УДК 004.451

С.Ю. Гавриленко[1], В.Г. Иванов[2], М.П. Шульга[1]

[1]*Национальный технический университет «ХПИ», Харьков*
[2]*Харьковский национальный университет радиоэлектроники, Харьков*

МЕТОД РАСШИРЕНИЯ ДИАПАЗОНА РАЗРЕШЕНИЙ НА ФАЙЛЫ ХОСТОВОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ, ИСПОЛЬЗУЮЩИЕСЯ В ГОСТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ

Рассмотрены способы обмена данными между гостевой и хостовой операционными системами. Предложен метод, позволяющий гостевым операционным системам отдельное обеспечение широкого контроля для каждого файла и каталога хостовой операционной системы за счет создания базы данных с правами доступа с помощью разработанного приложения и учета этих прав в программе для виртуализации.

Ключевые слова: *платформа виртуализации, виртуальная машина, хостовая операционная система, гостевая операционная система.*

Введение

Постановка проблемы. На сегодняшний день технология виртуализации значительно продвинулись вперед и нашла применение во многих областях [1]. Это обусловлено тем, что с одной стороны, пользоваться продуктами виртуализации (например, приложениями виртуальных машин) стало намного проще, они стали более надежными и функциональными, а с другой – значительно расширилась область их применения [2, 3]. Несколько одновременно запущенных виртуальных систем на одной физической машине существенно повышают гибкость ИТ-инфраструктуры и увеличивают эффективность использования аппаратных ресурсов [4]. В хостовой операционной системе физического компьютера платформа виртуализации устанавливается как обычная программа. С ее помощью создаются виртуальные машины (ВМ), в которых, в свою очередь, устанавливаются различные гостевые операционные системы Виртуальные машины могут использоваться для [5]:

- защиты информации и ограничение возможностей процессов;
- исследования производительности ПО или новой компьютерной архитектуры;
- эмуляции разных архитектур (например, эмулятор игровой приставки);
- оптимизации использования ресурсов мэйнфреймов и других мощных компьютеров (например, *IBM eServer*);
- моделирования информационных систем с клиент-серверной архитектурой на одной ЭВМ (эмуляция компьютерной сети с помощью нескольких виртуальных машин);
- упрощения управления кластерами – виртуальные машины могут просто мигрировать с одной физической машины на другую во время работы;
- создания переносных виртуальных машин, готовых к использованию на любой другой совместимой по архитектуре платформе.

В программах для виртуализации гостевым системам могут понадобиться данные, размещенные на хостовой ОС. Для этого существует сервис общих папок. С помощью этого сервиса можно задавать доступ каталогам хостовой ОС из гостевой ОС, которые будут там видны как сетевые папки. Для каждого каталога устанавливается тип доступа: полный или только для чтения, определяющий, можно ли производить изменения внутри этой папки. Вместе с тем возникает необходимость изменения типа доступа для отдельных файлов или каталогов, которые находятся в одном каталоге и имеют уже заданный тип доступа, что позволит избавиться от необходимости копирования данных на диск гостевой ОС, даст выигрыш во времени, а также экономию место на жестком диске за счет отказа от дублирования данных. Кроме того, ограничение доступа к отдельным файлам и каталогам обеспечит дополнительную безопасность данных.

Анализ литературы. Передача файлов является наиболее распространенным компьютерным сервисом для всех приложений – текстовых редакторов, электронной почты, баз данных или программ удаленного запуска [6]. На сегодняшний день существует несколько способов обмена данными между компьютерами. К ним можно отнести передачу данных по сети, использование сменных носителей. Все способы передачи данных, используемые для физических компьютеров, будут работать и для виртуальных машин [7, 8]. К сменным носителям, которые наиболее часто используются, можно отнести *USB Flash*, внешние винчестеры, подключаемые по *USB, CD\DVD* диски. К недостаткам носителей подключаемых по *USB* можно отнести их цену. Использование *CD*/*DVD* дисков требует очень много времени для обмена файлом (запись на диск, потом чтение).

Компьютеры реализуют коммуникационные протоколы в виде соответствующих программных эле-

ментов сетевой операционной системы, например, протоколы канального уровня, как правило, выполнены в виде драйверов сетевых адаптеров, а протоколы верхних уровней в виде серверных и клиентских компонент сетевых сервисов [9].

Поскольку современные ОС являются сетевыми, то наиболее удобными средством передачи файлов для виртуальных машин из существующих является передача данных по сети, используя такие протоколы как *FTP, SMB, NFS.*

Для большинства виртуальных машин реализована возможность доступа из гостевой ОС к файлам и каталогам хостовой ОС за счет установки прав доступа для каждого каталога [10].

Цель статьи: разработка метода расширения управления доступом к каждому каталогу и файлу хостовой операционной системы из гостевой операционной системы.

Результаты исследований

На каждый файл или каталог хостовой операционной системы можно выставить три типа прав доступа: полный доступ, только чтение, доступ запрещен.

Перечень разрешенных операций для них приведен в табл. 1.

Суть предлагаемого метода – создание в среде хостовой операционной системы базы данных прав доступа, изменения в которую могут вноситься специальной программой – менеджером. При применении данного метода данные, расположенные в одном каталоге, могут использоваться в разных гостевых операционных системах с различными степенями защиты.

Таблица 1

Разрешение операций для прав доступа объектов

Тип объекта	каталог			файл		
Тип доступа / Тип операции	полный доступ	только чтение	доступ запрещен	полный доступ	только чтение	доступ запрещен
Просмотр содержимого	✓	✓	×	✓	✓	×
Изменение содержимого	✓	×	×	✓	×	×
Удаление	✓	×	×	✓	×	×
Переименование	✓	×	×	✓	×	×

✓ – операцию разрешено исполнять;
× – операцию запрещено исполнять

Программная реализация алгоритма метода – приложение к виртуальной машине *VirtualBox*, описанное ниже.

Все записи о правах доступа находятся в базе данных прав доступа, которая представляет собой отдельный файл для каждой виртуальной машины. Имя файла совпадает с название виртуальной машины. Файл расположен в каталоге настроек данной виртуальной машины.

Структура данных об одном объекте (файл или каталог) в базе данных состоит из трех полей: пути расположения – строка в формате *UTF16*, имени объекта (также строка в формате *UTF16*), и атрибута прав доступа – 1 байт числового значения (рис. 1).

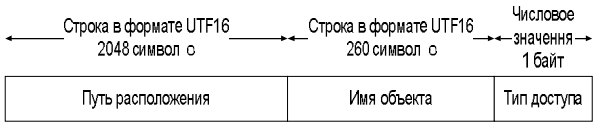

Рис. 1. Структура данных в базе данных прав доступа

Для изменения прав доступа разработана программа *Baseright*, – менеджер базы данных прав доступа, потребовавшая модификации текста программы *VirtualBox*, а именно, трех функций: *vbsfCreate*, *vbsfRename*, *vbsfRemove*. Они используются при работе гостевых ОС с файлами или каталогами общих каталогов: *vbsfCreate* вызывается при создании или открытии, *vbsfRename* – при переименовании, *vbsfRemove* – при удалении. В эти три функции перед выполнением операций с файлами или каталогами добавлена проверка прав доступа с помощью функции *GetKeyMon*, которая возвращает числовое значение атрибуту прав доступа из базы данных. Кроме того, при создании, удалении и переименовании объекта меняется запись в базе данных объектов.

Проведенное тестирование для гостевых ОС *Linux* и *Windows* показало работоспособность программы для файлов или каталогов с соответствующими атрибутами доступа. На рис. 2 приведена информация о правах доступа для каталога *D*:*FSetb**VirtualBox*. На рис. 3 приведено сообщение в случае открытия файла, доступ для которого запрещен.

Достоинства предложенного метода: отпадает необходимость в копировании данных для гостевой ОС; сокращается время на подготовку данных для приложений тестирования, поскольку отпадает необходимость в копировании данных; данные, расположенные в одном каталоге, могут использоваться в разных гостевых операционных системах, с более высокой защитой.

Недостатки метода – наличие временных затрат для выставления права доступа для отдельных файлов или каталогов; возможность ошибочных действий по отношению к файлам хостовой ОС.

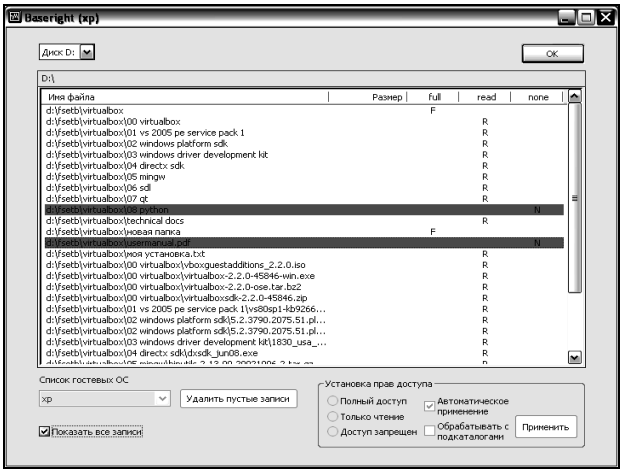

Рис. 2. Информация о правах доступа для каталога *D:\FSetb\VirtualBox*

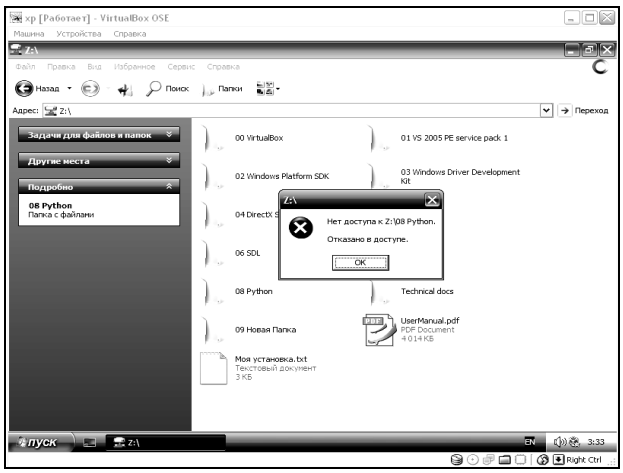

Рис. 3. Попытка открытия каталога с запрещенным доступом

Выводы

Предложен и обоснован метод расширения диапазона разрешений прав доступа к гостевой ОС, позволяющий ограничить права доступа для отдельных файлов и каталогов, которые находятся в общей папке. Разработано программное приложение и модифицировано существующее, что в итоге дает возможность гибкого управления доступом для файлов и каталогов хостовой операционной системы из гостевых операционных систем. Данная разработка может быть использована, например, в многоуровневых операционных системах с жестким разграничением доступа. **Направление дальнейших исследований –** проведение оценки дополнительных временных затрат при использовании предложенного метода.

Список литературы

1. Виртуализация и Vicrosoft Virtual Server 2005 / Роджер Диттнер, Кен Мейджорж и др. – М.: Бином, 2008. – 423 с.

2. Гультяев А. Виртуальные машины. Несколько компьютеров в одном / А.Гультяев. – СПб.: Питер, 2006. – 224 с.

3. Самойленко А. Тестирование ПО на виртуальных машинах [Электронный ресурс] / А. Самойленко. – Режим доступа к док.: http://www.ixbt.com/cm/virtualization-soft-testing.shtml.

4. Самойленко А. Виртуальные машины дома и в бизнесе [Электронный ресурс] / А. Самойленко. – Режим доступа к док.: http://www.ixbt.com/cm/virtualization-vm-home-business.shtml.

5. Самойленко А. Виртуальные машины на платформе Microsoft Virtual PC 2007 [Электронный ресурс] / А. Самойленко. – Режим доступа к докоменту: http://www.windowsfaq.ru/content/view/566/46/

6. Иртегов Д. Введение в операционные системы / Д. Иртегов. – СПб: Питер, 2002. – 223 с.

7 Ляш О.И. Опыт и перспективы использования виртуальных машин в профессиональной подготовке будущих учителей информатики [Электронный ресурс] / О.И. Ляш. – Режим доступа к документу: http://znetwork.ucoz.ru/publ/1-1-0-8.

8. Users Manual Xen v3.0 [Электронный ресурс]. – Режим доступа к документу: http://www.cl.cam.ac.uk/research/srg/netos/xen/readmes/user/user.html.

9. Солдатов В.П. Программирование драйверов Windows / В.П. Солдатов. – 2-е изд., перераб. и доп. – М.: ООО "Бином-Пресс", 2004. – 480 с.

10. Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000 / Д. Соломон, М. Руссинович. – 4-е изд. – СПб.: Питер. – Мастер-класс, 2005. –462 с.

Поступила в редколлегию 24.09.2009

Рецензент: д-р техн. наук, проф. И.В. Гребенник, Харьковский национальный университет радиоэлектроники, Харьков.

МЕТОД РОЗШИРЕННЯ ДІАПАЗОНУ ДОЗВОЛІВ НА ФАЙЛИ ХОСТОВОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ГОСТЬОВИХ ОПЕРАЦІЙНИХ СИСТЕМАХ

С.Ю. Гавриленко, В.Г. Іванов, М.П. Шульга

Розглянуто способи обміну даними між гостьовою та хостовою операційними системами. Запропоновано для гостьових операційних систем окреме забезпечення широкого контролю для кожного файлу і каталогу хостової операційної системи за рахунок створення бази даних із правами доступу за допомогою розробленого додатку та обліку цих прав у програмі для віртуалізації.

Ключові слова: *платформа віртуалізації, віртуальна машина, хостова операційна система, гостьова операційна система.*

METHOD EXPANSION OF THE RANGE OF PERMISSIONS TO FILES HOST HOST OPERATIONAL USED IN GUEST HOST OPERATIONAL

S.J. Gavrilenko, V.G. Ivanov, M.P. Shulga

Ways of data exchange between guest and host OS are considered. Necessity of expansion of a range of permissions to files and catalogues host OS from guest OS is proved. Separate maintenance of the wide control for each file and the catalogue

host OS at the expense of creation of a database with access rights by means of the developed application and the account of these rights in the program for виртуализации is offered for guest operational systems.

Keywords: *the platform of virtualization, the virtual car, host operational system, guest operational system.*