УТВЕРЖДЕН

96636777.58.29.11.001 ТУ – ЛУ

**Операционная система**

**«AlterOS»,**

**децимальный номер 96636777.58.29.11.001**

**Технические условия**

**96636777.58.29.11.001 ТУ**

Москва

2019

СОДЕРЖАНИЕ

[Перечень принятых сокращений 3](#_Toc44581698)

[1. Введение 4](#_Toc44581699)

[2. Технические требования 6](#_Toc44581700)

[2.1 Функциональные требования безопасности 6](#_Toc44581701)

[2.2 Требования к аппаратному обеспечению 8](#_Toc44581702)

[2.3 Требования к эксплуатационной документации 8](#_Toc44581703)

[2.4 Комплектность 9](#_Toc44581704)

[2.5 Требования к носителям данных 9](#_Toc44581705)

[2.6 Упаковка и маркировка 9](#_Toc44581706)

[3. Правила приемки 11](#_Toc44581707)

[3.1. Приемо-сдаточные испытания 11](#_Toc44581708)

[3.2. Типовые испытания 12](#_Toc44581709)

[3.3. Периодические испытания 12](#_Toc44581710)

[4. Методы контроля 14](#_Toc44581711)

[4.1. Общие требования 14](#_Toc44581712)

[4.2. Проверка соответствия техническим требованиям 14](#_Toc44581713)

[5. Транспортирование и хранение 16](#_Toc44581714)

[6. Указания по эксплуатации 17](#_Toc44581715)

[6.1. Общие указания 17](#_Toc44581716)

[6.2. Указания по обновлению 19](#_Toc44581717)

[7. Гарантии изготовителя 24](#_Toc44581718)

[Приложение А 25](#_Toc44581719)

Перечень принятых сокращений

|  |  |  |
| --- | --- | --- |
| КД | - | конструкторская документация |
| КСЗ | - | комплекс средств защиты |
| ЛВС | - | локальная вычислительная сеть |
| НСД | - | несанкционированный доступ |
| ОС | - | операционная система |
| ПД | - | программная документация |
| ПРД | - | правила разграничения доступа |
| ПЭВМ | - | персональная электронная вычислительная машина |
| ЗБ | - | задание по безопасности |
| СЗИ | - | средства защиты информации |
| СУБД | - | система управления базами данных |
| ТУ | - | технические условия |
| ФСТЭК | - | Федеральная служба по техническому и экспортному контролю |
| ЭД | - | эксплуатационная документация |

1. Введение

Настоящие технические условия распространяются на операционную систему «AlterOS» (далее по тексту – ОС «AlterOS»), децимальный номер 96636777.58.29.11.001.

Разработчик и производитель ОС «AlterOS»: ООО «Алми Партнер» (адрес осуществления лицензируемого вида деятельности: 603093, Нижегородская обл., г. Нижний Новгород, улица Ковровская, д. 21а, оф. 77 этаж 7). Лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации № 1891 от 8 августа 2019 года.

ОС «AlterOS» – это операционная система общего назначения (типа «А»), представляющая собой комплекс управляющих и обрабатывающих программ, которые, с одной стороны, выступают как интерфейс между устройствами вычислительной системы и прикладными программами, а с другой стороны – предназначены для управления устройствами, управления вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений.

ОС «AlterOS» является многопользовательской, многозадачной операционной системой, основанной на ядре Linux. Функции безопасности ОС «AlterOS» состоят из функций операционной системы, запущенной в режиме ядра, и доверенных процессов.

ОС «AlterOS» может применяться для защиты информации, не содержащей сведения, составляющие государственную тайну:

* в значимых объектах критической информационной инфраструктуры 1 категории;
* в государственных информационных системах 1 класса защищенности;
* в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности;
* в информационных системах персональных данных при необходимости обеспечения
1 уровня защищенности персональных данных;
* в информационных системах общего пользования II класса.

***Загрузчик ОС*** – позволяет выбрать какую из установленных на СВТ операционную систему стоит загружать и в каком режиме, также инициализирует параметры ядра Linux, подготавливает его к загрузке и обеспечивает загрузку. Загрузчик может по цепочке передавать управление СВТ другому загрузчику, обеспечивая более широкую поддержку ПО.

***Ядро (kernel) ОС*** – основной компонент ОС, отвечающий за управление процессами, виртуальной памятью и драйверами устройств.

Ядро ОС «AlterOS» представляет собой единый блок бинарного кода. Все коды ядра и структуры данных, в том числе драйверы устройств, коды распределения ресурсов и виртуальной памяти, сетевой поддержки, а также файловая система – хранятся в едином адресном пространстве. Преимуществом такой структуры является то, что не требуется никаких переключений при запросах процессами системных ресурсов или прерываниях от различных устройств.

Общее адресное пространство, однако, не препятствует модульности системы. По мере необходимости ОС «AlterOS» подгружает в память либо выгружает из нее указанные модули.

В ОС «AlterOS» все ядро работает в привилегированном режиме – режиме ядра. Никакая часть кода не работает в режиме пользователя. Фрагменты поддержки ОС, не требующие запуска в режиме ядра, помещаются в раздел системных библиотек.

***Разделяемые системные библиотеки (system libraries)*** содержат стандартный набор функций, используемых приложениями для запросов к системным сервисам ядра. В библиотеках хранится также код функций отдельных сервисов ядра, исполняемых в обычном режиме без привилегий ядра.

При обращении приложения к системным ресурсам, управление от части системы, работающей в пользовательском режиме, передается ядру. Библиотеки осуществляют контроль за корректностью представленного запроса и выполняют преобразование параметров/аргументов запроса к требуемому формату.

***Под системными утилитами***(***system utilities***, программы управления системой) понимают программы, отвечающие за выполнение отдельных специализированных задач управления (управляющих функций системы). Одни утилиты запускаются лишь один раз для инициализации и конфигурирования отдельных элементов системы, другие вызываются регулярно, например, утилиты принимающие запросы на регистрацию с терминалов системы, либо утилиты обновляющие файлы регистрации.

**Сведения о сертификации:**

ОС «AlterOS» сертифицирована в системе сертификации средств защиты информации Федеральной службы по техническому и экспортному контролю Российской Федерации по требованиям безопасности информации
№ РОСС RU.0001.01БИ00 на соответствие Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий – по 4 уровню доверия, Требованиям безопасности информации к операционным системам (ФСТЭК России, 2016), Профилю защиты операционных систем типа А четвертого класса защиты ИТ.ОС.А4.ПЗ (ФСТЭК России, 2017).

Настоящие ТУ являются обязательными для изготовителей, представителей отдела технического контроля (ОТК) при изготовлении, испытаниях, приемке, упаковке, хранении и транспортировании программного комплекса.

Пример записи обозначения ОС «AlterOS» в документации другой продукции и (или) при заказе:

Операционная система «AlterOS», децимальный номер 96636777.58.29.11.001.

1. Технические требования

ОС «AlterOS» должна соответствовать требованиям настоящих технических условий.

## Функциональные требования безопасности

Функциональные требования безопасности приведены в таблице 1.

Таблица 1 – Функциональные требования безопасности[[1]](#footnote-1)

| **Идентификатор компонента требований** | **Название компонента требований** |
| --- | --- |
| FAU\_GEN.1 | Генерация данных аудита |
| FAU\_ARP.1 | Сигналы нарушения безопасности |
| FAU\_SEL.1 | Избирательный аудит |
| FAU\_SAR.1 | Просмотр аудита |
| FAU\_SAR.2 | Ограниченный просмотр аудита |
| FAU\_SAR.3 | Выборочный просмотр аудита |
| FAU\_STG.1 | Защищенное хранение журнала аудита |
| FAU\_STG.3 | Действия в случае возможной потери данных аудита |
| FAU\_STG.4 | Предотвращение потери данных аудита |
| FDP\_ACC.1 | Ограниченное управление доступом |
| FDP\_ACF.1 | Управление доступом, основанное на атрибутах безопасности |
| FDP\_CRC\_EXT.1 | Восстановление информации |
| FDP\_ETC.2 | Экспорт данных пользователя с атрибутами безопасности |
| FDP\_IFC.2 | Полное управление информационными потоками |
| FDP\_IFF.1 | Простые атрибуты безопасности |
| FDP\_DDM\_EXT.1 | Уничтожение (стирание) информации |
| FDP\_RIP.2 | Полная защита остаточной информации |
| FDP\_RSI\_EXT.1 | Управление установкой программного обеспечения |
| FDP\_RSP\_EXT.1 | Правила запуска компонентов программного обеспечения |
| FDP\_RSP\_EXT.2 | Контроль запуска компонентов программного обеспечения |
| FIA\_AFL.1 | Обработка отказов аутентификации |
| FIA\_ATD.1 | Определение атрибутов пользователя |
| FIA\_OID\_EXT.1 | Идентификация объектов доступа |
| FIA\_SOS.1 | Верификация секретов |
| FIA\_UAU.2 | Аутентификация до любых действий пользователя |
| FIA\_UAU.5 | Сочетание механизмов аутентификации |
| FIA\_UAU.7 | Аутентификация с защищенной обратной связью |
| FIA\_UID.1 | Выбор момента идентификации |
| FIA\_UID.2 | Идентификация до любых действий пользователя |
| FIA\_USB.1 | Связывание пользователь-субъект |
| FMT\_MOF.1 | Управление режимом выполнения функций безопасности |
| FMT\_MSA.1 | Управление атрибутами безопасности |
| FMT\_MSA.3 | Инициализация статических атрибутов |
| FMT\_MTD.1 | Управление данными функций безопасности |
| FMT\_MTD.2 | Управление ограничениями данных ФБО |
| FMT\_SAE.1 | Ограниченная по времени авторизация |
| FMT\_SMF.1 | Спецификация функций управления |
| FMT\_SMR.1 | Роли безопасности |
| FMT\_UST\_ЕХT.1 | Поддержка наборов базовых конфигураций |
| FPT\_ACF\_EXT.1 | Управление доступом к компонентам операционной системы |
| FPT\_ITC.1 | Конфиденциальность экспортируемых данных функциональных возможностей безопасности объекта оценки при передаче |
| FPT\_BOP\_EXT.1 | Защита от переполнения буфера |
| FPT\_MTR\_EXT.1 | Монитор обращений |
| FPT\_APW\_EXT.1 | Защита хранимой аутентификационной информации |
| FPT\_TST.1 | Тестирование функциональных возможностей безопасности |
| FPT\_RCV.1 | Ручное восстановление |
| FPT\_STM.1 | Надежные метки времени |
| FPT\_FLS.1 | Сбой с сохранением безопасного состояния |
| FRU\_FLT.1 | Пониженная отказоустойчивость |
| FRU\_PRS.1 | Ограниченный приоритет обслуживания |
| FRU\_RSA.1 | Максимальные квоты |
| FTA\_MCS.2 | Ограничение на параллельные сеансы по атрибутам пользователя |
| FTA\_SSL.1 | Блокирование сеанса, инициированное ФБО |
| FTA\_SSL.2 | Блокирование, инициированное пользователем |
| FTA\_SSL.3 | Завершение сеанса, инициированное функциональными возможностями безопасности |
| FTA\_TSE.1 | Открытие сеанса с объектом оценки |
| FPO\_DFS\_EXT.1 | Изоляция процессов |
| FPO\_OBF\_EXT.1 | Блокирование файлов процессами |
| FPO\_RIP\_EXT.1 | Выделение случайных областей оперативной памяти |

## Требования к аппаратному обеспечению

Для установки и работы ОС «AlterOS» необходимо выполнение следующих аппаратных требований:

* **Минимальные требования для установки ОС «AlterOS»:**
	+ Процессор архитектуры x86\_64/i686;
	+ 2 Гб оперативной памяти;
	+ 8 Гб свободного места на жестком диске;
	+ Видеокарта с поддержкой разрешения 1024 х 768.

## Требования к эксплуатационной документации

Эксплуатационная документация должна поставляться в твердых копиях или в электронном виде на DVD. Документация не должна иметь дефектов после изготовления и должна соответствовать подлинникам эксплуатационной документации, хранящимся в архиве предприятия-изготовителя.

Состав эксплуатационной документации на ОС «AlterOS» включает в себя:

Таблица 2 – Документация на изделие

|  |  |  |
| --- | --- | --- |
| № | Наименование | Обозначение |
|  | Технические условия | 96636777.58.29.11.001 ТУ |
|  | Формуляр | 96636777.58.29.11.001 – 01 30 |
|  | Руководство оператора | 96636777.58.29.11.001 – 01 34 |
|  | Руководство администратора | 96636777.58.29.11.001 – 01 91 |

Требования к составу и содержанию документов предъявляются в соответствии с ГОСТ 2.601-2006 «Единая система эксплуатационной документации. Эксплуатационные документы», а также ЗБ.

1. Документ «Операционная система «AlterOS». Технические условия» должен быть выполнен в соответствии с ГОСТ 2.114-2016 «Технические условия» и содержать полный комплекс требований к продукции, ее изготовлению, приемке, а также методы, средства и оборудование, применяемое при контроле.
2. Документ «Операционная система «AlterOS». Формуляр» должен содержать сведения, удостоверяющие гарантии изготовителя, значения основных параметров и характеристик (свойств) ОС, сведения, отражающие техническое состояние ОС «AlterOS», сведения, которые вносят в период его эксплуатации, а также контрольные суммы дистрибутива, скриптов и исполняемых файлов программного обеспечения.
3. Документ «Операционная система «AlterOS». Руководство администратора» должен содержать описание действий по приемке поставленного средства, описание действий по безопасной установке и настройке средства, описание действий по реализации функций безопасности среды функционирования средства.
4. Документ «Операционная система «AlterOS». Руководство оператора» должен содержать описание режимов работы средства, описание принципов безопасной работы средства, описание функций и интерфейсов функций средства, доступных каждой роли пользователей, описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений, описание типов событий безопасности, связанных с доступными пользователю функциями средства, описание действий после сбоев и ошибок эксплуатации средства

## Комплектность

Комплектность поставки ОС «AlterOS» включает в себя:

* Операционная система «AlterOS». Формуляр 96636777.58.29.11.001 – 01 30, твердая копия;
* Инсталляционный диск (DVD1) с операционной системой «AlterOS» для аппаратных платформ архитектуры x86\_64, децимальный номер 96636777.58.29.11.001;
* Инсталляционный диск (DVD2) с операционной системой «AlterOS» для аппаратных платформ архитектуры i686, децимальный номер 96636777.58.29.11.001;
* Диск с эксплуатационной документацией на операционную систему «AlterOS», скриптами базовых конфигураций (Remote\_admin.sh, arm\_gos.sh) и скриптом rpmverify.pl (DVD3);
* Заверенная копия сертификата соответствия ФСТЭК России, твердая копия;
* Диск с обновлениями операционной системы «AlterOS» для аппаратных платформ архитектуры x86\_64/i686, децимальный номер 96636777.58.29.11.001 (DVD4).

## Требования к носителям данных

Носители данных не должны иметь деформаций, механических или иных повреждений и должны читаться без сбоев.

Информация, записанная на носителе данных, должна соответствовать эталону, хранящемуся на предприятии-изготовителе.

## Упаковка и маркировка

Упаковка должна обеспечивать защиту от внешних воздействий и сохранность
ОС «AlterOS» при хранении и транспортировке.

Упаковка должна содержать следующие данные:

1. децимальный номер (серийный номер);
2. наименование предприятия-изготовителя и его адрес;
3. наименование или условное обозначение ОС;
4. дату изготовления.

В качестве носителей информации при производстве продукции используются оптические DVD диски.

Общие требования к компакт-дискам установлены стандартами ГОСТ 27667-88 и ГОСТ 28376-89.

На маркировке диска указываются:

1. товарный знак или наименование предприятия-изготовителя;
2. наименование и условное обозначение изделия.

Знаком соответствия Системы сертификации средств защиты информации
по требованиям безопасности информации №РОСС RU.0001.01БИ00 должен маркироваться Формуляр. В Формуляре обязательно указывается номер знака соответствия.

Маркировка должна сохраняться в течение всего срока службы программного обеспечения во всех режимах и условиях, установленных данными техническими условиями. Поскольку качество клеящего слоя голографической наклейки не дает гарантии, что она удержится на диске в процессе его эксплуатации, то она вклеивается в Формуляр.

1. Правила приемки

## Приемо-сдаточные испытания

Приемо-сдаточные испытания проводит отдел технического контроля силами и средствами предприятия-изготовителя путем проверки каждого изделия в объеме и последовательности, приведенных в Таблице 3, на соответствие требованиям, указанным в настоящих ТУ.

Таблица 3 – Виды испытаний и проверок

|  |  |  |
| --- | --- | --- |
| Виды испытаний и проверки | Категория испытаний | Номер пункта |
|  | Приемо-сдаточные | Технические требования | Методы контроля |
| 1. Проверка документации
 | + | 2.3 | 4.2 |
| 1. Проверка комплектности
 | + | 2.4 | 4.2 |
| 1. Проверка дистрибутивных носителей
 | + | 2.5 | 4.2 |
| 1. Проверка соответствия дистрибутивных носителей эталону
 | + | 2.5 | 4.2 |
| 1. Проверка маркировки и упаковки программного комплекса
 | + | 2.6 | 4.2 |

Результаты испытаний считают положительными, а ОС выдержавшей испытания, если она испытана в полном объеме в последовательности, которая установлена в настоящих ТУ, и соответствует всем требованиям настоящих ТУ.

Если в процессе испытаний ОС будет выявлено несоответствие хотя бы по одному требованию настоящих ТУ, то проверяемую ОС считают не выдержавшей испытания и возвращают производителю для выявления причин дефектов, а также для проведения мероприятий по их устранению и повторного предъявления.

Принятыми считаются ОС, которые выдержали приемо-сдаточные испытания, укомплектованы, проштампованы клеймами ОТК. Принятые ОС подлежат сдаче на ответственное хранение предприятию-изготовителю.

## Типовые испытания

Типовые испытания проводятся изготовителем после внесения изменений в программы, данные или документацию на ОС «AlterOS».

Типовые испытания проводят на доработанной ОС по программе и методике регрессионных испытаний для верификации (валидации) того, что характеристики доработанной ОС не ухудшились вследствие какого-либо изменения.

Перед испытаниями ОС «AlterOS» проверяют помещение для испытаний, исправность аппаратуры и оборудования для испытаний.

Все испытания ОС «AlterOS» проводят в нормальных климатических условиях: температура окружающего воздуха от +15 до +35 °C, относительная влажность окружающего воздуха не более 75%, атмосферное давление от 84 до 107 кПа (от 630 до 800 мм рт. ст.).

Испытания ОС «AlterOS» должны проводиться до полного их завершения вне зависимости от результатов промежуточных испытаний.

Испытания могут быть прерваны или прекращены по следующим основаниям:

* 1. несоответствие ОС документации на неё;
	2. выхода из строя испытательного стенда.

При положительных результатах типовых испытаний ОС, изготовленных по измененной документации, их предъявляют на приемо-сдаточные испытания в установленном порядке.

При отрицательных результатах типовых испытаний предлагаемые изменения в ОС или технологию его изготовления не вносят.

Результаты типовых испытаний оформляют актом.

По результатам типовых испытаний могут быть даны рекомендации:

* 1. об изменении порядка поставки;
	2. об изменении документации на ОС «AlterOS»;
	3. о применении дополнительных мер по защите;
	4. другие предложения согласно требованиям применимых нормативных документов.

## Периодические испытания

Периодические испытания проводит предприятие-изготовитель для периодической проверки соответствия ОС всем требованиям, указанным в настоящих технических условиях, контроля стабильности технологического процесса производства ОС «AlterOS», подтверждения возможности продолжения ее изготовления по действующей конструкторской и технологической документации и приемки.

Периодические испытания проводят на экземпляре ОС «AlterOS», прошедшем приемо-сдаточные испытания. Периодические испытания проводят в соответствии с годовым графиком, не реже одного раза в год.

Программа периодических испытаний приведена в Таблице 4.

Таблица 4 – Программа периодических испытаний

|  |  |  |
| --- | --- | --- |
| Виды испытаний и проверки | Категория испытаний | Номер пункта |
|  | Периодические | Технические требования | Методы контроля |
| 1. Проверка соответствия ОС «AlterOS» функциональным требованиям безопасности
 | + | 2.1 | 4.1 |
| 1. Проверка качества документации
 | + | 2.3 | 4.2 |
| 1. Проверка комплектности программного комплекса на соответствие заявке
 | + | 2.4 | 4.2 |
| 1. Проверка качества дистрибутивных носителей
 | + | 2.5 | 4.2 |
| 1. Проверка соответствия дистрибутивных носителей эталону
 | + | 2.5 | 4.2 |
| 1. Проверка маркировки и упаковки программного комплекса
 | + | 2.6 | 4.2 |

Результаты испытаний считают положительными, а ОС выдержавшей испытания, если она испытана в полном объеме в последовательности, которая установлена в настоящих ТУ, и соответствует всем требованиям настоящих ТУ.

1. Методы контроля

## Общие требования

При проведении испытаний необходимо убедиться в работоспособности средств вычислительной техники, на которой будут проводиться испытания, с помощью тестов, поставляемых предприятиями-изготовителями этих технических средств. Кроме того, следует убедиться, что условия эксплуатации этих технических средств соответствуют техническим условиям или стандартам на них.

Перед проверкой соответствия ОС «AlterOS» функциональным требованиям безопасности, необходимо выполнить установку на испытательный стенд и настройку
ОС «AlterOS» в соответствии с описанием стенда, приведенном в документе «Операционная система «AlterOS». Тестовая документация. 96636777.58.29.11.001-01 51» и документом «Операционная система «AlterOS» Руководство администратора. 96636777.58.29.11.001 – 01 91». Для проверки функциональных требований безопасности необходимо выполнить тесты функций безопасности, приведенные в документе «Операционная система «AlterOS». Тестовая документация. 96636777.58.29.11.001-01 51».

## Проверка соответствия техническим требованиям

Проверка комплектности производится сравнением комплектности предъявленного образца к приемке с составом, указанным в ТУ.

ОС «AlterOS» соответствует требованиям ТУ, если комплектность предъявленного образца соответствует указанной в ТУ.

Проверка качества носителей состоит в визуальном определении отсутствия каких-либо механических или иных повреждений, в определении качества записи ОС «AlterOS» на носителе данных путем снятия контрольных сумм и сравнения их с эталоном.

Носители считаются выдержавшими испытания, если на них не обнаружено никаких повреждений и информация, записанная на оптический носитель, соответствует эталону.

Проверка документации в печатном виде на ОС согласно п. 2.3 (по составу, содержанию, качеству) производится путем визуального сравнения предъявленного комплекта с учтенными копиями, анализа наличия и целостности документов, оценки подписей.

ЭД на ОС «AlterOS» соответствует требованиям ТУ, если ЭД не содержит дефектов, затрудняющих чтение.

Проверка ЭД, поставляемой на диске вместе с дистрибутивным комплектом, осуществляется путем проверки соответствия дистрибутивного носителя эталону.

Проверка соответствия дистрибутивных носителей эталону производится путем сравнения контрольных сумм образца ОС, рассчитанных с использованием программы
«ФИКС-UNIX 1.0» (версия 1.0, сертификат соответствия ФСТЭК России № 680 от 30 октября 2002 г.) по алгоритму «Уровень 3, программно», с контрольными суммами, приведенными в Формуляре на изделие.

Проверка соответствия ОС требованиям к упаковке и маркировке производится путем оценки соответствия коробок и дисков, а также маркировки, нанесенной на них. ОС считается выдержавшей испытания, если она упакована, а маркировка соответствует требованиям
п. 2.6 настоящих ТУ.

1. Транспортирование и хранение

ОС должна транспортироваться в таре предприятия-изготовителя.

ОС в транспортной таре может транспортироваться автомобильным, железнодорожным, водным и авиационным (в герметизированных отсеках) видами транспорта на любое расстояние при условии защиты от грязи, атмосферных осадков.

Транспортирование должно осуществляться при температуре окружающего воздуха от минус 5 до плюс 50 ˚С и относительной влажности воздуха не более 80% при плюс 35 ˚С.

Хранение допускается только в закрытых помещениях в упакованном виде при температуре от плюс 15 до 35 ˚С и относительной влажности воздуха не более 75% при плюс 35 ˚С.

Условия транспортирования и хранения должны исключать резкие изменения температуры и влажности окружающего воздуха.

ОС должна храниться не более 3 лет.

Если ОС «AlterOS» при транспортировании или хранении подверглась резким изменениям климатических условий, ее необходимо выдержать не менее 2 ч при условиях хранения.

Нельзя касаться руками информационной поверхности компакт-дисков ОС «AlterOS».

ОС необходимо предохранять от воздействия прямого солнечного света. ОС должна храниться вдали от нагревательных приборов.

1. Указания по эксплуатации

## Общие указания

При эксплуатации программного обеспечения на объектах информатизации необходимо выполнить следующие организационно-технические мероприятия по защите информации:

1. Изделие должно использоваться только на совместимых с ним аппаратных средствах;
2. Установка, конфигурирование и управление ОС должно осуществляться в соответствии с эксплуатационной документацией;
3. Должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности средств вычислительной техники, на которых функционирует Изделие;
4. Должна быть обеспечена доверенная загрузка Изделия (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды);
5. Должны быть обеспечены необходимые ресурсы для выполнения функциональных возможностей безопасности Изделия, хранения резервных копий, создаваемых Изделием, а также защищенное хранение данных ОС и защищаемой информации;
6. Должно быть обеспечено ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации;
7. Должен обеспечиваться доверенный маршрут между Изделием и пользователями (администраторами, пользователями);
8. Должен обеспечиваться доверенный канал передачи данных между Изделием и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;
9. Должна быть обеспечена невозможность отключения (обхода) компонентов ОС;
10. Должны быть реализованы меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители информации (или за пределы информационной системы). В том числе должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации;
11. Должна осуществляться проверка целостности внешних модулей уровня ядра, перед их установкой в операционную систему;
12. Должно быть обеспечено выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;
13. Персонал, ответственный за функционирование ОС, должен обеспечивать функционирование ОС, в точности руководствуясь эксплуатационной документацией;
14. Лица, ответственные за эксплуатацию ОС, должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержались в тайне и были недоступны лицам, не уполномоченным использовать данную учетную запись;
15. Должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества;
16. Правом доступа к операционной системе должны обладать только доверенные лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, участвующего в эксплуатации изделия с данными организационно-техническими мероприятиями;
17. Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования данных организационно-технических мероприятий по защите информации;
18. Администратор безопасности должен периодически (не реже одного раза в месяц) проводить контроль целостности компонентов операционной системы с помощью программ контроля целостности;
19. Администратор безопасности должен обеспечить антивирусную защиту системы
с помощью средств антивирусной защиты, сертифицированных в Системе сертификации средств защиты информации по требованиям безопасности информации
№ РОСС RU.0001.01БИ00, согласно Мерам защиты информации в государственных информационных системах;
20. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности операционной системы работа должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации – владельца сети и организации-абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения;
21. Не допускается оставлять без контроля вычислительные средства при включенном питании и загруженной операционной системе. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;
22. Должны быть приняты меры по исключению вхождения пользователей в режим конфигурирования BIOS (например, с использованием парольной защиты);
23. Должна быть исключена возможность работы с ОС, если во время начальной загрузки не проходят встроенные тесты.
24. В случае применения шифрования данных на внешних носителях или шифрования информации при передаче ее по каналам связи, выходящим за пределы контролируемой зоны, данные криптографические средства защиты информации должны быть сертифицированы в системе сертификации ФСБ России.
25. ОС должна периодически (раз в месяц) подвергаться анализу контроля защищенности организацией, осуществляющей эксплуатацию, с помощью средств анализа защищенности,
а также открытых источников, содержащих базу уязвимостей, в том числе и с сайта разработчика;
26. Сертифицированный статус ОС сохраняется только при условии установки всех актуальных сертифицированных обновлений;
27. Обязательно установить обновления ОС «AlterOS» с диска с обновлениями ОС «AlterOS» согласно инструкции, представленной в Руководстве администратора.

## Указания по обновлению

 Обновления изделия, если при поставке обновлений не обговорено иное, осуществляются согласно условиям договора о поставке изделия и технического сопровождения в следующих вариантах:

* производится полная деинсталляция текущей версии ОС «AlterOS» с последующей установкой обновленной сертифицированной версии ОС «AlterOS» в полном соответствии с программной документацией;
* производится обновление с использованием сервисов цифровой дистрибуции и обновления репозитория сертифицированного изделия.

**Обновление изделия с комплекта поставки на физических носителях**

1. Производитель обеспечивает формирование нового комплекта поставки изделия.
2. Производитель направляет потребителям извещение об изменениях, содержащее развернутый перечень изменений в изделии, или публикует данное извещение на официальном общедоступном ресурсе.
3. По запросу потребителя производитель направляет в адрес потребителя дистрибутив в новом комплекте, извещения об изменениях эксплуатационной документации изделия в бумажном виде, а также заверенную копию сертификата соответствия СЗИ с внесенными изменениями.
4. Потребитель в соответствии с эксплуатационной документацией на изделие обязан выполнить обновление изделия с использованием, полученного от производителя дистрибутивного комплекта.
5. Потребитель после выполнения обновления обязан делать соответствующую отметку в эксплуатационной документации изделия с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.
6. **При возникновении нештатных ситуаций, сбоев и отказов в процессе установки или обновления изделия, потребитель, выявивший сбой, должен немедленно сообщить о проблеме производителю изделия путем обращения по телефону или другими доступными потребителю средствами связи.**

**Обновление изделия с использованием репозитория**

1. При обновлении и синхронизации уровней иерархического репозитория производитель использует только защищенные, т.е. доверенные каналы передачи данных.
2. Производитель публикует образы дистрибутивных дисков комплекта поставки изделия и бинарные установочные пакеты изделия в репозитории. Образы включают полный поставочный комплект документации на изделие и копию сертификата соответствия.
3. После обновления изделия в репозиториях производитель направляет потребителям извещение об изменениях, содержащее развернутый перечень изменений в изделии. В случае необходимости, по запросу потребителя, производитель дополнительно направляет в адрес потребителя комплект извещений об изменениях эксплуатационной документации изделия в бумажном виде, а также заверенную копию сертификата соответствия СЗИ с внесенными изменениями.
4. Порядок действий по синхронизации репозиториев и обновлению СЗИ описан в эксплуатационной документации на изделие.
5. Потребитель после выполнения обновления обязан делать соответствующую отметку в эксплуатационной документации изделия с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.
6. При возникновении нештатных ситуаций, сбоев и отказов в процессе загрузки, установки или обновления изделия, потребитель, выявивший сбой, должен немедленно сообщить о проблеме производителю изделия путем обращения по телефону или другими доступными потребителю средствами связи.
7. Для проверки того, что скаченный пакет подписан GPG-ключом разработчика необходимо выполнить команду: **rpm -K *<rpm-file>***. Если появляется сообщение «*ok*», значит подпись пакета была проверена, и она не испорчена. Чтобы просмотреть ключ, используемый для проверки, необходимо выполнить команду: **rpm -qa gpg-pubkey\***. Чтобы получить подробную информацию о ключе, необходимо выполнить команду **rpm -qi**, добавив в конце результат предыдущей команды.

**Устранение уязвимостей ОС**

Информирование потребителей о мерах, направленных на нейтрализацию выявленных уязвимостей ОС «AlterOS» и выпускаемых обновлениях ОС «AlterOS», выполняется путем публикации информации на информационном ресурсе предприятия-производителя
(<https://alter-os.ru/>). После проведения необходимых испытаний предприятие-производитель поставляет потребителям обновления ОС «AlterOS» на оптическом диске. При получении обновлений ОС «AlterOS», прошедших необходимые испытания, перед их установкой необходимо проверить целостность полученных файлов. Для инсталляции обновлений администратор безопасности должен выполнить следующие действия:

* провести расчет контрольных сумм файлов обновлений с использованием программы «ФИКС-UNIX 1.0» (версия 1.0, сертификат соответствия ФСТЭК России
№ 680 от 30 октября 2002 г.) по алгоритму «Уровень 3, программно». Сравнить контрольные суммы файлов обновлений с указанными на компакт-диске. При расхождении контрольных сумм с эталонными значениями необходимо обратиться
в службу поддержки производителя;
* произвести инсталляцию актуальных обновлений.

Производитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в изделии на протяжении всего его жизненного цикла, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях, методах безопасного использования изделия.

Производитель периодически, не реже одного раза в месяц, должен проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должны использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:

* https://cve.mitre.org/,
* https://nvd.nist.gov/,
* https://www.exploit-db.com/,
* http://www.rapid7.com/db/,
* http://www.cvedetails.com/,
* http://www.securitylab.ru/ и другие.

Процедура устранения уязвимостей ОС «AlterOS» должна обеспечивать возможность обновления ПО для устранения актуальных уязвимостей.

При анализе уязвимостей необходимо учитывать следующие критерии:

* тип ошибки;
* версию программного обеспечения, подверженную уязвимости;
* уровни опасности уязвимости (критическая, высокая, средняя, низкая);
* информацию об устранении.

В случае выявления информации об уязвимости ОС «AlterOS» и сред его функционирования из различных источников и отсутствия информации об этой уязвимости в БДУ (базе данных уязвимостей), производитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

При выявлении уязвимостей ОС «AlterOS» производитель должен осуществить следующие мероприятия:

* исправление уязвимости ОС «AlterOS»;
* разместить информационное сообщение об уязвимостях ОС «AlterOS» на специализированном разделе своего сайта (<https://alter-os.ru/>);
* довести информацию до конечных потребителей ОС «AlterOS» об организационно-технических мерах по устранению уязвимостей ОС «AlterOS»;
* производитель оповещает пользователей ОС «AlterOS» о необходимости установки обновленной версии ОС «AlterOS»;
* производитель обеспечивает гарантированную доставку конечным пользователям файла с обновленной версией ОС «AlterOS»;
* конечные пользователи обновляют ОС «AlterOS» с соответствующими отметками в разделах Формуляра;
* информацию об изменении версии ОС «AlterOS» производитель заносит в извещение об изменениях на СЗИ, и представляет его в Испытательную лабораторию, ФСТЭК России и доводит до сведения конечных потребителей ОС «AlterOS»;
* производитель обязан провести испытания ОС «AlterOS» в связи с внесением в него изменений (с привлечением испытательной лаборатории в случае внесения в сертифицированное средство защиты информации изменений, связанных с добавлением новых функций безопасности информации, или изменений в имеющиеся функции безопасности информации);
* в случае отсутствия, на момент проверки информации по выявленным уязвимостям
ОС «AlterOS», доступных релизов ОС «AlterOS» с устраненными уязвимостями, производитель должен разработать перечень (регламент) организационно–технических мероприятий, направленных на исключение возможности эксплуатации выявленной уязвимости злоумышленниками;
* производитель предоставляет конечному пользователю ОС «AlterOS» инструкцию по проведению организационно–технических мероприятий, направленных на исключение возможности эксплуатации выявленной уязвимости злоумышленниками в соответствующем разделе сайта производителя;
* в случае невозможности устранения уязвимостей ОС «AlterOS», в том числе путем применения обновления, производитель разрабатывает ограничения по применению ОС «AlterOS», которые незамедлительно доводит до испытательной лаборатории;
* если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, производитель незамедлительно и гарантированно с подтверждением доводит его до пользователей;
* производитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории
в ФСТЭК России. Пользователи реализуют указанное ограничение по применению
ОС «AlterOS»;
* если пользователь не может реализовать ограничение по применению ОС «AlterOS»,
он прекращает его применение;
* если уязвимость не устраняется путем установления ограничений по применению, производитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение ОС «AlterOS».
1. Гарантии изготовителя

Гарантийный срок эксплуатации ОС «AlterOS» – 3 года со дня передачи его потребителю (пользователю), включая срок хранения, с периодической перепроверкой дистрибутивного комплекта один раз в год на объекте эксплуатации.

Гарантийные обязательства предприятия-изготовителя ОС «AlterOS»
НЕ РАСПРОСТРАНЯЮТСЯ на его копии, изготовленные по инициативе потребителя (пользователя), без оформления соответствующих лицензионных документов порядком, согласованным с предприятием-разработчиком.

# Приложение А

(обязательное)

В документе использовались следующие нормативные документы:

1. Методический документ «Профиль защиты операционных систем типа «А» четвертого класса защиты ИТ.ОС.А4.ПЗ», ФСТЭК России, 2017.
2. РД «Защита от несанкционированного доступа к информации. Термины и определения». Гостехкомиссия России, 1992.
3. Сборник «Информационная безопасность и защита информации. Сборник терминов и определений». Гостехкомиссия России, 2001.
4. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
5. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
6. ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».
7. ГОСТ 28806-90 «Качество программных средств. Термины и определения».
8. ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению».
9. ГОСТ 2.114-2016 «Единая система конструкторской документации. Технические условия».
10. ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы».

**96636777.58.29.11.001 ТУ**

1. Подробное описание функциональных требований безопасности приведено в документе «Операционная система «AlterOS». Задание по безопасности 96636777.58.29.11.001 ЗБ» [↑](#footnote-ref-1)