Д-р.техн.наук В.Я. Геча, канд.техн.наук. С.Г. Семенцов

ПРИМЕНЕНИЕ UNIX-ПОДОБНЫХ СИСТЕМ В УПРАВЛЕНИИ ОБЪЕКТАМИ ЯДЕРНОЙ ЭНЕРГЕТИКИ

В соответствии с требованиями международных стандартов по обеспечению безопасности объектов ядерной энергетики при создании автоматизированной системы управления технологическими процессами (АСУТП) АЭС на первый план выходит требование открытости исходных текстов системного программного обеспечения (СПО). Такое же требование предъявляется к системному программному обеспечению локальной сети комплекса электрооборудования системы управления и защиты (ПО КЭ СУЗ) реактора типа ВВЭР-1000.

Для реализации этого требования была поставлена задача создания дистрибутива операционной системы для КЭ СУЗ на базе систем с открытыми исходными текстами, проведения тестирования и верификации, как самой операционной системы и прикладного ПО, так и интегрированных аппаратно-программных средств КЭ СУЗ. В значительной мере всем этим требованиям удовлетворяют системы на базе клонов операционной системы Unix, получивших название Unix-подобных систем [1].

Системное программное обеспечение систем управления и диагностики может быть реализовано как на базе специализированных платформ, так и под управлением Unix-подобных ОС общего применения. Открытость исходных кодов некоторых клонов Unix-систем, в частности ОС общего применения Linux, позволяет создать систему управления, ориентированную под конкретную задачу и обладающую набором необходимых функций [2,3].

В последние несколько лет в сфере системного программного обеспечения явно прослеживается тенденция к переходу от Windows-платформ и специализированных ОС к системам на базе ОС Linux. Причины этого очевидны: системы на базе ОС Linux сочетают в себе мощь архитектуры Unix и модульную структуру с открытостью исходных текстов, что позволяет создавать различные дистрибутивы ОС с широким набором прикладных программных модулей. Модульная структура ОС значительно упрощает процесс верификации и тестирования системы в соответствии с требованиями международных стандартов. Многозадачность, наличие графического интерфейса и средств разработки, работа с широким

спектром файловых систем, поддержка сети – все это делает ОС на базе Linux наиболее перспективной платформой для создания систем управления различного назначения [4,5].

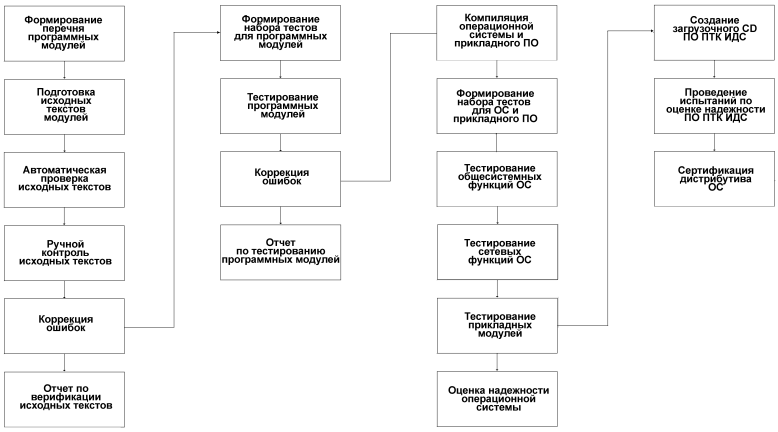
В международных стандартах (МЭК 60880, МЭК 60880-2), регламентирующих нормы разработки и тестирования систем управления защитой АЭС, рекомендуется максимальное использование ранее разработанного программного обеспечения (РПО). В этом аспекте применение ОС Linux оправдано с точки зрения стабильности системы, являющейся следствием оперативного исправления ошибок в исходных текстах. Аудит кода производится тысячами программистов во всем мире, поэтому уязвимые места системы, как правило, достаточно быстро удаляются. Такой подход выгодно отличает свободно распространяемые платформы от коммерческих продуктов.

Поскольку ОС Linux является системой общего применения, то для использования ее в системах управления АЭС необходимо проведение дополнительной верификации, как системных функций ОС, так и прикладных программных модулей [6]. Верификация системных функций включает в себя не только контроль исполнения тех или иных системных задач, но и аудит исходных текстов наиболее важных для безопасности системы компонентов. Для решения этой задачи на первом этапе определяется перечень программных пакетов (модулей) операционной системы необходимых для создания дистрибутива операционной системы. Перечень программных пакетов (модулей) формируется по принципу функциональности, т.е. пакеты делятся по функциональному назначению на общесистемные, интерфейсные, сетевые и т.д. Такое разделение обусловлено повышенными требованиями к функциям, отвечающим за устойчивое функционирование системы. В частности пакеты, необходимые только на этапе инсталляции и не влияющие на работу системы, пакеты, отвечающие за поиск нового оборудования при запуске системы, и т.д. могут быть проанализированы по упрощенной методике.

С учетом всех вышеперечисленных требований в НПП ВНИИЭМ на базе ОС ASP Linux 7.1 был создан специализированный дистрибутив системного программного обеспечения (СПО), получивший название «LiNEM», предназначенный для работы в составе программно-технического комплекса информационно-диагностической сети СУЗ реакторов типа ВВЭР-1000 [7]. Минимальный размер системы является одной из базовых характеристик LiNEM. Система изначально проектировалась максимально компактной и производительной, в то время как для других систем основной упор в проектировании делается на переносимость и другие факторы. При

создании дистрибутива LiNEM на всех этапах от аудита исходных текстов до интеграции с аппаратными средствами были использованы рекомендации МЭК 60880. В настоящее время ведутся работы по квалификации комплекса электрооборудования на базе СПО LiNEM по классу безопасности 3Н.

Для проведения верификации разработанного системного программного обеспечения была разработана методика верификации, включающая в себя выбор инструментов верификации и критериев приемки, методов аудита исходных текстов и тестирования, как отдельных программных модулей, так и интегрированной системы в целом. На рисунке приведена структурная схема процесса верификации.



Структурная схема процесса верификации

На первом этапе проводился автоматический контроль исходных текстов с использованием программных верификаторов. Для проведения автоматической проверки исходных текстов системного и прикладного ПО на предмет наличия потенциально опасных библиотечных вызовов был применен программный сканер безопасности flawfinder для языка C/C++ [3]. Такой выбор обусловлен:

- высоким уровнем алгоритмического базиса программы, поскольку ее автор является одним из ведущих специалистов в сфере обеспечения безопасности Linux-подобных ОС;
- возможностью контроля широкого спектра библиотечных вы-

зовов на различных платформах, что дает возможность объективно оценить уровень безопасности исходного кода;

- данный программный продукт постоянно обновляется, что позволяет учитывать особенности развития ПО и исправлять возможные ошибки.

На втором этапе осуществляется ручной контроль логической структуры наиболее важных с точки зрения обеспечения безопасности системных и прикладных модулей. По результатам аудита выработаны рекомендации по оптимизации кода системных и прикладных программных модулей. В частности предложено обновление версий для ряда пакетов, содержащих потенциально опасные языковые конструкции.

При проведении верификации СПО LiNEM был решен комплекс следующих задач:

- аудит исходных текстов на соответствие требованиям стандартов, а также проверка использования потенциально опасных библиотечных вызовов;
- оптимизация кода с учетом результатов аудита;
- проверка совместимости разработанного ПО с штатными аппаратными средствами;
- тестирование отдельных программных модулей и системных функций СПО;
- надежностные испытания системного и прикладного программного обеспечения.

На завершающем этапе проводились дополнительные испытания некоторых программных модулей. В частности контролировалось выполнение последними только тех функций, которые определены проектными спецификациями на них, и отсутствие функций, не предусмотренных проектом. Например для модулей СПО, предназначенных для обработки и визуализации диагностической информации задача подтверждения безопасности сводится к доказательству прозрачности модулей для входных данных в корректном формате и непрозрачности, устойчивости при неформатных входных данных.

Проведенные в НПП ВНИИЭМ комплексные испытания СПО LiNEM в течение 20000 ч показали, что разработанный дистрибутив обеспечивает стабильность работы системных служб и высокий уровень безопасности. В конце 2004 г. ПТК ИДС СУЗ с СПО LiNEM введен в эксплуатацию на 1-м блоке АЭС «Тяньвань» в КНР и 3-м блоке Калининской АЭС.

Заключение

Операционные системы семейства Linux все шире применяются в системах управления не только общего, но и специального назначения. Этот факт можно объяснить не только открытостью исходных текстов и архитектуры ОС, но и неоспоримыми преимуществами данной ОС по ряду параметров по сравнению с коммерческими системами. Немаловажным фактором является также модульная структура ОС Linux, что позволяет создавать на ее основе дистрибутивы для широкого спектра систем управления: от компактных ОСРВ [8], до многофункциональных ОС с графическим интерфейсом пользователя.

ЛИТЕРАТУРА

1. Кузнецов Д.. Операционная система Unix. М.: Мир. 1999.
2. Операционная система Unix (руководство пользователя) // www.null.ru. 1998.
3. Linux-подобные операционные системы в системах, важных для безопасности АЭС /Семенцов С.Г., Герман Н.Р., Саранцев П.В. //См. наст. том.
4. Lars Wirzenius. Руководство системного администратора ОС Linux // www.citforum.ru. 2001.
5. Larry Greenfield. Руководство пользователя Linux http:// www.linuxdoc.ru. 1994.
6. Концепция обеспечения безопасности Linux-подобных операционных систем в системах управления и защиты реакторов АЭС /Геча В.Я., Семенцов С.Г., Козлов С.А., Коноплев А.М. // См. наст. том.
7. Опыт создания специализированной операционной системы LiNEM для систем управления и защиты АЭС / Семенцов С.Г., Выпов П.А., Козлов С.А.// См. наст. том.
8. Общий подход к построению операционных систем реального времени в системах управления /Семенцов С.Г., Аксенов А.В., Кобзарев А.Н. // См. наст. том.