УТВЕРЖДЕН
КШДС.10514-01 31 01-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА

«АЛЬТ ЛИНУКС СПТ 7.0»

Описание применения

КШДС.10514-01 31 01

Книга № 3

Листов 37

2016

Литера

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

АННОТАЦИЯ

Настоящий документ представляет собой описание применения программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01.

Описание применения программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01 выполнено в соответствии с ГОСТ 19.502-78 и состоит из четырех разделов, в которых приведены сведения о ее функциональном назначении, дано описание области применения и описание задач, выполняемых операционной системой, а также методов их решения. Также перечислены требования к техническим средствам, необходимым для функционирования операционной системы, сведения о входных и выходных данных.

В первом разделе приведены назначение и возможности программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01, ее основные характеристики, а также ограничения, накладываемые на область ее применения.

Во втором разделе приведены требования к техническим и программным средствам, необходимым для функционирования программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01, приведены общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера.

В третьем разделе приведены определение задач программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01 и методы их решения.

В четвертом разделе указаны общие сведения о входных и выходных данных программного изделия «Операционная система «Альт Линукс СПТ 7.0» КШДС.10514-01.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

Программное изделие «Операционная система «Альт Линукс СПТ 7.0» (далее – ОС «Альт Линукс») предназначено для построения автоматизированных систем в рамках группового и корпоративного использования с целью автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений).

1.2. Функциональные возможности

ОС «Альт Линукс» обеспечивает выполнение следующих функций:

–управление процессами и информационными ресурсами;

–управление системными ресурсами;

–управление внешними устройствами;

–защита хранимых, обрабатываемых и передаваемых информационных ресурсов комплексом средств защиты (далее – КСЗ) операционной системы (далее – ОС);

–администрирование;

–поддержка пользовательского интерфейса;

–поддержка интерфейса прикладного программирования.

1.3. Основные характеристики

ОС «Альт Линукс» представляет собой совокупность интегрированных программных продуктов, созданных на основе ОС «Linux», и обеспечивает обработку, хранение и передачу информации в защищенной программной среде в круглосуточном режиме эксплуатации.

В состав ОС «Альт Линукс» входят следующие компоненты:

–«Ядро системы»;

–«Программа идентификации и аутентификации пользователей»;

–«Программа контроля целостности и восстановления»;

–«Программа взаимодействия с внешними устройствами»;

–«Программа регистрации и учета событий».

В структуре компонентов ОС «Альт Линукс» выделяются следующие функциональные элементы:

1) ядро ОС – программа (набор программ), выполняющая функции управления ОС и взаимодействия ОС с аппаратными средствами, а также решающая внутрисистемные задачи организации вычислительного процесса, такие как переключение контекста, управление памятью, обработка прерываний;

2) системные и сервисные приложения – компоненты, реализующие дополнительные функции ОС, всевозможные служебные программы, или утилиты.

В состав ядра ОС «Альт Линукс» входят следующие элементы:

–компоненты и модули ядра;

–КСЗ ядра – специальные пакеты программ, входящие в состав ядра ОС и системных библиотек, предназначенные для защиты ОС «Альт Линукс» от несанкционированного доступа к обрабатываемой (хранящейся) информации на персональной электронной вычислительной машине (далее – ПЭВМ).

В состав системных приложений ОС «Альт Линукс» входят следующие элементы:

1) системные библиотеки ОС – наборы программ (пакетов программ), решающих различные задачи и предназначенных для динамического подключения к работающим приложениям, которым необходимо выполнение этих задач;

3) КСЗ – специальные программные пакеты, входящие, в том числе, в состав ядра ОС и системных библиотек, предназначенные для защиты ОС от несанкционированного доступа к обрабатываемой (хранящейся) информации на ПЭВМ;

Примечание. Программные пакеты КСЗ, входящие в состав системных библиотек и ядра ОС, являются их неотъемлемой частью.

4) программные серверы – специальные приложения, предоставляющие пользователю специализированные услуги (почтовые службы, хранилище файлов, веб-сервер, система управления базой данных, обеспечение документооборота, хранилище данных пользователей и так далее) в локальной или глобальной сети и обеспечивающие их выполнение;

5) веб-серверы – программы, участвующие в организации доступа пользователей к сети Интернет с помощью клиент-серверной архитектуры. В состав ОС «Альт Линукс» включены программы веб-сервера Apache версии 2.2;

6) системы управления базами данных (далее – СУБД) – приложения, предназначенные для работы с данными, представленными в виде набора записей. СУБД осуществляет поиск, обработку и хранение данных в виде специальных таблиц, являющихся базой данных;

7) прочие серверные программы – программы, предоставляющие пользователю различные услуги по обработке, передаче, хранению информации: серверы протоколов, почтовые серверы, серверы приложений, серверы печати и прочие;

8) интерактивные рабочие среды – программы (пакеты программ), предназначенные для работы пользователя в ОС и предоставляющие ему удобный интерфейс для общения с ней;

9) командные интерпретаторы – специальные программы (терминалы), предназначенные для выполнения различных команд пользователей при работе с ОС;

10) графическая оболочка MATE (аналог рабочего стола ОС «Windows») – набор программ и технологий, предназначенных для управления ОС и предоставляющих пользователю графический интерфейс для работы;

11) прочие системные приложения – приложения (программы), оказывающие пользователю дополнительные системные услуги при работе с ОС (архиваторы, приложения для управления RPM-пакетами, приложения резервного копирования, приложения мониторинга системы, приложения для работы с файлами, приложения для настройки системы и другие);

12) электронные справочники – наборы внутрисистемных справочных страниц, описывающих работу команд и приложений, которые выполнены в виде примеров HOWTOs и справки man.

ОС «Альт Линукс» обладает следующими функциональными характеристиками:

–обеспечивает возможность обработки, хранения и передачи информации в защищенной программной среде;

–обеспечивается возможность запуска пользовательского программного обеспечения в сертифицированном окружении;

–обеспечивается возможность запуска пользовательского программного обеспечения в сертифицированном окружении;

–обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);

–обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;

–обеспечивает многопользовательский режим эксплуатации;

–обеспечивает поддержку мультипроцессорных систем;

–обеспечивает поддержку виртуальной памяти;

–обеспечивает поддержку запуска виртуальных машин;

–обеспечивает сетевую обработку данных.

ОС «Альт Линукс» 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.

КСЗ предназначен для выполнения функций защиты информации в объеме требований класса защищенности 4 в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) (далее – РД НСД) при соблюдении условий и указаний по эксплуатации в документе «Операционная система «Альт Линукс СПТ 7.0». Формуляр» КШДС.10514-01 30 01.

КСЗ соответствует требованиям уровня 3 контроля отсутствия недекларированных возможностей в соответствии с руководящим документом «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999 г.) (далее – РД НДВ).

1.4. Ограничения, накладываемые на область применения

При соблюдении условий и указаний по эксплуатации, ОС «Альт Линукс» может использоваться при проектировании и построении автоматизированных систем до класса защищенности «1В» включительно, за исключением случаев, когда обработка информации производится с использованием системы виртуализации.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к техническим средствам

Для функционирования ОС «Альт Линукс» требуется ПЭВМ, обладающая следующими минимально необходимыми характеристиками:

–аппаратная платформа – ПЭВМ типа IBM PC;

–процессоры архитектур x86-64, i586 (Intel или совместимый с ним процессор, включая AMD, при этом для версии ОС i586 процессор должен поддерживать технологию PAE);

–оперативная память – не менее 512 МБ (рекомендуется 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 и условия организационного и технологического характера

К пользователю ОС «Альт Линукс» предъявляется следующее требование: базовые навыки работы с ОС семейства «Linux».

К администратору ОС «Альт Линукс» предъявляются следующие требования:

–знание принципов построения и функционирования современных вычислительных систем, механизмов защиты информации;

–навыки работы с ОС семейства «Linux»;

–навыки администрирования общесистемного и прикладного программного обеспечения;

–навыки настройки средств защиты, используемых в составе ОС «Альт Линукс».

2.3. Ограничения на использование технического и программного характера

2.3.1. Ограничения на использование аппаратных платформ и базовых систем ввода-вывода

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.

2.3.2. Ограничения на действия при обнаружении уязвимостей

В случае обнаружения уязвимостей в программных модулях ОС «Альт Линукс» необходимо устранить уязвимость 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.

2.3.3. Ограничения, накладываемые на использование механизмов КСЗ

Ограничения, накладываемые на использование механизмов КСЗ с целью соответствия требованиями класса защищенности 4 в соответствии с РД НСД и требованиям уровня контроля 3 отсутствия недекларированных возможностей в соответствии с РД НДВ, приведены в документе «Операционная система «Альт Линукс СПТ 7.0». Руководство по КСЗ. Часть 2» КШДС.10514-01 97 01-2.

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Определение задачи

ОС «Альт Линукс» решает следующие основные задачи:

–организация дискреционного принципа контроля доступа к информации;

–организация мандатного принципа контроля доступа к информации;

–идентификация и аутентификация субъектов;

–разграничение доступа к сетевому взаимодействию и сбор статистики;

–сопоставление пользователя с устройством;

–контроль создания и удаления процессов;

–контроль распределения системных ресурсов;

–изоляция программных модулей процессов в пределах оперативной памяти ПЭВМ;

–синхронизация процессов;

–распределение оперативной памяти между прикладными задачами;

–очистка (обнуление) освобождаемых областей оперативной памяти ПЭВМ;

–доступ к периферийным устройствам;

–защита ввода и вывода на отчуждаемый физический носитель информации;

–буферизация данных;

–маркировка документов, выводимых на печать;

–взаимодействие с управляющими программами аппаратных средств;

–регистрация и журналирование событий, в том числе – событий безопасности;

–контроль целостности программных средств, КСЗ и обрабатываемой информации;

–обеспечение защиты от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

–осуществление контроля доступа субъектов доступа к средствам конфигурирования виртуальных машин (virt-manager, virsh, virt-install);

–предоставление возможности применения индивидуальных прав доступа субъектов виртуальной инфраструктуры к объектам;

–обеспечение контроля доступа субъектов доступа к файлам-образам, используемым для обеспечения работы виртуальных машин;

–обеспечение контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы и гипервизора;

–обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры;

–осуществление идентификации и аутентификации субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры (в т. ч. к средствам конфигурирования виртуальных машин);

–обеспечение блокирования доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

–обеспечение регистрации 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.

–осуществление контроля целостности компонентов, критически важных для функционирования гипервизора и виртуальных машин.

3.2. Методы решения

Для решения поставленных задач в ОС «Альт Линукс» логически выделены следующие системы:

1) система управления процессами, в состав которой входят следующие средства:
–службы контроля создания и удаления процессов,
–службы синхронизации процессов,
–службы контроля распределения системных ресурсов,
–подсистема межпроцессорного взаимодействия;
13) система управления памятью;
14) система работы с файлами;
15) система ввода-вывода, в состав которой входят следующие средства:
–службы буферизации данных,
–службы доступа к периферийным устройствам,
–службы взаимодействия с управляющими программами аппаратных средств,
–службы управления печатью;
16) система администрирования;
17) КСЗ, в состав которого входят следующие средства:
–службы идентификации и аутентификации субъектов доступа,
–службы управления потоками информации,
–службы регистрации событий,
–службы обеспечение целостности программных средств и обрабатываемой информации,
–средства восстановления.

3.2.1. Система управления памятью

Система управления памятью обеспечивает выполнение функций распределения оперативной памяти между прикладными задачами.

Оперативная память в ОС «Альт Линукс» имеет страничную организацию, в основе которой лежит принцип деления виртуального адресного пространства на части (страницы). Страницы всегда имеют фиксированный размер. Передача данных между оперативной памятью и дисковым накопителем всегда осуществляется в страницах.

В качестве схемы управления памятью в ОС «Альт Линукс» используется виртуальная память. В связи с этим процесс ОС «Альт Линукс» работает с виртуальными адресами, а не с физическими. Преобразование происходит посредством вычислений, используя таблицы дескрипторов и каталоги таблиц. ОС «Альт Линукс» поддерживает три уровня таблиц:

–каталог таблиц первого уровня PGD (Page Table Directory, PGD);
–каталог таблиц второго уровня PMD (Medium Page Table Directory, PMD);

–таблица дескрипторов PTE (Page Table Entry, PTE).

Преобразование виртуального адреса в физический осуществляется в три этапа:

1) указатель PGD, имеющийся в структуре описывающий каждый процесс, преобразуется в указатель записи PMD;

18) указатель записи PMD преобразуется в указатель в таблице дескрипторов PTE;

19) к реальному адресу, указывающему на начало страницы прибавляется смещение от ее начала.

Все данные об используемой процессом памяти хранятся ядром ОС в специальных структурах. На уровне процесса работа может вестись как со страницами напрямую, так и через специальные структуры ядра.

При открытии файла выполняется его отображение в память и добавление в страничный кэш. Реальный же запрос на отображение файла только возвращает адрес на уже кэшированные страницы.

3.2.2. Система управления процессами

Система управления процессами ОС «Альт Линукс» обеспечивает выполнение следующих функций:

1) управление процессами:
   –создание процессов,
   –управление процессов,
   –удаление процессов,
   –планирование процессорного времени;
2) распределение системных ресурсов;
3) синхронизация процессов и организация межпроцессного взаимодействия:
   –сокеты,
   –сигналы,
   –каналы,
   –очереди сообщений,
   –семафоры,
   –разделяемая память.

3.2.2.1. Управление процессами

Процессом в ОС «Альт Линукс» называется любая выполняющаяся программа. ОС «Альт Линукс» как многозадачная система характеризуется тем, что одновременно может выполняться множество процессов, принадлежащих одному или несколькими пользователями.

Одновременно в оперативной памяти может находиться несколько процессов, при этом каждому работающему процессу система присваивает уникальный PID (process identificator). Каждый процесс выполняется в собственном виртуальном адресном пространстве.

ОС «Альт Линукс» управляет образом процесса в оперативной памяти или сегментами кода и данных, определяющих среду выполнения. Сегмент кода, в свою очередь, содержит реальные инструкции центральному процессору. Данные, связанные с процессом, также

являются частью образа процесса, и хранятся в регистрах. Для оперативного хранения рабочих данных существует область памяти, выделяемая динамически, и способы ее использования меняются от процесса к процессу.

Процессы разделяются на функционирующие на уровне ядра операционной системы (kernel-space) и функционирующие вне ядра операционной системы (user-space). Процессы, функционирующие на уровне ядра, запускаются самим ядром ОС, либо в виде подгружаемых модулей ядра. Процессы, функционирующие в системном окружении, запускаются стандартным для приложений ОС «Альт Линукс» методом.

3.2.2.1.1. Создание процесса

Процесс порождается с помощью системного вызова. При создании нового процесса выполняется следующее:

1) выделяется память для описателя нового процесса в таблице процессов;
20) назначается уникальный идентификатор процесса PID;
21) создается логическая копия процесса, который выполняет полное копирование содержимого виртуальной памяти родительского процесса, копирование составляющих ядерного статического и динамического контекстов процесса-предка;
22) увеличиваются счетчики открытия файлов (порожденный процесс наследует все открытые файлы родительского процесса);
23) возвращается идентификатор процесса PID в точку возврата из системного вызова в родительском процессе и 0 – в процессе-потомке.

При порождении процесса, для него создается свой блок управления, который помещается в системную таблицу процессов, находящихся в ядре ОС. Эта таблица представляет собой массив структур блоков управления процессами.

В каждом блоке содержатся следующие данные, отслеживаемые ядром ОС:

–слово состояния процесса;
–приоритет;
–величина кванта времени, выделенного системным планировщиком;
–степень использования системным процессором;
–признак диспетчеризации;
–идентификатор пользователя, которому принадлежит процесс;
–эффективный идентификатор пользователя;
–реальный и эффективный идентификаторы группы;
–группа процесса;
–идентификатор процесса и идентификатор родительского процесса;
–размер образа, размещаемого в области подкачки;
–размер сегментов кода и данных;
–массив сигналов, ожидающих обработки.

3.2.2.1.2. Управление процессом

Для управления процессами ОС «Альт Линукс» использует два основных типа информационных структур:

–дескриптор процесса – содержит информацию о состоянии процесса, расположении образа процесса в оперативной памяти и на диске, о значении отдельных составляющих приоритета, а также его итоговое значение – глобальный приоритет, идентификатор пользователя, создавшего процесс, информация о родственных процессах, о событиях, осуществления которых ожидает данный процесс и другую информацию;

–контекст процесса – содержит информацию о процессе, необходимую для возобновления выполнения процесса с прерванного места: содержимое регистров процессора, коды ошибок выполняемых процессором системных вызовов, информацию обо всех открытых данным процессом файлов и незавершенных операциях ввода-вывода и другие данные, характеризующие состояние вычислительной среды в момент прерывания.

3.2.2.1.3. Завершение процесса

Завершение процесса выполняется с помощью системного вызова, при котором освобождаются все используемые ресурсы, такие как память и структуры таблиц ядра. Кроме того, завершаются и дочерние процессы, порожденные данным процессом. Затем из памяти удаляются сегменты кода и данных, после этого родительский процесс очищает все ресурсы, занимаемые дочерними процессами.

3.2.2.1.4. Планирование

В ОС «Альт Линукс» реализована вытесняющая многозадачность, основанная на использовании приоритетов и квантования.

Все процессы разбиты на несколько групп, называемых классами приоритетов. Каждая группа имеет свои характеристики планирования процессов.

Дочерний процесс наследует характеристики планирования родительского процесса, которые включают класс приоритета и величину приоритета в этом классе. Процесс остается в данном классе до тех пор, пока не будет выполнен системный вызов, изменяющий его класс. Существует три приоритетных класса приоритетов: класс реального времени, класс системных процессов и класс процессов разделения времени. Приоритетность процесса тем выше, чем больше число, выражающее приоритет.

Процессы системного класса используют стратегию фиксированных приоритетов. Системный класс зарезервирован для процессов ядра. Уровень приоритета процессу назначается ядром и никогда не изменяется.

Процессы реального времени также используют стратегию фиксированных приоритетов, но пользователь может их изменять. При наличии готовых к выполнению процессов реального времени другие процессы не рассматриваются.

Характеристики планирования процессов реального времени включают две величины: уровень глобального приоритета и квант времени. Для каждого уровня приоритета устанавливается по умолчанию своя величина кванта времени. Процессу разрешается использовать ресурсы процессора в течение указанного кванта времени, по истечении которого планировщик снимает данный процесс с выполнения.

В классе процессов разделения времени для распределения времени процессора между процессами используется стратегия динамических приоритетов, которая адаптируется к операционным характеристикам процесса.

Величина приоритета, назначаемого процессам разделения времени, вычисляется пропорционально значениям двух составляющих: пользовательской части и системной части. Пользовательская часть приоритета может быть изменена суперпользователем root и владельцем процесса, но в последнем случае только в сторону его снижения.

Системная составляющая позволяет планировщику управлять процессами в зависимости от длительности использования ими ресурсов процессора, не уходя в состояние ожидания.

3.2.2.2. Распределение системных ресурсов

Для запуска процесса, выполняемого в ОС «Альт Линукс», необходимы системные ресурсы, такие как память, порты ввода-вывода, память ввода-вывода, линии прерывания, а также каналы памяти прямого обращения DMA (Direct Access Memory).

Система управления ресурсами, реализованная в ОС «Альт Линукс», может управлять произвольными ресурсами, объединяя их в иерархическую структуру. Глобальные ресурсы системы (например, порты ввода-вывода) могут быть разделены на подмножества – например, относящиеся к какому-либо слоту аппаратной шины. Определенные драйверы, также, при желании, могут подразделять захватываемые ресурсы на основе своей логической структуры.

Область памяти, принадлежащая периферийному устройству, называется памятью ввода-вывода, чтение и запись портов и памяти ввода-вывода – работа драйвера. Порты и память ввода-вывода объединены общим названием – регион (или область) ввода-вывода.

Для предотвращения коллизий между различными устройствами в ОС «Альт Линукс» реализован механизм запроса/высвобождения регионов ввода-вывода (порты и память ввода-вывода). Этот механизм представляет программную абстракцию и не распространяется на аппаратные возможности.

Информация о зарегистрированных ресурсах доступна в текстовой форме и содержится в файлах /proc/ioports и /proc/iomem. Каждая строка данного файла отображает в шестнадцатеричном виде диапазон портов связанных с драйвером или владельцем устройства.

3.2.2.3. Синхронизация процессов и организация межпроцессного взаимодействия

К средствам для организации межпроцессного взаимодействия в ОС «Альт Линукс» относятся: сокеты, сигналы, коммуникационные и именованные каналы, сообщения (очереди сообщений), семафоры и разделяемая память.

3.2.2.3.1. Сокеты

Сокет домена UNIX (Unix domain socket, UDS) или IPC-сокет (сокет межпроцессного взаимодействия) – конечная точка обмена данными между процессами, работающими в одной и той же системе UNIX.

Доменные соединения UNIX являются по сути байтовыми потоками, схожими с сетевыми соединениями, но при этом все данные остаются внутри одного компьютера (то есть обмен данными происходит локально).

UDS используют файловую систему как адресное пространство имен, то есть они представляются процессами как иноды в файловой системе (системой создается специальный файл сокета по заданному пути). Это позволяет двум различным процессам открывать один и тот же сокет для взаимодействия между собой (через файл сокета любые локальные процессы смогут сообщаться путем чтения/записи из него). Однако, конкретное взаимодействие, обмен данными, не использует файловую систему, а только буферы памяти ядра.

Несмотря на то, что другие процессы распознают файлы сокетов как элементы каталога, чтение и запись файлов сокета могут осуществлять только те процессы, между которыми установлено соответствующее соединение.

Взаимодействие, основанное на использовании сокетов, является основным механизмом межсистемной и межпроцессной связи. Сокеты представляют собой программный интерфейс для обеспечения двусторонней связи типа «точка-точка» между двумя процессами. Интерфейс сокетов позволяет явно разделить во взаимодействии двух процессов серверную и клиентскую часть.

Взаимодействие процессов посредством сокетов может быть представлено в общем виде следующим алгоритмом:

–серверный процесс инициализирует сокет и привязывает его к определенному адресу и/или порту, после этого переключает сокет в режим ожидания подключения от клиентского процесса;

–клиентский процесс инициализирует сокет и привязывает его к определенному адресу и/или порту;

–клиентский процесс инициирует подключение к сокету серверного процесса.

После установки соединения информационный обмен между процессами может быть осуществлен в двустороннем направлении.

3.2.2.3.2. Сигналы

ОС «Альт Линукс» также обеспечивает возможность организации межпроцессного взаимодействия с помощью сигналов.

Сигналы представляют собой программные прерывания и позволяют уведомлять процесс или группу процессов о наступлении некоторого события. Когда сигнал послан процессу, ОС прерывает его выполнение. Источником сигнала может выступать как другой процесс, так и сама ОС.

Сигналы, посылаемые ОС, уведомляют о наступлении некоторых строго предопределенных ситуаций (например, завершение дочернего процесса, попытка выполнить недопустимую машинную инструкцию, попытка недопустимой записи в канал и другие), при этом каждому событию сопоставлен свой сигнал. Существуют также зарезервированные номера сигналов, семантика которых определяется пользовательскими процессами по своему усмотрению (например, процессы могут посылать друг другу сигналы с целью синхронизации).

Сигналы являются механизмом асинхронного взаимодействия. При получении сигнала процессом возможны три варианта реакции на полученный сигнал:

–процесс реагирует на сигнал стандартным образом, установленным по умолчанию (для большинства сигналов действие по умолчанию – это завершение процесса);

–процесс может установить специальную обработку сигнала, в этом случае по приходу сигнала вызывается функция-обработчик, определенная процессом;

–процесс может проигнорировать сигнал.

3.2.2.3.3. Каналы

В ОС «Альт Линукс» взаимодействие между процессами осуществляется также с помощью неименованных и именованных каналов. Файлы данного типа подобны сокетам, поскольку тоже используются для взаимодействия между процессами, однако, в отличие от сокетов, в именованных каналах данные передаются только в одном направлении.

Взаимодействие между родительским процессом и дочерним (процесс, порожденный родительским процессом) осуществляется по неименованному каналу, который представляет собой программный однонаправленный канал передачи данных между двумя родственными процессами (родителем и потомком). При необходимости двунаправленного информационного обмена родительский процесс создает два канала. Посторонний субъект вмешаться в обмен данными не может, так как обращение к неименованным каналам осуществляется только через механизм файловых дескрипторов, которые наследуются при порождении нового процесса.

Взаимодействие между независимыми процессами осуществляется по именованному каналу. Именованные каналы являются двунаправленными, что позволяет осуществлять обмен сообщениями между двумя процессами посредством единственного канала. Именованный канал обеспечивает возможность взаимодействия процессов, выполняющихся как на одной, так и на разных ПЭВМ, объединенных в локальную сеть.

Именованный канал создаётся явно с помощью команды mkfifo, и два различных процесса могут обратиться к нему по имени.

3.2.2.3.4. Очереди сообщений

Очередь сообщений представляет собой механизм, позволяющий процессам асинхронно посылать сообщения друг другу. Когда сообщение получено процессом, оно удаляется из очереди. Очередь сообщений существует независимо от процесса-источника и процесса-приемника: процесс-источник может отправить сообщение в очередь и завершиться, а сообщение, тем не менее, будет получено процессом-приемником. Сообщениям могут быть назначены приоритеты. Высокоприоритетные сообщения всегда принимаются первыми, независимо от количества сообщений в очереди.

3.2.2.3.5. Семафоры

Для синхронизации процессов в ОС «Альт Линукс» применяются семафоры. Семафоры используются как блокирующий механизм, позволяющий разграничить доступ параллельно работающих процессов к критическим информационным ресурсами и исключить возможность использования сегмента памяти двумя процессами одновременно.

3.2.2.3.6. Разделяемая память

Разделяемая память используется для того, чтобы увеличить скорость обмена данными между процессами. В большинстве случаев обмен информацией между процессами осуществляется через ядро, в то время как механизм взаимодействия процессов посредством разделяемой памяти позволяет осуществить обмен информацией, используя некоторую часть виртуального адресного пространства, куда помещаются и откуда считываются данные. После добавления разделяемого сегмента памяти к собственному виртуальному пространству пользовательский процесс может работать с ним как с обычным сегментом памяти.

3.2.3. Система работы с файлами

Система работы с файлами ОС «Альт Линукс» обеспечивает возможность работы с файлами, ссылками, каталогами и разделами и поддерживает следующие файловые системы:

1) общий интерфейс к файловым системам VFS (Virtual File System);

24) файловые системы, поддерживающие дискреционный контроль доступа к информации:

–сетевая файловая система NFS (Network File System),

–файловая система ReiserFS;

25) файловые системы, поддерживающие дискреционный и мандатный контроль доступа к информации:

–файловая система ext2 (Second Extended File System),

–файловая система ext3 (Third Extended File System),

–файловая система ext4 (Fourth Extended File System),

–файловая система XFS,

–файловая система JFS (Journaled File System).

ОС «Альт Линукс» позволяет выполнять следующие операции с файлами:

–создание и просмотр файла;

–копирование файла;

–переименование и перемещение файлов;

–удаление файлов;

–поиск файлов;

–изменение прав доступа к файлам.

Примечание. Для каждого файла в ОС «Альт Линукс» устанавливаются права доступа.

Жесткая ссылка представляет собой дополнительное имя для исходного файла и ссылается на номер индексного дескриптора исходного файла, следовательно, такие ссылки могут указывать только на файлы, расположенные в той же файловой системе, что и жесткая ссылка. При изменении файла жесткой ссылки, автоматически изменяется и обычный файл. При удалении жесткой ссылки, файл удаляется только в том случае, если на него нет больше жестких ссылок, в противном случае удаляется только ссылка.

Символическая ссылка представляет собой файл, при обращении к которому ОС обращается к другому файлу. В отличие от жестких ссылок символические ссылки могут указывать на файлы, расположенные в другой файловой системе, например, на монтируемом

носителе, или другом компьютере. В случае, если исходный файл удален, символическая ссылка не удаляется, но становится бесполезной. Символическая ссылка не имеет прав доступа, она наследует права доступа от файла, на который ссылается.

ОС «Альт Линукс» позволяет выполнять следующие операции с каталогами:

–просмотр содержимого каталога;

–вывод имени текущего каталога;

–создание и удаление каталога;

–смена каталога;

–изменение прав доступа к каталогу.

В случае, если дисковый накопитель из состава ПЭВМ разбит на разделы, на каждом разделе организуется отдельная файловая система с собственной структурой каталогов. Для пользователя файловая система представляет собой единое целое. В действительности, разные части файловой системы могут находиться на разных устройствах: разделах дискового накопителя, съемных носителях информации.

ОС «Альт Линукс» позволяет выполнять следующие операции с разделами:

–создание раздела;

–монтирование, размонтирование раздела;

–форматирование раздела;

–проверка файловой системы раздела.

3.2.4. Система ввода-вывода

Система ввода-вывода обеспечивает выполнение следующих функций:

–доступ к внешним устройствам;

–буферизация данных;

–взаимодействие с программами управления внешними устройствами ПЭВМ;

–службы управления печатью.

3.2.4.1. Доступ к внешним устройствам

В ОС «Альт Линукс» доступ к физическому устройству осуществляется с помощью специального файла устройства. При выполнении с файлом устройства операций открытия, чтения или записи осуществляется обмен данными с физическим устройством. Файлы устройств хранятся в каталоге /dev.

В ОС «Альт Линукс» используются стандартные имена устройств:

–ttyN – консоль;

–mouse – манипулятор типа «мышь»;

–audio – звуковая карта;

–modem – модем;

–ttySN – последовательный порт;

–lpN – параллельный порт;

–cuaN – могут обозначать последовательные порты;

–sdxN – накопитель на жестких магнитных дисках;

–fd0 – первый дисковод для гибких дисков;

–stN – стример с интерфейсом SCSI;

–nrtfN – запоминающее устройство на принципе магнитной записи на ленточном носителе, с последовательным доступом к данным с интерфейсом FDC;

–mdN – массив RAID;

–ethN – сетевая плата;

–null – пустое устройство.

Примечание. N – номер устройства (например, tty1 – первая консоль).

3.2.4.2. Буферизация данных

Система буферизации выполняет функцию кэш-памяти по отношению к дисковому накопителю. Кэширование дискового накопителя уменьшает среднее время доступа к данным, хранящимся на нем. Любой запрос на ввод/вывод к физическому устройству преобразуется в запрос к подсистеме буферизации, которая представляет собой буферный пул и комплекс программ управления пулом.

Буферный пул состоит из буферов, находящихся в области ядра. Размер отдельного буфера равен размеру блока данных на дисковом накопителе.

С каждым буфером связана специальная структура – заголовок буфера, в котором содержится следующая информация:

1) данные о состоянии буфера:

–занят/свободен,

–чтение/запись,

–признак отложенной записи,

–ошибка ввода-вывода;

26) данные об устройстве – источнике информации, находящейся в этом буфере:

–тип устройства,

–номер устройства,

–номер блока на устройстве;

27) адрес буфера;

28) ссылка на следующий буфер в очереди свободных буферов, назначенных для ввода-вывода какому-либо устройству.

Запрос к подсистеме буферизации выполняется с помощью следующих основных функций:

–функции синхронной записи;

–функции асинхронной записи;

–функции отложенной записи;

–функций получения блока данных.

В результате выполнения функции синхронной записи немедленно инициируется физический обмен с внешним устройством, процесс, выдавший запрос, ожидает результат выполнения операции ввода-вывода. В данном случае в процессе может быть предусмотрена

собственная реакция на ошибочную ситуацию. Такой тип записи используется, когда необходима гарантия правильного завершения операции ввода-вывода.

В результате выполнения функции асинхронной записи также немедленно инициируется физический обмен с устройством, однако завершения операции ввода-вывода процесс не дожидается. В этом случае возможные ошибки ввода-вывода не могут быть переданы в процесс, выдавший запрос. Такая операция записи целесообразна при поточной обработке файлов, когда ожидание завершения операции ввода-вывода не обязательно, но есть уверенность в повторении этой операции.

В результате выполнения функции отложенной записи передача данных из системного буфера не производится. В заголовке буфера создается отметка о том, что буфер заполнен и может быть выгружен, если потребуется его освободить.

Каждая из функций получения блока данных ищет в буферном пуле буфер, содержащий указанный блок данных. В случае, если такой блок в буферном пуле отсутствует, осуществляется поиск любого свободного буфера (при этом возможна выгрузка на дисковый накопитель буфера, содержащего в заголовке признак отложенной записи), либо организуется его загрузка в какой-нибудь свободный буфер. В случае, если свободные буферы отсутствуют, производится выгрузка буфера с отложенной записью.

3.2.4.3. Взаимодействие с программами управления внешними устройствами ПЭВМ

Программы управления внешними устройствами ПЭВМ предназначены для управления передачей данных между внешним устройством и оперативной памятью ПЭВМ.

Связь ядра ОС с такими программами обеспечивается с помощью двух системных таблиц:

–таблица блок-ориентированных устройств (устройства, например, дисковые накопители, информация на которых хранится в блоках фиксированного размера, имеющих свой собственный адрес);

–таблица байт-ориентированных устройств (устройства, например, терминалы, сетевое оборудование, генерирующие или потребляющие последовательность байтов).

Для связи используется следующая информация из индексных дескрипторов специальных файлов:

–класс устройства (байт-ориентированное или блок-ориентированное);

–тип устройства (ленточный носитель, накопитель на гибком магнитном диске, накопитель на жестком магнитном диске, устройство печати, дисплей, канал связи и другие);

–номер устройства.

Класс устройства определяет выбор таблицы блок- или байт-ориентированных устройств. Эти таблицы содержат адреса программных секций драйверов. Тип устройства определяет выбор драйвера.

3.2.4.4. Службы управления печатью

В ОС «Альт Линукс» основной системой печати является сервер печати Common UNIX Printing System (далее – CUPS).

Сервер печати CUPS функционирует в виде отдельной службы и может управляться выделенным администратором либо общим администратором системы (предусмотрена возможность частично передавать права по управлению заданиями пользователя).

В состав сервера печати CUPS входят следующие компоненты:

–диспетчер очереди печати (планировщик);

–система фильтрации;

–Back-end-система.

Сервер печати CUPS работает в соответствии со следующим алгоритмом:

–сервер печати принимает задание на печать от программы (активного процесса) и передает его диспетчеру очереди печати или планировщику;

–диспетчер очереди печати добавляет задание на печать в соответствующую очередь;

–мандатные правила разграничения доступа (далее – ПРД) позволяют запустить CUPS в отдельном домене, что предотвратит доступ к очереди документов со стороны произвольного пользователя, не имеющего соответствующих прав администратора печати;

–диспетчер очереди печати передает задание на печать в соответствии с очередью системе фильтрации;

–система фильтрации обрабатывает данные: осуществляет все необходимые преобразования данных в соответствии с применяемыми для этого задания фильтрами и переводит их в формат, понятный принтеру;

–Back-end-система отправляет переформатированные данные на устройства печати в соответствии с мандатными ПРД пользователя, инициализировавшего печать.

3.2.5. Система администрирования

Система администрирования обеспечивает возможность выполнения настройки конфигурации ОС, в частности:

–создание загрузочных дисков;

–конфигурирование параметров даты и времени, графической среды, средств ввода и вывода;

–настройка и управление системными сервисами и служебными программами;

–настройка и управление системой управления пакетами Advanced Packaging Tool (далее – APT);

–обновление ОС и прикладного ПО из ее состава;

–настройка и управление учетными записями и правами доступа пользователей;

–конфигурирование сети /etc/net и проверка ее работоспособности;

–настройка и управление средами виртуализации;

–настройка служб DNS;

–настойка и управление кэширующими прокси-серверами;

–настройка и управление печатью;

–настройка подключаемых носителей.

Примечание. Защита от ошибочных действий администратора предусматривает их обнаружение и отображение компонентами операционной системы.

3.2.6. КСЗ

КСЗ предназначен для обеспечения безопасности информации, хранящейся и обрабатываемой в ПЭВМ, а также управляет процессами аутентификации пользователей, создания новых пользователей, назначения прав доступа именованных субъектов и процессов к объектам ОС «Альт Линукс», регистрации системных событий и журналирования.

В состав КСЗ входят следующие логические компоненты:

–система управления доступом;

–система управления памятью (очистка);

–система управления программными пакетами;

–система обеспечения целостности;

–система сопоставления пользователя с устройством;

–система маркировки документов, выводимых на печать

–система протоколирования событий.

КСЗ обеспечивает выполнение следующих функций:

1) в части управления доступом:

–идентификацию и аутентификацию субъектов доступа,

–контроль доступа субъектов доступа к объектам доступа (файлам, каталогам, процессам), основанного на принципах мандатного и дискреционного контроля доступа к информации,

–настройку правил разграничения доступа субъектов к объектам доступа,

–защиту ввода и вывода на отчуждаемый физический носитель информации и сопоставление пользователя с устройством,

–изоляцию программных модулей одного процесса от программных модулей других процессов;

29) очистку (обнуление) освобождаемых областей оперативной памяти;

30) очистку внешней памяти на дисковых накопителях (безопасное удаление файлов);

31) обеспечение целостности ядра ОС, программы загрузки ядра и модулей КСЗ;

32) регистрацию следующих событий:

–использование идентификационного механизма и механизма аутентификации;

–запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

–создание и уничтожение объекта;

–действия по изменению ПРД.

Для каждого из этих событий регистрируется следующая информация:

–дата и время;

–субъект, осуществляющий регистрируемое действие;

–тип события (если регистрируется запрос на доступ, то отмечается объект и тип доступа);

–успешность события (обслужен ли запрос на доступ или нет).

–очистку памяти на дисковых накопителях (безопасное удаление файлов).

Наряду с этим ОС «Альт Линукс» включает в себя дополнительные функции защиты данных, реализуемые на уровне системных приложений и прикладных программ, например: системы управления базами данных, брандмауэры, proxy-серверы.

3.2.6.1. Система управления доступом

3.2.6.1.1. Идентификация и аутентификация

В ОС «Альт Линукс» для предотвращения несанкционированного доступа субъекта доступа (пользователя) в программную среду используются механизмы идентификации (определение пользователя по имени – логину) и аутентификации (подтверждение подлинности имени пользователя с помощью пароля) пользователя. Процедуры идентификации и аутентификации пользователя выполняются при каждой попытке доступа в ОС.

ОС «Альт Линукс» хранит следующую информацию о пользователе:

–имя пользователя – регистрационное имя субъекта доступа;

–идентификатор пользователя – индивидуальный числовой идентификатор субъекта доступа, используемый при выполнении процедуры идентификации в ОС (задается из диапазона «0..65535», число «0» соответствует пользователю root);

–идентификатор группы – числовой идентификатор первичной группы пользователя (помимо первичной группы пользователь может входить в состав других групп, идентификатор группы 0 соответствует группе root);

–пароль – пароль пользователя;

–реальное имя пользователя – обычно представляет собой реальное (фактическое) имя пользователя;

–домашний каталог пользователя – в качестве домашнего каталога используется каталог /home/<имя пользователя >;

–оболочка субъекта доступа – командный интерпретатор пользователя, который используется им по умолчанию (запускается при входе пользователя в ОС).

Информация о пользователе хранится в файле /etc/passwd, пароли в зашифрованном виде хранятся в файле /etc/tcb/<имя пользователя >/shadow.

Процедура идентификации и аутентификации субъекта в ОС «Альт Линукс» выполняется в соответствии со следующим алгоритмом:

–пользователь посылает запрос на доступ в ОС «Альт Линукс»;

–автоматически системой вызывается программа login, (используется для запуска нового сеанса в системе), которая выводит приглашение login на терминал пользователя;

–пользователь предъявляет свое регистрационное имя (далее – логин) и пароль;

–модули переключателя служб имен Name Service Switch (далее – NSS) перехватывают логин пользователя и осуществляют его поиск в файлах виртуальной базы данных пользователей системы (для конфигурации источников виртуальной БД пользователей используется файл /etc/nsswitch.conf): в файлах /etc/passwd, /etc/shadow, /etc/group;

–если модули NSS находят логин пользователя в файлах /etc/passwd, /etc/shadow, /etc/group, система обращается к подключаемым модулям аутентификации, Pluggable Authentication Modules (далее – PAM) и запускается процесс аутентификации;

–модули PAM сравнивают логин и пароль, предъявленные пользователем со значениями, хранящимися в базе данных: в файлах /etc/passwd, /etc/shadow, /etc/group;

–если введенные имя и пароль субъекта соответствуют значениям, хранящимся в базе данных, КСЗ предоставляет доступ субъекту в ОС, информация о результате попытки доступа сохраняется в системном журнале /var/log/;

–если введенные имя и пароль субъекта не идентичны значениям, хранящимся в базе данных, КСЗ отклоняет запрос доступа субъекта в ОС (для выполнения повторной попытки аутентификации субъект должен инициировать новый запрос доступа), информация о результате попытки доступа сохраняется в системном журнале.

В конфигурации файла /etc/nsswitch.conf можно указать несколько источников файлов базы данных пользователей, например, в качестве источника указать дерево каталогов LDAP. В случае, если логин и пароль пользователя будут отсутствовать в файлах /etc/passwd, /etc/shadow, /etc/group, модули NSS осуществляют поиск в дереве каталогов LDAP, после чего соответствующие модули PAM выполняют аутентификацию пользователя (или оповещают об ошибке в случае не соответствия логина и пароля).

В случае необходимости реализации сетевой аутентификации пользователей в системе предусмотрена возможность аутентификации с помощью Kerberos с хранением информации о пользователях в дереве каталогов LDAP (Kerberos может использоваться и для осуществления локальной аутентификации пользователей).

3.2.6.1.2. Управление доступом

В ОС «Альт Линукс» разграничение доступа субъектов доступа к объектам доступа осуществляется в соответствии с принципами дискреционного и мандатного управления доступом.

В ОС «Альт Линукс» различают следующие типы файлов:

–обычные файлы (предназначены для хранения символьных и двоичных данных);

–каталоги (предназначены для организации доступа к файлам);

–символические и жесткие ссылки (предназначены для предоставления доступа к файлам, расположенным на любых носителях);

–файлы блочных и символьных устройств (предоставление интерфейса для взаимодействия с аппаратным обеспечением компьютера);

–каналы и сокеты (организация межпроцессорного взаимодействия в операционной системе).

3.2.6.1.3. Подсистема дискреционного обеспечения контроля доступа

В соответствии с дискреционным принципом управления доступом для каждого файла и каталога в ОС «Альт Линукс» устанавливаются права доступа, определяющие возможность доступа пользователя к объекту доступа (файл, каталог), а также возможные операции над ним.

Права доступа устанавливаются отдельно для различных категорий пользователей:

–владелец – пользователь, создавший файл (для того чтобы создать файл необходимо иметь право записи в каталог, в котором создается файл, при этом для владельца устанавливаются права на чтение и запись, для всех остальных пользователей – только на чтение);

–группа – набор пользователей, организованных, например, для работы с определенным набором файлов (владелец может разрешить или запретить доступ к файлам для членов группы);

–прочие – все остальные пользователи.

Основными операциями, выполняемыми над объектами доступа в ОС «Альт Линукс», являются следующие:

–чтение (read, r);

–запись (write, w);

–исполнение (execution, x).

Чтение для файла означает право получать содержимое по индексному дескриптору. Для каталога – означает право получать список имен объектов, содержащихся в нем. В случае, если доступ на чтение к каталогу запрещен, процесс не сможет получить список имен, однако доступ непосредственно к файлу, находящемуся в каталоге, регулируется правом использования (исполнения) каталога, а не правом чтения.

Запись для файла означает право модифицировать содержимое по индексному дескриптору. Для каталога – означает право модифицировать список файлов. Без права на использование (исполнение) каталога право на запись практически неприменимо.

Использование для файла означает право запускать его в качестве программы. Различают бинарные исполняемые файлы, которые непосредственно загружаются в память в виде процесса (возможно, посредством динамической компоновки с разделяемыми библиотеками) и сценарии, для выполнения которых запускается процесс из другого файла, а текущий файл отдается ему в качестве параметра командной строки (следовательно, для работы запускаемого сценария требуется также доступ на чтение).

Для каталога доступ на использование (исполнение) означает право преобразовывать имена объектов, находящихся в каталоге, в индексные дескрипторы. Список имен файлов в каталоге, доступном процессу на чтение, но не на использование, будет виден, но сами файлы останутся недоступны.

Для работы с блочными и символьными устройствами в ОС при монтировании создаются специальные файлы, обеспечивающие произвольный или последовательный доступ соответственно типу устройства, которому они назначаются. Права доступа для учетных записей пользователя и вызываемых процессов назначаются на соответствующий созданный файл.

Права доступа к локальным сокетам назначаются на специальный файл сокета по заданному пути, через который к сокету будут сообщаться любые локальные процессы путем чтения/записи из него. При использовании сетевого сокета, создается абстрактный объект, привязанный к слушающему порту операционной системы и сетевому интерфейсу, затем ему присваивается INET-адрес, который имеет адрес интерфейса и слушающего порта, и далее обращение будет происходить к абстрактному объекту согласно назначенным правам.

Права доступа именованного канала аналогичны правам доступа к файлу. Обращение к именованному каналу осуществляется также как и к обычному файлу. В связи с этим, для работы с именованными каналами процессам необходимо предоставлять права доступа для чтения (записи) из (в) канал. При создании канала необходимо учитывать, что каналы создаются с правами доступа «0666», модифицированными маской прав доступа umask(2) вызывающего процесса. Также, утилита создания канала требует право на запись в родительский каталог.

Права доступа к символьным ссылкам всегда выглядят как «rwxrwxrwx», поскольку при использовании ссылки драйвер файловой системы пересчитывает реальный путь к файлу и применяет права доступа, определенные для реального пути уже без учета самой символьной ссылки.

При вычислении прав доступа принимается во внимание уровень доступа процесса к файлу, который вычисляется следующим образом:

–если UID файла и актуальный UID процесса совпадают, процесс считается владельцем файла;

–в противном случае, если GID файла совпадает с актуальным GID процесса или входит в список групп, процесс считается членом группы;

–если оба условия не выполнены, процесс считается чужим по отношению к файлу.

Права доступа включают список из девяти атрибутов (битов) файла, записываемых в форме «rwxrwxrwx»: по три вида доступа (чтение – read, запись – write, исполнение – execute) для трех групп – пользователя-владельца (u), группы-владельца (g) и всех остальных (o) соответственно. Каждый пункт в этом списке может быть либо разрешен, либо запрещен (равен 1 или 0). В случае, если некоторый доступ запрещен на некотором уровне, вместо символа пишется знак «-». Атрибуты неотторжимы от файла, так как хранятся в его метаданных (индексном дескрипторе), и не зависят от количества имён (ссылок на файл) и их расположении в дереве каталогов.

Права доступа файлового объекта могут быть изменены, если это разрешено текущими правилами (санкционировано). Модифицировать права доступа может только процесс-владелец (пользователь-владелец) файла, либо суперпользовательский (запущенный от имени пользователя root) процесс (UID процесса = 0).

Описанные выше права выставляются с помощью функции umask (user file creation mode mask). Umask одинаковым образом работает для всех объектов: каждый установленный бит umask запрещает выставление соответствующего бита прав. Исключением из этого запрета является бит исполняемости, который для обычных файлов зависит от создающей программы (трансляторы ставят бит исполняемости на создаваемые файлы, другие программы – нет), соответственно, исключением являются сокеты и каналы межпроцессного взаимодействия и монтируемые аппаратные устройства. В случае каталогов umask следует общему правилу.

При обращении процесса к объекту (с запросом доступа определенного вида) система проверяет совпадение идентификаторов владельцев процесса и владельцев файла в определенном порядке, и в зависимости от результата, применяет ту или иную группу прав.

В случае, если текущими правилами разрешено (санкционировано), права доступа файлового объекта могут быть изменены.

Кроме общей схемы разграничения доступа ОС «Альт Линукс» поддерживает также ACL, с помощью которых можно для каждого объекта задавать права всех субъектов на доступ к нему.

Механизм дискреционного разграничения доступа обеспечивает возможность санкционированного изменения списка пользователей и списка защищаемых файловых объектов.

3.2.6.1.4. Подсистема мандатного обеспечения контроля доступа SELinux

В ОС «Альт Линукс» механизм мандатного управления доступом реализуется при помощи системы мандатного обеспечения контроля доступа SELinux, реализованной на уровне ядра ОС. При этом принятие решения о запрете или предоставлении доступа субъекта к объекту принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности субъекта и мандатной метки объекта. С помощью SELinux задаются явные правила того, как субъекты (пользователи и процессы) могут обращаться к объектам доступа (файлам, устройствам и другим объектам).

В SELinux права доступа определяются самой системой при помощи специально определенных политик (наборов правил). Политики работают на уровне системных вызовов и применяются самим ядром, хотя имеется возможность реализации на уровне приложения.

ОС «Альт Линукс» содержит различные пакеты с политиками безопасности:

–selinux-policy-targeted – «целевая» политика (targeted) предназначена для защиты ОС от системных процессов, передающих и получающих сообщения через сетевые сервисы;

–selinux-policy-minimum – разработана на основе политики targeted и используется для разработки пользователями своих собственных политик безопасности, в связи с этим политика minimum содержит те же модули, что и политика targeted, однако не задействует их, следовательно, при политике minimum SELinux изначально не ограничивает никакие объекты системы безопасности;

–selinux-policy-mls – многоуровневая модель безопасности, реализующая модель разграничения доступа Белла – Лападулы, где всем объектам системы присваивается определенный классификационный уровень, являющийся комбинацией иерархических категорий (уровень безопасности) и неиерархических категорий;

–selinux-policy-altlinux – в политике все приложения (за исключением точек входа: systemd, kernel, login и ssh) выполняются домене generic_t, при этом решение о допустимости действий приложения выполняется на основе уровней и категорий, а в случае надобности, политика допускает создание дополнительных доменов для приложений для задания специфических ограничений;

–selinux-policy-strict – реализует подход «все, что не разрешено в явном виде, то запрещено», при котором пользователям и процессам разрешается доступ только к ряду определенных каталогов.

3.2.6.1.5. Управление доступом к сетевому взаимодействию

В ОС «Альт Линукс» осуществляется разграничение доступа к сетевому взаимодействию посредством пакета iptables, в рамках выполнения следующих функций:

–сбор статистики по сетевому трафику (учета статистики пакетов);

–разграничения доступа к сети отдельным приложениям;

–разграничения доступа к сети для определенных пользователей системы (кроме ICMP-пакетов, для которых невозможно определить владельца);

–фильтрации пакетов для входящих и исходящих соединений;

–фильтрации пакетов по дате\времени;

–фильтрации протоколов прикладного уровня.

3.2.6.2. Система управления памятью

В состав системы управления памятью входят следующие компоненты:

–подсистема управления оперативной памятью;

–подсистема управления внешней памятью.

3.2.6.2.1. Подсистема управления оперативной памятью

Каждый процесс в ОС «Альт Линукс» работает со своими виртуальными адресами (в собственном виртуальном адресном пространстве), трансляция которых в физические выполняется на аппаратном уровне с помощью ядра ОС. Пользовательский процесс лишен возможности напрямую обратиться к страницам основной памяти, занятым информацией, относящейся к другим процессам. Следовательно, процессы становятся изолированными друг от друга. Физическая память распределяется независимо от распределения виртуальной памяти отдельного процесса.

По завершению работы активного процесса КСЗ осуществляет очистку оперативной памяти (RAM-памяти), предоставляемой этому процессу. Очистка производится записью нулей или маскирующей информации в память при ее назначении пользователю или освобождении.

Страница памяти освобождается ядром ОС «Альт Линукс». Оно высвобождает страницы, начинающиеся с указанной, размера [размер_страницы * (2 ^ кратность)]. Область возвращается в массив свободных областей в соответствующую позицию и после этого происходит попытка объединить несколько областей для создания одной большего размера.

3.2.6.2.2. Подсистема управления внешней памятью

Внешняя память, используемая ОС, располагается на отдельном разделе диска, представленном в файловой системе специальным файлом, доступ к которому непосредственно из программы контролируется дискреционными и мандатными ПРД. По умолчанию доступ к разделам диска имеет только доверенный субъект или член группы «disk».

При первоначальном назначении или при перераспределении внешней памяти КСЗ может ограничивать доступ субъекта к остаточной HDD-информации через механизм «безопасного удаления» файлов (специальный атрибут файла, указывающий на необходимость перезаписи физической области носителя диска после удаления файла). Еще одним способом является использование команды shred, обеспечивающей безопасное удаление файлов.

3.2.6.3. Система управления программными пакетами

Для работы с программными пакетами в среде ОС «Альт Линукс» используется система управления программными пакетами APT, обеспечивающая контроль целостности и непротиворечивости установленного ПО.

Система управления программными пакетами APT решает следующие задачи:

–установка, удаление и обновление пакетов;

–разрешение зависимостей пакетов от общих ресурсов;

–поиск пакетов по заданным критериям;

–просмотр подробных сведений о пакетах;

–манипулирование ключами от репозиториев;

–контроль целостности.

В процессе функционирования система управления программными пакетами APT использует две базы данных, одна из которых описывает установленные в системе пакеты, а другая описывает внешний репозиторий, в котором содержится мета-информация о пакетах – индексы пакетов, содержащихся в репозитории, и сведения о них.

Система управления программными пакетами APT отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

3.2.6.4. Система обеспечения целостности

Подсистема обеспечения целостности из состава ОС «Альт Линукс» выполняет контроль целостности программных средств и обрабатываемой информации.

В ОС «Альт Линукс» для контроля целостности предусмотрено использование программы osec. Дополнительно программа osec обеспечивает возможность поиска потенциально опасных файлов, например, файлов с установленными битами прав смены идентификаторов пользователя (suid), группы (sgid) и с общедоступной записью.

При запуске программы osec в соответствии с конфигурационным файлом создается база данных (с соответствующими контрольными суммами), которая определяет текущее состояние программных средств и обрабатываемой информации. Далее осуществляется сравнение актуальных значений контрольных сумм с контрольными суммами, которые были получены при предшествующем запуске программы.

Наличие различий между контрольными суммами свидетельствует о том, что какие-либо файлы или их атрибуты (права доступа) были изменены.

В состав программы osec входят следующие компоненты:

–osec – программа сбора данных, результаты работы по умолчанию подаются в неформатированном виде в стандартный поток вывода stdout;

–osec_reporter – программа-фильтр для создания отчетов, принимает на вход неформатированный вывод программы osec и представляет данные в удобном виде для чтения (результаты работы также подаются в стандартный поток вывода stdout).

Программа osec поддерживает работу в двух режимах:

–режим «чтение»;

–режим «чтение-запись» (по умолчанию).

В режиме «чтение» в случае обнаружения изменений программа osec выполняет оповещение об обнаруженных изменениях с помощью вывода соответствующего сообщения в стандартный поток вывода. В режиме «чтение-запись» в случае обнаружения изменений программа osec оповещение об обнаруженных изменениях, а также сохраняет новое состояние системы в базу данных. Для каждого контролируемого каталога программа osec создает уникальный файл базы данных и помещает его в каталог базы данных, указанный в опции -D (db_path).

Периодичность контроля целостности для контролируемых файлов развернутой ОС «Альт Линукс» устанавливается нормативными документами АС, в которой будет использоваться ОС «Альт Линукс», и определяется администратором безопасности. Контроль осуществляется вручную либо с помощью настройки расписаний в специальных программных средствах.

Контроль целостности для контролируемых файлов ОС «Альт Линукс» должен выполняться с периодичностью не реже, чем 1 раз в месяц.

3.2.6.5. Система сопоставления пользователя с устройством

ОС «Альт Линукс» обеспечивает ввод-вывод информации на запрошенное пользователем устройство как для произвольно используемых им устройств, так и для идентифицированных (при совпадении маркировки).

ОС «Альт Линукс» включает в себя механизм, обеспечивающий надежное сопоставление мандатного контекста пользователя с мандатным уровнем и категориями, установленными для устройства. Кроме того, механизм сопоставления пользователя с устройством обеспечивает при проверке совпадения маркировок носителя и пользователя применение дискреционных ПРД.

3.2.6.6. Система маркировки документов, выводимых на печать

В ОС «Альт Линукс» основной системой печати является сервер печати Common UNIX Printing System (CUPS).

CUPS функционирует в виде отдельной службы и может управляться выделенным администратором либо общим администратором системы (предусмотрена возможность частично передавать права по управлению заданиями пользователя). CUPS имеет собственный веб-интерфейс для администрирования, работающий через Internet Printing Protocol (далее – IPP). CUPS использует IPP в качестве основы для управления заданиями и очередями.

Сервер печати CUPS обеспечивает маркировку выводимых на печать документов. Мандатные атрибуты автоматически связываются с заданием для печати на основе мандатного

контекста, получаемого с сетевого соединения. Сервер CUPS отслеживает непосредственную возможность печати документа на выбранном принтере: проверяется метка принтера, с которого задание было оправлено на печать, также проверяется метка печатаемого документа и отправляется с печатью на принтер.

При этом маркировка документов при печати через удаленный CUPS сервер через IPP не поддерживается. Печать маркировок на удаленный CUPS сервер возможна только при подключении к нему по протоколу LP, с полностью локальным преобразованием документа в формат принтера.

В случае, если необходима маркировка документов, то печать будет возможна только через локальный сокет. Перед непосредственным наложением штампа следует предварительно создать шаблон штампа и настроить сервер печати на его использование. Кроме того, необходимо учитывать, что в ходе печати будет создано дополнительное задание для печати «фонарика». Количество страниц документа также выводится в «фонарике».

Маркировка выводимых на печать документов сводится к ручному выбору соответствующих заранее подготовленных шаблонов верхней и нижней страниц. Этот метод имеет следующие допущения:

–наличие в общей очереди к принтеру документов, сформированных из данных различных уровней конфиденциальности;

–доступ к документам должен осуществляться исключительно со стороны процессов подсистемы печати и только от имени администратора безопасности системы, в таком случае вся ответственность за безопасность сведений различных уровней конфиденциальности ложится на администратора безопасности;

–шаблонное (одинаковое) представление «штампа № 1» для всех документов определенного уровня (с возможной подстановкой логина пользователя и файла-источника данных);

–недопустимость проставления штампа на отдельных чистых листах документа;

–допустимость проставления штампа с помощью штатного печатающего устройства.

3.2.6.7. Система протоколирования событий

В состав системы протоколирования событий входят следующие компоненты:

–подсистема журналирования;

–подсистема аудита.

3.2.6.7.1. Подсистема журналирования

В ОС «Альт Линукс» функция записи информации о системных событиях и событиях безопасности обеспечивается с помощью системной службы syslogd.

Подсистема журналирования функционирует в соответствии со следующим алгоритмом:

–программы (источники регистрируемых данных) формируют простые текстовые сообщения о происходящих в них событиях и передают их на обработку в ядро, инициализируя при этом системный вызов;

–системная служба syslogd сравнивает каждую поступившую запись с правилами, которые находятся в файле конфигурации /etc/syslog.conf: в случае обнаружения соответствия служба syslogd обрабатывает запись описанным в конфигурационном файле syslog.conf способом.

Подсистема журналирования в ОС «Альт Линукс» функционирует в соответствии со следующими основными положениями:

–формирование сообщений о событиях и их передача осуществляется по определенным правилам (протокол Syslog);

–передача текстовых сообщений осуществляется с использованием сетевых или доменных сокетов;

–источники сообщений могут располагаться на разных машинах.

Все регистрируемые сообщения по умолчанию записываются в каталог системного журнала /var/log, при необходимости могут быть указаны и другие хранилища (для каждой службы может быть установлено собственное хранилище или несколько хранилищ).

Примечание. Для очистки системных журналов от сообщений об устаревших событиях в ОС «Альт Линукс» используется служба logrotate.

3.2.6.7.2. Подсистема аудита

В состав подсистемы аудита входят следующие компоненты:

1) модуль ядра – перехватывает системные вызовы (syscalls) и выполняет регистрацию событий;

33) служба auditd – записывает зарегистрированное событие на диск в файл;

34) служба audispd – осуществляет пересылку сообщений (выступает в роли диспетчера) к другому приложению;

35) ряд вспомогательных служб:

–auditctl – служба, управляющая поведением системы аудита и позволяющая контролировать текущее состояние системы, создавать или удалять правила,

–aureport – служба, генерирующая суммарные отчеты о работе системы аудита,

–ausearch – служба, позволяющая производить поиск событий в журнальных файлах,

–autrace – служба, выполняющая аудит событий, порождаемых указанным процессом.

В ОС «Альт Линукс» регистрируются следующие типы событий:

–запуск и завершение работы ОС «Альт Линукс» (перезагрузка, остановка);

–запуск и остановка приложений;

–выполнение системных вызовов;

–использование механизма идентификации и аутентификации;

–запрос на доступ к защищаемому ресурсу;

–создание и уничтожение объекта;

–действия по изменению ПРД;

–инициация сетевого соединения или изменение сетевых настроек и другие.

Программы отсылают записи, предназначенные для протоколирования, системной службе auditd, которая идентифицирует тип каждой пришедшей записи и обрабатывает ее в соответствии с типом записи.

Для каждого из регистрируемых событий в журналах указывается следующая информация:

–дата и время;

–субъект, осуществляющий регистрируемое действие;

–тип события (если регистрируется запрос на доступ, то указываются объект и тип доступа);

–успешность осуществления события (обслужен запрос на доступ или нет).

3.2.6.8. Механизмы защиты системы виртуализации

Механизмы защиты системы виртуализации осуществляют выполнение следующих основных функций:

–обеспечение защиты от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

–осуществление контроля доступа субъектов доступа к средствам конфигурирования виртуальных машин (virt-manager, virsh, virt-install);

–предоставление возможности применения индивидуальных прав доступа субъектов виртуальной инфраструктуры к объектам;

–обеспечение контроля доступа субъектов доступа к файлам-образам, используемым для обеспечения работы виртуальных машин;

–обеспечение контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы и гипервизора;

–обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры;

–осуществление идентификации и аутентификации субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры (в т. ч. к средствам конфигурирования виртуальных машин);

–обеспечение блокирования доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

–обеспечение регистрации 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.

–осуществление контроля целостности компонентов, критически важных для функционирования гипервизора и виртуальных машин.

Указанные механизмы применимы при выключенной политике selinux-policy-altlinux, то есть при отсутствии необходимости мандатного разграничения доступа.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные

Обмен информацией между ОС «Альт Линукс» и внешними источниками осуществляется с помощью информационных сообщений по локальной вычислительной сети или сети Internet с использованием протоколов TCP/IP, ICMP, FTP, HTTP, POP, SMTP, IMAP, SLIP, PPP, RIP, IPX и NetBIOS.

Также входными данными являются управляющие команды пользователей и администраторов ПЭВМ, введенные с использованием клавиатуры и (или) манипулятора типа «мышь»:

–обращение субъектов доступа (процессов и команд СУБД) к защищаемым именованным объектам доступа – файлам (программам, библиотекам, файлам с пользовательской и служебной информацией), каталогам, специальным файлам (устройствам, ссылкам, каналам FIFO), базам банных и их элементам (таблицам, записям, полям записей, триггерам), а также средствам IPC (портам, сокетам, семафорам);

–атрибуты, определяющие полномочия субъектов доступа и правила разграничения доступа к объектам доступа.

4.2. Выходные данные

Выходными данными для ОС «Альт Линукс» являются результаты обработки управляющих команд со стороны пользователей, администратора и администратора безопасности, результаты обмена информацией между ОС «Альт Линукс» и внешними источниками по локальной вычислительной сети или сети Интернет с использованием протоколов TCP/IP, ICMP, FTP, HTTP, POP, SMTP, IMAP, SLIP, PPP, RIP, IPX и NetBIOS.

Также выходными данными является результаты использования субъектом доступа защищаемого объекта, предоставленного ему в соответствии с установленными правилами разграничения доступа. К таким результатам могут относиться: запуск программы, редактирование файла, создание сокетов, добавление данных в базы данных и другие действия.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

APT – Advanced Packaging Tool (система управления программными пакетами);

CUPS – Common UNIX Printing System (сервер печати для UNIX-подобных операционных систем);

DMA – Direct Memory Access (прямой доступ к памяти);

DNS – Domain Name System (служба имён доменов);

ext2 – Second Extended File System (файловая система);

ext3 – Third extended file system(файловая система);

FDC – Floppy Disk Controller (контроллер накопителя на гибких магнитных дисках);

FIFO – First-In, First-Out (дисциплина очереди «первый вошел – первый вышел»);

FTP – File Transfer Protocol (протокол передачи файлов);

HTTP – HyperText Transfer Protocol (протокол передачи гипертекстовых файлов);

IBM – International Business Machines;

IBM PC – IBM Personal Computer (персональный компьютер, совместимый с IBM);

IMAP – Interactive Mail Access Protocol (протокол интерактивного доступа к электронной почте);

IPX – Internetwork Packet Exchange (межсетевой пакетный обмен);

JFS – Journal File System (журналируемая файловая система);

LDAP – Lightweight Directory Access Protocol (протокол доступа к каталогам);

NetBIOS – Network Basic Input/Output System (протокол для работы в локальных сетях на ПЭВМ типа IBM PC);

NFS – Network File System (сетевая файловая система);

PID – Process Identificator (идентификатор процесса);

PPP – Point-to-Point Protocol (протокол передачи от точки к точке, протокол двухточечного соединения);

RAID – Redundant Array of Independent Disks (матрица независимых дисковых накопителей с избыточностью);

ReiserFS – Reiser File System (файловая система ReiserFS);

RIP – Routing Information Protocol (протокол для маршрутизации пакетов в компьютерной сети);

ROM – Read-Only Memory (постоянное запоминающее устройство);

SCSI – Small Computer Systems Interface (интерфейс малых компьютерных систем);

SGID – Set Group ID (специальные права доступа пользователя);

SLIP – Serial Line Internet Protocol (межсетевой протокол для последовательного канала);

SMTP – Simple Mail Transfer Protocol (простой протокол электронной почты);

SUID – Set User ID (специальные права доступа пользователя);

TCP/IP – Transmission Control Protocol/Internet Protocol (протокол управления передачей/протокол Internet, стек протоколов Internet);

VFS – Virtual File System (виртуальная файловая система);

XFS	– журналируемая файловая система;
КСЗ	– комплекс средств защиты;
ОС	– операционная система;
ПО	– программное обеспечение;
ПРД	– правила разграничения доступа;
ПЭВМ	– персональная электронная вычислительная машина;
СУБД	– система управления базами данных.

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в документе*	*№ документа*	*Входящий № сопроводитель-ного документа и дата*	*Подпись*	*Дата*
	измененных	*замененных*	*новых*	*аннулирован-ных*					