



АКЦИОНЕРНОЕ ОБЩЕСТВО  
«Аладдин Р.Д.»

УТВЕРЖДЕН  
АЛДЕ.467669.004–ЛУ

## USB-НОСИТЕЛЬ «JACARTA SF/ГОСТ»

Руководство по эксплуатации

Часть 2

Руководство администратора для  
среды функционирования Linux

АЛДЕ.467669.004РЭ2

Листов 87

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

## Содержание

1	Описание и работа изделия.....	5
1.1	Общие сведения об изделии .....	5
1.2	Характеристики.....	7
1.3	Устройство и работа.....	11
2	Использование по назначению .....	17
2.1	Порядок работы с изделием .....	17
2.2	Подготовка изделия к использованию.....	18
3	Техническое обслуживание .....	29
4	Текущий ремонт.....	30
5	Хранение и транспортирование.....	31
6	Установка и настройка .....	32
6.1	Общие сведения о программах из комплекта программных средств изделия USB-носитель «JaCarta SF/ГОСТ».....	32
6.2	Установка программ в ОС MSVC 3.0 и настройка изделия.....	38
6.3	Установка программ в MSVC 5.0, АЛЪТ 8 СП, ОС РОСА и настройка изделия.....	43
6.4	Установка программ в Astra Linux Special Edition 1.2 и 1.3 «Смоленск» .....	47
6.5	Установка программ в Astra Linux Special Edition 1.4 «Смоленск» и Astra Linux Special Edition 1.5 «Смоленск» .....	51
6.6	Установка программ в Astra Linux Special Edition 1.6 «Смоленск», Astra Linux Special Edition 8.1 «Ленинград» и «Эльбрус-Д» (ТВГИ.00950-1) .....	56
6.7	Форматирование в ОС семейства Linux.....	67
6.8	Удаление программ.....	69
	Приложение А (обязательное) Политика управления использованием специализированных съемных машинных носителей информации.....	71
	Приложение Б (обязательное) Проверка работоспособности изделия.....	74
	Приложение В (справочное) Термины и определения .....	80
	Приложение Г (справочное) Перечень принятых сокращений .....	86

Первое применение

Справ.№

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Лист	№ докум.	Подп.	Дата
Разраб.		Беленко А.Н.		
Пров.		Страхов О.В.		
Н.Контр.		Бойко А.В.		
Утв.				

<b>АЛДЕ.467669.004РЭ2</b>		
USB-НОСИТЕЛЬ «JACARTA SF/ГОСТ» Руководство по эксплуатации. Часть 2		Литера О <sub>1</sub>
		Лист 2
		Листов 87
Руководство администратора для среды функционирования Linux		АО "Аладдин Р.Д"

Руководство по эксплуатации изделия АЛДЕ.467669.004 «USB-носитель «JaCarta SF/ГОСТ» состоит из трёх книг:

- Часть 1 (РЭ1) — содержит описание работы изделия, его технические характеристики, способы использования, а также руководство по установке программных средств «Программа главного администратора», «Программа администратора» и «Программа пользователя» и последовательность действий, необходимых для ввода изделия в эксплуатацию с помощью данных программных средств в ОС семейства Windows (см. п. 2.1 Порядок работы с изделием).

- Часть 2 (РЭ2) — содержит описание работы изделия, его технические характеристики, способы использования, а также руководство по установке программных средств «Программа главного администратора», «Программа администратора» и «Программа пользователя» и последовательность действий, необходимых для ввода изделия в эксплуатацию с помощью данных программных средств в ОС семейства Linux (см. п. 2.1 Порядок работы с изделием).

- Часть 3 (РЭ3) — содержит описание работы изделия, его технические характеристики, инструкцию по использованию устройства.

В руководстве администратора для ОС Linux на изделии «USB-носитель «JaCarta SF/ГОСТ» содержатся сведения о составе изделия и принципе его действия. В нём описаны основные технические характеристики изделия и рабочие параметры, необходимые для его эксплуатации. В руководство включены описания действий по безопасной установке и настройке программного обеспечения на средствах вычислительной техники под управлением операционных систем (ОС) семейства Linux; условия хранения и транспортирования изделия; подготовка и порядок его использования; действия по текущему ремонту; данные по техническому обслуживанию и описание действий для подготовки к утилизации.

Руководство по эксплуатации изделия предназначено для персонала, прошедшего необходимое обучение и ознакомленного с документами:

- а) АЛДЕ.467669.004ПС «USB-носитель «JaCarta SF/ГОСТ». Паспорт».
- б) RU.АЛДЕ.03.01.005-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа главного администратора. Руководство оператора»;
- в) RU.АЛДЕ.03.01.006-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора»;
- г) RU.АЛДЕ.03.01.007-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа пользователя. Руководство оператора»;

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

						<i>Лист</i>
					<b>АЛДЕ.467669.004РЭ2</b>	3
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		

д) АЛДЕ.03.12.001-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Локальный сервер авторизации. Руководство оператора»;

е) АЛДЕ.02.02.001-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа диагностики. Руководство оператора».

Полный состав эксплуатационной документации, поставляемой с изделием, указан в документе «Ведомость эксплуатационных документов» (АЛДЕ.467669.004ВЭ).

При работе с изделием к уполномоченным пользователям с ролью администратор выдвигаются следующие дополнительные требования:

– пользователь с ролью администратор должен обладать навыками администрирования ОС семейства Linux.

Инв. № подл.	Подпись и дата				Лист
	Взам. инв. №				
	Инв. № дубл.				
Подпись и дата					Лист
Инв. № дубл.					
Взам. инв. №					
Подпись и дата					Лист
Инв. № дубл.					
Взам. инв. №					
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2

# 1 Описание и работа изделия

## 1.1 Общие сведения об изделии

### 1.1.1 Состав и назначение изделия

Изделие АЛДЕ.467669.004 «USB-носитель «JaCarta SF/ГОСТ» представляет собой персональное средство криптографической защиты информации и специализированное средство для безопасного хранения и переноса информации и может быть использовано, как:

– персональное средство криптографической защиты информации JaCarta-2 ГОСТ – защищенное устройство с аппаратной реализацией российских алгоритмов шифрования, хеширования, электронной подписи, обеспечивающее безопасное создание, использование и хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта (далее – СКЗИ, персональное СКЗИ).  
Обозначение изделия – АЛДЕ.26.20.40.140.001;

– специализированное средство для безопасного хранения и переноса информации, предназначенное для предотвращения несанкционированного отчуждения (переноса) информации пользователя, в том числе информации ограниченного доступа, с зарегистрированного (учтенного) специализированного съемного машинного носителя информации.  
Обозначение изделия – АЛДЕ.467669.003;

– персональное СКЗИ и специализированное средство для безопасного хранения и переноса информации.

Изделие АЛДЕ.467669.003 является неотъемлемой частью изделия АЛДЕ.467669.004.

В состав изделия АЛДЕ.467669.004 USB-носитель «JaCarta SF/ГОСТ» входит комплект программного обеспечения, обеспечивающий выполнение изделием своих функций.

В основной комплект программ, устанавливаемых на АРМ входят<sup>1</sup>:

- а) RU.АЛДЕ.03.01.005-01 Программа главного администратора;
- б) RU.АЛДЕ.03.01.006-01 Программа администратора;
- в) RU.АЛДЕ.03.01.007-01 Программа пользователя;
- г) RU.АЛДЕ.03.12.001-01 Локальный сервер авторизации;
- д) RU.АЛДЕ.02.02.002-01 Интерфейсная криптобиблиотека jсPKCS11-2.

Для работы с изделием также используются следующие дополнительные компоненты:

- а) RU.АЛДЕ.02.01.004-01 Программный комплекс обеспечения совместимости;
- б) RU.АЛДЕ.02.02.003-01 Библиотека поддержки СКЗИ «КриптоПро CSP»;
- в) RU.АЛДЕ.02.02.004-01 Библиотека поддержки СКЗИ «Secret Net»;
- г) RU.АЛДЕ.02.02.001-01 Программа диагностики;

<sup>1</sup> Подробнее о составе АРМ в разделах 2.2.3 и 2.2.4 на с. 20 и в разделе 6 на с. 32.

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

										Лист
										5
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

д) RU.АЛДЕ.02.02.005-01 Программа подготовки обновлений.

Работа с СКЗИ реализуется с помощью программ:

- а) RU.АЛДЕ.01.01.007-01 СПО «JaCarta Admin»;
- б) RU.АЛДЕ.02.13.002-03 Утилита контроля целостности;
- в) RU.АЛДЕ.02.13.029-01 Программа администрирования.

Примечание — RU.АЛДЕ.01.01.001-04 «Встроенное программное средство JaCarta OS» входит в комплект поставки изделия в исполнении 5 и предназначено только для обновления. Для всех других исполнений изделия программное средство поставляется в составе изделия в предустановленном виде.

### 1.1.2 Исполнения изделия

Изделие USB-носитель «JaCarta SF/ГОСТ» поставляется в нескольких исполнениях, незначительно отличающихся конструктивными характеристиками.

Исполнения 1 и 2 – являются наиболее старыми исполнениями и более не поставляются. Однако, указанные исполнения могут быть обновлены до исполнений 3 и 4 путём замены программного обеспечения (включая встроенное ПО). При этом исполнение 1 обновляется до исполнения 3, а исполнение 2 до исполнения 4.

Исполнения 3 и 4 также могут быть обновлены до исполнений 6 и 7 (соответственно).

Исполнения 6 и 7 описаны в настоящем руководстве.

С подробной информацией об исполнениях изделия вы можете ознакомиться в документе АЛДЕ.467669.004ПС «USB-носитель “JaCarta SF/ГОСТ”. Паспорт».

**ВНИМАНИЕ!** Исполнение 5 изделия АЛДЕ.467669.004 USB-носитель «JaCarta SF/ГОСТ» предназначено только для обновления изделий.

### 1.1.3 Внешний вид изделия

Внешний вид изделия приведен ниже, на рисунках 1 и 2.



Рисунок 1 – Внешний вид USB-носителя «JaCarta SF/ГОСТ», тип 1, исполнение 6 АЛДЕ.467669.004-06, варианты корпуса 1 и 2

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						6



Рисунок 2 – Внешний вид USB-носителя «JaCarta SF/ГОСТ», тип 2, исполнение 7  
АЛДЕ.467669.004-07, варианты 1, 2 и 3

## 1.2 Характеристики

Характеристики изделия «USB-носитель «JaCarta SF/ГОСТ» приведены ниже в таблицах 1 и 2.

Таблица 1 – Технические характеристики изделия

Наименование характеристики	Значение характеристики
Поддерживаемые платформы	<ul style="list-style-type: none"> <li>– Windows XP SP3;</li> <li>– Windows 7 SP1;</li> <li>– Windows 8;</li> <li>– Windows 8.1;</li> <li>– Windows 10;</li> <li>– Windows Server 2003 (x64);</li> <li>– Windows Server 2008 (x64);</li> <li>– Windows Server 2008 R2 (x64);</li> <li>– Windows Server 2012 (x64);</li> <li>– Astra Linux 1.2 SE «Смоленск»;</li> <li>– Astra Linux 1.3 SE «Смоленск»;</li> <li>– Astra Linux 1.4 SE «Смоленск»;</li> <li>– Astra Linux 1.5 SE «Смоленск»;</li> <li>– Astra Linux 1.6 SE «Смоленск»;</li> <li>– Astra Linux 8.1 SE «Ленинград»;</li> <li>– Альт 8 СП Рабочая станция (64 бит);</li> <li>– Альт 8 СП «Рабочая станция для Эльбрус»;</li> <li>– Альт 8 СП Сервер (64 бит);</li> <li>– МСВС 3.0 (ФЛИР.80001-12 изм. №4);</li> <li>– МСВС 5.0 (ЦАВМ.11004-01 изм. №7);</li> <li>– ОС РОСА «НИКЕЛЬ» (КСФТ.00564-01-1);</li> <li>– ОС РОСА «НИКЕЛЬ» (КСФТ.00564-01-2);</li> <li>– ОС «Эльбрус-Д» (ТВГИ.00950-1).</li> </ul>
Совместимость с программными средствами	<p>Изделие совместимо с:</p> <ul style="list-style-type: none"> <li>– программным обеспечением Secret Net: v.7.6, v.8.5, v.8.6;</li> <li>– SecretNet LSP v 1.7, 1.8, 1.9, 1.10;</li> <li>– программным изделием «Антивирус Dr. Web для рабочих станций Windows» версия 5.0, Серийный образец;</li> <li>– программным изделием «Dr. Web® Enterprise Suite. Антивирусная защита для рабочих станций и серверов Windows» версия 5.0, Серийный образец;</li> <li>– программным изделием «Антивирус Dr. Web для файловых серверов для МСВС 3.0» версия 5.0, Серийный образец;</li> <li>– программным изделием «Антивирус Dr. Web для МСВС 3.0» версия 5.0, Серийный образец;</li> </ul>

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						7

Наименование характеристики	Значение характеристики
	<ul style="list-style-type: none"> <li>– программным изделием “Антивирус Dr.Web® Enterprise Suite для MCBC 3.0” версия 6.0 RU.72110450.00301-06, Серийный образец;</li> <li>– программным изделием “Dr.Web Enterprise Security Suite” версия 6.0 RU.72110450.00300-06, Серийный образец;</li> <li>– программным изделием “Dr.Web Security Space” RU.72110450.00005-09, Серийный образец;</li> <li>– программным изделием “Dr.Web Enterprise Security Suite” RU.72110450.00311-09, Серийный образец;</li> <li>– программным изделием “Антивирус Касперского 8.0 для Linux File Servers” 643.46856491.00049 05 Серийный образец;</li> <li>– программным изделием “Kaspersky Endpoint Security 10 для Windows” 643.46856491.00068-05, Серийный образец;</li> <li>– программным изделием “Kaspersky Security 10 for Windows Servers” 643.46856491.00084-02, Серийный образец;</li> <li>– программным изделием “Kaspersky Security Center совместно с Kaspersky Private Security Network” 643.46856491.00082-03, Серийный образец;</li> <li>– программным изделием “Kaspersky Security 8.0 для Linux Mail Server” 643.46856491.00061-04, Серийный образец;</li> <li>– программным изделием “Kaspersky Security Center 10” 643.46856491.00069-05, Серийный образец;</li> <li>– программным изделием “Kaspersky Anti Targeted Attack Platform” 643.46856491.00086-03, Серийный образец;</li> <li>– программным изделием “Kaspersky Endpoint Security 10 Service Pack 1 для Linux” 643.46856491.00091-01, Серийный образец;</li> <li>– программным изделием “Kaspersky Endpoint Security для Windows (версия 11.0.0.6499)” 643.46856491.00100-01, Серийный образец;</li> <li>– программным изделием “Kaspersky Security 10.1 for Windows Servers” 643.46856491.10084-03, Серийный образец;</li> <li>– программным изделием “Kaspersky Security 8.0 для Linux Mail Server” 643.46856491.10061-06, Серийный образец;</li> <li>– программным изделием “Kaspersky Endpoint Security 10 для Linux” 643.46856491.10105-01, Серийный образец;</li> <li>– программным изделием “Kaspersky Security Center 11” 643.46856491.10069-06, Серийный образец;</li> <li>– программным изделием “Kaspersky Endpoint Security 10 для Linux (Исполнение – Эльбрус)” 643.46856491.10108-01, Серийный образец.</li> </ul>
Возможность хранения в энергонезависимой памяти ключевых контейнеров программных СКЗИ	USB-носитель обеспечивает возможность хранения в энергонезависимой памяти ключевых контейнеров программных СКЗИ («КриптоПро CSP» версий 4.0, 5.0)
Маркировка	<ul style="list-style-type: none"> <li>– На лицевой части корпуса изделия нанесён (выдавлен) логотип – блестящая полированная углубленная надпись на шероховатой матовой поверхности USB-носителя.</li> <li>– На боковой поверхности корпуса изделия нанесен стойкий к истиранию 32-битный уникальный серийный номер (УСН) изделия.</li> <li>– Номер имеет вид: XXXXXXXX, где X – шестнадцатеричный символ 0-9, A, B, C, D, E, F (длина номера – 8 символов). Например, «C723E8BF».</li> <li>– Номер изделия, наносимый на корпус, предназначен для идентификации и учета. Номер является машиночитаемым, и</li> </ul>

Подпись и дата	Инв. № дубл.	Взам. инв. №	Подпись и дата	Инв. № подл.
----------------	--------------	--------------	----------------	--------------



Наименование характеристики	Значение характеристики
	<p>доступен при подключении изделия к средству вычислительной техники с использованием программных средств «Программа администратора» и «Программа пользователя».</p> <p>– Также при подключении изделия к средству вычислительной техники в программах «Программа администратора» и «Программа пользователя» определяется серийный номер MicroSD-карты изделия (флеш-памяти) и серийный номер изделия в зависимости от исполнения:</p> <p>Исполнение 6, тип 1 в формате REDMILXXXXXXXXX,  Исполнение 7, тип 2 в формате BLUEMILXXXXXXXXX,  где XXXXXXXX – это УСН изделия, нанесенный на боковую поверхность корпуса.</p>

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

Изм.	Лист	№ документа	Подпись	Дата	<p>Изм.</p> <p>Лист</p> <p>№ документа</p> <p>Подпись</p> <p>Дата</p>
Изм.	Лист	№ документа	Подпись	Дата	
Изм.	Лист	№ документа	Подпись	Дата	

Изм.	Лист	№ документа	Подпись	Дата	Лист
------	------	-------------	---------	------	------

АЛДЕ.467669.004РЭ2

Таблица 2 – Эксплуатационные характеристики изделия

Наименование характеристики	Значение характеристики
Рабочая температура, °С	от 15 до 25 включительно
Температура хранения, °С	от минус 40 до плюс 85 включительно
Относительная влажность воздуха эксплуатации при температуре от плюс 15 до плюс 25 °С, %	от 45 до 75 включительно
Относительная влажность воздуха хранения, %	Не более 100% включительно (без конденсата)
Срок хранения данных в памяти, годы	Не менее 10
Количество циклов перезаписи в одну ячейку Флеш-памяти MicroSD-карты	Не менее 10000
Потребляемый ток, мА	300. Электрическое питание осуществляется по шине USB. Изделие не имеет встроенных источников питания (батареяк, аккумуляторов)
Рабочее напряжение, В	от 4.75 до 5.25 включительно
Объем флеш-памяти, ГБ	8 или 16, или 32
Пылезащищенность	Корпус защищает внутренний монтаж и детали (микросхемы) от попадания пыли. Пыль может попасть на контактную площадку внутри незащищенной части USB-разъема, но до начала эксплуатации ее необходимо удалить продуванием. Допускается хранение изделия с надетым на USB-разъем защитным колпачком в постоянно пыльных помещениях. Допускается использование изделия в пыльных помещениях. Соответствует степени защиты IP57 по ГОСТ 14254.
Соответствие стандартам	USB-носитель соответствует требованиям следующих документов: – ГОСТ-Р ИСО/МЭК 7816-4-2013; – «PC/SC Workgroup Specifications Revision 2.01.14» (PC/SC версия 2.01.14, части 1 - 10); – «Universal Serial Bus Specification Revision 2.0» (USB версия 2.0); – «Universal Serial Bus. Device Class: Smart Card. CCID. Specification for Integrated Circuit(s) Cards Interface Devices. Revision 1.1» (CCID версия 1.1); – ITU-T Rec.X.509 (X.509); – PKCS#11 (версия 2.30); – USB-носитель совместим с USB версии 3.0 (работает с контроллером USB версии 3.0, но контроллер должен поддерживать или быть включен в режиме совместимости с USB версии 2.0); – ГОСТ 30805.22-2013; – ГОСТ CISPR 24-2013.

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						10

## 1.3 Устройство и работа

### 1.3.1 Назначение составных частей

Изделие АЛДЕ.467669.004 USB-носитель «JaCarta SF/ГОСТ» включает в себя:

а) Персональное средство криптографической защиты информации «JaCarta-2 ГОСТ» (АЛДЕ.26.20.40.140.001). Функциональные возможности изделия описаны в следующих документах:

1) 46538383.62.001.ФО «Средство криптографической защиты информации «Криптотокен 2 ЭП» в составе изделия JaCarta ГОСТ. Исполнения 9 и 10. Формуляр»;

2) 46538383.62.001.ИЗ «Средство криптографической защиты информации «Криптотокен 2 ЭП» в составе изделия JaCarta ГОСТ. Исполнения 9 и 10. Правила пользования»;

3) 46538383.62.008.ФО «Средство криптографической защиты информации «АРМ администратора безопасности JaCarta. Формуляр»;

4) 46538383.62.008.ИЗ «АРМ администратора безопасности JaCarta. Правила пользования».

б) «USB-носитель «JaCarta SF/ГОСТ». Специализированное средство для безопасного хранения и переноса информации» (АЛДЕ.467669.003) включает в свой состав:

1) изделие АЛДЕ.467669.002 «Специализированный съемный машинный носитель информации» (далее – специализированный съемный машинный носитель информации, машинный носитель). Специализированный съемный машинный носитель информации предназначен для хранения информации пользователя (данных пользователя) в разделах встроеной флеш-памяти;

2) программное изделие RU.АЛДЕ.03.01.003-01 «Комплект программных средств» (далее – комплект программных средств). Комплект программных средств предназначен для организации взаимодействия пользователей и средств вычислительной техники с подключаемыми специализированными съемными машинными носителями информации.

Специализированный съемный машинный носитель информации (б.1) включает в свой состав:

- изделие АЛДЕ.467669.001 «Электронный носитель»;
- RU.АЛДЕ.01.01.001-04 «Встроенное программное средство «JaCarta OS» (далее – встроенное программное средство).

Электронный носитель основан на изделии АЛДЕ.467359.001 «Аппаратная платформа JaCarta-2» и включает в себя:

- ведущий микроконтроллер изделия;
- микроконтроллер смарт-карты;
- microSD-карту (флеш-память);

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

Лист

АЛДЕ.467669.004РЭ2

11

Изм. Лист № документа Подпись Дата

- печатный узел JaCarta-2;
- корпус;
- съёмный колпачок.

Хранение и перенос информации осуществляется на microSD-карте из состава изделия (во встроенной флеш-памяти).

### 1.3.2 Структура флеш-памяти изделия

Встроенную флеш-память можно использовать следующим образом:

а) область флеш-памяти «Открытый CD-ROM раздел»<sup>1</sup>. Информация в данном разделе доступна пользователю только для чтения, без возможности её изменения. Раздел «Открытый CD-ROM раздел» идентифицируется операционной системой как DVD/CD-ROM дисковод с постоянно подключённым CD-ROM диском. При этом:

1) «Открытый CD-ROM раздел» может быть записан только при инициализации специализированного съёмного машинного носителя информации при функционировании специализированного средства для безопасного хранения и переноса информации в режиме «администратор».

2) «Открытый CD-ROM раздел» может быть отформатирован как загрузочный диск, на который может быть записан эталонный образ операционной системы и прикладных программных средств, необходимых для автономной работы на различных средствах вычислительной техники.

3) «Открытый CD-ROM раздел» появляется в операционной системе сразу при подключении специализированного съёмного машинного носителя информации.

б) область флеш-памяти «Скрытый CD-ROM раздел». Информация в данном разделе доступна пользователю только для чтения, без возможности её изменения. Раздел доступен пользователю, успешно прошедшему идентификацию и аутентификацию. «Скрытый CD-ROM раздел» идентифицируется операционной системой как DVD/CD-ROM дисковод с постоянно подключённым CD-ROM диском только на тех средствах вычислительной техники, на которых установлены компоненты программного комплекса интеграции и администрирования.

в) область флеш-памяти «Открытый RW раздел». Информация пользователя в данном разделе доступна на чтение-запись. «Открытый RW раздел» идентифицируется операционной системой как постоянно подключённое дисковое устройство (машинный носитель информации). При этом:

---

<sup>1</sup> Здесь и далее определены условные наименования условных разделов флеш-памяти. Наименования присвоены с учетом их видимости операционной системой и возможности записи на них информации. В качестве прототипа приняты наименования, используемые для носителей оптической записи.

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

					<b>АЛДЕ.467669.004РЭ2</b>	<i>Лист</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		12

1) наличие данного раздела не является обязательным для функционирования специализированного съемного машинного носителя информации. Решение о его включении в состав машинного носителя информации принимается администратором;

2) «Открытый RW раздел» может использоваться для хранения и переноса информации между средствами вычислительной техники;

3) «Открытый RW раздел» появляется в операционной системе при подключении специализированного съемного машинного носителя информации.

**ВНИМАНИЕ!** В данный раздел не должна помещаться информация пользователя, относящаяся к информации ограниченного доступа, так как контроль отчуждения информации для данного раздела флеш-памяти не осуществляется.

г) область флеш-памяти «Скрытый RW раздел». Информация пользователя в данном разделе доступна на чтение-запись. Раздел доступен пользователю, успешно прошедшему идентификацию и аутентификацию. Раздел «Скрытый RW раздел» идентифицируется операционной системой как постоянно подключённое дисковое устройство (машинный носитель информации) только на средствах вычислительной техники, на которых установлены компоненты программного комплекса интеграции и администрирования.

д) область флеш-памяти «Скрытый системный раздел». Информация в данном разделе доступна на чтение-запись только для встроенного программного средства.

**ВНИМАНИЕ!** Скрытый системный раздел создаётся автоматически, не виден администратору изделия и не учитывается в общем числе разделов при инициализации.

Количество разделов флеш-памяти изделия задаётся при его инициализации и должно быть не менее одного и не более четырех а) – г), а также, не должно быть более одного раздела каждого вида.

Для работы с информацией на скрытом CD-ROM и скрытом RW дисковом накопителе необходимо пройти авторизацию на АРМ Пользователя в программном средстве «Программа пользователя».

При этом, авторизация на рабочем месте пользователя возможна с помощью одного из способов:

- при предъявлении ключевого контейнера администратора с помощью средства защиты от несанкционированного доступа Secret Net/Secret Net Studio и пароля пользователя;
- при подтверждении полномочий пользователя с помощью специализированного съемного машинного носителя информации, инициализированного контейнером Администратора (далее – ЭН Администратора доступа) и пароля пользователя;
- с помощью настраиваемого программного средства АЛДЕ.03.12.001-01. «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Локальный сервер авторизации» (далее – Локальный сервер

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						13

авторизации) при предъявлении пароля пользователя;

– с помощью ключевого контейнера автономного доступа, при условии предъявления пароля пользователя.

ЭН Администратора доступа создаётся при вводе изделия в эксплуатацию с помощью АРМ Главного Администратора, а также программных средств «Программа главного администратора» и «Программа администратора».

Авторизация пользователя с помощью ЭН Администратора доступа или Локального сервера авторизации с точки зрения пользователя – описана в документе АЛДЕ.467669.004РЭЗ. «USB-носитель «JaCarta SF/ГОСТ». Руководство по эксплуатации. Часть 3. Руководство пользователя».

Краткое описание всех разделов флеш-памяти изделия представлено ниже в таблице 3. Обратите внимание, что таблица 3 содержит краткое представление информации представленной в этом разделе, и предназначена только для ознакомления.

Таблица 3 – Разделы флеш-памяти USB-носителя «JaCarta SF/ГОСТ»

Название раздела	Описание	Представление на АРМ пользователя
Открытый CD-ROM	Раздел флеш-памяти изделия, представляющий CD-ROM с файловой системой CDFS	При подключении изделия определяется как CD-ROM (файловая система CDFS)
Скрытый CD-ROM	Раздел флеш-памяти изделия, представляющий CD-ROM с файловой системой CDFS, доступный после аутентификации пользователя	При подключении изделия не определяется (недоступен) до аутентификации пользователя в Программе пользователя. После аутентификации определяется как CD-ROM (файловая система CDFS)
Открытый RW	Раздел флеш-памяти изделия, представляющий съемное дисковое устройство	Определяется как постоянно подключенное дисковое устройство при подключении изделия к АРМ пользователя
Скрытый RW	Раздел флеш-памяти изделия, представляющий съемное дисковое устройство, доступное после аутентификации пользователя в Программе пользователя	При подключении изделия к АРМ не определяется (недоступен) до аутентификации пользователя. После аутентификации пользователя в Программе пользователя определяется как постоянно подключенное дисковое устройство
Служебный раздел (Скрытый системный раздел)	Раздел контролируется встроенным программным средством «JaCarta OS» и используется для хранения служебной информации, связанной с изделием, включая Системный журнал	Не виден пользователям

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭЗ	Лист
						14

### 1.3.3 Возможности использования изделия

В зависимости от конфигурации изделия, которая производится с помощью комплекта программных средств из состава изделия, USB-носитель «JaCarta SF/ГОСТ» может использоваться:

- специализированное средство для безопасного хранения и переноса информации, предназначенное для предотвращения несанкционированного отчуждения (переноса) информации пользователя, в том числе информации ограниченного доступа, с зарегистрированного (учтенного) специализированного съемного машинного носителя информации. (далее – электронный носитель, ЭН);
- только как средство криптографической защиты информации (далее – СКЗИ);
- как комбинированное устройство СКЗИ и ЭН.

Ввод изделия в эксплуатацию как ЭН подразделяется на следующие виды электронных носителей с управлением доступом к данным:

– ЭН пользователя. Возможна конфигурация изделия с разделами: Открытый CD-ROM, скрытый CD-ROM, открытый RW, скрытый RW. Как было указано выше, количество разделов флеш-памяти для ЭН Пользователя может быть не менее одного и не более четырех, при этом не должно быть более одного раздела каждого вида.

– ЭН администратора доступа — электронный носитель, который имеет возможность авторизовывать доступ к скрытым разделам флеш-памяти (скрытый CD-ROM, скрытый RW) для ЭН Пользователя на АРМ Пользователя. При этом сам ЭН Администратора доступа не имеет скрытых разделов флеш-памяти.

Ввод USB-носителя в эксплуатацию как СКЗИ выполняется с помощью программных средств из состава СКЗИ «Криптотокен 2 ЭП».

Ввод изделия в эксплуатацию как комбинированного устройства выполняется Администратором доступа как с помощью программных средств «Программа главного администратора», «Программа администратора», «Программа пользователя», которые входят в состав программного комплекса интеграции и администрирования и соответствующего автоматизированного рабочего места (далее – АРМ), так и с помощью программных средств из состава СКЗИ «Криптотокен 2 ЭП».

Подробный ввод изделия в эксплуатацию рассмотрен в п. 2.2.3 Подготовка изделия к вводу в эксплуатацию в качестве СКЗИ и п. 2.2.4 Подготовка изделия к вводу в эксплуатацию в качестве ЭН.

USB-носитель «JaCarta SF/ГОСТ» работает на основе ролевой модели управления доступом.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						15

Таблица 4 – Роли пользователей изделия

Роль	Основная программа АРМ	Функции и возможности
Гость	–	Просмотр информации на открытых разделах флеш-памяти
Пользователь ЭН	RU.АЛДЕ.03.01.007-01 Программа пользователя	Просмотр защищаемой информации, хранимой на скрытых разделах изделия
Администратор (доступа) ЭН	RU.АЛДЕ.03.01.006-01 Программа администратора	Инициализация носителей на основе правил, создаваемых главным администратором изделия. Управление (администрирование ЭН пользователя). Авторизация подключения скрытых разделов. Обновление изделий. Аудит изделий.
Главный администратор	RU.АЛДЕ.03.01.005-01 Программа главного администратора	Управление политиками безопасности изделия. Создание ключевых контейнеров администратора (элементов аутентификации и носителей правил).
Пользователь СКЗИ	–	Использование электронной подписи.
Администратор СКЗИ	RU.АЛДЕ.02.13.029-01 Программа администрирования	Инициализация и обезличивание СКЗИ. Считывание журнала СКЗИ.

**ВНИМАНИЕ!** Кроме основной программы на АРМ могут устанавливаться дополнительные, в частности, в подразделе «2.2.4.2» (с.22) в основном сценарии использования, на АРМ Главного администратора и администратора устанавливаются две основные программы.

Инв. № подл.					Лист
	Инв. № дубл.	Взам. инв. №	Подпись и дата	Подпись и дата	
Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	Лист
Изм.	Лист	№ документа	Подпись	Дата	<p style="text-align: center;">АЛДЕ.467669.004РЭ2</p> <p style="text-align: right;">16</p>



## 2 Использование по назначению

### 2.1 Порядок работы с изделием

Работа с изделием осуществляется в следующем порядке:

а) Приёмка партии изделий представителями заказчика и проведение подготовительных процедур:

- 1) ознакомление персонала с эксплуатационной документацией на изделие;
- 2) определение состава административного персонала (таблица 4 с. 16);
- 3) определения перечня средств вычислительной техники для работы с изделием USB-носитель «JaCarta SF/ГОСТ»;

4) разработка необходимой организационно-распорядительной и организационно-технической документации.

б) Подготовка средств вычислительной техники к вводу в эксплуатацию изделия USB-носитель «JaCarta SF/ГОСТ», в том числе: настройка параметров безопасности ОС и установка программ из состава изделия на АРМ, определённые для работы с изделием в соответствии с пунктом (а). Подробная информация о подготовке СБТ и установке программ приведена в разделах 2.2.4.2 (с. 22) и 6.1.3 (с. 35).

в) Подготовка изделий USB-носитель «JaCarta SF/ГОСТ» к вводу в эксплуатацию, и ввод в эксплуатацию:

- 1) реализация правил эксплуатации изделия в виде ключевых контейнеров;
- 2) инициализация изделий в качестве ЭН;
- 3) инициализация изделий в качестве СКЗИ (опционально);
- 4) сохранение ключевых контейнеров СЗИ (опционально);
- 5) настройка локального сервера авторизации, создание контейнеров автономного монтирования;
- 6) форматирование RW-разделов специализированного съёмного машинного носителя;
- 7) передача ЭН конечным пользователям.

г) Эксплуатация изделий.

д) Вывод изделий из эксплуатации, утилизация (раздел 2.3.3 с. 27).

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата					Лист
									17
					Изм.	Лист	№ документа	Подпись	Дата

## 2.2 Подготовка изделия к использованию

### 2.2.1 Эксплуатационные ограничения

Нормальными (расчетными) условиями эксплуатации изделия являются<sup>1</sup>:

- непрерывная работа без отключения USB-носителя от средства вычислительной техники – не более 24 часов в день;
- циклов записи в EEPROM-память USB-носителя – не более 500 в сутки;
- циклов «Подключение/отключение USB-носителя» – не более 6 в сутки;
- допустимое количество выхода из строя USB-носителей из-за отказа электронных компонентов в течение всего гарантийного срока эксплуатации — не более 2% от общего числа изделий в поставляемой партии.

Отклонения условий эксплуатации от нормальных могут приводить к преждевременному износу и выработке ресурса изделия. При соблюдении нормальных (расчетных) условий эксплуатации наработка не превысит следующих предельных значений ресурса USB-носителя:

- 10 000 часов общей наработки изделия;
- 5 000 циклов «Подключение/отключение USB-носителя»;
- 10 000 циклов записи в флеш-память USB-носителя.

Информация о наработке сохраняется в системном журнале USB-носителя и может быть использована в качестве рекомендации о необходимости замены изделия на новое. При превышении предельных значений наработки безотказное функционирование USB-носителя изготовителем не гарантируется, а гарантийные обязательства на данное изделие не распространяются. При этом, превышение предельных значений наработки хотя бы по одному параметру, указанных выше, может явиться причиной отказа изготовителя от гарантийных обязательств.

Изделие «USB-носитель «JaCarta SF/ГОСТ» предназначено для использования в отапливаемых помещениях и может эксплуатироваться в условиях круглосуточной или сменной работы с техническими перерывами.

Нормальными климатическими условиями эксплуатации USB-носителя являются:

- температура окружающего воздуха: от плюс 15 до плюс 25 °С;
- относительная влажность окружающего воздуха при температуре от плюс 15 до плюс 25 °С: от 45 до 75%;
- атмосферное давление: от 630 до 800 мм рт. ст. (от 84 до 107 кПа).

<sup>1</sup> Значения параметров нормальных (расчетных) условий эксплуатации изделия рассчитываются исходя из 245 рабочих дней в году.

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

					АЛДЕ.467669.004РЭ2					<i>Лист</i>
										18
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>						

Объём флеш-памяти изделия определяется в сопроводительной документации на конкретный образец продукции.

Для USB-носителя не допускается:

- воздействие статического разряда напряжением более 5000 В;
- воздействие радиации и сильных электромагнитных полей;
- однократные ударные воздействия эквивалентные свободному падению с высоты более 1 м либо аналогичные ударные воздействия;
- случайные вибрации степени жёсткости выше 4с по ГОСТ 30631–99:
  - 1) в диапазоне 10–200 Гц, спектральная плотность ускорения не должна превышать 0,3 м2/с3 при среднеквадратическом значении ускорения 8 м/с2;
  - 2) в диапазоне 200–2000 Гц, спектральная плотность ускорения не должна превышать 0,1 м2/с3 при среднеквадратическом значении ускорения 15 м/с2.

## 2.2.2 Требования безопасности при подготовке изделия к использованию

1) JaCarta SF/ГОСТ используется совместно со средствами вычислительной техники. Средства вычислительной техники должны быть исправны и заземлены, персонал, допущенный к работе со средствами вычислительной техники, должен пройти соответствующий занимаемой должности инструктаж и обладать необходимой группой электробезопасности. Использование средств вычислительной техники при работе с изделием должно осуществляться при условии выполнения общих требований документов «Правила технической эксплуатации электроустановок потребителей» и «Правила по охране труда при эксплуатации электроустановок».

2) К работе с JaCarta SF/ГОСТ должен допускаться персонал, изучивший эксплуатационные документы, соответствующие выполняемым ролям; прошедший обучение и проверку знаний в соответствии с инструкциями, регламентирующими порядок эксплуатации защищенных машинных носителей.

3) Ввод JaCarta SF/ГОСТ в эксплуатацию должен проводиться в соответствии с настоящим руководством по эксплуатации.

4) Эксплуатация USB-носителя должна проводиться при нормальных климатических условиях, представленных выше.

5) Не допускается использование USB-носителя в случае повреждения USB-разъема или повреждения его контактной группы, наличия в разъеме следов влаги, грибков, солей, мусора или других загрязнений. Внимательно осматривайте носитель на предмет наличия повреждений.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						19

6) Не допускается подключение USB-носителя к заведомо повреждённым USB-интерфейсам средств вычислительной техники, либо подключение через USB-удлинители, не гарантирующие выполнение требований по питанию, выдвигаемых к стандартному исправному USB-интерфейсу в соответствии со спецификацией, и приведённых в таблице 2.

При выполнении работ по техническому обслуживанию запрещается:

- 1) подключать оборудование к неисправной сети электроснабжения и средствам вычислительной техники с неисправным заземлением;
- 2) осуществлять перемещение оборудования, подключенного к сети электроснабжения;
- 3) использовать неисправное оборудование и средства измерительной техники с истекшим сроком поверки.

### 2.2.3 Подготовка изделия к вводу в эксплуатацию в качестве СКЗИ

Чтобы подготовить изделие к эксплуатации в качестве СКЗИ, необходимо использовать АРМ 46538383.62.008 «Средство криптографической защиты информации «АРМ администратора безопасности JaCarta».

Перед подготовкой изделия к работе в качестве СКЗИ администратор доступа должен ознакомиться со следующей эксплуатационной документацией:

- Руководство оператора программы администрирования СКЗИ «АРМ администратора безопасности» (RU.АЛДЕ.02.13.029-01 34 02). Данный документ содержит сведения, необходимые для эксплуатации средства криптографической защиты информации (СКЗИ) «АРМ администратора безопасности» – автоматизированного рабочего места администратора безопасности (АРМ АБ).
- Правила пользования средства криптографической защиты информации «АРМ администратора безопасности JaCarta» (46538383.62.008.ИЗ). Данный документ предназначен для операторов «АРМ администратора безопасности», выполняющих администрирование СКЗИ «Криптотокен 2 ЭП». Исполнение 9» в составе изделий JaCarta-2 ГОСТ.

### 2.2.4 Подготовка изделия к вводу в эксплуатацию в качестве ЭН

#### 2.2.4.1 Понятия, используемые при описании ввода носителя в эксплуатацию

**Ввод в эксплуатацию** – комплексный процесс, включающий приёмку, первичную поверку изделий, заполнение эксплуатационной документации, подготовку рабочих мест и инициализацию USB-носителей.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						20

Обратите внимание, что часть процессов по вводу изделия в эксплуатацию определяется внутренними нормативными документами Вашей организации.

**Инициализация** – процесс начальной установки параметров изделия USB-носитель «JaCarta SF/ГОСТ». Изделие инициализировано, если заданы следующие параметры:

- выбраны и созданы разделы изделия;
- созданы журналы аудита изделия;
- создан ПИН-код;
- для изделия установлены политики безопасности;
- на изделие записаны закрытые ключи.

Изделие не инициализировано, если параметры имеют неопределенное значение. Неинициализированное изделие не подлежит передаче пользователю. Процесс инициализации изделия выполняется в «Программе администратора» с помощью соответствующего *ключевого контейнера*, создаваемого Главным администратором изделия.

Обратите внимание, что для создания и управления ЭН администратора необходим ключевой контейнер администратора доступа и неинициализированный USB-накопитель, а для инициализации ЭН Пользователя – и ключевой контейнер пользователя и ЭН администратора.

**Обезличивание** – процесс очистки изделия «USB-носитель «JaCarta SF/ГОСТ» от персональных данных пользователя. Изделие является обезличенным, если у него очищена флеш-память и сброшен ПИН-код. Процедура обезличивания выполняется в «Программе администратора». После процедуры обезличивания данные, сохраненные на изделии «USB-носитель «JaCarta SF/ГОСТ» восстановлению не подлежат.

**Ключевой контейнер** – это способ хранения закрытых ключей и правил эксплуатации конкретного изделия. Ключевой контейнер является файлом, содержащим информацию для управления изделиями USB-носитель «JaCarta SF/ГОСТ». Для доступа к ключевому контейнеру устанавливается пароль. Ключевые контейнеры необходимо перевыпускать после указанного при установке правил срока эксплуатации. Информация о необходимых для этого действиях описана в документе RU.АЛДЕ.03.01.006-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора».

**Ключевой контейнер администратора доступа** – ключевой контейнер, предназначенный для инициализации и обезличивания ЭН Администратора доступа. Создание ключевого контейнера администратора доступа выполняется в «Программе главного администратора».

**ВНИМАНИЕ!** Ключевой контейнер администратора должен сохраняться до вывода из эксплуатации (или обезличивания) всех инициализированных на его основе носителей, включая ЭН пользователей.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						21

*Ключевой контейнер пользователя* – ключевой контейнер, предназначенный для инициализации и обезличивания ЭН Пользователя. Создание ключевого контейнера пользователя выполняется в программе главного администратора.

**ВНИМАНИЕ!** Ключевой контейнер пользователя должен сохраняться до вывода из эксплуатации (или обезличивания) всех инициализированных на его основе носителей пользователей.

*Ключевой контейнер для обновления разделов CD-ROM* – ключевой контейнер, предназначенный для перезаписи доступных только для чтения «разделов CD-ROM» изделия. Данный ключевой контейнер формируется в программе главного администратора.

*Автономный доступ* – подключение скрытых разделов флеш-памяти ЭН Пользователя с помощью ключевого контейнера автономного доступа на любом средстве вычислительной техники. Данное подключение скрытых разделов выполняется в программе пользователя.

*Ключевой контейнер автономного доступа к скрытым разделам флеш-памяти* – файл, предназначенный для обеспечения автономного доступа к скрытым разделам флеш-памяти ЭН Пользователя. Данный файл можно создать с помощью программы администратора.

*Локальный сервер авторизации* – сетевой сервер, с помощью которого пользователь может подключить скрытые разделы флеш-памяти ЭН (входит в комплект поставки) в том числе через удалённое подключение. Подключение осуществляется с помощью *ключевого контейнера локального сервера авторизации*.

*Ключевой контейнер локального сервера авторизации* – ключевой контейнер, предназначенный для доступа к скрытым разделам флеш-памяти ЭН Пользователя с помощью программы «Локальный сервер авторизации». Данный ключевой контейнер создается в программе администратора и передается администратором доступа на локальный сервер авторизации.

#### 2.2.4.2 Подготовка АРМ

Для ввода в эксплуатацию USB-носителей JaCarta SF/ГОСТ, необходимо подготовить АРМ:

а) АРМ главного администратора с установленными программами:

1) RU.АЛДЕ.03.01.005-01 «USB-носитель «JaCarta SF/ГОСТ». Программа главного администратора»;

2) RU.АЛДЕ.03.01.006-01 «USB-носитель «JaCarta SF/ГОСТ». Программа администратора».

*Назначение АРМ:* создание ключевых контейнеров и подготовки к эксплуатации ЭН Администратора доступа.

б) АРМ администратора доступа с установленными программами:

Подпись и дата	Име. № дубл.	Взам. инв. №	Подпись и дата	Име. № подл.						Лист
					АЛДЕ.467669.004РЭ2					22
Изм.	Лист	№ документа	Подпись	Дата						

1) RU.АЛДЕ.03.01.005-01 «USB-носитель «JaCarta SF/ГОСТ». Программа главного администратора»;

2) RU.АЛДЕ.03.01.007-01 «USB-носитель «JaCarta SF/ГОСТ». «Программа пользователя»

*Назначение АРМ:* подготовка носителей к эксплуатации, управление ЭН Пользователей, создание *ключевых контейнеров авторизации и ключевых контейнеров локального сервера авторизации*, используемых для авторизации средств вычислительной техники для работы с конкретными ЭН пользователя.

в) АРМ пользователя:

1) «Программа пользователя». АРМ Пользователя используется для работы с ЭН Программы пользователя.

2) В том случае, если Пользователю необходима возможность хранения в энергонезависимой памяти ключевых контейнеров программных СКЗИ (КриптоПро CSP 4.0, 5.0) необходимо установить программное средство RU.АЛДЕ.02.02.003-01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Библиотека поддержки СКЗИ «КриптоПро CSP». Инструкция по использованию изделия для хранения ключевого контейнера КриптоПро CSP описана в документе «ЖТЯИ.00050-03 90 03 КриптоПро CSP. Инструкция по использованию».

*Назначение АРМ:* Подключение скрытых разделов изделия JaCarta SF/ГОСТ на рабочем месте пользователя.

Примечание — Установка программ производится в соответствии с подразделом 6 настоящего документа.

#### 2.2.4.3 Подготовка носителей JaCarta SF/ГОСТ к использованию

Перед использованием изделия пользователь с ролью «(главный) администратор» должен:

- а) проверить состояние упаковки и вынуть изделие из заводской упаковки;
- б) проверить комплект поставки в соответствии с Паспортом (АЛДЕ.467669.004ПС) и гарантийным талоном на изделие;
- в) убедиться в отсутствии механических повреждений изделия;
- г) извлечь изделие из пенала, снять защитный колпачок;
- д) подключить изделие к АРМ Главного администратора или АРМ Администратора доступа.

#### 2.2.4.4 Последовательность действий для подготовки изделия в качестве ЭН администратора доступа или ЭН пользователя

Чтобы подготовить изделия к эксплуатации как ЭН, необходимо выполнить действия, указанные ниже.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						23

На АРМ Главного администратора:

- а) запустите программу главного администратора;
- б) подключите USB-носитель «JaCarta SF/ГОСТ» к АРМ Администратора доступа;
- в) выберите в выпадающем меню подключенный USB-носитель;
- г) выберите необходимые политики и создайте *ключевой контейнер администратора доступа*;

Примечание — Действия, необходимые для создания ключевого контейнера администратора доступа, описаны в документе RU.АЛДЕ.03.01.005-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа главного администратора. Руководство оператора». запустите программу администратора.

д) в программе администратора выполните инициализацию USB-носителя в качестве ЭН Администратора доступа, используя ключевой контейнер администратора доступа, созданный в пункте а) – г);

Примечание — Действия по инициализации ЭН администратора доступа описаны в документе RU.АЛДЕ.03.01.006-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора».

**ВНИМАНИЕ!** Запуск инициализации изделия должен осуществляться непосредственно с АРМ, на котором производится инициализация. Инициализация не может осуществляться с помощью протокола RDP (Remote desktop protocol).

е) в программе главного администратора создайте ключевой контейнер пользователя, используя созданный ключевой контейнер администратора доступа и инициализированный с помощью действий, описанных в пунктах а) – е) ЭН Администратора доступа.

Примечание — Действия, необходимые для создания ключевого контейнера пользователя, описаны в документе RU.АЛДЕ.03.01.005-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа главного администратора. Руководство оператора».

ж) Передайте на АРМ администратора доступа инициализированный ЭН администратора доступа, созданный на шаге е), а также ключевой контейнер пользователя созданный на шаге ж).

**ВНИМАНИЕ!** Рекомендуется подготовить резервный ЭН администратора доступа и ключевой контейнер пользователя, созданный с его помощью. Для этого необходимо повторить шаг е) используя ключевой контейнер администратора доступа, созданный в пункте г).

Примечание — С помощью резервного ЭН администратора доступа можно будет выполнять все необходимые функции администрирования для ЭН пользователей, инициализированных основным ЭН Администратора доступа.

На АРМ Администратора доступа выполните следующие действия:

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

									Лист
									24
Изм.	Лист	№ документа	Подпись	Дата					



а) запустите программу администратора;

б) выполните инициализацию ЭН пользователя, используя переданные с АРМ Главного администратора ключевой контейнер пользователя и инициализированный ЭН Администратора доступа;

Примечание — Действия, необходимые для создания ключевого контейнера пользователя, описаны в документе RU.АЛДЕ.03.01.005-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа главного администратора. Руководство оператора».

в) в том случае, если инициализированный ЭН Пользователя должен иметь скрытый RW раздел, Администратору доступа необходимо подключить его в Программе пользователя. Действия, требуемые для подключения скрытых разделов Флеш-памяти, описаны в документе RU.АЛДЕ.03.01.007-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа пользователя. Руководство оператора»;

г) выполните форматирование RW-раздела (см. п. 6.7 на с. 67).

### 2.3 Использование изделия

#### 2.3.1 Правила эксплуатации

Для изделия необходимо соблюдать следующие правила эксплуатации:

– **запрещается извлекать изделие из USB-порта средства вычислительной техники и/или прерывать подачу питания на него при мигающем световом индикаторе.** Неисполнение данного правила может привести к потере или порче записываемых во флеш-память изделия данных или нарушению его работоспособности. Информация обо всех некорректно прерванных операциях (во время чтения/записи данных на флеш-память, выполнения криптографических вычислений и т.п.) фиксируется в системном журнале USB-носителя и может служить основанием для выявления и подтверждения фактов нарушения правил эксплуатации и отказа изготовителя от гарантийных обязательств;

– **запрещается использование изделия при несоответствии параметров электрического питания от USB-порта средства вычислительной техники.** Если изделию не хватает необходимой мощности электрического питания, то оно может не начать работу или работать неустойчиво (со сбоями или отказами), которые могут привести к потере и/или искажению данных. Параметры электрического питания должны соответствовать следующим значениям: напряжение питания от 4.75 до 5.25 В при силе тока 300 мА;

– **извлечение изделия должно выполняться только после успешного выполнения процедуры «Безопасное извлечение устройств и дисков» (для операционных систем семейства Microsoft Windows) или команды (процедуры) размонтирования (для**

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

операционных систем семейства Linux). Это связано с особенностями работы операционных систем с внешними запоминающими устройствами (дисками): для ускорения работы часть данных сохраняется в памяти средства вычислительной техники, и при некорректном извлечении USB-носителя эти данные скорее всего будут потеряны (не будут принудительно записаны на изделие во время выполнения процедуры извлечения);

- **запрещается использование средств виртуализации для средств вычислительной техники**, на которых предполагается выполнять подключение скрытых разделов флеш-памяти USB-носителя (разделы «Скрытый CD-ROM раздел» и «Скрытый RW раздел»);

- **извлечение изделия с подключенными скрытыми разделами флеш-памяти (разделы «Скрытый CD-ROM раздел» и «Скрытый RW раздел»), должно выполняться только после успешного выполнения команды «Отключить скрытые разделы».** Команда выполняется с использованием программы «Программа пользователя»;

- **не рекомендуется открытие хранимых на изделии документов непосредственно на самом USB-носителе.** Для дальнейшей работы с документами необходимо копирование их на средство вычислительной техники. Это связано с тем, что при открытии документов на USB-носителе происходит преждевременное исчерпание ресурсов памяти изделия за счет работы автоматического сохранения;

- **запрещается использование изделия в случае повреждения USB-разъема или повреждения его контактной группы, наличия в разъеме следов влаги, грибков, солей, мусора или других загрязнений.** При попадании/образовании влаги внутри USB-разъема необходимо удалить ее продуванием;

- **запрещается использовать изделие с признаками нарушения целостности корпуса.** Нарушение целостности корпуса USB-носителя – это не только снятие гарантийных обязательств со стороны производителя, но и потенциальный риск утечки конфиденциальных данных, записываемых на USB-накопитель;

- **не рекомендуется подключать USB-накопители к средствам вычислительной техники целостность которых была нарушена;**

- **не рекомендуется подключать USB-накопители к средствам вычислительной техники через вкладки, USB-удлинители, USB-хабы и другие промежуточные устройства.** При подключении USB-накопителя внимательно осматривайте разъём на наличие дополнительных устройств, которые может разместить злоумышленник;

- **запрещается извлекать USB-носитель «JaCarta SF/ГОСТ» при проведении обновления встроенного программного средства на него до завершения обновления (и/или прерывать подачу питания на него).** Подобные действия могут привести к выходу изделия из эксплуатации;

- **хранение и транспортировка изделия должны осуществляться в соответствии с разделом 5 (с. 31).**

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					Лист
										26

### 2.3.2 Режимы работы изделия в качестве ЭН и необходимые средства для управления им

Режимы работы изделия, введенного в эксплуатацию как ЭН, а также необходимые средства по управлению им, указаны ниже в таблице 5.

Таблица 5 – Режимы работы изделия в качестве ЭН и необходимые средства для управления им

	Гость	Пользователь	Администратор
ЭН пользователя	-	ПИН-код Пользователя и программное средство «Программа пользователя»	ЭН администратора доступа, программное средство «Программа администратора», Ключевой контейнер пользователя
ЭН администратора доступа	-	Ключевой контейнер администратора доступа и пароль к данному ключевому контейнеру, программное средство «Программа администратора»	Ключевой контейнер администратора доступа, пароль к данному ключевому контейнеру, программное средство «Программа главного администратора»

### 2.3.3 Подготовка изделия к утилизации

**ВНИМАНИЕ!** Обезличивание осуществляется в следующем порядке: сначала обезличиваются все ЭН пользователей, затем – ЭН администраторов.

Подготовка изделия USB-носитель «JaCarta SF/ГОСТ» к утилизации выполняется в следующем порядке:

а) вывод из эксплуатации СКЗИ (в том числе удаление ключевых контейнеров СКЗИ записанных в энергонезависимую память накопителя);

б) вывод из эксплуатации USB-накопителя JaCarta SF/ГОСТ.

При подготовке изделия к утилизации необходимо выполнить следующие операции, используя программу администратора:

а) запустите на АРМ Администратора программу администратора;

б) укажите ключевой контейнер, с помощью которого был инициализирован конкретный носитель;

в) выберите конкретный носитель и нажмите кнопку активировать;

г) обезличьте электронный носитель пользователя или электронный носитель администратора доступа.

**ВНИМАНИЕ!** Не удаляйте ключевые контейнеры до полного вывода изделия из эксплуатации.

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

										Лист
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					27

Примечание — Действия, необходимые для обезличивания электронного носителя, описаны в документе RU.АЛДЕ.03.01.006-01 34 01 «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора».

После выполнения всех указанных выше операций у изделия будет сброшен ПИН-код Пользователя/Администратора доступа, а также будет очищена флеш-память.

В случае, если изделие использовалось как СКЗИ, процедура утилизации определяется действующими нормативными документами в области информационной безопасности, а также внутренними нормативными актами организации-эксплуатанта. Производителем рекомендуется произвести дробление электронных компонентов изделия (микроконтроллер общего назначения, микроконтроллер смарт-карты, карта флеш-памяти) с использованием механических средств с достижением максимального размера остаточного зерна не более 2х2 мм.

При утилизации изделия следует выполнять следующие рекомендации:

- не рекомендуется утилизировать изделие вместе с бытовыми отходами.

Подробнее рекомендации по утилизации изделия описаны в документе АЛДЕ.467669.004ПС «USB-носитель “JaCarta SF/ГОСТ”. Паспорт».

Инв. № подл.	Подпись и дата					
	Инв. № дубл.					
	Взам. инв. №					
Инв. № подл.	Подпись и дата					
	Инв. № дубл.					
	Взам. инв. №					
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						28

### 3 Техническое обслуживание

Особых указаний по техническому обслуживанию изделия не прилагается.

Перед началом работы необходимо проводить внешний осмотр состояния изделия.

В ходе эксплуатации изделия периодически должна удаляться пыль с корпуса мягкой обтирочной ветошью. Изделие при этом должно быть отключено от АРМ.

При необходимости организовывается периодическая (плановая) проверка работоспособности изделия. Порядок проведения периодической (плановой) проверки работоспособности приведён в приложении Б.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата					Лист
									29
					Изм.	Лист	№ документа	Подпись	Дата

#### 4 Текущий ремонт

Ремонт изделия производится предприятием-изготовителем.

Инв. № подл.	Подпись и дата					
	Изм. № дубл.					
	Взам. инв. №					
Подпись и дата				Лист		
Инв. № дубл.						
Взам. инв. №						
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	30

## 5 Хранение и транспортирование

Изделие USB-носитель «JaCarta SF/ГОСТ» должно храниться в упаковке предприятия-изготовителя с соблюдением следующих климатических условий:

- температура окружающего воздуха: от минус 40 до плюс 85°С;
- относительная влажность воздуха: не более 100%, без конденсата.

Изделие должно храниться в отапливаемых складских помещениях, на стеллажах или в упаковке, при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей.

Не допускается изменение температуры окружающего воздуха более чем на 20°С в час.

После хранения изделия при температуре ниже 0°С при последующем повышении температуры внутри изделия и на контактной группе его USB-разъема возможно образование влаги, которая может вызвать его неисправность или повреждение. В данном случае, до начала использования изделие необходимо полностью высушить (удалить конденсат), соблюдая следующий температурный режим:

- нагревание изделия не более 20°С в час;
- максимальная температура нагревания изделия: плюс 40°С;
- срок хранения изделия составляет не более 3-х (трех) лет.

Инд. № подл.	Подпись и дата	Взам. инв. №	Инд. № дубл.	Подпись и дата	АЛДЕ.467669.004РЭ2					Лист				
														31
Изм.	Лист	№ документа	Подпись	Дата										

## 6 Установка и настройка

В настоящем разделе указаны сведения, относящиеся к установке программ на АРМ. По окончании установки, для использования функциональных возможностей продукта, пожалуйста, воспользуйтесь документами вида «Руководство оператора» на конкретное программное средство.

Обратите внимание, в разделе 2.1 на с. 17, приведена общая последовательность работы с изделием.

### 6.1 Общие сведения о программах из комплекта программных средств изделия USB-носитель «JaCarta SF/ГОСТ»

#### 6.1.1 Общие сведения о программах

Комплект программных средств предназначен для реализации функций безопасности изделия на стороне средств вычислительной техники и обеспечивает:

- инициализацию специализированных съемных машинных носителей информации;
- локальное управление и настройку возможности использования изделия на конкретных средствах вычислительной техники;
- локальное управление и настройку прав доступа пользователей к информации в разделах флеш-памяти специализированных съемных машинных носителей информации;
- проверку прав доступа пользователей к разделам флеш-памяти специализированного съемного машинного носителя информации. Управление доступом осуществляется совместно со встроенным программным средством;
- взаимодействие с подключаемыми специализированными съемными машинными носителями информации;
- работоспособность изделия в среде функционирования (работу изделия в среде операционных систем семейства Linux).

Комплект программных средств включает в свой состав:

- Программное средство RU.АЛДЕ.03.01.004-01 «Программный комплекс интеграции и администрирования» (далее – ПКИА). Программный комплекс обеспечивает применение специализированного съемного машинного носителя информации по назначению и предназначен для организации взаимодействия пользователей и средств вычислительной техники с подключаемыми специализированными съемными машинными носителями информации, а также локальное управление машинными носителями. ПКИА включает в себя программные компоненты, каждый из которых является самостоятельным программным средством. Состав ПКИА описан в таблице 6.

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата					Лист
									32
					Изм.	Лист	№ документа	Подпись	Дата



- RU.АЛДЕ.01.01.001-04 Встроенное программное средство JaCarta OS (только в исполнении 5. В остальных случаях входит в состав ССМНИ).
- Программное средство «Программный комплекс обеспечения совместимости» (RU.АЛДЕ.02.01.004-01). Программный комплекс обеспечивает работоспособность специализированного USB-носителя в среде операционных систем Astra Linux SE 1.2 «Смоленск», Astra Linux 1.3 «Смоленск», MCBC 3.0. Программный комплекс обеспечения совместимости включает в себя программные компоненты, описанные в таблице 7.

Таблица 6 – Назначение и функции программ из состава изделия (ПКИА)

Обозначение и название программы	Описание и назначение (функции) программы
Программа главного администратора RU.АЛДЕ.03.01.005-01	Программа обеспечивает выбор и установку правил эксплуатации изделия USB-носитель «JaCarta SF/ГОСТ» пользователем с ролью «главный администратор». Программа предназначена для создания ключевых контейнеров, необходимых для инициализации специализированных съёмных носителей информации из состава изделия USB-носитель «JaCarta SF/ГОСТ», в том числе: <ul style="list-style-type: none"> <li>– создание ключевого контейнера администратора доступа;</li> <li>– создание ключевого контейнера пользователя;</li> <li>– создание ключевого контейнера для обновления разделов CD-ROM электронных носителей пользователя.</li> </ul>
Программа администратора RU.АЛДЕ.03.01.006-01	Программа обеспечивает взаимодействие администратора с USB-носителями «JaCarta SF/ГОСТ». Программа предназначена для отправки запросов встроенному программному средству носителя информации и обеспечивает: <ul style="list-style-type: none"> <li>– аутентификацию администратора в программе на основе ключевого контейнера, созданного главным администратором;</li> <li>– инициализацию и присвоение идентификатора пользователя конкретному специализированному машинному носителю информации;</li> <li>– установку и обновление информации в доступных только для чтения разделах флеш-памяти изделия;</li> <li>– разблокирование изделия в случае его блокировки;</li> <li>– сброс ПИН-кода пользователя;</li> <li>– обновление закрытых ключей изделия;</li> <li>– создание ключевых контейнеров для локального сервера авторизации и контейнеров автономного доступа;</li> <li>– подготовка изделия USB-носитель «JaCarta SF/ГОСТ» к работе с СЗИ семейства «Secret Net» и СКЗИ «КриптоПРО CSP» (при установленных библиотеках поддержки);</li> <li>– аудит изделия;</li> <li>– обновление изделия.</li> </ul>
Программа пользователя RU.АЛДЕ.03.01.007-01	Программа обеспечивает взаимодействие пользователя с USB-носителями «JaCarta SF/ГОСТ». Программа предназначена для отправки запросов встроенному программному средству носителя информации и обеспечивает: <ul style="list-style-type: none"> <li>– идентификацию и аутентификацию пользователей;</li> <li>– проверку прав доступа пользователей к разделам флеш-памяти машинного носителя информации;</li> <li>– отображение информации о USB-носителе «JaCarta SF/ГОСТ».</li> </ul>
Локальный сервер авторизации	Программа обеспечивает взаимодействие программы пользователя

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						33

Обозначение и название программы	Описание и назначение (функции) программы
RU.АЛДЕ.03.12.001-01	с ключевым контейнером, расположенным на локальном сервере авторизации. Основное назначение программы: – загрузка ключевых контейнеров для локального сервера авторизации; – проверка идентификационных данных пользователя; – авторизация подключения скрытых разделов флеш-памяти на рабочем месте пользователя.
Программа диагностики RU.АЛДЕ.02.02.001-01	Программа обеспечивает проверку работоспособности специализированных съемных машинных носителей информации.  Основное назначение: контроль и выявление неисправностей, сбор информации о техническом состоянии машинных носителей.
Программа подготовки обновлений RU.АЛДЕ.02.02.005-01	Программа обеспечивает взаимодействие администратора с USB-носителями «JaCarta SF/ГОСТ».  Основное назначение: модернизация изделий АЛДЕ.26.20.21.120.001 в исполнениях 1, 2, 3, 4 и АЛДЕ.467669.004 в исполнениях 6, 7 Входит в изделие только в исполнении 5.
Интерфейсная библиотека jсPKCS11-2 RU.АЛДЕ.02.02.002-01	Библиотека предназначена для организации взаимодействия программного комплекса интеграции и администрирования со специализированными съемными машинными носителями информации путем преобразования функций программного комплекса в APDU-команды специализированного съемного машинного носителя информации.  Для ОС Linux библиотека обязательно устанавливается на APM.
Библиотека поддержки СКЗИ «КриптоПро CSP» RU.АЛДЕ.02.02.003-01	Библиотека предназначена для организации взаимодействия специализированных съемных машинных носителями информации и СКЗИ «КриптоПро CSP»;  Основное назначение: обеспечение хранения контейнера СКЗИ.
Библиотека поддержки СЗИ семейства «Secret Net» RU.АЛДЕ.02.02.004-01	Библиотека поддержки СЗИ семейства «Secret Net».

Таблица 7 – Назначение и функции программ из состава изделия (ПКОС)

Обозначение и название программы	Описание и назначение (функции) программы
Программа установки программного комплекса обеспечения совместимости RU.АЛДЕ.02.01.003-01	Инсталляционный пакет для установки программ из состава комплекса  Программа обеспечивает автоматизированную установку компонентов программного комплекса обеспечения совместимости на средства вычислительной техники.
Программа управления смарт-картами Драйвер интерфейса USB	Программа предназначена для отправки запросов встроенному программному средству носителя информации. Драйвер интерфейса USB для взаимодействия со специализированным съемным машинным носителем информации. Программное средство предназначено для организации взаимодействия программ, установленных на СВТ со специализированными съемными машинными носителями информации

Изм. № подл. Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						34

## 6.1.2 Названия дистрибутивных файлов

Дистрибутивы программного обеспечения изделия USB-носитель «JaCarta SF/ГОСТ» для ОС семейств Linux – это инсталляционные пакеты в формате \*.deb или \*.rpm (зависит от ядра ОС).

Для установки программ подходят только пакеты из соответствующей директории поставочного диска.

## 6.1.3 Установка программ и порядок работы с изделием

В соответствии с подразделом 2.1 Порядок работы с изделием (с.17) в рамках подготовки к вводу в эксплуатацию изделия USB-носитель «JaCarta SF/ГОСТ» осуществляется (в указанном непосредственно в разделе документа порядке):

- а) настройка параметров безопасности среды функционирования;
- б) обеспечение совместимости программ из состава изделия и среды функционирования (системных программных средств (операционных систем), установленных на СВТ);
- в) установка необходимых компонентов операционных систем (пакетов);
- г) установка программ из состава изделия на АРМ, определённых для работы с изделием в соответствии с пунктом а). Подробная информация об установке программ приведена в разделах 2.2.4.2 (с. 22) и 6 (с. 32).

**ВНИМАНИЕ!** В настоящем руководстве по эксплуатации рассматриваются только основные сценарии, связанные с настройкой безопасности ОС. При необходимости, процесс установки программ может быть дополнительно настроен администратором безопасности Вашей организации в соответствии с руководством администратора на соответствующую операционную систему.

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

										Лист
										35
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

## 6.1.4 Требования к среде функционирования программ

### 6.1.4.1 Операционные системы

Программы из состава ПКИА могут использоваться на СВТ под управлением операционных систем, указанных в таблице 1 [с. 7].

**Примечание:** 1. Не поддерживаются редакции Windows, предназначенные для использования на компьютерах с архитектурой IA-64 (с процессорами Itanium).

2. «Программа главного администратора», «Программа администратора» ограниченно функционируют на СВТ под управлением MSVC 3.0.

### 6.1.4.2 Аппаратные требования

Минимальные требования к выполнению программ удовлетворяют минимальным требованиям ОС, в которых выполняются программы.

В состав АРМ Главного администратора, АРМ Администратора и АРМ пользователя должны входить мониторы. Разрешение экрана монитора АРМ должно быть не менее 800x600 точек.

Связь между программами, описанными в таблице 6 и изделием USB-носитель «JaCarta SF/ГОСТ» осуществляется через USB-порты 2.0 типа А, в которые включается изделие.

АРМ Главного администратора и АРМ Администратора должны быть оснащены не менее чем двумя USB-портами.

Не рекомендуется использовать порты USB-концентраторов или USB-порты, расположенные на передней панели стационарного АРМ для подключения более одного изделия. Такие порты не всегда обеспечивают требуемое для работы изделий USB-носитель «JaCarta SF/ГОСТ» питание, что может привести к сбоям в работе и потере данных.

**Примечание** — Пожалуйста, ознакомьтесь с правилами эксплуатации изделия, описанными в разделе 2.3.1 на с. 25

Для работы, программе главного администратора необходимо постоянно подключённое изделие USB-носитель «JaCarta SF/ГОСТ».

Подготовка контейнеров управления изделиями USB-носитель «JaCarta SF/ГОСТ» пользователя, осуществляется с помощью подключенного инициализированного ЭН администратора доступа. ЭН администратора доступа, используемый для создания ключевых контейнеров пользователя, в дальнейшем будет использоваться для управления инициализируемыми изделиями USB-носитель «JaCarta SF/ГОСТ» пользователя.

АРМ главного администратора должно быть оснащено следующими устройствами ввода: клавиатура и мышь компьютерная.

Подпись и дата
Име. № дубл.
Взам. име. №
Подпись и дата
Име. № подл.

					<b>АЛДЕ.467669.004РЭ2</b>	<i>Лист</i>
						36
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>		

### 6.1.4.3 Требования к пользователю

Пользователи программных средств «Программа администратора» и «Программа главного администратора» должны ознакомиться с эксплуатационной документацией на изделие, указанной в документе RU.АЛДЕ.467669.004ВЭ «Ведомость эксплуатационных документов», и обладать навыками работы в среде функционирования средства.

Для установки программ рекомендуется ознакомиться с настоящим руководством.

### 6.1.4.4 Прочие требования

Администратор доступа должен при необходимости:

а) проверить контрольные суммы дистрибутивов и файлов исполняемых программ. Проверка осуществляется в порядке, установленном в документе АЛДЕ.467669.004ПС «USB-носитель «JaCarta SF/ГОСТ». Паспорт»;

б) установить расположенные на дополнительном машинном носителе информации необходимые компоненты (для удобства «Пользователя»);

в) установить программу «Библиотека поддержки СКЗИ «КриптоПро CSP» (поддержка работы с СКЗИ «КриптоПро CSP»);

г) установить программу «библиотека поддержки СЗИ семейства «SecretNet» (для обеспечения совместимости с продуктами семейства «Secret Net Studio»);

д) установить на АРМ Пользователей программу «Программа пользователя».

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						37

## 6.2 Установка программ в ОС МСВС 3.0 и настройка изделия

**ВНИМАНИЕ!** Не допускается одновременное использование более двух изделий USB-носитель «JaCarta SF/ГОСТ» с ОС МСВС 3.0.

### 6.2.1 Дистрибутивные файлы для МСВС 3.0

Названия файлов из состава дистрибутива и пути к распакованным файлам.

Таблица 8 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА и ПКOC для ОС МСВС 3.0

Имя пакета	Путь распаковки и имя файла
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_x32.rpm, где «xxx» - версия программы	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_x32.rpm, где «xxx» - версия программы	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jPKCS11-2</b>	
libjckt2_3.5.3.xxx_x32.rpm, где «xxx» - версия программы	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_x32.rpm, где «xxx» - версия программы	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>pcsc-ccid (ПКOC)</b>	
libusb9-1.0.9.55-1.МСВС3.0.12.i386.rpm	/usr/local/libusb-1.0.9/include/libusb-1.0/libusb.h /usr/local/libusb-1.0.9/lib/libusb-1.0.a /usr/local/libusb-1.0.9/lib/libusb-1.0.so.0.1.0 /usr/local/libusb-1.0.9/lib/libusb-1.0.la /usr/local/libusb-1.0.9/lib/pkgconfig/libusb-1.0.pc
ccid-1.4.24.55-1.МСВС3.0.12.i386.rpm	/etc/init.d/pcscd /usr/local/pcsc-lite/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist /usr/local/pcsc-lite/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Linux/libccid.so
pcsc-lite-1.8.17.55-1.МСВС3.0.12.i386.rpm	/usr/local/pcsc-lite/share/doc/pcsc-lite/README.polkit /usr/local/pcsc-lite/share/doc/pcsc-lite/README.DAEMON /usr/local/pcsc-lite/share/man/man5/reader.conf.5 /usr/local/pcsc-lite/share/man/man8/pcscd.8 /usr/local/pcsc-lite/bin/pcsc-spy.1 /usr/local/pcsc-lite/sbin/pcscd /usr/local/pcsc-lite/include/PCSC/winscard.h /usr/local/pcsc-lite/include/PCSC/wintypes.h /usr/local/pcsc-lite/include/PCSC/ifdhandler.h /usr/local/pcsc-lite/include/PCSC/reader.h /usr/local/pcsc-lite/include/PCSC/debuglog.h /usr/local/pcsc-lite/include/PCSC/pcsc-lite.h /usr/local/pcsc-lite/lib/libpcscspy.la /usr/local/pcsc-lite/lib/libpcsc-lite.la /usr/local/pcsc-lite/lib/libpcscspy.so.0.0.0 /usr/local/pcsc-lite/lib/libpcsc-lite.so.1.0.0 /usr/local/pcsc-lite/lib/pkgconfig/libpcsc-lite.pc /etc/profile.d/pcsc-lite.sh

### 6.2.2 Установка программ в МСВС 3.0

#### 6.2.2.1 Распаковка пакетов

Распаковка пакетов осуществляется в порядке, установленном пунктом 6.2.2.2.

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						38

Для распаковки rpm-пакетов выполните из ELK-терминала следующую команду:

```
sudo rpm -ivh <имя пакет>
```

где <пакет установки> – путь к rpm-пакету установки с указанием имени файла.

Например:

```
sudo rpm -ivh /home/jcsfuser_XXXXXX_32.rpm
```

В результате в каталог `/opt/jacartasfutils/bin/` будет распакована «Программа пользователя» версии XXXXXX.

### 6.2.2.2 Порядок распаковки (установки)

а) Ознакомьтесь с текстовыми файлами из директории дистрибутива ПО/Linux/МСВС3.

б) Распакуйте пакеты программного комплекса обеспечения совместимости из состава дистрибутива:

- 1) `libusb9-1.0.9.50-1.MCBC3.0.12.i386.rpm`
- 2) `pcsc-lite-1.8.17.50-1.MCBC3.0.12.i386.rpm`
- 3) `ccid-1.4.24.50-1.MCBC3.0.12.i386.rpm`

в) Распакуйте пакет `libjck2_3.5.3.xxx_x32.rpm`

г) Распакуйте пакеты для МСВС 3.0 из состава дистрибутива, устанавливая необходимые для конкретного АРМ программы.

**ВНИМАНИЕ!** Установка пакета «Библиотеки поддержки СКЗИ «КриптоПро CSP» осуществляется после установки пакетов КриптоПро в порядке, установленном производителем СКЗИ<sup>1</sup>.

### 6.2.3 Предварительная установка параметров для возможности использования скрытых разделов Флеш-памяти изделия для ОС МСВС3.0

Для того, чтобы Пользователю ЭН, использующему ОС МСВС 3.0, была доступна возможность работы с более чем одним разделом флеш-памяти изделия, необходимо установить возможность использования нескольких LUN для одного физического устройства.

Для увеличения числа LUN-ов (Logical Unit Number) для одного устройства выполните действия а) – д).

а) в файл конфигурации модулей системы `/etc/modules.conf` добавьте строку:  
`options scsi_mod max_scsi_luns=8`

б) Выполните резервное копирование образа загрузочного RAM-диска (`initrd`):

<sup>1</sup> <https://www.cryptopro.ru/support/docs>. Библиотека поддержки обеспечивает, в том числе, работу с контейнерами КриптоПро устаревших версий 3.6, 3.9, 4.0.

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

1) Запустите командную оболочку Linux.

2) Выполните команду:

```
cp /boot/initrd-$(uname -r).img /boot/initrd-$(uname -r).img.bak
```

в) Выполните создание нового образа загрузочного RAM-диска, используя команду:

```
mkinitrd -f -v /boot/initrd-2.4.32-$(uname -r).img $(uname -r)
```

г) Выполните перезагрузку конфигурации загрузчика Linux Loader, используя команду:

```
lilo
```

д) Выполните перезагрузку системы, используя команду:

```
reboot
```

После выполнения указанных выше действий пользователя для ОС МСВС 3.0 будет доступна возможность работать с несколькими разделами флеш-памяти изделия.

## 6.2.4 Установка автоматического монтирования скрытых разделов флеш-памяти изделия для ОС МСВС 3.0

**ВНИМАНИЕ!** Не допускается одновременное использование более двух изделий USB-носитель «JaCarta SF/ГОСТ» с операционной системой МСВС 3.0.

Для установки автоматического монтирования подключенных скрытых разделов флеш-памяти изделия в ОС МСВС 3.0, пользователю, обладающему правами администрированиями операционной системы (root), необходимо выполнить следующие действия:

- откройте файл `/etc/updfstab.conf.default` для редактирования;
- добавьте в него два правила для подключения изделий АО "Аладдин Р.Д":

```
device aladdin {
    partition 1
    ignoremulti true
    match    hd Aladdin
}
```

```
device aladdinA {
    partition 1
    ignoremulti true
    match    hd Aladdin
}
```

- откройте файл `/etc/security/console.perms` для редактирования;
- добавьте в файл разрешения для пользователя, обладающего правами «owner»,

на точки монтирования:

```
<aladdin>=/mnt/aladdin*
```

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

										Лист
										40
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					



```
<console> 0660 <aladdin> 0660 root.disk
```

д) добавьте права запуска `/bin/mount` и `/bin/umount` пользователя, обладающего правами «owner».

Данную операцию можно выполнить, с помощью команд:

```
chmod +S /bin/mount
```

```
chmod +S /bin/umount
```

е) Перезагрузите ОС. После перезагрузки ОС данные изменения будут сохранены.

## 6.2.5 Начало работы и основной сценарий работы пользователя

До начала работы пользователя с изделием, RW-разделы должны быть отформатированы в соответствии с подразделом 6.7 «Форматирование в ОС семейства Linux».

**ВНИМАНИЕ!** Форматирование разделов в защищённых ОС требует определённого набора привилегий, которым по умолчанию обладает только суперпользователь.

Процесс монтирования открытых разделов флеш-памяти изделия под учётной записью пользователя происходит следующим образом:

а) Пользователь подключает к АРМ инициализированный ЭН. На рабочем столе отобразятся ярлыки «CD-ROM», «CD-ROM1», «Накопитель /dev/sdb1» и «Накопитель /dev/sdc1».

б) В случае, если на ЭН есть открытые разделы флеш-памяти, пользователь может сразу выполнить их монтирование. Для этого необходимо дважды кликнуть мышью на CD-ROM и /dev/sdb1 или кликнуть правой кнопкой мышки на соответствующие ярлыки, вызывать меню и выбрать пункт «Монтировать».

в) В результате действий, описанных в пункте б) открытый CD-ROM раздел будет примонтирован в каталог `/mnt/cdrom`, а открытый RW-раздел – в каталог `/mnt/aladdin`. Разделы будут примонтированы в соответствии с правами текущего пользователя.

Процесс монтирования скрытых разделов флеш-памяти изделия под учётной записью пользователя происходит следующим образом:

а) После выполнения действий с открытыми разделами, пользователь может подключить скрытые разделы флеш-памяти с помощью приложения «Программа пользователя» (см. документ RU.АЛДЕ.03.01.007-01 34 01. «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа пользователя. Руководство оператора»).

б) В случае если на ЭН есть скрытые разделы Флеш-памяти, то после выполнения действий, описанных в пункте а) их можно примонтировать. Для этого необходимо дважды

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата						Лист
										41
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

кликнуть мышью на CD-ROM1 и /dev/sdc1 или кликнуть правой кнопкой мышки на соответствующие ярлыки, вызывать меню и выбрать пункт «Монтировать».

в) В результате скрытый CD-ROM1 раздел будет примонтирован в каталог /mnt/cdrom1, а скрытый RW-раздел в каталог /mnt/aladdin1 с правами для текущего пользователя на чтение и запись.

г) При подключении другого ЭН к АРМ необходимо повторить пункты а) – г).

Инв. № подл.	Подпись и дата				Лист	
	Инв. № дубл.					42
	Взам. инв. №					
Подпись и дата						
Инв. № подл.						
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	

## 6.3 Установка программ в МСВС 5.0, АЛТ 8 СП, ОС РОСА и настройка изделия

Установка программ в МСВС 5.0, АЛТ 8 СП и ОС РОСА различается только в части настроек безопасности операционных систем и наборе пакетов установки. В ОС Альт 8 СП и ОС РОСА используется механизм безопасности SELinux.

### 6.3.1 Дистрибутивные файлы для МСВС 5.0, Альт 8 СП и ОС РОСА

Названия файлов из состава дистрибутива и пути к распакованным файлам представлены в таблицах 9 и 10.

Таблица 9 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА и ПКОС для ОС МСВС 5.0, Альт 8 СП Рабочая станция, Альт 8 СП Сервер и ОС РОСА.

Имя пакета	Путь распаковки и имя файла
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jcPKCS11-2</b>	
libjckt2_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcsfmkt-3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/usr/lib64/libjcsfmkt.so.3.5.3 /usr/lib64/libjcsfmkt.so.1 (symlink на libjcsfmkt.so.3.5.3) /usr/lib64/libjcsfmkt.so (symlink на libjcsfmkt.so.3.5.3)
jcPKCS11-2_2.7.2.499_x64.rpm	/usr/lib64/jcverify /usr/lib64/libASEP11.so /usr/lib64/libjckt2.so /usr/lib64/libjcPKCS11-2.so.2.7.2 /usr/lib64/libjcPKCS11ds.so
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cprocsp-rdr-jakarta-msvs-64-3.6.408.741-4.x86_64.rpm	/opt/cprocsp/lib/amd64/librdrjakarta.so.[version] /opt/cprocsp/share (файлы поддержки кодировок)
cprocsp-rdr-jakarta-64-5.0.0.1238-4.x86_64.rpm	/opt/cprocsp/lib/amd64/librdrjakarta.so.[version] /opt/cprocsp/share (файлы поддержки кодировок)

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

						Лист
						43
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	

Таблица 10 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА Альт 8 СП «Рабочая станция под Эльбрус»

Имя пакета	Путь распаковки и имя файла
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_e2k-8c_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_e2k-8c_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_e2k-8c_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jPKCS11-2</b>	
libjckt2_3.5.3.xxx_e2k-8c_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_e2k-8c_x64.rpm, где «xxx» - версия сборки программы	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcpkcs11-2_2.7.2.499_e2k-8c_x64.rpm	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
jcsfmkt_3.5.3.624_e2k-8c_x64.rpm	/usr/lib64/libjcsfmkt.so.3.5.3 /usr/lib64/libjcsfmkt.so.1 (symlink на libjcsfmkt.so.3.5.3) /usr/lib64/libjcsfmkt.so (symlink на libjcsfmkt.so.3.5.3)
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cprocsp-rdr-jacarta-64-5.0.0.1238-4.e2k.rpm	/opt/cprocsp/lib/e2k64/librdrjacarta.so.[version] /opt/cprocsp/share (файлы поддержки кодеровок)

### 6.3.2 Установка программ в МСВС 5.0, Альт 8 СП и ОС РОСА

#### 6.3.2.1 Отключение SELinux (только для ОС Альт 8 СП и ОС РОСА)

До начала установки программ на ОС Альт 8 СП Рабочая станция (64 бит), ОС Альт 8 СП Сервер (64 бит) и ОС Альт 8 СП «Рабочая станция для Эльбрус» необходимо выполнить следующие действия:

а) Войдите в учетную запись суперпользователя в соответствии с разделом 6.3 документа «Руководство администратора» на операционную систему Альт 8 (Сервер или рабочая станция), представленного на официальном сайте компании «Базальт СПО».

б) В командной оболочке (консоли) временно (до перезагрузки СВТ) отключена систему принудительного контроля ядра SELinux (механизм мандатного контроля доступа):

```
setenforce 0
```

в) Перейдите к инструкциям в подпунктах 6.3.2.2–6.3.2.3.

Подпись и дата
Име. № дубл.
Взам. инв. №
Подпись и дата
Име. № подл.

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист 44
------	------	-------------	---------	------	--------------------	------------

Перед установкой программ на ОС РОСА необходимо выполнить следующие действия:

а) добавить параметр загрузки ядра `selinux=0` в файле `/boot/grub2/grub.cfg`;

**ВНИМАНИЕ!** После включения этой настройки система не пройдет верификацию, графическое окружение станет недоступным, но терминальный режим останется полностью работоспособным.

б) для загрузки ОС РОСА с графическим окружением после отключения SELinux необходимо удалить виджет «Контекст Безопасности»;

в) после установки программ для SF/ГОСТ необходимо удалить параметр `selinux=0` в файле `/boot/grub2/grub.cfg`.

### 6.3.2.2 Распаковка пакетов

Распаковка пакетов осуществляется в порядке, установленном пунктом 6.3.2.3.

Для распаковки rpm-пакетов выполните из командной оболочки (командной строки/терминала) следующую команду:

```
sudo rpm -ivh <имя пакет>
```

где <пакет установки> – путь к rpm-пакету установки с указанием имени файла.

Например:

```
sudo rpm -ivh /home/jcsfadmin_3.5.3.xxx_x64.rpm
```

В результате в каталог `/opt/JaCartaSFGOSTSuite/` будет распакована «Программа администратора» версии `xxxxxxx`.

### 6.3.2.3 Порядок распаковки (установки)

а) Установите пакеты `pcsc-lite`, `libpcsclite`, `pcsc-lite-ccid` с загрузочного диска ОС Альт 8 СП или MCBC 5.0.

б) Установите (распакуйте) пакет `libjckt2_x86_64.rpm` из дистрибутива USB-носитель «JaCarta SF/ГОСТ».

в) Установите (распакуйте) пакеты из дистрибутива USB-носитель «JaCarta SF/ГОСТ» соответствующие APM.

г) Перезагрузите СВТ для включения SELinux.

**ВНИМАНИЕ!** Установка пакета «Библиотеки поддержки СКЗИ «КриптоПро CSP» осуществляется после установки пакетов КриптоПро в порядке, установленном производителем СКЗИ<sup>1</sup>.

<sup>1</sup> <https://www.cryptopro.ru/support/docs>. Библиотека поддержки обеспечивает, в том числе, работу с контейнерами КриптоПро устаревших версий 3.6, 3.9, 4.0.

Подпись и дата
Име. № дубл.
Взам. инв. №
Подпись и дата
Име. № подл.

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						45

### 6.3.3 Начало работы с изделием

Ввод носителей в эксплуатацию осуществляется в соответствии с эксплуатационными документами б) – е), указанными на с. 4.

**ВНИМАНИЕ!** В случае размещения АРМ главного администратора и АРМ администратора на СВТ под управлением МСВС 5.0, АЛЪТ 8 СП и ОС РОСА, необходимо учитывать следующее:

При выполнении инициализации ЭН Администратора доступа/Пользователя с CD-ROM разделами, имеющими ненулевой размер (Открытый CD-ROM, Скрытый CD-ROM), вспомогательные временные разделы флеш-памяти с файлами OPEN.ISO и HIDDEN.ISO должны монтироваться в каталог с указанным путем и именем. Если путь к каталогу и его имя не будут заданы, то в Программе администратора отобразится ошибка записи CD-ROM раздела.

Выполнять монтирование временных разделов можно либо вручную, используя команду `mount` при каждой инициализации изделий, либо настроив автоматическое монтирование.

Для установки автоматического монтирования вспомогательных разделов флеш-памяти, выполните следующее<sup>1</sup>:

а) Создайте файл `/etc/udev/rules.d/automount.rules`;

б) Внесите в файл, созданный в пункте а) правила для обработки подключения и отключения съемных носителей (пример для пользователя с `uid=1000`, если необходимо задать правила для другого пользователя, необходимо указать верный `uid`):

```
ACTION=="add" KERNEL=="sd[c-z][0-9]" RUN+="/bin/mkdir -p /mnt/%k"
RUN+="/bin/mount -o uid=1000 /dev/%k /mnt/%k"
ACTION=="remove" KERNEL=="s*" RUN+="/bin/umount /mnt/%k"
RUN+="/bin/rmdir /mnt/%k"
```

в) Выполните перезагрузку ОС, чтобы новые правила вступили в силу или выполните команду:

```
sudo udevadm control --reload-rules
```

По правилам, описанным выше, любое обнаруженное устройство, подходящее по маске `sd[c-z][0-9]` (например, `sde1`) будет монтировано в каталог `/mnt/<имя устройства>` (например, `/mnt/sde1`). Образ Открытого CD-ROM раздела OPEN.ISO будет доступен по пути `/mnt/sde1/OPEN.ISO`

Маску для правил автоматического монтирования Администратор должен указать в соответствии с используемой конфигурацией ОС. Например, если подключаемые в ОС отобра-

<sup>1</sup> Подробную информацию о правилах монтирования можно получить, выполнив команду `man udev`

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						46

жаются, начиная с буквы b (/dev/sdb1), то и маска в правилах автоматического монтирования должна быть указана sd[b-z][0-9].

До начала работы пользователя с изделием, RW-разделы должны быть отформатированы в соответствии с подразделом 6.7 «Форматирование в ОС семейства Linux».

**ВНИМАНИЕ!** Форматирование разделов в защищённых ОС требует определённого набора привилегий, которым по умолчанию обладает только суперпользователь.

## 6.4 Установка программ в Astra Linux Special Edition 1.2 и 1.3 «Смоленск»

### 6.4.1 Дистрибутивные файлы для Astra Linux 1.2 SE и Astra Linux 1.3 SE

Названия файлов из состава дистрибутива и пути к распакованным файлам.

Таблица 11 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА и ПКОС для Astra Linux SE 1.2 и Astra Linux SE 1.3

Имя пакета	Путь распаковки и имя файла
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jсPKCS11-2</b>	
libjckt2_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcsfmkt_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/usr/lib/libjcsfmkt.so.3.5.3 /usr/lib/libjcsfmkt.so.1 (symlink) /usr/lib/libjcsfmkt.so (symlink)
jcpkcs11-2_2.7.2.499_x64.deb	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
<b>pcsc-ccid (ПКОС)</b>	
libusb9_1.0.9.55_smolensk1.2_amd64.deb libusb9_1.0.9.55_smolensk1.3_amd64.deb	/usr/local/libusb-1.0.9/include/libusb-1.0/config.h /usr/local/libusb-1.0.9/lib/libusb-1.0.a /usr/local/libusb-1.0.9/lib/libusb-1.0.so.0.1.0 /usr/local/libusb-1.0.9/lib/libusb-1.0.la /usr/local/libusb-1.0.9/lib/pkgconfig/libusb-1.0.pc
pcscd_1.8.17.55_smolensk1.2_amd64.deb pcscd_1.8.17.55_smolensk1.3_amd64.deb	/usr/local/pcsc-lite/share/doc/pcsc-lite/README.polkit /usr/local/pcsc-lite/share/doc/pcsc-lite/README.DAEMON /usr/local/pcsc-lite/share/man/man5/reader.conf.5 /usr/local/pcsc-lite/share/man/man8/pcscd.8 /usr/local/pcsc-lite/share/man/man1/pcsc-spy.1 /usr/local/pcsc-lite/bin/pcsc-spy

Имя. № подл.    Подпись и дата    Взам. инв. №    Подпись и дата    Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист 47
------	------	-------------	---------	------	--------------------	------------

	/usr/local/pcslite/sbin/pcscd /usr/local/pcslite/include/PCSC/winscard.h /usr/local/pcslite/include/PCSC/wintypes.h /usr/local/pcslite/include/PCSC/ifdhandler.h /usr/local/pcslite/include/PCSC/reader.h /usr/local/pcslite/include/PCSC/debuglog.h /usr/local/pcslite/include/PCSC/pcslite.h /usr/local/pcslite/lib/libpcscspy.la /usr/local/pcslite/lib/libpcslite.la /usr/local/pcslite/lib/libpcscspy.so.0.0.0 /usr/local/pcslite/lib/libpcslite.so.1.0.0 /usr/local/pcslite/lib/pkgconfig/libpcslite.pc /etc/profile.d/pcslite.sh /etc/ld.so.conf.d/pcslite.conf
libccid_1.4.24.55_smolensk1.2_amd64.deb libccid_1.4.24.55_smolensk1.3_amd64.deb	/usr/local/pcslite/lib/pcsc/drivers/ifd-ccid.boundle/Contents/Linux/libccid.so /usr/local/pcslite/lib/pcsc/drivers/ifd-ccid.boundle/Contents/Info.plist /etc/init.d/pcscd
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cproesp-rdr-jakarta-64_3.6.408.741-4_amd64.deb	/opt/cproesp/lib/amd64/librdrijakarta.so.[version] /opt/cproesp/share (файлы поддержки кодировок)
cproesp-rdr-jakarta-64_5.0.0.1238-4_amd64.deb	/opt/cproesp/lib/amd64/librdrijakarta.so.[version] /opt/cproesp/share (файлы поддержки кодировок)

## 6.4.1 Установка программ в Astra Linux 1.2 SE и Astra Linux 1.3 SE

### 6.4.1.1 Распаковка пакетов

Распаковка пакетов осуществляется в порядке, установленном пунктом 6.4.1.2.

Для распаковки (установки) deb-пакетов выполните из терминала fly следующую команду:

```
sudo dpkg -i <пакет установки>
```

где <пакет установки> – путь к deb-пакету установки с указанием его имени.

Например:

```
sudo dpkg -i jcsfadmin_3.5.3.xxx_x64.deb
```

В результате в каталог /opt/JaCartaSFGOSTSuite/ будет распакована «Программа администратора» версии xxx.

### 6.4.1.2 Порядок распаковки (установки)

а) Ознакомьтесь с текстовыми файлами из директории дистрибутива ПО/Linux/Astra\_Linux\_SE\_1.2 и ПО/Linux/Astra\_Linux\_SE\_1.3

б) Распакуйте пакеты программного комплекса обеспечения совместимости из состава дистрибутива:

- 1) libusb9\_1.0.9.50\_smolensk1.2\_amd64.deb
- 2) pcscd\_1.8.17.50\_smolensk1.2\_amd64.deb
- 3) libccid\_1.4.24.50\_smolensk1.2\_amd64.deb

Подпись и дата
Име. № дубл.
Взам. инв. №
Подпись и дата
Име. № подл.

										Лист
										48
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					



или

- 1) libusb9\_1.0.9.50\_smolensk1.3\_amd64.deb
- 2) pcscd\_1.8.17.50\_smolensk1.3\_amd64.deb
- 3) libccid\_1.4.24.50\_smolensk1.3\_amd64.deb

в) Распакуйте пакет libjckt2\_3.5.3.xxx\_x64.deb  
г) Распакуйте пакеты из состава дистрибутива, устанавливая необходимые для конкретного АРМ программы.

**ВНИМАНИЕ!** Установка пакета «Библиотеки поддержки СКЗИ «КриптоПро CSP» осуществляется после установки пакетов КриптоПро в порядке, установленном производителем СКЗИ<sup>1</sup>.

#### 6.4.1.3 Настройка мандатного доступа

После установки программ из состава изделия выполните редактирование последней строки в файле /etc/init.d/pcscd, изменив строку «execaps -c 0x100 -- » на «execaps -c 0x100 -- nohup /usr/local/pcsclite/sbin/pcscd </dev/null >> /var/log/pcscd.log 2>&1 &»

#### 6.4.2 Начало работы с изделием

Ввод носителей в эксплуатацию осуществляется в соответствии с эксплуатационными документами б) – е), указанными на с. 4.

**ВНИМАНИЕ!** В случае размещения АРМ главного администратора и АРМ администратора на СВТ под управлением ОС Astra Linux 1.4 SE «Смоленск» или ОС «Astra Linux 1.5 SE «Смоленск», необходимо учитывать следующее:

При выполнении инициализации ЭН Администратора доступа/Пользователя с CD-ROM разделами, имеющими ненулевой размер (Открытый CD-ROM, Скрытый CD-ROM), вспомогательные временные разделы флеш-памяти с файлами OPEN.ISO и HIDDEN.ISO должны монтироваться в каталог с указанным путем и именем. Если путь к каталогу и его имя не будут заданы, то в программе администратора отобразится ошибка записи CD-ROM раздела.

Выполнять монтирование временных разделов можно либо вручную, используя команду mount при каждой инициализации изделий, либо настроить автоматическое монтирование.

Для установки автоматического монтирования вспомогательных разделов флеш-памяти, выполните следующее:

\_\_\_\_\_

<sup>1</sup> <https://www.cryptopro.ru/support/docs>. Библиотека поддержки обеспечивает, в том числе, работу с контейнерами КриптоПро устаревших версий 3.6, 3.9, 4.0.

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

					<b>АЛДЕ.467669.004РЭ2</b>	<i>Лист</i>
						49
Изм.	Лист	№ документа	Подпись	Дата		

д) Создайте файл /etc/udev/rules.d/automount.rules;

е) Внесите в файл, созданный в пункте а) правила для обработки подключения и отключения съемных носителей (пример для пользователя с uid=1000, если необходимо задать правила для другого пользователя, необходимо указать верный uid):

```
ACTION=="add" KERNEL=="sd[c-z][0-9]" RUN+="/bin/mkdir -p /mnt/%k"
RUN+="/bin/mount -o uid=1000 /dev/%k /mnt/%k"
```

```
ACTION=="remove" KERNEL=="s*" RUN+="/bin/umount /mnt/%k"
RUN+="/bin/rmdir /mnt/%k"
```

ж) Выполните перезагрузку ОС, чтобы новые правила вступили в силу или выполните команду:

```
sudo udevadm control --reload-rules
```

По правилам, описанным выше, любое обнаруженное устройство, подходящее по маске sd[c-z][0-9] (например, sde1) будет монтировано в каталог /mnt/<имя устройства> (например, /mnt/sde1). Образ Открытого CD-ROM раздела OPEN.ISO будет доступен по пути /mnt/sde1/OPEN.ISO

Маску для правил автоматического монтирования Администратор должен указать в соответствии с используемой конфигурацией ОС. Например, если подключаемые в ОС отображаются, начиная с буквы b (/dev/sdb1), то и маска в правилах автоматического монтирования должна быть указана sd[b-z][0-9].

До начала работы пользователя с изделием, RW-разделы должны быть отформатированы в соответствии с подразделом 6.7 «Форматирование в ОС семейства Linux».

**ВНИМАНИЕ!** Форматирование разделов в защищённых ОС требует определённого набора привилегий, которым по умолчанию обладает только суперпользователь.

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

										Лист
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					50

## 6.5 Установка программ в Astra Linux Special Edition 1.4 «Смоленск» и Astra Linux Special Edition 1.5 «Смоленск»

### 6.5.1 Дистрибутивные файлы для Astra Linux 1.4 SE и Astra Linux 1.5 SE

Названия файлов из состава дистрибутива и пути к распакованным файлам.

Таблица 12 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА для Astra Linux SE 1.4 «Смоленск» и Astra Linux SE 1.5 «Смоленск»

Дистрибутивный файл	Путь к каталогу, в котором будет установлена программа
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jсPKCS11-2</b>	
libjckt2_3.5.3.xxx_x64.deb, где «xxx» - версия сборки библиотеки	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_x64.deb, где «xxx» - версия сборки библиотеки	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcsfmkt2_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/usr/lib/libjcsfmkt.so.3.5.3 /usr/lib/libjcsfmkt.so.1 (symlink) /usr/lib/libjcsfmkt.so (symlink)
jcpkcs11-2_2.7.2.499_x64.deb	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cprosp-rdr-jacarta-64_3.6.408.741-4_amd64.deb	/opt/cprosp/lib/amd64/librdrijacarta.so.[version] /opt/cprosp/share (файлы поддержки кодировок)
cprosp-rdr-jacarta-64_5.0.0.1238-4_amd64.deb	/opt/cprosp/lib/amd64/librdrijacarta.so.[version] /opt/cprosp/share (файлы поддержки кодировок)

### 6.5.1 Установка программ в Astra Linux 1.4 SE и Astra Linux 1.5 SE

#### 6.5.1.1 Распаковка пакетов

Для распаковки (установки) deb-пакетов выполните из терминала fly следующую команду:

```
sudo dpkg -i <пакет установки>
```

где <пакет установки> – путь к deb-пакету установки с указанием имени файла.

Инд. № подл.      Подпись и дата      Взам. инв. №      Подпись и дата      Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата	<b>АЛДЕ.467669.004РЭ2</b>	Лист 51
------	------	-------------	---------	------	---------------------------	------------

Например:

```
sudo dpkg -i /media/jcsfadmin_3.5.3.xxx_x64.deb
```

В результате в каталог /opt/JaCartaSFGOSTSuite/ будет распакована (установлена) «Программа администратора» версии xxx.

### 6.5.1.2 Порядок распаковки (установки) в Astra Linux 1.4

а) Проверьте наличие (статус) пакетов в системе с помощью команды:

```
dpkg -s libccid libpcsc-lite1 pcscd libusb-0.1-4
```

1) Не установленные пакеты будут отображены в сообщении:

```
dpkg-query: пакет «имя_пакета» не установлен.
```

2) Установленные пакеты будут иметь статус:

```
Package: package_name
```

```
Status: install ok installed
```

б) Распакуйте (установите) недостающие пакеты из состава дистрибутива Astra Linux 1.4 SE:

1) Вставьте загрузочный диск Astra Linux 1.5 Special Edition в дисковод (или подключите DVD-дисковод виртуальной машины).

2) Выполните подключение дисковода:

```
sudo apt-cdrom add
```

3) Обновите список доступных пакетов:

```
sudo apt-get update
```

4) Установите недостающие пакеты с дистрибутива, например:

```
sudo apt-get install pcscd libccid
```

в) Распакуйте пакет libjct2\_3.5.3.xxx\_x64.deb

г) Распакуйте другие пакеты из состава дистрибутива USB-носитель «JaCarta SF/ГОСТ», устанавливая необходимые для конкретного АРМ программы.

### 6.5.1.3 Настройка мандатного доступа в Astra Linux 1.4 SE «Смоленск»

В операционной системе Astra Linux 1.4 SE «Смоленск» в качестве механизма безопасности может быть развернут (опционально) мандатный контроль доступа.

а) При необходимости проведите настройку механизма безопасности операционной системы:

1) Добавьте строку /usr/sbin/pcscd в файл /etc/parsec/privsock.conf;

1) Добавьте в скрипт запуска демона pcscd (обычно расположен в /etc/init.d/pcscd/) строку

```
PATH=/usr/lib/parsec/bin:$PATH
```

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						52

#### 6.5.1.4 Настройки безопасности в ОС Astra Linux 1.5 «Смоленск». За-мкнутая программная среда

В операционной системе Astra Linux 1.5 SE «Смоленск» в качестве механизма безопасности операционной системы может быть выбран режим «замкнутая программная среда».

Этот механизм безопасности подразумевает проверку ЭП исполняемых файлов ELF, входящих в состав устанавливаемого ПО. Для обеспечения установки пакетов из состава дистрибутива USB-носитель «JaCarta SF/ГОСТ», выполните следующие действия

а) В каталог `/etc/digisig/keys/` поместите переданный на оптическом диске, входящем в комплект поставки, открытый (публичный) ключ `ZAO_Aladdin_pub_key.gpg`

**ВНИМАНИЕ!** В случае, если механизм замкнутой программной среды уже используется в операционной системе, каталог `/etc/digisig/keys/` может быть недоступен. Выполните копирование от имени администратора, воспользовавшись командой `sudo cp <путь к файлу ключа> /etc/digisig/keys/`

б) В файле `/etc/digisig/digisig_initramfs.conf` проверьте значения параметров:

```
DIGSIG_ENFORCE=1
```

```
DIGSIG_LOAD_KEYS=1
```

в) Введите и выполните команду:

```
update-initramfs -u -k all
```

г) Перезагрузите компьютер.

#### 6.5.1.5 Настройки безопасности в ОС Astra Linux 1.5 «Смоленск». Мандатное управление доступом

В операционной системе Astra Linux 1.5 SE «Смоленск» в качестве механизма безопасности операционной системы может быть развёрнут мандатный контроль доступа.

а) При необходимости проведите настройку механизма безопасности операционной системы:

1) Добавьте строку `/usr/sbin/pcscd` в файл `/etc/parsec/privsock.conf`;

2) Добавьте в скрипт запуска демона `pcscd` (обычно расположен в `/etc/init.d/pcscd/`) строку

```
PATH=/usr/lib/parsec/bin:$PATH
```

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						53

### 6.5.1.6 Порядок установки программ в Astra Linux 1.5 SE «Смоленск»

После настройки механизмов безопасности изделия установите (распакуйте) необходимые для работы с изделием пакеты:

а) Проверьте наличие (статус) пакетов в системе с помощью команды:

```
dpkg -s libccid libpcsc-lite1 pcscd libusb-0.1-4
```

1) Неустановленные пакеты будут отображены в сообщении:

```
dpkg-query: пакет «имя_пакета» не установлен.
```

2) Установленные пакеты будут иметь статус:

```
Package: package_name
```

```
Status: install ok installed
```

б) Распакуйте (установите) недостающие пакеты из состава дистрибутива Astra Linux 1.5 SE:

1) Вставьте загрузочный диск Astra Linux 1.5 Special Edition в дисковод (или подключите DVD-дисковод виртуальной машины).

2) Выполните подключение дисковода:

```
sudo apt-cdrom add
```

3) Обновите список доступных пакетов:

```
sudo apt-get update
```

4) Установите недостающие пакеты с дистрибутива Astra Linux 1.5 SE «Смоленск», например:

```
sudo apt-get install pcscd libccid libpcsc-lite1
```

в) Распакуйте (установите) пакет из дистрибутива изделия USB-носитель «JaCarta SF/ГОСТ»

```
sudo dpkg -i /<путь>/libjckt2_3.5.3.xxx_x64.deb
```

Распакуйте другие пакеты из состава дистрибутива USB носитель «JaCarta SF/ГОСТ», устанавливая программы, необходимые для конкретного АРМ.

### 6.5.2 Начало работы и основной сценарий работы пользователя

Ввод носителей в эксплуатацию осуществляется в соответствии с эксплуатационными документами б) – е), указанными на с. 4.

**ВНИМАНИЕ!** В случае размещения АРМ главного администратора и АРМ администратора на СВТ под управлением ОС Astra Linux 1.4 SE «Смоленск» или ОС «Astra Linux 1.5 SE «Смоленск», необходимо учитывать следующее:

При выполнении инициализации ЭН Администратора доступа/Пользователя с CD-ROM разделами, имеющими ненулевой размер (Открытый CD-ROM, Скрытый CD-ROM), вспомога-

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

										Лист
										54
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

тельные временные разделы флеш-памяти с файлами `OPEN.ISO` и `HIDDEN.ISO` должны монтироваться в каталог с указанным путем и именем. Если путь к каталогу и его имя не будут заданы, то в программе администратора отобразится ошибка записи CD-ROM раздела.

Выполнять монтирование временных разделов можно либо вручную, используя команду `mount` при каждой инициализации изделий, либо настроить автоматическое монтирование.

Для установки автоматического монтирования вспомогательных разделов флеш-памяти, выполните следующее:

а) Создайте файл `/etc/udev/rules.d/automount.rules`;

б) Внесите в файл, созданный в пункте а) правила для обработки подключения и отключения съемных носителей (пример для пользователя с `uid=1000`, если необходимо задать правила для другого пользователя, необходимо указать верный `uid`):

```
ACTION=="add" KERNEL=="sd[c-z][0-9]" RUN+="/bin/mkdir -p /mnt/%k"
RUN+="/bin/mount -o uid=1000 /dev/%k /mnt/%k"
```

```
ACTION=="remove" KERNEL=="s*" RUN+="/bin/umount /mnt/%k"
RUN+="/bin/rmdir /mnt/%k"
```

в) Выполните перезагрузку ОС, чтобы новые правила вступили в силу или выполните команду:

```
sudo udevadm control --reload-rules
```

По правилам, описанным выше, любое обнаруженное устройство, подходящее по маске `sd[c-z][0-9]` (например, `sde1`) будет монтировано в каталог `/mnt/<имя устройства>` (например, `/mnt/sde1`). Образ Открытого CD-ROM раздела `OPEN.ISO` будет доступен по пути `/mnt/sde1/OPEN.ISO`

Маску для правил автоматического монтирования Администратор должен указать в соответствии с используемой конфигурацией ОС. Например, если подключаемые в ОС отображаются, начиная с буквы `b` (`/dev/sdb1`), то и маска в правилах автоматического монтирования должна быть указана `sd[b-z][0-9]`.

До начала работы пользователя с изделием, RW-разделы должны быть отформатированы в соответствии с подразделом 6.7 «Форматирование в ОС семейства Linux».

**ВНИМАНИЕ!** Форматирование разделов в защищённых ОС требует определённого набора привилегий, которым по умолчанию обладает только суперпользователь.

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

Изм.	Лист	№ документа	Подпись	Дата						

АЛДЕ.467669.004РЭ2

Лист  
55

6.6 Установка программ в Astra Linux Special Edition 1.6 «Смоленск», Astra Linux Special Edition 8.1 «Ленинград» и «Эльбрус-Д» (ТВГИ.00950-1)

6.6.1 Дистрибутивные файлы для Astra Linux 1.6 SE, Astra Linux SE 8.1 «Ленинград» и «Эльбрус-Д» (ТВГИ.00950-1)

Названия файлов из состава дистрибутива и пути к распакованным файлам представлены в таблицах 13 и 14.

Таблица 13 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА для Astra Linux SE 1.6 «Смоленск»

Дистрибутивный файл	Путь к каталогу, в котором будет установлена программа
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	
jcsfuser_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jсPKCS11-2</b>	
libjckt2_3.5.3.xxx_x64.deb	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_x64.deb	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcsfmkt2_3.5.3.xxx_x64.deb, где «xxx» - версия сборки	/usr/lib/libjcsfmkt.so.3.5.3 /usr/lib/libjcsfmkt.so.1 (symlink) /usr/lib/libjcsfmkt.so (symlink)
jcpkcs11-2_2.7.2.499_x64.deb	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cproccsp-rdr-jacarta-64_3.6.408.741-4_amd64.deb	/opt/cproccsp/lib/amd64/libdrjcarta.so.[version] /opt/cproccsp/share (файлы поддержки кодировок)
cproccsp-rdr-jacarta-64_5.0.0.1238-4_amd64.deb	/opt/cproccsp/lib/amd64/libdrjcarta.so.[version] /opt/cproccsp/share (файлы поддержки кодировок)

Таблица 14 – Названия файлов из состава дистрибутива и пути распаковки программ из состава ПКИА для Astra Linux SE 8.1 «Ленинград» и «Эльбрус-Д» (ТВГИ.00950-1)

Дистрибутивный файл	Путь к каталогу, в котором будет установлена программа
<b>Программа администратора</b>	
jcsfadmin_3.5.3.xxx_e2k-8c_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfadmin
<b>Программа главного администратора</b>	
jcsfkeyadmin_3.5.3.xxx_e2k-8c_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfkeyadmin
<b>Программа пользователя</b>	

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист 56
------	------	-------------	---------	------	--------------------	------------



jcsfuser_3.5.3.xxx_e2k-8c_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfuser
<b>Локальный сервер авторизации</b>	
jcsfserverd_3.5.3.xxx_e2k-8c_x64.deb, где «xxx» - версия сборки	/opt/JaCartaSFGOSTSuite/jcsfserverd /etc/jcsfgost/jcsfserverd/jcsfserverd
<b>Интерфейсная библиотека jсPKCS11-2</b>	
libjckt2_3.5.3.xxx_e2k-8c_x64.deb	/opt/JaCartaSFGOSTSuite/libjckt2.so /etc/jcsfgost/plistconf
<b>Программа диагностики</b>	
jcsfdiag_3.5.3.xxx_e2k-8c_x64.deb	/opt/JaCartaSFGOSTSuite/jcsfdiag
<b>Библиотека поддержки СЗИ семейства «Secret Net»</b>	
jcsfmkt_3.5.3.xxx_e2k-8c_x64.deb, где «xxx» - версия сборки	/usr/lib/libjcsfmkt.so.3.5.3 /usr/lib/libjcsfmkt.so.1 (symlink) /usr/lib/libjcsfmkt.so (symlink)
jcpkcs11-2_2.7.2.499_e2k-8c.deb	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
jcpkcs11-2_2.7.2.499-astra_e2k-8c.deb	/usr/lib/jcverify /usr/lib/libASEP11.so /usr/lib/libjckt2.so /usr/lib/libjcPKCS11-2.so.2.7.2 /usr/lib/libjcPKCS11ds.so /usr/share/doc/jcpkcs11-2/changelog.gz /usr/share/doc/jcpkcs11-2/copyright
<b>Библиотека поддержки СКЗИ «КриптоПро CSP»</b>	
cproccsp-rdr-jakarta-64_5.0.0.1238-4_e2k-8c.deb	/opt/cproccsp/lib/lib64/librdrijakarta.so.[version] /opt/cproccsp/share (файлы поддержки кодировок)

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

### 6.6.1.1 Распаковка пакетов (общий алгоритм)

Для распаковки deb-пакетов выполните из терминала `fly` следующую команду:

```
sudo dpkg -i <пакет установки>
```

где <пакет установки> – путь к deb-пакету установки с указанием имени файла.

Например:

```
sudo dpkg -i jcsfadmin-3.5.3.xxx.x86_64.deb (версии AstraLinux 1.6 SE «Смоленск»)
```

или

```
sudo dpkg -i jcsfadmin-3.5.3.xxx.x86_64.deb (версии AstraLinux 8.1 SE «Смоленск» и ОС «Эльбрус-Д»)
```

В результате в каталог `/opt/JaCartaSFGOSTSuite/` будет распакована «Программа администратора» версии `xxx`.

### 6.6.1.2 Настройки безопасности в ОС Astra Linux 1.6 «Смоленск». За-мкнутая программная среда

В операционной системе Astra Linux 1.6 SE «Смоленск» в качестве механизма безопасности операционной системы может быть выбран режим «замкнутая программная среда».

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						57

Этот механизм безопасности подразумевает проверку ЭП исполняемых файлов ELF, входящих в состав устанавливаемого ПО.

Для работы с ключом выполните следующие действия:

а) Скопируйте на СВТ открытый ключ `aladdin_pub.key` с поставочного диска JaCarta SF/ГОСТ и поместите его в директорию `/etc/digisig/keys` (либо `/etc/digisig/legacy`);

**ВНИМАНИЕ!** В случае, если механизм замкнутой программной среды уже используется в операционной системе, каталог `/etc/digisig/keys/` может быть недоступен. Выполните копирование от имени администратора, воспользовавшись командой `sudo cp <путь к файлу ключа> /etc/digisig/keys/`

б) Откройте файл `/etc/digisig/digisig_initramfs.conf` с помощью редактора (например, `nano`) от имени администратора:

```
sudo nano /etc/digisig/digisig_initramfs.conf
```

в) В файле `/etc/digisig/digisig_initramfs.conf` проверьте (установите) значения параметра `DIGSIG_ELFMODE` (1 или 2, в зависимости от действующих политик безопасности), например:

```
DIGSIG_ELFMODE=1
```

г) Сохраните изменения (`<Ctrl>+<o>`) и выйдите из редактора `nano` (`<Ctrl>+<x>`).

д) Введите и выполните команду:

```
sudo update-initramfs -u -k all
```

е) Перезагрузите СВТ.

### 6.6.1.3 Порядок (установки) распаковки в Astra Linux 1.6 «Смоленск»

Для обеспечения работы программ из состава ПО «Комплект программных средств» (RU.АЛДЕ.03.01.003-01) в ОС Astra Linux 1.6:

а) Перейдите к файлу `/etc/x11/fly-dm/fly-dmrc`

б) Найдите в указанном файле параметр `#ServerUID`

в) Раскомментируйте параметр и установите его, как `ServerUID=root`

г) Выполните команду `systemctl restart fly-dm`

После настройки механизма безопасности изделия «замкнутая программная среда» (опционально) и настройки параметров отображения рабочего стола, установите (распакуйте) необходимые для работы с изделием пакеты:

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист
										58
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

а) Проверьте наличие (статус) пакетов в системе с помощью команды:

```
sudo dpkg -s libccid libpcsclite1 pcsd libusb-0.1-4
```

1) Неустановленные пакеты будут отображены в сообщении:

```
sudo dpkg-query: пакет «имя_пакета» не установлен.
```

2) Установленные пакеты будут иметь статус:

```
Package: package_name
Status: install ok installed
```

б) Распакуйте (установите) недостающие пакеты из состава дистрибутива Astra Linux 1.6 SE:

1) Вставьте загрузочный диск Astra Linux 1.6 Special Edition в дисковод (или подключите DVD-дисковод виртуальной машины).

2) Выполните подключение дисковода:

```
sudo apt-cdrom add
```

3) Обновите список доступных пакетов:

```
sudo apt-get update
```

4) Установите недостающие пакеты с дистрибутива Astra Linux 1.6 SE «Смоленск», например:

```
sudo apt-get install pcsd libccid
```

При необходимости, следуйте инструкциям, отображаемым в командной строке терминала Fly.

в) Распакуйте (установите) пакет из дистрибутива изделия USB-носитель «JaCarta SF/ГОСТ»

```
sudo dpkg -i /<путь>/libjckt2_amd64.deb
```

г) Распакуйте другие пакеты из состава дистрибутива USB носитель «JaCarta SF/ГОСТ», устанавливая программы, необходимые для конкретного АРМ.

#### 6.6.1.4 Проверка корректности записи сведений об изделии

Для корректного отображения изделий выполните следующие действия:

а) От имени суперпользователя (root) откройте в редакторе nano файл Info.plist:

```
sudo nano /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist
```

б) Убедитесь, что в первых или последних строках списка (массива) ifdVendorID, расположенного в файле, в наличии запись, идентифицирующая производителя изделия:

```
<string>0x24DC</string>
```

в) На той же порядковой позиции в списке ifdProductID, расположенном в файле, в наличии запись, идентифицирующая изделие

```
<string>0x0406</string>
```

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						59

г) На аналогичной позиции в списке `ifdFriendlyName`, расположенном в файле присутствует название изделия:

```
<string>Aladdin R.D. JaCarta SF GOST</string>
```

д) При необходимости внесите соответствующие записи в списки (массивы), таким образом, чтобы они занимали одну позицию (например, строка 1 в каждом массиве)

е) Сохраните внесённые изменения нажатием кнопок `<Ctrl> + <O>`. Подтвердите сохранение нажав `<Enter>`.

ж) Закройте редактор `naipo` в терминале нажатием кнопок `<Ctrl> + <X>`.

### 6.6.1.5 Настройки безопасности в ОС Astra Linux 1.6 «Смоленск». Мандатное управление доступом

В операционной системе Astra Linux 1.6 SE «Смоленск» в качестве механизма безопасности операционной системы могут быть развёрнуты мандатное управление доступом и контроль целостности (МКЦ)

При необходимости работы с учётом политик мандатного контроля целостности, необходимо:

- настроить мандатные политики в отношении служб из состава изделия;
- произвести форматирование носителей в форматах `ext2`, `ext3` или `ext4`;
- установить необходимые атрибуты у пользователей изделия;
- установить правила использования устройств.

Для реализации работы на СВТ под управлением ОС Astra Linux 1.6 SE «Смоленск» с развёрнутым МКЦ с ненулевым уровнем конфиденциальности и уровнем целостности отличным от 63, после установки необходимых пакетов из дистрибутива ОС на настраиваемом АРМ:

а) Выдайте для учётной записи учётной записи администратора ОС привилегии, необходимые для настройки АРМ:

- `parsec_cap_priv_sock`;
- `parsec_cap_mac_sock`;
- `parsec_cap_ignmacvl`;
- `parsec_cap_chmac`.

Для этого перейдите Главное меню → Панель управления → Вкладка «Безопасность» → Вкладка «Политика безопасности» → Пользователи → Учётная запись администратора → Привилегии (см. рисунок 3).

После выдачи привилегий не забудьте подтвердить их выдачу.

На рисунке (в примере), имя администратора *Astra*.

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

										Лист
										60
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					

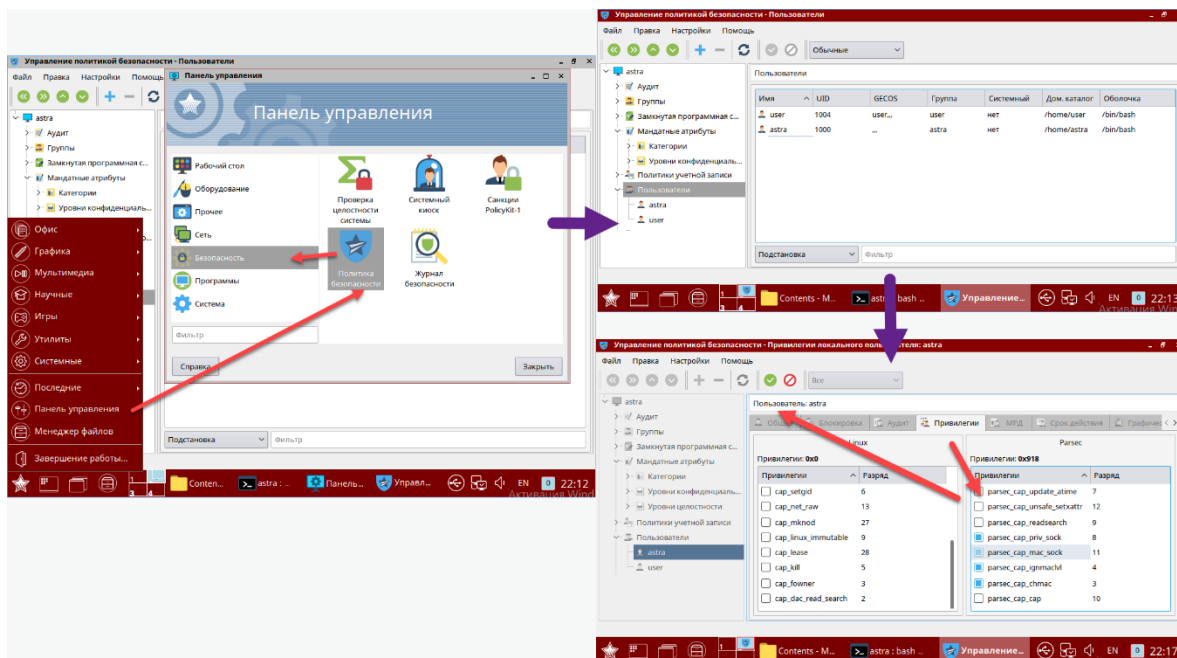


Рисунок 3 – Выдача привилегий учётной записи администратора ОС на APM

б) Перезагрузите СБТ.

в) Укажите для используемых служб корректный уровень доступа.

Для службы pcsd это возможно в двух вариантах: все пользователи (метка «ehole») или некоторые пользователи (для конкретных мандатных меток).

Для присвоения метки «Ehole»:

1) Представьте содержимое файла `/lib/systemd/system/pcsd.service` в виде (с помощью редакторов nano, vim или kate):

```
[Unit]
Description=PC/SC Smart Card Daemon
#requires=pcsd.socket

[Service]
ExecStart=/usr/sbin/pcsd --foreground
ExecReload=/usr/sbin/pcsd --hotplug
CapabilitiesParsec=PARSEC_CAP_PRIV SOCK

[Install]
#Also=pcsd.socket
WantedBy=multi-user.target
```

2) Откройте Терминал Fly (командная строка) и введите команды, отключающие pcsd.socket и перезапускающие службу pcsd:

```
sudo systemctl daemon-reload
sudo systemctl disable pcsd.socket
```

Подпись и дата	
Имя, № дубл.	
Взам. инв. №	
Подпись и дата	
Имя, № подл.	

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						61

```
sudo systemctl restart pcscd.service
```

3) Перезагрузите средство вычислительной техники.

4) Откройте «Терминал fly» и введите следующие команды:

```
sudo systemctl daemon-reload
```

```
sudo systemctl restart pcscd.service
```

```
sudo systemctl enable pcscd.service
```

5) Проверьте присвоение метки ehole файлу pcscd.comm:

```
sudo pdp-ls -Ma /var/run/pcscd/pcscd.comm
```

6) Если атрибуты файла pcscd.comm, совпадают со строкой ниже, то операция прошла успешно.

```
srw-rw-rw-m-1      root      root      Уровень_0:Низкий:нет:ehole  
/var/run/pcscd.comm
```

7) В случае, если атрибуты файла pcscd.comm не соответствуют указанным выше – отключите автозапуск службы pcscd.service командой

```
sudo systemctl disable pcscd.service
```

8) Повторите действия, описанные в пунктах 1–7.

Для запуска сервиса pcscd с конкретной ненулевой меткой безопасности в ОС Astra Linux 1.6:

1) Представьте содержимое файла /lib/systemd/system/pcscd.service в

виде:

```
[Unit]  
Description=PC/SC Smart Card Daemon
```

```
[Service]  
ExecStart=/usr/sbin/pcscd --foreground  
ExecReload=/usr/sbin/pcscd --hotplug  
PDPLabel=X:Y:Z
```

где атрибуты PDPLabel X, Y, Z это:

<Уровень>:<Уровень целостности>:<Категории>, например 1:63:0

```
[Install]  
WantedBy=multi-user.target
```

2) После чего необходимо перезапустить службу pcscd и добавить её в автозапуск:

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable pcscd.service
```

```
sudo systemctl restart pcscd.service
```

```
sudo systemctl status pcscd.service
```

3) Проверьте метку службы pcscd:

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						62

```
sudo pdpl-ps <номер> pcsd.service
```

где <номер> это номер службы, отображаемый при вводе команды `sudo systemctl pcsd.service`

Настройка доступа к разделам защищенного машинного носителя осуществляется с помощью встроенной утилиты Astra Linux 1.6 – fly-admin-smc (управление политикой безопасности).

Для задания правил использования конкретного раздела конкретного устройства необходимо совершить следующие действия:

- 1) Запустить утилиту `fly-admin-smc`.
- 2) Перейти на вкладку «Устройства» выбранной утилиты.
- 3) Щелчком правой кнопки мыши в поле «Устройства» открыть контекстное меню и выбрать опцию «Создать».
- 4) Выполнить инструкцию, записанную в открывшемся окне «Добавить устройство» – подключить (или переподключить) накопитель, к разделам которого настраивается доступ.
- 5) Выбрать раздел, для которого настраиваются правила доступа.
- 6) Открыть вкладку «Свойства», расположенную в правой части окна «Добавить устройство» и выбрать конкретный идентификатор раздела, для которого будет настроена политика доступа, после чего нажать кнопку «Да» в нижней части окна.  
**Важно!** Настройка каждого правила доступа к одному и тому же разделу (для разных уровней доступа) должна проводиться с разными идентификаторами, например, для открытого RW раздела, для уровня доступа 0, выбирается идентификатор ID\_SERIAL, а для уровня 1 – ID\_SERIAL\_SHORT;
- 7) В открывшемся окне «Регистрация нового устройства» установить флажок в чекбокс «Включено», ввести наименование раздела в поле «Наименование», на вкладке «Общие» выбрать разрешение для конкретного пользователя и группы, а на вкладке МРД установить параметры «Уровень» и «Категория».
- 8) Нажать «Применить изменения».
- 9) Повторить действия 1–8 необходимое количество раз, задавая необходимые правила для всех разделов.
- 10) Перезагрузить средство вычислительной техники.

Для операционных систем МСВС 3.0 и МСВС 5.0:

Для каждого пользователя и для каждого уровня секретности, для которых предполагается запуск программ выполнить следующие команды:

```
г) sudo chmac '0:0:rwrxrx' /tmp
```

В данном примере указан «0:0» – несекретный уровень. Для работы другом уровне секретности необходимо указать его номер по маске «x:x». Первая цифра обозначает уровень, вторая – категорию.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата					Лист	
										АЛДЕ.467669.004РЭ2
Изм.	Лист	№ документа	Подпись	Дата					Формат А4	

д) `sudo chmac -f '0:0:rwxrwx' /home/$username`

Указать уровень секретности для пользователя по маске «х:х». В данном примере «\$username» – имя пользователя, который будет запускать программу главного администратора, программу администратора или программу пользователя.

Для того чтобы ЭН отображался в «Программе пользователя» и «Программе администратора» необходимо прописать информацию о носителе в список `Info.plist`. Информация для необходимых для этого действий указана в документе «RU.АЛДЕ.03.01.007-01 34 01. USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа пользователя. Руководство оператора». Также возможен еще один способ: после установки «Программа пользователя» выполнить установку пакета `jcPKCS11-2-2.3.X.rpm`, находящемся в каталоге `Secret_Net` поставляемого дистрибутива. Данное действие позволит автоматически прописать необходимый список носителей в `Info.plist`. После установки пакета `jcPKCS11-2-2.3.X.rpm` следует перезагрузить операционную систему.

## 6.6.2 Установка автоматического монтирования разделов Флеш-памяти изделия для ОС Astra Linux 1.6 и ОС Astra Linux 8.1

При выполнении инициализации ЭН Администратора доступа/Пользователя с CD-ROM разделами, имеющими ненулевой размер (Открытый CD-ROM, Скрытый CD-ROM), вспомогательные временные разделы Флеш-памяти с файлами `OPEN.ISO` и `HIDDEN.ISO` должны монтироваться в каталог с указанным путем и именем. Если путь к каталогу и его имя не будут заданы, то в программе администратора отобразится ошибка записи CD-ROM раздела.

Выполнять монтирование временных разделов можно либо вручную, используя команду `mount` при каждой инициализации изделий, либо настроить автоматическое монтирование.

Для того, чтобы выполнить установку автоматического монтирования вспомогательных разделов флеш-памяти, необходимо выполнить следующие действия:

а) В директории `/etc/udev/rules.d/` создать файл локальных правил `11-local.rules`

**ВНИМАНИЕ:** 11 – порядковый номер создаваемого правила. Если правило с этим номером уже создано в системе, создайте файл с незанятым номером в диапазоне от 01 до 99.

б) Откройте файл и внесите следующие записи, вызывающие системную службу (создайте сценарий обработки):

```
KERNEL=="sd[a-z][0-9]",      SUBSYSTEMS=="usb",      ACTION=="add",
RUN+="/bin/systemctl start usb-mount@%k.service"
```

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

																			Лист
																			64
Изм.	Лист	№ документа	Подпись	Дата															



```
KERNEL=="sd[a-z][0-9]",      SUBSYSTEMS=="usb",      ACTION=="remove",
RUN+=" /bin/systemctl stop usb-mount@%k.service"
```

в) Для регистрации правил системой и включения их в работу – перезагрузите локальные правила (udev), введя следующую команду через консоль или командную строку используемого командера (в случае работы через командер):

```
udevadm control --reload-rules
```

г) В директории /etc/systemd/system/ создать файл, который будет использоваться в качестве системной службы

```
usb-mount@.service:
```

д) Откройте файл и внесите следующие записи

```
[Unit]
Description=Mount USB Drive on %i
[Service]
Type=oneshot
RemainAfterExit=true
ExecStart=/usr/local/bin/usb-mount.sh add %i
ExecStop=/usr/local/bin/usb-mount.sh remove %i
```

е) В директории /usr/local/bin/ создайте файл usb-mount.sh

ж) Откройте файл и внесите следующие записи:

```
#!/bin/bash
# Этот сценарий вызывается из системного юнита как сценарий обработки подключения/отключения накопителей.
usage() {
    echo "Использование: $0 {add|remove} device_name (например, sdb1)"
    exit 1
}

if [[ $# -ne 2 ]]; then
    usage
fi

ACTION=$1
DEVBASE=$2
DEVICE="/dev/${DEVBASE}"

# Проверям, не примонтировано ли уже устройство
MOUNT_POINT=$(/bin/mount | /bin/grep ${DEVICE} | /usr/bin/awk '{ print $3 }')

do_mount() {
    if [[ -n ${MOUNT_POINT} ]]; then
        echo "Предупреждение: ${DEVICE} уже смонтировано в ${MOUNT_POINT}"
    fi
    exit 1
}
```

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Лист	№ документа	Подпись	Дата

<b>АЛДЕ.467669.004РЭ2</b>	<i>Лист</i>
	65

```

fi
# Получаем информацию об устройстве: метка $ID_FS_LABEL, идентификатор
$ID_FS_UUID, тип файловой системы $ID_FS_TYPE
eval $(/sbin/blkid -o udev ${DEVICE})
# Создаём точку монтирования:
LABEL=${ID_FS_LABEL}
if [[ -z "${LABEL}" ]]; then
    LABEL=${DEVBASE}
elif /bin/grep -q " /media/${LABEL} " /etc/mtab; then
# Если точка монтирования уже существует изменяем имя:
    LABEL+="-${DEVBASE}"
fi
MOUNT_POINT="/media/${LABEL}"
echo "Точка монтирования: ${MOUNT_POINT}"
/bin/mkdir -p ${MOUNT_POINT}
# Глобальные опции монтирования
OPTS="rw,relatime"
# Специфические опции монтирования:
if [[ ${ID_FS_TYPE} == "vfat" ]]; then
    OPTS+=",users,gid=100,umask=000,shortname=mixed,utf8=1,flush"
fi
if ! /bin/mount -o ${OPTS} ${DEVICE} ${MOUNT_POINT}; then
    echo "Ошибка монтирования ${DEVICE} (статус = $?)"
    /bin/rmdir ${MOUNT_POINT}
    exit 1
fi
echo "**** Устройство ${DEVICE} смонтировано в ${MOUNT_POINT} ****"
}
do_unmount() {
    if [[ -z ${MOUNT_POINT} ]]; then
        echo "Предупреждение: ${DEVICE} не смонтировано"
    else
        /bin/umount -l ${DEVICE}
        echo "**** Размонтировано ${DEVICE} ****"
    fi
}

```

Инд. № подл.
Подпись и дата
Взам. инв. №
Инд. № дубл.
Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						66

## # Удаление пустых каталогов

```
for f in /media/* ; do
    if [[ -n $(/usr/bin/find "$f" -maxdepth 0 -type d -empty) ]];
    then
        if ! /bin/grep -q " $f " /etc/mstab; then
            echo "**** Удаление точки монтирования $f"
            /bin/rmdir "$f"
        fi
    fi
done
}
case "${ACTION}" in
add) do_mount ;;
remove) do_unmount ;;
*) usage ;;
esac
```

з) Сделайте созданный файл исполняемым, для этого в командной строке введите:  
chmod +x /usr/local/bin/usb-mount.sh

и) Перезагрузите компьютер.

До начала работы пользователя с изделием, RW-разделы должны быть отформатированы в соответствии с подразделом 6.7 «Форматирование в ОС семейства Linux».

**ВНИМАНИЕ!** Форматирование разделов в защищённых ОС требует определённого набора привилегий, которым по умолчанию обладает только суперпользователь.

## 6.7 Форматирование в ОС семейства Linux

Для операционных систем семейства Linux форматирование RW-разделов возможно с помощью утилиты командной строки `fdisk`, либо с помощью команды `mkfs`.

Использование данной утилиты возможно только от имени администратора, поэтому для ее запуска выполните команду:

```
sudo -i
```

а) выполните команду:

```
fdisk -l
```

или

```
lsblk
```

Подпись и дата	Инв. № дубл.	Взам. инв. №	Подпись и дата	Инв. № подл.					Лист
					АЛДЕ.467669.004РЭ2				67
Изм.	Лист	№ документа	Подпись	Дата					

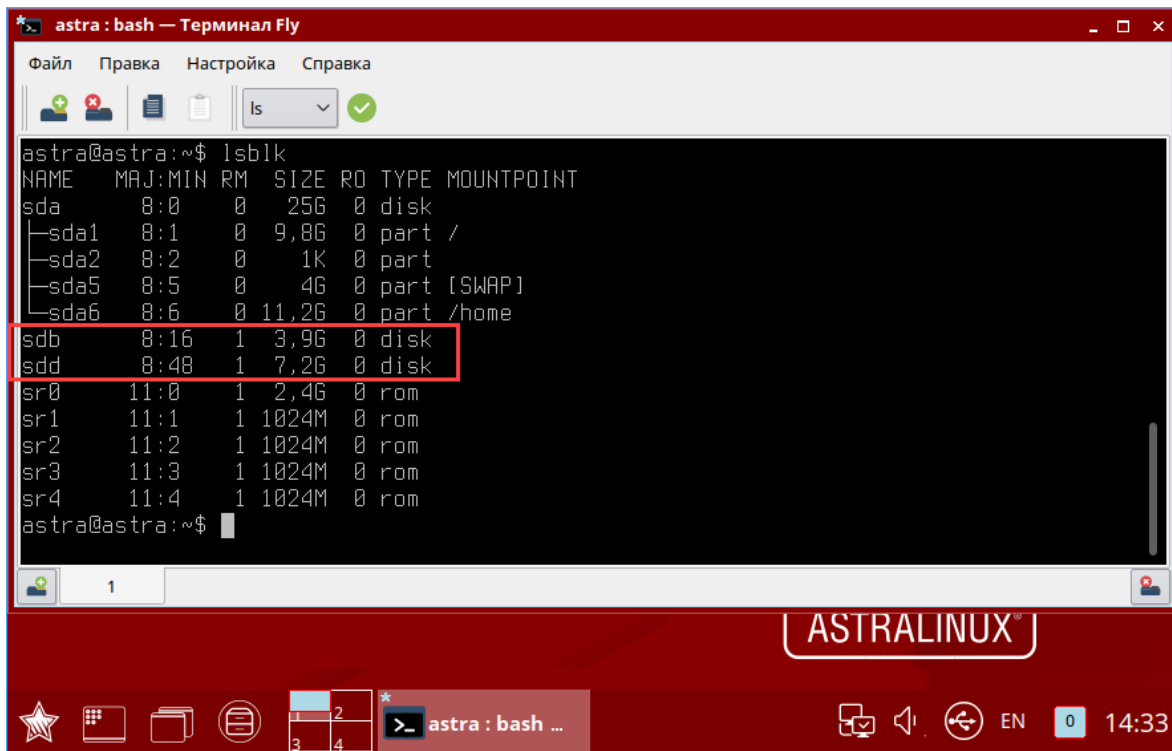


Рисунок 4 – Отображение блочных устройств с помощью команды lsblk

б) Из перечня подключенных дисков и их разделов, содержащегося в ответах команд выберите диск, соответствующий по размеру, созданному при инициализации USB-носителя (например, если размер RW раздела был указан 1 Гбайт, то выбрать диск размера 1 Гбайт). Кроме того, в fdisk-l, что на диске нет верной таблицы разделов. Например:

"На диске /dev/sdc отсутствует верная таблица разделов"

Таким образом дальнейшие действия в данном примере будут производиться с диском sdc.

в) выполните форматирование раздела с помощью команды:

mkfs.<тип фс> <путь к диску>

или

mkfs -t <тип фс> <путь к диску>

Например:

mkfs.ext2 /dev/sdb

Важно! Если RW-раздел впоследствии будет использоваться в ОС Astra Linux 1.6 при использовании мандатных политик доступа, то производить его форматирование нужно только в ext2, ext3, ext4. Мандатные метки на разделы с другим типом файловых систем не устанавливаются!

Важно! Если RW-раздел впоследствии будет использоваться в ОС MCBC 3.0, то производить его форматирование нужно только в FAT32. Для того, чтобы сразу отформатировать в NTFS нужно использовать указанный выше способ.

Подпись и дата
Име. № дубл.
Взам. инв. №
Подпись и дата
Име. № подл.

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						68

## 6.8 Удаление программ

### 6.8.1 Удаление программ для ОС семейств: МСВС, Альт Линукс и Astra Linux

а) Для того, чтобы удалить программы для ОС семейства МСВС или АЛЪТ Линукс, установлен пакет, выполните команду:

```
sudo rpm -e jcscfadmin/jcscfkeyadmin или sudo rpm -e jcscfuser
```

б) Удаление программ с помощью использования графической утилиты для ОС МСВС:

1) в главной панели нажмите кнопку **«Менеджер программ»**. Выполните поиск по имени и в появившемся поле ввода введите **«jcscfadmin»** (Программа администратора), **«jcscfkeyadmin»** (Программа главного администратора) или **«jcscfuser»** (Программа пользователя). Нажмите кнопку **«Искать»**. Если программа установлена, то она отобразится в списке установленных программ.

2) выделите программу, нажмите правой кнопкой мыши. В появившемся списке выберите **«Выделить/снять выделение»**. В результате данных действий программа будет подсвечена зеленым цветом.

3) далее нажмите кнопку **«Удалить»** в главной панели. В появившемся диалоговом окне будет указана программа, которая будет удалена. Нажмите кнопку **«Далее»**.

4) в появившемся диалоговом окне выбрать в случае необходимости желаемые опции удаления программы из предоставленного списка и нажать кнопку **«Да»**. Программа успешно удалена.

в) Для ОС Astra Linux и других ОС семейства Linux, на которую в данном случае был установлен пакет, для того, чтобы удалить Программу пользователя, Программу администратора или Программу главного администратора, выполните следующее:

1) выполните команду:

```
sudo dpkg -P jcscfadmin/jcscfkeyadmin или sudo dpkg -P jcscfuser
```

2) выполните команду:

```
sudo dpkg --purge jcscfadmin/jcscfkeyadmin или sudo dpkg --purge jcscfuser
```

г) Удаление программ с помощью использования графической утилиты Synaptic для ОС Astra Linux:

1) запустите Synaptic;

2) нажмите кнопку **«Поиск»** и в появившемся поле ввода ввести **«jcscfadmin»**, **«jcscfkeyadmin»** или **«jcscfuser»**.

3) если программа установлена, то в списке программ она будет отмечена зеленым цветом.

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

										Лист
Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2					69

4) выделите программу, нажмите правой кнопкой мыши и в появившемся списке нажмите «Отметить к удалению».

5) нажмите на кнопку «Применить» в главной панели Synaptic и подтвердите удаление. Программа успешно удалена.

Инв. № подл.	Подпись и дата			
	Инв. № дубл.			
	Взам. инв. №			
Подпись и дата				
Инв. № подл.				
Изм.				
Лист				
№ документа				
Подпись				
Дата				
АЛДЕ.467669.004РЭ2				
Лист				
70				

## Приложение А (обязательное)

### Политика управления использованием специализированных съемных машинных носителей информации

Функциональные возможности безопасности специализированного средства для безопасного хранения и переноса информации обеспечивают выполнение *политики управления использованием подключаемых съемных машинных носителей информации* для специализированных съемных машинных носителей информации (далее – Политика управления использованием специализированных съемных машинных носителей информации, Политика управления использованием).

Специализированный съемный машинный носитель информации, входящий в состав специализированного средства для безопасного хранения и переноса информации (далее – специализированного средства), является персонифицированным изделием. Его применение по назначению должно осуществляться физическим лицом – уполномоченным пользователем специализированного съемного машинного носителя информации. Закрепление (регистрация и учет) специализированного съемного машинного носителей информации осуществляется при его инициализации в качестве специализированного средства с помощью программного ключевого контейнера уполномоченным пользователем с ролью «администратор».

Политика управления использованием представляет собой совокупность правил, определяющих использование специализированных средств для безопасного хранения и переноса информации со средствами вычислительной техники. Правила определяют возможность использования открытых и скрытых разделов флеш-памяти изделия на средствах вычислительной техники и возможность доступа к информации, хранящейся в данных разделах.

Управление использованием специализированных средств для безопасного хранения и переноса информации осуществляется по следующим правилам:

- Настройка возможности использования специализированных съемных машинных носителей информации осуществляется уполномоченным пользователем с ролью «администратор».
- Проверка возможности использования инициализированного специализированного съемного машинного носителя информации выполняется при каждой попытке его подключения к средствам вычислительной техники.
- Возможность использования открытых разделов флеш-памяти специализированного средства предоставляется при его подключении к средствам вычислительной техники, на которых могут быть не установлены компоненты программного комплекса интеграции и администрирования.
- Возможность использования скрытых разделов флеш-памяти специализирован-

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

							<i>Лист</i>
						<i>АЛДЕ.467669.004РЭ2</i>	71
<i>Изм.</i>	<i>Лист</i>	<i>№ документа</i>	<i>Подпись</i>	<i>Дата</i>			

ного средства блокируется или разрешается при его подключении к средствам вычислительной техники, на которых установлены компоненты программного комплекса интеграции и администрирования, в соответствии с правами использования, основанными на идентификационной информации: специализированных съемных машинных носителей информации; средств вычислительной техники; пользователей; сочетании данной идентификационной информации.

– Санционирование (авторизация) возможности использования (подключения) скрытых разделов специализированного средства осуществляется по итогам проверки всей используемой совокупности идентификационной информации.

– Блокирование возможности использования скрытых разделов специализированного съемного машинного носителя информации на конкретном средстве вычислительной техники осуществляется, если результат проверки хотя бы одной идентификационной информации из всей совокупности является отрицательным (не соответствует установленным требованиям к идентификации) или в случае, пользователь не был успешно аутентифицирован.

– Предоставление возможности использования скрытых разделов флеш-памяти на конкретном средстве вычислительной техники осуществляется, если результат проверки всей совокупности идентификационной информации является положительным и пользователь был успешно аутентифицирован.

– При невозможности получения идентификационной информации, необходимой для санкционирования (авторизации), или при обнаружении возможного нарушения безопасности осуществляется блокирование возможности использования (подключения) скрытых разделов специализированного средства для безопасного хранения и переноса информации.

– Аудит возможности использования (подключения) специализированных средств для безопасного хранения и переноса информации ведется при подключении к средствам вычислительной техники постоянно, вне зависимости от результатов проверки идентификационной и аутентификационной информации.

Дополнительно к правилам управления использованием функциональными возможностями объекта оценки реализуются следующие правила управления доступом к информации в открытых и скрытых разделах специализированного съемного машинного носителя информации:

– Настройка прав доступа пользователей и правил управления доступом к информации в открытых и скрытых разделах инициализированного специализированного съемного машинного носителя информации осуществляется уполномоченным пользователем с ролью «администратор». Настройка прав доступа осуществляется посредством установки для разделов инициализированного специализированного съемного машинного носителя параметров (признаков): «чтение» («только чтение») или «чтение и запись».

– Проверка правил управления доступом и предоставление доступа пользователям

Изм.	Лист	№ документа	Подпись	Дата
------	------	-------------	---------	------

Подпись и дата

Име. № дубл.

Взам. инв. №

Подпись и дата

Име. № подл.

					АЛДЕ.467669.004РЭ2		Лист
							72



к информации в открытых разделах осуществляется вне зависимости от результатов проверки возможности использования специализированного средства для безопасного хранения и переноса на средствах вычислительной техники.

– Проверка правил управления доступом и предоставление доступа пользователям к информации в скрытых разделах выполняется после санкционирования (авторизации) возможности использования (подключения) скрытых разделов специализированного съемного машинного носителя информации на средствах вычислительной техники.

– Предоставление доступа пользователям для чтения или чтения и записи информации в разделах специализированного съемного машинного носителя информации осуществляется в соответствии с параметрами (признаками) скрытых разделов: «чтение» («только чтение») или «чтение и запись».

Другие типы подключаемых программно-аппаратных устройств не попадают под действие правил Политики управления использованием специализированных съемных машинных носителей информации.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата				Инв. № инв. №	Подпись и дата				Лист		
																АЛДЕ.467669.004РЭ2	
																	73
	Изм.	Лист	№ документа	Подпись		Дата											

## Приложение Б (обязательное)

### Проверка работоспособности изделия

#### Б.1 Общая информация о проверке работоспособности изделия

Б.1.1 Объект проверки: “USB-носитель «JaCarta SF/ГОСТ». Специализированное средство для безопасного хранения и переноса информации” (далее – специализированное средство), инициализированное ключевым контейнером администратора.

Б.1.2 Цель проведения проверки: проверка работоспособности изделия – выполнения изделием функций безопасности, описанных политикой безопасности, приведенной в приложении А.

Б.1.3 Тип проверки: периодическая, плановая.

Б.1.4 Размер межпроверочного интервала: не более одного года.

#### Б.2 Общие требования к условиям, обеспечению и проведению проверки

Б.2.1 Место проведения проверки: проверка проводится на территории организации-эксплуатанта; на средстве вычислительной техники, определяемом как АРМ администратора доступа.

Б.2.2 Требования к условиям проведения проверки: испытания должны проводиться в климатических условиях, соответствующих эксплуатационной документации на изделие:

- температура окружающего воздуха, °С 20 ± 5;
- относительная влажность воздуха при температуре от плюс 15 до плюс 25 °С, % от 45 до 75;
- атмосферное давление: от 630 до 800 мм рт. ст. (от 84 до 107 кПа).

Б.2.3 Требования к подготовке объекта проверки

Б.2.4 Нарботка объекта проверки не должна превышать предельных значений ресурса USB-носителя:

- 10 000 часов общей наработки изделия;
- 5 000 циклов «Подключение/отключение USB-носителя»;
- 10 000 циклов записи во флеш-память.

Б.2.5 Требования к обслуживанию объекта в процессе проверки

В процессе проверки проводятся работы в объеме контрольного осмотра:

– убедитесь, что выполняются правила эксплуатации, приведённые в разделе 2.3.1 [с. 25].

Б.2.6 Требования к персоналу

а) Испытания проводятся сотрудником организации-эксплуатанта, выполняющим роль «администратор безопасности».

б) Сотрудник, ответственный за проведение проверки должны быть ознакомлен с

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

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						74

правилами технической эксплуатации электроустановок потребителей и правилами по охране труда при эксплуатации электроустановок, а также эксплуатационной документацией на изделие, указанной в настоящем документе в разделе «Введение» (с. 3).

### Б.3 Требования безопасности

Б.3.1 Требования безопасности при подготовке изделия изложены в разделе 2.2.1 настоящего руководства по эксплуатации.

### Б.4 Порядок проведения испытаний

№	Перечень операций	Ожидаемый результат	Примечание
1.	Провести контрольный осмотр изделия. При осмотре визуально убедиться в отсутствии повреждений на корпусе, свидетельствующих о вскрытии машинного носителя информации – голографическая наклейка не должна быть разрушена.	Повреждения, свидетельствующие о вскрытии машинного носителя информации – отсутствуют. Голографическая наклейка, разрушающаяся при вскрытии носителя – не разрушена.	При отрицательном результате перейти к п.12
2.	Выполнить сличение уникального идентификационного номера проверяемого специализированного средства с выданным пользователю.	Уникальный номер специализированного съемного машинного носителя информации соответствует с номером машинного носителя информации, выданного пользователю.	При отрицательном результате перейти к п.12
3.	Подключить специализированное средство для безопасного хранения и переноса информации, инициализированное контейнером администратора в USB-разъем АРМ администратора. Подключить специализированное средство для безопасного хранения и переноса информации, инициализированное контейнером пользователя, сгенерированным с помощью ЭН администратора, в USB-разъем АРМ администратора.	Светодиодные индикаторы, расположенные в корпусах машинных носителей информации, зажигаются, отображая работу изделия.	При отрицательном результате перейти к п.12

Инд. № подл.	Подпись и дата
Взам. инв. №	Подпись и дата
Инд. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						75

Инд. № подл.	Подпись и дата	Взам. инв. №	Инд. № дубл.	Подпись и дата
Изм.	Лист	№ документа	Подпись	Дата

4.	<p>Проверить доступность открытых разделов специализированных средств для безопасного хранения и переноса информации (пользователя и администратора) – открытые разделы, созданные при первичной инициализации изделий должны быть доступны сразу после подключения.</p>	<p>В операционной системе, развернутой на АРМ администратора отображаются открытые разделы изделий, созданные при первичной настройке изделий.</p>	<p>При отрицательном результате перейти к п.12</p>
5.	<p>Создать тестовый текстовый файл test.txt с произвольным текстом внутри. Попробовать осуществить запись в открытые CD-ROM разделы изделий (при их наличии). Скопировать произвольно выбранные файлы с CD-ROM разделов.</p> <p>Попробовать осуществить запись в открытые CD-RW разделы изделий. Скопировать записанный файл с устройства. Проверить доступность информации в файле.</p>	<p>Запись в открытые CD-ROM разделы не производится.</p> <p>Открытые CD-ROM разделы доступны только для чтения информации.</p> <p>Открытые RW-разделы доступны для чтения и записи информации</p>	<p>При отрицательном результате перейти к п.12</p>
6.	<p>Запустить программу администратора, установленную на АРМ администратора. Указать путь к контейнеру администратора, с помощью которого было инициализирован ЭН администратора. Ввести аутентификационную информацию от контейнера. Активировать контейнер.</p> <p>Перейти в раздел программы «Администрирование», на вкладку «Управление». Проверить возможность смены ПИН-кода в секции «Электронный носитель» для ЭН администратора и ЭН пользователя. Убедиться в запросе аутентификационной информации.</p> <p>Перейти в раздел «Аудит» попробовать получить доступ к журналам</p>	<p>Смена ПИН-кода ЭН администратора осуществляется только при вводе актуальной аутентификационной информации администратора доступа (ПИН-код).</p> <p>Смена ПИН-кода ЭН пользователя осуществляется только при вводе актуальной аутентификационной информации пользователя (ПИН-код).</p> <p>Администратору предоставляется доступ к журналам изделий</p> <p>Генерация ключей автономного доступа не производится. Выводится сообщение «Неверный режим».</p>	<p>При отрицательном результате перейти к п.12</p>

АЛДЕ.467669.004РЭ2

Лист

76

Инд. № подл.	Подпись и дата	Взам. инв. №	Инд. № дубл.	Подпись и дата

	аудита. Перейти в раздел «контейнеры» выбрать специализированное средство пользователя. Попробовать сгенерировать ключи автономного доступа.		
7.	<p>Перейти в раздел программы «Ключевой контейнер» и деактивировать контейнер администратора. Указать путь к контейнеру пользователя.</p> <p>Получить доступ к контейнеру пользователя.</p> <p>В разделах программы администратора «Администрирование», «Аудит», «Контейнеры» убедиться в возможности управления изделием пользователя, просмотра и сохранения журналов, возможности генерации ключевых контейнеров для авторизации СВТ на использование скрытых разделов устройства пользователя. Деактивировать ключевой контейнер. Закрыть программу администратора.</p>	<p>Доступ к контейнеру пользователя и управлению устройством пользователя допускается при вводе аутентификационной информации контейнера пользователя и авторизации действий с помощью ПИН-кода ЭН администратора пользователя.</p> <p>После ввода необходимой идентификационной информации администратору доступно управление ЭН пользователя, просмотр журналов, генерация ключей автономного доступа для авторизации (санкционирования) СВТ для работы с ЭН пользователя.</p>	При отрицательном результате перейти к п.12
8.	<p>Отключить специализированное средство, инициализированное ключевым контейнером администратора.</p> <p>Запустить программу пользователя, установленную на АРМ администратора.</p> <p>Убедиться, что объект проверки отображается в программе пользователя как ЭН пользователя. Проверить отображение уникального идентификационного номера изделия.</p> <p>Попробовать провести авторизацию пользователя выбрав в секции «Режим доступа» пункт администратор доступа.</p>	<p>В программе пользователя, установленной на АРМ администратора, ЭН пользователя отображается в формате REDMILXXXXXXXXX или BLUEMILXXXXXXXXX, где REDIML или BLUEMIL – это тип изделия, а XXXXXXXX – уникальный номер изделия, совпадающий с нанесенным на корпус ЭН пользователя.</p> <p>Отображение скрытых разделов не осуществляется без предоставления полной идентификационной информации – если средство вы-</p>	При отрицательном результате перейти к п.12

Изм.	Лист	№ документа	Подпись	Дата

АЛДЕ.467669.004РЭ2

Инд. № подл.	Подпись и дата	Взам. инв. №	Инд. № дубл.	Подпись и дата
Изм.	Лист	№ документа	Подпись	Дата

	Убедиться, что без авторизации средства вычислительной техники с помощью ЭН администратора доступа, т.е. без полного ввода идентификационной информации – скрытые разделы недоступны.	числительной техники не авторизованно ЭН администратора доступа.	
9.	<p>Подключить специализированное средство, инициализированное ключевым контейнером администратора доступа.</p> <p>Убедиться, что объект проверки отображается в программе пользователя как ЭН администратора доступа.</p> <p>Осуществить авторизацию с помощью ЭН администратора доступа.</p> <p>Ввести аутентификационную информацию пользователя и администратора.</p> <p>Убедиться в том, что скрытые диски, созданные при первичной инициализации изделия, определяются в системе.</p>	<p>Объект проверки отображается в программе пользователя как ЭН администратора доступа.</p> <p>После предоставления программе пользователя полного объема идентификационной информации и прохождения аутентификации осуществляется доступ к скрытым разделам изделия.</p>	При отрицательном результате перейти к п.12
10.	<p>С помощью ранее созданного тестовый текстовый файл test.txt попробовать осуществить запись в скрытый CD-ROM раздел изделия (при их наличии). Скопировать произвольно выбранные файлы с CD-ROM разделов.</p> <p>Попробовать осуществить запись в скрытый CD-RW раздел изделий. Скопировать записанный файл с устройства. Проверить доступность информации в файле.</p>	<p>Скрытый CD-ROM раздел доступен только для чтения.</p> <p>Скрытый RW-раздел доступен для чтения и записи.</p>	При отрицательно результате перейти к п.12

Инд. № подл.	Подпись и дата	Взам. инв. №	Инд. № дубл.	Подпись и дата

11.	<p>С помощью программы пользователя отключить скрытые разделы ЭН пользователя.</p> <p>Осуществить попытку подключения скрытых разделов изделия, вводя неверный ПИН-код пользователя или администратора.</p> <p>Убедиться в блокировке скрытых разделов изделия.</p> <p>Запустить программу администратора.</p> <p>С помощью программы администратора разблокировать ЭН пользователя.</p> <p>Считать журналы ЭН пользователя.</p> <p>Убедиться в наличии записей о блокировке изделия в журнале доступа изделия.</p>	<p>При вводе неверной аутентификационной информации осуществляется блокировка изделия.</p> <p>С помощью программы администратора возможна разблокировка изделия.</p>	При отрицательно результате перейти к п.13
12.	<p>Отключить программу пользователя.</p> <p>Отключить специализированные средства пользователя и администратора.</p> <p>Завершить проверку и зафиксировать результаты.</p>	<p>В случае успешного прохождения всех шагов проверки продолжить эксплуатацию изделий. Изделие выполняет свои функции безопасности и работоспособно.</p> <p>В случае отрицательного результата прервать эксплуатацию изделия. Изделие не выполняет свои функции безопасности и неработоспособно.</p>	При отрицательно результате перейти к п.12

Изм.	Лист	№ документа	Подпись	Дата

АЛДЕ.467669.004РЭ2

Лист

79

# Приложение В (справочное)

## Термины и определения

Термин	Значение
Информация	Сведения (сообщения, данные) независимо от формы их представления.
Данные	Информация, представленная в формализованном виде, пригодном для обработки, интерпретации и обмена автоматическими средствами (средствами вычислительной техники) с возможным участием оператора.
Обработка информации (данных)	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации с данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение данных.
Изделие	Любой предмет или набор предметов производства, подлежащих изготовлению на предприятии. В данном документе – USB-носитель «JaCarta SF/ГОСТ»
USB-носитель «JaCarta SF/ГОСТ»	USB-носитель «JaCarta SF/ГОСТ» представляет собой: <ul style="list-style-type: none"> <li>– персональное средство криптографической защиты информации (далее – СКЗИ) – защищенное устройство с аппаратной реализацией российских алгоритмов шифрования, хэширования, электронной подписи, обеспечивающее безопасное создание, использование и хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта;</li> <li>– специализированное средство для безопасного хранения и переноса информации, обеспечивающее защиту от несанкционированного доступа к защищаемым разделам памяти, в том числе и со стороны вредоносного программного обеспечения (компьютерных вирусов).</li> </ul>
Программный комплекс интеграции и администрирования изделия «USB-носитель «JaCarta SF/ГОСТ»	Программный комплекс, включающий в себя прикладные программные средства «Программа пользователя» и «Программа администратора», программное средство «Интерфейсная библиотека jсPKCS11-2», программное средство «Библиотека поддержки СКЗИ «КриптоПро CSP», программное средство «Библиотека поддержки СЗИ семейства «Secret Net», а также Программа установки программы главного администратора, Программа установки программы администратора, Программа установки программы пользователя.
Пользователь электронного носителя (Пользователь ЭН)	Субъект доступа, имеющий права доступа к разделам памяти электронного носителя, соответствующие роли «Пользователь ЭН». Физическое лицо - пользователь электронного носителя, которому присвоена роль «Пользователь ЭН» имеет доступ к открытым и скрытым разделам флеш-памяти электронного носителя.

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						80



Термин	Значение
Пользователь средств криптографической защиты информации (Пользователь СКЗИ)	<p>Доступ осуществляется на авторизованных средствах вычислительной техники после успешной идентификации.</p> <p>Субъект доступа, имеющий права доступа к СКЗИ «Криптотокен 2 ЭП». Исполнение 9 (46538383.62.001), соответствующие роли «Пользователь СКЗИ».</p> <p>Физическое лицо - пользователь электронного носителя, которому присвоена роль «Пользователь СКЗИ» имеет доступ:</p> <ul style="list-style-type: none"> <li>– к открытым разделам флеш-памяти электронного носителя;</li> <li>– к функциям СКЗИ «Криптотокен 2 ЭП». Исполнение 9»;</li> <li>– к функциям и ключевым контейнерам СКЗИ «КриптоПро CSP».</li> </ul> <p>Доступ осуществляется на авторизованных средствах вычислительной техники после успешной идентификации.</p>
Администратор автоматизированной системы	<p>Пользователь автоматизированной системы, отвечающий за эксплуатацию системы и поддержание ее в работоспособном состоянии. Как правило, администратор имеет в автоматизированной системе расширенные права по доступу к объектам, а также по выполнению различных операций.</p> <p>Под термином «Администратор» (начинается с прописной буквы) понимается пользователь, имеющий расширенные права по доступу к объектам, а также по выполнению различных операций.</p>
Администратор доступа	<p>Пользователь ЭН, который обладает возможностью авторизовывать доступ к скрытым (защищаемым) разделам на АРМ пользователя.</p>
Администратор электронного носителя (Администратор ЭН)	<p>Субъект доступа, имеющий права доступа к разделам памяти электронного носителя, соответствующие роли «Администратор ЭН».</p> <p>Физическое лицо — пользователь электронного носителя, которому присвоена роль «Администратор ЭН» имеет доступ к открытым и скрытым разделам, а также системному разделу электронного носителя. Доступ осуществляется с применением служебных программных средств на авторизованных средствах вычислительной техники после успешной идентификации.</p>
Администратор средств криптографической защиты (Администратор СКЗИ)	<p>Субъект доступа, имеющий права доступа к СКЗИ, соответствующие роли «Администратор СКЗИ».</p> <p>Физическое лицо — пользователь электронного носителя, которому присвоена роль «Пользователь СКЗИ» имеет доступ:</p> <ul style="list-style-type: none"> <li>– к открытым разделам Флеш-памяти электронного носителя;</li> <li>– к функциям СКЗИ «Криптотокен 2 ЭП». Исполнение 9»;</li> <li>– к функциям и ключевым контейнерам СКЗИ «КриптоПро CSP».</li> </ul> <p>Доступ осуществляется с применением служебных программных средств на авторизованных средствах вычислительной техники после успешной идентификации.</p>
Права доступа	<p>Совокупность правил, устанавливающих допустимое взаимодействие между субъектом доступа и</p>

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	

Изм.	Лист	№ документа	Подпись	Дата	<b>АЛДЕ.467669.004РЭ2</b>	Лист
						81

Термин	Значение
	объектом доступа в автоматизированной системе. Как правило, права доступа рассматриваются как совокупность данных правил, применяемых к конкретному субъекту доступа или объекту доступа.
Роль	Заранее определенная совокупность прав доступа для субъекта доступа.
Автономный доступ	Подключение скрытых разделов флеш-памяти ЭН Пользователя с помощью файла автономного доступа к скрытым разделам флеш-памяти. Подключение скрытых разделов флеш-памяти ЭН Пользователя выполняется в «Программе пользователя».
Инициализация	Процесс начальной установки параметров изделия USB-носитель «JaCarta SF/ГОСТ» называется его инициализацией. Изделие инициализировано, если данные параметры заданы. Изделие не инициализировано, если параметры имеют неопределенное значение. Неинициализированное изделие не подлежит передаче пользователю. Процесс инициализации изделия выполняется в программном средстве «Программа администратора» с помощью соответствующего ключевого контейнера (ключевого контейнера администратора доступа для инициализации ЭН Администратора доступа и ключевого контейнера пользователя для инициализации ЭН Пользователя).
Обезличивание	Изделие USB-носитель «JaCarta SF/ГОСТ» является обезличенным, если у него очищена Флеш-память и сброшен ПИН-код. Процедура обезличивания выполняется в «Программе администратора». После процедуры обезличивания данные, сохраненные на изделии USB-носитель «JaCarta SF/ГОСТ» восстановлению не подлежат.
Ключевой контейнер	Файл с информацией для управления изделиями USB-носитель «JaCarta SF/ГОСТ». Для доступа к данному файлу устанавливается пароль. Ключевой контейнер необходимо перевыпускать после одного года эксплуатации. Информация необходимых для этого действий описана в документе RU.АЛДЕ.03.01.006-01 34 01. «USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора».
Ключевой контейнер администратора доступа	Ключевой контейнер, предназначенный для инициализации и обезличивания ЭН Администратора доступа. Создание ключевого контейнера администратора доступа выполняется в программном средстве «Программа главного администратора».
Ключевой контейнер пользователя	Ключевой контейнер, предназначенный для инициализации и обезличивания ЭН Пользователя. Создание ключевого контейнера пользователя выполняется в программном средстве «Программа главного администратора».
Ключевой контейнер для обновления разделов CD-ROM	Ключевой контейнер, предназначенный для перезаписи разделов CD-ROM изделия. Данный Ключевой контейнер формируется в «Программе главного администратора».
Файл автономного доступа к скрытым разделам Флеш-памяти	Файл, предназначенный для автономного доступа к скрытым разделам Флеш-памяти ЭН Пользователя. Данный файл можно создать с помощью «Программы администратора».

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						82

Термин	Значение
Локальный сервер авторизации	Сервер, с помощью которого пользователь может подключить скрытые разделы Флеш-памяти ЭН (входит в комплект поставки).
Ключевой контейнер локального сервера авторизации	Ключевой контейнер, предназначенный для доступа к скрытым разделам Флеш-памяти ЭН Пользователя с помощью Локального сервера авторизации. Данный ключевой контейнер создается в «Программе администратора».
Программа главного администратора	Прикладное программное средство, предназначенное для создания ключевых контейнеров, применяемых при управлении изделиями USB-носитель «JaCarta SF/ГОСТ».
Программа администратора	Прикладное программное средство, предназначенное для разметки модуля Флеш-памяти, загрузки ISO-образа и подготовки скрытого раздела пользователя, подготовки к эксплуатации ЭН Администратора доступа и ЭН Пользователя, подготовки к отправке в другую организацию конфиденциальных материалов с помощью ЭН Пользователя, аудита ЭН, обновления ПО ЭН, подготовки изделия USB-носитель «JaCarta SF/ГОСТ» к работе с СЗИ семейства «Secret Net» и СКЗИ «КриптоПро CSP».
Программа пользователя	Прикладное программное средство, предназначенное для авторизации АРМ для работы со скрытыми разделами Флеш-памяти изделия, а также для смены ПИН-кода Пользователя ЭН, смены ПИН-кода Пользователя СКЗИ и приема из другой организации конфиденциальных материалов с помощью ЭН Пользователя.
Конфигурация	Структурированная совокупность свойств (конструктивных, функциональных и эксплуатационных характеристик) предполагаемого к разработке, разрабатываемого или существующего изделия.
Автоматизированное рабочее место (АРМ)	Совокупность технических (аппаратных) средств вычислительной техники, системного <sup>1</sup> и прикладного программных средств. Автоматизированные рабочие места предназначены для организации доступа пользователя к информационным ресурсам автоматизированной системы.
АРМ Главного администратора	На данном АРМ должны быть установлены «Программа главного администратора» и «Программа администратора». АРМ Главного администратора используется для создания ключевых контейнеров и подготовки к эксплуатации ЭН Администратора доступа.
АРМ Администратора доступа	На данном АРМ должны быть установлены «Программа администратора» и «Программа пользователя». АРМ Администратора доступа используется для подготовки к эксплуатации и для управления ЭН Пользователей.
АРМ Пользователя	На данном АРМ должна быть установлена «Программа пользователя». АРМ Пользователя используется для подключения скрытых разделов Флеш-памяти ЭН и других задач «Программы пользователя».
Программное средство электронной вычислительной машины (Программное средство)	Программа, записанная на носителях данных, являющаяся продуктом (продукцией) промышленного

<sup>1</sup> Как правило в состав Автоматизированного рабочего места входят клиентские системное и прикладное программные средства.

Име. № подл.      Подпись и дата      Взам. инв. №      Име. № дубл.      Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						83

Термин	Значение
Программа	производства, снабженная программной документацией и предназначенная для распространения.
Программное обеспечение	Данные, предназначенные для управления конкретными компонентами автоматизированной системы в целях реализации определенного алгоритма.
Программное обеспечение	Совокупность программных средств (программ) системы обработки информации (средств вычислительной техники) и программных документов, необходимых для эксплуатации этих программ
Операционная система	Совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности средства вычислительной техники (системы обработки информации) за счет автоматизированного управления его работой и предоставляемого пользователю определенного набора услуг.
Специальные (специализированные) программные средства	Прикладные или системные, или системные и прикладные программные средства, разработанные для управления конкретными техническими средствами (оборудованием, моделью оборудования).
Драйвер	Программа, предназначенная для управления работой периферийных устройств.
Служебная программа, Программа обслуживания (Utility program)	Программа, предназначенная для оказания услуг общего характера пользователям и обслуживающему персоналу автоматизированной системы (системы обработки информации).
Вычислительная сеть	Взаимосвязанная совокупность территориально рассредоточенных систем обработки данных (средств вычислительной техники), средств и (или) систем передачи данных, обеспечивающая пользователям дистанционный (удаленный) доступ к ее ресурсам и коллективное использование этих ресурсов.
Локальная вычислительная сеть	Вычислительная сеть, охватывающая небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных. Как правило под небольшой территорией понимают здание, предприятие, учреждение.
Безопасность информации (данных)	Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.
Защита информации от несанкционированного доступа	Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.
Средства защиты информации	Технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации
Криптографическая защита информации	Защита информации от несанкционированного доступа, заключающаяся в обеспечении безопасности информации (данных) криптографическими методами (с помощью ее криптографического преобразования).
Средства криптографической защиты информации	Средства защиты информации, реализующие защиту информации криптографическими методами (реализующее алгоритмы криптографического преобразования информации).

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						84

Термин	Значение
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
Идентификация	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов или процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в автоматизированной системе для данного субъекта или объекта.
Идентификатор доступа	Уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код - предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и др. устройства).
Метка ЭН	Произвольное поле для дополнительной идентификации электронного носителя длиной не более 32 символов.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Или действия по проверке подлинности субъекта доступа в информационной системе.
Аутентификатор доступа	Признак субъекта доступа, подтверждающий принадлежность субъекту доступа предъявленного им идентификатора
ПИН-код	Личный опознавательный номер. Используется в качестве идентификационных данных (идентификатора доступа) при идентификации пользователя.
Средство вычислительной техники (Вычислительная машина, Электронная вычислительная машина, ЭВМ)	Совокупность (комплекс) технических (аппаратных) и программных средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач.

Име. № подл.	Подпись и дата
Взам. инв. №	Име. № дубл.
Подпись и дата	
Име. № подл.	

Изм.	Лист	№ документа	Подпись	Дата	АЛДЕ.467669.004РЭ2	Лист
						85

Приложение Г (справочное)  
Перечень принятых сокращений

АРМ	–	Автоматизированное рабочее место
ПО	–	Программное обеспечение
ПК	–	Персональный компьютер
ЭН	–	Электронный носитель
ЭП	–	Электронная подпись
СКЗИ	–	Средство криптографической защиты информации
АС	–	Автоматизированная система
ПИН-код	–	Персональный идентификационный номер
ОС	–	Операционная система
СЗИ	–	Средство защиты информации
НСД	–	Несанкционированный доступ

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата
--------------	----------------	--------------	--------------	----------------

					АЛДЕ.467669.004РЭ2	Лист
						86
Изм.	Лист	№ документа	Подпись	Дата		

# Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	Замененных	новых	Аннулированных					

Подпись и дата	
Инь. № дубл.	
Взам. инв. №	
Подпись и дата	
Инь. № подл.	

Инь. № подл.	
--------------	--