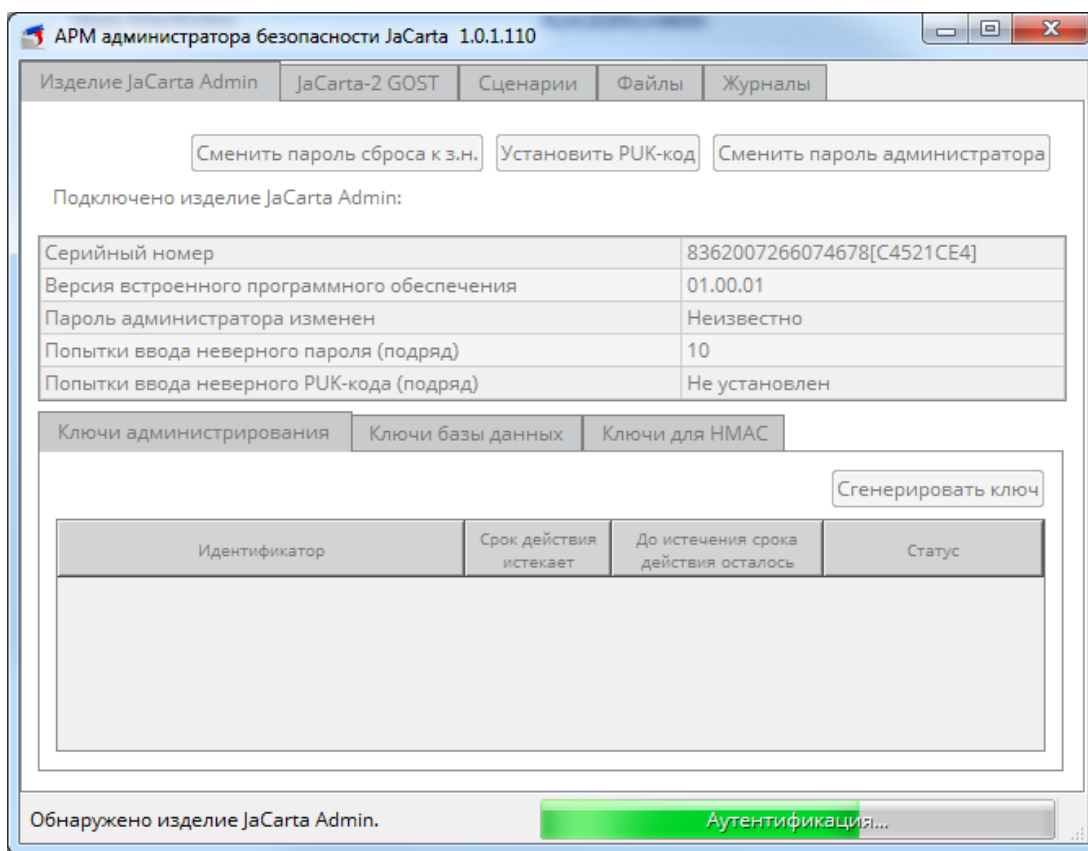


Рисунок 3 – Окно ПА с отображением процесса аутентификации

- если подключённое изделие JaCarta Admin является новым, выполните:
  - обновление внутреннего состояния ДСЧ изделия JaCarta Admin, нажав **OK** (рисунок 4);

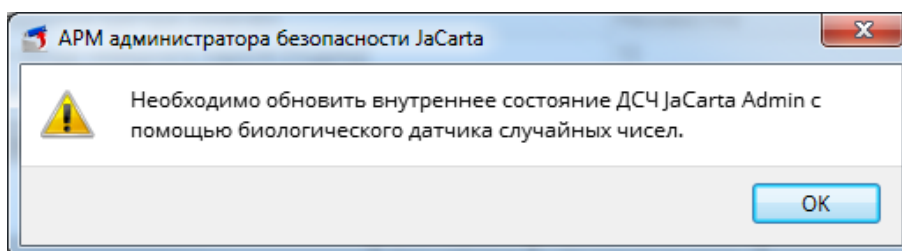


Рисунок 4 – Окно предупреждения о необходимости обновления внутреннего состояния ДСЧ

- убедитесь в том, что в системе установлена английская раскладка клавиатуры; если это не так, установите её;
- нажимайте указанные клавиши на клавиатуре (рисунок 5), пока не станет доступной кнопка **ОК**;

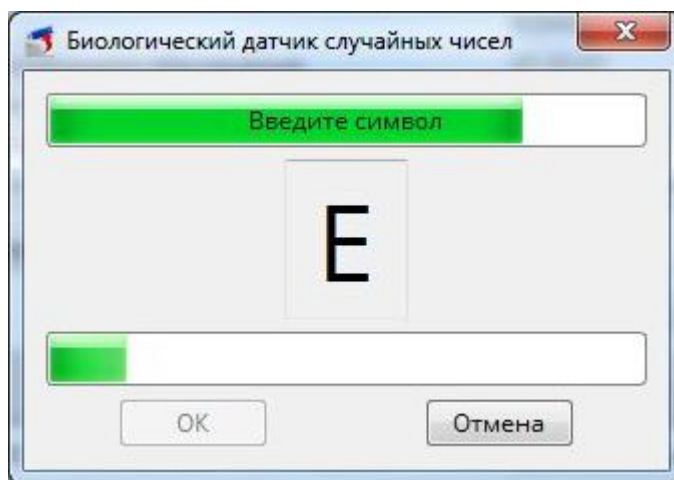



Рисунок 5 – Окно биологического ДСЧ

 Верхний индикатор в этом окне отображает время, остающееся на нажатие указанной клавиши, а нижний индикатор – количество точно и вовремя нажатых клавиш.

- щёлкните **ОК** (рисунок 6);

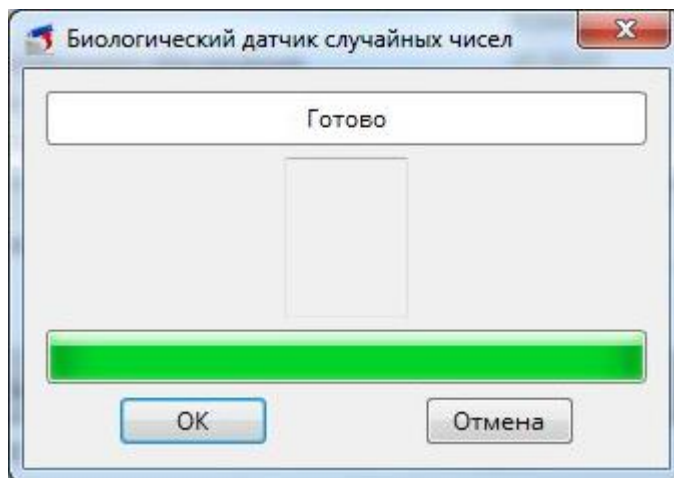


Рисунок 6 – Окно биологического ДСЧ

- дождитесь завершения аутентификации (см. рисунок 3, с. 18);
- смените установленный на производстве пароль администратора изделия JaCarta Admin (см. «Смена установленного на производстве пароля администратора изделия JaCarta Admin», с. 23);
- если ПА запускается впервые – закройте кнопкой **ОК** показанное на рисунке 7 окно с сообщением о том, что будет создана новая база данных (БД);

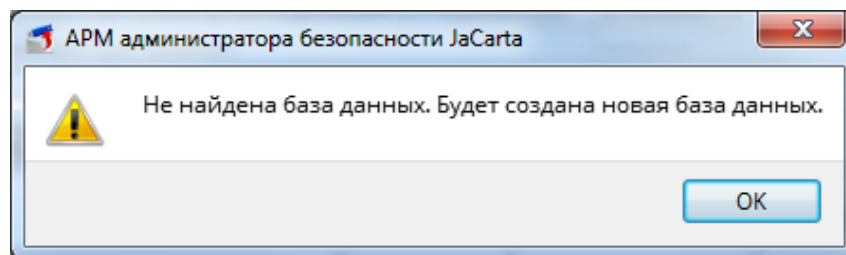


Рисунок 7 – Окно сообщения о создании новой базы данных

- если ключ БД по умолчанию не установлен – установите его, щёлкнув **ОК** (рисунок 8);

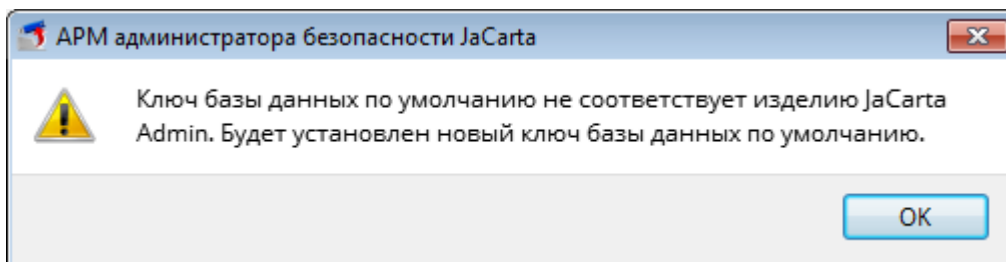


Рисунок 8 – Окно сообщения об установке ключа БД по умолчанию

- если в изделии JaCarta Admin не обнаружится подходящий ключ БД – сгенерируйте новый ключ, для чего щёлкните **ОК** (см. рисунок 9);

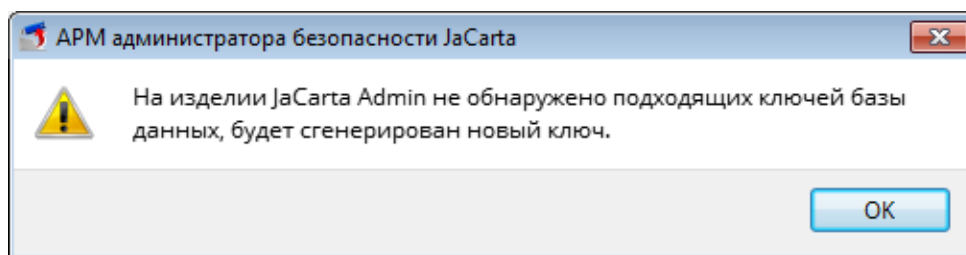


Рисунок 9 – Окно предложения генерации нового ключа БД

- нажимайте указанные клавиши на клавиатуре до завершения процесса генерации (см. рисунок 5, с. 19);
- щёлкните **ОК** (см. рисунок 6, с. 19).

Учётные данные сгенерированного ключа базы данных появятся на вкладке «Ключи базы данных» (рисунок 10).

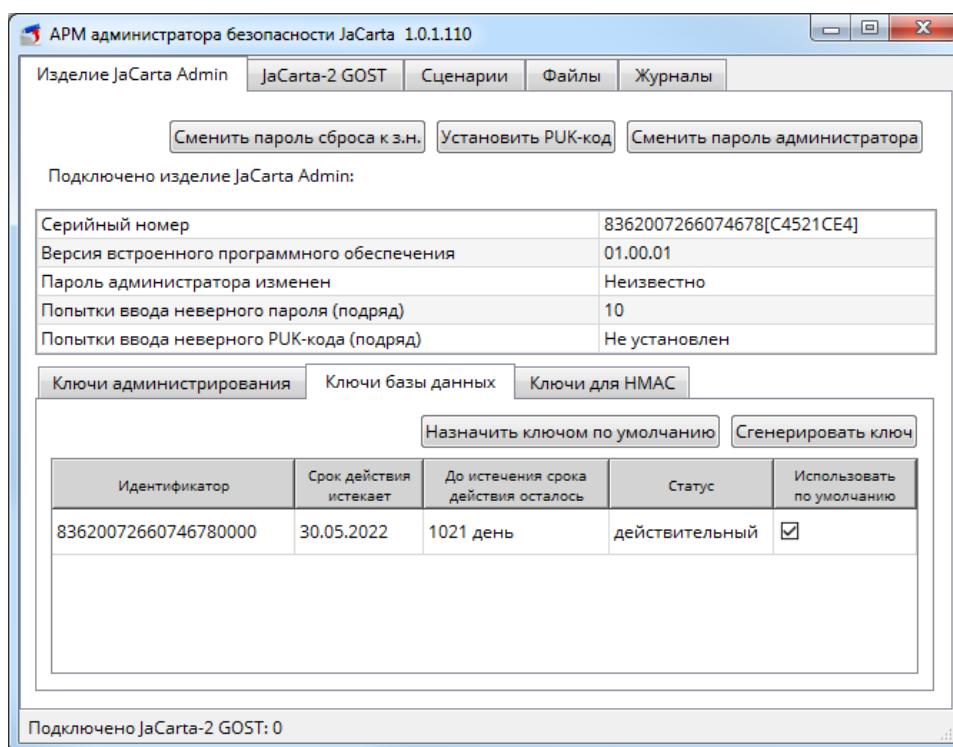


Рисунок 10 – Учётные данные сгенерированного ключа базы данных

## 5.2 Работа с файлом базы данных

Для создания файла БД или работы с файлом БД в произвольной директории:

- запустите интерпретатор командной строки;
- запустите исполняемый файл ПА с параметром `-dbpath1` и указанным в кавычках полным именем файла БД (см. рисунок 11, с. 21).<sup>2</sup>

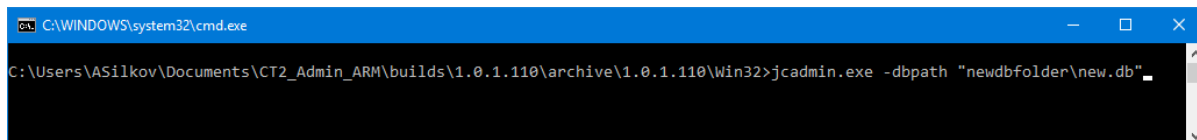


Рисунок 11 – Окно запуска ПА с параметром `-dbpath`

При наличии файла БД по указанному пути ПА использует его для работы.

При отсутствии данного файла ПА его там создаст, для этого:

- закройте кнопкой **ОК** показанное на рисунке 7 окно с сообщением о том, что будет создана новая БД;
- закройте кнопкой **ОК** показанное на рисунке 12 окно с сообщением о том, что будет выбран самый новый ключ базы данных.

---

<sup>1</sup> Параметр `-dbpath` можно комбинировать с параметром `-scriptLoad`, но только в следующем порядке: `jcadmin -scriptLoad "<путь для загрузки шаблонов сценариев сценариев>" -dbpath "<путь к файлу базы данных>"`.

<sup>2</sup> Допускается использовать относительный путь.

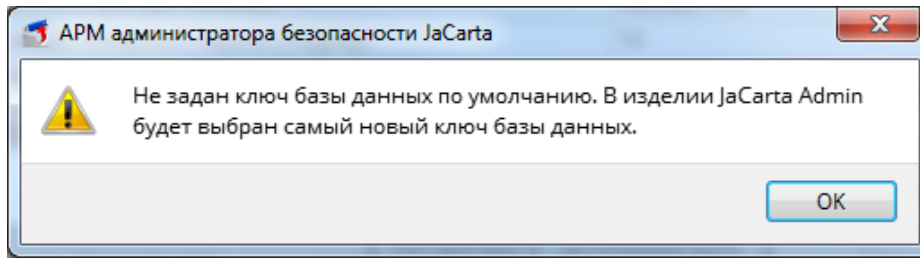



Рисунок 12 – Окно сообщения о выборе ключа БД

### 5.3 Смена пароля сброса изделия JaCarta Admin к заводским настройкам

Для смены пароля сброса изделия JaCarta Admin к заводским настройкам:

- во вкладке «Изделие JaCarta Admin» щёлкните **Сменить пароль сброса к з.н.**;
- введите текущий и новый пароль сброса к заводским настройкам изделия JaCarta Admin (рисунок 13), при этом если вы хотите, чтобы вводимый новый пароль отображался, щёлкните  («Показать пароль»);

На новых изделиях JaCarta Admin пароль сброса к заводским настройкам имеет значение 1234567890.

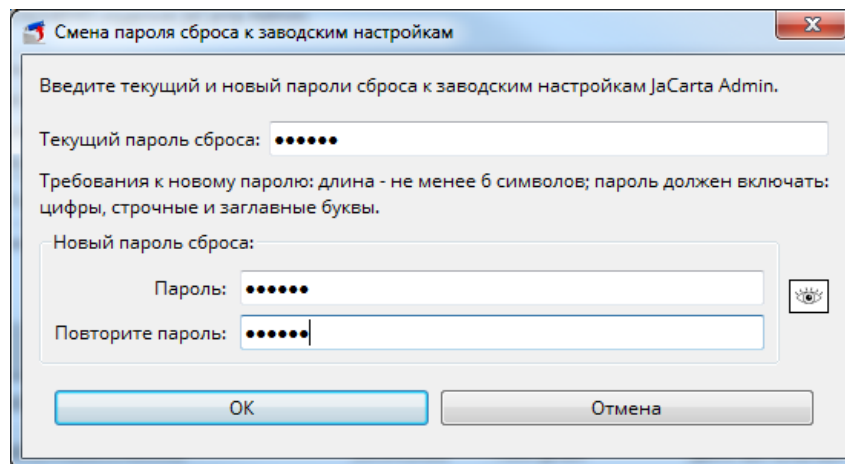


Рисунок 13 – Окно смены пароля сброса изделия JaCarta Admin к заводским настройкам

- щёлкните **ОК** (рисунок 14).

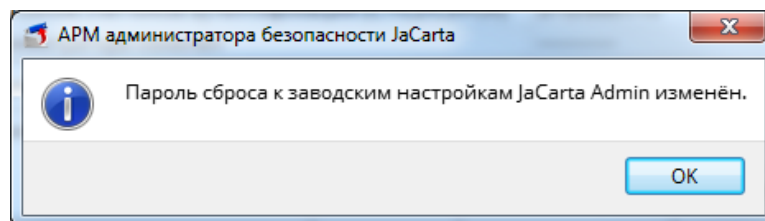



Рисунок 14 – Окно сообщения об успешной смене пароля сброса изделия JaCarta Admin к заводским настройкам

Надёжно храните заданное значение пароля сброса изделия JaCarta Admin к заводским настройкам. Не существует возможности вернуть пароль сброса к заводским настройкам к значению по умолчанию.

## 5.4 Настройка PUK-кода изделия JaCarta Admin

Для настройки значения PUK-кода изделия JaCarta Admin:

- во вкладке «Изделие JaCarta Admin»:
  - если значение PUK-кода не было прежде задано, щёлкните **Установить PUK-код**;
  - если необходимо сменить значение PUK-кода, щёлкните **Сменить PUK-код**;
- в открывшемся окне (рисунок 15):
  - дважды введите новое значение PUK-кода, при этом если вы хотите, чтобы вводимое новое значение отображалось, щёлкните  («Показать пароль»);
  - щёлкните **ОК**;

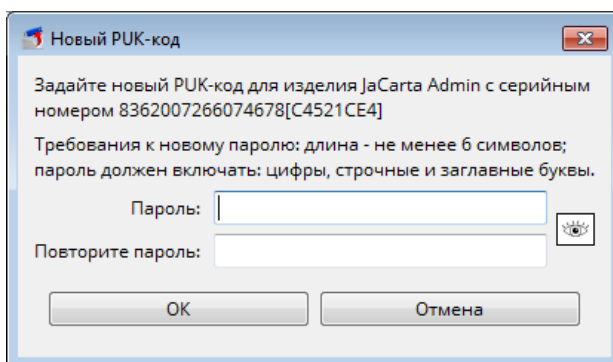


Рисунок 15 – Окно ввода PUK-кода изделия JaCarta Admin

- в открывшемся окне с сообщением об успешной смене PUK-кода щёлкните **ОК** (рисунок 16).

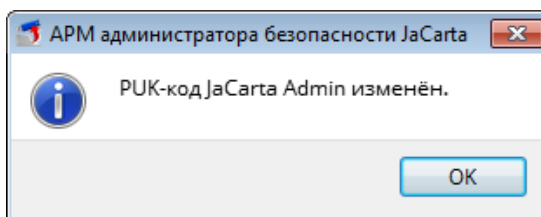


Рисунок 16 – Окно сообщения об успешной смене PUK-кода изделия JaCarta Admin

## 5.5 Смена пароля администратора изделия JaCarta Admin

### 5.5.1 Смена установленного на производстве пароля администратора изделия JaCarta Admin

Для смены установленного на производстве пароля администратора изделия JaCarta Admin:

- закройте кнопкой **ОК** окно с сообщением о необходимости смены пароля (рисунок 17);

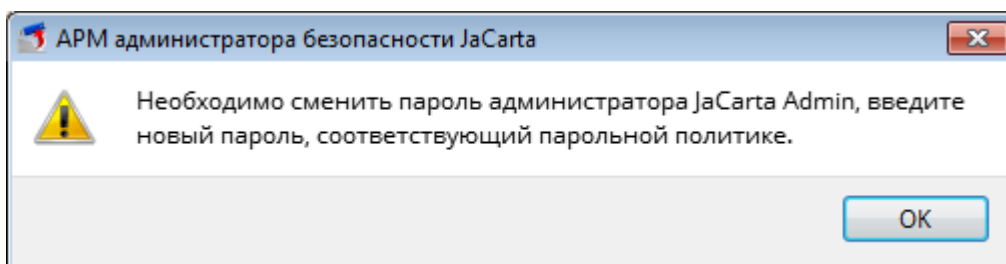



Рисунок 17 – Окно с информацией о необходимости смены пароля администратора изделия JaCarta Admin

- в открывшемся окне (рисунок 18):
  - дважды введите новый пароль, при этом если вы хотите, чтобы вводимое новое значение отображалось, щёлкните  («Показать пароль»);
  - щёлкните **ОК**.

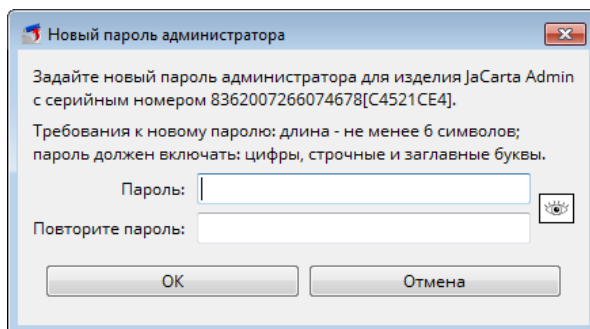


Рисунок 18 – Окно ввода нового значения пароля администратора

- в окне с сообщением об успешной смене пароля администратора щёлкните **ОК** (рисунок 19).

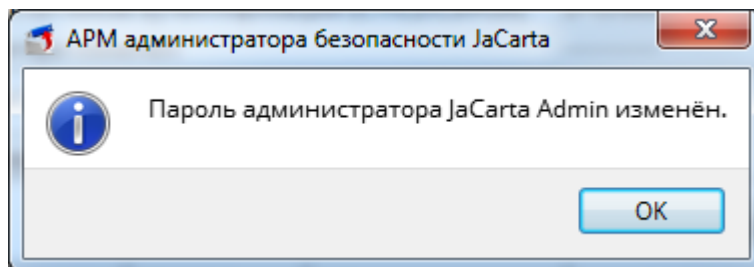



Рисунок 19 – Окно сообщения об успешной смене пароля администратора

После смены установленного на производстве пароля администратора изделия JaCarta Admin выполните следующее:

1. Закройте программу администрирования.
2. Повторно запустите программу администрирования (см. «Начало работы», с. 17).
3. Смените пароль сброса изделия к заводским настройкам на значение, отличное от значения этого пароля по умолчанию (см. «Смена пароля сброса изделия JaCarta Admin к заводским настройкам», с. 22).

#### 5.5.2 Смена пароля администратора изделия JaCarta Admin, установленного администратором ранее

Для смены пароля администратора изделия JaCarta Admin, установленного администратором ранее:

- во вкладке «Изделие JaCarta Admin» щёлкните **Сменить пароль администратора**;
- в открывшемся окне (рисунок 18):
  - дважды введите новый пароль, при этом если вы хотите, чтобы вводимое новое значение отображалось, щёлкните  («Показать пароль»);
  - щёлкните **ОК**.
- в окне с сообщением об успешной смене пароля администратора щёлкните **ОК** (рисунок 19).



### 5.5.3 Сброс счётчика последовательных неудачных попыток ввода пароля администратора изделия JaCarta Admin при смене этого пароля

При смене пароля администратора изделия JaCarta Admin устанавливается максимальное значение счётчика последовательных неудачных попыток ввода этого пароля.

## 5.6 Генерация ключа администрирования

Для генерации ключа администрирования:

- откройте вкладку «Изделие JaCarta Admin» основного окна ПА;
- откройте вкладку «Ключ администрирования» (рисунок 20);
- нажмите кнопку «Сгенерировать ключ»;
- нажимайте указанные клавиши на клавиатуре до завершения процесса генерации (см. рисунок 5, с. 19);
- щёлкните **ОК** (см. рисунок 6, с. 19).

Учётные данные ключа администрирования появятся на вкладке «Ключи администрирования» (рисунок 20);

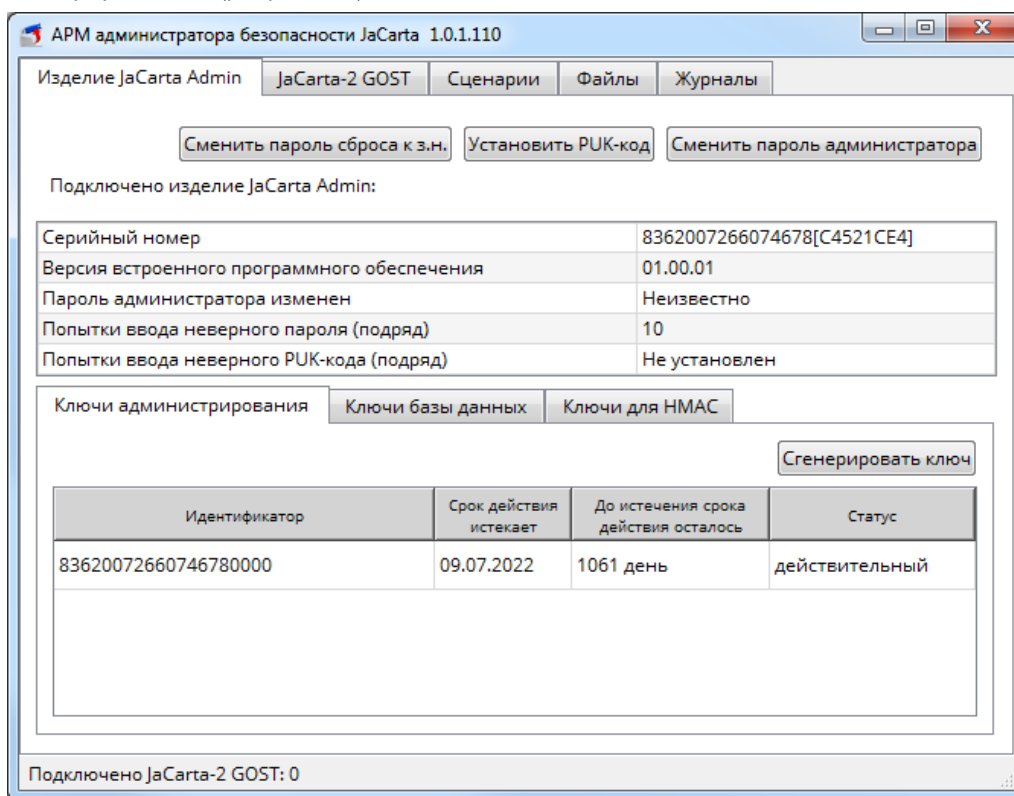


Рисунок 20 – Вкладка «Ключи администрирования»

## 5.7 Генерация ключа базы данных

Для генерации ключа базы данных:

- откройте вкладку «Изделие JaCarta Admin» основного окна ПА;
- откройте вкладку «Ключи базы данных» (рисунок 21);
- нажмите кнопку «Сгенерировать ключ»;

- нажимайте указанные клавиши на клавиатуре до завершения процесса генерации (см. рисунок 5, с. 19);
- щёлкните **ОК** (см. рисунок 6, с. 19).

Учётные данные сгенерированного ключа появятся на вкладке «Ключ базы данных» основного окна ПА (рисунок 21).

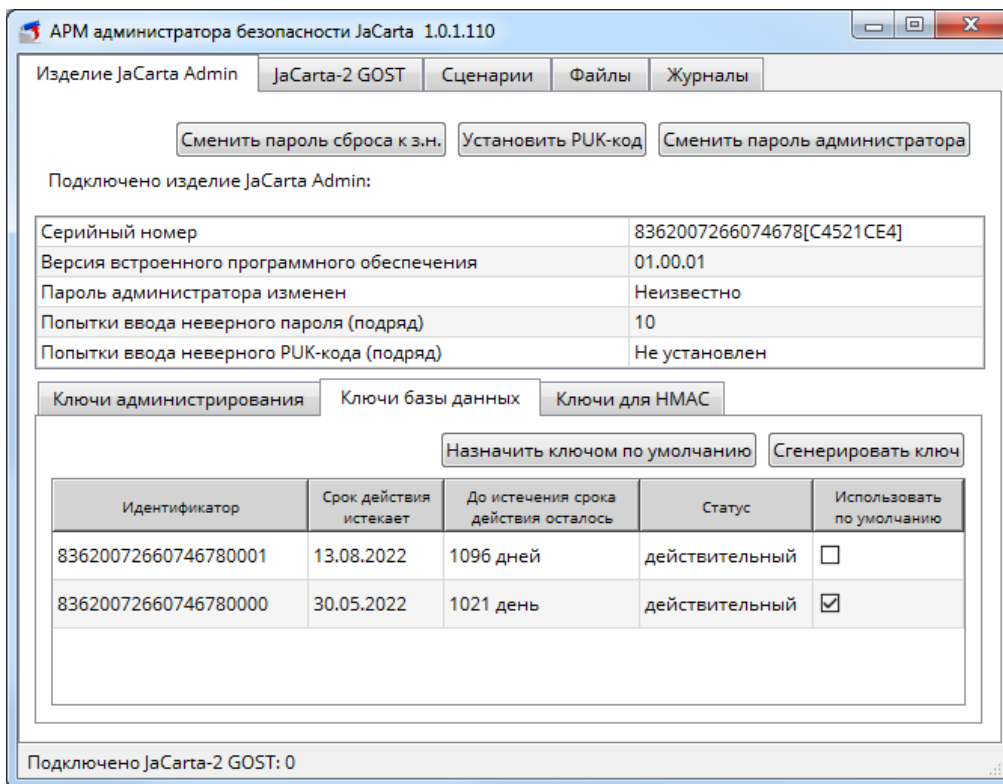


Рисунок 21 – Вкладка «Ключи базы данных»

## 5.8 Выбор ключа базы данных по умолчанию

Для назначения ключа базы данных по умолчанию:

- откройте вкладку «Изделие JaCarta Admin» основного окна ПА;
- откройте вкладку «Ключи базы данных» (рисунок 21);
- выберите необходимый ключ базы данных;
- нажмите кнопку «Назначить ключом по умолчанию».

В столбце «Использовать по умолчанию» строки, содержащей учётные данные ключа базы данных по умолчанию, появится отметка .

## 5.9 Генерация ключа для НМАС

Для генерации ключа для НМАС:

- откройте вкладку «Изделие JaCarta Admin»;
- откройте вкладку «Ключи для НМАС» (рисунок 22);



Рисунок 22 – Вкладка «Ключи для НМАС»

- нажмите кнопку «Сгенерировать ключ»;
- нажимайте указанные клавиши на клавиатуре до завершения процесса генерации (см. рисунок 5, с. 19);
- щёлкните **ОК** (см. рисунок 6, с. 19);
- введите назначение ключа для НМАС (см. рисунок 23);

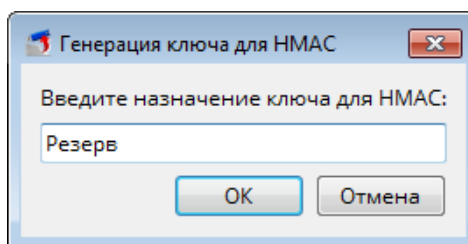


Рисунок 23 – Окно ввода назначения ключа для НМАС

Учётные данные сгенерированного ключа появятся на вкладке «Ключи для НМАС» (рисунок 22).

Сведения о назначении ключа для НМАС появятся в автоматически созданном файле сценария с именем «secret\_key\_notes\_”Полный серийный номер изделия JaCarta Admin[Краткий серийный номер изделия JaCarta Admin]”» (см. рисунок 24 и рисунок 25).

Не удаляйте данный сценарий.

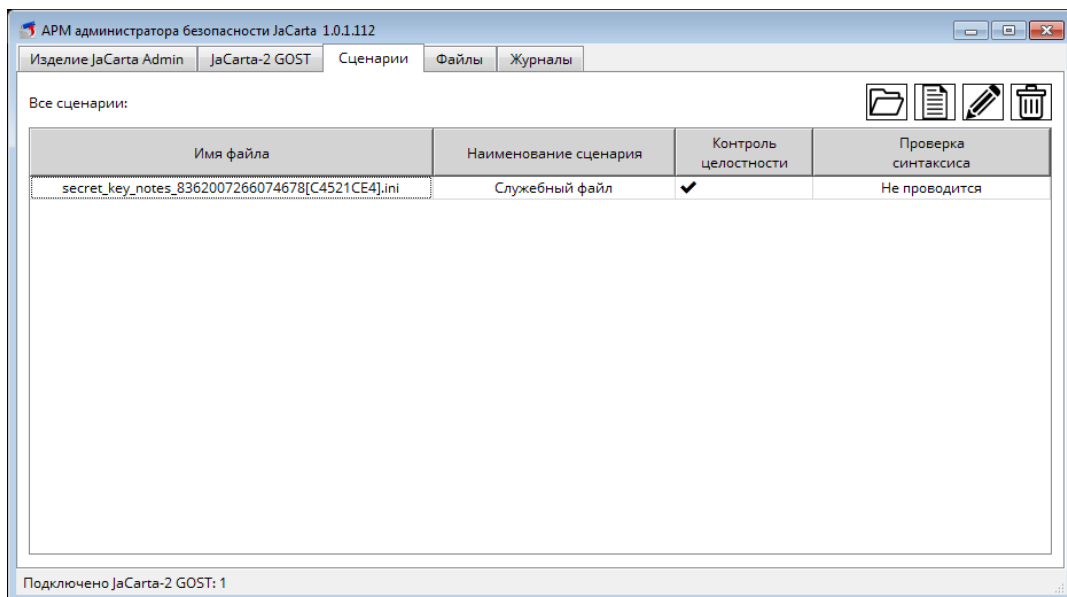


Рисунок 24 – Окно с автоматически созданным при генерации ключа для НМАС файлом сценария

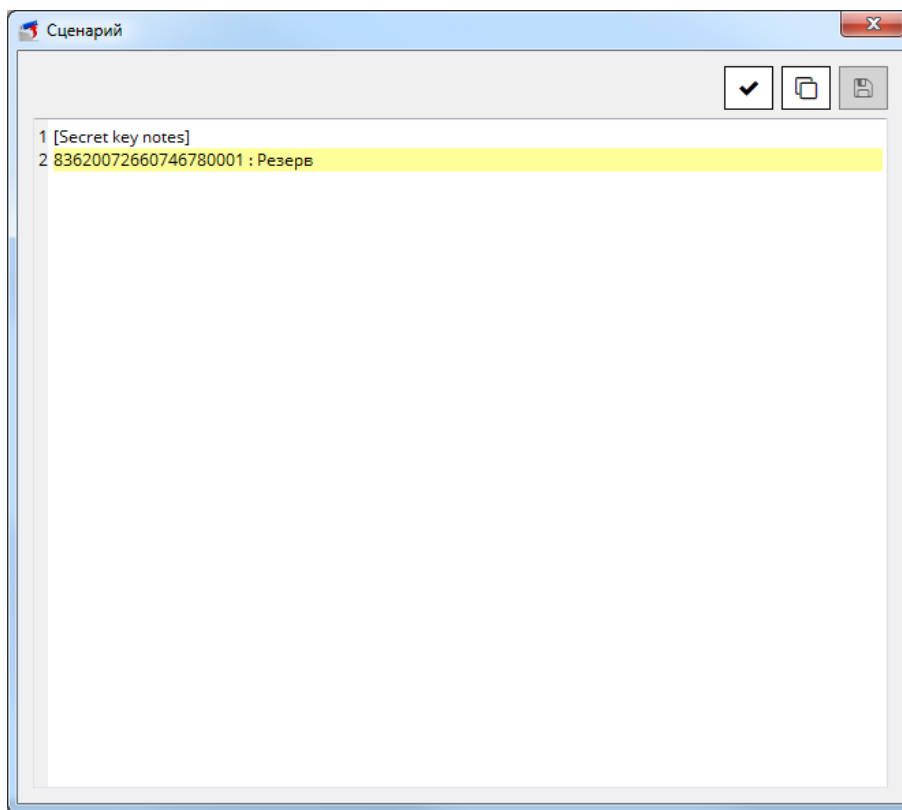


Рисунок 25 – Окно с информацией о назначении сгенерированного ключа для НМАС

## 5.10 Импорт ключа для НМАС

Для импорта ключа для НМАС:

- откройте вкладку «Изделие JaCarta Admin» основного окна ПА;
- откройте вкладку «Ключи для НМАС»;
- нажмите кнопку «Импортировать ключ»;

- выберите файл ключа (см. рисунок 26);

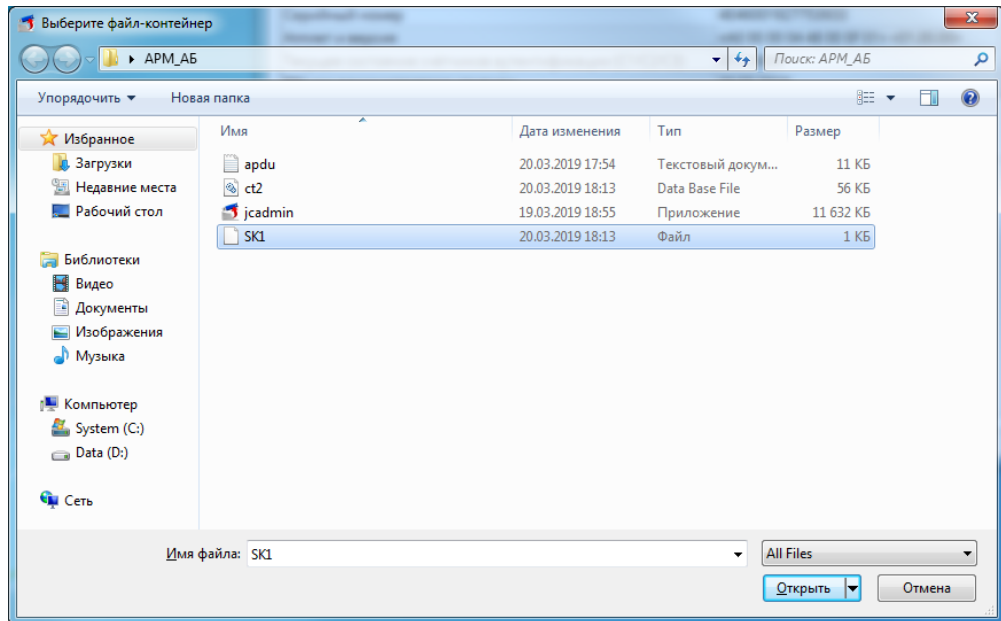


Рисунок 26 – Окно выбора файла ключа для НМАС

- нажмите кнопку открыть;
- введите пароль ключевого контейнера (см. рисунок 27) и нажмите кнопку **OK**;

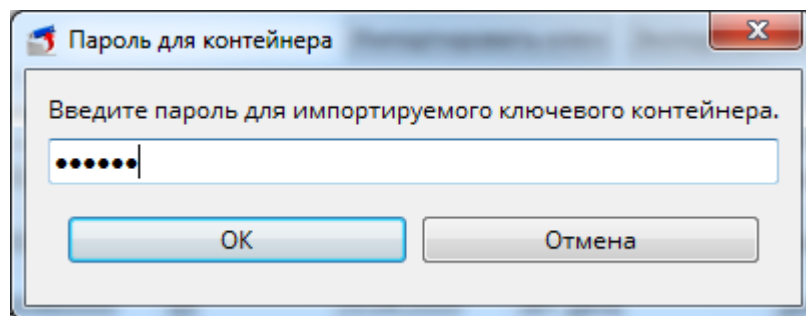


Рисунок 27 – Окно ввода пароля ключевого контейнера при импорте ключа

- введите назначение ключа для НМАС (см. рисунок 28);

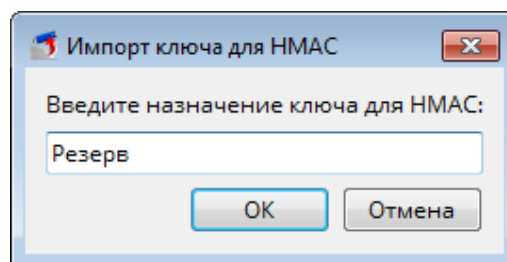


Рисунок 28 – Окно ввода назначения импортируемого ключа для НМАС

- Нажмите кнопку **ОК** (см. рисунок 29).

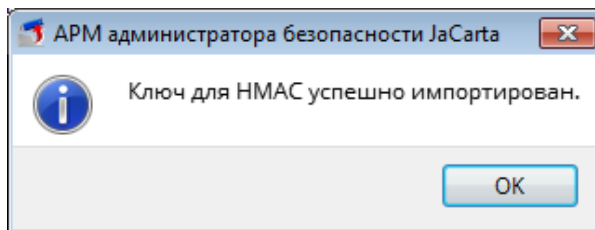



Рисунок 29 – Окно сообщения об успешном импорте ключа для HMAC

Информация об импортированном ключе для HMAC появится на вкладке «Ключи для HMAC» основного окна ПА и в автоматически созданном файле сценария с именем «secret\_key\_notes\_”*Полный серийный номер изделия JaCarta Admin*[*Краткий серийный номер изделия JaCarta Admin*]”.ini».

### 5.11 Экспорт ключа для HMAC

Для экспорта секретного ключа:

- откройте вкладку «Изделие JaCarta Admin» основного окна ПА;
- откройте вкладку «Ключи для HMAC»;
- выберите ключ, который необходимо экспортировать;
- нажмите кнопку «Экспортировать ключ»;
- введите пароль для экспортируемого ключевого контейнера (см. рисунок 30). При необходимости нажмите кнопку «Показать пароль» ;

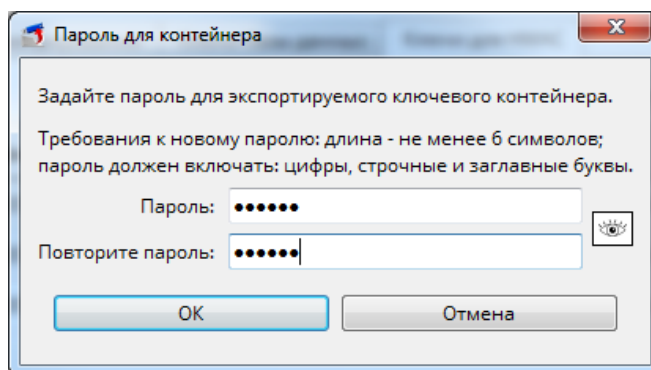


Рисунок 30 – Окно ввода пароля создаваемого ключевого контейнера

- нажмите кнопку **ОК**;

- задайте имя файла экспортируемого ключевого контейнера(см. рисунок 31);

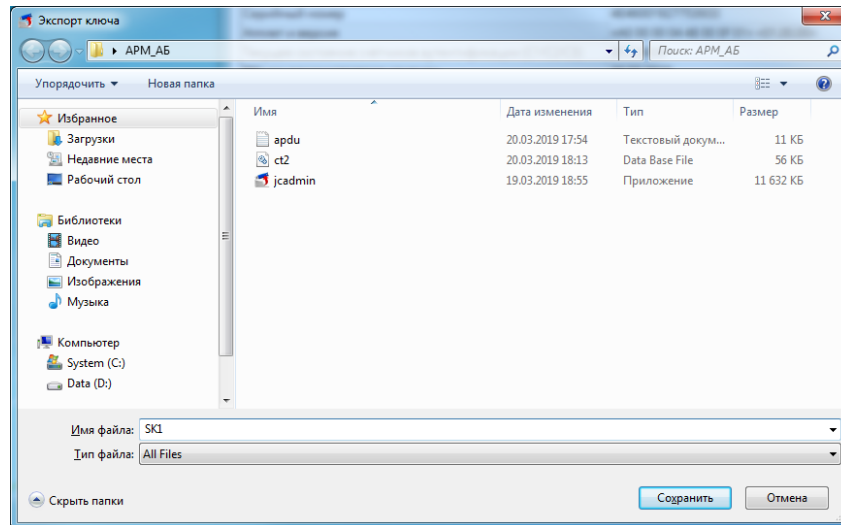


Рисунок 31 – Окно ввода имени файла экспортируемого ключевого контейнера

- нажмите кнопку **ОК** (см. рисунок 32).

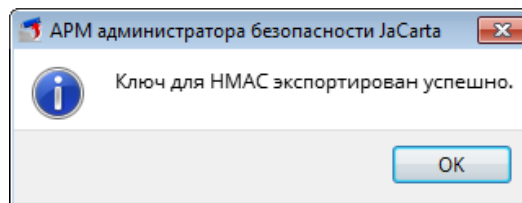


Рисунок 32 – Окно сообщения об успешном экспорта ключа для НМАС

## 5.12 Администрирование изделий JaCarta-2 ГОСТ

Запущенный на выполнение сценарий администрирования изделий JaCarta-2 ГОСТ выполняется в потоковом режиме, т.е. выполняются для всех подключённых на момент запуска сценария изделий JaCarta-2 ГОСТ и для всех вновь подключаемых изделий JaCarta-2 ГОСТ до тех пор, пока пользователь АРМ АБ не выполнит команду останова сценария.

При подключении изделия JaCarta-2 ГОСТ к АРМ АБ JaCarta ПА считывает информацию об изделии и отображает её во вкладке «JaCarta-2 GOST» основного окна ПА (см. рисунок 33).

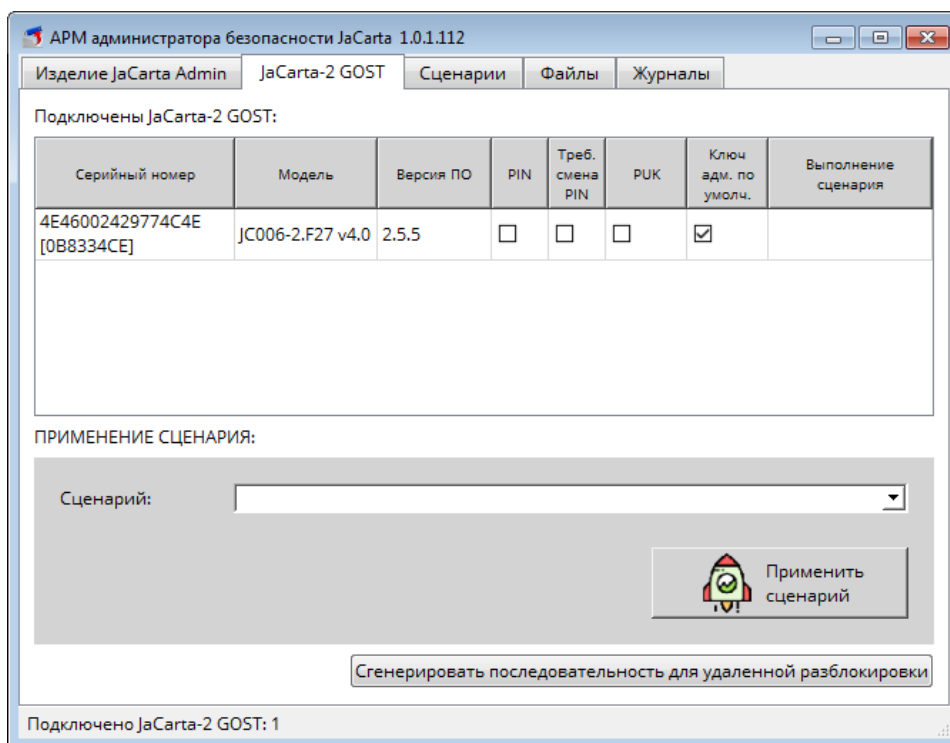


Рисунок 33 – Вкладка JaCarta-2 GOST основного окна программы

В поле «Серийный номер» указаны полный и краткий серийные номера. Отметки  в столбцах «PIN», «PUK» (см. «Операции администрирования изделий JaCarta-2 ГОСТ», с.41, описания операций SET\_PIN и SET\_PUK) означают, что соответствующие значения кодов были заданы. Отметка  в поле «Треб. Смена PIN» означает, что задано требование смены PIN-кода пользователя изделия JaCarta-2 ГОСТ (см. описание операции SET\_PIN с. 42). Отметка  в поле «Ключ адм. по умолч.» означает, что ключ администратора безопасности изделия JaCarta-2 ГОСТ имеет значение по умолчанию, в противном случае в поле будет изображение . Если в изделии JaCarta-2 ГОСТ установлен режим предъявления ключа администратора с установкой защищённого канала, и указанное изделие было подключено после начала выполнения сценария, то соответствующая отметка в поле «Ключ адм. по умолч.» появится после завершения текущего сценария.

Для администрирования изделия JaCarta-2 ГОСТ:

- подключите изделия JaCarta-2 ГОСТ к ЭВМ АРМ АБ;
- проконтролируйте появление учётных данных изделий JaCarta-2 ГОСТ на вкладке «JaCarta-2 GOST» основного окна ПА (см. рисунок 33);

откройте выпадающий список «Сценарий:» и выберите нужный сценарий и нажмите кнопку «Применить сценарий» (см. рисунок 34);

Если необходимый сценарий не отображается в выпадающем списке «Сценарий:», проверьте синтаксис данного сценария (см. «Проверка синтаксиса сценария» с. 52).



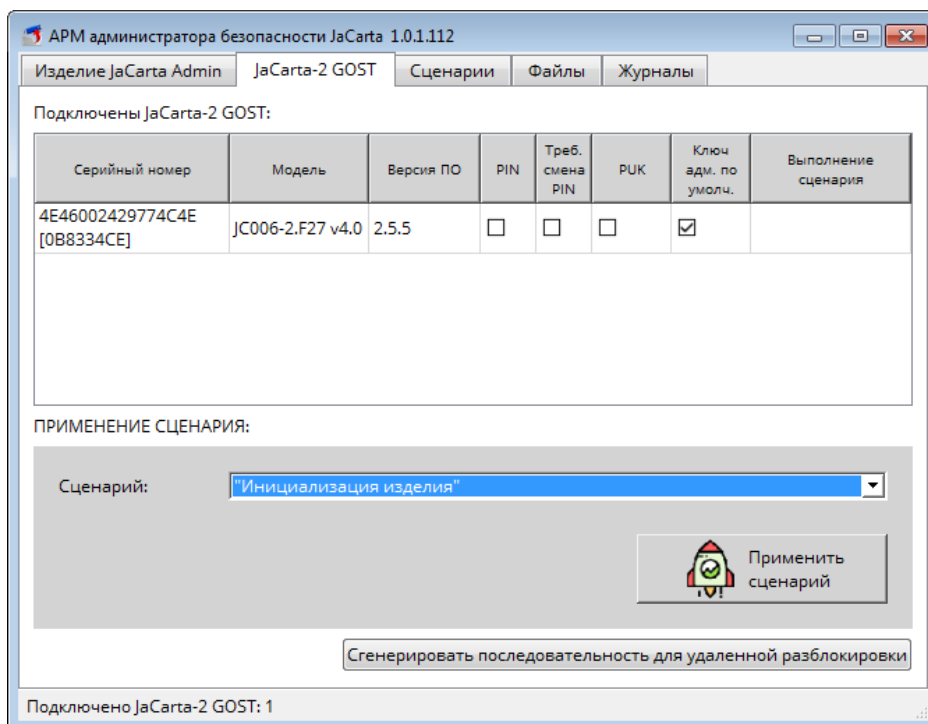


Рисунок 34 – Выбор сценария

- дождитесь завершения выполнения сценария, о чём будет символизировать появление отметки в поле «Статус выполнения сценария» (см. рисунок 35 и рисунок 36);

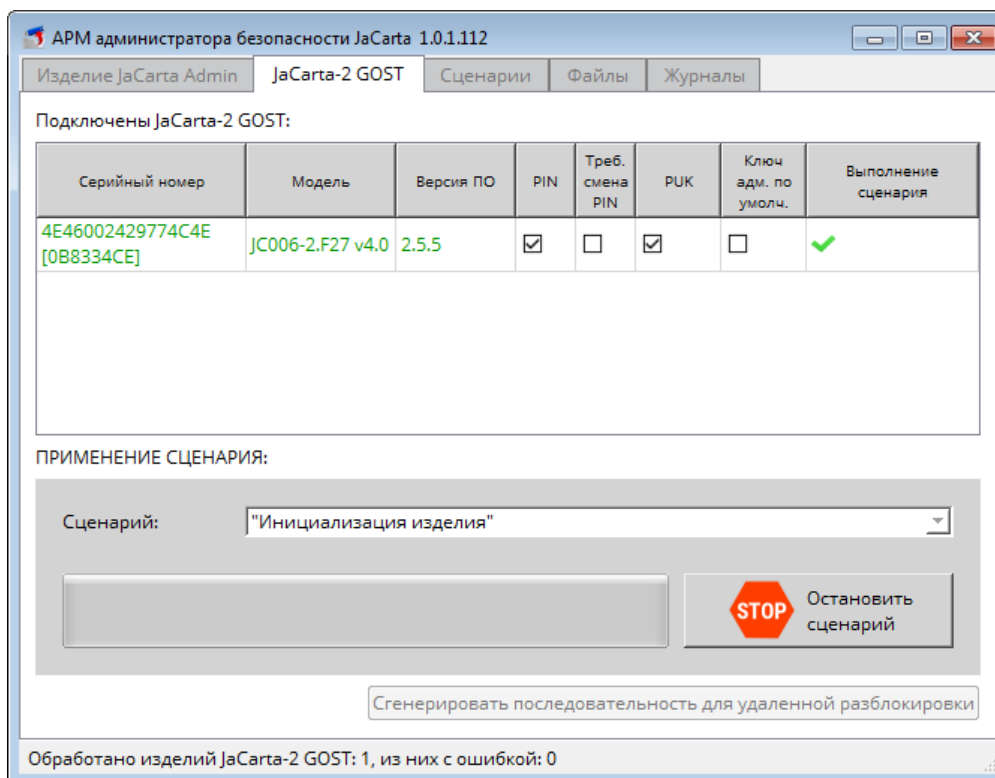


Рисунок 35 – Успешное завершение применения сценария

Текущее выполнение сценария отменить нельзя. Нажатие кнопки «Остановить сценарий» не отменяет текущее выполнение сценария!

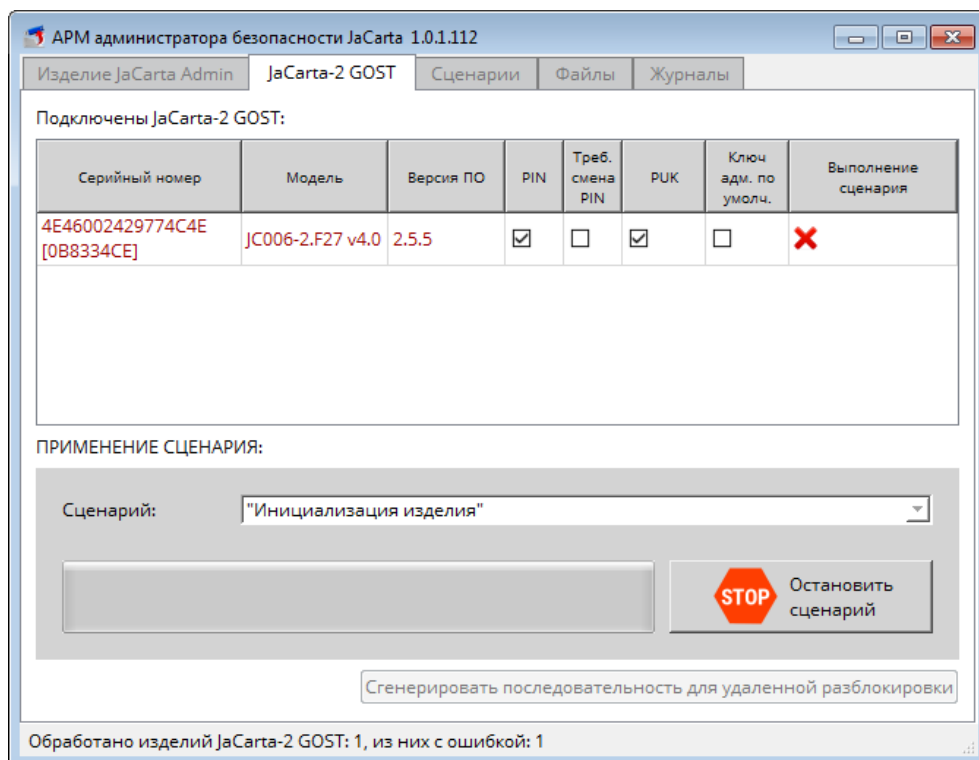


Рисунок 36 – Неудачное завершение применения сценария

- нажмите кнопку «Остановить сценарий» для завершения работы со сценарием.

### 5.13 Ввод изделий JaCarta-2 ГОСТ в эксплуатацию

При вводе изделий JaCarta-2 ГОСТ в эксплуатацию после выполнения требований правил пользования [1] выполните их инициализацию, смену паролей сброса к заводским настройкам и ключей администратора безопасности на значения, отличные от значений по умолчанию. Для этого подготовьте и выполните по отношению к каждому из таких изделий сценарии, содержащие операции INIT, SET\_PININIT и SET\_SO\_KEY (см. «Подготовка сценариев АРМ АБ», с. 40).

### 5.14 Генерация последовательности для удалённой разблокировки изделия JaCarta-2 ГОСТ

Перед началом генерации последовательности для удалённой разблокировки выясните у пользователя заблокированного изделия JaCarta-2 ГОСТ значение счётчика успешно выполненных разблокировок и полный серийный номер изделия JaCarta-2 ГОСТ.

Для генерации последовательности удалённой разблокировки изделия JaCarta-2 ГОСТ:

- нажмите кнопку «Сгенерировать последовательность для удалённой разблокировки» вкладки «JaCarta-2 ГОСТ» основного окна ПА (см. рисунок 37);

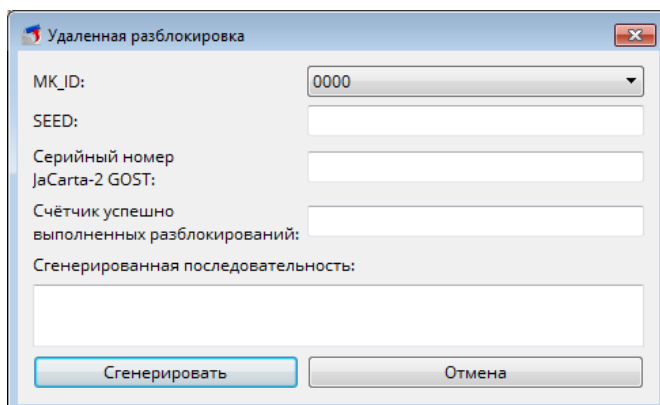


Рисунок 37 – Окно генерации последовательности для удалённой разблокировки

- выберите значение МК\_ID (краткий идентификатор ключа администрирования, использованного ранее при генерации ключа АБ изделия JaCarta-2 ГОСТ, см. описание операции SET\_SO\_KEY на с.42);
- введите значение дополнительного секрета SEED (если он был использован при генерации ключа АБ изделия JaCarta-2 ГОСТ, см. описание операции SET\_SO\_KEY на с.42), полученные у пользователя изделия JaCarta-2 ГОСТ полный серийный номер разблокируемого изделия JaCarta-2 ГОСТ и значение счётчика успешно выполненных разблокировок;
- нажмите кнопку «Сгенерировать».

Значение последовательности отобразится в текстовом поле (см. рисунок 38).

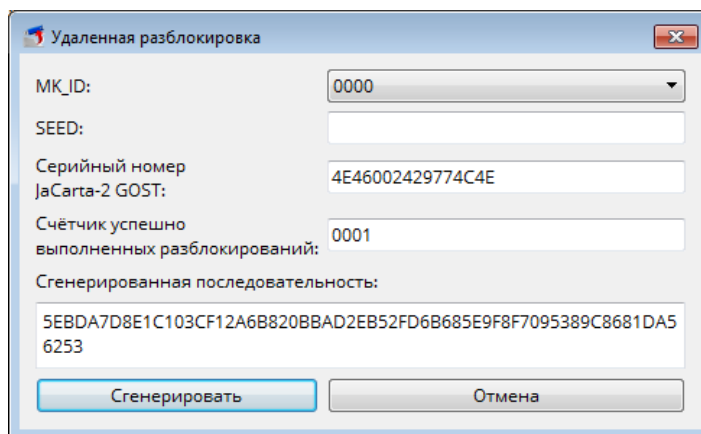



Рисунок 38 – Окно со сгенерированной последовательностью для удалённой разблокировки

## 5.15 Работа с файлами в базе данных

### 5.15.1 Загрузка файла в базу данных

Для загрузки файла в БД:

- откройте вкладку «Файлы» основного окна программы (рисунок 39);
- нажмите кнопку «Загрузить файл»  ;
- выберите файл для загрузки в БД и нажмите кнопку «Открыть»;
- проконтролируйте появление учётных данных загруженного файла (рисунок 39);

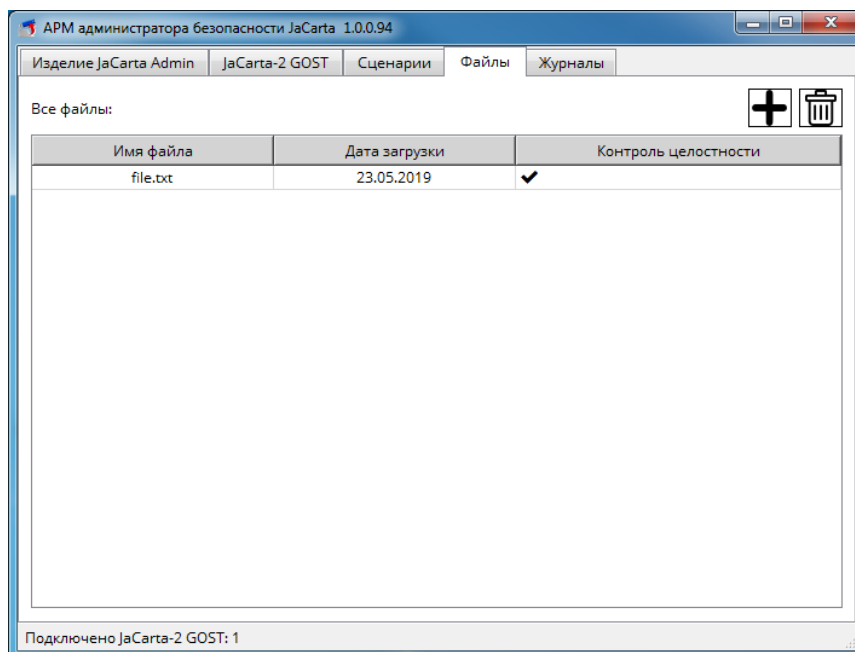



Рисунок 39 – Вкладка «Файлы»

#### 5.15.2 Удаление файла из базы данных

Для удаления файла из БД СКЗИ «АРМ АБ JaCarta»:

- откройте вкладку «Файлы» основного окна программы (см. рисунок 39);
- выберите необходимый файл;
- нажмите кнопку «Удалить файл» .

#### 5.16 Сброс изделия JaCarta-2 ГОСТ к заводским настройкам

Сброс изделия JaCarta-2 ГОСТ к заводским настройкам осуществляется при помощи файла сценария, содержащего операцию – INIT\_PIN с параметром PIN\_DATA. Значение параметра PIN\_DATA определено в качестве параметра PIN\_DATA операции SET\_PININIT в сценарии, с помощью которого было задано последнее значение PIN-кода сброса к заводским настройкам. Если операция SET\_PININIT ни разу не применялась, то PIN\_DATA=1234567890.

Сброс к заводским настройкам не затрагивает режим предъявления ключа администратора.

*Изделия JaCarta-2 ГОСТ с версией ПО 2.5.3 не поддерживают сброс к заводским настройкам. Версия ПО изделия JaCarta-2 ГОСТ отображается в поле «Версия ПО» на вкладке JaCarta-2 GOST основного окна ПА (см. рисунок 33).*

#### 5.17 Блокировка изделия JaCarta Admin

К блокировке изделия JaCarta Admin приводит ввод пароля, приведший к исчерпанию отведённых попыток ввода (см. с.17).

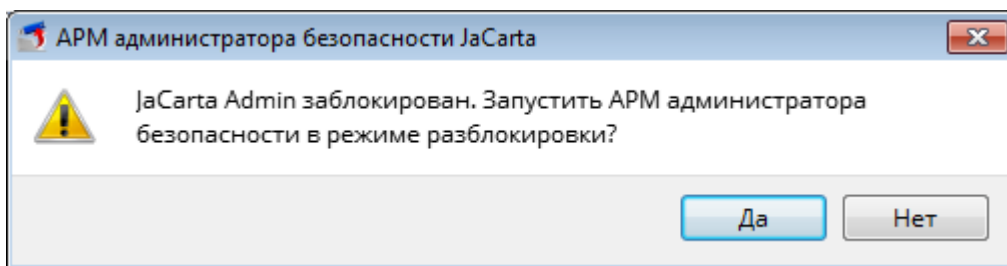


Рисунок 40 – Окно сообщения о блокировке изделия JaCarta Admin

## 5.18 Разблокировка изделия JaCarta Admin

Если оставшееся количество попыток ввода неверного пароля подряд равно нулю, PUK-код установлен и количество оставшихся попыток ввода неверного PUK-кода подряд не равно нулю, то доступна разблокировка изделия JaCarta Admin с помощью PUK-кода.

Для разблокировки изделий JaCarta Admin:

1. Запустите ПА и подключите заблокированное изделие JaCarta Admin.
2. Нажмите «Да» в окне сообщения о блокировке изделия JaCarta Admin (см. рисунок 40).
3. Введите PUK-код и нажмите кнопку «Разблокировать» или «Заккрыть» (при необходимости) (см. рисунок 41).

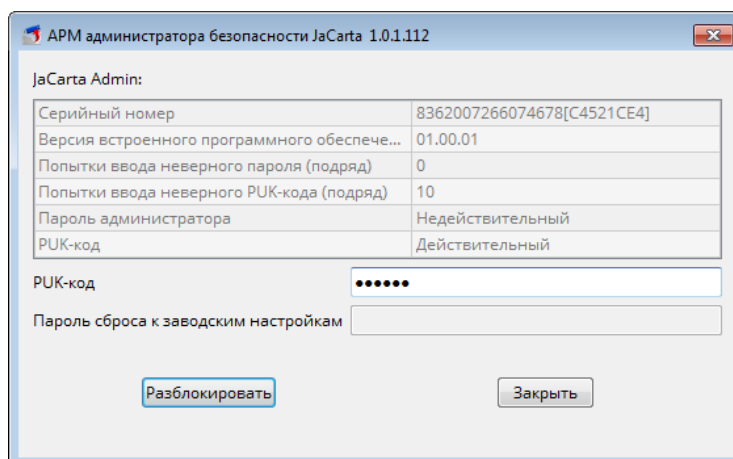


Рисунок 41 – Окно ввода PUK-кода

4. Нажмите кнопку **OK** (см. рисунок 42).

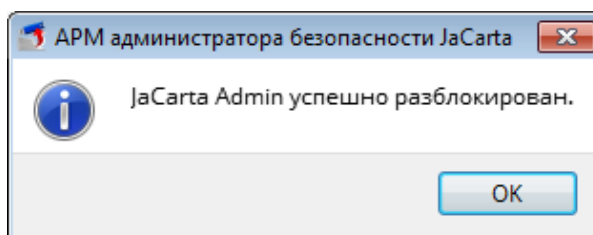


Рисунок 42 – Окно сообщения об успешной разблокировке изделия JaCarta Admin

При каждом неверном вводе значения PUK-кода значение счётчика PUK уменьшается на единицу. После разблокировки количество попыток ввода неверного пароля подряд и неверного PUK-кода подряд максимизируется.

## 5.19 Сброс изделия JaCarta Admin к заводским настройкам

Если оставшееся количество попыток ввода неверного пароля подряд равно нулю, а PUK-код не установлен, то доступен сброс к заводским настройкам.

Для сброса изделия JaCarta Admin к заводским настройкам:

1. Запустите ПА.
2. Подключите заблокированное изделие JaCarta Admin.
3. Введите пароль сброса (см. рисунок 43).

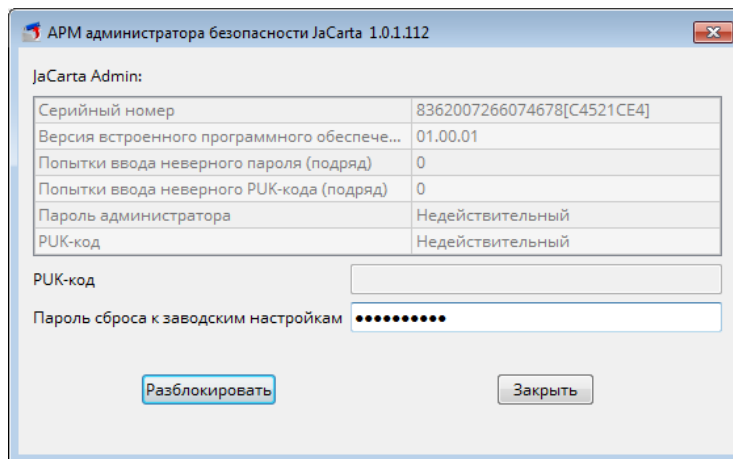


Рисунок 43 – Окно ввода пароля сброса изделия JaCarta Admin к заводским настройкам

4. Нажмите кнопку «Разблокировать» или «Закреть» (при необходимости).
5. Нажмите кнопку «Продолжить» или «Отмена» (при необходимости) (см. рисунок 44 и рисунок 45).

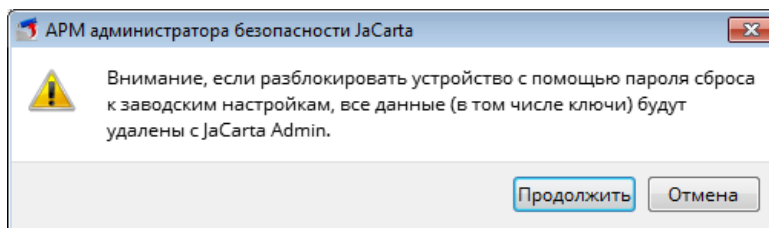


Рисунок 44 – Окно подтверждения сброса изделия JaCarta Admin к заводским настройкам

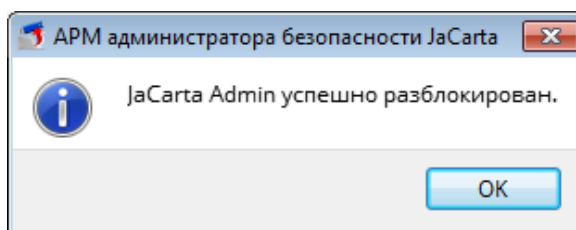


Рисунок 45 – Окно информирования о завершении сброса изделия JaCarta Admin к заводским настройкам

После сброса изделия JaCarta Admin к заводским настройкам необходимо создать новую базу данных (см. «Работа с файлом базы данных» на с. 21).

## 5.20 Завершение работы

Для завершения работы:

- дождитесь завершения выполняемых операций;
- закройте программу.

**|** *Не извлекайте изделия во время работы с ними.*

## 5.21 Резервирование данных

Резервирование данных ПА осуществляется путём создания резервной копии файла ct2.db (см. таблицу 1).

## 5.22 Удаление программы

При выводе СКЗИ «АРМ АБ JaCarta» из эксплуатации удалите папку, созданную при установке программы (с. 15).

## 6. Подготовка сценариев АРМ АБ

### 6.1 Структура файла сценария

Файл сценария — это текстовый файл, содержащий описание последовательности выполняемых операций АРМ АБ следующего вида:

```
[Settings]
SCRIPT_NAME="Название_сценария"
```

```
[Step00]
Action=LOGIN
MK_ID=
MK_SEED=
```

```
[Step01]
Action=ACTION1
Param1=Value1
...
ParamN=ValueM
```

```
[Step02]
Action=ACTION2
...
```

```
[Step99]
Action=LOGOUT
```

Файл сценария содержит одну секцию *[Settings]* и одну или несколько секций *[StepNN]*, где NN — номер секции, который принимает значения 00–99.

Каждая операция описывается в отдельной секции *[StepNN]*; для описания операции в секции должно быть указано обязательное поле Action, а также могут быть указаны поля дополнительных параметров. Операции выполняются в порядке возрастания номеров секций *[StepNN]*, начиная с номера 00 до последнего либо до первой некорректной операции. Пропуск и дублирование номеров не допускаются.

Файлы сценариев хранятся в БД на ЭВМ АРМ АБ.

### 6.2 Заголовок сценария

Секция *[Settings]* определяет название сценария, отображаемое в пользовательском интерфейсе ПА.

Параметр SCRIPT\_NAME — имя сценария, помещённое в кавычки.

Пример:

```
[Settings]
SCRIPT_NAME="Инициализация"
```



### 6.3 Операции администрирования изделий JaCarta-2 ГОСТ

1. LOGIN – начать сеанс работы с изделием JaCarta-2 ГОСТ: обновить внутреннее состояние ПДСЧ в изделии JaCarta-2 ГОСТ, установить защищённый канал (ЗК), проверить ключ администратора безопасности.

Параметры операции:

МК\_ID – полный или краткий идентификатор ключа администрирования, хранящегося в изделии JaCarta Admin. Является опциональным параметром: в случае если параметр не указан, для аутентификации в изделии JaCarta-2 ГОСТ используется ключ администратора безопасности по умолчанию (устанавливается в изделии JaCarta-2 ГОСТ при его производстве). Вместо идентификатора ключа в качестве значения параметра могут использоваться ключевые слова LATEST или ALL. При указании в качестве значения параметра МК\_ID ключевого слова LATEST будет использован ключ с наибольшим значением идентификатора. При указании в качестве значения параметра МК\_ID ключевого слова ALL операция LOGIN будет выполняться поочерёдно со всем существующими ключами администратора в изделии JaCarta Admin. Перебор ключей начинается с ключа с наибольшим значением идентификатора и останавливается в случае успешного выполнения операции либо после перебора всех ключей;

- МК\_SEED – дополнительный секрет диверсификации ключа АБ (в кодировке Base64), заданный при выполнении операции SET\_SO\_KEY. Опциональный параметр (допускается пустое значение параметра).

*Необходимо тщательно хранить значение параметра МК\_SEED. Если данный параметр был задан, то он становится обязательным.*

Пример:

```
[Step00]
Action=LOGIN
МК_ID=
МК_SEED=
```

2. LOGOUT – закрыть ЗК, завершить сеанс работы с изделием JaCarta-2 ГОСТ. Если операция LOGOUT в сценарии отсутствует, то после завершения сценария ЗК не разрывается.

Пример:

```
[Step10]
Action=LOGOUT
```

3. INIT – инициализировать изделие JaCarta-2 ГОСТ. Операция удаляет из используемой «Криптотокен 2 ЭП» памяти изделия JaCarta-2 ГОСТ все данные (объекты, файлы, PIN-коды пользователя и подписи, PUK-код и др.), кроме тех, которые были сохранены в процессе производства, внутреннего состояния ПДСЧ и ключа администратора безопасности. Кроме того, при выполнении этой операции PIN-код сброса к заводским настройкам приобретает значение по умолчанию.

Пример:

```
[Step01]
Action=INIT
```

4. INIT\_DEF – инициализировать изделие JaCarta-2 ГОСТ аналогично операции INIT и установить ключ администратора безопасности в значение по умолчанию с предъявлением в открытом виде.

Пример:

```
[Step01]
```

```
Action=INIT_DEF
```

5. INIT\_PIN – инициализировать изделие JaCarta-2 ГОСТ и сбросить к заводским настройкам при предъявлении PIN-кода сброса к заводским настройкам, где PIN\_DATA – значение PIN-кода сброса к заводским настройкам. Для успешного выполнения этой операции не должно быть установленного ЗК с изделием JaCarta-2 ГОСТ (если к изделию JaCarta-2 ГОСТ была успешно применена команда LOGIN, после неё и перед операцией IT\_PIN должна быть успешно применена операция LOGOUT).

Пример:

```
[Step00]
```

```
Action=INIT_PIN
```

```
PIN_DATA=z"~tFqB5LQIEe^&wucV+
```

6. SET\_SO\_KEY – сменить ключ администратора безопасности.

Параметры операции:

MK\_ID – полный или краткий идентификатор ключа администрирования, хранящегося в изделии JaCarta Admin, используемого для выработки нового ключа АБ. Кроме того, в качестве значения параметра MK\_ID помимо идентификатора ключа может быть использовано ключевое слово LATEST. В этом случае будет использован ключ с наибольшим значением идентификатора;

- MK\_SEED – дополнительный секрет диверсификации ключа АБ (значение в кодировке Base64). Опциональный параметр (допускается пустое значение параметра). Значение параметра применяется в операции LOGIN;
- MK\_SM – флаг, определяющий режим предъявления ключа администратора (00 – в открытом виде, 01 – требуется установка защищённого канала).

Пример:

```
[Step01]
```

```
Action=SET_SO_KEY
```

```
MK_ID=4E460024462850460000
```

```
MK_SM=01
```

```
MK_SEED=
```

7. SET\_PIN – установить PIN-код пользователя.

Параметр операции: PIN\_DATA – значение PIN-кода, текстовая строка длиной от 6 до 32 символов в кодировке Windows-1251 (в строке не должны использоваться непечатные символы с кодами 00h–1Fh и 7Fh).

Пример:

```
[Step03]
```

```
Action=SET_PIN
```

```
PIN_DATA=AZ<!3cpj6e
```

8. SET\_PUK – установить PUK-код.

Параметр операции: PUK\_DATA – значение PUK-кода, текстовая строка длиной от 6 до 32 символов в кодировке Windows-1251 (в строке не должны использоваться непечатные символы с кодами 00h–1Fh и 7Fh).

Пример:

```
[Step04]
Action=SET_PUK
PUK_DATA=tFea7s5SAC6eyCs:{f
```

9. SET\_PININIT – установить PIN-код сброса к заводским настройкам.

Параметр операции: PIN\_DATA – значение PIN-кода сброса к заводским настройкам, текстовая строка длиной от 6 до 32 символов в кодировке Windows-1251 (в строке не должны использоваться непечатаемые символы с кодами 00h–1Fh и 7Fh).

Пример:

```
[Step05]
Action=SET_PININIT
PIN_DATA=z"~tFqB5LQIEe^&wucV+
```

10. UNBLOCK – разблокировать изделие JaCarta-2 ГОСТ (выполняет разблокирование PIN-кода пользователя, PIN-кода подписи и PUK-кода изделия JaCarta-2 ГОСТ).

Пример:

```
[Step01]
Action=UNBLOCK
```

11. SET\_PASSWORD\_POLICY – установить парольную политику.

Параметр операции: DATA – двухбайтовое значение, задающее тип PIN-кода и соответствующую парольную политику.

Параметр имеет следующий формат:

- 1 байт – тип PIN-кода:
  - 02h – PIN-код пользователя;
  - 03h – PIN-код подписи;
- 1 байт – битовая структура, определяющая парольную политику:
  - b7–b5 – приращение минимальной длины кода (в зависимости от значения этих битов минимальная длина может составлять от 6 до 13 символов);
  - b4 – необходимость смены PIN-кода;
  - b3 – обязательное наличие специальных символов (!, \$, #, % и др. символов, коды которых находятся в диапазонах 20h–2Fh, 3Ah–40h, 5Bh–60h и 7Bh–7Eh);
  - b2 – обязательное наличие цифр (от 0 до 9, т.е. символов, коды которых находятся в диапазоне 30h–39h);
  - b1 – обязательное наличие строчных букв (от a до z или от а до я в кодировке Windows-1251, т.е. символов, коды которых находятся в диапазонах 61h–7Ah и E0h–FFh);
  - b0 – обязательное наличие прописных букв (от A до Z или от А до Я в кодировке Windows-1251, т.е. символов, коды которых находятся в диапазонах 41h–5Ah и C0h–DFh).

Значение параметра представляется в шестнадцатеричном виде текстовой строкой.

Пример:

```
[Step04]
Action=SET_PASSWORD_POLICY
DATA=0254
```

## 12. GENERATE\_KEY\_PAIR – сгенерировать собственную ключевую пару изделия JaCarta-2 ГОСТ<sup>1</sup>.

Параметры операции:

- KEYA – двухбайтовое значение, задающее алгоритм и параметры электронной подписи (ЭП) в следующем формате:
  - 1 байт – алгоритм, по которому следует выполнять преобразования с использованием генерируемой ключевой пары. Допустимые значения:
    - 01h – ЭП по ГОСТ Р 34.10-2001 [3];
    - 02h – ЭП по ГОСТ Р 34.10-2012 [4] с длиной хэша 256 бит;
  - 1 байт – параметры криптографических преобразований. Допустимое значение: 01h (т.е. набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet и id-GostR3410-2001-CryptoPro-XchA-ParamSet [3]).

Значение параметра представляется в шестнадцатеричном виде текстовой строкой.

Пример:

[Step09]

Action=GENERATE\_KEY\_PAIR

KEYA=0201

## 13. IMPORT\_PUBLIC\_KEY – импортировать открытый ключ.

Параметры операции:

- KEYA – двухбайтовое значение, задающее алгоритм и параметры электронной подписи (ЭП) в следующем формате:
  - 1 байт – стандарт, по которому следует выполнять преобразования с импортируемым ключом. Допустимые значения:
    - 01h – ГОСТ Р 34.10-2001 [3];
    - 02h – ГОСТ Р 34.10-2012 [4] с длиной хэш-кода 256 бит;
  - 1 байт – параметры криптографических преобразований. Допустимое значение: 01h (т.е. набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet и id-GostR3410-2001-CryptoPro-XchA-ParamSet [3]).

Если определён параметр CERTIFICATE, то параметр KEYA должен отсутствовать.

Значение параметра представляется в шестнадцатеричном виде текстовой строкой.

- CVERIFY – признак разрешения проверки сертификата импортируемым открытым ключом (область использования открытого ключа включает проверку подписи сертификата [5]):
  - CVERIFY=01 – проверка сертификата разрешена;
  - CVERIFY=00 – проверка сертификата запрещена (значение по умолчанию).

При отсутствии параметра CVERIFY проверка сертификата импортируемым ключом запрещается.

*Запрещается устанавливать признак разрешения проверки сертификата для открытого ключа, область использования которого не включает проверку подписи сертификата [5].*

---

<sup>1</sup> Собственная ключевая пара изделия JaCarta-2 ГОСТ предназначена для использования при построении защищённого канала между изделием JaCarta-2 ГОСТ и терминалом другими СКЗИ, использующими компоненты СКЗИ «Криптотокен 2 ЭП». Эта ключевая пара имеет идентификатор 00h.

- DATA – открытый ключ в явном виде (конкатенация координат x|y, представленных в порядке следования байтов от младшего к старшему, little-endian). 64-байтовое значение в шестнадцатеричном представлении. Поле не указывается, если указано поле CERTIFICATE;
- CERTIFICATE – имя файла сертификата открытого ключа в базе данных на жёстком диске ЭВМ АРМ АБ. При наличии поля DATA поле CERTIFICATE игнорируется.

Из указанного сертификата извлекаются следующие сведения:

- стандарт и параметры криптографических преобразований с открытым ключом;
- признак разрешения проверки сертификата открытым ключом;
- значение открытого ключа.

*Используемый сертификат должен быть проверен сторонними программно-аппаратными средствами до его загрузки в ЭВМ АРМ АБ.*

*Стандарт и параметры криптографических преобразований с открытым ключом должны соответствовать одному из вариантов, приведённых выше в описании параметра KEYA.*

*Признак разрешения проверки сертификата ключом, импортируемым из сертификата применяется только при одновременном выполнении следующих условий:*

- CVERIFY=01;
- поле TBSCertificate сертификата содержит поле Version, и это поле имеет значение 3;
- в сертификате имеется расширение Key Usage (OID 2.5.29.15), разрешающее проверку подписи под сертификатами (keyCertSign, «подписывание сертификатов»).

Пример:

[Step07]

Action=IMPORT\_PUBLIC\_KEY

CVERIFY=01

CERTIFICATE=test.cer

или

[Step07]

Action=IMPORT\_PUBLIC\_KEY

KEYA=0101

DATA=E2D5BC32C5416D0BABAACD214197FB09B7A6323841C46715DADAB2A6A3ADC7BC03589C24  
FF42CB85EB3A01D48BA40F13BA229EA43FD1B81DD210E595DC426ECD7

14. IMPORT\_SECRET\_KEY – импортировать в изделие JaCarta-2 ГОСТ ключ для HMAC.

Параметры операции:

- МК\_ID – полный или краткий идентификатор ключа для HMAC в изделии JaCarta Admin;
- HMAC – флаг вида «HMAC=01» или «HMAC=00». При установке флага в 01, импортируемый в изделии JaCarta-2 ГОСТ ключ для HMAC вычисляется путём диверсификации входного ключа для HMAC. Если флаг не равен 01, а также при отсутствии данного поля, импортируемым ключом является входной ключ для HMAC.

Пример:

```
[Step02]
Action=IMPORT_SECRET_KEY
МК_ID=0001
HMAC=01
```

15. DELETE\_KEY – удалить ключ.

Параметр операции: DATA – 2-байтовое значение с идентификационными данными ключа.

Имеет следующий формат:

- 1 байт – тип ключа. Допустимые значения:
  - 01h – доверенный открытый ключ;
  - 02h – секретный ключ.
- 1 байт – идентификатор ключа (1-255).

Значение параметра представляется в шестнадцатеричном виде текстовой строкой.

Пример:

```
[Step08]
Action=DELETE_KEY
DATA=0101
```

16. WRITE\_SERVICE\_INFO – записать служебную информацию в изделие JaCarta-2 ГОСТ.

Параметры операции:

- TAG – тип служебной информации, которую следует записать. Указывается одним байтом в шестнадцатеричном представлении. Допустимые значения:
  - 01 – записать метку изделия JaCarta-2 ГОСТ;
  - 08 – записать значения параметров стороны В, используемых для установки защищённого канала по протоколу [5];
  - 09 – записать настройки задержек по времени при разблокировании PIN-кодов и PUK-кода;
  - 0A – записать настройки APDU-ответа на команду выбора апплета
- DATA – данные служебной информации. Указываются последовательностью байтов в шестнадцатеричном представлении. В зависимости от значения параметра TAG данные служебной информации должны содержать:
  - При TAG = 01: значение новой метки изделия JaCarta-2 ГОСТ – последовательность длиной 1–20 байтов, представленных в шестнадцатеричном виде текстовой строкой (для обеспечения совместимости с программным обеспечением «Аладдин Р. Д.» при записи метки изделия JaCarta-2 ГОСТ рекомендуется использовать шестнадцатеричные представления символов, соответствующие кодировке Windows-1251);
  - При TAG = 08: значения новых параметров стороны В, используемых для установки защищённого канала по протоколу [5]:
    - 4 байта – значение IDB;
    - 1 байт – значение ind;
    - 16 байт – значение salt;
    - 64 байта – значение QPW.
  - При TAG = 09 – количество раз, которое надо выполнить команду «Разблокировать» (для обеспечения необходимой длительности задержки процесса разблокирования):
    - 2 байта: для разблокирования PIN-кода пользователя;
    - 2 байта: для разблокирования PIN-кода подписи;
    - 2 байта: для разблокирования PUK-кода
  - При TAG = 0A – битовая структура со следующими значениями битов:
    - b7–b1 – зарезервированы;
    - b0 – настройки APDU-ответа на команду выбора апплета:
      - 0 – не включать информацию об изделии JaCarta-2 ГОСТ в APDU-ответ на команду выбора апплета;
      - 1 – включать информацию об изделии JaCarta-2 ГОСТ в APDU-ответ на команду выбора апплета.

Пример:

[Step06]

Action=WRITE\_SERVICE\_INFO

TAG=0A

DATA=01

17. SELECT\_FILE – выбрать файл или папку в изделии JaCarta-2 ГОСТ.

Параметры операции:

- NAME – полный путь к файлу или папке в соответствии с приложением 1 («Файловая система изделия», с. 85).

Пример:

```
[Step05]
Action=SELECT_FILE
NAME=e00ef001
```

18. CREATE\_DIR – создать папку в текущей папке в изделии JaCarta-2 ГОСТ.

Текущая папка должна быть предварительно выбрана с помощью операции SELECT\_FILE.

Параметры операции:

- NAME – 2-байтовое значение идентификатора папки в соответствии с приложением 1 («Файловая система изделия», с. 85);
- AC – права доступа к папке (два байта в шестнадцатеричном представлении, формат см. в приложении 1 «Файловая система изделия», с. 85).

Пример:

```
[Step02]
Action=CREATE_DIR
NAME=e00e
AC=0db7
```

19. DELETE\_FILE – удалить файл (файл данных или папку) в изделии JaCarta-2 ГОСТ. Удаляет файл, выбранный предварительно с помощью операции SELECT\_FILE.

Пример:

```
[Step06]
Action=DELETE_FILE
```

20. CHANGE\_ACCESS – изменить настройки прав доступа к выбранному файлу (файлу данных или папке) в изделии JaCarta-2 ГОСТ. Файл должен быть предварительно выбран с помощью операции SELECT\_FILE.

Параметр операции: AC – права доступа к файлу или папке (два байта в шестнадцатеричном представлении, формат двухбайтового слова см. в приложении 1 «Файловая система изделия», с. 85).

Пример:

```
[Step05]
Action=CHANGE_ACCESS
AC=0db7
```



21. CREATE\_FILE – создать файл данных в текущей папке в изделии JaCarta-2 ГОСТ. Текущая папка должна быть предварительно выбрана с помощью операции SELECT\_FILE.

Параметры операции:

- DATA – данные для файла (бинарные данные в кодировке Base64 [2]);  
или
- FNAME – имя файла с бинарными данными в БД на жёстком диске ЭВМ АРМ АБ. При наличии поля DATA поле FNAME игнорируется;
- NAME – 2-байтовое значение идентификатора файла в соответствии с в приложении 1 «Файловая система изделия», с. 85;
- AC – права доступа к файлу (два байта в шестнадцатеричном представлении, формат см. приложение 1 «Файловая система изделия», с. 85).

Пример:

[Step04]

```
Action=CREATE_FILE
FNAME=test_notes.txt
NAME=f001
AC=0db7
```

Или

[Step04]

```
Action=CREATE_FILE
DATA=RbQ0lnLmRbI=
NAME=f001
AC=0db7
```

22. WRITE\_FILE – записать данные в выбранный файл в изделии JaCarta-2 ГОСТ. Файл должен быть предварительно выбран с помощью операции SELECT\_FILE.

Параметры операции:

- Содержимое для записи:
  - DATA – данные для файла (бинарные данные в кодировке Base64 [2]);  
или
  - FNAME – имя файла с бинарными данными в БД на жёстком диске ЭВМ АРМ АБ. При наличии поля DATA поле FNAME игнорируется;
- OFFSET – смещение от начала файла в изделии JaCarta-2 ГОСТ в байтах 0000h–7FEFh (2-байтовое значение в шестнадцатеричном представлении).

Пример:

[Step06]

```
Action=WRITE_FILE
DATA=0JHRg9C00YzRgtC1INGB0YfQsNGB0YLQu9C40LLRiyE=
```

Сумма смещения и длины записываемых данных не должна превышать величину размера файла.

23. READ\_FILE – прочитать данные из выбранного файла в изделии JaCarta-2 ГОСТ и записать их в журнал операций с изделием JaCarta-2 ГОСТ (с. 55). Файл должен быть предварительно выбран с помощью операции SELECT\_FILE. Данные будут записаны в кодировке Base 64 [2].

Параметры операции:

- OFFSET – смещение от начала файла в изделии JaCarta-2 ГОСТ 0000h–7FEDh (двухбайтовое значение в шестнадцатеричном представлении) – необязательный параметр, при его отсутствии файл считывается с начала;
- LENGTH – длина фрагмента данных, считаемых из файла в изделии JaCarta-2 ГОСТ – необязательный параметр; при его отсутствии файл считывается до конца.

Пример:

[Step06]

Action=READ\_FILE

OFFSET=0009

LENGTH=0040

Образцы сценариев приведены в приложении 2 («Примеры сценариев операций», с. 87).

## 6.4 Создание файла сценария

Для создания файла сценария:

- откройте вкладку «Сценарии» основного окна ПА (см. рисунок 46);

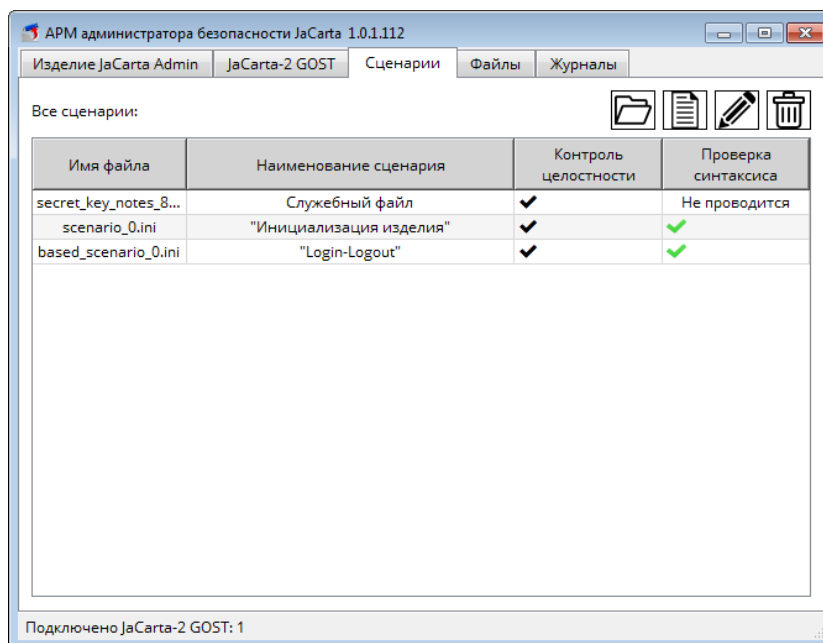



Рисунок 46 – Окно перечня файлов сценариев

- нажмите кнопку «Создать новый сценарий»  ;

- введите текст сценария в открывшемся окне (см. рисунок 47);

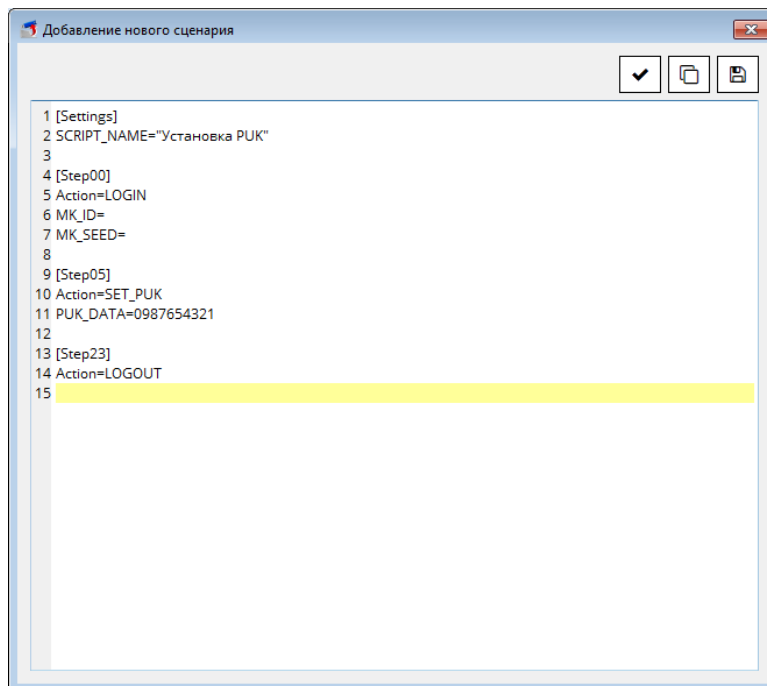


Рисунок 47 – Окно сценария

- нажмите кнопку «Проверить сценарий»  для проверки синтаксиса сценария. При наличии ошибок будет появляться окно сообщения с информацией об ошибке (см. п. 8.2).

В этом случае следует:

- нажимать кнопку **OK** окна сообщения с информацией об ошибке;
- устранять ошибки;
- выполнять повторные проверки синтаксиса сценария до появления сообщения: «Сценарий успешно прошёл проверку синтаксиса» (см. рисунок 48);

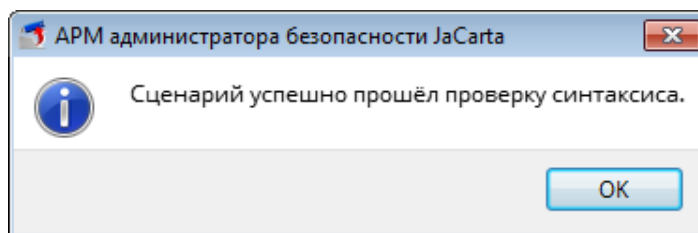



Рисунок 48 – Окно сообщения об успешном завершении проверки синтаксиса

- нажмите кнопку «Сохранить сценарий»  для сохранения файла сценария;
- введите имя файла сценария в окне «Сохранить сценарий» и нажмите ОК (см. рисунок 49).

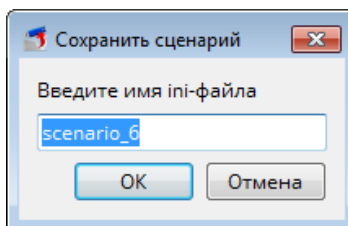


Рисунок 49 – Окно ввода имени файла сценария




## 6.5 Проверка синтаксиса сценария

Проверка синтаксиса происходит:

- при нажатии кнопки «Проверить синтаксис»  вкладки «Сценарии» основного окна ПА;
- старте ПА;
- сохранении файла сценария;
- загрузке шаблона сценария;


нажатии кнопки «Применить сценарий» вкладки JaCarta-2 GOST основного окна ПА.

Для проверки синтаксиса сценария:

1. Откройте вкладку «Сценарии» основного окна ПА.
2. Выберите необходимый сценарий.
3. Откройте сценарий для редактирования путём нажатия кнопки «Редактировать сценарий» .
4. Нажмите кнопку «Проверить синтаксис» .
5. Устраните ошибки при необходимости.
6. Сохраните сценарий путём нажатия на кнопку «Сохранить сценарий» .



*ПА не позволяет применять сценарии с некорректным синтаксисом и не отображает их в списке, используемом при выборе сценария для применения (см. «Администрирование изделий JaCarta-2 ГОСТ», с. 32).*

Автоматически создаваемые при генерации ключей HMAC (см. «Генерация ключа для HMAC» на с. 27) сценарии не требуют проверки синтаксиса.

Проверка синтаксиса таких сценариев возможна только при нажатии кнопки .


## 6.6 Редактирование сценария

Для редактирования сценария:

- откройте вкладку «Сценарии» основного окна ПА;
- выберите сценарий;
- нажмите кнопку «Редактировать сценарий»  основного окна ПА;
- редактируйте сценарий;
- нажмите кнопку «Сохранить сценарий»  для сохранения файла сценария.

## 6.7 Удаление сценария

Для удаления сценария:

- откройте вкладку «Сценарии» основного окна ПА;
- выберите сценарий (допускается удаление только одного сценария за раз);
- нажмите кнопку «Удалить сценарий»  основного окна ПА;
- нажмите кнопку **ОК**;

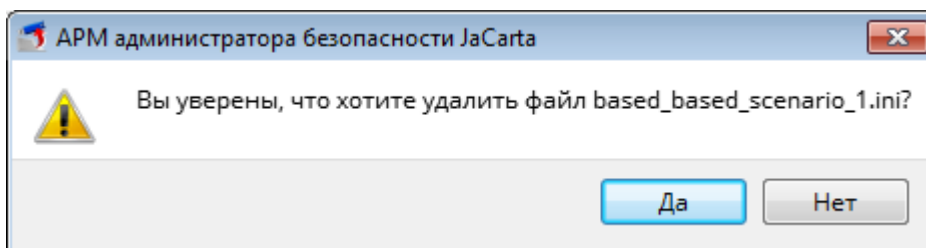


Рисунок 50 – Окно подтверждения удаления файла

## 6.8 Создание шаблона сценария

Шаблон сценария представляет из себя текстовый файл с расширением ini, который может быть загружен в БД ПА и использован для подготовки сценариев администрирования.

Для создания шаблона сценария:

- откройте любой текстовый редактор;
- наберите необходимый текст в кодировке Windows-1251;
- сохраните файл с расширением ini.

## 6.9 Загрузка шаблона сценария

Для загрузки шаблона сценария в БД ПА:

- откройте вкладку «Сценарии» основного окна ПА;
- нажмите кнопку «Загрузить шаблон сценария»;
- выберите необходимый шаблон сценария (см. рисунок 51) и нажмите кнопку «Открыть»;

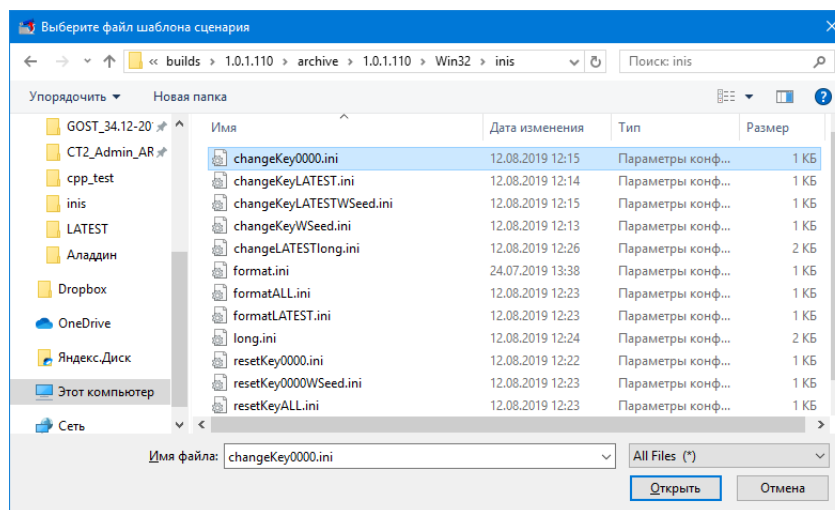


Рисунок 51 – Окно выбора сценария

- Нажмите кнопку «ОК».

## 6.10 Автоматическая загрузка шаблонов сценариев

Для автоматической загрузки шаблонов сценариев в БД ПА:

- запустите интерпретатор командной строки;
- запустите исполняемый файл ПА с параметром `-scriptLoad` и указанным в кавычках шаблоном абсолютных или относительных полных имён тех файлов шаблонов сценариев, которые должны быть загружены (см. рисунок 52);

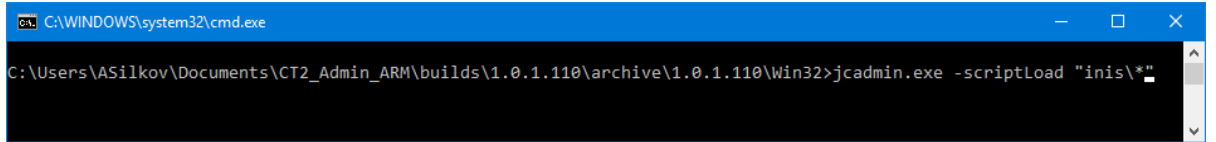


Рисунок 52 – Окно запуска ПА с автоматической загрузкой сценариев

- введите пароль администратора изделия JaCarta Admin и нажмите «ОК»;
- нажмите «ОК» для завершения работы с ПА.

## 7. Журналы

ПА ведёт следующие журналы:

- JaCarta GOST – журнал операций с изделием JaCarta-2 ГОСТ;
- «Выполненные сценарии» – журнал выполненных сценариев;
- «Брак» – журнал ошибок;
- JaCarta Admin – журнал операций с изделием JaCarta Admin.

Для просмотра необходимого журнала:


- откройте соответствующую вкладку основного окна ПА;
- выберите желаемый журнал для просмотра.

Журналы создаются для каждого изделия JaCarta-2 ГОСТ и изделия JaCarta Admin отдельно.

Журналы операций с изделием JaCarta-2 ГОСТ, выполненных сценариев и ошибок располагаются в папках с именами, совпадающими с полными серийными номерами администрируемых изделий JaCarta-2 ГОСТ. Имя каждого из этих журналов состоит из полного идентификатора ключа базы данных.

Для поиска журналов, относящихся к определённому изделию JaCarta-2 ГОСТ, необходимо ввести значение полного серийного номера изделия JaCarta-2 ГОСТ в текстовое поле и нажать кнопку «Фильтр».

Ошибки, возникающие при работе с изделием JaCarta-2 ГОСТ, которые невозможно связать ни с одним изделием JaCarta-2 ГОСТ, помещаются в журнал UNKNOWN.

Просмотр журнала, созданного для неиспользуемого в текущем сеансе работы изделия JaCarta Admin, невозможен. Недоступные для просмотра журналы помечаются символом .

При ошибке доступа к журналу (например, в результате повреждения) создаётся новый журнал с именем, образованным путём добавления увеличивающегося суффикса к прежнему имени. Например, вместо 4E460017662550470000\_20190417 создаётся журнал 4E460017662550470000\_20190417\_1.

### 7.1 Журнал операций с изделием JaCarta-2 ГОСТ

Для просмотра журнала:

1. Откройте вкладку JaCart2 GOST вкладки «Журналы» основного окна ПА.
2. Выберите необходимый журнал (см. рисунок 53).

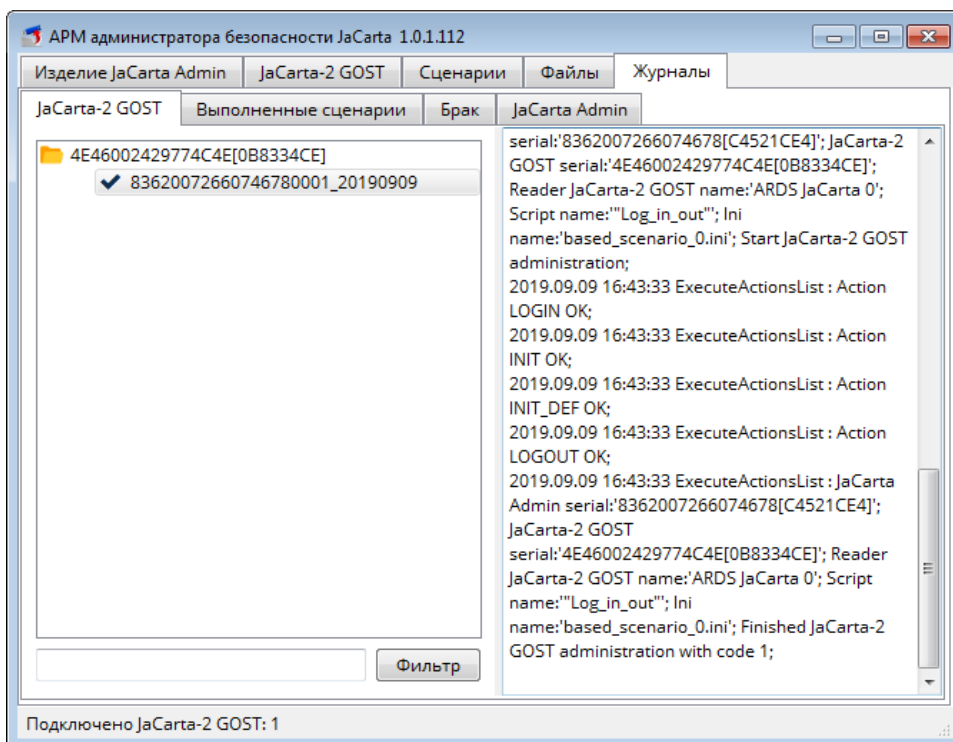


Рисунок 53 – Отображение журнала операций с изделием JaCarta-2 ГОСТ

При каждом выполнении сценария в журнале операций над изделием JaCarta-2 ГОСТ фиксируется:

- дата и время начала выполнения сценария;
- полный и краткий серийные номера изделия JaCarta Admin (JaCarta Admin serial);
- полный и краткий серийные номера администрируемого изделия JaCarta-2 ГОСТ (JaCarta-2 GOST serial);
- имя устройства чтения смарт-карт администрируемого изделия JaCarta-2 ГОСТ (Reader JaCarta-2 GOST name);
- имя сценария (Script name);
- имя файла сценария (Ini name);
- тип выполняемых действий (Start JaCarta-2 GOST administration);
- выполняемые операции:
  - дата и время выполнения операции;
  - полный и краткий серийные номера администрируемого изделия JaCarta-2 ГОСТ;
  - название операции (Action);
  - результат выполнения (**OK** или «failed with code -1»);
  - или (для операций, имеющих дополнительные (не указываемые в сценарии) параметры, вырабатываемые автоматически в ходе выполнения сценария)
  - дата и время выработки дополнительных параметров операции;
  - название операции (Action);
  - полный и краткий серийные номера администрируемого изделия JaCarta-2 ГОСТ;

<sup>1</sup> Сообщение failed with code -1 означает, что операция не была выполнена.



- названия и значения дополнительных параметров операции;
- дата и время выполнения операции;
- полный и краткий серийные номера администрируемого изделия JaCarta-2 ГОСТ;
- название операции (Action);
- результат выполнения (**OK** или «failed with code -1»);
- дата и время завершения выполнения сценария;
- сообщение и завершении администрирования изделия JaCarta-2 ГОСТ (Finished JaCarta-2 GOST administration with code 1)<sup>1</sup>.

## 7.2 Журнал выполненных сценариев

Для просмотра журнала:

1. Откройте вкладку «Выполненные сценарии» вкладки «Журналы» основного окна ПА.
2. Выберите необходимый журнал (см. рисунок 54).

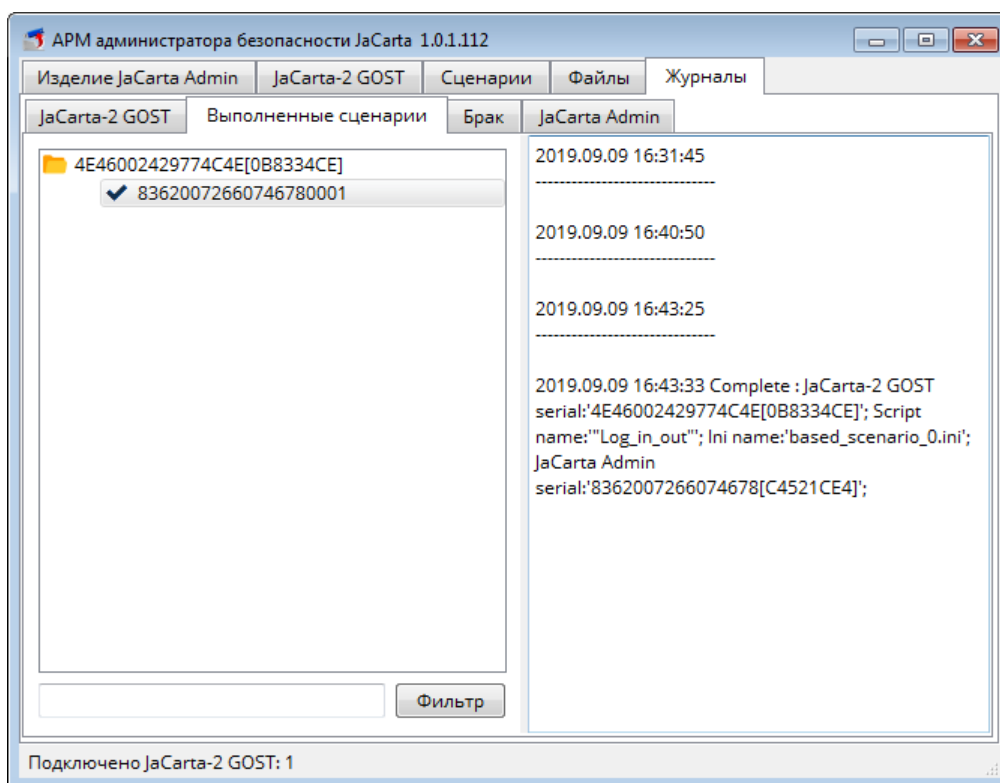


Рисунок 54 – Отображение журнала выполненных сценариев

При каждом успешном выполнении сценария администрирования изделия JaCarta-2 ГОСТ в журнале выполненных сценариев фиксируется:

- дата и время завершения выполнения сценария;
- полный и краткий серийные номера администрируемого изделия JaCarta-2 ГОСТ;
- имя выполненного сценария;
- полный и краткий серийные номера изделия JaCarta Admin.

<sup>1</sup> Только для случая успешного завершения сценария. Сообщение Finished JaCarta-2 GOST administration with code 1 означает, что сценарий выполнен полностью (выполнены все операции сценария).

### 7.3 Журнал ошибок

Для просмотра журнала:

1. Откройте вкладку «Брак» вкладки «Журналы» основного окна ПА.
2. Выберите необходимый журнал (см. рисунок 55).

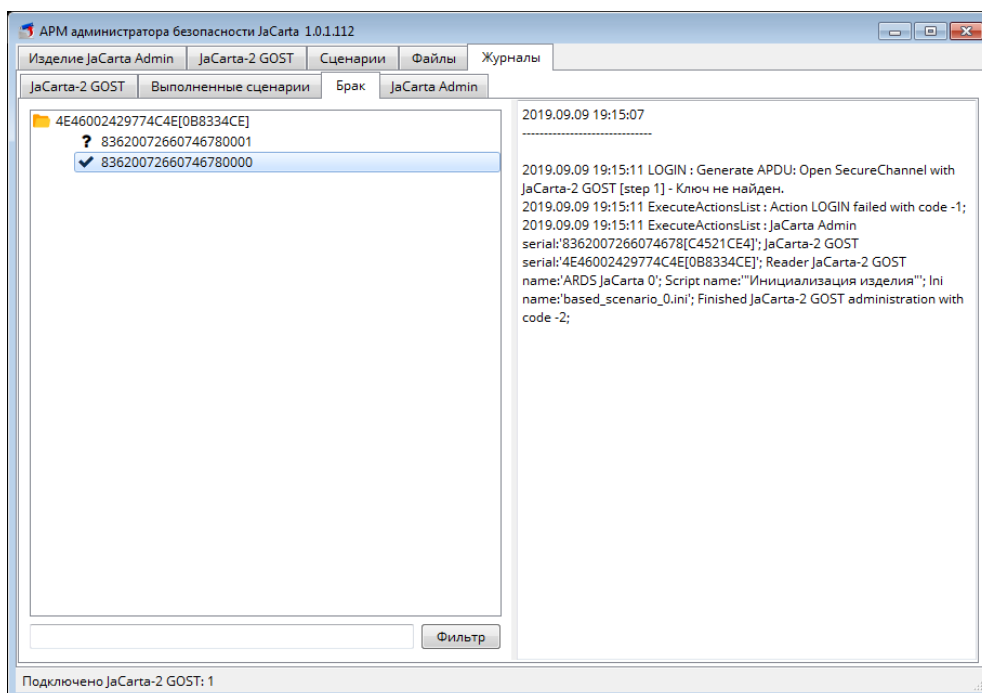


Рисунок 55 – Отображение журнала ошибок

В журнале ошибок фиксируется:

- дата и время ошибки;
- имя операции, вызвавшей ошибку (если ошибка вызвана выполнением операции сценария администрирования, в противном случае вместо имени операции будет находиться надпись «ExecuteActionsList»);
- описание ошибки.

### 7.4 Журнал операций с изделием JaCarta Admin

Журналы операций с изделием JaCarta Admin располагаются в папках с именами, соответствующими году, числу и месяцу создания этих журналов. Имя журнала операций с изделием JaCarta Admin состоит из краткого серийного номера изделия JaCarta Admin, полного идентификатора ключа базы данных и даты создания журнала.

Для просмотра журнала операций с изделием:

1. Откройте вкладку JaCarta Admin вкладки «Журналы» основного окна ПА.
2. Выберите необходимый журнал (см. рисунок 56).

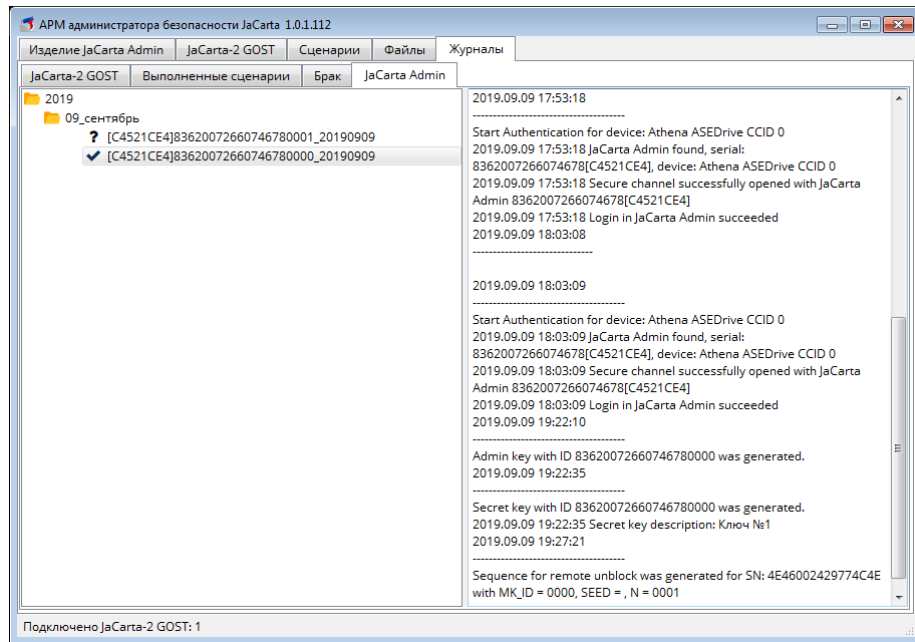


Рисунок 56 – Отображение журнала операций с изделием JaCarta Admin

В журнале операций с изделием JaCarta Admin фиксируется:

- дата и время проведения операции;
- сведения об операции.

## 8. Сообщения оператору

### 8.1 Сообщения строки состояния

Сообщения строки состояния ПА приведены в таблице 2.

Таблица 2 – Сообщения строки состояния ПА

Текст сообщения	Описание
"Подключено JaCarta-2 GOST: «Количество подключённых изделий JaCarta-2 ГОСТ»"	По умолчанию в строке состояний отображается количество подключённых в текущий момент времени изделий JaCarta-2 ГОСТ
"Подключите изделие JaCarta Admin"	Сообщение отображается при старте программы либо при извлечении изделия JaCarta Admin
"Открытие базы данных..."	Сообщение отображается в процессе открытия базы данных
"Генерация ключа администрирования..."	Сообщение отображается в процессе генерации ключа администрирования в изделии JaCarta Admin
"Генерация ключа базы данных..."	Сообщение отображается в процессе генерации ключа базы данных в изделии JaCarta Admin
"Генерация ключа для НМАС"	Сообщение отображается в процессе генерации ключа для НМАС в изделии JaCarta Admin и добавления описания ключа в базу данных
"Импорт ключа для НМАС"	Сообщение отображается в процессе импорта ключа для НМАС в изделие JaCarta Admin и добавления описания ключа в базу данных
"Экспорт ключа для НМАС"	Сообщение отображается в процессе экспорта ключа для НМАС из изделия JaCarta Admin и сохранения ключа в файл-контейнер
"Проверка сценария..."	Сообщение отображается в процессе проверки сценария, перед непосредственным применением сценария к изделию JaCarta-2 ГОСТ
"Обработано JaCarta-2 GOST: «Количество обработанных изделий JaCarta-2 ГОСТ», из них с ошибкой: «Количество изделий JaCarta-2 ГОСТ, обработанных с ошибкой»"	Сообщение начинает отображаться при старте применения сценария
"Генерация последовательности удаленной разблокировки..."	Сообщение отображается в процессе генерации последовательности для удалённого разблокирования
"Обновление списка журналов..."	Сообщение отображается при обновлении списка журналов
"Обнаружено изделие JaCarta Admin. Аутентификация..."	Сообщение отображается при обнаружении изделия JaCarta Admin и старте процесса аутентификации (получение информации об изделии JaCarta Admin, ввод пароля)

Текст сообщения	Описание
	Сообщение отображается в процессе подготовки механизма защиты ключей, хранящихся в памяти изделия JaCarta Admin, к использованию, в том числе при смене пароля изделия JaCarta Admin по умолчанию
"Обнаружено изделие JaCarta Admin. Открытие защищенного канала..."	Сообщение отображается в процессе построения защищённого канала с изделием JaCarta Admin
"Обнаружено изделие JaCarta Admin. Аутентификация успешно завершена."	Сообщение отображается после успешной аутентификации в изделии JaCarta Admin
"Смена ключа по умолчанию..."	Сообщение отображается в процессе смены ключа БД по умолчанию
"Обновление списка ini-файлов..."	Сообщение отображается в обновления списка ini-файлов
"Обновление списка файлов..."	Сообщение отображается в обновления списка файлов

## 8.2 Сообщения в диалоговых окнах

Сообщения в диалоговых окнах описаны в формате: Статус «Заголовок» «Сообщение». Под статусом понимается вид диалогового окна: 1) окно ошибки (см. рисунок 57), 2) окно предупреждения (см. рисунок 58) 3) информационное окно (см. рисунок 59).

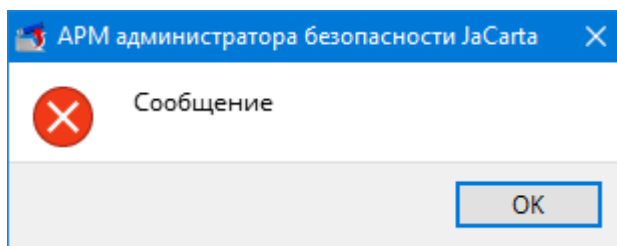


Рисунок 57 – Окно ошибки

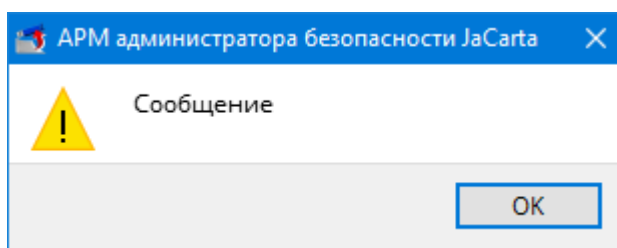


Рисунок 58 – Окно предупреждения

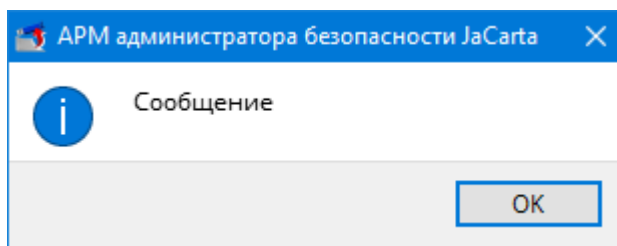


Рисунок 59 – Информационное окно

Сообщения диалоговых окон ПА приведены в таблице 3.

Таблица 3 – Сообщения диалоговых окон ПА

Статус	Текст сообщения	Описание
Ошибка 	"Связь с JaCarta Admin нарушена, переподключите устройство."	Сообщение выводится при возникновении ошибки при проверке доступности JaCarta Admin
Ошибка 	"Ошибка базы данных"	Сообщение выводится при ошибках доступа к базе данных. Например, при его повреждении, отсутствии прав на доступ к файлу БД
Ошибка 	"Ошибка считывания списка ключей с JaCarta Admin"	Сообщение выводится, если возникла ошибка при получении списка ключей с изделия JaCarta Admin. Например, при потере связи с изделием JaCarta Admin после открытия базы данных во время получения списка ключей
Ошибка 	"Не удалось считать с JaCarta Admin идентификатор ключа базы данных"	Сообщение выводится, если произошла ошибка при получении производного ключа БД с изделия JaCarta Admin
Ошибка 	"Ошибка установки ключа базы данных по умолчанию"	Сообщение выводится, если произошла ошибка при записи в БД идентификатора ключа по умолчанию
Ошибка 	"Ошибка работы с JaCarta Admin. «Описание ошибки»"	Сообщение выводится, если произошла ошибка взаимодействия с изделием JaCarta Admin. Описание ошибки выводится при наличии такового. Предусмотренные описания ошибок приведены в данном подразделе ниже
Ошибка 	"Не удалось сгенерировать ключ."	Сообщение выводится при ошибке в ходе генерации ключа в изделии JaCarta Admin
Ошибка 	"Ошибка генерации ПСЧ на JaCarta Admin."	Сообщение выводится при ошибке генерации псевдослучайной последовательности на JaCarta Admin.
Ошибка 	"Ошибка вычисления авторизационных данных"	Сообщение выводится, если возникла ошибка при выполнении криптографических функций в ходе авторизации
Ошибка 	"Не удалось внести в базу данных информацию о смене пароля администратора"	Сообщение выводится при ошибке записи в БД информации о дате смены пароля администратора изделия JaCarta Admin
Ошибка 	"Не удалось добавить в базу данных описание сгенерированного ключа"	Сообщение выводится при ошибке добавления в БД записи в ini-файл описания сгенерированного ключа для HMAC

Статус	Текст сообщения	Описание
Ошибка 	"Не удалось считать данные ini-файла из базы данных"	Сообщение выводится при ошибке чтения данных ini-файла из БД
Ошибка 	"Не удалось удалить ini-файл"	Сообщение выводится при ошибке удаления ini-файла из БД
Ошибка 	"Не удалось добавить ini-файл"	Сообщение выводится при ошибке добавления ini-файла в БД. Например, если файл с таким именем уже существует
Ошибка 	"Ошибка открытия файла-контейнера"	Сообщение выводится при возникновении ошибки при открытии файла-контейнера
Ошибка 	"Ошибка извлечения ключа из контейнера"	Сообщение выводится при возникновении ошибки в ходе извлечения ключа из файла-контейнера
Ошибка 	"Ошибка импорта ключа для HMAC в JaCarta Admin. «Описание ошибки»"	Сообщение выводится при возникновении ошибки при импорте ключа из файла-контейнера в изделие JaCarta Admin. Описание ошибки выводится при наличии такового. Предусмотренные описания ошибок приведены в данном подразделе ниже
Ошибка 	"Не удалось добавить в базу данных описание импортированного ключа."	Сообщение выводится при ошибке добавления в базу данных записи в ini-файл описания импортированного ключа для HMAC.
Ошибка 	"Ошибка экспорта ключа для HMAC из JaCarta Admin. «Описание ошибки»"	Сообщение выводится при возникновении ошибки экспорта ключа для HMAC из изделия JaCarta Admin
Ошибка 	"Ошибка работы с контейнером"	Сообщение выводится при возникновении ошибки добавления ключа в файл-контейнера
Ошибка 	"Ошибка сохранения экспортируемого ключа в файл"	Сообщение выводится при возникновении ошибки открытия выходного файла-контейнера
Ошибка 	"Не удалось считать ключи с JaCarta Admin. «Описание ошибки»"	Сообщение выводится, если произошла ошибка при выработке ключа на изделии JaCarta Admin. Описание ошибки выводится при наличии такового. Предусмотренные описания ошибок приведены в данном подразделе ниже
Ошибка 	"Не удалось добавить ключевой материал в базу данных"	Сообщение выводится при ошибке добавления в БД записи с ключевым материалом












Статус	Текст сообщения	Описание
Ошибка 	"Не удалось удалить файл из базы данных"	Сообщение выводится при возникновении ошибки при удалении файла из БД
Ошибка 	"Ошибка сохранения ini-файла"	Сообщение выводится при возникновении ошибки сохранения файла после редактирования
Ошибка 	"Не удалось загрузить файл: «Имя файла» так как его размер превышает максимально допустимый (32 КБ)."	Сообщение выводится, если при загрузке файла в БД СКЗИ «АРМ АБ JaCarta» выбран файл слишком большого размера
Ошибка 	"Не удалось загрузить файл: «Имя файла» так как его размер превышает максимально допустимый (1 МБ)."	Сообщение выводится, если при загрузке шаблона сценария в БД СКЗИ «АРМ АБ JaCarta» выбран файл слишком большого размера
Ошибка 	"Не удалось считать данные файла: «Имя файла»"	Сообщение выводится при загрузке файла в БД СКЗИ «АРМ АБ JaCarta» после нажатия кнопки «Загрузить новый файл» если файл не содержит данных
Ошибка 	"Не удалось добавить в базу данных файл: «Имя файла»"	Сообщение выводится при загрузке файла в БД СКЗИ «АРМ АБ JaCarta» после нажатия кнопки «Загрузить новый файл» если в БД уже существует файл с таким именем
Ошибка 	"Некорректный идентификатор ключа базы данных"	Сообщение выводится, если обнаружен идентификатор ключа неверной длины
Ошибка 	"Неверное значение текущего пароля сброса к заводским настройкам."	Сообщение выводится при попытке смены пароля сброса к заводским настройкам, если пользователь ввёл неверное значение текущего пароля сброса к заводским настройкам.
Ошибка 	"Неверное значение пароля сброса к заводским настройкам"	Сообщение выводится при попытке разблокировки изделия JaCarta Admin с неверным паролем сброса к заводским настройкам
Ошибка 	"Необходимо сначала добавить корректный ini-файл."	Сообщение выводится, если после нажатия кнопки «Применить сценарий» не обнаружено корректных сценариев
Ошибка 	"Ini-файл некорректный"	Сообщение выводится, если после нажатия кнопки «Применить сценарий» проверка синтаксиса сценария завершилась ошибкой
Ошибка 	"Не удалось считать список журналов из базы данных"	Сообщение выводится, если при обновлении списка журналов не удалось считать данные из БД



Статус	Текст сообщения	Описание
Ошибка 	"Переподключите устройство «Имя считывателя»"	Сообщение выводится, если при обнаружении считывателя (изделие JaCarta Admin не подключено) не удалось установить соединение со считывателем
Ошибка 	"Подключенное устройство «Имя считывателя» не распознано как JaCarta Admin."	Сообщение выводится, если на смарт-карте не обнаружен АРМ-апплет с актуальным идентификатором
Ошибка 	"Подключенная версия JaCarta Admin не поддерживается."	Сообщение выводится, если на смарт-карте обнаружен АРМ-апплет устаревшей версии
Ошибка 	"Пароль администратора недействительный"	Сообщение выводится при подключении изделия JaCarta Admin если подключаемое изделие JaCarta Admin заблокировано и пользователь отказался запускать АРМ администратора безопасности в режиме разблокировки.
Ошибка 	"Введен неверный пароль администратора JaCarta Admin («Имя считывателя»). Количество попыток до блокировки изделия: «N». "	Сообщение выводится при возникновении ошибки при открытии защищённого канала с изделием JaCarta Admin, например при вводе неверного пароля. N – количество попыток
Ошибка 	"Не удалось аутентифицироваться в JaCarta Admin: «имя считывателя». Количество попыток до блокировки изделия: «N». "	Сообщение отображается при возникновении ошибки в процессе подготовки механизма защиты ключей, хранящихся в памяти изделия JaCarta Admin, к использованию. N – количество попыток
Ошибка 	"Не удалось открыть базу данных. Количество попыток до блокировки изделия: «N».	Сообщение выводится, если не удалось открыть базу данных. N – количество попыток
Ошибка 	"Произошла неизвестная ошибка."	Сообщение выводится, если при подключении изделия JaCarta Admin произошла ошибка, для которой не предусмотрено отдельное сообщение
Ошибка 	"Не удалось установить ключи шифрования базы данных."	Сообщение выводится при возникновении ошибки при установке ключа шифрования журналов в БД
Ошибка 	"Не удалось считать информацию с JaCarta-2 GOST, переподключите устройство: «Имя считывателя»"	Сообщение выводится, если возникла ошибка при получении информации с изделия JaCarta-2 ГОСТ
Ошибка 	"Ошибка сервиса CCID. Перезапустите приложение"	Сообщение выводится при возникновении ошибки в работе подсистемы мониторинга считывателей смарт-карт

Статус	Текст сообщения	Описание
Ошибка 	"Ошибка установления контекста XXX"	Сообщение выводится при возникновении ошибки установления контекста подсистемы смарт-карт ОС. XXX – краткое название подсистемы смарт-карт ОС (WinSCard для Windows или PC/SC Lite для Linux)
Ошибка 	"Ошибка считывания списка устройств XXX"	Сообщение выводится при возникновении ошибки считывания списка устройств XXX. XXX – краткое название подсистемы смарт-карт ОС (WinSCard для Windows или PC/SC Lite для Linux)
Ошибка 	"Не удалось установить соединение с изделием «Имя считывателя»"	Сообщение выводится при обнаружении считывателя, с которым не удалось установить соединение, а изделие JaCarta Admin уже было обнаружено.
Ошибка 	"Ошибка при создании журналов в базе данных."	Сообщение выводится при возникновении ошибки при создании журнала в базе данных
Ошибка 	"Непредвиденная ошибка при создании журналов в базе данных."	Сообщение выводится при возникновении ошибки при создании журнала в базе данных для которой нет отдельного описания
Ошибка 	"Пароль и повтор пароля не совпадают."	Сообщение выводится при вводе нового значения при смене пароля администратора, PUK-кода, пароля сброса к заводским настройкам, если значение и его повтор не совпадают
Ошибка 	"Пароль должен содержать хотя бы одну цифру"	Сообщение выводится при вводе нового пароля (смена пароля администратора, PUK-кода, пароля сброса к заводским настройкам) если пароль не соответствует парольной политике
Ошибка 	"Пароль должен содержать хотя бы одну заглавную букву на русском или английском языке"	Сообщение выводится при вводе нового пароля (смена пароля администратора, PUK-кода, пароля сброса к заводским настройкам) если пароль не соответствует парольной политике
Ошибка 	"Пароль должен содержать хотя бы одну строчную букву на русском или английском языке"	Сообщение выводится при вводе нового пароля (смена пароля администратора, PUK-кода, пароля сброса к заводским настройкам) если пароль не соответствует парольной политике
Ошибка 	"Минимальная длина пароля: «Минимальная длина пароля»"	Сообщение выводится при вводе нового пароля (смена пароля администратора, PUK-кода, пароля сброса к заводским настройкам) если длина пароля не соответствует парольной политике
Ошибка 	"Пароль должен содержать хотя бы один спецсимвол [!@#\$%^&*]."	Сообщение выводится при вводе нового пароля (смена пароля администратора, PUK-кода, пароля сброса к заводским настройкам) если пароль не содержит специальных символов

Статус	Текст сообщения	Описание
Ошибка 	"Ошибка ввода счётчика успешно выполненных разблокирований."	Сообщение выводится при вводе некорректного значения счётчика успешно выполненных разблокирований при генерации последовательности для удалённой разблокировки. Например в том случае, если после открытия диалога генерации последовательности для удалённой разблокировки заменить изделие JaCarta Admin на другое изделие JaCarta Admin с меньшим количеством ключей администрирования и выбрать идентификатор ключа которого нет в изделии
Ошибка 	"Ошибка ввода серийного номера"	Сообщение выводится после нажатия кнопки «Сгенерировать» в окне генерации последовательности для удалённой разблокировки, если в окне введён некорректный полный серийный номер разблокируемого устройства
Ошибка 	"Ошибка ввода SEED"	Сообщение выводится после нажатия кнопки «Сгенерировать» в окне генерации последовательности для удалённой разблокировки, если в окне введён некорректный seed
Ошибка 	"Ошибка расчёта UID"	Сообщение выводится после нажатия кнопки «Сгенерировать» в окне генерации последовательности для удалённой разблокировки, если не удалось сгенерировать идентификатор (UID) изделия JaCarta-2 ГОСТ
Ошибка 	"Ошибка генерации последовательности. Связь с JaCarta Admin нарушена."	Сообщение выводится, если после нажатия кнопки «Сгенерировать последовательность для удалённой разблокировки» отсутствует соединение с изделием JaCarta Admin
Ошибка 	"Ошибка генерации последовательности в JaCarta Admin. «Описание ошибки»"	Сообщение выводится после нажатия кнопки «Сгенерировать» в окне генерации последовательности для удалённой разблокировки, если изделие JaCarta Admin не может сгенерировать последовательность. Описание ошибки выводится при наличии такового. Предусмотренные описания ошибок приведены в данном подразделе ниже
Ошибка 	"Неверное имя файла"	Сообщение выводится при возникновении ошибки ввода имени сохраняемого ini-файла. Например, если не введено имя для сохранённого файла
Ошибка 	"При проверке файла произошла ошибка «Описание ошибки»"	Сообщение выводится после нажатия кнопки "Проверить синтаксис" в окне редактирования сценария, если при проверке файла найдена синтаксическая ошибка. Если при проверке удалось обнаружить в какой секции имеется ошибка, то выводится имя секции
Ошибка 	"Ошибка генерации ПСЧ."	Сообщение выводится при возникновении ошибки ДСЧ

Статус	Текст сообщения	Описание
Ошибка 	"Ошибка записи в журнал «Имя журнала» базы данных."	Сообщение выводится при ошибке записи сообщения в журнал
Ошибка 	"Произошла ошибка при взаимодействии с устройством «Имя считывателя». Переподключите его!"	Сообщение выводится при возникновении ошибки при взаимодействии с устройством чтения смарт-карт в режиме разблокировки
Ошибка 	"Не удалось добавить в базу данных файл: <Полное имя файла>. Файл с таким именем <Имя файла> уже существует (измените имя файла)."	Сообщение выводится при попытке загрузить в БД файл, если его имя совпадает с именем уже существующего в БД файла
Ошибка 	"Не удалось добавить в базу данных файл: <Имя файла сценария>. Файл с таким именем уже существует (измените имя файла)."	Сообщение выводится при попытке сохранить сценарий, если его имя совпадает с именем уже существующего сценария
Ошибка 	"Произошла неизвестная ошибка. Приложение будет перезапущено."	Сообщение выводится при аварийном завершении программы в ОС Windows
Ошибка 	"Произошла неизвестная ошибка. Приложение будет закрыто."	Сообщение выводится при аварийном завершении программы в ОС Linux
Ошибка 	"Ошибка запуска режима загрузки сценариев. Не указан шаблон пути к файлам сценариев."	Сообщение выводится при запуске ПА с параметром – scriptLoad при некорректно заданном шаблоне пути к шаблонам сценариев
Ошибка 	"Ошибка запуска режима загрузки сценариев. Шаблоны сценариев не найдены."	Сообщение выводится при запуске ПА с параметром – scriptLoad, если не найдены шаблоны сценариев
Ошибка 	"Не удалось открыть файл: <Путь к файлу>."	Сообщение выводится при запуске ПА с параметром – scriptLoad, если не удалось открыть файл шаблона сценария
Ошибка 	"Не удалось считать данные из файла: <Путь к файлу>."	Сообщение выводится при запуске ПА с параметром – scriptLoad, если шаблон сценария пуст или не удалось считать из него данные
Ошибка 	"Не удалось добавить ini-файл в базу данных."	Сообщение выводится при запуске ПА с параметром – scriptLoad, при ошибке добавления файла в базу данных

Статус	Текст сообщения	Описание
Ошибка 	"Ошибка открытия файла шаблона"	Сообщение выводится после нажатия кнопки «Загрузить шаблон сценария» вкладки «Сценарии» при возникновении ошибки при автоматическом открытии файла шаблона сценария
Предупреждение 	"Не найдена база данных. Будет создана новая база данных"	Сообщение выводится в процессе открытия БД, если файл БД не обнаружен
Предупреждение 	"Не задан ключ базы данных по умолчанию. В изделии JaCarta Admin будет выбран самый новый ключ базы данных."	Сообщение выводится при открытии БД, если ключ базы данных по умолчанию не установлен (отсутствует запись о ключе по умолчанию в БД)
Предупреждение 	"Истёк срок действия ключа базы данных по умолчанию. В изделии JaCarta Admin будет выбран самый новый ключ базы данных."	Сообщение выводится при открытии базы данных, если истёк срок действия ключа базы данных по умолчанию.
Предупреждение 	"Ключ базы данных по умолчанию не соответствует изделию JaCarta Admin. Будет установлен новый ключ базы данных по умолчанию."	Сообщение выводится при открытии базы данных, если ключ базы данных не соответствует изделию JaCarta Admin.
Предупреждение 	"Необходимо сменить пароль администратора JaCarta Admin, введите новый пароль, соответствующий парольной политике."	Сообщение выводится в процессе подготовки механизма защиты ключей, хранящихся в памяти изделия JaCarta Admin, если в изделии JaCarta Admin установлен пароль администратора по умолчанию
Предупреждение 	"Отмена генерации ключа."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге генерации ключа.
Предупреждение 	"Не удалось сгенерировать ключ, повтор процедуры."	Сообщение выводится, если при генерации ключа в изделии JaCarta Admin, изделие JaCarta Admin вернуло сообщение об ошибке
Предупреждение 	"На изделии JaCarta Admin не обнаружено подходящих ключей базы данных, будет сгенерирован новый ключ."	Сообщение выводится, если на изделии JaCarta Admin не найдены ключи базы данных или у всех найденных ключей БД истёк срок действия
Предупреждение 	"Отмена изменения пароля администратора."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге изменения пароля администратора

Статус	Текст сообщения	Описание
Предупреждение 	"Отмена выбора файла-контейнера."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге выбора файла-контейнера
Предупреждение 	"Отмена ввода пароля контейнера."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге ввода пароля контейнера при импорте ключа для HMAC
Предупреждение 	"Выберите ключ, который вы хотите экспортировать"	Сообщение выводится, если пользователь нажал кнопку «Экспортировать ключ», но не выбрал ни одного ключа в таблице ключей для HMAC
Предупреждение 	"Выберите один ключ, который вы хотите экспортировать"	Сообщение выводится при нажатии кнопки «Экспортировать ключ», если выбрано более одного ключа из таблицы ключей для HMAC
Предупреждение 	"Отмена ввода пароля для ключевого контейнера."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге ввода пароля контейнера при экспорте ключа для HMAC
Предупреждение 	"Выберите файл, который вы хотите отредактировать"	Сообщение выводится при нажатии кнопки «Редактировать сценарий», если не выбран ни один файл в таблице сценариев
Предупреждение 	"Выберите один файл, который вы хотите отредактировать"	Сообщение выводится при нажатии кнопки «Редактировать сценарий», если выбрано более одного файла из таблицы сценариев
Предупреждение 	"Выберите файл, который вы хотите удалить"	Сообщение выводится при нажатии кнопки «Удалить сценарий» или «Удалить файл», если не выбран ни один файл из таблицы
Предупреждение 	"Выберите один файл, который вы хотите удалить"	Сообщение выводится при нажатии кнопки «Удалить сценарий» или «Удалить файл», если выбрано более одного файла из таблицы
Предупреждение 	"Отмена изменения PUK-кода JaCarta Admin."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге изменения PUK-кода JaCarta Admin
Предупреждение 	"Отмена изменения пароля сброса к заводским настройкам JaCarta Admin."	Сообщение выводится после нажатия кнопки «Отмена» в диалоге изменения пароля сброса к заводским настройкам JaCarta Admin

Статус	Текст сообщения	Описание
Предупреждение 	"Перед генерацией последовательности для удаленной разблокировки необходимо сгенерировать хотя бы один ключ администрирования"	Сообщение выводится при нажатии кнопки «Сгенерировать последовательность для удаленной разблокировки», если в изделии JaCarta Admin не обнаружено ни одного ключа администрирования
Предупреждение 	"Выберите ключ базы данных, который вы хотите назначить ключом по умолчанию."	Сообщение выводится при нажатии кнопки «Назначить ключом по умолчанию», если не выбран ни один ключ из таблицы ключей базы данных
Предупреждение 	"Выберите один ключ базы данных, который вы хотите назначить ключом по умолчанию."	Сообщение выводится при нажатии кнопки «Назначить ключом по умолчанию», если выбрано более одного ключа из таблицы ключей базы данных
Предупреждение 	"Изделие JaCarta Admin извлечено"	Сообщение выводится после извлечения изделия JaCarta Admin
Предупреждение 	"Необходимо обновить внутреннее состояние ДСЧ JaCarta Admin с помощью биологического датчика случайных чисел."	Сообщение выводится при первом подключении изделия JaCarta Admin
Предупреждение 	"Отмена выбора файла шаблона."	Сообщение выводится после нажатия кнопки «Загрузить шаблон сценария» вкладки «Сценарии» ПА при отмене выбора файла шаблона сценария
Информация 	"Ключ для НМАС успешно импортирован"	Сообщение выводится после успешного импорта ключа для НМАС в изделие JaCarta Admin
Информация 	"Ключ для НМАС экспортирован успешно"	Сообщение выводится после успешного экспорта ключа для НМАС из изделия JaCarta Admin
Информация 	"Пароль администратора JaCarta Admin изменён."	Сообщение выводится после успешной смены пароля администратора изделия JaCarta Admin

Статус	Текст сообщения	Описание
Информация 	"PUK-код JaCarta Admin изменён."	Сообщение выводится после успешной смены PUK-кода изделия JaCarta Admin
Информация 	"Пароль сброса к заводским настройкам JaCarta Admin изменён."	Сообщение выводится после успешной смены пароля сброса изделия JaCarta Admin к заводским настройкам
Информация 	"На изделии «Имя считывателя» не найден апплет JaCarta-2 GOST"	Сообщение выводится при обнаружении изделия на котором не обнаружен апплет JaCarta-2 GOST (изделие JaCarta Admin уже было обнаружено ранее)
Информация 	"Сценарий успешно прошёл проверку синтаксиса."	Сообщение выводится в случае успешного завершения проверки синтаксиса
Информация 	"JaCarta Admin успешно разблокирован."	Сообщение выводится после успешной разблокировки изделия JaCarta Admin
Информация 	Стандартное использование: jcadmin [-dbpath <Путь к файлу БД>]  Режим загрузки сценариев: jcadmin -scriptLoad "<Шаблон пути к файлам сценариев>" [-dbpath <Путь к файлу БД>]  Режим разблокировки JaCarta Admin: jcadmin -unlock	Сообщение выводится после запуска ПА с параметром -help
Информация 	Файл шаблонов успешно загружен	Сообщение выводится после запуска ПА с параметром -scriptLoad после завершения загрузки всех шаблонов сценариев

Для формирования сообщений диалоговых окон предусмотрены следующие описания ошибок:

- "Некорректная длина поля данных APDU-команды.";
- "Не удалось обновить внутренне состояние датчика случайных чисел.";
- "Недопустимое значение параметра APDU-команды.";
- "Недопустимое значение инструкции APDU-команды.";
- "Недопустимое значение класса APDU-команды.";
- "Неизвестная ошибка.";

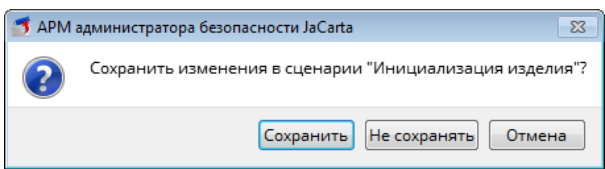
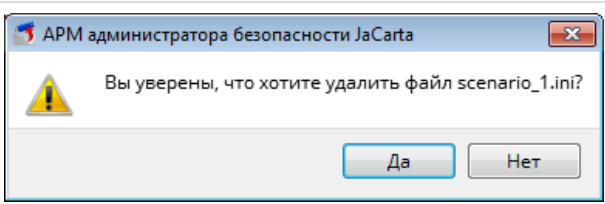
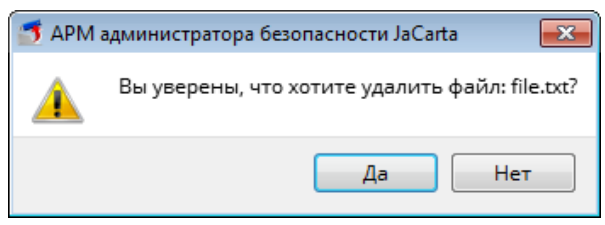
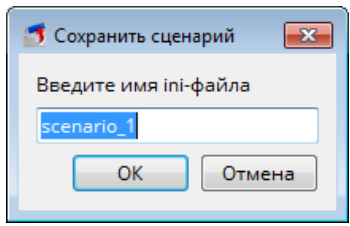
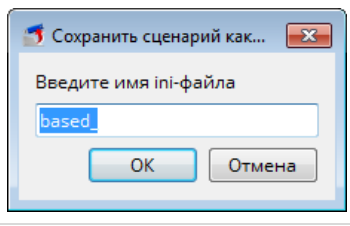
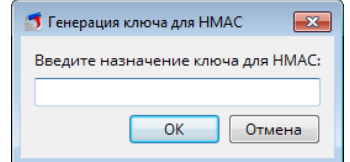


- "Отсутствует имитовставка в APDU-команде.";
- "Ошибка расшифрования либо нарушение целостности зашифрованной APDU-команды.";
- "Не удалось расшифровать ключ.";
- "Ключ не найден.";
- "Неизвестная ошибка «Код Ошибки»".

### 8.3 Сообщения, запрашивающие данные или выбор пользователя

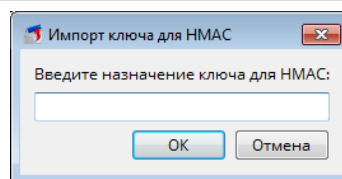
Сообщения, запрашивающие данные или выбор пользователя, приведены в таблице 4:

Таблица 4 – Сообщения, запрашивающие данные или выбор пользователя

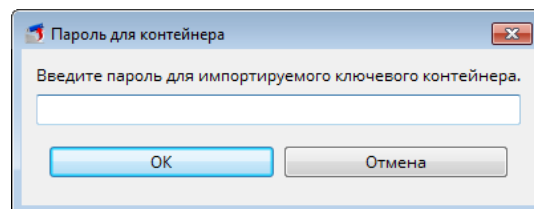
Описание	Окно сообщения
Сообщение при закрытии редактора сценария в случае наличия несохранённых изменений	
Сообщение после нажатия кнопки «Удалить сценарий»	
Сообщение после нажатия кнопки «Удалить файл»	
Сообщение при сохранении нового файла-сценария	
Сообщение после нажатия кнопки «Сохранить сценарий как...» в окне редактирования сценариев	
Сообщение после нажатия кнопки «Сгенерировать ключ» вкладки «Ключи для HMAC»	

**Описание****Окно сообщения**

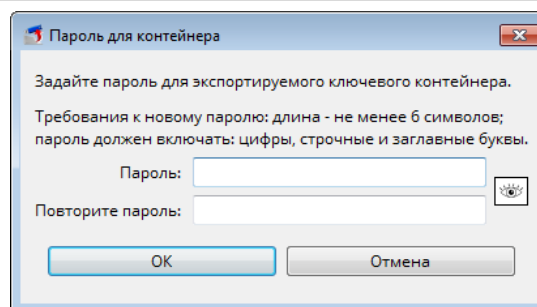
Сообщение после ввода пароля для импортируемого ключевого контейнера при импорте ключа для НМАС



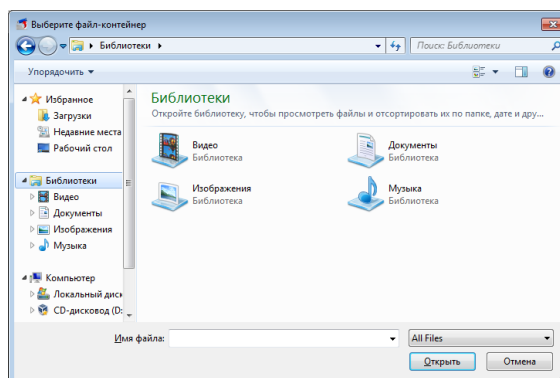
Пример окна ввода пароля или РУК-кода без описания парольной политики



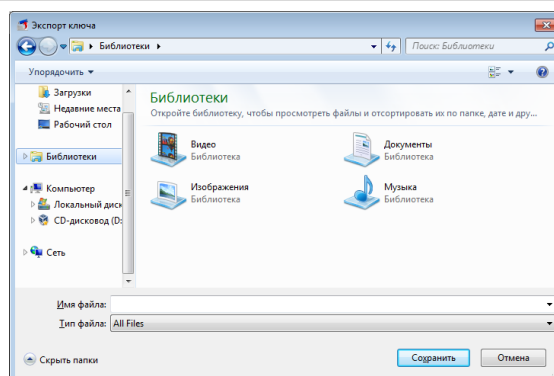
Пример окна ввода пароля или РУК-кода с описанием парольной политики




Окно выбора файла-контейнера для импорта ключа для НМАС

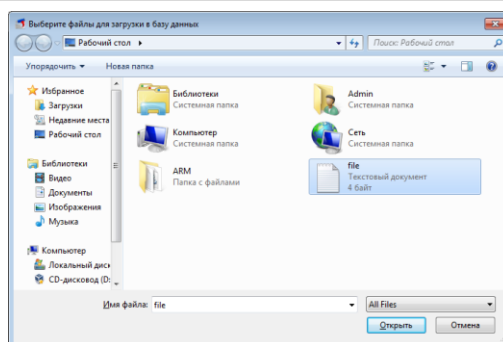


Окно сохранения файла-контейнера с ключом для НМАС при экспорте

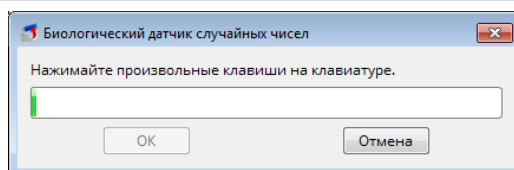


**Описание****Окно сообщения**

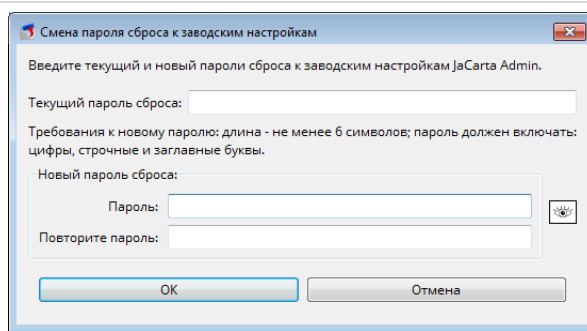
Окно загрузки файлов в БД после нажатия кнопки  «Загрузить новый файл» вкладки «Файлы» основного окна ПА



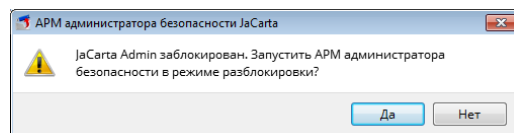
Окно ввода материала для генерации ключа. Выводится после нажатия кнопок генерации ключей



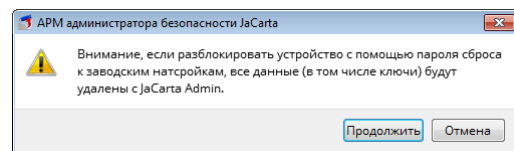
Окно смены пароля сброса к заводским настройкам



Окно, выводимое при подключении заблокированного изделия JaCarta Admin



Окно, выводимое при сбросе к заводским настройкам изделия JaCarta Admin



## 8.4 Сообщения в журналах

### 8.4.1 Сообщения в журнале операций с изделием JaCarta Admin

Сообщения журнала операций с изделием JaCarta Admin приведены в таблице 5.

Таблица 5 – Сообщения в журнале операций с изделием JaCarta Admin

Текст сообщения	Описание
"Login in JaCarta Admin succeeded"	Сообщение заносится в журнал после успешной подготовки механизма защиты ключей, хранящихся в памяти изделия JaCarta Admin, к использованию
"<ТИП КЛЮЧА> key with ID <ID ключа> was generated."	Сообщение заносится в журнал после успешной генерации ключа в изделии JaCarta Admin. Возможные значения поля <ТИП КЛЮЧА>: "Admin", "DataBase", "Secret". <ID ключа> – полный идентификатор ключа
"JaCarta Admin password successfully changed"	Сообщение заносится в журнал после успешной смены пароля администратора изделия JaCarta Admin
"Secret key description: <Назначение ключа для HMAC>"	Сообщение заносится в журнал после успешной генерации или импорта ключа для HMAC и ввода его назначения
"Secret key with ID <ID ключа> was imported."	Сообщение заносится в журнал после успешного импорта ключа для HMAC в изделие JaCarta Admin
"Secret key with ID <ID ключа> was exported."	Сообщение заносится в журнал после успешного экспорта ключа для HMAC из изделия JaCarta Admin
"Start Authentication for device: <Имя считывателя>"	Сообщение заносится в журнал при обнаружении устройства чтения смарт-карт и начале аутентификации
"Connection failed for device: <Имя считывателя>"	Сообщение заносится в журнал при возникновении ошибки во время соединения с устройством чтения смарт-карт в ходе аутентификации
"JaCarta Admin not found on device: <Имя считывателя>"	Сообщение заносится в журнал, если в ходе аутентификации подключённое изделие не распознано как изделие JaCarta Admin
"JaCarta Admin version is not supported."	Сообщение заносится в журнал, если в ходе аутентификации обнаружено, что версия АРМ-апплета подключённого изделия JaCarta Admin устарела
"JaCarta Admin found, serial: <Полный серийный номер изделия JaCarta Admin>[<Краткий серийный номер изделия JaCarta Admin>], device: <Имя считывателя>"	Сообщение заносится в журнал после успешной подготовки изделия к использованию ключей
"Authentication counters are invalid on JaCarta Admin."	Сообщение выводится, если исчерпано количество попыток ввода пароля
"Failed to open secure channel with JaCarta Admin <Имя считывателя>"	Сообщение заносится в журнал в случае возникновения ошибки в ходе построения защищённого канала с изделием JaCarta Admin

Текст сообщения	Описание
"Secure channel successfully opened with JaCarta Admin: <Полный серийный номер JaCarta Admin>"[<Краткий серийный номер JaCarta Admin>]"	Сообщение заносится в журнал после успешного построения защищённого канала с изделием JaCarta Admin
"Failed to open DataBase"	Сообщение заносится в журнал в случае возникновения ошибки при открытии базы данных
"Sequence for remote unblock was generated for SN: <Полный серийный номер JaCarta-2 GOST> with MKID = <Идентификатор ключа>, SEED = <Значение SEED>, N = <Счётчик успешно выполненных разблокирований>"	Сообщение заносится в журнал после успешной генерации последовательности для удалённой разблокировки
"Authentication counters are invalid on JaCarta Admin"	Сообщение заносится в журнал, если после исчерпания оставшихся попыток ввода неверного пароля и разблокирования изделия JaCarta Admin на другом АРМ АБ была продолжена работа на исходном АРМ АБ.
"JaCarta Admin PUK successfully changed"	Сообщение заносится в журнал при успешной смене или установке PUK-кода:
"JaCarta Admin PIN_RESET successfully changed"	Сообщение заносится в журнал при успешной смене пароля сброса к заводским настройкам
"JaCarta Admin RNG is not initialized, start RNG update. Serial: <Полный серийный номер>[<Краткий серийный номер JaCarta Admin>]"	Сообщение заносится в журнал при обновлении внутреннего состояния программного ДСЧ изделия JaCarta Admin
"Failed to update RNG on JaCarta Admin"	Сообщение заносится в журнал при неудачном обновлении внутреннего состояния программного ДСЧ изделия JaCarta Admin

## 8.4.2 Сообщения в журналах ошибок, выполненных сценариев и операций с изделием JaCarta-2 ГОСТ

### 8.4.2.1 Сообщения центрального потока выполнения сценария

Сообщения центрального потока выполнения сценария, который вызывает отдельные операции, записываются с полем названия операции <ExecuteActionsList>.

Сообщения <ExecuteActionsList> в журнал ошибок приведены в таблице 6.

Таблица 6 – Сообщения <ExecuteActionsList> в журнале ошибок ПА

Текст сообщения	Описание
"Context JaCarta-2 GOST not found"	Нет доступа к изделию JaCarta-2 ГОСТ
"Context JaCarta Admin not found"	Нет доступа к изделию JaCarta Admin
"Script Name not found"	Не задано наименование сценария
" JaCarta-2 GOST serial not found"	Не удалось считать серийный номер изделия JaCarta-2 ГОСТ
"JaCarta Admin serial not found"	Не удалось считать серийный номер изделия JaCarta Admin
"get action <Номер операции> error; "	Нет доступа к экземпляру операции
"Action <Наименование операции> failed with code <Код ошибки>; "	Операция завершилась с ошибкой. Код ошибки: -1
"JaCarta Admin serial:'<Полный серийный номер JaCarta Admin>[<Краткий серийный номер JaCarta Admin>]'; JaCarta-2 GOST serial:'<Полный серийный номер JaCarta-2 ГОСТ> [<Краткий серийный номер изделия JaCarta-2 ГОСТ>]'; Reader JaCarta-2 GOST name:'<Наименование устройства чтения смарт-карт>; Script name:'<Наименование сценария> '; Ini name:'Имя файла сценария'; Finished JaCarta-2 GOST administration with code <Код ошибки>; "	Выполнение сценария завершилось с ошибкой. Код ошибки: -2

Сообщения <ExecuteActionsList> в журнал операций с изделием JaCarta-2 ГОСТ приведены в таблице 7.

Таблица 7 – Сообщения &lt;ExecuteActionsList&gt; в журнале операций с изделием JaCarta-2 ГОСТ

Текст сообщения	Описание
"JaCarta Admin serial:'<Полный серийный номер изделия JaCarta Admin>[<Краткий серийный номер JaCarta Admin>]'; JaCarta-2 GOST serial:'<Полный серийный номер изделия JaCarta-2 ГОСТ> [<Краткий серийный номер изделия JaCarta-2 ГОСТ>]'; Reader JaCarta-2 GOST name:'<Наименование устройства чтения смарт-карт>'; Script name:'<Наименование сценария> '; Ini name:'Имя файла сценария'; Start JaCarta-2 GOST administration; "	Начало применения сценария
"Action <Наименование операции> skipped (WARNING! Not supported!)"	Операция не поддерживается
"Action <Наименование операции> failed with code <Код ошибки>; "	Операция завершилась с ошибкой. Код ошибки: -1
"Action <Наименование операции> ОК; "	Операция завершилась успешно
"JaCarta Admin serial:'<Полный серийный номер изделия JaCarta Admin>[<Краткий серийный номер JaCarta Admin>]'; JaCarta-2 GOST serial:'<Полный серийный номер изделия JaCarta-2 ГОСТ>[<Краткий серийный номер изделия JaCarta-2 ГОСТ>]'; Reader JaCarta-2 GOST name:'<Наименование устройства чтения смарт-карт>'; Script name:'<Наименование сценария>'; Ini name:'Имя файла сценария'; Finished JaCarta-2 GOST administration with code <Код ошибки>; "	Выполнение сценария завершилось успешно. Код ошибки: 1

#### 8.4.2.2 Сообщения операций администрирования изделий JaCarta-2 ГОСТ

Сообщения операций администрирования изделий JaCarta-2 ГОСТ в журнал операций с изделием JaCarta-2 ГОСТ и журнал ошибок записываются в формате: "<Наименование операции(Action)> : <Сообщение>".

##### 8.4.2.2.1 Сообщения операций в журнал ошибок

Сообщения операций в журнал ошибок ПА приведены в таблице 8.

Таблица 8 – Сообщения операций в журнале ошибок ПА

Текст сообщения	Описание
"init error"	Операция не инициализирована
"Context JaCarta-2 GOST not found"	Нет доступа к изделию JaCarta-2 ГОСТ
"Context JaCarta Admin not found"	Нет доступа к изделию JaCarta Admin
"JaCarta-2 GOST not found on <Имя считывателя>"	Не установлено соединение с изделием JaCarta-2 ГОСТ
"JaCarta Admin not found on <Имя считывателя>"	Не установлено соединение считывателя с АРМ-апплетом

Текст сообщения	Описание
"Secure Channel not found on JaCarta Admin <Полный серийный номер изделия JaCarta Admin>[<Краткий серийный номер изделия JaCarta Admin>]"	Не установлен защищённый канал с изделием JaCarta Admin
"JaCarta-2 GOST serial number is not checked <Полный серийный номер изделия JaCarta-2 ГОСТ>[<Краткий серийный номер изделия JaCarta-2 ГОСТ>]"	Не удалось считать серийный номер изделия JaCarta-2 ГОСТ, в необходимый момент
"MK_ID is not belong this JaCarta Admin"	Идентификатор ключа не соответствует изделию JaCarta Admin
"Bad MK_ID length"	Указана неверная длина идентификатора ключа
"UID calculate error"	Ошибка вычисления UID
"Unknown exception"	Возникло непредвиденное исключение
"Текст исключений стандартной библиотеки"	Возникло исключение типа std::runtime_error
"length out"	Ошибка работы с файлом, выход за его размер
"Get data chunk(size)"	Ошибка чтения порции данных файла
"Error executing: '<Описание действия>' Error code: <Код ошибки <sup>1</sup> >"	Возникла ошибка при отправке APDU-команды (см. таблицу 9)
"Invalid RAPDU executing: '<Описание действия>'"	APDU-ответ неверной длины (см. таблицу 9)
"Invalid SW executing: '<Описание действия>' SW = <SW APDU-ответа>"	APDU-ответ содержит код ошибки (см. таблицу 9)

Возможные варианты содержания поля <Описания действия> текста сообщения, приведённого в таблице 8 представлены в таблице 9:

Таблица 9 – Возможные варианты содержания поля <Описания действия>

Содержание поля	Описание
"Generate APDU: Open SecureChannel with JaCarta-2 GOST [step 1]"	Подготовка к установке защищённого канала между изделиями. Первое обращение к изделию JaCarta Admin
"Open SecureChannel with JaCarta-2 GOST [step 1]"	Подготовка к установке защищённого канала между изделиями. Первое обращение к изделию JaCarta-2 ГОСТ

<sup>1</sup> Коды ошибок SCARD, Windows System или pcsc-lite



Содержание поля	Описание
"Generate APDU: Open SecureChannel with JaCarta-2 GOST [step 2]"	Продолжение установки защищённого канала между изделиями. Второе обращение к изделию JaCarta Admin
"Open SecureChannel with JaCarta-2 GOST [step 2]"	Продолжение установки защищённого канала между изделиями. Второе обращение к изделию JaCarta-2 ГОСТ
"Generate APDU: Open SecureChannel with JaCarta-2 GOST [step 3]"	Завершение установки защищённого канала между изделиями. Подготовка к предъявлению ключа администратора безопасности
"Open SecureChannel with JaCarta-2 GOST [step 3]"	Предъявление ключа администратора безопасности
"Open SecureChannel with JaCarta-2 GOST [step 4]"	Проверка результата предъявления ключа администратора безопасности
"Send init-PIN to JaCarta-2 GOST"	PIN-код сброса к заводским настройкам послан изделию JaCarta-2 ГОСТ
"<Название APDU-команды> : generate APDU on JaCarta Admin"	Команда <Название APDU-команды> сгенерирована изделием JaCarta Admin (см. таблицу 10)
"<Название APDU-команды> : send APDU to JaCarta-2 GOST"	Команда <Название APDU-команды> отправлена изделию JaCarta-2 ГОСТ (см. таблицу 10)
"<Название APDU-команды> : decrypt JaCarta-2 GOST response"	Расшифрован ответ изделия JaCarta-2 ГОСТ на команду <Название APDU-команды> (см. таблицу 10)

Возможные варианты содержания поля <Название APDU-команды> приведены в таблице 10.

Таблица 10 – Возможные варианты содержания поля <Название APDU-команды>

Содержание поля	Описание
"LOGOUT"	Команда обусловлена операцией LOGOUT
"INIT"	Команда обусловлена операцией INIT
"Change SO-key to default"	Команда обусловлена операцией INIT_DEF, устанавливает ключ администратора безопасности в значение по умолчанию с возможностью предъявления в открытом виде
"Set SO Key"	Команда обусловлена операцией SET_SO_KEY
"SET_PIN"	Команда обусловлена операцией SET_PIN
"SET_PUK"	Команда обусловлена операцией SET_PUK
"SET_PININIT"	Команда обусловлена операцией SET_PININIT
"UNBLOCK"	Команда обусловлена операцией UNBLOCK
"Set password policy"	Команда обусловлена операцией SET_PASSWORD_POLICY

Содержание поля	Описание
"Generate key pair"	Команда обусловлена операцией <code>GENERATE_KEY_PAIR</code>
"Import public key"	Команда обусловлена операцией <code>IMPORT_PUBLIC_KEY</code>
"Import secret key"	Команда обусловлена операцией <code>IMPORT_SECRET_KEY</code>
"Delete key object"	Команда обусловлена операцией <code>DELETE_KEY</code>
"Write service info"	Команда обусловлена операцией <code>WRITE_SERVICE_INFO</code>
"Select file"	Команда обусловлена операцией <code>SELECT_FILE</code>
"Create dir"	Команда обусловлена операцией <code>CREATE_DIR</code>
"Delete file"	Команда обусловлена операцией <code>DELETE_FILE</code>
"Change access"	Команда обусловлена операцией <code>CHANGE_ACCESS</code>
"Create temp buffer"	Команда обусловлена операцией <code>CREATE_FILE</code> , создаёт в памяти изделия JaCarta-2 ГОСТ буфер для записи данных, определяемых параметром <code>DATA</code> или <code>FNAME</code>
"Chunk sent to temp buffer"	Команда обусловлена операцией <code>CREATE_FILE</code> , записывает данные в созданный в памяти изделия JaCarta-2 ГОСТ буфер. При необходимости данные разбиваются на части и передаются последовательно несколькими командами
"Save buffer as new file"	Команда обусловлена операцией <code>CREATE_FILE</code> , сохраняет буфер как файл, определённый параметрами <code>NAME</code> и <code>AC</code>
"Chunk sent to file"	Команда обусловлена операцией <code>WRITE_FILE</code> , записывает данные в файл, выбранный с помощью последней выполненной операции <code>SELECT_FILE</code> . При необходимости данные разбиваются на части и передаются последовательно несколькими командами
"Get file size"	Команда обусловлена операцией <code>READ_FILE</code> , служит для получения информации о размере файла, выбранного с помощью последней выполненной операции <code>SELECT_FILE</code>
"Get data chunk"	Команда обусловлена операцией <code>READ_FILE</code> , считывает данные из файла, выбранного с помощью последней выполненной операции <code>SELECT_FILE</code> . При необходимости данные разбиваются на части и считываются последовательно несколькими командами

## 8.4.2.2.2 Сообщения операций в журнале операций с изделием JaCarta-2 ГОСТ

Сообщения операций в журнале операций с изделием JaCarta-2 ГОСТ приведены в таблице 11.

Таблица 11 – Сообщения операций в журнале операций с изделием JaCarta-2 ГОСТ

Текст сообщения	Описание
"SET_SO_KEY : МК_ID: <Идентификатор ключа>; МК_SEED: <Seed мастер-ключа>; "	Сообщение выводится после успешного завершения операции SET_SO_KEY
"IMPORT_PUBLIC_KEY : Public key ID: <Идентификатор ключа> Public key attr: <Параметры ключа> "	Сообщение выводится после успешного завершения операции IMPORT_PUBLIC_KEY
"IMPORT_SECRET_KEY : JaCarta Admin serial: <Полный серийный номер изделия JaCarta Admin> [<Краткий серийный номер JaCarta Admin>]; МК ID: <Идентификатор ключа>; HMAC: <HMAC поле операции >; Secret key ID: <Идентификатор ключа>"	Сообщение выводится после успешного завершения операции IMPORT_SECRET_KEY
"SELECT_FILE : file path: <Путь к файлу>"	Сообщение выводится после успешного завершения операции SELECT_FILE
"CREATE_DIR : dir name: <Идентификатор папки>"	Сообщение выводится после успешного завершения операции CREATE_DIR
"CREATE_FILE : file name: <Путь к файлу>"	Сообщение выводится после успешного завершения операции CREATE_FILE
"WRITE_FILE : offset: <Смещение>; data : <Данные>"	Сообщение выводится после успешного завершения операции WRITE_FILE
"READ_FILE : file size: <Длина файла>; offset: <Смещение>; data : <Данные>;"	Сообщение выводится после успешного завершения операции READ_FILE




## 8.4.2.2.3 Сообщения операций в журнале выполненных сценариев

Сообщения в журнал выполненных сценариев записываются в формате:

"Complete : JaCarta-2 GOST serial:'<Полный серийный номер изделия JaCarta-2 ГОСТ>[<Краткий серийный номер JaCarta-2 ГОСТ>]'; Script name:'<Наименование сценария> '; Ini name:'Имя файла сценария'; JaCarta Admin serial:'<Полный серийный номер изделия JaCarta Admin>[<Краткий серийный номер JaCarta Admin>]';"

## 8.5 Информация о контроле целостности

Для каждого журнала, сценария, или файла возле его имени отображается результат проверки на контроль целостности:

-  – контроль целостности пройден успешно;
-  – обнаружено нарушение контроля целостности (целостность нарушена или произошёл сбой выполнения процедуры контроля);
-  – контроль целостности не удалось осуществить, так как в изделии JaCarta Admin не найден необходимый ключ базы данных.

## ПРИЛОЖЕНИЕ 1

### ФАЙЛОВАЯ СИСТЕМА ИЗДЕЛИЯ JACARTA-2 ГОСТ

Файловая система изделия JaCarta-2 ГОСТ предназначена для хранения произвольных данных в древовидной структуре, состоящей из папок и файлов данных. Каждому файлу/папке при создании присваивается уникальный в пределах содержащей его папки идентификатор размером 2 байта. Идентификатор корневой папки – 3F00h.

Полный путь к файлу – это последовательность двухбайтовых идентификаторов, не включающая идентификатор корневой папки.

Каждый файл/папка имеет 2-байтовый параметр, регламентирующий права доступа к нему согласно таблице 1.

Таблица 1 – Права доступа к файлам и папкам (двухбайтовое слово)

Бит	b <sub>15</sub>	b <sub>14</sub>	b <sub>13</sub>	b <sub>12</sub>	b <sub>11</sub>	b <sub>10</sub>	b <sub>9</sub>	b <sub>8</sub>	b <sub>7</sub>	b <sub>6</sub>	b <sub>5</sub>	b <sub>4</sub>	b <sub>3</sub>	b <sub>2</sub>	b <sub>1</sub>	b <sub>0</sub>
Роль	–	–	–	–	П	А	Г	П	А	Г	П	А	Г	П	А	Г
Права доступа к файлам (и допустимые значения битов)	– (не используются)				Изменение прав доступа			Удаление			Запись			Чтение		
	0	0	0	0	0;1	0;1	0	0;1	0;1	0	0;1	0;1	0; 1	0; 1	0; 1	0; 1
Права доступа к папкам (и допустимые значения битов)	– (не используются)				Изменение прав доступа			Удаление			Создание файла в папке			Получение списка файлов в папке		
	0	0	0	0	0;1	0;1	0	0;1	0;1	0	0;1	0;1	0	1	1	1

Обозначения в таблице 1:

- П – бит, определяющий право доступа пользователя (1 – операция разрешена; 0 – операция запрещена);
- А – бит, определяющий право доступа администратора безопасности (1 – операция разрешена; 0 – операция запрещена);
- Г – бит, определяющий право доступа гостя (1 – операция разрешена; 0 – операция запрещена).

Файловая система на новых изделиях JaCarta-2 ГОСТ состоит из единственной корневой папки со следующими свойствами:

- идентификатор 3F00h;
- права доступа 0437h согласно табл. 1, т.е. по умолчанию в коревой папке:
  - получение списка файлов возможно в любом режиме работы ПО изделия JaCarta-2 ГОСТ;
  - создание файлов возможно только в режиме пользователя или администратора безопасности;
  - изменение прав доступа возможно только в режиме администратора безопасности.

В каждый момент времени один из файлов считается выбранным. По умолчанию выбранным файлом является корневая папка.

Если выбранным файлом является папка, эта папка называется текущей папкой.

Если выбранным файлом является файл данных, текущей является папка, к которой принадлежит выбранный файл.

Выбор файла осуществляется с помощью операции SELECT\_FILE (см. раздел «Операции администрирования изделий», с. 41).

Изделие JaCarta-2 ГОСТ может содержать не более 256 файлов.

Размер файла данных не может превышать 32746 байт.

## ПРИМЕРЫ СЦЕНАРИЕВ ОПЕРАЦИЙ

### Сценарий сброса к заводским настройкам

```
[Settings]
SCRIPT_NAME="Сброс к заводским настройкам"
[Step00]
Action=INIT_PIN
PIN_DATA=z"~tFqB5LQIEe^&wucV+
```

### Сценарий смены ключа администратора безопасности и инициализации изделия JaCarta-2 ГОСТ

Сценарий выполняет смену ключа АБ по умолчанию (в новом изделии JaCarta-2 ГОСТ) на новый ключ АБ, и начальную установку остальных параметров изделия JaCarta-2 ГОСТ. Содержимое файла-сценария:

```
[Settings]
SCRIPT_NAME="Смена ключа АБ и инициализация"
[Step00]
Action=LOGIN
MK_ID=
MK_SEED=
[Step01]
Action=SET_SO_KEY
MK_ID=0000
MK_SM=01
MK_SEED=
[Step02]
Action=INIT
[Step03]
Action=SET_PIN
PIN_DATA=1234567890
[Step04]
Action=SET_PUK
PUK_DATA=1234567890
[Step05]
Action=LOGOUT
```

## Контакты

### Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания «Аладдин Р. Д.»

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) (общий)

Web: <https://www.aladdin-rd.ru>

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

### Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:  
[www.aladdin-rd.ru/support/index.php](http://www.aladdin-rd.ru/support/index.php)



## Ресурсы

### Список литературы

- 1 46538383.62.008.ИЗ. АРМ администратора безопасности JaCarta. Правила пользования [Текст].

---

- 2 RFC 4648. The Base16, Base32, and Base64 Data Encodings [Текст]. – 18 с.

---

- 3 RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms [Текст]. – 51 с.

---

- 4 ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Текст]. – Введ. 2012–08–07. – М. : Стандартинформ, 2012. – 33 с.

---

- 5 Р 50.1.115–2016. Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля [Текст]. – Введ. 2016–11–28. – М. : Стандартинформ, 2016. – 23 с.

## Предметный указатель

### A

AC, 48, 49

### C

CERTIFICATE, 45

CHANGE\_ACCESS, 48

CREATE\_DIR, 48

CREATE\_FILE, 49

CVERIFY, 44, 45

### D

DATA, 43, 45, 47, 49

DELETE\_FILE, 48

DELETE\_KEY, 46

### F

FNAME, 49

### G

GENERATE\_KEY\_PAIR, 44

### H

HMAC, 46

### I

IMPORT\_PUBLIC\_KEY, 44

IMPORT\_SECRET\_KEY, 46

Information Property List, 15

INIT, 41

INIT\_DEF, 42

INIT\_PIN, 42

### K

Key Usage, 45

KEYA, 44

keyCertSign, 45

### L

LENGTH, 50

LOGIN, 41

LOGOUT, 41

lsusb, 15

### M

MK\_ID, 41, 42, 46

MK\_SEED, 41, 42

MK\_SM, 42

### N

NAME, 48, 49

### O

OFFSET, 49, 50

### R

READ\_FILE, 50, 82

### S

SELECT\_FILE, 48

SET\_PASSWORD\_POLICY, 43

SET\_PIN, 42

SET\_PININIT, 43

SET\_PUK, 42

SET\_SO\_KEY, 42

### T

TAG, 47

TBSCertificate, 45

### U

UNBLOCK, 43

### W

WRITE\_FILE, 49

WRITE\_SERVICE\_INFO, 47

### A

администратор безопасности, 2

Аннотация, 2

### Ж

Журнал UNKNOWN, 55

### К

Ключ

базы данных, 20

БД по умолчанию, 20

- О** строки состояния, 60  
центрального потока, 78
- Офис, 88
- П** Сценарий
- Параметр SCRIPT\_NAME, 40
- остановка, 33
- ПДСЧ, 41
- применение, 32, 52
- редактирование, 52
- Подписывание сертификатов, 45
- сброса к заводским настройкам, 87
- смены ключа администратора, 87
- Р**
- Разблокировка, 35
- С**
- Сброс к заводским настройкам, 87
- Секция [Settings], 40
- Сообщения
- в журнал выполненных сценариев, 83
  - диалоговых окон, 62
  - запрашивающие данные или выбор пользователя, 73
  - операций администрирования, 79
  - операций в журнал ошибок, 79
- Т** Техподдержка, 88
- Ф**
- Файл
- загрузка в базу данных, 35
  - сценария, 40
  - удаление из базы данных, 36
- Файловая система изделия JaCarta-2 ГОСТ, 85
- Э** ЭВМ АРМ АБ, 13

