УТВЕРЖДЕН
КШДС.10514-01ТУ-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА

«АЛЬТ ЛИНУКС СПТ 7.0»

Технические условия

КШДС.10514-01ТУ

2017

Литера

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

СОДЕРЖАНИЕ

Настоящие технические условия распространяются на программное изделие «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01, предназначенное для автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений) всех возможных типов и направлений, и являются обязательным документом при изготовлении, контроле качества и приемке программного изделия.

Пример записи в других документах и (или) при заказе:

Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01.

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Программное изделие «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01 (далее – ПИ) предназначено для автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений) всех возможных типов и направлений.

1.2. ПИ представляет собой совокупность интегрированных программных продуктов, созданных на основе операционной системы «Linux». ПИ может обеспечивать обработку, хранение и передачу информации в круглосуточном режиме эксплуатации, а также позволяет запускать пользовательское программное обеспечение в сертифицированном окружении.

1.3. ПИ поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других ПЭВМ через каналы передачи данных или сетевые соединения.

1.4. В структуре ПИ выделяют следующие функциональные элементы:

- ядро операционной системы;
- системные библиотеки;
- комплекс встроенных средств защиты информации ПИ (далее – КСЗ);
- системные приложения;
- программные серверы;
- веб-серверы;
- системы управления базами данных;
- прочие серверные программы;
- интерактивные рабочие среды;
- командные интерпретаторы;
- прочие системные приложения.

КСЗ состоит из специальных программных пакетов, в том числе из состава ядра ОС и системных библиотек и предназначен для защиты ОС от НСД к информации на ПЭВМ.

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

ПИ должно соответствовать требованиям настоящих технических условий (далее – ТУ) и комплекта документации согласно КШДС.10514-01.

2.1. Общие параметры и характеристики (свойства)

2.1.1. Для изготовления ПИ должен использоваться носитель информации вида DVD-R емкостью не менее 4,5 ГБ или CD-R емкостью не менее 600 МБ, принятый ОТК предприятия-изготовителя носителя информации. Допускается использование носителя информации с приемкой ОТК, а также сертифицированных носителей информации ведущих фирм-производителей.

Срок хранения носителя информации с момента его изготовления до момента записи на него информации при изготовлении ПИ не должен превышать 12 месяцев.

2.1.2. Носитель информации, предназначенный для изготовления ПИ, не должен иметь видимых механических дефектов.

2.1.3. Носитель информации, предназначенный для изготовления ПИ, должен пройти входной контроль на предприятии-изготовителе ПИ на соответствие требованиям п.п. 2.1.1 – 2.1.2 настоящих ТУ.

2.1.4. Эксплуатационная документация на ПИ должна соответствовать требованиям стандартов ЕСПД и должна быть укомплектована по КШДС.10514-01 20 01.

2.1.5. В соответствии с требованиями законодательства в области защиты информации должна быть обеспечена возможность использования ПИ при построении:

– автоматизированных систем до класса защищенности «1В» включительно;
– информационных систем персональных данных до уровня 1 защищенности включительно;
– государственных информационных систем до класса 1 защищенности включительно (с учетом нейтрализации (блокирования) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом);
– автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до класса 1 защищенности включительно.

2.1.6. Минимальные характеристики технических средств, используемых для функционирования ПИ должны быть следующими:

– аппаратная платформа – ПЭВМ типа IBM PC;
– процессоры архитектур x86-64, i586 (Intel или совместимый с ним процессор, включая AMD, при этом для ОС i586 процессор должен поддерживать технологию PAE);
– объем оперативной памяти – не менее 512 МБ (рекомендуется от 1 ГБ и более);
– объем доступного пространства накопителя на жестких магнитных дисках не менее 2 ГБ (рекомендуется 15 ГБ и более);
– периферийные устройства ввода/вывода – устройство чтения и записи компакт-дисков.

2.2. Требования назначения

ПИ должно предоставлять следующие возможности:

1) работа с файлами и каталогами;

2) управление процессами:
– контроль создания и удаления процессов,
– контроль распределения системных ресурсов,
– синхронизация процессов,
– межпроцессное взаимодействие;

3) распределение оперативной памяти между прикладными задачами;

4) организация ввода-вывода:
– доступ к периферийным устройствам,
– буферизация данных,
– взаимодействие с управляющими программами аппаратных средств;

5) виртуализация на базе гипервизора QEMU/KVM;

6) администрирование системных приложений и комплекса средств защиты (далее – КСЗ).

2.2.1. При соблюдении условий эксплуатации ПИ должно реализовывать функции защиты информации в объеме требований 4-го класса защищенности в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992), а именно:

2.2.1.1. ПИ должно реализовывать дискреционный принцип контроля доступа, в частности обеспечивать:

– реализацию дискретных ПРД в файловых системах ext2, ext3, ext4, xfs, btrfs и tmpfs;
– реализацию дискретных ПРД при сетевом взаимодействии.

2.2.1.2. ПИ должно обеспечивать мандатный принцип контроля доступа, в том числе:

– реализацию мандатных ПРД в файловых системах ext2, ext3, ext4, xfs, btrfs и tmpfs;
– реализацию мандатных ПРД при сетевом взаимодействии.

2.2.1.3. ПИ должно обеспечивать очистку памяти:

– очистку внешней памяти;
– очистку оперативной памяти.

2.2.1.4. ПИ должно обеспечивать аутентификацию и идентификацию пользователей посредством реализации механизмов:

– локальной идентификации и аутентификации;
– доменной LDAP идентификации и аутентификации;
– доменной LDAP идентификации и аутентификации по протоколу Kerberos.

2.2.1.5. ПИ должно обеспечивать периодический контроль целостности посредством реализации следующих механизмов:

– контроля целостности КСЗ;
– контроля целостности файлов паролей и списка групп.

2.2.1.6. ПИ должно обеспечивать регистрацию:

1) ПИ должно осуществлять регистрацию следующих событий:
– использование механизмов идентификации и аутентификации,
– запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.),
– создание и уничтожение объектов,
– действия по изменению ПРД;

2) для каждого события должна регистрироваться следующая информация:
– дата и время,
– субъект, осуществляющий регистрируемое действие,
– тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа),
– успешно ли осуществилось событие (обслужен запрос на доступ или нет);

3) ПИ должно содержать средства выборочного ознакомления с регистрационной информацией;

4) должна быть предусмотрена регистрация всех попыток доступа и всех действий выделенных пользователей (администраторов защиты и т.п.).

2.2.1.7. ПИ должно обеспечивать маркировку документов:

– настройку параметров печати;
– создание шаблона штампа;
– маркировку защищаемой информации при выводе на документ в соответствии с произведенными настройками.

2.2.1.8. ПИ должно обеспечивать изоляцию программных модулей одного процесса (одного субъекта) от программных модулей других процессов (других субъектов).

2.2.1.9. ПИ должно обеспечивать защиту ввода и вывода на отчуждаемый физический носитель информации

ПИ должно различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (вывода на «помеченное» устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

2.2.1.10. ПИ должно обеспечивать сопоставление пользователя с устройством

ПИ должно обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

2.2.1.11. ПИ должно обеспечивать возможность тестирования:

– реализации ПРД (перехвата запросов на доступ, правильного распознавания санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верного сопоставления меток субъектов и объектов, запроса меток вновь вводимой информации, средств защиты механизма разграничения доступа, санкционированного изменения ПРД);
– невозможности присвоения субъектом себе новых прав;
– очистки оперативной и внешней памяти;
– работы механизма изоляции процессов в оперативной памяти;
– маркировки документов;
– защиты ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
– идентификации и аутентификации;

– запрета на доступ несанкционированного пользователя;
– работы механизма, осуществляющего контроль за целостностью СВТ.

2.2.2. Требования к механизмам защиты системы виртуализации ПИ

2.2.2.1. ПИ должно обеспечивать защиту от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа.

2.2.2.2. ПИ должно осуществлять контроль доступа субъектов доступа к средствам конфигурирования виртуальных машин (virt-manager, virsh, virt-install).

2.2.2.3. ПИ должно предоставлять возможность применения индивидуальных прав доступа субъектов к объектам.

2.2.2.4. ПИ должно обеспечивать контроль доступа субъектов доступа к файлам-образам, используемым для обеспечения работы виртуальных машин.

2.2.2.5. ПИ должно обеспечивать контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы и гипервизора.

2.2.2.6. ПИ должно обеспечивать изоляцию различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры.

2.2.2.7. ПИ должно осуществлять идентификацию и аутентификацию субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры (в т. ч. к средствам конфигурирования виртуальных машин).

2.2.2.8. ПИ должно блокировать доступ к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации.

2.2.2.9. ПИ должно обеспечивать регистрацию следующих типов событий:

– запуск (завершение) работы компонентов виртуальной инфраструктуры (виртуальных машин, гипервизора и т. д.);
– вход (выход) субъектов доступа в/из гипервизор(а);
– изменения прав доступа к файлам-образам виртуальных машин.

2.2.2.10. ПИ должно осуществлять контроль целостности компонентов, критически важных для функционирования гипервизора и виртуальных машин.

2.3. Комплектность ПИ

Комплектность ПИ должна соответствовать таблице (Таблица 1).

Таблица 1 – Комплектность ПИ

Обозначение	**Наименование**	**Кол. шт.**	**Примечание**
КШДС.10514-01	Операционная система «Альт Линукс СПТ 7.0» 64-бит	1	Поставляется на DVD-R
	Операционная система «Альт Линукс СПТ 7.0» 32-бит	1	Поставляется на DVD-R
	Комплект эксплуатационных документов по КШДС.10514-01 20 01	1 комплект	Поставляется на CD-R
	Операционная система «Альт Линукс СПТ 7.0». Формуляр КШДС.10514-01 30 01	1	Входит в состав комплекта эксплуатационных документов по КШДС.10514-01 20 01 Поставляется в печатном виде
	Копия сертификата соответствия ФСТЭК России	1	Поставляется в печатном виде
	Упаковка	1	Бокс

2.4. Требования к целостности

2.4.1. Изготовление ПИ должно осуществляться методом копирования программного документа КШДС.10514-01 12 02 на носители DVD-R с последующим подсчетом контрольной суммы.

2.4.2. После записи информации на носитель информации изготовитель должен произвести контроль записанной информации при участии представителя ОТК. В процессе контроля должно быть осуществлено считывание информации с каждого носителя и подсчет контрольной суммы. Подсчет контрольной суммы должен осуществляться с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0 (далее – ФИКС-UNIX 1.0) по алгоритму «Уровень 3, программно».

Контрольные суммы носителей, входящих в состав установочного комплекта ПИ представлены в таблице (Таблица 1).

Таблица 1 – Контрольные характеристики ПИ

Наименование диска	Контрольная сумма
Альт Линукс СПТ 7.0 DVD 64-бит	573D6B6B
Альт Линукс СПТ 7.0 DVD 32-бит	59FCD0AF
Альт Линукс СПТ 7.0 CD Документация	2C9F6B1B

2.4.3. Контрольная сумма всей информации, записанной на носителе, должна соответствовать значению, приведенному на этикетке документа КШДС.10514-01 12 02.

2.5. Маркировка

2.5.1. На носители информации, на которых размещено ПИ, должны быть нанесены этикетки. Виды этикеток приведены в приложениях (Приложение 1 и Приложение 2) к настоящему документу.

На рисунке 1.1 Приложения 1 приведена схема этикетки бокса с носителями информации, на которые записано ПИ.

На рисунке 2.1 Приложения 2 приведена схема этикетки носителей информации, на которые записано ПИ и документация на ПИ.

Сертифицированные образцы должны быть маркированы знаком соответствия системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00, наносимым в правый верхний угол защитного пластикового футляра ПИ.

2.5.2. Маркировка ПИ заключается в нанесении маркировочной информации на этикетку футляра (бокса) и на этикетки носителей информации. Данные, содержащиеся на этикетке бокса и этикетках носителей, представлены в таблицах ниже (Таблица 2 и Таблица 3).

Таблица 2 – Маркировочная информация, содержащаяся на этикетке бокса ПИ

Номер графы	Содержание
1	Наименование программного изделия
2	Характеристики программного изделия
3	Краткое описание программного изделия
4	Краткое описание конфигурации ПИ
5	Краткое описание конфигурации ПИ
6	Краткое описание конфигурации ПИ
7	Краткий перечень характеристик «Преимущества»

8	Краткий перечень характеристик «Основные компоненты»
9	Комплектация
10	Права и способы использования ПИ
11	Лицензии и торговые марки

Таблица 3 – Маркировочная информация, содержащаяся на этикетке носителей

Номер графы	**Содержание**
1	Наименование программного изделия
2	Штамп представителя ОТК
3	Дата выпуска программного изделия (год)
4	Заводской номер
5	Значение контрольной суммы
6	Разрядность версии ПИ (носители с ПИ), обозначение документации
7	Лицензии и торговые марки

2.5.3. Маркировочную информацию на этикетки наносят шариковым пишущим узлом с черной пастой до их наклейки на носитель информации или индивидуальную упаковку (бокс). Допускается изготовление этикеток средствами вычислительной техники.

2.5.4. На нерабочую поверхность носителя информации должна наноситься (наклеиваться) этикетка, содержащая маркировочную информацию о ПИ.

Этикетка на носитель информации должна содержать следующую информацию:
- наименование и обозначение ПИ;
- заводской номер;
- порядковый номер и количество носителей информации (в случае необходимости);
- значение контрольной характеристики ПИ.

2.5.5. В документ КШДС.10514-01 30 01 в разделе об упаковке и маркировке вносится следующая информация:

- название компании-изготовителя;
- учетный (заводской) порядковый номер;
- год и месяц выпуска.

Сертифицированные образцы продукции маркируются знаком соответствия системы сертификации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Знак соответствия наносится на правый верхний угол лицевой стороны вкладыша в футляр для хранения компакт-диска. Номер знака соответствия заносится в формуляр и в базу данных предприятия-изготовителя.

2.6. Упаковка

Упаковывание должно производиться в тару, которая должна обеспечивать защиту от механических и климатических воздействий при пересылке и хранении по ГОСТ 21552-84.

3. ПРАВИЛА ПРИЕМКИ

3.1. Общие положения

3.1.1. Приемка ПИ должна производиться согласно требованиям настоящих ТУ.

3.1.2. Для контроля качества и приемки ПИ устанавливаются следующие категории испытаний:

- приемо-сдаточные;
- периодические.

3.1.3. Основными документами при проведении испытаний являются:

- настоящие ТУ;
- комплект эксплуатационных документов по КШДС.10514-01 20 01.

3.1.4. В процессе проведения испытаний должны соблюдаться правила техники безопасности.

3.1.5. Испытания ПИ проводятся до полного их завершения. К началу проведения испытаний должны быть завершены мероприятия по подготовке испытаний, предусматривающие следующее:

- проверку готовности мест проведения испытаний;
- наличие и готовность средств обеспечения, гарантирующих создание условий и режимов испытаний;
- создание необходимых условий для проведения испытаний.

3.1.6. При внесении изменений в текст программы ПИ должны быть проведены повторные сертификационные испытания системы или инспекционный контроль.

3.2. Приемо-сдаточные испытания

3.2.1. Приемо-сдаточные испытания проводятся с целью проверки соответствия ПИ требованиям настоящих ТУ.

3.2.2. Приемо-сдаточные испытания ПИ проводит ОТК силами и средствами предприятия-изготовителя с целью контроля каждого экземпляра требованиям настоящих ТУ. При этом проводится проверка контрольной суммы дистрибутива ПИ. Снятие контрольной суммы должно осуществляться с использованием программы «ФИКС-UNIX 1.0» по алгоритму «Уровень-3, программно». Полученные контрольные суммы должны соответствовать контрольным суммам эталонного образца ПИ.

3.2.3. На приемо-сдаточные испытания ПИ предъявляется в комплектности, определенной в подразделе 2.3 настоящих ТУ.

3.2.4. Состав и последовательность приемо-сдаточных испытаний должны соответствовать таблице (Таблица 4). Последовательность проведения приемо-сдаточных испытаний может быть изменена по согласованию с представителем ОТК.

Таблица 4 – Перечень приемо-сдаточных испытаний

Наименование испытаний и проверок	**Пункт требований настоящих ТУ**	**Пункт методов контроля настоящих ТУ**
Проверка требований к комплектности	2.3	4.2
Проверка требований целостности	2.4	4.3
Проверка требований к маркировке	2.5	4.4
Проверка требований к упаковке	2.6	4.5
Проверка документации	2.1.4	4.6
Проверка носителей информации	2.1.1 – 2.1.3	4.7

3.2.5. По результатам испытаний составляется заключение о соответствии ПИ требованиям настоящих ТУ и заполняется формуляр.

3.2.6. Если в процессе испытаний будет обнаружено несоответствие хотя бы одному требованию настоящих ТУ, то принимаемый экземпляр ПИ считается не выдержавшим испытания и возвращается для выявления причин дефектов, а также для проведения мероприятий по их устранению и повторного предъявления. В акте об анализе и устранении дефектов отражаются причины несоответствия требованиям ТУ и методы их исправления.

3.2.7. Повторное предъявление ПИ на приемку осуществляется в порядке, установленном в настоящих ТУ.

3.2.8. Повторные испытания проводятся в полном объеме, установленном в настоящих ТУ для приемо-сдаточных испытаний. В зависимости от результатов анализа дефектов, обнаруженных при испытаниях, повторные испытания допускается проводить только по

требованиям, которым ПИ не соответствовало, а также по требованиям, для которых испытания не проводились.

3.2.9. ПИ считается окончательно принятым и подлежащим отгрузке потребителю, если оно соответствует требованиям настоящих ТУ, принято ОТК, а также упаковано и сдано на склад предприятия-изготовителя на ответственное хранение.

3.3. Периодические испытания

3.3.1. Периодические испытания проводятся с целью:

– периодического контроля качества изделия;
– контроля стабильности технологического процесса в период между предшествующими и очередными испытаниями;
– подтверждения возможности продолжения изготовления изделия по действующей конструкторской, нормативно-технической и технологической документации.

3.3.2. Периодические испытания проводятся предприятием-изготовителем при участии и под контролем ОТК, который дает заключение по результатам данных испытаний.

3.3.3. Периодичность испытаний устанавливается не реже одного раза в год по графику, утвержденному руководителем предприятия и согласованному ОТК на предприятии-изготовителе, если не указаны другие сроки в контрактах на поставку.

3.3.4. Периодические испытания должны проводиться в объеме и последовательности приведенной в таблице (Таблица 5).

Таблица 5 – Перечень периодических испытаний

Наименование испытаний и проверок	**Пункт требований настоящих ТУ**	**Пункт методов контроля настоящих ТУ**
Проверка требований к комплектности	2.3	4.2
Проверка требований целостности	2.4	4.3
Проверка требований к маркировке	2.5	4.4
Проверка требований к упаковке	2.6	4.5
Проверка документации	2.1.4	4.6
Проверка функциональных характеристик	2.1.1 – 2.1.3, 2.2	4.7, 4.9

3.3.5. Если ПИ выдержало периодические испытания, то качество изделий контролируемого периода считается подтвержденным данными испытаниями, а также считается подтвержденной возможность дальнейшего изготовления и приемки ПИ по той же документации, по которой изготовлено ПИ, прошедшее периодические испытания, до получения результатов очередных периодических испытаний.

3.3.6. Если ПИ, отобранное на периодические испытания, не выдержало испытаний, то приемку и отгрузку принятых изделий приостанавливают до выявления причин возникновения дефектов, их устранения и получения положительных результатов повторных испытаний.

3.3.7. Предприятие-изготовитель совместно с представителем ОТК анализируют результаты периодических испытаний для выявления причин появления и характера дефектов. По результатам анализа составляют перечень дефектов, обнаруженных при периодических испытаниях, и мероприятий по устранению дефектов и (или) причин их появления.

3.3.8. Если обнаружено, что несоответствие настоящим ТУ обусловлено ошибкой в порядке или условиях проведения испытаний или допущенной в процессе изготовления распознаваемой ошибкой, что может быть немедленно устранено, то повторные испытания, после устранения причин несоответствия настоящим ТУ, проводят на том же экземпляре ПИ, начиная с проверки требования, по которому было выявлено несоответствие.

3.3.9. Если обнаружено, что несоответствие настоящим ТУ на периодических испытаниях обусловлено ошибкой технологического процесса или другими причинами, устранение которых требует анализа и доработки (ремонта) проверяемого образца, то повторные испытания, после проведения мероприятий по устранению дефектов и их причин, проводят в полном объеме на удвоенном количестве образцов ПИ.

3.3.10. В технически обоснованных случаях в зависимости от характера выявленных дефектов допускается, по согласованию с представителем ОТК, проводить повторные периодические испытания в следующих случаях:

– если обнаружены несоответствия ПИ установленным требованиям;
– если испытания могли повлиять на возникновение дефектов.

3.3.11. Если характер дефектов испытуемого ПИ снижает его тактико-технические характеристики, то все принятые и отгруженные ПИ, в которых могут быть дефекты, возвращаются предприятию-изготовителю на доработку (замену), а все принятые и не отгруженные изделия за контролируемый период, в которых могут быть дефекты, обнаруженные при испытаниях, должны быть доработаны или заменены годными.

3.3.12. При получении положительных результатов повторных периодических испытаний приемку ПИ и их отгрузку возобновляют.

3.3.13. ПИ, прошедшие периодические испытания, после перепроверки в объеме приемо-сдаточных испытаний ОТК подлежат отгрузке.

4. МЕТОДЫ КОНТРОЛЯ (ИСПЫТАНИЙ)

4.1. Общие положения

4.1.1. Общие требования безопасности при проведении испытаний должны соответствовать ГОСТ 12.3.019-80.

4.1.2. Изготовление и испытания ПИ должны проводиться в нормальных климатических условиях испытаний:

- температура окружающего воздуха – от 15 до 35˚С;
- относительная влажность окружающего воздуха – от 45 до 75%;
- атмосферное давление – от 86 до 106 кПа (от 645 до 795 мм рт. ст.).

При температуре свыше 30˚С относительная влажность не должна превышать 70%.

4.2. Проверка соответствия ПИ требованиям подраздела 2.3 настоящих ТУ производится сличением состава предъявляемого изделия с составом, указанным в таблице (Таблица 1).

Проверка считается успешной, если состав предъявленного на испытания изделия соответствует комплектности, указанной в таблице (Таблица 1) настоящих ТУ.

4.3. Проверка соответствия ПИ требованиям подраздела 2.4 настоящих ТУ производится путем считывания информации с носителя, подсчета контрольной характеристики информации в соответствии с методикой, приведенной в настоящих ТУ, и сравнения ее со значением, указанным на этикетке документа КШДС.10514-01 12 02.

ПИ считается соответствующим требованиям подраздела 2.4 настоящих ТУ, если при проверке установлено, что вычисленное значение контрольной суммы информации на носителе соответствует значению контрольной суммы информации, приведенной на этикетке документа КШДС.10514-01 12 02, и значению, приведенному в КШДС.10514-01 30 01.

4.4. Проверка соответствия ПИ требованиям подраздела 2.5 настоящих ТУ производится внешним осмотром.

Проверка считается успешной, если при осмотре установлено, что ПИ имеет этикетки установленного образца в соответствии с требованиями подраздела 2.5 настоящих ТУ, маркировочная информация и ее расположение на этикетках соответствует требованиям настоящих ТУ.

4.5. Проверка соответствия ПИ требованиям подраздела 2.6 настоящих ТУ производится осмотром упаковки предъявляемого ПИ.

Проверка считается успешной, если упаковка ПИ произведена в соответствующую тару комплектно и имеет правильную маркировку.

4.6. Проверка соответствия ПИ требованиям п. 2.1.4 настоящих ТУ проводится внешним осмотром и сличением состава комплекта эксплуатационной документации с документом КШДС.10514-01 20 01.

Проверка считается успешной, если дефекты в эксплуатационной документации не обнаружены, установлено соответствие комплектности эксплуатационной документации документу КШДС.10514-01 20 01.

4.7. Проверка соответствия ПИ требованиям п.п. 2.1.1 – 2.1.3 настоящих ТУ проводится рассмотрением сопроводительной документации на носителе информации и визуальным осмотром поверхности на отсутствие видимых механических дефектов.

Проверка считается успешной, если носитель информации принят ОТК производителя, не имеет видимых механических дефектов, а установленный срок хранения носителя информации не превышал 12 месяцев.

4.8. Проверка соответствия ПИ требованиям пп. 2.1.4 настоящих ТУ производится путем осмотра и оценки комплекта документов на соответствие требованиям стандартов ЕСПД и на соответствие комплектности по КШДС.10514-01 20 01.

ПИ считается соответствующим требованиям пп. 2.1.4, если при проверке установлено, что комплект документов соответствует требованиям стандартов ЕСПД и укомплектована в соответствии с КШДС.10514-01 20 01.

4.9. Проверка соответствия ПИ требованиям подраздела 2.2 проводится в соответствии с подробным описанием, приведенным в документе КШДС.10514-01 51 01.

ПИ считается соответствующим требованиям подраздела 2.2, если проверки проведены успешно в соответствии с документом КШДС.10514-01 51 01.

5. ТРАСПОРТИРОВАНИЕ И ХРАНЕНИЕ

5.1. Транспортирование и хранение изделия производится согласно ГОСТ 21552-84.

5.2. ПИ, упакованное в транспортную тару, может транспортироваться любым видом транспорта на любое расстояние.

5.3. При транспортировании и хранении носителей информации с размещенным на них ПИ должны быть исключены их механические повреждения, удары и перегибы, а также попадание на носитель информации органических растворителей и прямого солнечного света.

5.4. Носители информации с размещенным на них ПИ должны храниться в боксах в помещении при температуре от 15 до 35 С и относительной влажности воздуха от 45 до 75%.

5.5. Носители информации с размещенным на них ПИ, которые подвергались воздействию температуры и относительной влажности воздуха, отличных от значений, установленных в качестве рабочих, необходимо перед использованием выдержать в нормальных условиях окружающей среды не менее 24 ч.

5.6. Не допускается хранение носителей информации с размещенным на них ПИ в одном помещении с химикатами и другими веществами, способными вызвать разрушения пластмасс и лакокрасочных покрытий.

6. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

6.1. Ввод в эксплуатацию и эксплуатация ПИ должны производиться в соответствии с эксплуатационной документацией на ПИ.

6.2. Нормальными климатическими условиями эксплуатации ПИ являются:

– температура окружающего воздуха от 15 до 35˚С;
– относительная влажность воздуха от 45 до 75 %;
– атмосферное давление от 86 до 106 кПа (от 645 до 795 мм рт. ст.).

6.3. Носитель информации следует вынимать из футляра на возможно короткое время, не допуская попадания на носитель информации прямого солнечного света. Брать носитель информации следует только за отверстие в центре и (или) за край, не касаясь пальцами при этом рабочей поверхности.

6.4. Для очистки рабочей поверхности носителя информации от загрязнения ее можно протереть мягкой хлопковой тканью, увлажненной дистиллированной водой, перемещая ткань от центра к периферии носителя информации, с последующей протиркой сухой тканью для удаления остаточных следов капель воды.

6.5. Перед эксплуатацией изделия необходимо внимательно ознакомиться с комплектом документации на ПИ, в том числе необходимыми организационными мерами, рекомендуемыми изготовителем в эксплуатационной документации.

6.6. При эксплуатации ПИ на объектах информатизации необходимо обеспечить обязательное выполнение организационно-технических мероприятий по защите информации:

– осуществление ввода в эксплуатацию и эксплуатации ПИ в соответствии с требованиями эксплуатационной документации;
– разработка нормативных документов, определяющих порядок допуска пользователей к ресурсам ПИ и назначения их полномочий;
– наличие администратора безопасности ПИ, отвечающего за правильную настройку и эксплуатацию КСЗ ПИ (роли администратора безопасности и администратора могут быть назначены одному лицу);
– администрирование ПИ с автоматизированного рабочего места, расположенного в пределах контролируемой зоны, на котором должно быть установлено сертифицированное по требованиям безопасности информации средство антивирусной защиты с последними обновлениями баз данных признаков компьютерных вирусов;
– запрет установки любых программных средств, не предусмотренных политикой безопасности предприятия, а также любых средств разработки и отладки программного обеспечения на объектах вычислительной техники с установленным ПИ;
– регулярное (не реже чем раз в две недели) выполнение администратором безопасности контроля состава установленного программного обеспечения на предмет его соответствия политике безопасности предприятия;
– ежедневная проверка ПИ на наличие вредоносного программного обеспечения;
– сохранение в секрете идентификаторов (имен) и паролей (кодов) пользователей/администраторов;

– периодическая (не реже чем раз в месяц) смена паролей (кодов) пользователей/администраторов;

– обязательное изменение паролей предустановленных учетных записей перед началом эксплуатации;

– отключение возможности удалённой авторизации для учётных записей из-за пределов контролируемой зоны;

– отключение возможности использования паролей из словарей, установка ограничений на минимальную длину и сложность пароля;

– включение задержки после определённого количества неуспешных попыток аутентификации;

– принудительное завершение сессии пользователей в веб-интерфейсах сервисов ОС Альт Линукс при отсутствии соответствующей активности;

– не допускается использование аппаратных платформ и версий базовых систем ввода-вывода и UEFI-драйверов, содержащих известные уязвимости, описанные в общедоступных источниках информации. В случае если используемая аппаратная платформа, версия базовой системы ввода-вывода или версия UEFI-драйвера содержит уязвимость, то ее использование допускается только после применения патча, представленного разработчиком данной аппаратной платформы, версии базовой системы ввода-вывода или версии UEFI-драйвера (официального патча). При отсутствии такого патча использование аппаратной платформы, версии базовой системы ввода вывода или версии UEFI-драйвера не допускается;

– не допускается изменение прав доступа к веб-панели альтератора (по умолчанию, доступна только root);

– при настройке подключения к FTP-серверу необходимо использовать chroot и не включать анонимного пользователя;

– для сервера печати CUPS использовать дайджест-аутентификацию;

– для безопасной работы с ПИ swap-разделы необходимо отключать, поскольку очистка swap-разделов не выполняется КСЗ ПИ;

– очистку внешней памяти необходимо осуществлять путем удаления объектов с помощью утилиты shred, для всех файловых систем, кроме tmpfs. Очистка внешней памяти для файловой системы tmpfs выполняется в рамках очистки оперативной памяти, ввиду размещения tmpfs в ОЗУ;

– после установки ПИ необходимо включить механизм очистки оперативной памяти, отключенный по умолчанию;

– при включенной политике selinux-policy-altlinux необходимо учитывать, что доступ к ПИ возможен только при использовании механизма локальной идентификации и аутентификации, в этом случае запрещается использовать механизм идентификации и аутентификации на сервере LDAP, в том числе с сетевой аутентификацией Kerberos;

– при включенной политике selinux-policy-altlinux необходимо учитывать, что запись в объекты межпроцессного взаимодействия типа очередь сообщений не допускается;

– при включенной политике selinux-policy-altlinux необходимо учитывать, что работа со средой виртуализации запрещена;

–

– для достижения сопоставления внешних и внутренних классификационных меток необходимо обеспечить соответствие классификационных меток объектов, добавляемых в систему (внешних классификационных меток), набору иерархических классификаций и неиерархических категорий, применяемых для формирования внутренних классификационных меток в соответствии с selinux-policy-altlinux, иными словами, для организации корректного функционирования мандатного разграничения в сети, на ее рабочих станциях должна быть установлена ПИ с включенной политикой selinux-policy-altlinux;

– необходимо учитывать, что сохранение контекста безопасности при добавлении пользователя из другой системы не осуществляется (его нужно назначать дополнительно), однако при удаленном подключении пользователя контекст сохраняется (в случае, если классификационные метки пользователя и его пользовательская информация хранятся на ПЭВМ с ПИ, к которой осуществляется подключение);

– при использовании механизмов регистрации и учета (аудита):

1) для осуществления аудита создания и уничтожения объектов, для каталога, в котором редактируется перечень объектов доступа, должно быть задано соответствующее правило аудита,

2) для осуществления аудита запроса на доступ к защищаемому ресурсу (чтение, запись, исполнение, изменение ПРД), для этого ресурса должно быть задано соответствующее правило аудита,

3) для осуществления аудита запуска и завершения программ и программных процессов необходимо задать правило аудита для соответствующих системных вызовов;

– в рамках работы со средой виртуализации создание и первоначальная конфигурация виртуальных машин должна осуществляться администратором безопасности;

– в рамках работы со средой виртуализации легитимными является работа с qemu\kvm;

– в рамках работы со средой виртуализации к средствам конфигурирования виртуальных машин относятся virt-manager, virsh, virt-install;

– выполнение удаленного подключения к виртуальным машинам должно осуществляться по протоколам VNC и SPICE;

– осуществление физической охраны аппаратной части автоматизированной системы, в которой эксплуатируется ПИ, предусматривающей контроль доступа в помещения, где расположены компоненты автоматизированной системы, посторонних лиц, не имеющих доступа к ресурсам ПИ, наличие надежных препятствий для несанкционированного проникновения в помещения с компонентами автоматизированной системы, особенно в нерабочее время;

– периодическая (не реже чем раз в неделю) проверка целостности программной и информационной частей ПИ администратором безопасности;

– периодическое (не реже чем раз в месяц) тестирование администратором безопасности функций защиты информации системы, в которой эксплуатируется ПИ;

– периодический (еженедельный) поиск актуальных уязвимостей и сведений об уязвимостях ПИ, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности;

– в случае обнаружения уязвимости в программных модулях ПИ ее устранение осуществляется путем установки сертифицированного обновления, либо путем принятия иных

организационно-технических мер, направленных на затруднение возможности эксплуатации уязвимости. При этом сами меры носят временный характер, а их использование допустимо до момента выпуска соответствующего обновления;

– администратор безопасности должен получать информацию о выходе обновлений ПИ на официальном сайте разработчика или путём информирования по электронной почте. Обновления вводятся в эксплуатацию после проведения инспекционного контроля. Для поддержания ПИ в сертифицированном статусе администратор безопасности должен устанавливать обновления. Автоматическое обновление сертифицированного ПИ не допускается;

– проверка администратором безопасности полученных обновлений и корректности их применения при помощи «ФИКС-UNIX 1.0» по алгоритму «Уровень-3, программно»;

– в случае отказа от получения критического обновления должны быть разработаны ограничения по применению ПИ, которые должны отражаться в нормативных документах и (или) политике безопасности организации-потребителя. Если невозможно реализовать ограничения по применению ПИ, то его использование прекращается;

– в случае обнаружения «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения, работа должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

– для обеспечения защиты компонентов виртуальной инфраструктуры на базе гипервизора QEMU/KVM после установки ОС в конфигурации «Офисный сервер» необходимо произвести доустановку программного пакета polkit. При этом программный пакет polkit работает только с системой инициализации systemd, и при установке ОС в конфигурации «Офисный сервер» необходимо убедиться, что на шаге выбора дополнительно устанавливаемых пакетов отмечен демон инициализации systemd;

– в системах с поддержкой Intel AMT при невозможности обновления прошивки с исправлением уязвимости CVE-2017-5689 отключить клиентский режим AMT настройкой «Disable CCM» и отключить автоматическую инициализацию AMT настройкой «Disable HBE».

7. ТРЕБОВАНИЯ ПО ПОРЯДКУ ОБНОВЛЕНИЯ СЕРТИФИЦИРОВАННОЙ ВЕРСИИ ПИ

7.1. Для ПИ должен быть разработан, регламентирован и поддерживаться механизм управления обновлениями.

Под управлением понимается выпуск обновления, его тестирование и проверки, а также доведение обновления до пользователей.

7.2. Порядок информирования пользователей

При выпуске критических обновлений (влияющих на безопасность ПИ) разработчик должен информировать потребителей (пользователей) путем публикации новостных сообщений на официальном сайте разработчика `https://www.basealt.ru` и посредством уведомлений по электронной почте.

7.3. Порядок получения обновлений

7.3.1. Для поддержания ПИ в сертифицированном статусе потребитель должен получать и устанавливать обновления.

7.3.2. В случае отказа от получения критического обновления разрабатываются ограничения по применению ПИ, которые должны отражаться в нормативных документах и политике безопасности организации-потребителя. Если невозможно реализовать ограничения по применению ПИ, то его использование должно быть прекращено.

7.3.3. После применения обновления потребитель (пользователь) должен выполнить расчет контрольных сумм контролируемых исполняемых файлов ПИ при помощи «ФИКС-UNIX 1.0» по алгоритму «Уровень-3, программно», перечень которых приведен в разделе «Контрольные характеристики» КШДС.10514-01 30 01.

7.4. Порядок установки и настройки обновлений

7.4.1. ПИ, имеющее прямой выход в Интернет, должны получать обновления при помощи модуля «Сервер обновлений» Центра управления по сети Интернет из специального репозитория (`http://ftp.altlinux.org/pub/distributions/ALTLinux/c7/`) в соответствии с выбранной веткой для нужного дистрибутива.

7.4.2. ПИ, не имеющие прямого выхода в сеть Интернет, должны получать обновления одним из двух способов:

– установка отдельного сервера обновлений на базе ПИ, находящегося вне защищенного контура, и организация ограниченного доступ к этому серверу;

– получение обновлений ПИ с ftp-сервера разработчика (`http://ftp.altlinux.ru/pub/distributions/ALTLinux/c7/images`) и доставка полученных образов к обновляемым компьютерам на дисках и выполнение обновления.

7.5. Контакты разработчика:

Официальный сайт:

`http://www.basealt.ru`

Адрес технической поддержки:

`support@basealt.ru`

8. ГАРАНТИИ ИЗГОТОВИТЕЛЯ (ПОСТАВЩИКА)

8.1. Предприятие-изготовитель гарантирует соответствие качества ПИ требованиям настоящих технических условий при соблюдении потребителем условий и правил хранения и эксплуатации, установленных эксплуатационной документацией.

8.2. Гарантийный срок эксплуатации ПИ – 5 лет со дня приемки. По дополнительному соглашению с заказчиком срок может быть продлен.

8.3. Гарантийный срок хранения и службы носителя информации определяется его техническими характеристиками.

8.4. Действие гарантийных обязательств на ПИ прекращается, если эксплуатирующей организацией (заказчиком) были внесены изменения в ПИ без согласования с предприятием-изготовителем или ПИ было передано сторонней организации.

ПРИЛОЖЕНИЕ 1

Этикетка для маркировки бокса ПИ

<table>
<tr><td colspan="3">(3)</td><td rowspan="4">(1)</td></tr>
<tr><td colspan="3">(4)</td></tr>
<tr><td colspan="3">(5)</td></tr>
<tr><td colspan="3">(6)</td></tr>
<tr><td>(7)</td><td>(8)</td><td>(9)</td><td rowspan="2">(2)</td></tr>
<tr><td colspan="3">(10)</td></tr>
<tr><td colspan="3">(11)</td><td>(11)</td></tr>
</table>

Рис. 1.1

ПРИЛОЖЕНИЕ 2

Этикетки для маркировки носителей информации ПИ

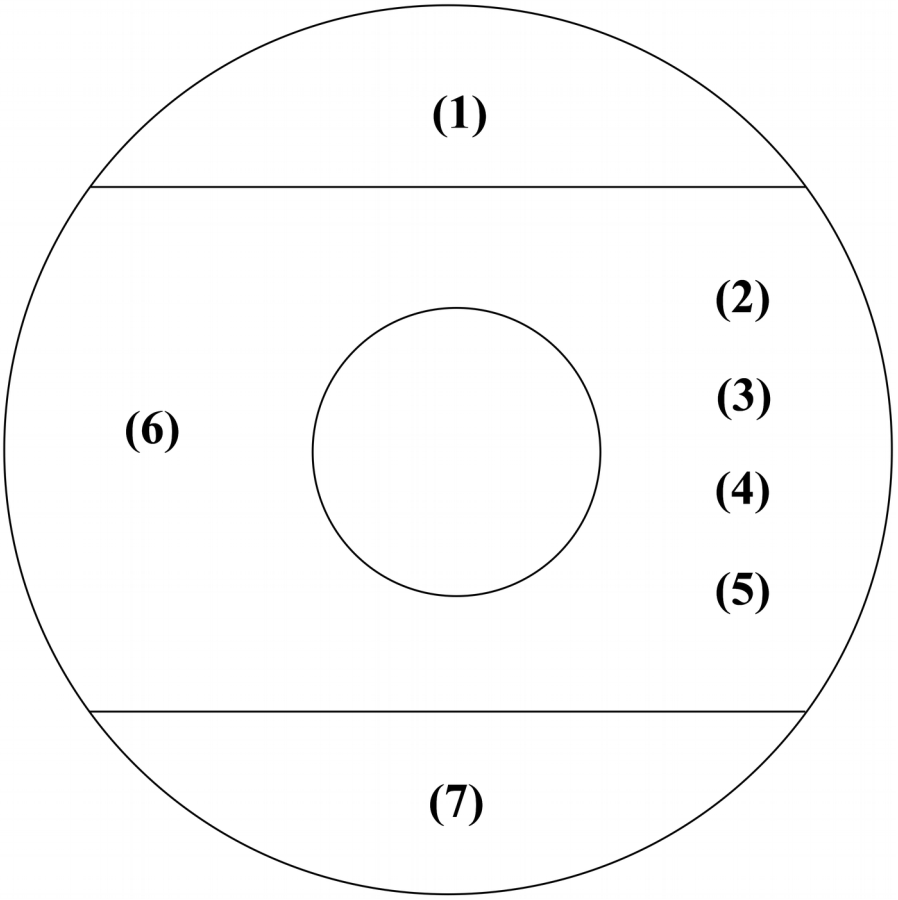

Рис. 2.1

ПРИЛОЖЕНИЕ 3

Перечень ссылочных документов

1) ГОСТ 12301-2006 «Коробки из картона, бумаги и комбинированных материалов. Общие технические условия»;

2) ГОСТ 12.3.019-80 «Система стандартов безопасности труда. Испытания и измерения электрические. Общие требования безопасности»;

3) ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;

4) Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999);

5) Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992);

6) Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие термины и сокращения:

CD-R	– Compact Disc-Recordable (записываемый компакт-диск);
DVD-R	– Digital Versatile Disc-Read (цифровой многоцелевой диск);
LDAP	– Lightweight Directory Access Protocol (облегченный протокол доступа к каталогам);
ЗСВ	– защита среды виртуализации;
КСЗ	– комплекс средств защиты;
ЛУ	– лист утверждения;
ОПС	– ограничение программной среды;
ОТК	– отдел технического контроля;
ПИ	– программное изделие;
РД	– руководящий документ;
ТУ	– технические условия;
УПД	– управление доступом субъектов доступа к объектам доступа;
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю.

Лист регистрации изменений

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в документе*	*№ документа*	*Входящий № сопроводитель-ного документа и дата*	*Подпись*	*Дата*
	измененных	*замененных*	*новых*	*аннулиро-ванных*					
1	-	Все	-	-	32	КШДС.420-2017	-		20.01.2017
2	-	6, 11, 12, 15, 22-24, 26	-	-	32	КШДС.421-2017	-		10.06.2017