Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

Введение

Актуальность исследования.

В последние годы в средствах массовой информации стали активно использоваться термины "виртуализация", "виртуальный" в применении к самым разнообразным областям и с вкладыванием различного смысла в эти термины. Термин "виртуальный" (лат. Virtualis) имеет два значения: 1) возможный; такой, который может или должен проявиться при определѐнных условиях, но в реальности не существующий; 2) созданный на экране компьютера; воспроизводимый компьютерными средствами [51]. Из множества словосочетаний, в состав которых входит прилагательное виртуальный, наиболее близким к точным техническим терминам является понятие виртуальной машины, с которым зачастую напрямую и связывается термин виртуализация. Виртуальная машина (ВМ) определяется как совокупность ресурсов, которые эмулируют поведение реальной машины [85]. Концепция ВМ появилась в Кембридже, штате Массачусетс, в конце 1960-х годов как расширение концепции виртуальной памяти манчестерской вычислительной машины Atlas. В последние годы ВМ снова набирают популярность, поскольку на смену мэйнфреймам пришли серверы и серверные комплексы, обслуживающие большие группы потребителей. Стремительный рост числа пользователей информационными технологиями, происходящий одновременно с непрекращающимся ростом производительности современных компьютеров, привѐл к возобновлению интереса к проблеме виртуализации. Под виртуализацией при этом понимается технология, которая позволяет разделить один физический сервер на несколько виртуальных машин, на каждой из которых может быть создана своя виртуальная среда, имитирующая для пользователя полную среду вычислительной системы со своей операционной системой (ОС) [25].

По мнению многих экспертов и исследователей в области информационных технологий [1 , 3 , 10, 19, 53, 54, 79, 83, 88, 90-94, 103, 106], виртуализация становится одной из самых важных технологий в области ИТ-инфраструктуры. Производители электронных устройств и компьютерных компонентов выпускают все больше новых устройств, поддерживающих технологию аппаратной виртуализации [35, 53 , 62, 102, 104, 105]. Разработчики ОС активно развивают свои

продукты с учетом появления возможностей виртуализации [57, 79, 109, 75, 92, 94]. На рынке ОС появились новые игроки, специализирующиеся на построении виртуальной ИТ-инфраструктуры предприятий [74, 90, 91, 94, 109]. На базе технологии виртуализации развивается концепция обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю через компьютерную сеть (КС) в виде сервиса, позволяющего использовать Web-интерфейс для удаленного доступа к выделенным ресурсам (концепция облачных вычислений) [71]. ВМ могут эффективно использоваться в качестве стандартных блоков для построения систем с высоким уровнем защиты. На базе технологии виртуализации можно создавать компьютерные среды с различными категориями защиты, тем самым решая проблему обеспечения информационной безопасности и надѐжности. Именно эти функции становятся даже более важными, чем организация многозадачности, для чего виртуализация когда-то была задумана [24]. С каждым годом все больше организаций при строительстве внутренней сети используют решения, основанные на технологии виртуализации [18, 27, 29, 54].

Активное развитие технологий в области виртуализации и использование их различными организациями при построении своих КС подтверждают необходимость рассмотрения данных информационных технологий в аспекте защищенности информации [67, 87, 89]. На сегодняшний день обеспечение доступности является одной из наиболее важных проблем [15]. Существуют большое количество угроз, связанных с нарушением доступности информационных ресурсов КС [8, 9, 39, 41-43]. Во-первых, это угрозы атак типа "отказ в обслуживании" различных видов: переполнение буфера, превышение пропускной способности канала связи, загрузка процессора, отправка поддельных команд, вызов ложного срабатывания [2, 4, 23, 46 , 99]. Во-вторых, нагрузки, возникающие в результате одновременного обращения пользователей КС к ее информационным ресурсам [2]. В-третьих, отказ оборудования, на котором построена КС [5, 6, 40]. Применение технологии виртуализации при построении КС является одним из вариантов решения данной проблемы. Это достигается за счет:

- более рационального использования ресурсов аппаратного обеспечения, на базе которого строится КС;

- возможности реализации прозрачной отказоустойчивости (такой отказоустойчивости системы, при которой продолжается функционирование системы даже в случае выхода из строя одного или нескольких ее элементов);

- возможности оперативного перераспределения нагрузки (динамическая инфраструктура) [19 , 21 , 24, 25, 27, 28, 35 , 44, 47, 60 , 62 , 65, 66, 70, 72, 73, 76, 83, 93, 95, 103].

В данной работе под "программным средством, реализующим технологию аппаратной виртуализации" подразумевается комплекс программных продуктов (операционная система виртуализации, система централизованного управления виртуальной средой, консоль управления), использующих поддержку технологии виртуализации со стороны оборудования. При помощи этих средств осуществляется построение и управление виртуальной средой [15, 24, 35, 60, 68, 70, 79, 93, 107]. На сегодняшний день существуют несколько таких комплексов программных продуктов:

- VMware vShare – программный продукт компании VMware;

- Microsoft Windows Server 2008R2– программный продукт компании Microsoft;

- Citrix Server – программный продукт компании Citrix Systems.

Каждый из этих программных продуктов разработан на базе различных ОС, имеет собственную уникальную архитектуру и по-разному обеспечивает защищенность информационных ресурсов. Каждый из них обладает своими возможностями и особенностями. Известные результаты сравнения программных продуктов не содержат оценок защищенности информационных ресурсов от деструктивных информационных воздействий[1] (ДИВ), направленных на нарушение доступности [24, 25, 59, 60, 81]. С учетом изложенного тема данной дипломной работы, заключающейся в проведении сравнительного анализапрограммных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение защищаемой информации в КС.

[1]Деструктивное информационное воздействие - это несанкционированное информационное (специально организованной информацией – вредоносными программами, специальными сигналами) воздействие на информационную, информационно-телекоммуникационную систему, приводящее к выводу системы из строя или к нарушению функционирования этой системы в результате разрушения (нарушения) ее информационно-технологической структуры.

Цель и задачи исследования. Целью настоящей работы является проведение сравнительного анализа программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступностизащищаемой информации в КС.

Для достижения поставленной цели в работе решались задачи:

- формирование описательной модели программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС;

- разработка алгоритма оценки программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС;

- экспериментальные исследования программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС;

- оценка экономических показателей эффективности сравнительного анализа программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступностизащищаемой информации в КС;

- рассмотрение исследуемой проблематики с точки зрения обеспечения безопасности жизнедеятельности.

Объект исследования. Объектом исследования является программное средство, реализующее технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС.

Предмет исследования. Предметом исследования является алгоритм оценкипрограммных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС.

Методы исследования. Для реализации намеченной цели исследования и решения поставленных задач используются методы теории рисков, теории вероятности, математической статистики и системного анализа, методы имитационного моделирования, методы планирования эксперимента.

Научная новизна. В работепредставлена описательная модель программных средств, реализующих технологию аппаратной виртуализации, отличающаяся тем, что рассматривает программные средств, реализующие технологию аппаратной

виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации в КС.

Впервые представленалгоритм оценки программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступностизащищаемой информации в КС.

Предложена имитационная модель КС, использующей технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации, отличающаяся тем, что оценивает защищенность информации от ДИВ, направленных на нарушение ее доступности на основании показателя функции риска.

Впервые представлены рекомендации по выбору программных средств, реализующих технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации.

На защиту выносятся следующие основные результаты работы:

- описательная модель программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС;
- алгоритм оценки программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступностизащищаемой информации в КС;
- имитационная модель КС, использующей технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации;
- результаты сравнения программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС.

Практическая ценность работы заключается в разработке рекомендаций по выбору программного средства для построения КС, важным критерием функционирования которой является обеспечение доступности информации.

Результаты исследования программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение

доступностизащищаемой информации в КС были использованы в ходе выполнения плановой НИР ГНИИИ ПТЗИ ФСТЭК России- Слух.

Разработанные алгоритм оценки программных средств и имитационная модель КС, использующей технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации, могут быть использованы для развитияметодического обеспечения оценки программных средств, реализующих технологию аппаратной виртуализации.

Структура и объем работы. Работа состоит из введения, пяти глав, заключения и списка литературы, включающего 109 наименований.

Содержание работы изложено на 174 страницах машинописного текста, проиллюстрировано 46 рисунками и 36 таблицами, 1 приложением.

Заключение

Работа посвящена исследованию программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС. В ходе еѐ выполнения были получены следующие основные результаты:

1. Разработана описательная модель программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение защищаемой информации в КС. Приведено описание и основные характеристики технологии аппаратной виртуализации, суть которой заключается в оказании поддержки технологии виртуализации со стороны аппаратного обеспечения для того чтобы более эффективно реализовать представление аппаратных ресурсов компьютера в виде ВМ, а также для решении некоторых сложностей, возникающих в результате такого представления. Представлено описание моделируемых ДИВ, направленных на нарушение доступности защищаемой информации, и отмечены те ДИВ, которым позволяет противодействовать использование технология виртуализации. Рассмотрена архитектура программных средств, реализующих технологию аппаратной виртуализации.

2. Предложеналгоритм оценки программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение защищаемой информации в КС. Алгоритм используются для проведения сравнительного анализа СВ. Алгоритм основан на вычислении показателя защищенности информации при помощи функции риска в результате проведения компьютерных экспериментов с имитационной моделью КС, использующей технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации.

3. Разработана имитационная модель КС, использующей технологию аппаратной виртуализации, в условиях ДИВ, направленных на нарушение доступности защищаемой информации. Проведены экспериментальные

исследования на разработанной имитационной модели. В результате анализа данных, полученных во время проведения компьютерных экспериментов, предложены рекомендации по выбору СВ для построения КС, использующей технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации.

4. Проведена оценка экономических показателей эффективности работ проведения сравнительного анализа программных средств, реализующих технологию аппаратной виртуализации, при ДИВ, направленных на нарушение доступности защищаемой информации в КС. Проведен расчет экономического ущерба от реализации ДИВ, направленного на КС, использующую технологию аппаратной виртуализации.Расчеты показали, что данная работа является экономически эффективной.

Список литературы

1 Александров А.А. Спирали аппаратной виртуализации. Открытые системы. 2007, №3.

2 Андреев Д.А, Тишков С.А., Сердечный А.Л., Плотников Д.Г. К вопросу о классификации атак типа "отказ в обслуживании". Информация и безопасность. 2010, №1, с. 47-54.

3 Барсков А. Упростить и виртуализировать. Журнал сетевых решений/LAN. 2010, №7+8.

4 Безкоровайный Д. Обнаружение инцидентов ИБ в виртуальной инфраструктуре. Информационная безопасность. 2010, №1, с.28-29.

5 Богатырев В.А. Надежность и эффективность резервированных компьютерных сетей//Информационные технологии. -2006 -№ 9. -С. 25-30.

6 Богатырев В.А., Колмогорцев Е.Л.. Выбор рационального варианта конфигурации отказоустойчивой системы управления. Информационные технологии моделирования и управления. 2007, №1, с.134-139.

7 Борохов С.В., Синицын И.Н., Рыков А.С. Экспертная оценка эффективности построения системы безопасности информационно-телекоммуникационных систем высокой доступности. Наукоемкие технологии. 2006, №2, с.5-29.

8 Володин А.В., Устинов Г.Н. О гарантии доставки сообщений // Документальная электросвязь, 1999, 1. ООО НПФ «АДЕЛИЗ», с. 10-12.

9 Володин А.В., Устинов Г.Н., Цибин В.В. Сеть передачи данных —модель угроз информационной безопасности // Вестник связи. 1999, № 4, 52-57.

10 Волохов В.М., Варламов Д.А., Сурков Н.Ф., Пивушков А.В. Виртуальные вычислительные среды: использование на GRID полигонах. Вестник Южно-Уральского государственного университета. Серия: Математическое моделирование и программирование. 2009, №17, с.24-35.

11 Вентцель Е.С. Теория вероятностей и ее инженерные приложения: учеб. пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. – М.: Высшая школа, 2003. – 464с.

12 Вентцель Е.С. Теория вероятностей: учеб. для втузов / Е.С. Вентцель – М.: Высш. шк, 1998. – 576 с.

13 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения: учеб. пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. – М.: Высш. шк, 2000. – 383 с.

14 Выгодский М.Я. Справочник по высшей математике / М.Я. Выгодский. – М.: Наука, 1973. – 872 с.

15 Галатенко В., Дорошин И. Доступность как элемент информационной безопасности. Jet Info. Информационный бюллетень. № 2(33) 1997. с.5-22.

16 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – 12-е изд., стереотип. – М.: Высшая школа, 2005. – 479 с.

17 ГОСТ Р 50922-96 Защита информации. Основные термины и определения.

18 Грам В. Технологии виртуализации и повышение эффективности функционирования корпоративных предложений [Электронный ресурс]. Режим доступа: http://knowledgeforit.com/content/view/373574/169/.

19 Григин И.Е. Динамические виртуальные среды данных в распределенных системах. Известия высших учебных заведений. Приборостроение. 2007, №1, с.14-17.

20 Джонс Т.М. Виртуальный Linux: обзор методов виртуализации, архитектур и реализаций [Электронный ресурс]. Режим доступа: http://www.ibm.com/developerworks/ru/library/l-linuxvirt/index.html.

21 Долгополов В.С., Захаров В. П., Козлова Л.М., Козмидиади В.А., Обухова О.Л. Методы реализации отказоустойчивости приложений с недетерминированным поведением. Системы и средства информатики. 2006, №1, с.374-385.

22 Егоров В.Ю. Особенности диспетчеризации процессов при функционировании виртуальных машин. Системы и средства информатики. 2009, №2, с.58-67.

23 Ефремов А. Сетевые атаки и средства борьбы с ними // Computer Weekly № 14, 1998, с. 14-17.

24 Захаров В.Н. Виртуализация как информационная технология. Системы и средства информатики. 2006, №3, с.279-298.

25 Захаров В.Н. Вопросы эффективной реализации технологии виртуальных машин. Наукоемкие технологии. 2006, №2, с.51-67.

26 Злобина И.А. Экономика информационной безопасности: учеб. пособие / И.А. Злобина – Воронеж: Воронежский государственный технический университет, 2005. – 196 с.

27 Зорин В. Технологии виртуализации и защищенность информационных систем. Информационная безопасность. 2009, №7+8, с.30-31.

28 Зыль С. Безопасность систем жесткого реального времени. Открытые системы. СУБД. 2008, №7.

29 Ильин В.А., Крюков А.П., Шамардин Л.В., Демичев А.П., Горбунов И.Н. Способ запуска и обработки в гриде заданий, подготовленных для различных сред исполнения. Вычислительные методы и программирование: новые вычислительные технологии. 2008, №2, с.41-47.

30 Информационная безопасность и защита информации. Сборник терминов и определений. – М.: Гостехкомиссия России. 2001.

31 Карайчев Г.В., Нестеренко В.А. Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети. Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки. 2008, №1, с.10-13.

32 Карпов Ю. Имитационное моделирование систем. Введение в моделирование с Anylogic 5. -СПБ.: БВХ-Петербург, 2005. - 400 с.: ил.

33 Колмогорцев Е.Л. Модель производительности распределенной иерархической системы управления с резервированием коммуникационной подсистемы//Информационные технологии моделирования и управления. -2006 -№ 9(34). -С. 1172-1178.

34 Корн Г. Справочник по математике для научных работников и инженеров / Г. Корн. – М.: Наука, 1977. – 832 с.

35 Костров Д. Виртуализация ЦОД. Информационная безопасность. 2009, №1, с.32.

36 Криспин Л., Грегори Д. Гибкое тестирование: практическое руководство для тестировщиков ПО и гибких команд. — М.: «Вильямс», 2010. — 464 с.

37 Ларкин Е.В., Котов В.В., Котова Н.А., Соколов В.А. К вопросу о моделировании отказоустойчивых систем с помощью сетей Петри-Маркова. Фундаментальные исследования. 2007, №5, с.37.

38 Лукацкий А.В. Атаки на информационные системы. «Электроника. Наука. Технологии и Бизнес». 2000, 1, с.42-44.

39 Лукацкий А.В. Обнаружение атак — СПб.: БХВ-Петербург, 2001.-624 с.

40 Матвеевский В.Р. Надежность технических систем. Учебное пособие – Московский государственный институт электроники и математики. М., 2002 г. – 113 с.

41 Медведовский И., Семьянов П., Леонов Д. Атака на ИНТЕРНЕТ. Изд. 2-е. М.: «ДМК», 1999,0.18.

42 Медведовский И., Семьянов П., Платонов В. Атака через ИНТЕРЖТ. Под ред.П.Д.Зегжды.СПб.:Мир и семья, 1997.- 200с.

43 Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. 3-е изд. М.: Изд. ДМК, 2000.

44 Мейлихов И. Невиртуальные угрозы виртуализированных инфраструктур. Безопасность виртуальной инфраструктуры: новые вызовы, новые решения. Информационная безопасность. 2009, №5, с.32-34.

45 Месарович М. Общая теория систем: математические основы / М. Месарович, Д. Мако, Я. Такахара. – М.: Мир, 1973. – 344 с.

46 Милославская И.Г. Толстой А.И. Интрасети: обнаружение вторжений.,. Учебное пособие для вузов. - М.: ЮНИТИ-ДАНА. 2001. - 400 с.

47 Миркин А.Л., Петров В.А. Система миграции виртуальных серверов в режиме реального времени. Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2008, №3, с.103-109.

48 Мишин К.Н. Имитационное моделирование аномальных явлений в компьютерных сетях. Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. 2007, с. 120-128.

49 Ненашев С., Ковтунович Л. Нагрузочное тестирование систем обеспечения информационной безопасности. Информационная безопасность. 2009, №1, с.28-29.

50 Никифоров В.В., Шкиртиль В.И. Оценка времени отклика прикладных задач в системах реального времени с многоядерными процессорами. // Известия высших учебных заведений. Приборостроение. 2008, №12, с. 38-44.

51 Новейший словарь иностранных слов и выражений. — М.: АСТ, 2002.

52 Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. - СПБ.: Питер, 2010. -944 с.: ил.

53 Орлов С. Виртуализация под защитой. Журнал сетевых решений/LAN. 2010, №6.

54 Орлов С. Системы хранения и серверы: технологические тенденции. Журнал сетевых решений/LAN. 2010, №6.

55 Остапенко А.Г. Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств / А.Г. Остапенко, Ю.К. Язов, Р.В. Батищев, О.А. Середа // Информация и безопасность. – 2001. – №2. – С. 4-11.

56 Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. – 2005. – Вып. 2. – С. 28-32.

57 ОтиМ. Microsoft System Center против VMware vSphere. Windows IT Pro. 2010, №2.

58 Парфенов В.И. Защита информации (Словарь). – Воронеж: НП РЦИБ "Факел", 2003.– 293 с.

59 Петров В.А., Тормасов А.Г., Миркин А.Л. Длительность миграции виртуальных серверов в распределенной системе. Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2009, №1, с.26-36.

60 Пичугов К. Безопасность виртуальной инфраструктуры: новые вызовы, новые решения. Информационная безопасность. 2009, №5, с.54-55.

61 Плешков А. Ошибки планирования в рамках стратегического управления проектами по информационной безопасности. Нагрузочное тестирование систем обеспечения информационной безопасности. Информационная безопасность. 2009, №1, с.42-43.

62 По материалам корпорации Cisco Systems. Стратегия Cisco в области ЦОД. BYTEmag.ru. 2009, №3, http://www.bytemag.ru/articles/detail.php?ID=14178.

63 Приходько А.Я. Словарь-справочник по информационной безопасности / А.Я. Приходько. – М.: СИНТЕГ, 2001. – 124 с.

64 Пугачев В.С. Теория вероятностей и математическая статистика: учеб. пособие. – 2-е изд., исправл. и дополн. – М.: ФИЗМАТЛИТ, 2002. – 496 с.

65 Риндле К. Динамические инфраструктуры. Журнал сетевых решений/LAN. 2010, №7+8.

66 Руднев М. Хранение данных и, резервное копирование в сетях. Компьютер-Пресс, 2000, № 7 (Тематический выпуск: хранение и защита данных), с.40-43.

67 Рыбалко А.А. Виртуализация как основа систем компьютерной безопасности нового поколения. Вестник Московского авиационного института. 2009, №2, с.2.

68 Рыбалко А.А. Виртуализация серверов внешнего периметра в модели защиты корпоративной сети//Материалы XVI Международной конференции по механике и современным прикладным программным системам (ВМСППС2009), 25-31 мая 2009 г., Алушта. М.: Изд-во МАИ-ПРИНТ, 2009. С. 614-616.

69 Рыбалко А.А. Виртуализация Web-сервисов как средство эффективной защиты от внешних атак. Технологии Microsoft в теории и практике программирования: Тр. V Всерос. конф. Студентов, аспирантов и молодых ученых. Центральный регион. Москва, 1-2 апреля 2008 г. М.: Вузовская книга, 2008. С. 151-152.

70 Рыбалко А.А. Моделирование системы защиты облачных сервисов с использованием механизмов виртуализации. Вестник Московского авиационного института. 2009, №6, с.20.

71 Рыбалко А.А. Технологии виртуализации в фокусе задач компьютерной безопасности//Материалы VII Международной конференции по неравновесным процессам в соплах и струях (NPNJ2008), 24-31 мая 2008 г., Алушта. М.: Изд-во МАИ, 2008. С. 350-352.

72 Рыбалко А.А. Управление виртуальной инфраструктурой, автоматизация средств обеспечения надежности и безопасности серверов внешнего периметра. Технологии Microsoft в теории и практике программирования//Тр. VI Всерос. конф. студентов, аспирантов и молодых ученых. Центральный регион. Москва, 1-2 апреля 2009 г. М.: Вузовская книга, 2009.

73 Самойленко А.Технический обзор возможностей VMware vSphere 4.1 [Электронный ресурс]. Режим доступа: http://www.vmgu.ru/articles/vmware-vsphere-41-tech-guide.

74 Самойленко А.Экономика инфраструктуры виртуализации: TCO, ROI, Payback, NPV, и каким образом VMware может работать как банк? [Электронный ресурс]. Режим доступа: http://www.vmgu.ru/articles/vmware-bank-infrastructure.

75 Селезнев А.В. Организация резервного копирования в локальных и корпоративньос сетях. Сети и системы связи. 1996, № 10, с.110.

76 Строгалев В.П., Толкачева И.О. Имитационное моделирование: Учеб. пособие. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 280 с.: ил.

77 Таненбаум Э. Архитектура компьютера. -СПб.: Питер, 2003. -704 с.

78 Таненбаум Э. Современные операционные системы. 3-е изд. - Спб.: Питер, 2010. -1120 с.: ил.

79 Тарасов А.Г. Расширяемая система мониторинга вычислительного кластера. Вычислительные методы и программирование. 2009, №2, с.1-12.

80 Тестирование производительности систем виртуализации ESXi, KVM, Xen [Электронный ресурс]. Режим доступа: http://www.64bit.ru/?p=383.

81 Тетюшев А.В. Отказоустойчивые самовосстанавливающиеся информационные системы. Информационные технологии моделирования и управления. 2007, №1, с.120-126.

82 Тихович Д. Технологии виртуализации VMware: динамическая ИТ-инфраструктура уже сегодня. VMware, Inc. 2008, .-С 24.

83 Толкачев И.В., Батищев Р.В., Балашов Ю.С. Применение "времени отклика" как основного параметра реакции автоматизированной системы на атаку "отказ в обслуживании". 2008, №1, с.138-140.

84 Толковый словарь по вычислительным системам / Под ред. В. Иллингуорта, Э.Л. Глейзера, И.К. Пайла / Пер. санг лийского. — М.: Машиностроение, 1989.

85 Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. -М.: Радио и связь, 1991. -132 с.

86 Федеральный закон "Об информации, информационных технологиях и защите информации" №146. – 2006.

87 Халяпин С. Современные подходы к виртуализации. Банковские технологии. 2008, №11, с.8-12.

88 Царегородцев А.В. Информационная безопасность в распределенных управляемых системах: монография / А.В. Царегородцев. – М.: РУДН, 2003. – 217 с.

89 Черняк Л. Виртуализация на фоне новых протоколов. Открытые системы. СУБД. 2008, №8.

90 Черняк Л. Виртуализация серверов стандартной архитектуры. Открытые системы. СУБД. 2008, №3, с.40-47.

91 Черняк Л. На пути к тотальной виртуальности. Открытые системы. СУБД. 2009, №5.

92 Черняк Л. Реальная безопасность виртуальных серверов. Открытые системы. СУБД. 2009, №3.

93 Черняк Л. Современная виртуализация хранения. Открытые системы. СУБД. 2009, №8.

94 Ширмаков А. Безопасность виртуальной инфраструктуры. Открытые системы. СУБД. 2009, №6, с.30-31.

95 Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: учеб. пособие для вузов/ А.Г. Шоломицкий – М.: Изд. дом ГУ ВШЭ, 2005. – 400 с.

96 Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества / Р. Шторм. – М.: Издательство "МИР", 1970. – 368 с.

97 Шубинский И.Б.Элементы теории функциональной отказоустойчивости информационных систем. Известия Санкт-Петербургской лесотехнической академии. 2001, №167, с.176-183.

98 Язов Ю.К., Бурушкин А.А., Панфилов А.П. Марковские модели процессов реализации сетевых атак типа "отказ в обслуживании". Информация и безопасность. 2008, №1, с.79-84.

99 Язов Ю.К., Седых И.М. Метод количественной оценки защищенности информации в компьютерной системе. Телекоммуникации. 2006, №6, с.46-48.

100 Эрингтон Д., Джаккуот Б. Виртуальная серверная среда HP: сделайте адаптивную инфраструктуру реальностью в вашем центре обработки данных. М.: ИНТУИТ.РУ, 2007.— 518 с.: ил., табл.

101 AMD64 Virtualization Codenamed «Pacifica» Technology. Secure VirtualMachine Architecture Reference Manual. Advanced Micro Devices33047 — Rev. 3.01 — May 2005.

102 Bittman T. Server Virtualization: Emerging to Mainstream at Lightspeed//Gartner Symposium ITxpo, 2009, p.20.

103 Intel Vanderpool Technology for IA-32 Processors (VT-x) Preliminary Specification, Intel Order Number C. 97063-001, January 2005.

104 Intel Virtualization Technology Specification for the Intel Itanium Architecture (VT-i), Revision 2.0, April 2005.

105 ITDynamics. Тестирование производительности гипервизоров виртуальных машин [Электронный ресурс]. Режим доступа: http://www.it-dynamics.ru/index.php/inmenu-31/3/60-2009-05-05-06-34-21/ 2009.

106 McAllister, Neil. Server virtualization. ComputerWorld. 2007. №9.

107 Goldworm B., Skamarock A. Blade Servers and Virtualization: Transforming Enterprise Computing While Cutting Costs//Wiley Publishing, Inc. 2007, p.411.

108 Takemura C., Crawford L.S. The book of Xen. A Practical Guide for the System Administrator // No Starch Press. October 2009, p.316.

109 XenServer Performance Monitoring for Scalability Testing, [Electronic resource]. – Electronic data. – Citrix inc. 2010. – Mode acess: http://support.citrix.com/servlet/KbServlet/download/22712-102-642229/XenServer Performance Monitoring for ScalabilityTesting.pdf

8 (952) 106-88-60 vk.com/a.projectit a.projectit