

УДК 519.6

ВИРТУАЛИЗАЦИЯ КАК ТЕХНОЛОГИЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ИТ-ИНФРАСТРУКТУРЫ

М. Ю. Осипов, И. Л. Бондарь, Р. А. Семенов, Т. Ю. Серова
(РФЯЦ-ВНИИЭФ)

Рассматривается технология виртуализации серверов при развертывании сетевых служб в локальных сетях, описаны принципы построения виртуальной ИТ-инфраструктуры. Сформулированы преимущества применения данного подхода к техническим средствам ИТ-инфраструктуры. Приводится разработанная и используемая в подразделении РФЯЦ-ВНИИЭФ функциональная схема ИТ-инфраструктуры на базе технологии виртуализации.

Ключевые слова: виртуализация, ИТ-инфраструктура, сервер, локальная сеть, сетевая служба, виртуальная машина, системные ресурсы, VMware.

Введение

При масштабном внедрении информационных технологий в различные системы со временем возникает вопрос эффективности, которая может рассматриваться с разных позиций: надежности, минимизации времени решения задач, уменьшения эксплуатационных издержек за счет снижения избыточности оборудования и сокращения требуемого персонала. При оценке эксплуатационной эффективности системы обычно рассматривается ее представление в виде совокупности ресурсов, традиционный подход к использованию которых принципиально конфликтен. Например, достижение высокой надежности за счет дублирования оборудования приводит к увеличению эксплуатационных издержек и снижению производительности.

ИТ-инфраструктура представляет собой совокупность программно-аппаратных компонентов. Для больших предприятий характерна сложная разветвленная ИТ-инфраструктура. Поддержание ее работоспособности требует больших материальных и временных затрат. Решение новых задач требует развертывания все новых и новых служб, что, в свою очередь, ведет к увеличению общего количества серверов. Постепенно это приводит к разрастанию ИТ-инфраструктуры и

соответственно возрастанию нагрузки на обслуживающий персонал.

Одним из решений данной проблемы является виртуализация серверов, которая подразумевает запуск на одном физическом сервере нескольких виртуальных машин, представляющих собой виртуальные серверы. Технология виртуализации позволяет отделить операционную систему (ОС) с установленной на ней программной средой от физических компонентов вычислительной машины. Такой подход позволяет размещать на одной физической машине несколько виртуальных с возможностью быстрой миграции и восстановления операционных сред, что значительно повышает коэффициент использования вычислительных ресурсов физической машины, мобильность и доступность сетевых служб в случае проведения профилактики или аппаратного сбоя, максимальную гибкость в отношении развертывания серверов, поддержания их жизнеспособности и управления.

В процессе виртуализации ИТ-инфраструктуры создается виртуальная инфраструктура — комплекс систем на основе виртуальных машин, обеспечивающих функционирование всей ИТ-инфраструктуры, который обладает новыми возможностями при сохранении существующей схемы деятельности ИТ-ресурсов.

Принципы построения виртуальной ИТ-инфраструктуры

Виртуальная машина использует физические ресурсы одного компьютера, а виртуальная инфраструктура — физические ресурсы всей ИТ-среды, формируя из компьютеров, а также из подключенных к ним сетей и хранилищ единое информационное пространство ИТ-ресурсов (рис. 1).

Виртуальная инфраструктура предоставляет возможность динамического распределения физических ресурсов для балансировки нагрузки в соответствии с потребностями пользователей. При существенном увеличении количества занимаемых физических ресурсов одной виртуальной машиной (или их недостатка для нее) возможен перенос на другой сервер либо этой машины, либо других, менее задействованных машин, исполняемых на этом же оборудовании.

Виртуальная инфраструктура включает в себя следующие компоненты:

- гипервизоры на каждом узле для полной виртуализации компьютера;
- службы распределенных систем на основе виртуализации (например, управление ресурсами) для оптимального распределения доступных ресурсов между виртуальными машинами;
- средства автоматизации, обеспечивающие возможности оптимизации ИТ-процессов (например, инициализации или восстановления в критических ситуациях);
- службы прикладного уровня, исполняемые на виртуальных машинах инфраструктуры для предоставления целевых услуг пользователям.

Благодаря отделению всей программной среды от исходной аппаратной инфраструктуры



Рис. 1. Виртуальная ИТ-инфраструктура

виртуализация позволяет объединить ряд серверов, инфраструктур хранения и сетей в единую совокупность ресурсов, динамически, безопасно и надежно распределяемую между приложениями по мере необходимости. Это дает возможность создавать вычислительную инфраструктуру с максимальной эффективностью, доступностью, автоматизацией и гибкостью, состоящую из недорогих серверов [1].

Практическое применение технологий виртуализации

Предпосылками для внедрения технологии виртуализации в локальную вычислительную сеть (ЛВС) одного из подразделений РФЯЦ-ВНИИЭФ явились следующие критерии:

- наличие в инфраструктуре множества служб, использующих разные программные платформы и разное аппаратное оборудование;
- наличие критически важных служб, работающих в круглосуточном режиме;
- неравномерная загрузка и использование существующего оборудования;
- наличие в ИТ-инфраструктуре служб, функционирующих на устаревшем оборудовании.

Для построения виртуальной ИТ-инфраструктуры выбрано решение от компании VMware [2] исходя из того, что продукты данной компании занимают лидирующее положение на рынке виртуализации и являются стандартом *де-факто*. Необходимо отметить, что решения ряда других компаний на данный момент обладают достаточными функциональными возможностями и также подходят для построения виртуальной ИТ-инфраструктуры, но в продуктах VMware управление соответствующими функциями реализовано более детально и эргономично. Сторонние компании, выпускающие сопутствующее ПО для продуктов виртуализации, в первую очередь выпускают свои продукты для решений VMware.

ТСО (*Total Cost of Ownership* — совокупная стоимость владения) типовой ИТ-инфраструктурой указана в табл. 1, исходные параметры для ее подсчета приведены в табл. 2. Расчет выполнялся при помощи калькулятора TCO, доступного на сайте <http://www.vmc-company.ru/solutions/virtualization-calc/calc.php>. Анализируя стоимость решений, указанную в табл. 1, можно видеть, что экономия при

Таблица 1

Совокупная стоимость владения типовой ИТ-инфраструктурой с использованием и без использования VMware

Показатель	Срок использования		
	1 год	2 года	3 года
Стоимость без VMware, дол.	171 897	351 132	537 705
Стоимость с VMware, дол.	143 282	203 903	337 764
Экономия, дол.	28 615	147 229	199 941
Количество серверов виртуализации	3	3	4
Коэффициент консолидации серверов	8	8	8

Таблица 2

Исходные параметры для подсчета ТСО типовой ИТ-инфраструктурой

Исходные параметры	Значение
Количество серверов, имеющихся в настоящее время	20
Процент закупаемых под новые задачи серверов относительно количества имеющихся в настоящее время	10
Среднее количество портов SAN на один сервер	2
Среднее количество портов LAN на один сервер	3
Стоимость одного порта SAN оборудования, дол.	2 000
Стоимость одного порта LAN оборудования, дол.	1 000
Затраты на 1 администратора в месяц, дол.	1 600
Количество физических серверов, обслуживаемых одним администратором	10
Стоимость нового сервера, дол.	2 000
Стоимость кВт/ч, руб.	1,8
Стоимость 1 кв. м площади датацентра в год, дол.	350
Стоимость хост-сервера (HP ProLiant BL480c 2*Xeon® 5150, 16 Гб RAM), дол.	10 000
Количество хостов ESX, обслуживаемых одним администратором	10
Количество виртуальных серверов, обслуживаемых одним администратором	30
Среднее количество виртуальных серверов на одном физическом после консолидации	8
Стоимость лицензий VMware Infrastructure Enterprise на 2 процессора + поддержка уровня GOLD (12/5) на 2 года, дол.	8 000

построении ИТ-инфраструктуры с использованием технологии виртуализации компании VMware особенно существенна в долгосрочной перспективе.

Наличие в VMware возможности создания шаблонов виртуальных машин (готовых образов) позволяет сократить время развертывания серверов (время создания новых виртуальных машин). Таким образом, отсутствие необходимости установки и настройки ОС и ПО позволяет сократить период внедрения (развертывания) новых сетевых служб, исполняемых на виртуальных серверах.

В РФЯЦ-ВНИИЭФ разработана система автоматизированного поддержания работоспособности виртуальных серверов, исполняющих сетевые службы, которая упрощает процесс контроля за функционированием основных служб и

производит их перезапуск в случае отказа. Это решение содержит:

- подсистему автоматического распознавания сбоев в работе виртуальных машин, исполняющих основные сетевые службы;
- подсистему автоматического восстановления виртуальных машин;
- подсистему автоматического резервного копирования виртуальных машин;
- механизм автоматической передачи информационных сообщений о сбоях в работе виртуальных машин

и не использует дополнительных продуктов VMware, требующих добавочных вложений.

В качестве системы мониторинга применено открытое ПО компании Zabbix Sia — ZABBIX [3], предназначенное для мониторинга состояния се-

товых служб, серверов и различного сетевого оборудования. Продукт разработан как клиент-серверное приложение и имеет WEB-интерфейс для управления.

В разработанной системе ZABBIX является средством определения и визуализации состояния сетевых служб. С его же помощью организован механизм запуска программ проверок и восстановления работоспособности сетевых служб. Для обеспечения автоматизации мониторинга этих функций потребовалось создание проверок правильности функционирования каждой сетевой службы, сценариев резервного копирования образов работающих виртуальных машин и восстановления работоспособных виртуальных машин путем копирования эталонных образов из архива.

Функционирование подсистемы автоматического распознавания сбоев в работе виртуальных машин можно продемонстрировать на примере почтовой службы. Определение ее работоспособности производится проверкой правильности откликов на команды протоколов SMTP [4] и POP3 [5] по приему и отправке коротких текстовых сообщений. Вместе с письмом передается уникальное число, которое позволяет срав-

нить (идентифицировать) отправленное и принятое сообщения. Посредством анализа поведения почтового сервера по сценарию определяется корректность функционирования служб отправки и получения почты.

На рис. 2 приведен пример отображения состояния контролируемой службы. График представляет собой временную диаграмму доступности сетевой службы, где состояние 1 свидетельствует о доступности службы, а 0 — о сбое в ее работе.

Задача подсистемы автоматического восстановления работоспособного состояния сетевой службы предполагает не только замену неработоспособной виртуальной машины путем копирования эталонного образа из архива (рис. 3), но и периодическое резервное копирование виртуальной машины (рис. 4). Период копирования выбран исходя из особенностей эксплуатации виртуальной машины. В конкретных условиях использования системы резервирование осуществляется ночью, в период с 2 до 5 часов.

Наличие функции резервного копирования образа виртуальной машины позволяет восстановить работоспособность службы на этом же или другом виртуальном сервере сразу после опреде-

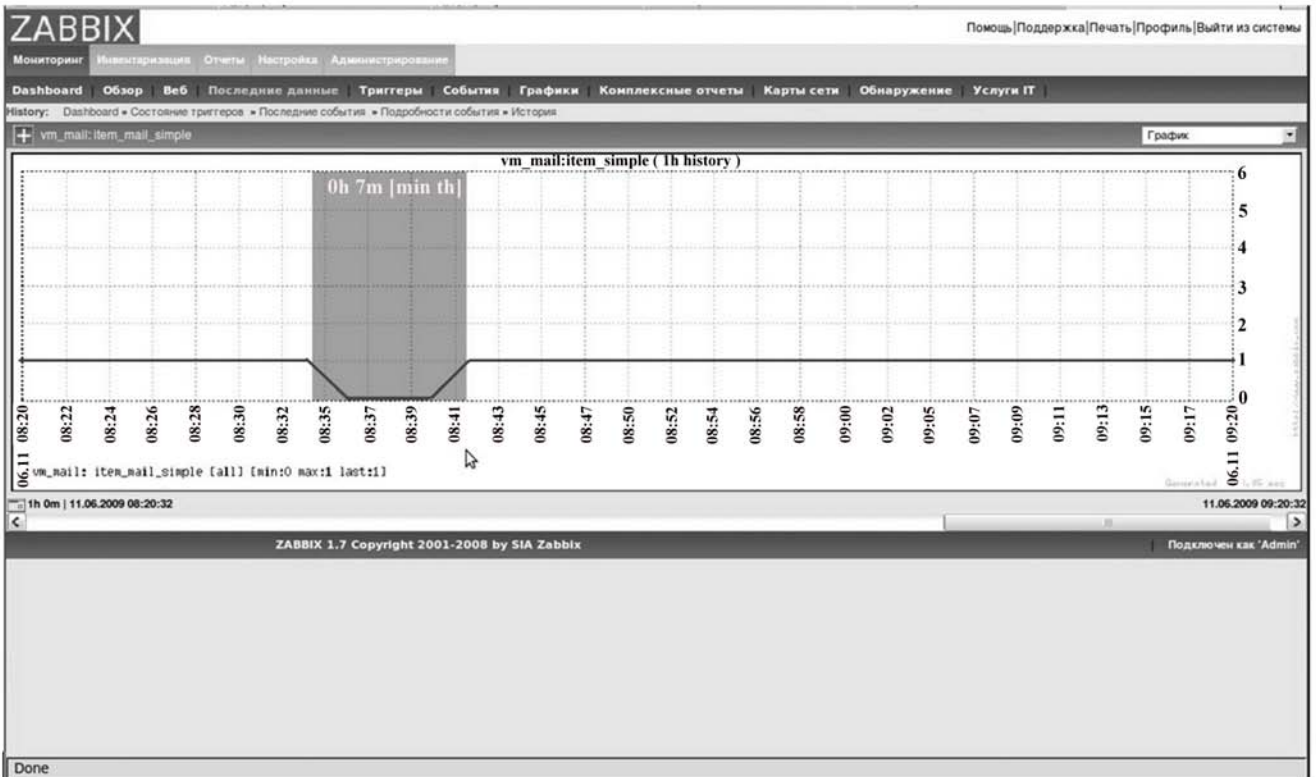


Рис. 2. Отображение состояния сетевых служб

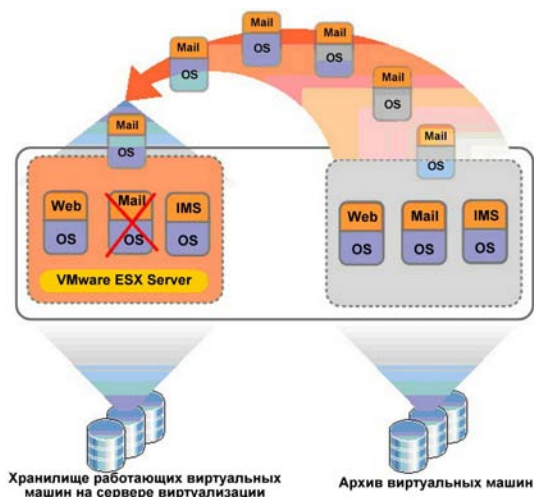


Рис. 3. Восстановление работоспособных виртуальных машин путем копирования эталонных образов из архива

ления отказа. Автоматизирован также процесс отправки сообщения администратору сразу после обнаружения сбоя в работе сетевой службы. Таким образом, администратор освобождается от необходимости мгновенного реагирования на сбойную ситуацию в работе службы, что позволяет разбираться с причинами отказа в удобное для него время, не ухудшая при этом доступность услуг для пользователей.

На данный момент система используется для управления следующими службами, размещенными на виртуальных машинах:

- почтовой службой и службой новостей;
- службой мгновенных сообщений Jabber;
- LDAP-сервером.

Особенностью данной системы является способность проверки корректности работы именно сетевых служб в отличие от подобных систем, которые контролируют работу только самой виртуальной машины.

Тестирование разработанной системы показало следующий результат: на восстановление работоспособности сетевой службы — это определение сбойной ситуации в ее работе, копирование резервной копии из архивного хранилища, удаление сбойной виртуальной машины из списка зарегистрированных и ее перемещение в хранилище для вышедших из строя, регистрация и включение новой виртуальной машины — требуется около 15 минут. Следует учитывать, что готовый образ виртуальной машины, исполняющей типовую сетевую службу, в среднем занима-

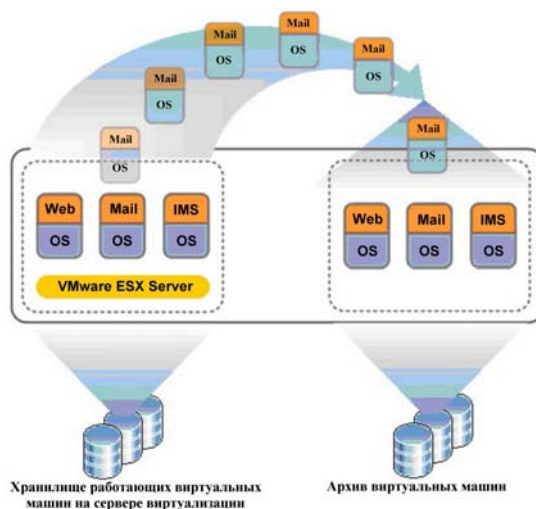


Рис. 4. Резервное копирование образов работающих виртуальных машин в архив

ет 8-10 Гб. На аналогичные действия, выполненные в неавтоматическом режиме администратором, требуется гораздо больше времени, что обусловлено наличием человеческого фактора.

Функциональная схема ИТ-инфраструктуры на базе технологии виртуализации ЛВС подразделения РФЯЦ-ВНИИЭФ представлена на рис. 5.

Физические узлы объединены в кластер, на котором работает множество виртуальных серверов, исполняющих сетевые службы. Разработанная авторами система мониторинга размещена на отдельном физическом сервере. Она контролирует доступность служб, т. е. проверяет корректность их работы, периодически инициирует резервное копирование образов виртуальных машин в хранилище данных и в случае нештатной ситуации посредством взаимодействия с ОС узлов перезагружает виртуальные машины, предварительно инициируя при необходимости перенос копий из архива. Сетевые службы, исполняемые на виртуальных машинах, доступны всем пользователям обычным способом, при этом все подробности их функционирования от пользователей скрыты. Мониторинг сетевых служб, работа пользователей со службами, обмен образами виртуальных машин между архивным хранилищем данных и хранилищем работающих виртуальных машин на кластере осуществляется по обычным каналам связи (Ethernet).

Данная ИТ-инфраструктура реализована на базе бесплатного решения от VMware. Однако существует коммерческий продукт VMware vSphere 4, предназначенный для виртуализации

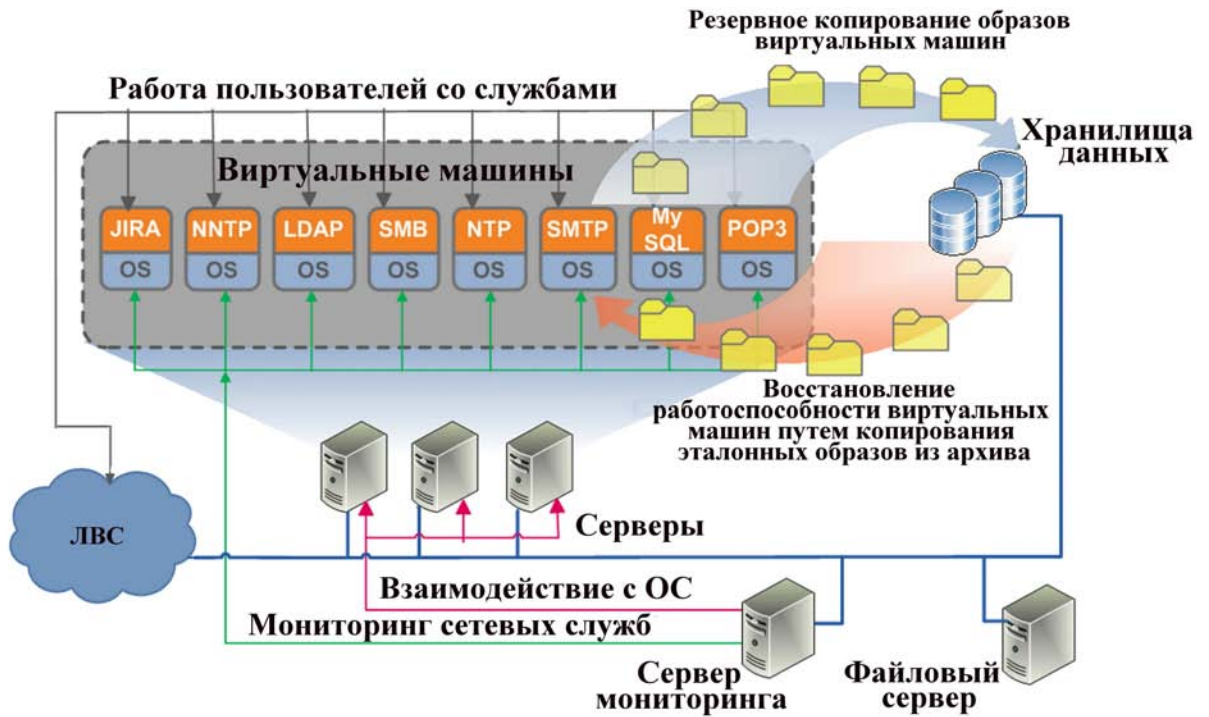


Рис. 5. Функциональная схема ИТ-инфраструктуры

серверов, хранилищ и сетевых средств, позволяющий многим неизменяемым ОС и их приложениям независимо выполняться на виртуальных машинах при разделении физических ресурсов. VMware vSphere 4 обладает встроенными средствами управления, оптимизации ресурсов, обеспечения повышенной надежности приложений и автоматизации процессов. Эти средства позволяют сократить оперативные затраты, повысить эффективность эксплуатации, гибкость и уровни сервиса.

Один из компонентов vSphere, VMware VirtualCenter, обеспечивает централизованное управление, автоматизацию процессов, оптимизацию ресурсов и высокую доступность виртуальной ИТ-инфраструктуры (рис. 6), что упрощает эксплуатацию, повышает эффективность и надежность. VirtualCenter включает в себя широкий набор интерфейсов служб, обеспечивающих интеграцию с продуктами управления инфраструктурой от других производителей, а также разработку специализированных решений [6].

Использование vSphere дает следующие преимущества:

- возможность управления виртуальными машинами из внешней сети по защищенному каналу;
- единую точку управления всеми серверами через Virtual Control Center;

- мониторинг и балансировку работы виртуальных машин на серверном поле посредством анализа загрузки физического компьютера или виртуальной машины (если ресурсов виртуальной машине требуется больше, чем есть на текущем физическом компьютере, и эти ресурсы может предоставить другой компьютер, машина автоматически перемещается на него);
- возможность обслуживания физических серверов в рабочее время без прерывания предоставления услуг;
- минимально возможное время восстановления после сбоя;
- существенный рост качества и времени доступности ИТ-сервисов;
- снижение рисков критических сбоев в ИТ-инфраструктуре.

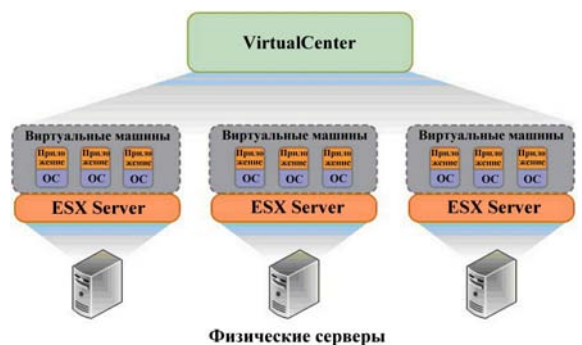


Рис. 6. Принцип работы VMware VirtualCenter

Кроме того, группа компаний "Код безопасности" выпустила продукт Security Code vGate for VMware Infrastructure, предназначенный для обеспечения безопасности виртуальной инфраструктуры на базе систем VMware Infrastructure 3 и VMware vSphere 4. vGate имеет сертификат Федеральной службы по техническому и экспортному контролю (ФСТЭК) России, позволяющий применять продукт в автоматизированных системах уровня защищенности до класса 1Г [7] включительно и в информационных системах обработки персональных данных (ИСПДн) до класса К1 [8] включительно. Применение vGate дает возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих данные ограниченного доступа, и упрощает аттестацию автоматизированных систем.

В будущем технология виртуализации позволит сократить затраты на замену аппаратного обеспечения, поскольку виртуальные серверы не привязаны к конкретному оборудованию. Также при предъявлении новых требований к информационной структуре обеспечена возможность расширения функциональности виртуальной инфраструктуры путем использования дополнительных интеграционных модулей как от компании VMware, так и от сторонних производителей.

Список литературы

1. Основы виртуализации. <http://www.vmware.com/ru/technology/virtual-infrastructure.html>
2. VMware. <http://www.vmware.com/ru/>
3. ZABBIX. <http://www.zabbix.com>
4. Открытая энциклопедия Википедия на русском языке. <http://ru.wikipedia.org/wiki/SMTP>
5. Открытая энциклопедия Википедия на русском языке. <http://ru.wikipedia.org/wiki/POP>
6. Виртуализация. http://www.ulyssys.com/ing.ru/page.articles/articles_id.3.htm
7. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Утверждено решением председателя Государственной технической комиссии при Президенте РФ от 30 марта 1992 г. http://www.fstec.ru/_docs/doc_3_3_004.htm
8. Приказ ФСТЭК России, ФСБ РФ, Мининформсвязи РФ от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных". <http://www.zki.infosec.ru/law/personal/146/>

Статья поступила в редакцию 08.11.10.
