Канд. техн. наук. С. Г.Семенцов, инж. П.А.Выпов, инж. С.А.Козлов

ОПЫТ СОЗДАНИЯ СПЕЦИАЛИЗИРОВАННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ LINEM ДЛЯ СИСТЕМ УПРАВЛЕНИЯ И ЗАЩИТЫ АЭС

При разработке программно-технического комплекса информационно-диагностической сети (ПТК ИДС) комплекса электрооборудования АЭС «Тяньвань» и «Бушер» возникла задача создания дистрибутива системного ПО на базе систем с открытыми исходными кодами, получившего название LiNEM, и включающего в себя собственно ОС и дополнительные сервисные модули.

В значительной мере всем требованиям, предъявляемым к ПО систем, важных для безопасности АЭС, удовлетворяют системы на базе клонов свободно распространяемой операционной системы Linux [1,2]. В этой связи было принято решение о разработке системы на базе отечественного дистрибутива ОС ASPLinux 7.1.

Структура типичного дистрибутива общего применения Linux представляет собой ядро и набор инсталляционных пакетов (например RPM-пакетов для дистрибутивов семейства RedHat) (рис. 1).

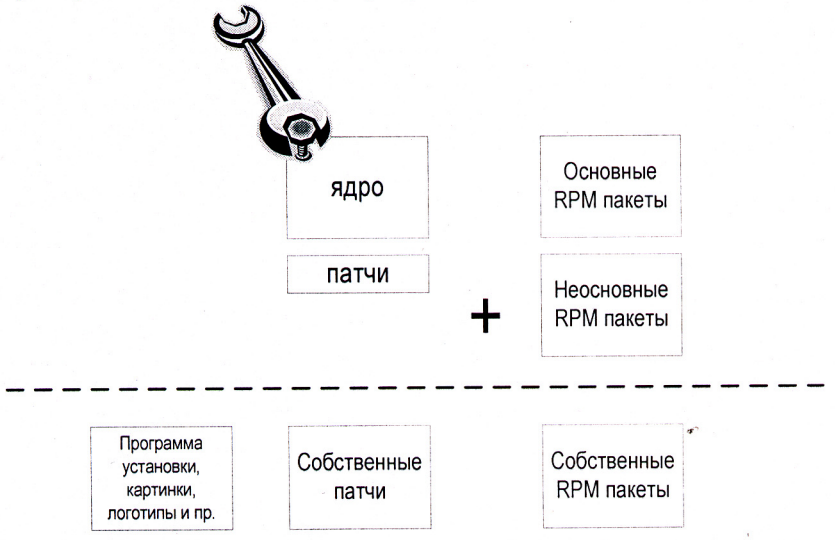

Рис. 1. Обобщенная структура Linux-дистрибутива общего применения

Ядро и основные инсталляционные пакеты у всех дистрибутивов в рамках одного семейства примерно одинаковы [3]. Различия проявляются, как правило, лишь в наборе «заплаток» (патчей), вносимых в ядро с той или иной целью, наборе RPM- пакетов, которые добавляются в дистрибутив в зависимости от назначения дистрибутива, типа инсталляционной программы и функциональных требований к системе. Патчи добавляют в ядро новые модули или вносят изменения в уже существующие либо для исправления ошибок, либо для расширения функций. Разработчики дистрибутивов вносят свои изменения путем добавления в ядро собственных патчей или патчей сторонних разработчиков, которые представляют собой исправления в ядре, но которые по тем или иным причинам не вошли в официальную версию ядра Linux. Также добавляются RPM-пакеты, например конфигурационные утилиты (такие как kudzu, harddrake, Xconfigurator или Yast2) и пакеты, автоматизирующие процесс обновления дистрибутива через Интернет (например yum).

В общем случае RPM-пакет представляет собой заархивированный набор из файлов трех категорий [4]:

- исполняемые файлы (скрипты или бинарные файлы), статические или динамические библиотеки;
- конфигурационные файлы и вспомогательные файлы. Заголовочные файлы для библиотек или базы данных;
- файлы документации: README, страницы man, ссылка на собственный сайт sourceforge.net или gnu.org.

По своей внутренней структуре ОС Linux имеет четко выраженную модульную организацию, т.е. состоит из функциональных частей с чёткими границами. Существование таких границ позволяет существенно сократить размер дистрибутива за счет отказа от ненужных в данной конфигурации функций, исправить или заменить необходимые функции. Необходимый набор функций системы может быть реализован с помощью одного или нескольких RPM-пакетов, но важно то, что эти пакеты могут быть удалены из дистрибутива без последствий для работоспособности системы, т.е. они почти полностью независимы друг от друга. Существуют логические зависимости пакетов друг от друга, представляющих собой дерево зависимостей, но этими зависимостями можно пренебречь. Немаловажно также то, что каждый RPM-пакет имеет независимую от других документацию, что позволяет принять решение о необходимости его использования в дистрибутиве. На рис. 2 приведена обобщенная структура организации дистрибутивов Linux семейства RedHat. Можно выделить набор базовых пакетов, каждый из которых состоит из ряда RPM-пакетов.

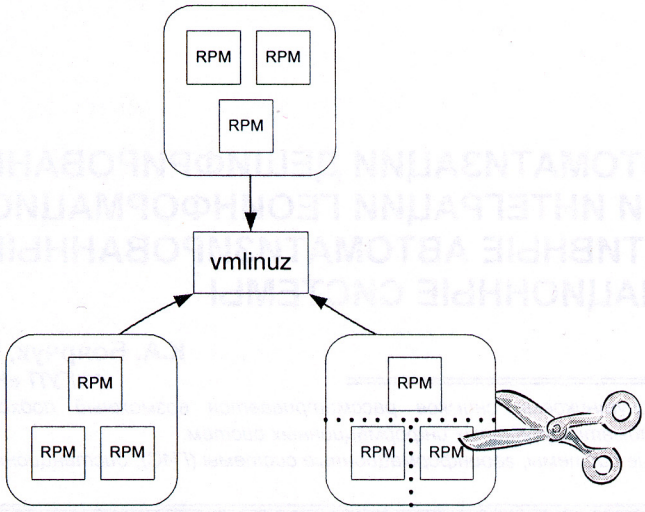

Рис. 2. Обобщенная структура организации модулей внутри дистрибутива семейства RedHat

При разработке ОС LiNEM было необходимо максимально сократить размер дистрибутива, использовать только минимально необходимый набор пакетов (чем меньше пакетов, тем меньше вероятность конфликтов и сбоев) и максимально стабильные версии пакетов, обеспечить совместимость с разрабатываемым прикладным ПО и широким спектром аппаратных средств.

Алгоритм действий по разработке специализированного Linux-дистрибутива можно представить следующим образом:

- анализ необходимости применения данного RPM-пакета. Если пакет действительно необходим, то есть ли альтернативы его использования, т.е. пакеты меньшего размера, более стабильные;
- анализ необходимости использования данного драйвера или подсистемы и его реализации на уровне ядра или внешнего модуля;
- достаточно ли этих пакетов и модулей для того, чтобы реализовать требуемый функциональный набор? Если нет, то необходима разработка прикладного ПО;
- редактирование связей элементов дистрибутива - скриптов и конфигурационных файлов пакета initscripts, загрузчика LILO и пр.

В предельном случае Linux дистрибутив в минимально возможной конфигурации представляет собой следующую структуру, показанную на рис. 3.

На рисунке представлено ядро Linux (vmlinuz) в минимальной конфигурации, в котором деактивированы все неиспользуемые сервисы, и исполняемый файл init, реализующий функции интерфейса с внешними модулями [5]. Такая структура вполне работоспособна, однако не совсем удобна, поскольку большую часть функциональных требований придется реализовать в этом исполняемом файле.

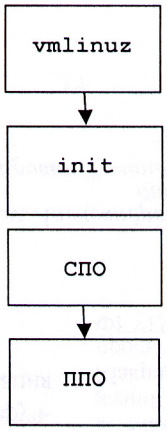

Рис. 3. Структура минимальной конфигурации Linux дистрибутива

Более удобной представляется следующая схема (рис. 4) – стандартная для большинства Linux дистрибутивов общего применения.

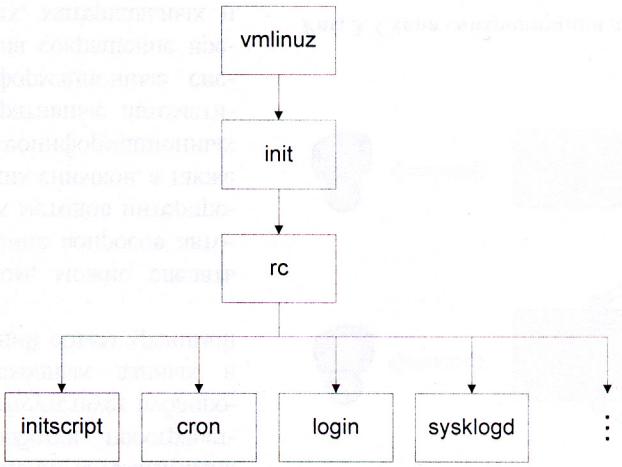

Рис. 4. Структура взаимодействия ядра и программ ОС LiNEM

Здесь исполняемый файл **init** умеет только запускать файл **rc** и переключать режимы (reset, shutdown, 1, 2, 3, 4, 5). Файл **rc** включает и выключает все остальные исполняемые файлы:

- **initscript** выполняется только при запуске и запускает

- initscript выполняется только при запуске и запускает прикладные программы при инициализации системы;

- cron следит за календарем и выполняет программы при наступлении определенного часа или даты;

- login следит за консолью и выполняет другие программы (например оболочку) только по запросу пользователя;

- различные программы, с маской названий (****)d, например syslog**d** (системный журнал), которые выполняются беспрерывно от момента старта системы до ее выключения (или переключения режима **rc**), их также называют «демонами».

Эти основные программы просты в конфигурировании: rc и initscript – это редактируемые текстовые файлы, а init, login и cron управляются конфигурационными файлами. Также тривиальны и базовые службы, такие как sysklogd. К ним и монтируются все остальные системные и прикладные пакеты Linux системы.

В настоящее время в НПП ВНИИЭМ разработаны два варианта дистрибутива LiNEM: собственно сам дистрибутив и программа аварийной загрузки и восстановления системы.

Программа загрузки и восстановления представляет собой максимально упрощенный вариант ОС LiNEM, предназначенный для восстановления основного или резервного сервера ПТК ИДС после сбоя с помощью программы-установщика **restore** (рис.5).

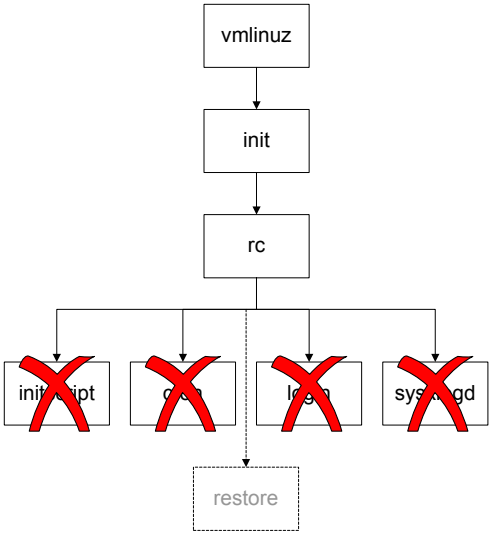

Рис. 5. Структура взаимодействия модулей программы загрузки

Эта программа выполняет следующие действия:

- выполняет тесты памяти и жёсткого диска для сервера, на котором произошёл сбой;
- копирует с CD на жесткий диск эталонный образ системы и подсчитывает контрольную сумму;
- перезагружает сервер.

Дистрибутив LiNEM представляет собой полноценный вариант Linux дистрибутива (рис. 6), в котором, по сравнению с программой загрузки и восстановления, были произведены следующие изменения:

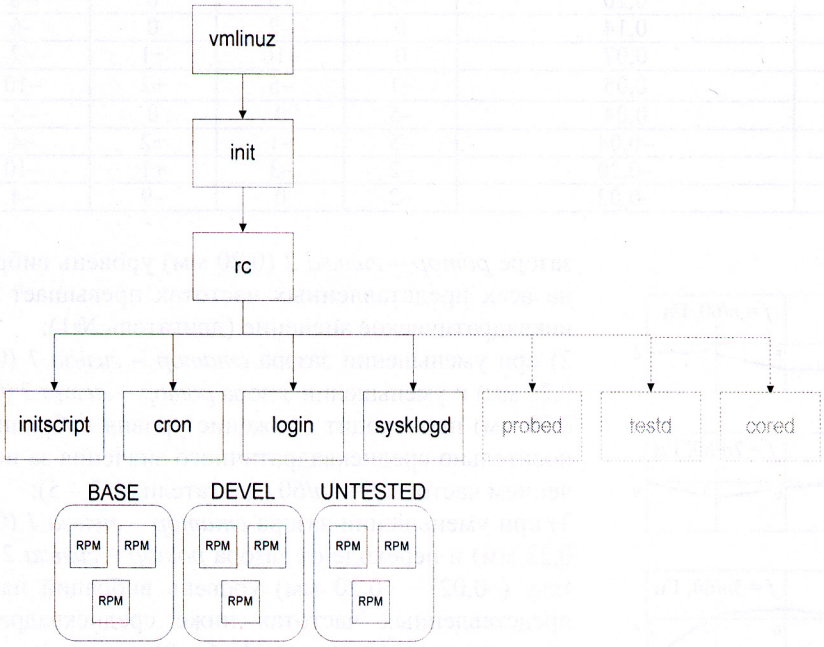

Рис. 6. Структура дистрибутива LiNEM

- внешние изменения. Подобраны и минимизированы наборы RPM-пакетов для разных профилей работы: например «серверные станции ПТК ИДС», «станция разработчика прикладного ПО» и «рабочая станция». Исправлены скрипты rc и initscript;
- внутренние изменения. RPM-пакеты, ориентированные на работу в серверных станциях ПТК ИДС, были собраны заново с использованием библиотек и инструментов, ориентированных на повышение надёжности ПО;
- системные службы **probed, testd** и **cored** реализуют функции

по повышению безопасности работы серверов, **probed** следит за состоянием ресурсов и реагирует на системные события (превышен расход памяти, количество обращений к диску (свопу) превысило лимит и т.д.), **testd** запускает аппаратные тесты памяти, файловой системы и служб из пакетов тестовых программ LTP, OHCP и собственные оригинальные тесты, **cored** следит за появлением в системе файлов дампа памяти.

В числе характерных особенностей использования специализированного дистрибутива LiNEM в составе ПТК ИДС можно отметить следующие:

- аппаратное и программное обеспечение для каждого нового проекта («Бушер», «Тяньвань» и пр.) немного отличается от предыдущего, появляются обновления к отдельным пакетам и пр., поэтому для каждого проекта предполагается сборка нового дистрибутива (LiNEM версии 1.0, 1.1 и т.д.), включающего в себя драйверы новых устройств и др.;
- сборка пакетов с использованием отладочного режима компилятора и использование специальных программных модулей позволяет получить значительный объем информации при крахе системы, что позволяет выявить причину сбоя, например инструмента LKCD, который в случае появления в системе core-файла с помощью отладчика в пакетном режиме получает обратный стек вызовов и точное место краха и сохраняет их для последующего анализа;
- минимизация количества и объема RPM-пакетов дает возможность сократить размер дистрибутива до нескольких десятков Мбайт и разместить его на одном компакт-диске;
- группировка RPM-пакетов по целевому назначению: **BASE** – базовый набор пакетов для рабочего сервера, оттестированный для работы в составе ПТК ИДС; **DEVEL** – набор пакетов для разработки, аудита и верификации программного обеспечения, **UNTESTED** – программное обеспечение общего назначения, позволяет значительно упростить процесс аудита и тестирования нового ПО и расширить область применения дистрибутива;
- архитектура системы обеспечивает более широкие возможности при сборке дистрибутива, например позволяет использование надёжного ядра старой версии, старой версии библиотеки С, но самых свежих пакетов прикладного ПО и драйверов аппаратных средств;
- использование узко-ориентированной установочной программы и использование целевых профилей со специально подобранными наборами RPM-пакетов дает возможность значительно повысить надежность системы.

Как уже отмечалось в других работах, при разработке дистрибу-

тива широко применялись средства статического и динамического анализа пакетов системного программного обеспечения, что позволило выявить отдельные потенциальные или реальные ошибки в этих пакетах, внести исправления, использовать более старую или новую версию этого пакета или использовать альтернативную версию пакета.

Для некоторых наиболее интенсивно работающих подсистем используются резервные версии RPM-пакетов. Программа мониторинга core-файлов определяет, какому RPM-пакету принадлежит исполняемый файл, вызвавший сбой, и если у такого RPM-пакета есть резервная версия, то новая версия заменяется на старую. Процесс управляется прикладной программой обеспечения жизнедеятельности (ПОЖ).

Дистрибутив LiNEM прошел процедуру верификации и тестирования в течение 20000 ч на аппаратных средствах стенда оценки надежности СПО и был допущен к использованию в составе аппаратных средств ПТК ИДС [6,7]. В настоящее время ОС LiNEM функционирует в составе КЭ СУЗ на 1-м энергоблоке АЭС «Тяньвань». Таким образом, дистрибутив LiNEM является одним из немногих отечественных специализированных дистрибутивов удовлетворяющих требованиям по надежности, отказоустойчивости и безопасности, предъявляемым к ПО систем важных для безопасности АЭС.

ЛИТЕРАТУРА

1. Кузнецов С. Д. Операционная система Unix. М.: Мир. 1999.
2. Операционная система Unix (руководство пользователя) //www.null.ru. 1998.
3. Larry Greenfield. Руководство пользователя Linux http:// www.linuxdoc.ru. 1994.
4. Lars Wirzenius. Руководство системного администратора ОС Linux // www.citforum.ru. 2001.
5. Иан Соммервилль. Инженерия программного обеспечения, 6-е издание// М.: Вильямс. 2002.
6. www.dwheeler.com/flawfinder.
7. http://www.splint.org.