

# Задачи верификации ОС Linux в контексте ее использования в государственном секторе

*В. П. Иванников, А. К. Петренко*

*Труды Института системного программирования РАН*

*8 ноября 2006 г*

В последние годы наблюдается устойчивый рост интереса к Open Source модели разработки и распространения программного обеспечения (ПО). Интерес растет как к модели в целом, так и к операционной системе (ОС) Linux, в частности. Основным фактором, поддерживающим эту тенденцию, является низкая цена, а часто и бесплатный доступ к открытому ПО. Однако, одного фактора низких цен недостаточно. За последние 5-6 лет существенно повысилось качество ОС Linux, построена целая отрасль промышленности, которая занимается распространением, поддержкой, системной интеграцией решений, основанных на этой операционной системе. Эти изменения в технологии и структуре рынка информационных технологий (ИТ) изменили позицию государственных структур и крупнейших корпораций, определяющих основные процессы и приоритеты в области ИТ.

Государственные структуры, помимо экономии средств, которую сулят решения на базе Linux, видят в развитии ИТ на основе Linux следующие преимущества.

- Выбирая Linux платформу, государство уходит от зависимости от монопольного поставщика ПО (часто таким монополистом является Microsoft).
- Открытый код снимает многие проблемы, связанные с безопасностью ПО, в частности, проблемы так называемого вредоносного ПО (malware), существующего, например, в виде закладок и вирусов, и проблемы уязвимости ПО по отношению к различным видам атак.
- Linux предоставляет легальный, фактически неограниченный доступ к развитию базового ПО, в частности, к добавлению к базовой функциональности специальных возможностей.

До недавнего времени широкому распространению Linux в государственных структурах мешало отсутствие офисных приложений, поддерживающих работу с документами (речь идет о программах типа Microsoft Word, Excel, PowerPoint и др.). Сейчас ситуация меняется, в ОС Linux развивается новая линия - Desktop Linux, а также разрабатываются базовые офисные приложения (например, проект OpenOffice.org, веб-браузер Mozilla и др.), которые готовы обеспечить основные потребности пользователей офисных приложений.

Такие крупные корпорации как IBM, HP, Sun, Novell, Intel и другие развернули целые программы по поддержке Linux индустрии. В первую очередь их интерес также обусловлен снижением цены комплексной программно-аппаратной поставки в случае, если выбирается ОС Linux, а не Windows. Это дает конкурентные преимущества на рынке поставщиков комплексных решений. Также важны факторы, связанные с уходом от монополизма Microsoft. Для компаний-поставщиков аппаратных платформ (IBM, Intel) важна возможность модификации ОС с целью демонстрации уникальных преимуществ аппаратных решений. Примером международной программы, преследующей такие цели, является Gelato. Цель Gelato - развить Linux и другое базовое ПО с тем, чтобы показать конкурентные преимущества 64-хбитной аппаратной платформы Itanium. Еще одним

источником интереса для компаний поставщиков программно-аппаратных платформ и крупных комплексных решений является упрощение, а следовательно и удешевление собственно интеграции.

С ростом надежности и разнообразия возможностей, которые предоставляются операционной системой (ОС) Linux, она становится все более привлекательной для использования по различному назначению, в том числе для решения задач государственного управления и в системах управления критичных по безопасности.

Сторонники модели «открытого кода», на которой построена ОС Linux, рассматривая вопросы надежности, подчеркивают преимущество этой модели, обусловленное многократным и многосторонним анализом исходных текстов ОС огромным сообществом разработчиков Linux. Их утверждения верны, но лишь отчасти. В действительности, многие дефекты ОС удается выявить и даже предотвратить в процессе внесения новых изменений в исходные тексты. Но вся правда состоит в том, что многие дефекты ждут своего выявления в течение долгого времени и далеко не все удается выявить. Это приводит к выводу, что «открытый код», сам по себе, не является панацеей, а для доведения системы до необходимого уровня надежности необходимо использовать весь спектр современных средств контроля качества, в первую очередь современные средства тестирования.

Надежность операционной системы имеет несколько измерений и, соответственно, зависит от нескольких факторов, которые, в конечном счете, определяют качество решения задач в системах, базирующихся на данной ОС. Помимо основного фактора в работе ОС - безотказности, имеется и ряд других, в совокупности не менее важных. Речь идет, например, о

- безопасности вычислений (защита от несанкционированного доступа, от несанкционированного изменения поведения ОС и др.);
- переносимости приложений;
- соответствии требованиям различных стандартов (например, сетевым стандартам) и др.

Поскольку задача повышения надежности ОС Linux во всех измерениях требует огромных усилий и продолжительного времени, необходимо определить наиболее приоритетные направления в решении этой задачи. Таким направлением является доведение надежности Linux до уровня требований стандартов. Успешное решение этой проблемы существенно продвинет нас и в упрощении переносимости приложений, и в обеспечении безопасности вычислений.

На Unix- и Linux-системах проблема переносимости приложений, в частности, их установки стоит существенно острее, чем на Windows. Это, с одной стороны, ведет к усложнению процесса установки, и, с другой стороны, негативно сказывается на надежности систем в целом. Решение этой проблемы лежит в русле разработки и внедрения единого стандарта интерфейса взаимодействия между операционной системой и приложениями, который такую совместимость обеспечит. На роль такого стандарта может претендовать стандарт Linux Standard Base (LSB). Он наследует многие требования стандарта открытых систем POSIX, но за счет более строгих требований к интерфейсам позволяет решать проблемы переносимости эффективнее, чем стандарт POSIX.

Стандартизация не может ограничиваться только разработкой стандартов. Для того, чтобы удостовериться, что некоторая реализация удовлетворяет требованиям стандартов, нужно

проводить разнообразные проверки, включая испытания на различных данных, в различных окружениях. Кроме того, существуют и другие виды проверок: проверка наличия всех необходимых составляющих ядра ОС и библиотек, проверка контрольных сумм в дистрибутивных пакетах, проверка соответствия компонентов ядра и библиотек и др. Самым сложным (соответственно, самым качественным) видом проверок является проверка на тестовых примерах, иногда называемая динамическим тестированием.

Среди всех видов тестирования выделяется так называемое аттестационное тестирование, которое в первую очередь направлено на подготовку решения о выдаче (или не выдаче) официального свидетельства/сертификата о соответствии продукта требованиям стандарта. В случае LSB в сертификации нуждаются как поставщики операционных систем, реализующих LSB, так и поставщики приложений, которые объявляют, что их продукт будет работать на любой операционной системе, отвечающей требованиям LSB. Сертификация на соответствие LSB, естественно, повышает конкурентные преимущества сертифицированных продуктов.

Как правило, аттестационные испытания хорошо формализованы, они определяются набором детальных регламентирующих документов. Сертификацию на соответствие LSB проводит Open Group по поручению FSG (<http://www.opengroup.org/lsb/cert/>). В отличие от сертификации на соответствие POSIX, LSB сертификация не сопряжена с контактами со специальными аккредитованными сертифицирующими организациями и представляется более простой и прозрачной, как и всё в мире open source. Для того, чтобы показать, что тот или иной продукт удовлетворяет требованиям LSB, необходимо под контролем представителя FSG пропустить официальный набор тестов и предоставить отчеты по результатам пропуска тестов.

Отметим, что сертификационные тесты (как и любые тесты) не могут гарантировать, что реализация не нарушает требований стандарта - отчет по результатам тестирования в лучшем случае лишь констатирует, что «нарушений не обнаружено». К сожалению, такова общая практика в технологиях тестирования. В связи с этим помимо тестирования на соответствие (*conformance testing*) для более глубокой проверки выполняются функциональные, нагрузочные, стресс-тесты, тесты производительности и другие виды тестов. Они необходимы для того, чтобы получить более основательное заключение о тех или иных характеристиках программного продукта. Добротное функциональное тестирование существенно сложнее тестирования на соответствие. Именно по этой причине в дополнение к открытым сертификационным тестам необходимо создавать наборы эффективных тестов, в частности, дающих существенно более высокий уровень доверия к совместимости приложений, работающих под управлением ОС Linux.

Итак, ОС Linux уже сейчас готова к широкому использованию в государственном секторе. Однако это не означает, что все технические проблемы, в частности, проблемы переносимости приложений и проблемы надежности ОС уже полностью решены - здесь имеется широкое поле деятельности. В первую очередь речь идет о совершенствовании стандартов и решении вопросов инфраструктуры, обеспечивающей внедрение стандартов и упрощающей разработку ОС и приложений, которые этим стандартам удовлетворяют. Итог состоит в следующем:

- для повышения надежности систем, базирующихся на ОС Linux, и, в частности, переносимости приложений нужно вести работы по внедрению современных стандартов;
- основным стандартом, который нацелен на решение задач переносимости, является стандарт LSB;

- важнейшим механизмом внедрения стандарта LSB является разработка разноплановых и эффективных тестов и разворачивание работ по сертификации операционных систем и приложений на соответствие требованиям стандарта LSB.

Вместе с тем надо отметить, что решение перечисленных задач потребует достаточно много времени и усилий. Для того, чтобы утверждать это можно изучить историю и современное состояние группы стандартов POSIX (*Operating System Interface for Computing Environment*). POSIX развивается уже около 20 лет, однако до сих пор нельзя сказать, что как текст стандарта, так и качество его сертификационного набора теста являются безупречными. В таком положении находятся многие другие стандарты, задающие требования к программным интерфейсам. Разработка качественного набора тестов, проверяющего, насколько реализация интерфейса выполняет требования стандарта, также является непростой задачей. Еще более сложной является задача установления, насколько корректно приложение пользуется некоторым стандартным интерфейсом. В идеале хотелось бы, чтобы проверка реализации интерфейса на выполнение требования стандарта автоматически гарантировала, что любое приложение, корректно использующие данный интерфейс будет функционировать на данной реализации. Достижение этого идеала требует как развития методов спецификации требований, так и методов верификации реализаций интерфейсов и приложений.

Таким образом, стандартизация интерфейсов Linux и верификация Linux являются важными инфраструктурными задачами, которые нужно решать для успешного широкого распространения Linux. Решение этих задач является необходимым условием для успешного внедрения Linux в госструктурах, так как без решения проблем переносимости приложений широкое внедрение Linux невозможно.

Ниже приводится подборка материалов по растущему распространению ОС Linux в госструктурах и по проблемам тестирования и сертификации ОС Linux.

Краткая библиография по использованию Linux в госструктурах

1. USA: Linux в госструктурах  
<http://www.linuxjournal.com/article/7932>  
[RedHat с новостями про использование Linux в госструктурах](#)  
[колонка в CNN о Linux в госструктурах](#)  
[Linux в военных структурах USA](#)  
[о преимуществах Linux для госструктур](#)
2. Европа  
[http://www.businessweek.com/magazine/content/04\\_45/b3907083\\_mz054.htm](http://www.businessweek.com/magazine/content/04_45/b3907083_mz054.htm)  
<http://www.computerworld.com/industrytopics/financial/story/0,10801,103198,00.html>  
[Германия](#)  
[Швейцария](#)  
[краткий обзор по странам](#)
3. [Подборка новостей о переходе на Linux в госструктурах](#)
4. [Корея](#)
5. Китай  
<http://trends.newsforge.com/article.pl?sid=05/12/08/2034216&from=rss>  
<http://www.linuxelectrons.com/article.php/20051005183120307>  
<http://www.infoworld.com/articles/hn/xml/02/08/13/020813hncchina.html>  
<http://www.wsws.org/articles/2000/jul2000/lin-j15.shtml>
6. Индия  
<http://trends.newsforge.com/trends/06/01/27/1644258.shtml?tid=138>

- <http://economictimes.indiatimes.com/cms.dll/articleshow?artid=24598339>  
<http://atulchitnis.net/writings/oss-govt.php>  
[http://sify.com/news\\_info/fullstory.php?id=13562974](http://sify.com/news_info/fullstory.php?id=13562974)
7. Япония  
[http://www.newsfactor.com/story.xhtml?story\\_id=01300000AQCK](http://www.newsfactor.com/story.xhtml?story_id=01300000AQCK)  
[http://www.newsfactor.com/story.xhtml?story\\_id=38516](http://www.newsfactor.com/story.xhtml?story_id=38516)  
<http://people.valinux.co.jp/~sado/articles/japanwantsdebian.html>
  8. [Сайт Novell с новостями об использовании Linux в госструктурах](#)
  9. Австралийские госструктуры  
<http://www.novell.com/success/comsuper.html>  
<http://www.novell.com/success/mbf.html>
  10. [Европа, Бл. Восток и Африка](#)
  11. [Латинская и Южная Америки](#)

Краткая библиография по тестированию и сертификацию на соответствие LSB

1. [Сайт программы сертификации LSB.](#)
2. [открытие World's Second Linux Standards Testing Lab в Китае.](#)
3. [Страница Проекта Linux Kernel Testing.](#)
4. [Open POSIX Test Suite](#) - поддерживаемый Intel проект по созданию открытого тестового набора для проверки соответствия спецификациям, функционального и стресс-тестирования, а также тестирования производительности для функций, описанных в разделе System Interfaces стандарта IEEE Std 1003.1 (POSIX.1).
5. [Высказывания Ulrich Drepper](#), ведущего сотрудника Red Hat, в своем Live Journal о тестовом наборе для сертификации LSB.