Часть 3

Управление виртуализованной ИТ-инфраструктурой предприятия

Что такое виртуализация?

- Виртуализация – это метод сокрытия конкретных физических характеристик ИТ-ресурсов от тех представлений, в рамках которых другие системы, приложения и/или пользователи пользуются этими ресурсами.
- Это совокупность технологий взаимного отображения множества реальных ИТ-ресурсов предприятия на их логические представления, и наоборот.

Что такое виртуализация?

- «Виртуализация – это замена физических элементов распределенной ИТ-среды (будь то аппаратура или программное обеспечение), их искусственными (иначе - виртуальными) «клонами», которые, являясь достаточно близкими копиями оригиналов, избавляют нас от доставляющей массу неудобств необходи-мости иметь дело с сами оригиналами».
  Ф.Хэпгуд.
- Это базовая конструкция или методология, скрывающая за собой подлинные механизмы распределения множества реальных ИТ-ресурсов в многопользовательской вычислительной среде.

Цель и задачи виртуализации

- **Основная цель виртуализации - повышение эффективности использования имеющихся корпоративных ИТ-ресурсов предприятия;**
- **Задачи виртуализации:**

- **Упрощение механизмов мониторинга и управления реальными ИТ-ресурсами ИКС;**
- **Поддержка оперативного выделения и гибкого динамического перераспределения объемов ИТ-ресурсов в точном соответствии с потребностями конкретных пользователей или приложений, а также требованиями QoS;**
- **Повышение общего уровня надежности и информационной безопасности в ИКС.**

Объекты виртуализации в рамках ИКС предприятия

- Центры обработки данных ИКС;
- Отдельные серверы, серверные кластеры, мид- или мэйнфреймы;
- Системы хранения данных;
- Телекоммуникационные ресурсы ИКС;
- Операционные системы;
- Приложения (прикладное ПО);
- Данные;
- Рабочие места пользователей.

Спектр виртуализации

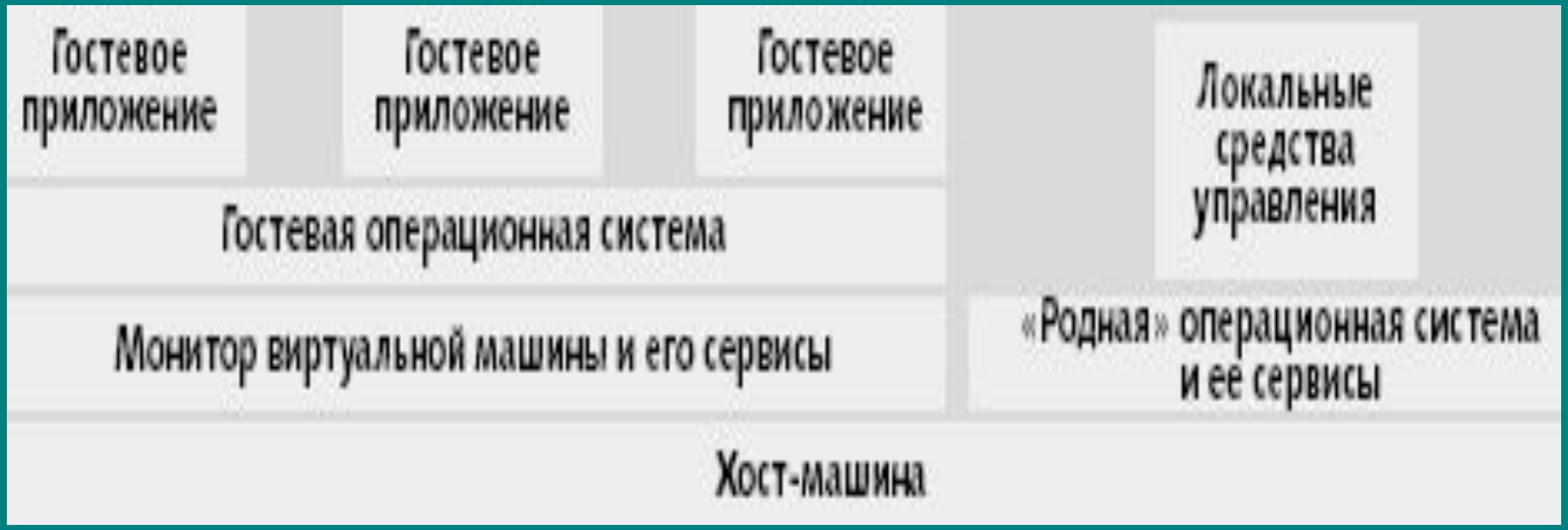
ПРЕИМУЩЕСТВА ВИРТУАЛИЗАЦИИ

- Повышение эффективности использования имеющихся ИТ-ресурсов ИКС предприятия;
- Относительная простота управления виртуальной ИТ-инфраструктурой ИКС;
- Повышение надежности, живучести и информационной безопасности ИКС;
- Расширение возможностей по гибкому выделению ресурсов (масштабируемость) для данных, пользователей и приложений в рамках модели вычислений «по требованию»;
- Возможность реализации сервис-ориентированных архитектур (SOA).

Общая характеристика виртуализации

- Виртуальная машина может быть использована для консолидации нагрузки отдельных недогруженных серверов на меньшем количестве серверов. Таким образом можно повысить КПД, сэкономить на стоимости аппаратуры и управлении, на затратах на поддержание окружающей среды и на администрирование;
- Виртуализация позволяет сохранить аппаратную и программную среду для унаследованных приложений в тех случаях, когда появляются новые компьютеры. Она облегчает условия миграции программного обеспечения и данных на новые платформы;
- Средства виртуализации упрощают создание надежных платформ. Ненадежные приложения могут быть взаимно изолированы, разведены по своим «песочницам» (sandbox);
- Виртуализация помогает эмулировать среду, где одновременно работают несколько операционных систем;
- При разработке программ можно априорно определить ограничения той среды, в которой они будут работать;
- Виртуальная машина может воплощать в себе реально не существующие, пока еще только разрабатываемые аппаратные средства и сетевые соединения в рамках ИКС предприятия;
- Средства виртуализации могут стать важнейшим инструментом при широком распространении многоядерных процессоров. За счет их использования можно гибко масштабировать системы, увеличивая количество физических процессоров или ядер на порядки.

Классическая архитектура виртуальной машины



VMM - Virtual Machine Monitor – монитор (гипервизор) ВМ

Виртуализация серверов

С технической точки зрения возможны два типа виртуализации серверов — *вертикальная* и *горизонтальная*. Первый тип ближе к традиционной мэйнфреймовской модели; он предполагает сегментирование (партиционирование) ресурсов мощных серверов на разделы, поставку вычислительных услуг по требованию, а также динамическое управление ресурсами и нагрузкой.

Второй основывается на противоположной идее — на кластеризации мелких серверов. Вертикальную виртуализацию можно реализовать аппаратными средствами; в таком случае разделы можно назвать физическими, и программными - на логические разделы. Физические разделы — атрибуты серверов корпоративного класса. Логическое деление (Virtual Partitions, vPars) на разделы поддерживается такими операционными системами, как Solaris, AIX и HP-UX, работающих на RISC-процессорах или на Itanium.

На платформе Windows для логического деления на разделы используются продукты ESX Server и GSX Server (VMware) и Virtual Server (Connectix). Горизонтальная виртуализация в основном сводится к созданию больших серверных ферм.

Виртуализация сетей

Виртуализация сетей строится на использовании интеллектуальных маршрутизаторов, коммутаторов и другого сетевого оборудования, предназначенного для создания виртуальных локальных сетей (VLAN). В основном виртуализация достигается путем деления реального физического диапазона пропускания на несколько независимых и безопасных друг для друга каналов.

Виртуализация сети позволяет целому ряду устройств быть фиксировано подключенными к единой физической цепи, однако определение логической топологии этой сети путем сборки ее логически независимых сегментов может осуществляться динамически. Средствами виртуализации сетевые ресурсы превращаются в единый управляемый пул.

Подобный унифицированный подход к созданию сетевых конфигураций упрощает процесс развертывания, повышает безопасность и эффективность контроля. У пользователей появляется возможность реализовывать требуемые сетевые политики и обеспечивать каждому из виртуальных сегментов требуемое качество обслуживания.

Виртуализация систем хранения

Объединение в один пул различных систем хранения повышает практически все эксплуатационные характеристики системы в целом, в том числе более высокую готовность, лучшее использование дискового пространства, возможность централизованного управления. В зависимости от используемых технологий в этот пул могут включаться либо только сетевые ресурсы NAS (network attached storage) и SAN, либо еще и диски, непосредственно подключенные к серверам (direct attached storage, DAS).

Виртуализация систем хранения — это дополнительный уровень абстракции между физическими устройствами и логическими томами, который скрывает в себе лишние инфраструктурные детали. Существует множество технических решений для практического воплощения виртуализации систем хранения, различающихся местом расположения механизма виртуализации.

Он может находиться непосредственно в устройстве (array-based storage virtualization), в таком случае виртуализованные устройства доступны любому серверу, подключенному к сети хранения, в сети (network-based storage virtualization) или в серверах (server-based storage virtualization).

Виртуализация приложений

Пока не сложилось строгого определения того, что есть виртуализованное приложение. Обычно под ним подразумевают возможность распределенного выполнения одного приложения на одном или нескольких компьютерах, в синхронном или асинхронном режиме. В качестве примера обычно приводится выполнение приложений в среде grid. Но главный пример – это SOA!

Одним из примеров законченных решений для виртуализации приложений является программный продукт UpScale компании Ejasent (Veritas Software). Инструментарий UpScale позволяет перемещать приложения с одного сервера на другой, не прерывая работу приложения. Для выполнения подобных действий UpScale изготавливает «моментальный снимок» состояния приложения и передает его на другой сервер.

В качестве еще одного примера виртуализации приложений можно привести технологию SystemGuard компании SoftGrid. Эта технология позволяет выполнять на клиентских АРМ приложения, хранящиеся на серверах. В основе ее лежит пакетирование приложений: при передаче приложение, как пакет данных в сети, несет с собой свою собственную конфигурационную «обвязку».

Виртуализация ввода-вывода

Виртуализация ввода-вывода – организация унифицированных механизмов доступа к тем или иным территориально распределенным ИТ-ресурсам, физическое местоположение которых в корпоративном пространстве должны быть скрыто от конечных пользователей ИКС предприятия.

Ключевым элементом виртуализированного ввода/вывода является замена реальных физических портов логическими сервисами, выполняющими функции соединений IP или Fibre Channel. Когда в виртуализированной среде сервер обращается за соответствующим сервисом, коммутатор типа InfiniBand осуществляет переадресацию к нужному порту или шлюзу.

При этом множество разнотипных подключений можно заменить одним подключением к скоростному коммутатору типа InfiniBand.

Виртуализация Центров обработки данных

Виртуализация ЦОД — это комплексное решение проблемы абстракции всех физических ИТ-ресурсов ЦОД, существующих в виде конкретных устройств, путем их представления в виде пулов логических ресурсов, образующих единое корпоративное пространство (виртуально однородную информационно-вычислительную среду).

Она позволяет системному администратору перемещать приложения, работающие на виртуальных машинах, с одного физического процессора на другой, причем не только в пределах одного сервера, а в пределах всего ЦОД. Мобильность приложений в пределах ЦОД открывает возможность для сохранения их работоспособности в процессе перестройки Центра, увеличивает возможности балансирования нагрузки, например, позволяет перемещать приложения на более производительные процессоры при повышении нагрузки и наоборот (масштабирование).

Особенности виртуальных решений

Упрощается миграция программного обеспечения, системы приобретают большую мобильность. Появляется возможность для выполнения устаревших приложений, которые не могут работать на новом оборудовании.

Виртуализованные машины более безопасны с точки зрения изоляции приложений, поэтому они являются более надежной платформой.

Виртуальная машина может работать в условиях более жестких ограничений на операционную среду, что может быть критично в случаях, когда необходимо обеспечить требуемое качество обслуживания (QoS) для всей совокупности приложений.

Использование виртуальных машин позволяет условно «использовать» то оборудование, которое на данный момент в системе отсутствует, например, в целях моделирования перспективной аппаратной платформы.

Улучшаются условия для отладки и мониторинга приложений. Так, на виртуальной машине легче и безопаснее отлаживать программное обеспечение, которое в состоянии нарушить нормальную работу реальной машины.

Возможности аппаратной виртуализации

1. Изоляция систем. Применяется для обеспечения независимости виртуальных машин. Гостевые ОС и приложения распределяются в зависимости от их критичности и функциональных возможностей. Например, в ЦОД мультисервисной телекоммуникационной системы компоненты системы информационной безопасности (сетевые экраны) и серверы, поддерживающие обработку голосовых сообщений, разворачиваются в гостевой ОС Linux, а серверы потоковой обработки данных — под управлением Windows Server на единой аппаратной платформе. Для обеспечения отказоустойчивости гостевые ОС могут дублироваться, и тем самым время простоя в случае отказа может быть сведено к минимуму.

2. Консолидация нагрузки. Используется для объединения физических серверов в виде отдельных виртуальных машин, каждая из которых имеет собственную операционную систему. При этом единый административный интерфейс позволяет организовать эффективное управление физическими и виртуальными ресурсами. Динамическое выделение и перераспределение ресурсов сервера дает возможность быстро перемещать выполняющиеся приложения, в зависимости от рабочих нагрузок. Если раньше такая возможность использовалась преимущественно для обеспечения отказоустойчивости, то теперь, в условиях предоставления ресурсов по требованию (utility computing), она становится одной из основных обеспечивающих технологий ЦОД.

Возможности аппаратной виртуализации

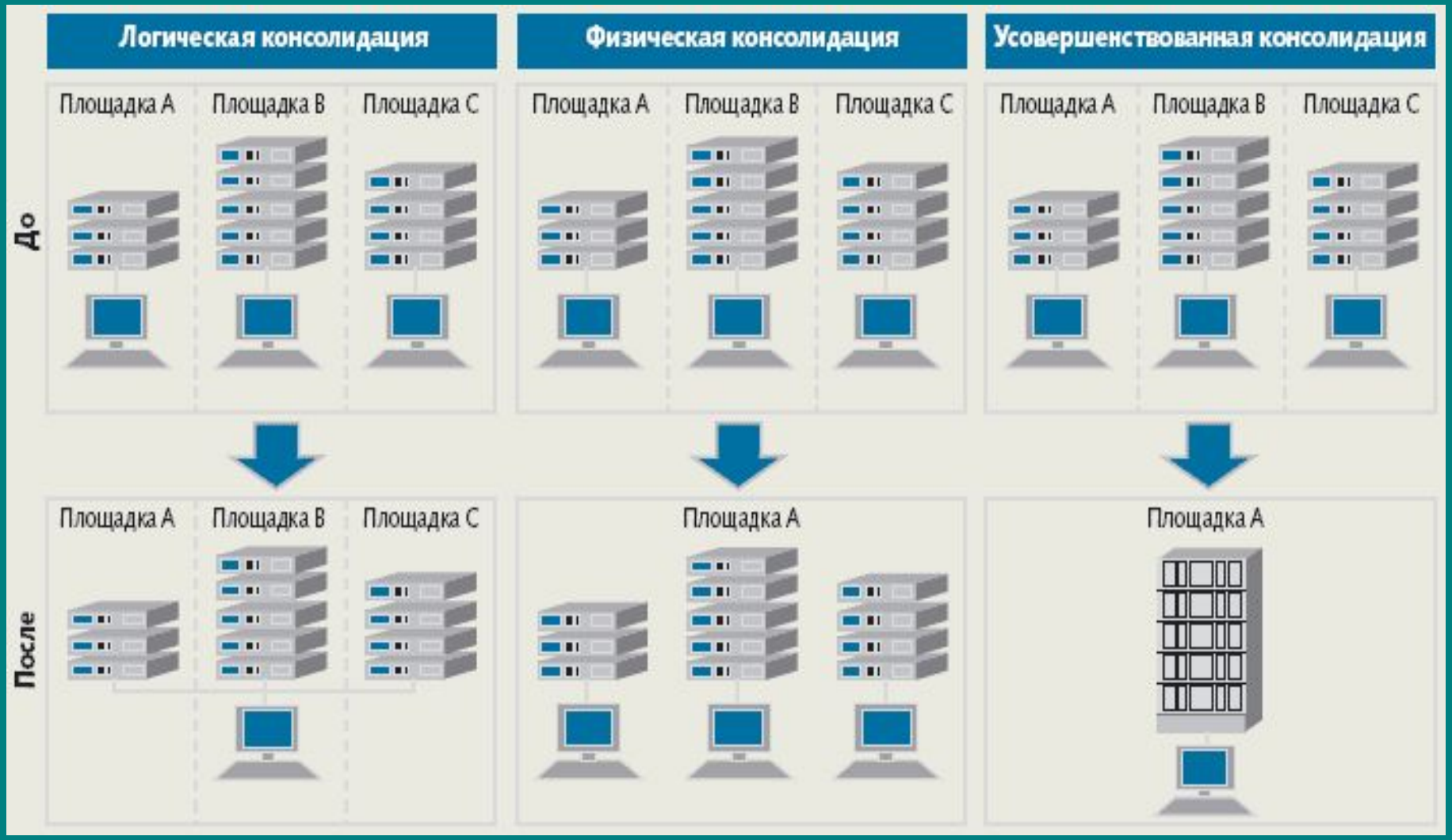
3. Миграция. Применяется для обеспечения возможности перемещения операционных систем вместе со всеми выполняющимися приложениями. Благодаря «посредничеству» монитора виртуальных машин удается обойти многие проблемы, возникающие при перемещении на уровне процессов (например, сохранение установленных сетевых соединений или привязки к выделенным областям оперативной или внешней памяти). После миграции виртуальной машины исходную машину можно безболезненно остановить, что удобно, например, для выполнения регламентных работ. При миграции виртуальной машины полностью сохраняется состояние оперативной памяти как для ядра ОС (управляющие блоки TCP), так и для выполняющихся приложений. Таким образом, при перемещении работающей системы сохраняются все установленные соединения и не требуется повторное подключение активных пользователей, что очень важно, например, в телекоммуникационных, финансовых и др. системах.

4. Безопасность. Аппаратная поддержка виртуализации не только упрощает логику и программную реализацию монитора виртуальных машин, что делает его менее уязвимым от компьютерных атак, но и усиливает изоляцию виртуальных машин. Вход в каждую из исполняемых на консолидированном сервере операционных систем может быть защищен собственным паролем, что позволяет более эффективно контролировать доступ пользователей, принадлежащих к различным подразделениям и рабочим группам.

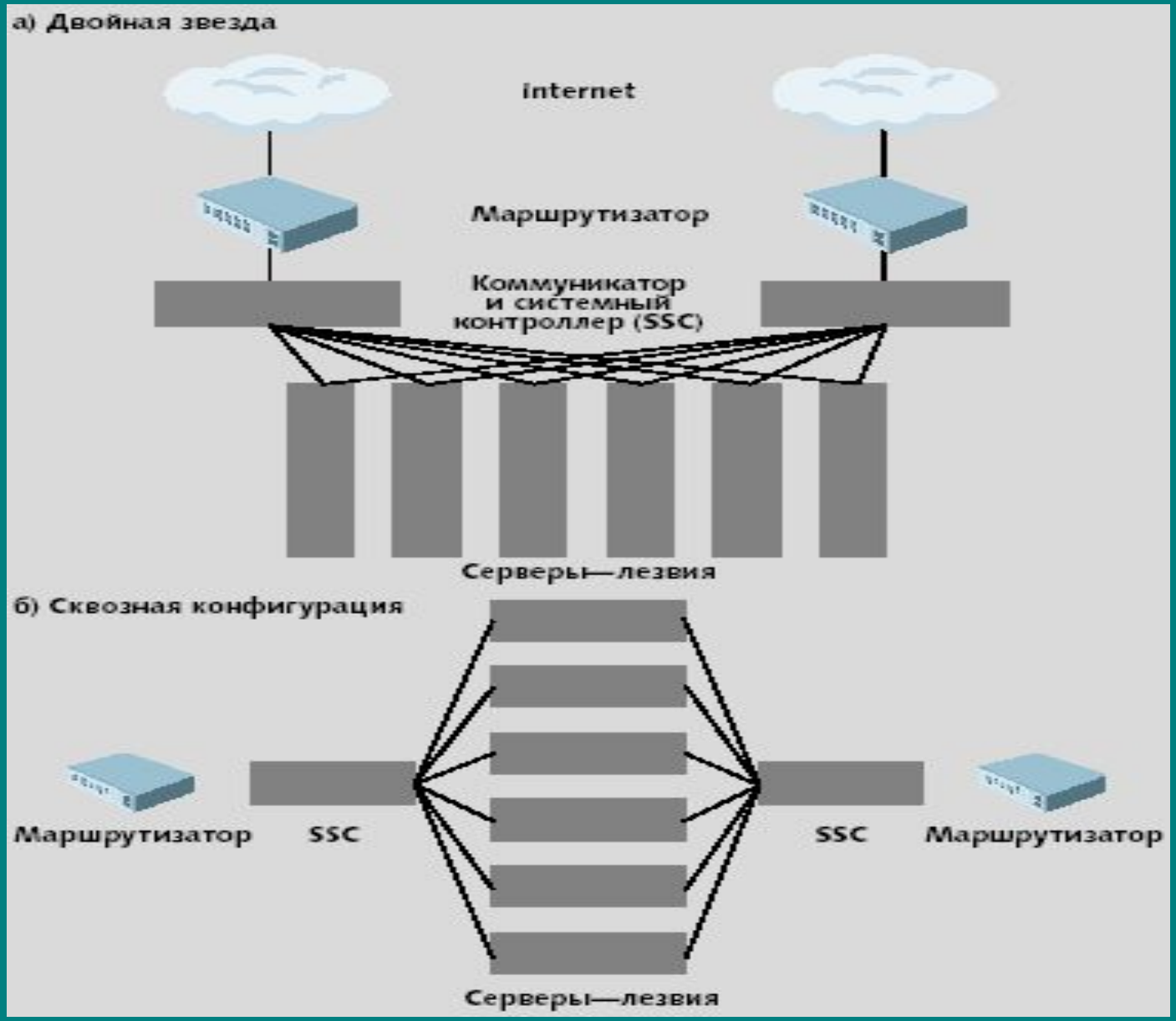
Виртуализация: консолидация и партиционирование ИТ-ресурсов

- Консолидация – объединение физически неоднородных ИТ-ресурсов в логически однородную виртуализованную среду;
- Партиционирование – разбиение физически однородных ИТ-ресурсов на логически неоднородные сегменты с гетерогенной операционной средой.

Типы консолидации серверов

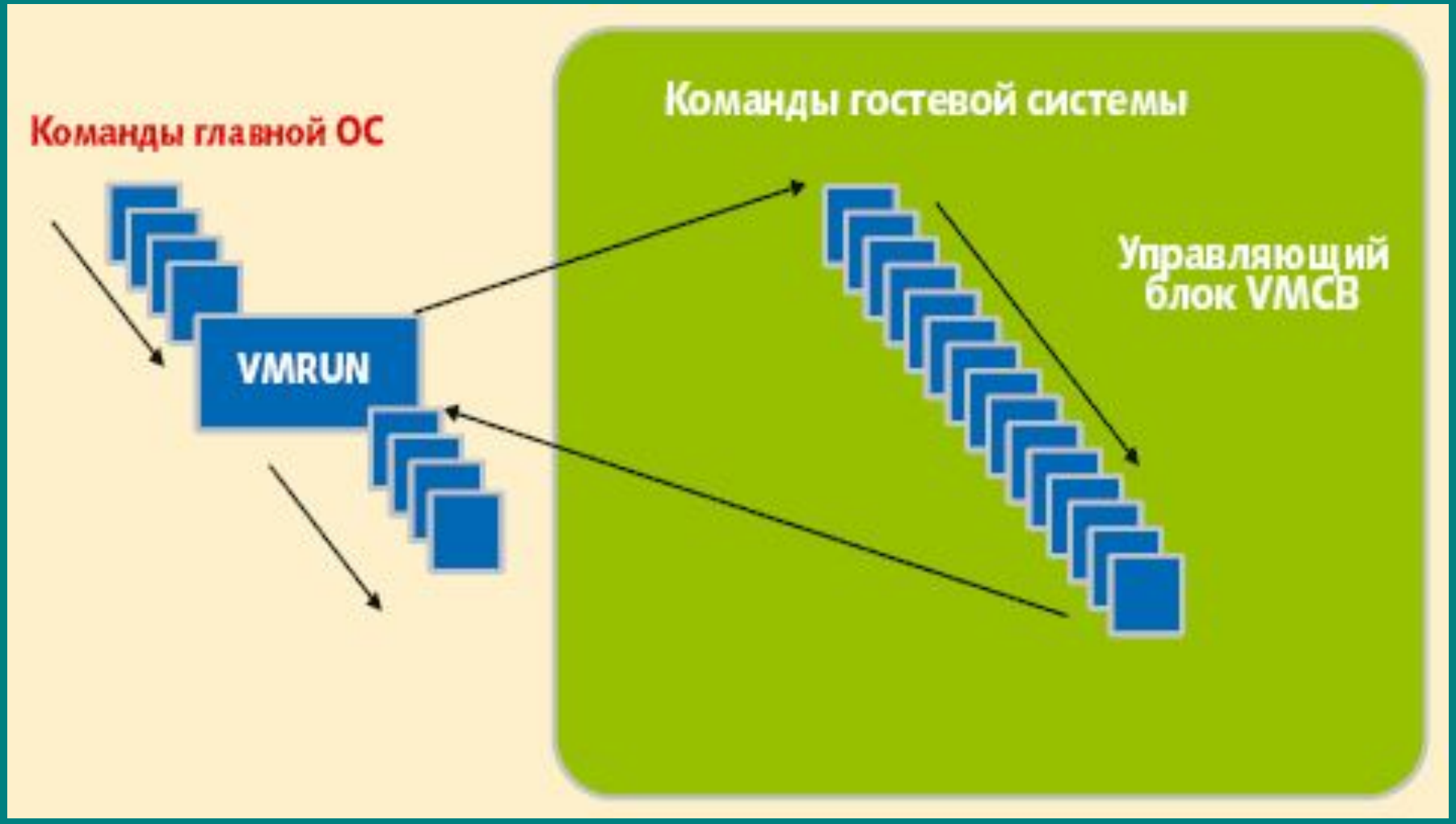


Варианты консолидации серверных «лезвий»



Управление нагрузкой и деление на разделы (партиционирование)

Аппаратная виртуализация в рамках AMD-V



Технологии виртуализации: от серверов – до ЦОД

Проблемы планирования и управления реализацией виртуальных решений

- Расчет затрат и оценка эффективности проектов виртуализации с точки зрения ROI;
- Инвентаризация парка техники и ПО, решение проблем совместимости;
- Проблемы развертывания виртуальных решений и процессов миграции в рамках ИКС предприятия;
- Управление и контроль функционирования систем;
- Планирование стратегии восстановления систем после сбоев;
- Управление обновлениями и задачи масштабирования в рамках виртуальной ИТ-инфраструктуры ИКС;
- Обеспечение необходимого уровня информационной безопасности в виртуальной среде предприятия;
- Проблемы подготовки специалистов в области виртуализации.

Базовые технологии виртуализации серверов

- Естественная виртуализация (VMWare Server - EMC, MS Virtual Server 2005 R2 – Microsoft, Virtual Iron);
- Паравиртуализация (Sun xVM Server – Sun Microsystems, XenServer – Citrix Systems);
- Высокоуровневая виртуализация на уровне операционных систем (Linux-VServer, SWSoft - Virtuozzo, OpenVZ, Solaris Containers и др.).

Технологии виртуализации серверов

Основные подходы к виртуализации серверов

- При естественной виртуализации виртуальная машина эмулирует реальное аппаратное обеспечение, что позволяет использовать в качестве гостевых обычные операционные системы, а команды, требующие себе особых привилегий, отрабатываются средствами VMM. В данную категорию попадают продукты VMware и Microsoft.
- Паравиртуализация. По существу, паравиртуализация отличается распределением функций между VM и VMM. В данном случае основная работа выполняется гостевыми ОС и только отдельные функции отставлены за операционной системой VMM. Это неполная виртуализация, добавление «пара» можно было бы заменить «псевдо», но в литературе принят именно термин «паравиртуализация». Пример — Xen.
- Высокоуровневая виртуализация на уровне ОС позволяет в рамках одной операционной среды выделить разделы для выполнения независимых гостевых ОС. Наиболее известные проекты: Linux-VServer, Virtuozzo, OpenVZ, Solaris Containers и FreeBSD Jails. Концептуально на физических серверах средствами операционной системы создаются частные виртуальные серверы (virtual private server), что, по существу, является разбиением ресурсов на независимые разделы, которые называют «контейнерами». Производители ОС для этих целей снабжают свои продукты виртуализационными возможностями. Например, HP расширила функциональность и упростила развертывание и виртуализацию критичных бизнес-задач в окружении HP-UX 11i v3.

Особенности виртуализации с VMM

- ***Увеличивается число используемых ОС внутри компании.*** Хотя количество физических серверов уменьшается, однако имеется столько же гостевых ОС, как и раньше. Более того, ситуация может ухудшаться — некоторые из этих виртуальных машин могут быть неактивны большую часть времени и не получать обновления автоматически, что представляет серьезную угрозу безопасности сети.
- ***Субоптимальное управление ресурсами не очень удобно.*** Каждая операционная система внутри VM распоряжается ими самостоятельно. Однажды выделенную для VM память потом будет сложно «забрать» обратно, так как нет возможности контролировать гостевую ОС. Это также сказывается на масштабируемости — невозможно отдать неиспользуемые ресурсы одной из виртуальных машин, тогда как любому контейнеру в любой момент все ресурсы потенциально доступны.
- ***Эмуляция оборудования гипервизором приводит к потере производительности.*** Кроме того, становится невозможной оптимизация работы драйверов высокопроизводительных устройств.

Особенности виртуализации на уровне ОС

Высокоуровневая виртуализация лучше справляется с задачами, чувствительными к производительности. Во-первых, весь ввод-вывод использует стандартный код стандартной операционной системы и драйверов, гарантированно и полностью сохраняя оптимизации, заложенные производителем и избегая лишних накладных расходов на эмуляцию виртуального оборудования. Во-вторых, переключение между разными операционными системами остается крайне тяжелой в вычислительном смысле операцией, даже при аппаратной поддержке виртуализации. «Контейнеры» используют единственное ядро, у них нет такой проблемы.

С другой стороны, изменения в поведении ОС в контейнере приводят к плохой применимости этого типа виртуализации в случае разработки и тестирования. Ограничения самой ОС также иногда сужают рамки применимости «контейнеров», например, лимит на количество сессий в клиентских версиях Windows ограничивает и количество доступных по сети контейнеров. Наконец, использование единого ядра тоже представляет собой проблему при запуске разных ОС, — например, Linux и Windows на одном физическом сервере.

Применимость базовых технологий виртуализации к решению бизнес-задач

	Гипервизор	ОС	Вместе
Разработка и тестирование ПО			
Виртуализация клиентских версий операционных систем			
Консолидация унаследованных операционных систем			
Консолидация критичных для бизнеса серверов			
Консолидация критичных по производительности рабочих нагрузок			
Централизованная виртуальная инфраструктура рабочих мест			
Обеспечение непрерывности бизнес-процессов			
Software-as-a-Service			
Развертывание и поддержка ИТ-инфраструктуры			

 Технология практически не применима

 Технология применима в отдельных случаях

 Технология применима во многих случаях, но имеется большой класс задач, когда с точки зрения бизнеса применение неоправдано

 Технология применима в большинстве случаев

 Технология практически всегда применима

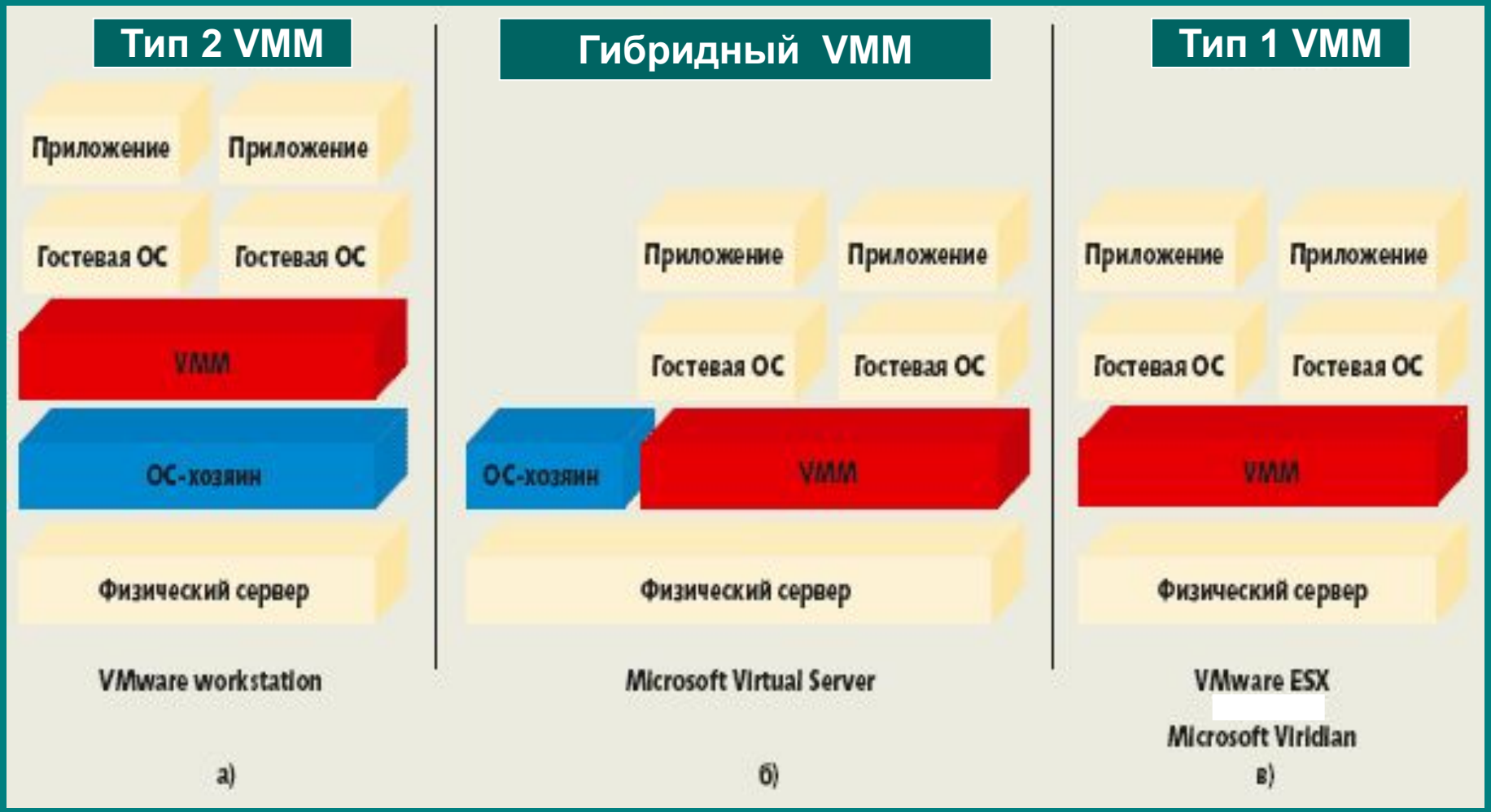
Ограничения на виртуализацию с VMM

Эквивалентность. Монитор VMM должен следить за тем, чтобы программа выполнялась в среде, почти полностью соответствующей среде невиртуализирован-ной машины, за несколькими исключениями. Исключения распространяются на доступность системных ресурсов, временную диаграмму процессов и подключенные периферийные устройства.

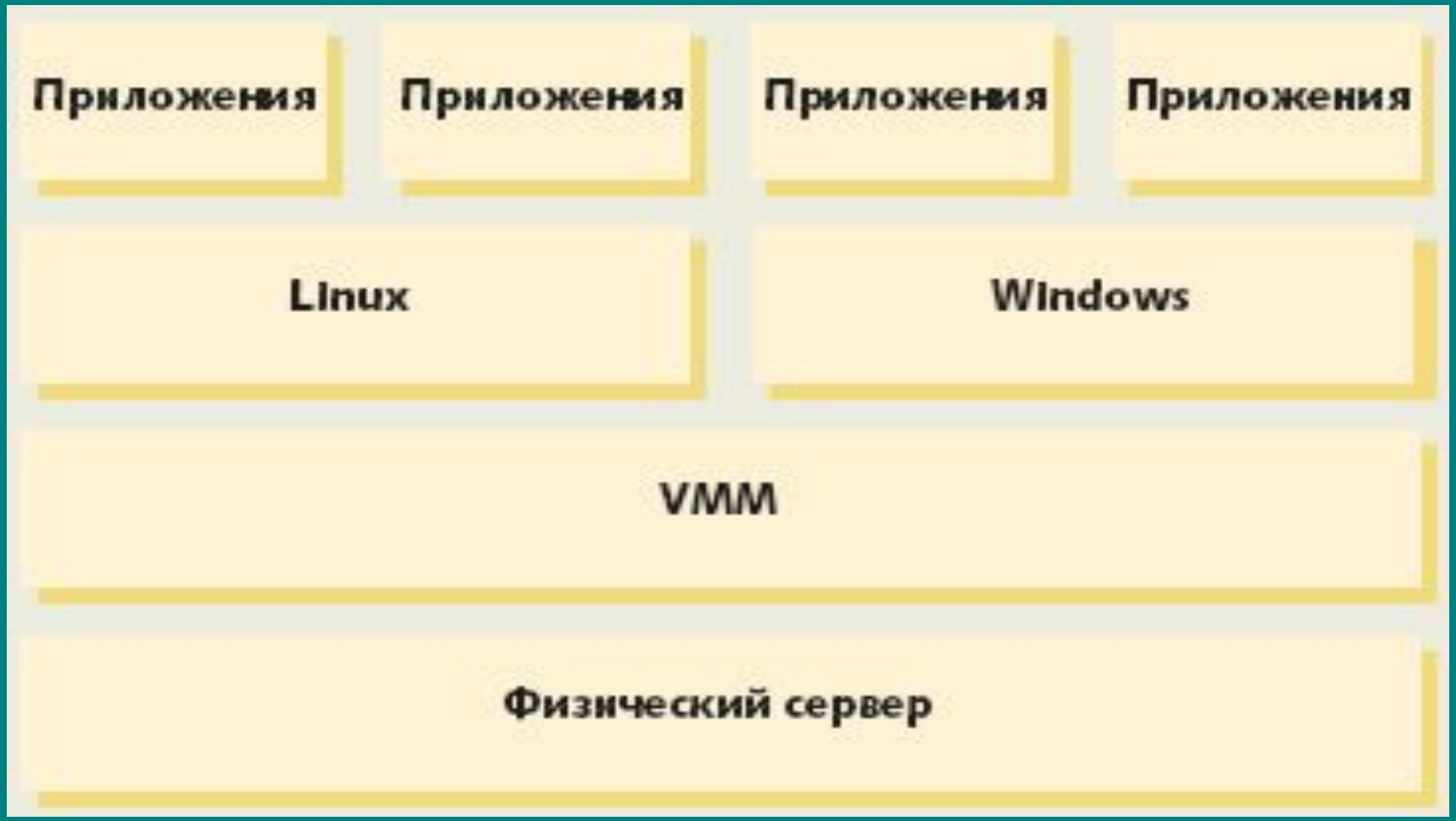
Полнота управления. VMM должен быть способен управлять всеми системными ресурсами, но не выходя за отведенные для него границы ресурсов.

Эффективность. Значительная часть машинных команд должна выполняться без участия VMM, а те команды, которые не могут быть таким образом выполнены, должны интерпретироваться средствами VMM.

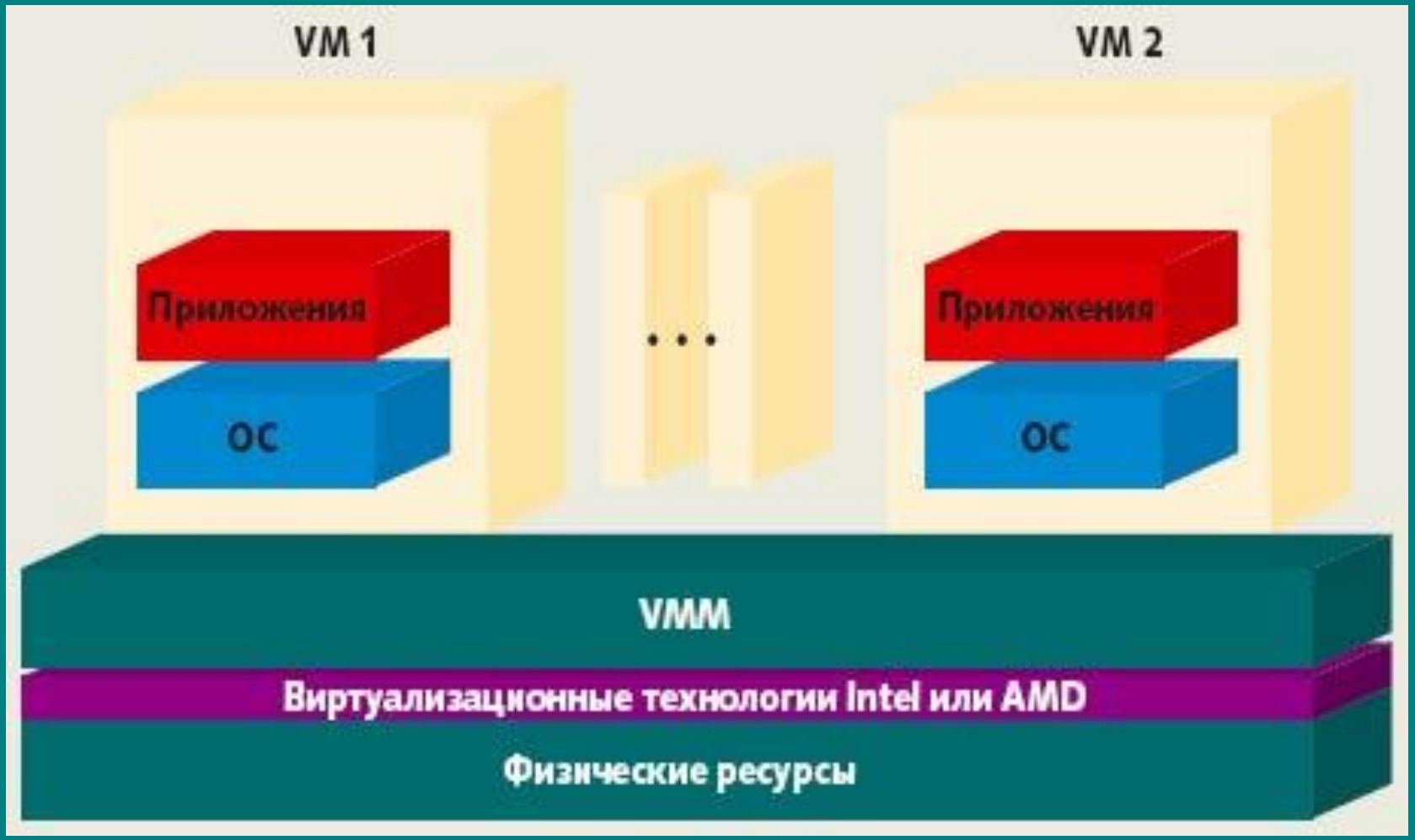
Три типа виртуальных машин с VMM



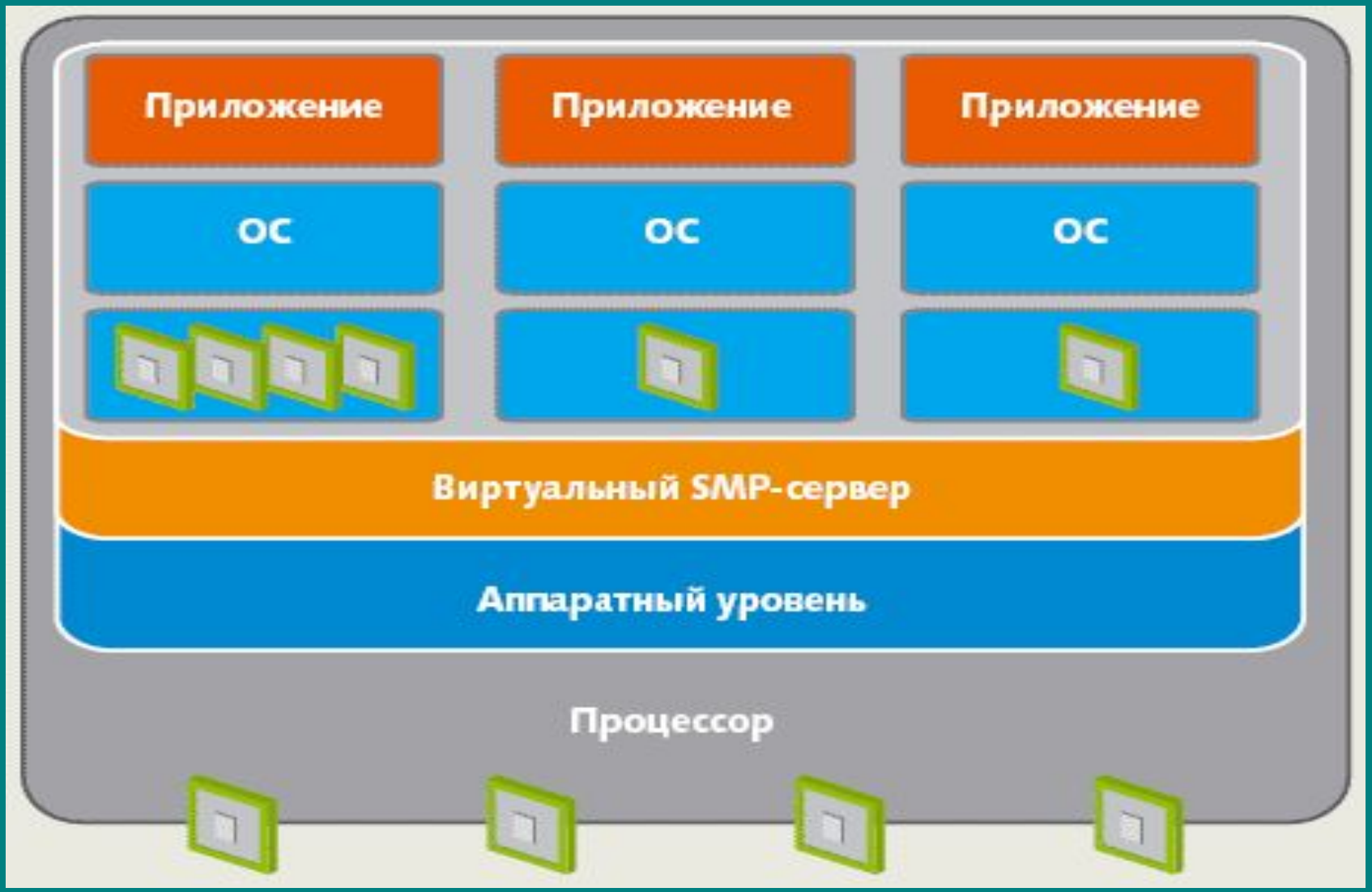
УПРОЩЕННАЯ МОДЕЛЬ ВИРТУАЛИЗАЦИИ СЕРВЕРОВ (виртуализация на «голом железе» по типу 1)



Аппаратная поддержка виртуальных машин (по типу 1)



Виртуальный SMP-сервер VMWare Virtual SMP



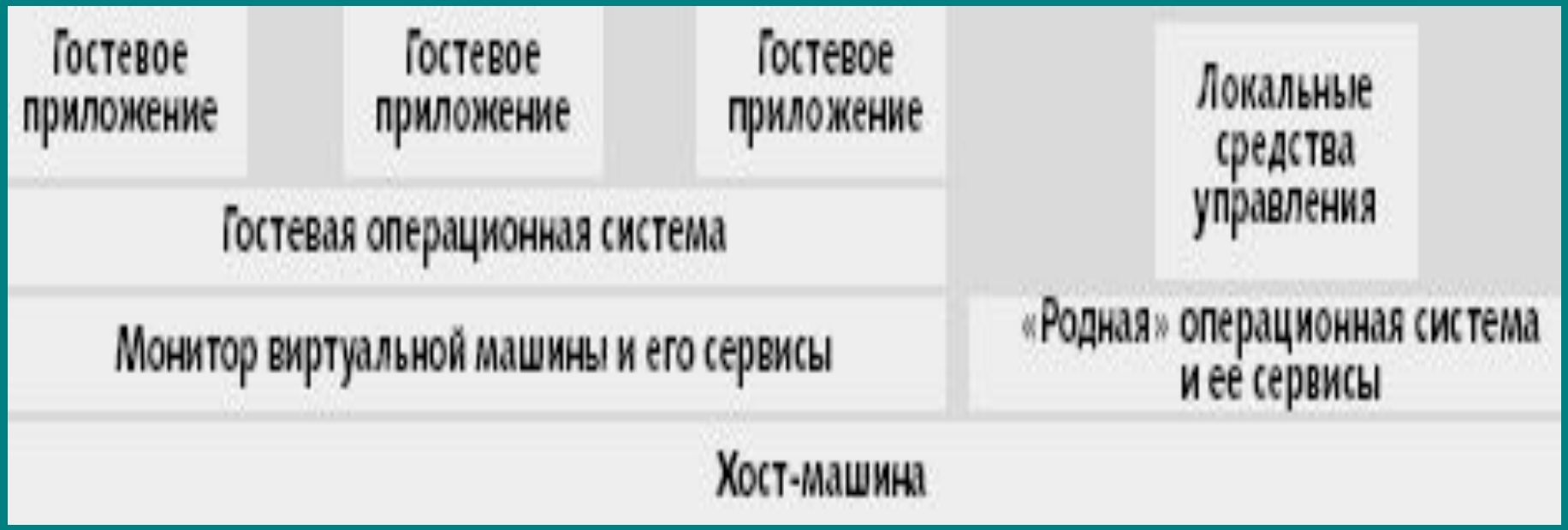
Архитектура Windows Server Virtualization

Виртуализация на базе VMWare ESX Server (тип 1)

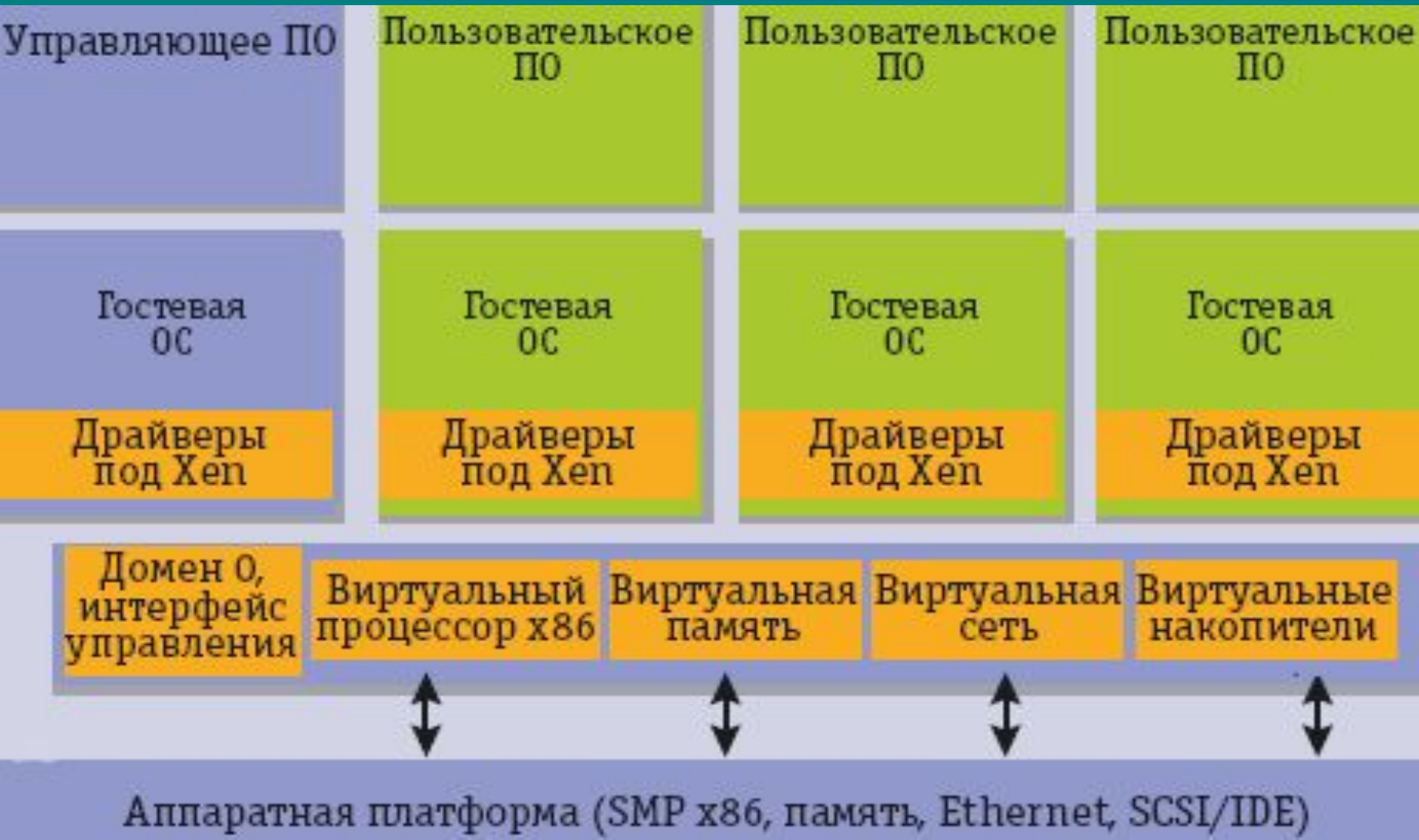
Виртуализация VMWare GSX Server/MS Virtual Server 2005 (тип 2)

Архитектура виртуальной системы на базе MS Virtual Server 2005 R2 (Тип 2)

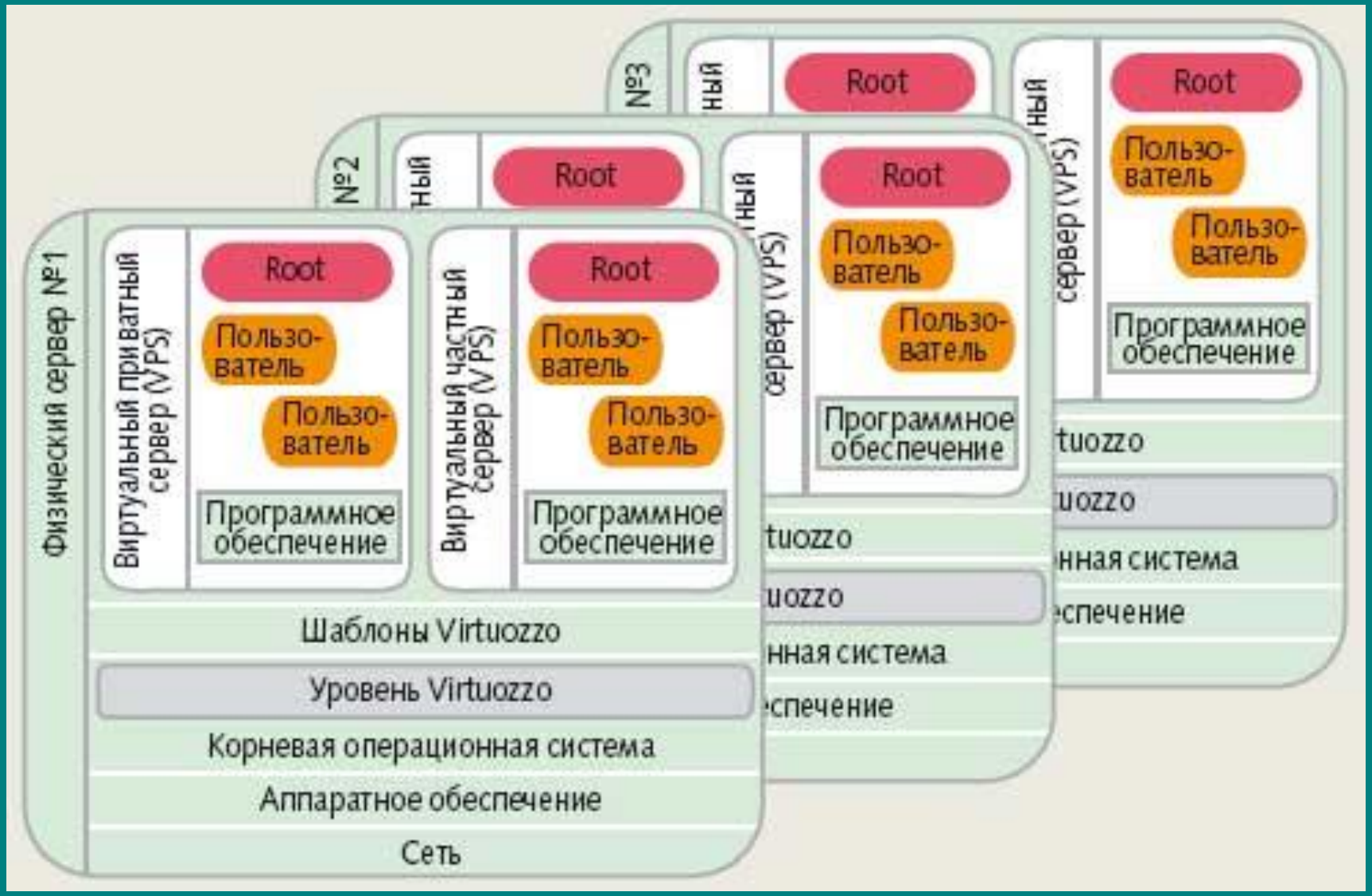
Архитектура с гибридным VMM



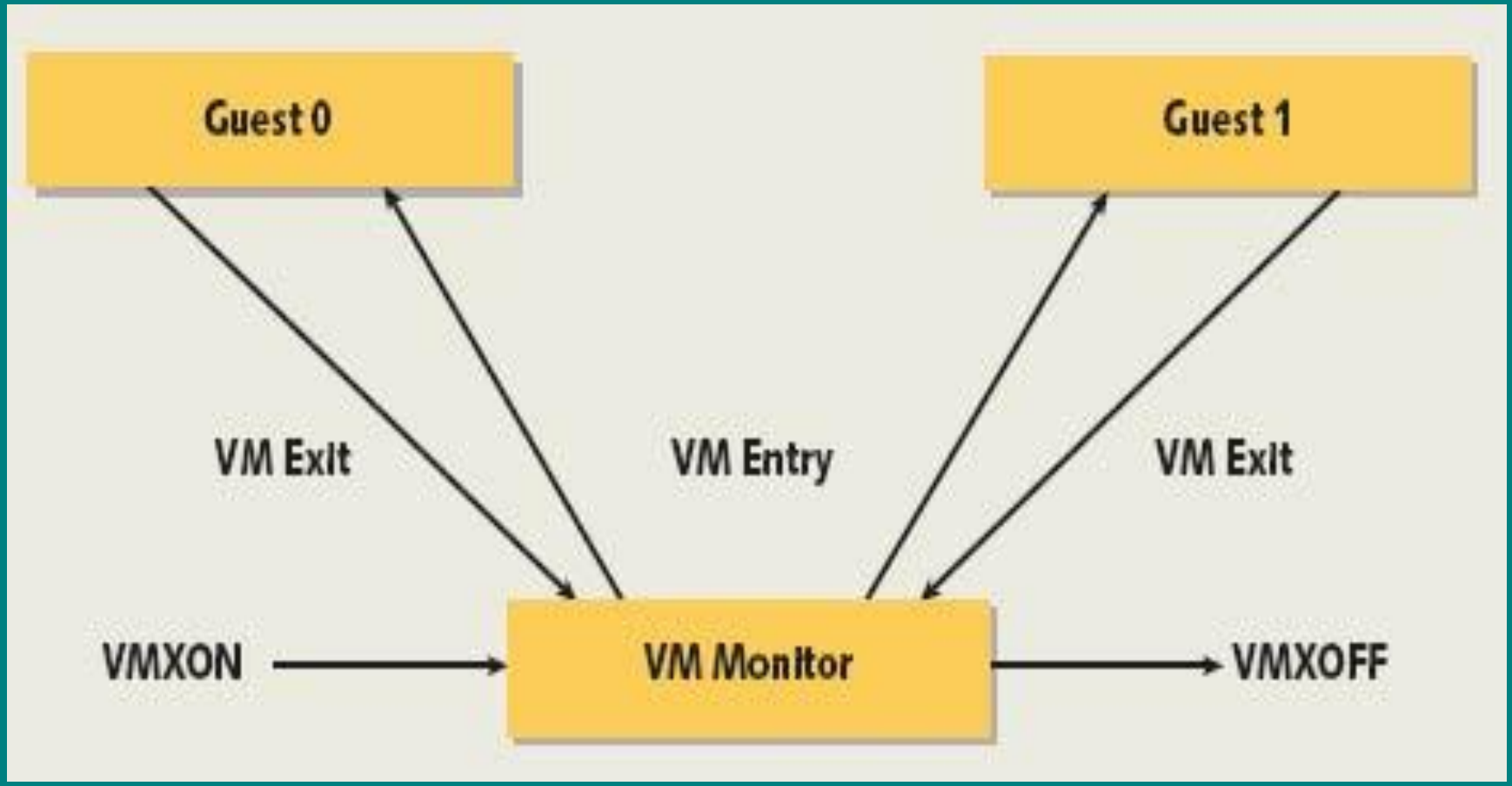
Архитектура гипервизора Xen



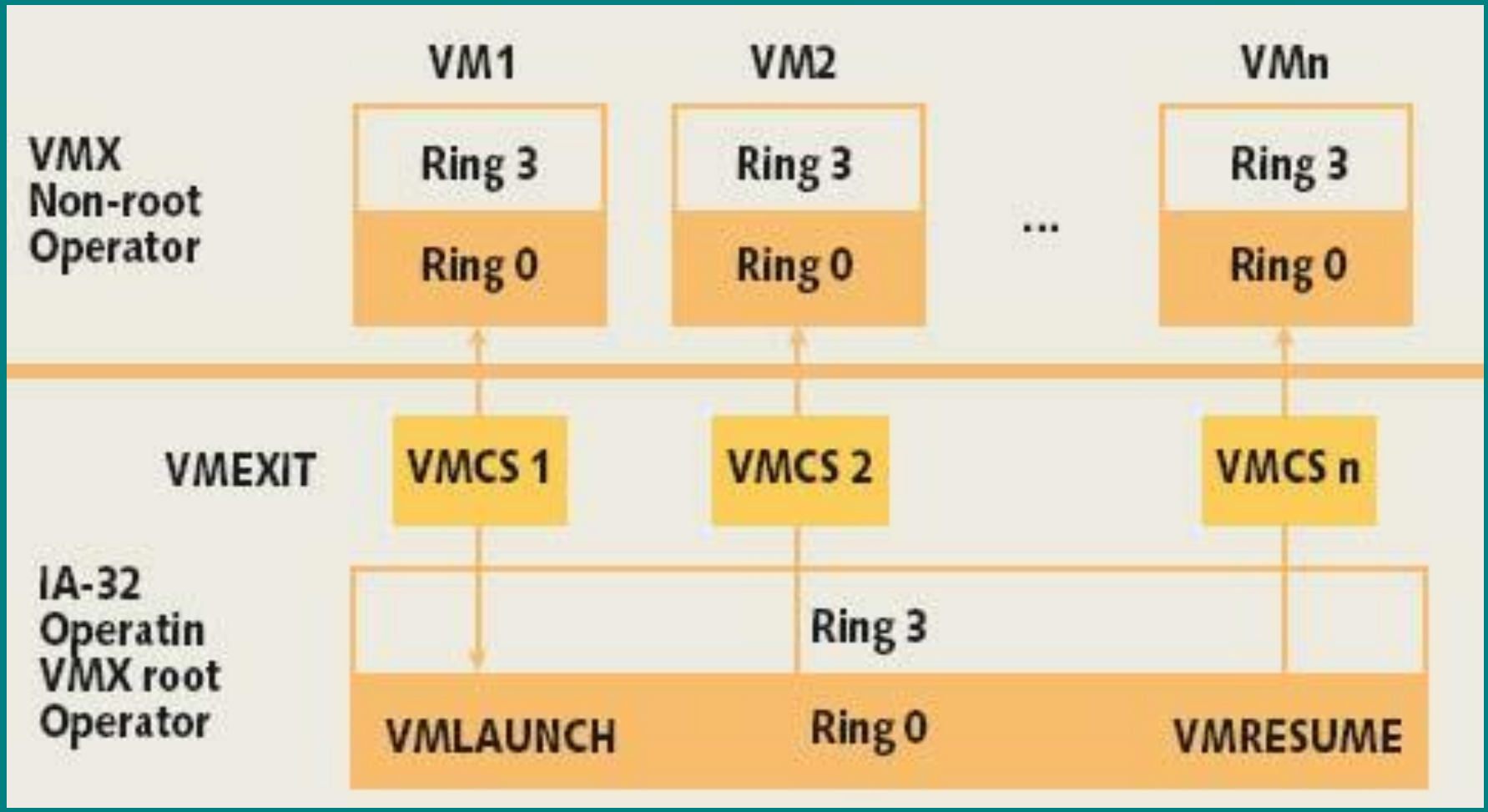
Архитектура высокоуровневой виртуализации Virtuozzo (SWSoft-Parallels)



Жизненный цикл монитора VMM



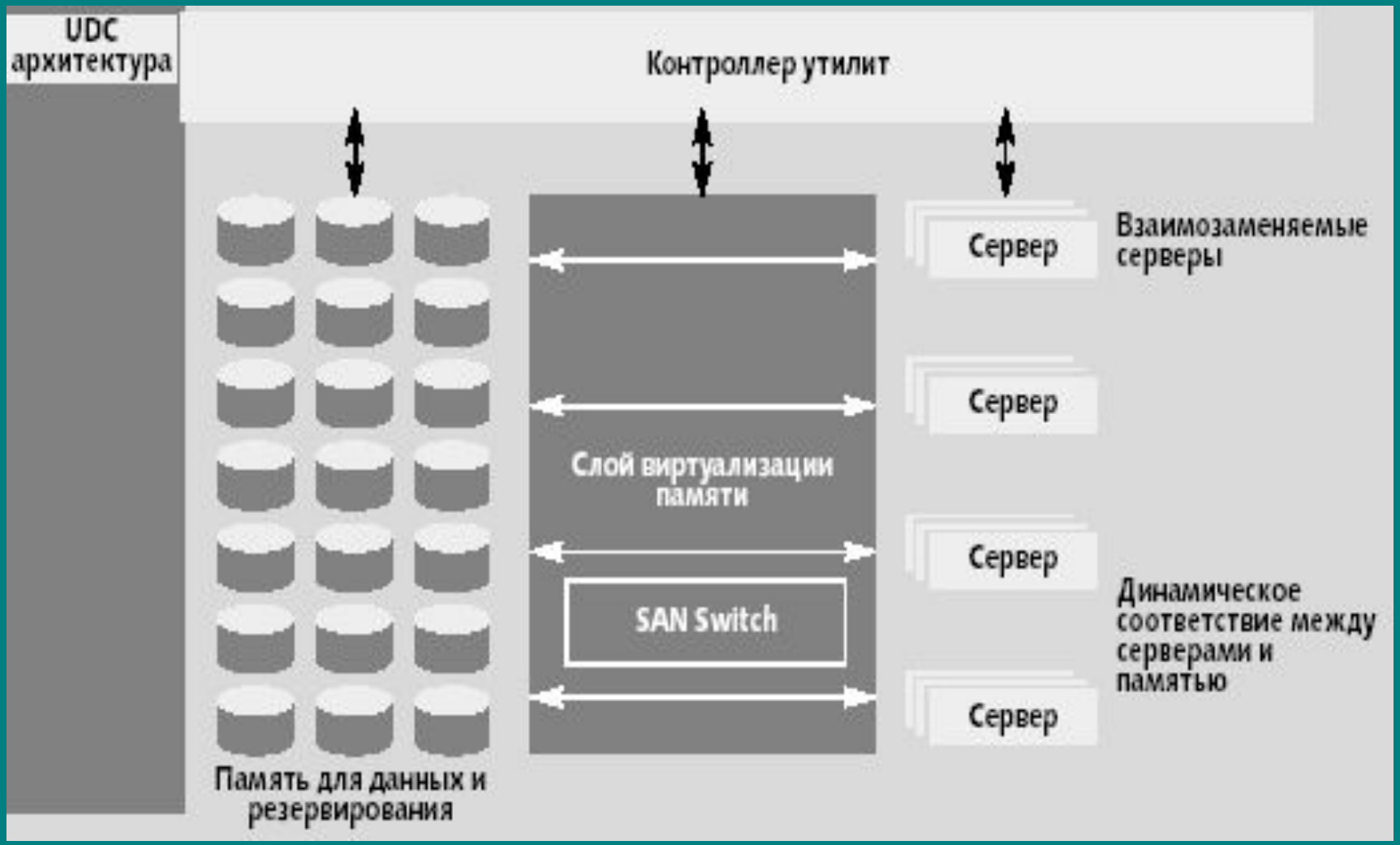
Архитектура Intel Virtualization Technology



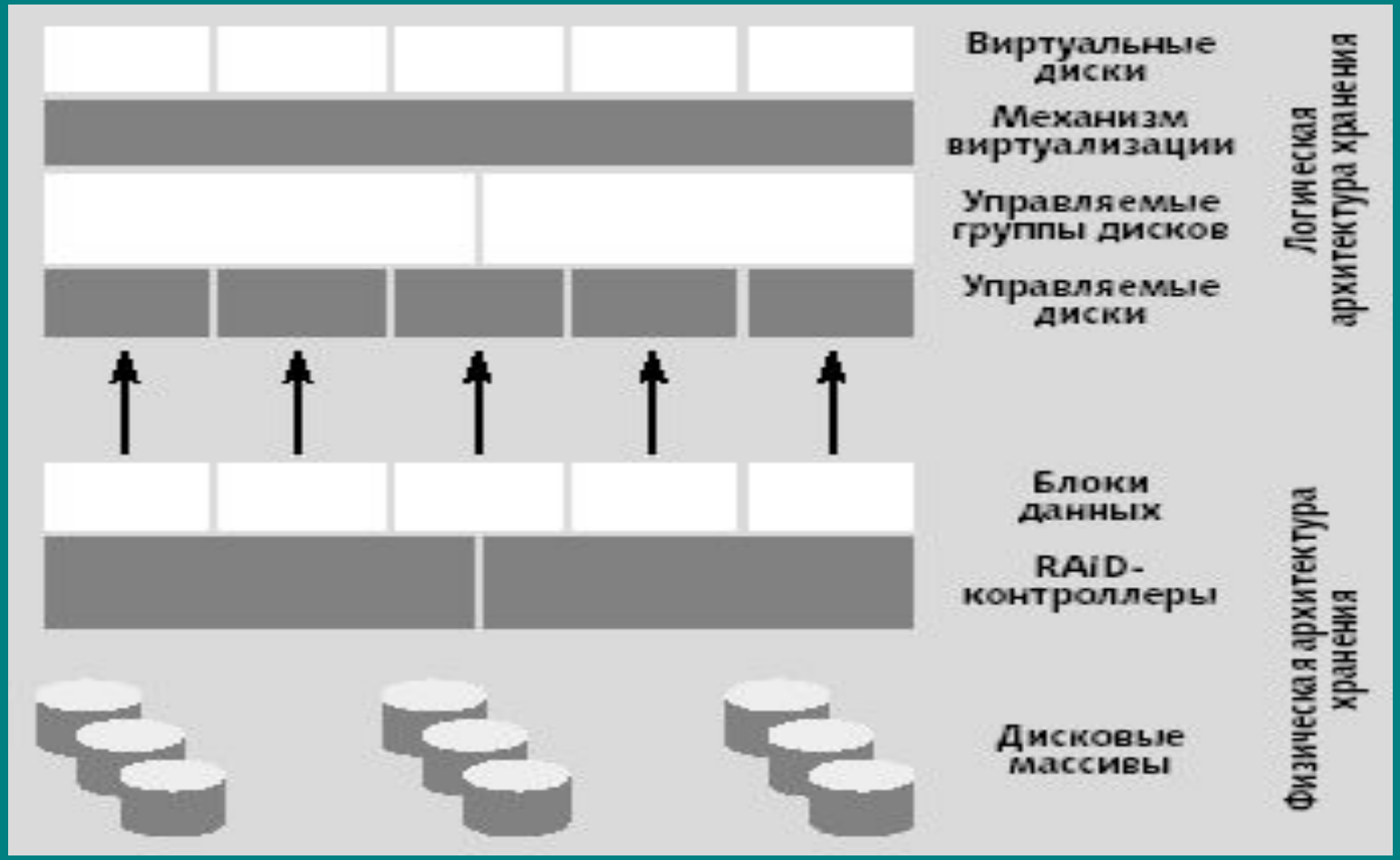
Монитор виртуальных машин в архитектуре Intel-VT

ВИРТУАЛИЗАЦИЯ ПРИЛОЖЕНИЙ (архитектура системы на базе MS Soft Grid)

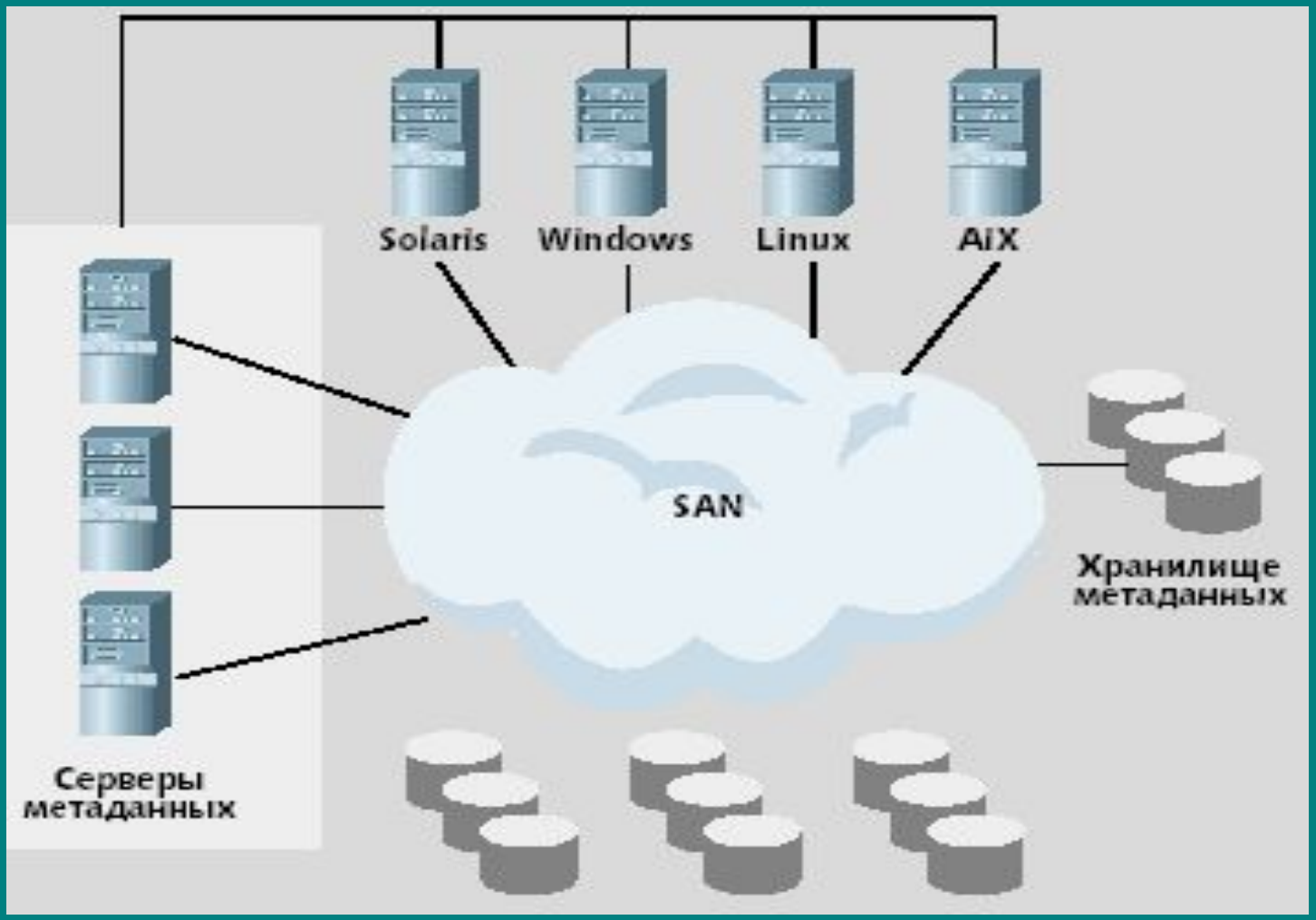
ВИРТУАЛИЗАЦИЯ ПАМЯТИ



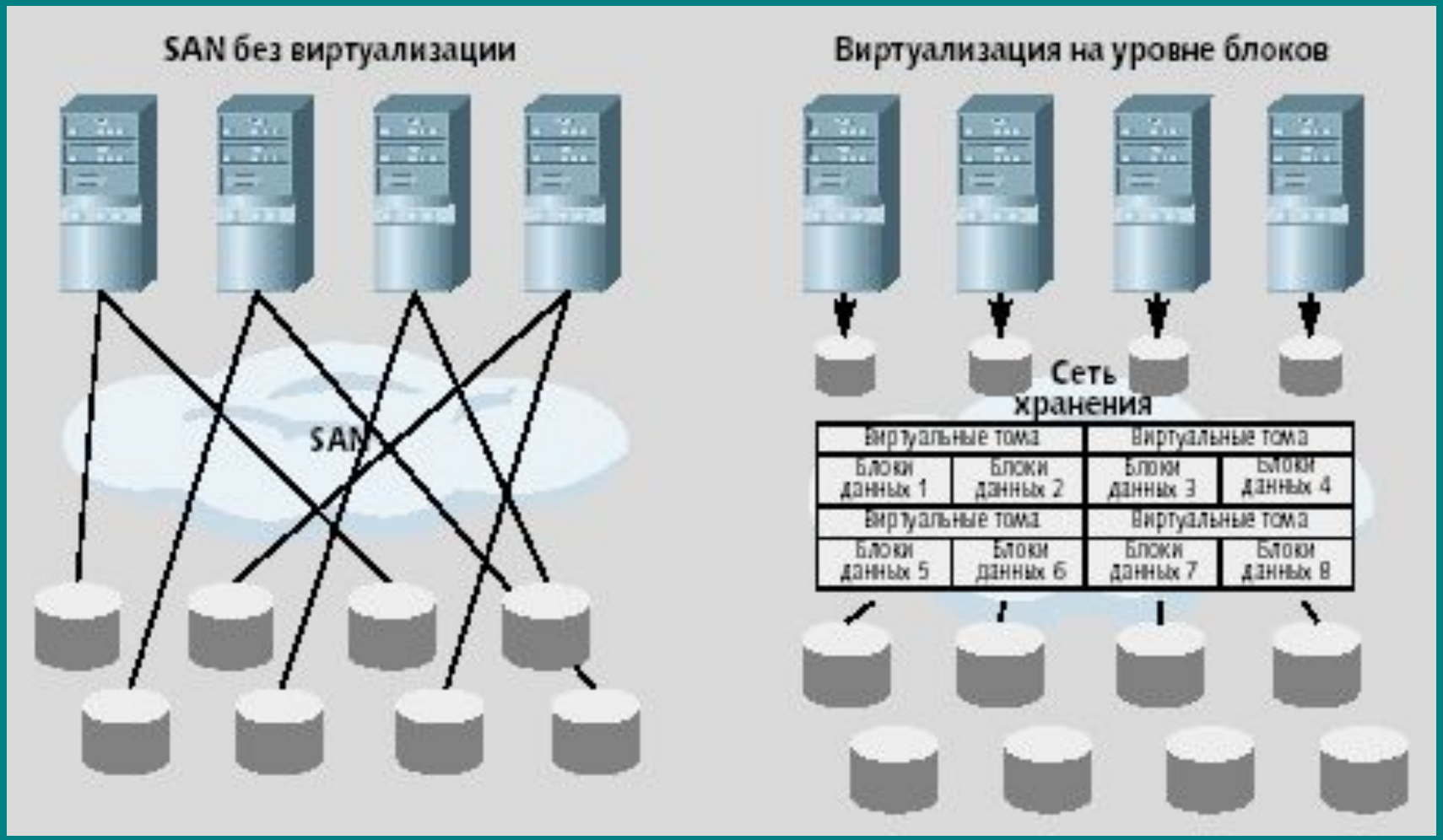
Виртуализация и управление сетями хранения (SAN)



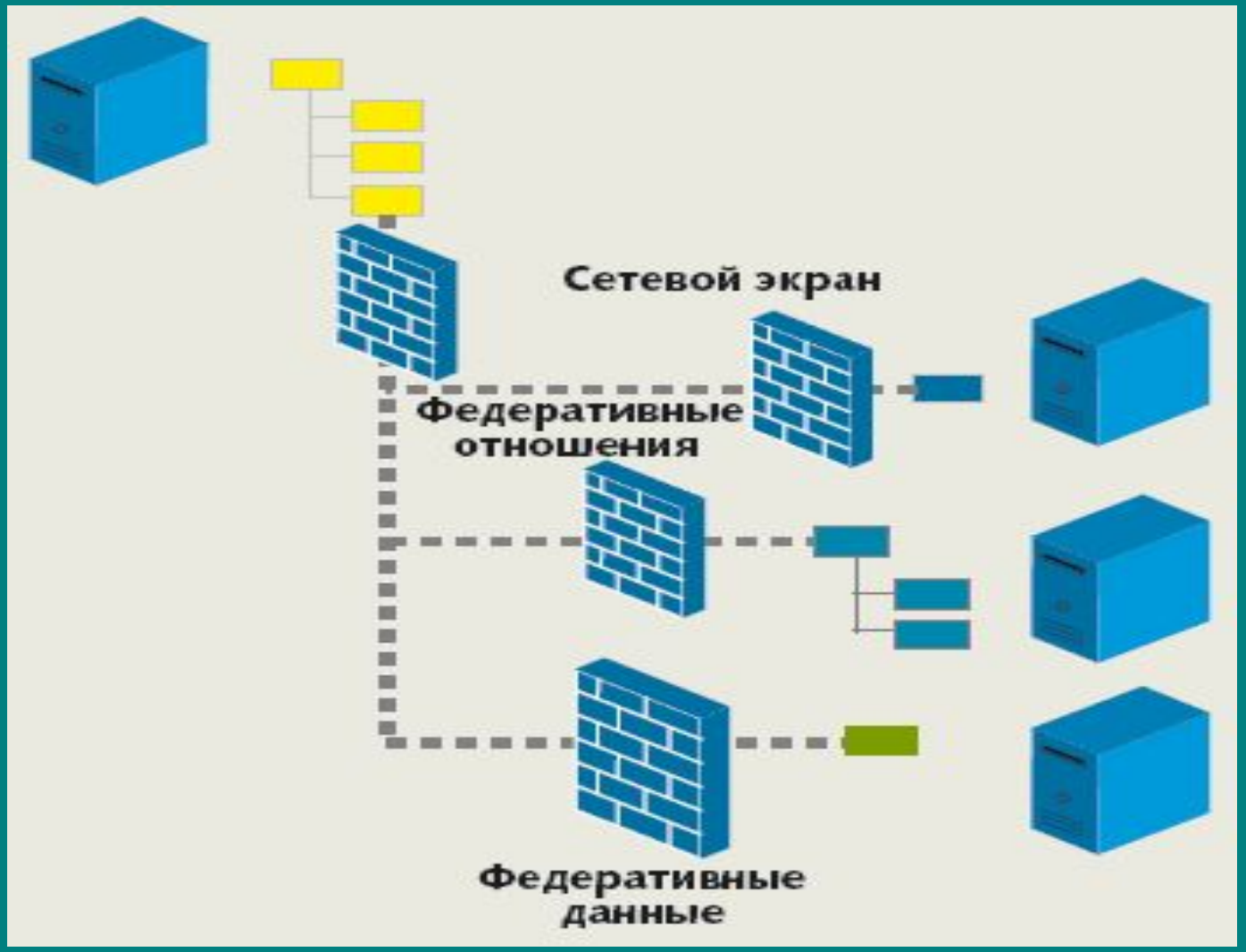
Виртуализация на уровне данных



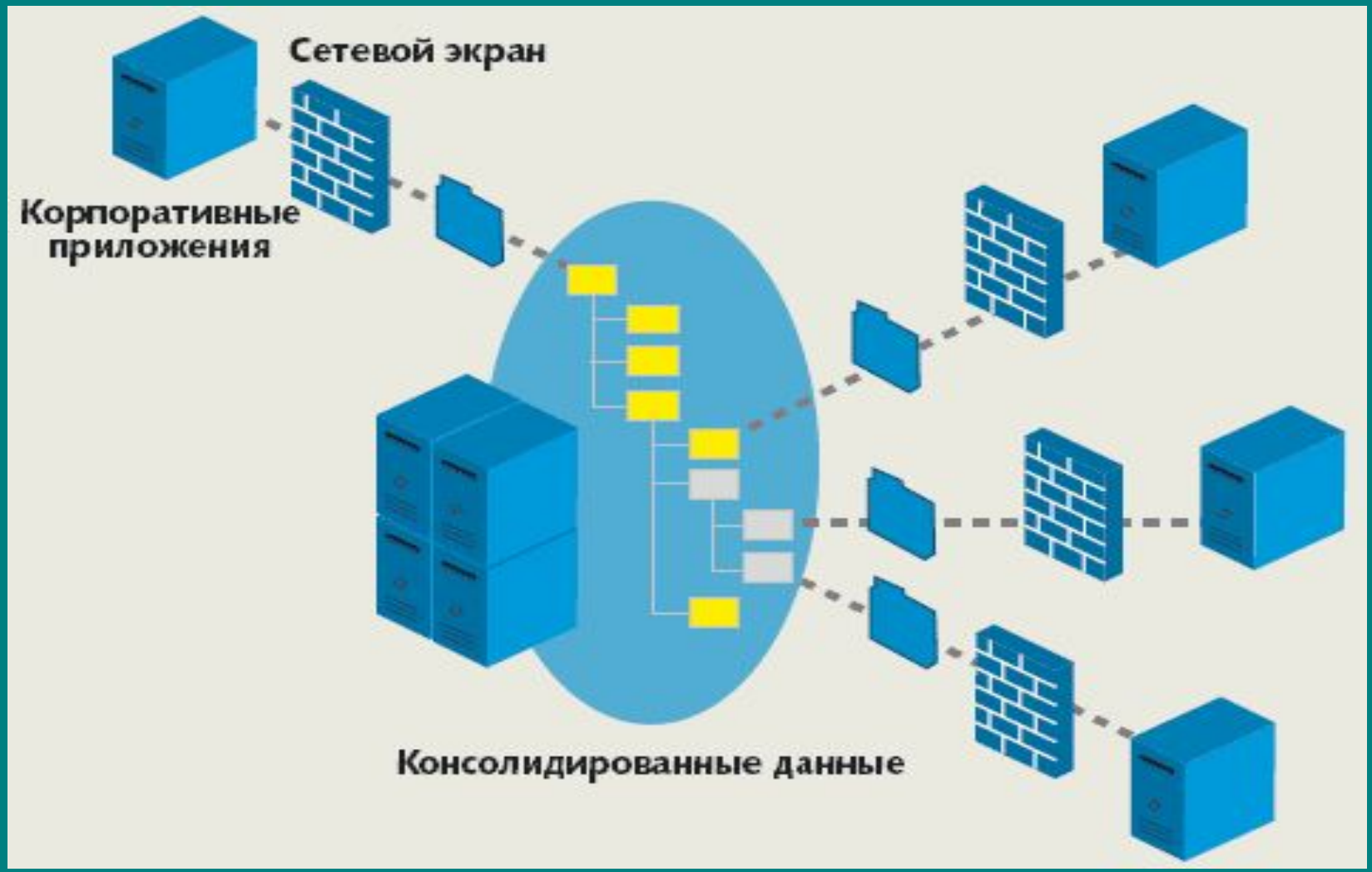
Виртуализация данных на уровне блоков



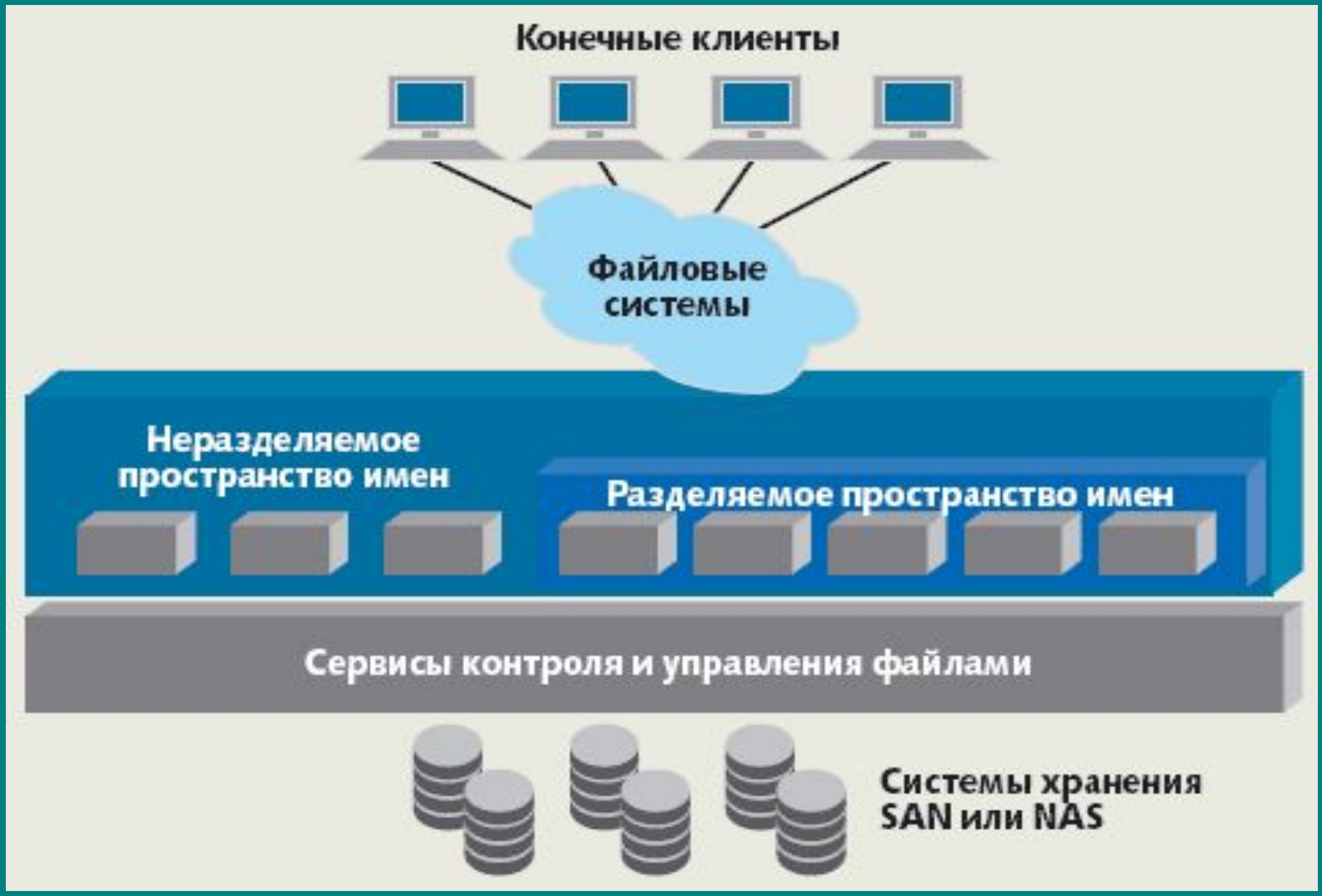
Федеративная архитектура системы хранения данных (традиционная)



Консолидированная архитектура системы хранения данных

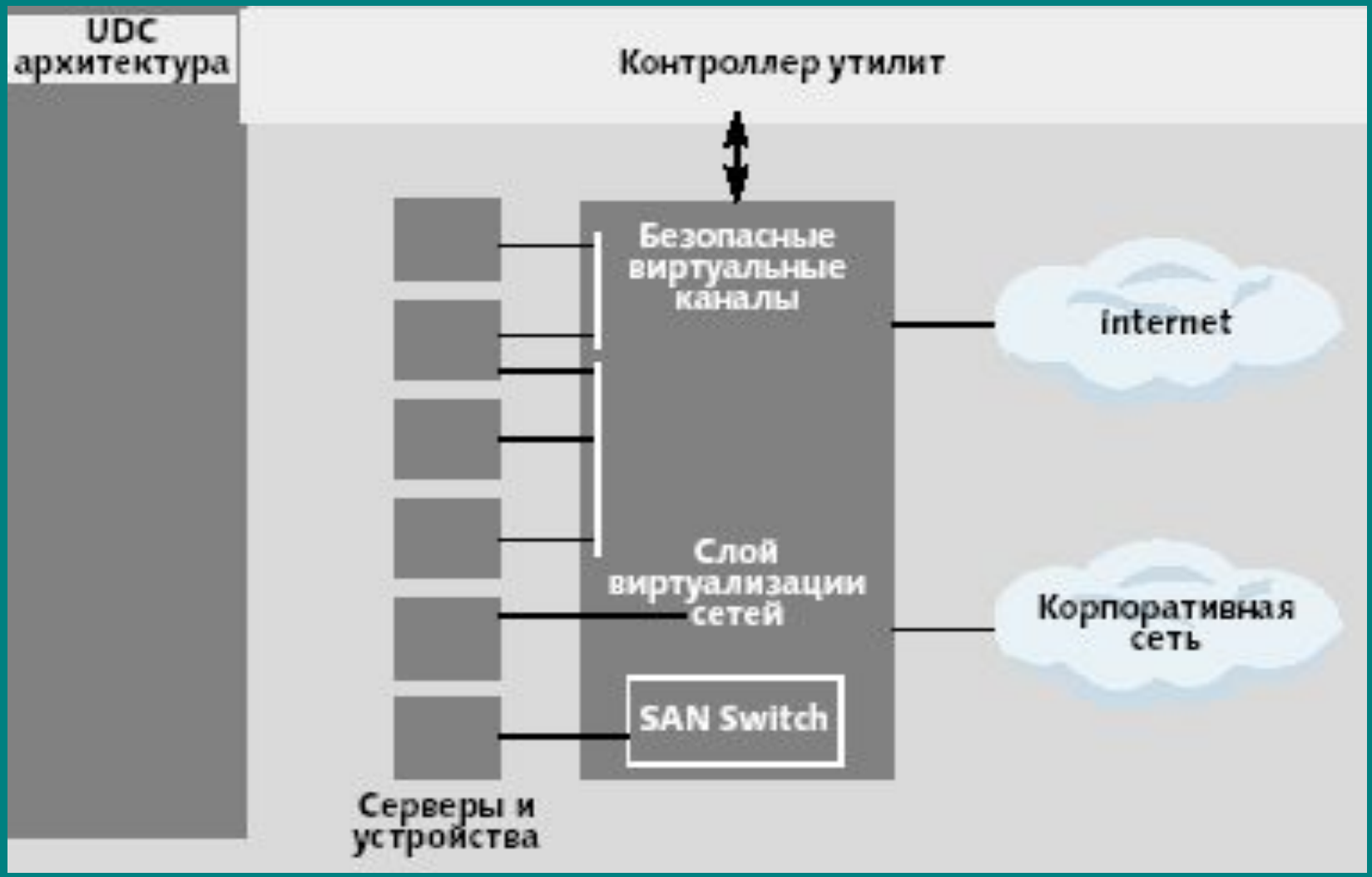


Консолидированная архитектура хранения FAN

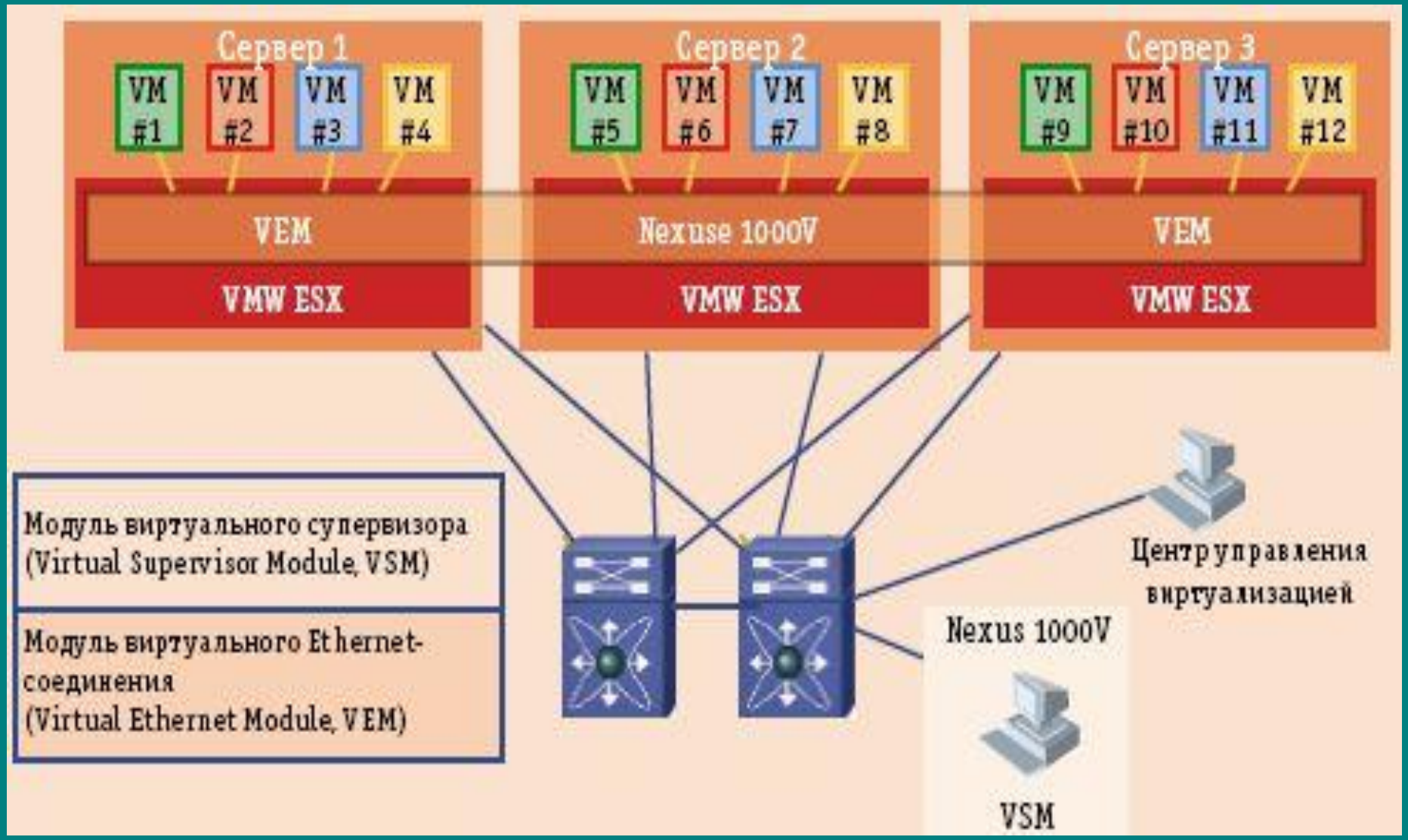


FAN – File Area Networking

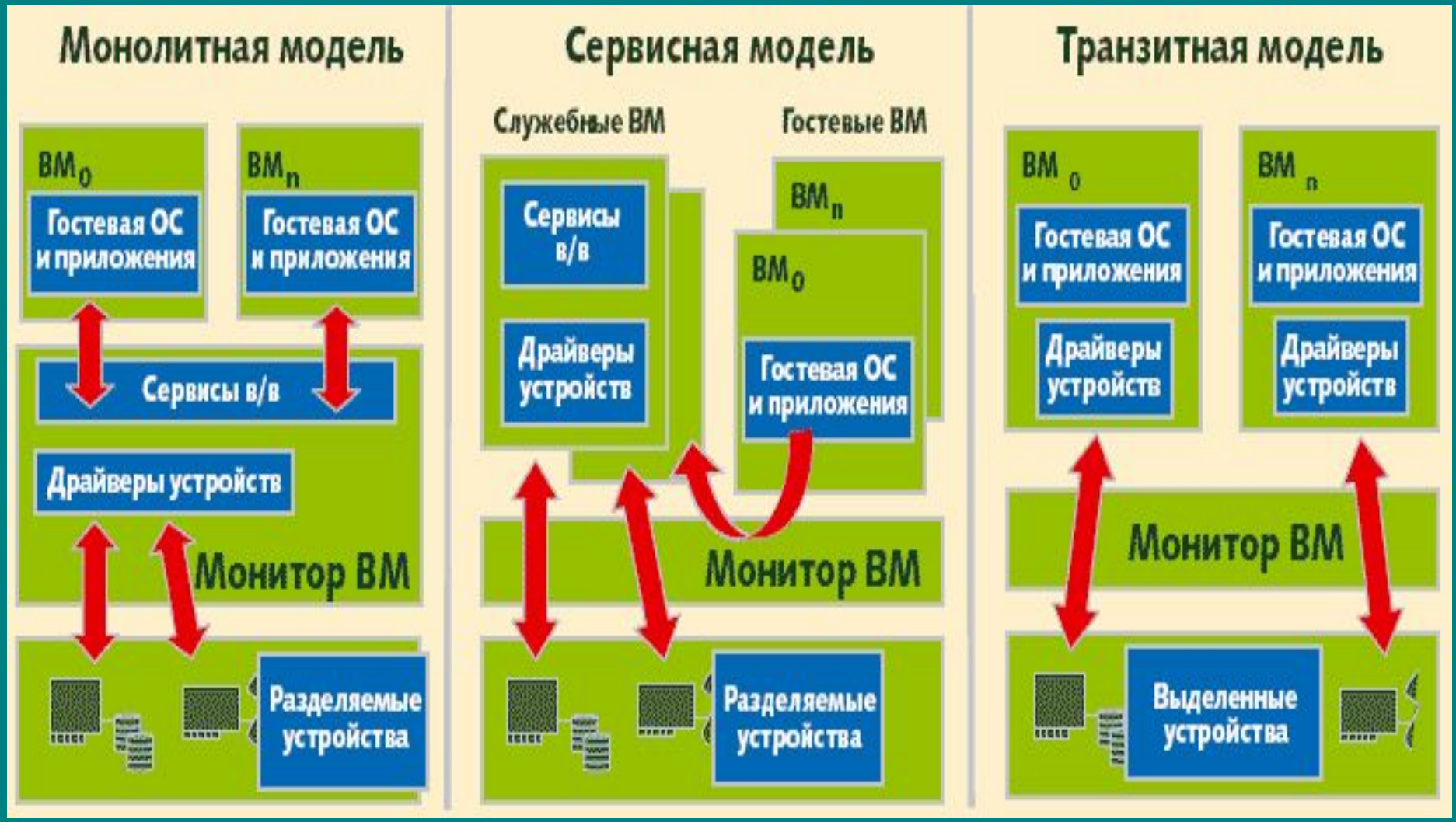
ВИРТУАЛИЗАЦИЯ СЕТЕЙ



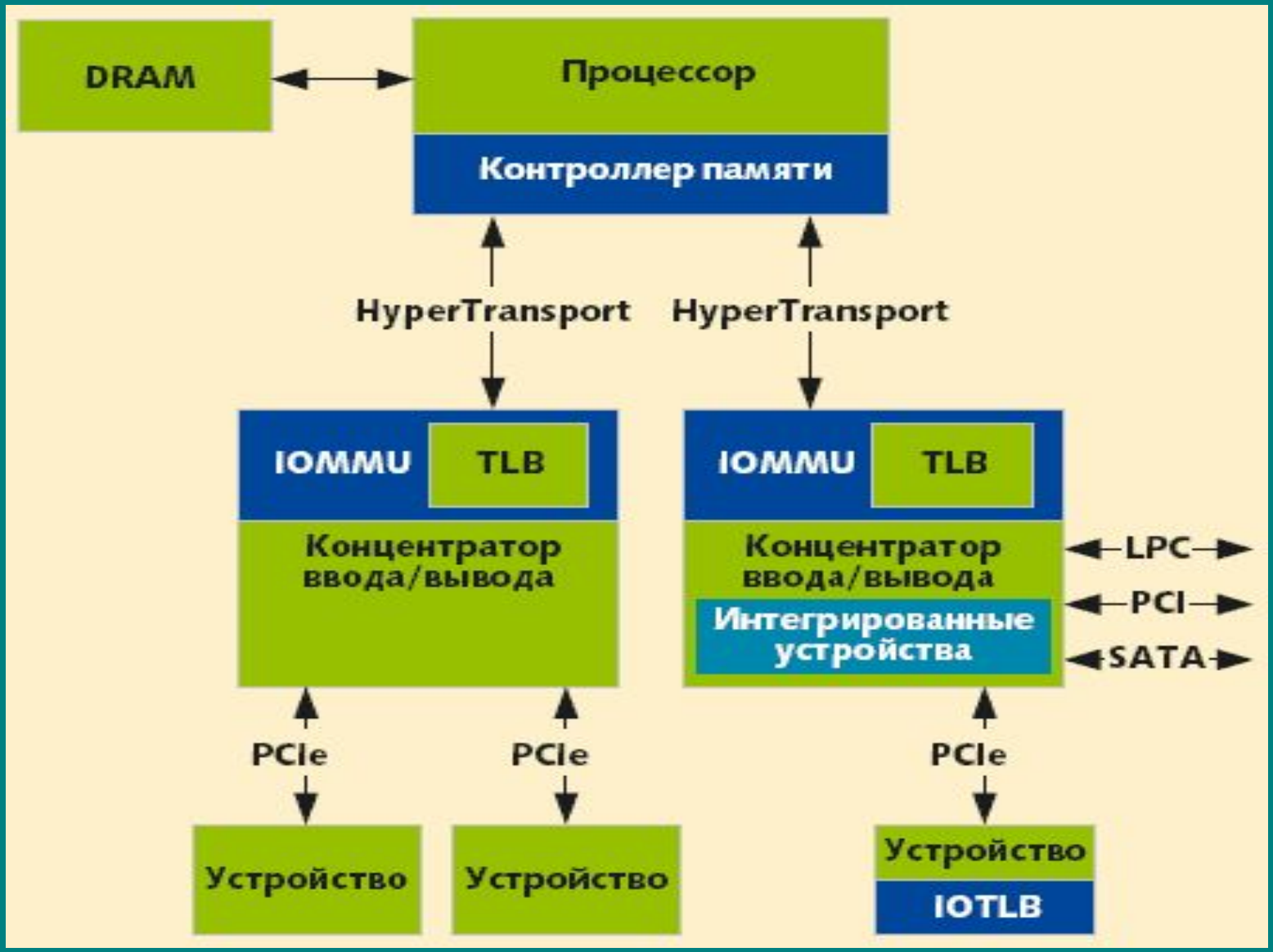
Архитектура виртуализации на базе Cisco Nexus 1000V



Базовые модели виртуализации ввода-вывода



Технология виртуализации ввода - вывода

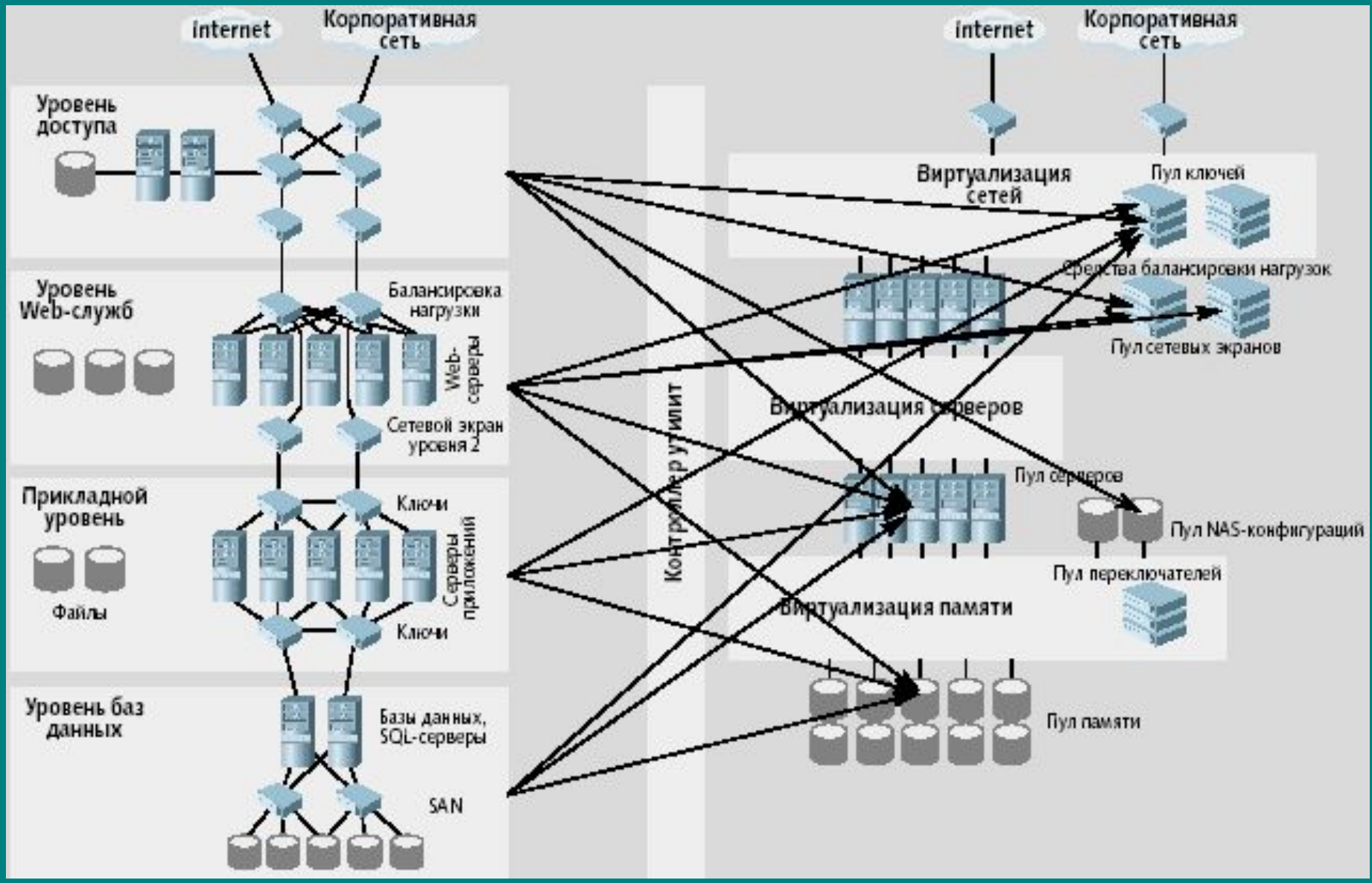


Развитие взглядов на архитектуру ЦОД

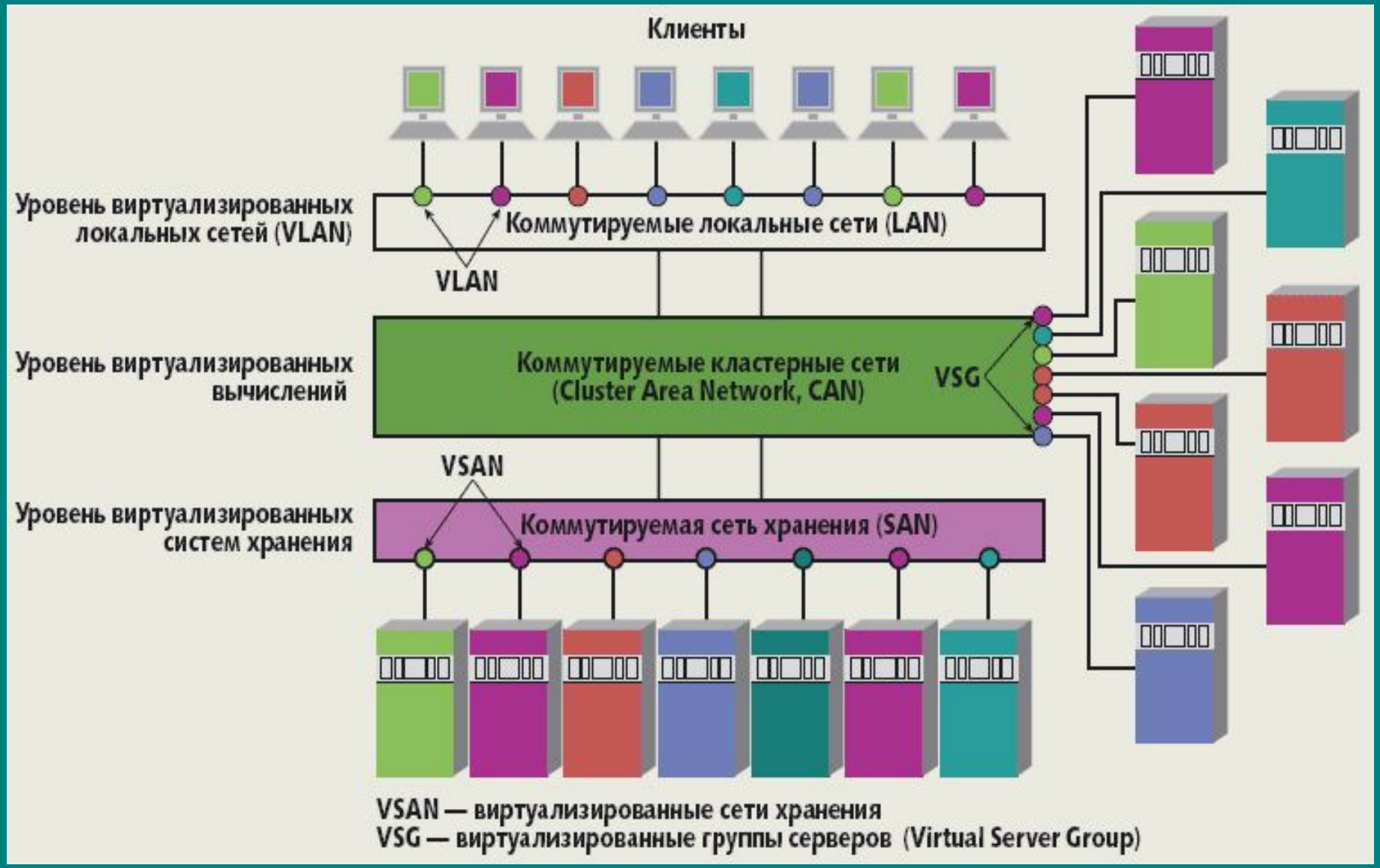
Архитектура перспективного (Next Generation) ЦОД

Многоуровневая модель перспективной архитектуры ЦОД

Виртуализация центров обработки данных



Архитектура полностью виртуализированного ЦОД



Виртуальные предприятия и виртуальная экосистема

Проблемы информационной безопасности в свете виртуализации ИТ-инфраструктуры предприятия

Безопасность виртуальных решений

Комплекс проблем, связанных с обеспечением безопасности любых виртуальных ИТ-систем, в том числе и виртуализованных серверов стандартной архитектуры, по целому ряду причин существенно сложнее, чем это может показаться на первый взгляд. В них, по сравнению с традиционными системами, резко возрастает число потенциальных угроз, причем множество возникающих проблем, как правило, разделено тонкой гранью на два очень близких подмножества.

Все направление в целом именуется как «Virtualization Security», что можно перевести как «виртуализация и безопасность», а упомянутые два подмножества обозначаются как «virtualizing security» и «securing virtualization». Первое из них, правильнее всего, можно определить как «безопасность технологий виртуализации», а второе – как «виртуализация средств безопасности» (см. след. слайд).

Неизвестные ранее сложности, связанные с обеспечением безопасности, возникают по причине динамической природы виртуальных систем, которые в процессе их жизненного цикла создаются, функционируют, уничтожаются и мигрируют. Поэтому в таких системах невозможно снабдить каждый элемент, подвергаемый новым типам угроз, статическими средствами защиты, как это делается в классических системах. Отсюда потребность в виртуализации «второго порядка» – т.е. в виртуализации самих средств обеспечения безопасности.

Безопасность в разрезе виртуализации

Специфика безопасности в виртуальных средах

- Информация обрабатывается в гостевых машинах, которые находятся под полным контролем гипервизора, способного незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства;
- Администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору, становится критически важным субъектом безопасности системы – фактически он может получить доступ к ресурсам в обход существующей политики информационной безопасности;
- Средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение к ним дает возможность получить доступ к гипервизорам серверов виртуализации, а затем и к конфиденциальным данным, обрабатываемым на гостевых машинах;
- Традиционные средства защиты информации, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора, являющегося фактически нарушителем, реализующим атаку «человек посередине», при взаимодействии гостевой ВМ с устройствами;
- Диски гостевых машин обычно размещаются в сетевых хранилищах, которые должны физически защищаться как самостоятельные уст-ва;
- Традиционные МЭ не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, однако этот сетевой трафик не покидает сервера виртуализации и не проходит через физические МЭ и другое сетевое оборудование;
- Каналы передачи служебных данных серверов виртуализации обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые могут содержать конфиденциальные данные.

Анализ уязвимостей виртуальной среды

Программное обеспечение системы управления виртуальными машинами имеет обычные уязвимости, как и обычное ПО, с тем отличием, что здесь особо угрожающим является проникновение, при котором взломщик не просто пробивает брешь, а получает доступ ко всему внутреннему пространству – получает «ключи от замка» (keys to the castle). Другая часть уязвимостей относится к операционным угрозам, и она возникает в случаях, когда персоналу не хватает знаний и умений для работы с виртуальной средой, и тогда могут возникнуть эпизоды, подобные «эффекту домино».

Специфические уязвимости виртуальных машин (ВМ) связаны с операционными угрозами, они могут быть вызваны неконтролируемой экспансией виртуальных машин, неопределенностью состояния ВМ (приостановлена/активна), динамической миграцией (Live Migration), подверженностью атакам типа воспроизведения (Replay Attacks) и удержания данных (Data Retention).

Виртуальные машины могут «похищаться» поодиночке или даже целыми группами. При этом гипервизор, адаптированный к определенной аппаратной платформе, тоже может быть атакован с использованием так называемых «руткитов» (Hardware Virtualization Rootkits). Обнаружение и борьба с ними на пользовательском уровне очень сложны, т.е. надо делать более защищенные гипервизоры. Так, в VMware изначально проектировали свои продукты с учетом необходимости в обеспечении безопасности ВМ.

УЯЗВИМОСТИ ВИРТУАЛЬНОЙ СРЕДЫ

Новые риски безопасности

Виртуализация порождает новые риски, которые можно разделить на две категории. Возникновение первой группы рисков связано с тем, что виртуальная среда динамична, а многие методы администрирования рассчитаны на статические системы. Риски этого типа усугубляются тем, что автоматизация управления еще недостаточно развита, а виртуализация требует существенного человеческого участия, причем 90% системных нарушений порождают люди. Когда все серверы собраны в одну стойку и виртуализованы, создается ложное впечатление, будто кроме специалистов по виртуализации теперь никто больше и не требуется. Однако специалисты по виртуализации априори не могут обладать требуемой для обеспечения безопасности квалификацией (это не их профиль!).

Проблема усложняется тем, что виртуальная инфраструктура менее удобна для обновления, поскольку она не статична. Еще больше проблем возникает в связи с тем, что серверы могут «мигрировать», а в процессе миграции создаются условия для их перехвата и подмены. Шифрование, возможно, единственный способ борьбы с последствиями хищения виртуальных машин, но возникает конфликт между безопасностью и производительностью: для большей безопасности следует установить криптографическую защиту на путях миграции серверов, но это приведет к замедлению каналов связи. Поэтому передача ВМ в процессе оперативной миграции серверов осуществляется открытым текстом, оставляя тем самым возможность для атак типа «человек посередине».

Новые риски безопасности (окончание)

Вторая группа рисков связана с эффектом множественности ВМ. Сосуществование в одной системе нескольких десятков или даже тысяч виртуальных серверов может приводить к неожиданным (для системных администраторов) результатам.

Возможность неконтролируемого создания новых виртуальных машин без дополнительных значительных инвестиций может привести к неадекватному разрастанию их числа, это явление получило специальное название Virtual Sprawl, «виртуальной экспансии», которая чревата не только увеличением трудозатрат на администрирование, но еще и тем, что система может повести себя совершенно непредусмотренным образом.

Так, при изменении нагрузок может возникать лавинообразный процесс миграции, который в свою очередь будет вызывать каскадные «падения» физических серверов, своего рода «эффект домино». Управление такими конфигурациями ВМ представляет собой отдельную сложную задачу. На данный момент ее решение осуществляется чисто интуитивными методами.

Перечень новых угроз для виртуальной инфраструктуры:

- Атака на гипервизор с виртуальной машины;
- Атака на гипервизор из физической сети;
- Атака на диск виртуальной машины;
- Атака на средства администрирования виртуальной инфраструктуры;
- Атака на ВМ с другой виртуальной машины;
- Атака на сеть репликации виртуальных машин;
- Неконтролируемый рост числа ВМ.

Почему традиционных средств защиты не достаточно

Если нарушитель получает доступ к среде виртуализации, операционная среда традиционных СЗИ оказывается полностью скомпрометированной.
Тогда, из среды гипервизора нарушитель может *незаметно для традиционных СЗИ, работающих на виртуальных машинах*:

- **Копировать и блокировать все потоки данных, идущие на все внешние устройства (HDD-устройства, принтеры, USB-порты, сеть, дискеты и т.д.);**
- **Читать и изменять данные на дисках виртуальных машин даже тогда, когда они физически выключены и не работают, т.е. без участия системного программного обеспечения этих виртуальных машин (!!!).**

Атака на гипервизор

Описание угрозы:

1. Нарушитель может совершить НСД к серверу виртуализации (т.е. фактически, к самому гипервизору)
2. Сам сервер виртуализации может содержать ошибки и уязвимости (ошибки разработчиков гипервизора).

Пример:

Уведомление о безопасности: VMSA-2009–0007(DoS-уязвимость продуктов VMwareESX и ESXiom 1 июня 2009)
http://securityvulns.ru/Vdocument916.html

Меры защиты:

1.Своевременная установка обновлений ПО среды виртуализации
2.Ограничение запуска программ при помощи СЗИ и/или орг. мероприятий (на усмотрение администратора системы или служб ИБ).

Атака на диск виртуальной машины

Описание угрозы:

В «физическом мире», чтобы похитить HDD компьютера, нужно получить к нему непосредственный доступ, вскрыть корпус и демонтировать диск. В виртуальном ИТ-пространстве достаточно скопировать файл, содержащий полный образ HDD виртуальной машины.

Меры защиты:

Защита данных виртуальных машин путем разграничения доступа к дискам виртуальных машин, реализуемого сертифицированными СЗИ от НСД и МЭ, контролирующими протоколы и файловые форматы виртуальной инфраструктуры (SCSI, iSCSI, VMFS, LUN masking и т.п.).

Примечание. Есть также особые нетрадиционные приемы.

Атака на средства администрирования

Описание угрозы:

Получив доступ к средствам администрирования, нарушитель получает возможность по похищению, уничтожению, искажению любых данных во всей виртуальной ИТ-инфраструктуре.

Меры защиты:

Защита периметра сети администрирования путем разграничения доступа к серверам виртуальных машин и средствам управления ИТ-инфраструктуры. Защита может быть реализована комбинированием сертифицированных средств защиты: МЭ и СЗИ от НСД, устанавливаемых на средства администрирования виртуальной инфраструктуры и по периметру сети управления.

Атака на виртуальную машину с другой виртуальной машины

Описание угрозы:

Виртуальные машины одного физического сервера могут обмениваться трафиком напрямую, т.е. без участия физических сетевых коммутаторов. Таким образом, использование физических МЭ не будет эффективным.

Меры защиты:

Модернизация существующих МЭ, их перенос в виртуальную среду. Создание специализированных СЗИ от НСД и МЭ, контролирующих трафик внутри сервера виртуализации (эмуляция сверхнадежных МЭ).

Атака на сеть репликации виртуальных машин

Описание угрозы:

По сети репликации виртуальных машин передаются сегменты их оперативной памяти. Средства виртуализации не осуществляют шифрование этих данных. Возможность перехвата этих данных — прямая угроза безопасности.

Меры защиты:

Сеть репликации должна быть изолирована от остальных сетей организационными мерами, либо потребуется обязательное использование СКЗИ для соответствующих каналов репликации .

Неконтролируемый рост числа виртуальных машин

Описание угрозы:

Простота создания и ввода в эксплуатацию виртуальных машин может создать проблемы для безопасности. Часть новых ВМ не получает должного уровня администрирования: не устанавливаются обновления безопасности, ВМ не настраиваются в соответствии с политикой безопасности.

Меры защиты:

Требуется организация централизованного процесса управления жизненным циклом ВМ, регламентированное управление назначением прав, централизованный механизм установки обновлений на виртуальные машины.

Средства защиты виртуальной среды

Для защиты виртуальной инфраструктуры могут использоваться следующие продукты:

- **Security Code vGate*for VMware Infrastructure* —для защиты среды виртуализации VMWare ESX Server;**
- **Secret Net 5.1 —для защиты внутри виртуальных машин (при условии обеспечения защиты среды виртуализации), терминальных клиентов и физических рабочих мест;**
- **“Соболь”—для обеспечения контроля целостности и доверенной загрузки элементов администрирования виртуальной инфраструктуры и среды виртуализации;**
- **МЭ 3 класса “Континент”—для разграничения доступа к сети администрирования.**

Итоговые рекомендации

Виртуальная ИТ-инфраструктура повышает степень интеграции вычислительных средств, уменьшая количество физического оборудования при таком же или еще большем количестве сетевых приложений, сервисов, рабочих мест и т.п., что означает усложнение структуры взаимодействия субъектов. Поэтому повышать защищенность виртуальной инфраструктуры нужно комплексно, путем комбинации сетевых и локальных средств защиты с одновременной интеграцией широкого набора механизмов обеспечения информационной безопасности, а именно:

- ✔ средств сетевой аутентификации и авторизации пользователей;
- ✔ межсетевого экранирования как внутри сервера виртуализации между гостевыми машинами, так и по всему периметру создаваемой виртуальной ИТ-инфраструктуры;
- ✔ систем регистрации, сбора и корреляционного анализа событий информационной безопасности;
- ✔ средств разграничения доступа (и делегирования полномочий) к виртуальным машинам и к самому серверу виртуализации (в особенности - к его гипервизору);
- ✔ систем контроля целостности конфигураций распределенных компонентов виртуальной ИТ-инфраструктуры;
- ✔ средств антивирусной защиты и управления доступом ко всем элементам виртуальной ИТ-инфраструктуры.

Технологии «облачной» виртуализации

Что такое «облака»

Cloud Computing («облачные вычисления») – это высокоорганизованная территориально распределенная самоуправляемая компьютерная среда, предоставляющая разнообразные виды ИТ-сервисов конечным пользователям по всему информационному пространству качественно и в полном соответствии с их потребностями. Это новая парадигма предоставления ИТ-услуг «по требованию» с оплатой в полном соответствии с соглашениями по SLA (QoS).

ВИДЫ «ОБЛАЧНОЙ» ВИРТУАЛИЗАЦИИ

Платформные облака

- Тип 1: облако Google
- Тип 2: облако Microsoft
- Тип 3: крупные облака от IBM и Apple, Yahoo!, EMC, HP/EDS, Amazon, Facebook, Adobe и др.

Облака услуг

- Тип 4: облака сервис–провайдеров (массовый рынок хостинга, горизонтальные провайдеры хостинга, Telco/ISP, ISV SaaS, онлайн-услуги, MSP, провайдеры корпоративных клиентов)
- Тип 5: внутренние облака больших компаний, обслуживающие филиалы, отделы, дочерние компании, сотрудников и партнеров

Трехуровневая модель Cloud Computing

«Вычисления в облаке» представляются в виде решений модели *ИТ как сервис* (IT as a service, ITaaS), имеющих трехуровневую архитектуру:

- приложения высокого уровня, предоставляемые по требованию в модели «программное обеспечение как сервис»(Software as a Service, SaaS);
- программное обеспечение промежуточного слоя, предоставляющее сервисы приложений или среду времени исполнения в модели «платформы как сервис» (Platform as a Service, PaaS) для приложений в «облаке»;
- гибкая инфраструктура – и, следовательно, «инфраструктура как сервис» (Infrastructure as a Service, IaaS) распределенных сервисных ЦОД, подключаемых через глобальные сети типа Internet.

Данная трехуровневая архитектура реализуется как на общедоступной основе (то есть через общедоступные «облака», ресурсы которых не принадлежат предприятию), так и на корпоративной основе (частные «облака», ресурсами которых предприятие управляет централизованно). При любой реализации сервисы, предоставляемые через «облако», являются совместно используемыми и удаленными по отношению к конечным пользователям.

Три составляющие Cloud Computing

- IaaS является основой технологии «облачных вычислений», т.е. строительными блоками ИТ-инфраструктуры предприятия. В основном IaaS приобретают и используют ИТ-менеджеры, чьи обязанности связаны с общей обработкой, хранением, управлением базами данных и другими основными ресурсами и ИТ-приложениями. К сервисам данной категории относятся: предоставление по требованию ресурсов центральных процессоров, виртуальный веб-хостинг и хранение по требованию. Самыми заметными решениями в этой области на сегодняшний день являются EC2 компании Amazon, Cloud Servers компании GoGrid и продукты Joyent.
- PaaS – это новая концепция, возникшая почти одновременно с cloud computing. Предоставление платформы в виде сервиса позволяет разработчикам проектировать, создавать и тестировать приложения, работающие в инфраструктуре провайдера «облака», а затем, опять же по запросу, предоставлять эти приложения пользователям. Первыми решениями на этом рынке стали Google App Engine, Microsoft Azure, веб-сервисы Amazon и Force.com компании Salesforce.com.
- SaaS – это способ предоставления сервисов, с которыми непосредственно работает конечный пользователь. Вместо того, чтобы хранить ПО на своем компьютере, пользователь согласно модели SaaS обращается к провайдеру за полнофункциональным приложением. Электронная почта Yahoo, Google Apps, Salesforce.com, WebEx и Microsoft Office Live – это продукты категории «сервисы в облаке».

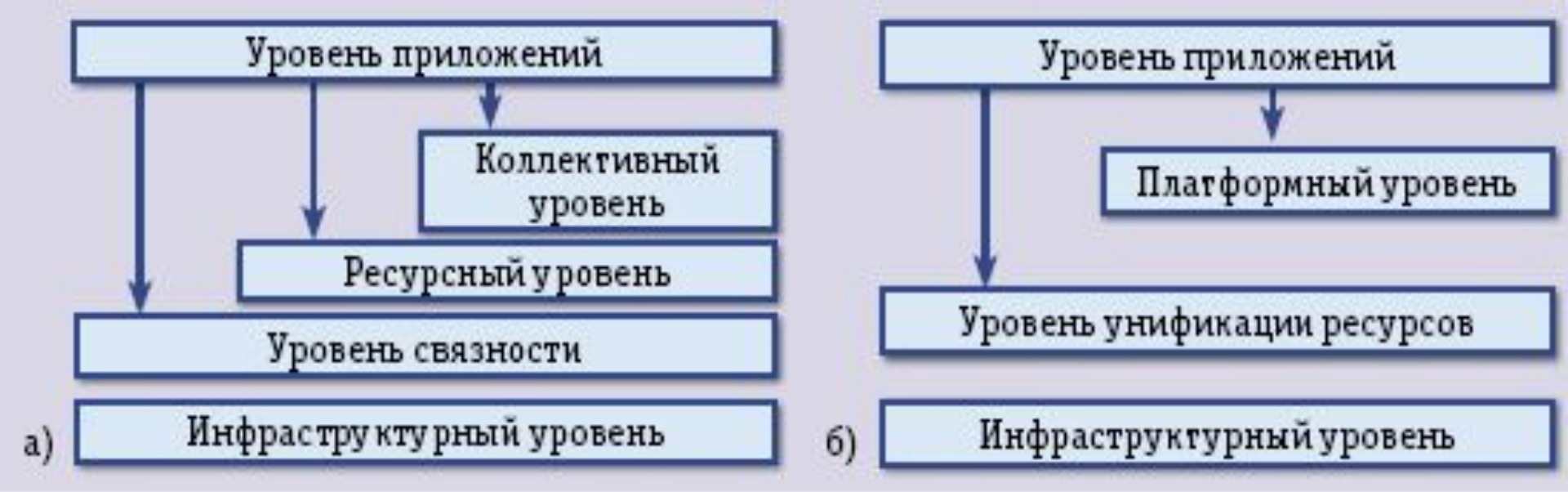
Классическая архитектура «облаков» (Cloud Computing)

Общая характеристика «облачных вычислений»

Помимо очевидной эволюции технологий, «вычисления в облаке» отражают изменения в сфере продаж и предоставления доступа к ИТ. Вычисления в облаке – это альтернатива традиционной стратегии предоставления ИТ, в рамках которой разделяемые удаленные ИТ-ресурсы обеспечивают возможности масштабирования вычислений по IP-сетям в виде платных виртуализованных сервисов, предоставляемых по требованию. В результате на ИТ-рынке сегодня формируется новый взгляд на ИТ-продукты – в эту категорию переходит не только индивидуальное аппаратное и программное обеспечение, но и интегрированные платформы и ИТ-инфраструктуры. По мере того как «облачные» сервисы становятся массовыми, пользователи начинают получать все большую отдачу, поскольку ситуация развивается по восходящей спирали:

- ✔ благодаря усовершенствованиям технологии снижаются расходы на инфраструктуру и появляется возможность увеличить эффективность операций;
- ✔ снижение расходов становится более действенным, давая возможность увеличить экономию, обусловленную ростом масштаба производства, и стимулируя спрос со стороны потребителей ИТ-продуктов и услуг;
- ✔ высокий спрос усиливает конкуренцию, что приводит к снижению цен и способствует росту инвестиций в новые технологии.

Сравнение архитектурных моделей Grid и Cloud Computing



Сравнение архитектур grid (а) и cloud computing (б)

Архитектурные компоненты PaaS

Традиционные платформы	PaaS	
Приложение	Приложение, предоставляемое как сервис	
Интеграция приложений	Программные интерфейсы, технологии «коллажей» приложений (mashup) и интеграции типа SaaS-to-SaaS, а также SaaS в качестве ПО промежуточного слоя	Среда для разработки «облачных приложений»
Платформы данных	«Коммунальные» (multitenant) базы данных, метаданные	
Общие сервисы управления	Сборка и мониторинг Безопасность и аутентификация Управление производительностью приложений	
Среда выполнения	Вычислительное облако	
Виртуализованная инфраструктура	Системы хранения как сервисы Вычисления как сервисы	
Управление физической инфраструктурой	Дистанционные технологии для управления инфраструктурой	
Физическая инфраструктура	Центр обработки данных	

Общая характеристика PaaS

С точки зрения разработчика любая платформа для поддержки приложений, попадающая в категорию PaaS, представляет собой набор технологий и инструментов, необходимых для разработки, внедрения, интеграции и размещения *программ, предоставляемых как сервисы* (Software as a Service, SaaS). Будучи сетевым по сути, по своей форме этот тип платформ состоит практически из тех же самых компонентов, что и традиционные платформы, но в данном случае эти компоненты представлены в форме сетевых ресурсов.

Существует несколько заметно различающихся между собой подходов к созданию платформ PaaS. В наиболее общем виде их можно представить в рамках семиуровневой модели OSI. В основании модели лежат аппаратные и программные технологии, предоставляющие виртуализованные вычислительные ресурсы.

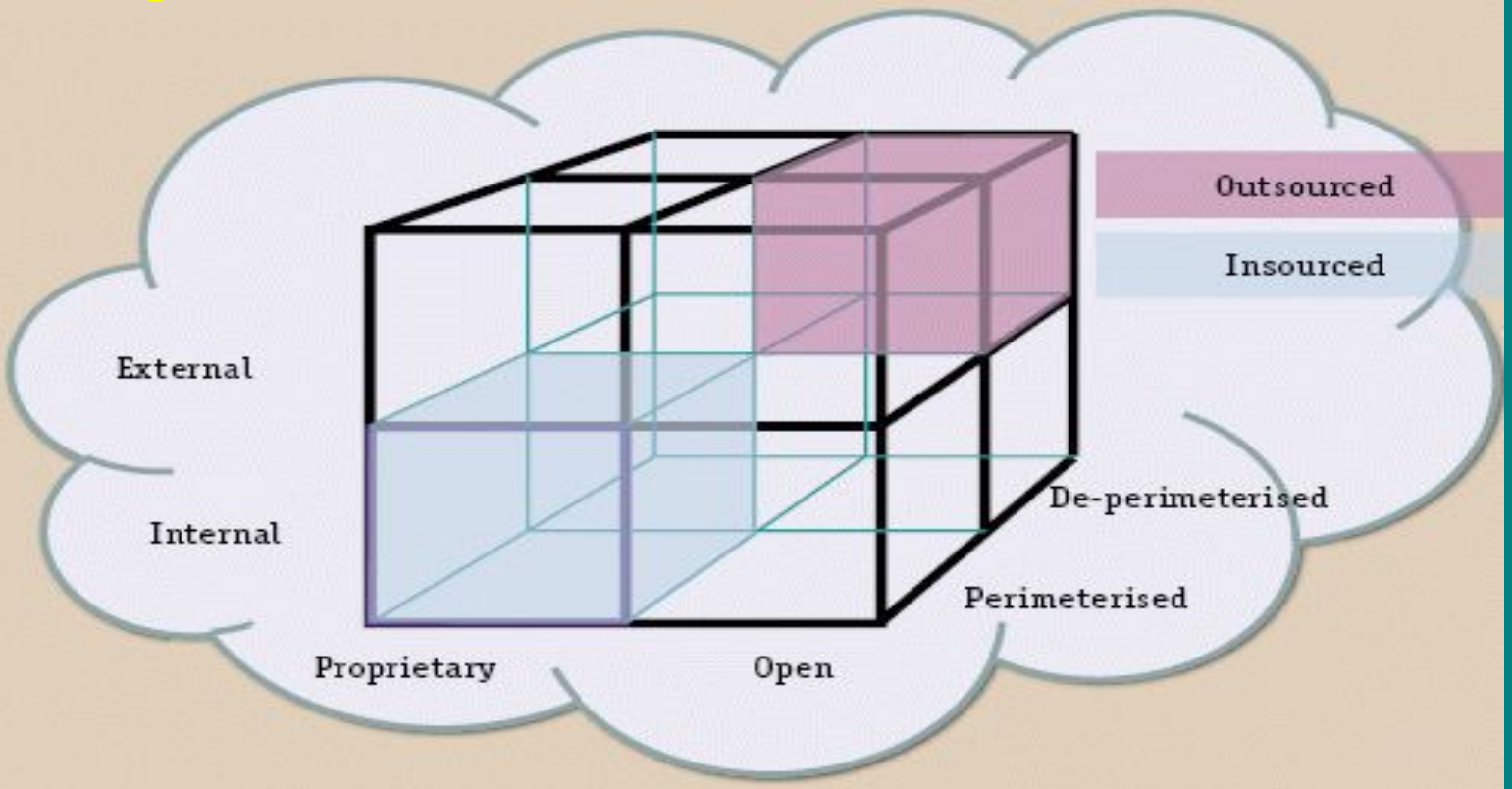
Далее с использованием парадигмы Cloud Computing, эти ресурсы собираются в «облака» и переводятся в форму сервисов. Еще выше в модели располагаются средства для «коммунального» доступа к данным и метаданным, а на вершине — интерфейсы API и интеграционные средства.

Архитектурные компоненты SaaS

«Облака» как совокупность сервисов

Облака как совокупность сервисов

Кубическая модель «облаков»



Измерение 1. Внутреннее или внешнее (Internal/External). Определяет место хранения данных, внутри организации, например на каких-то виртуальных дисках, или вне ее, например на Amazon SC3.

Измерение 2. Специальное или открытое (Proprietary/Open). Определяет владельцев технологии, например, облако может быть построено по открытым стандартам.

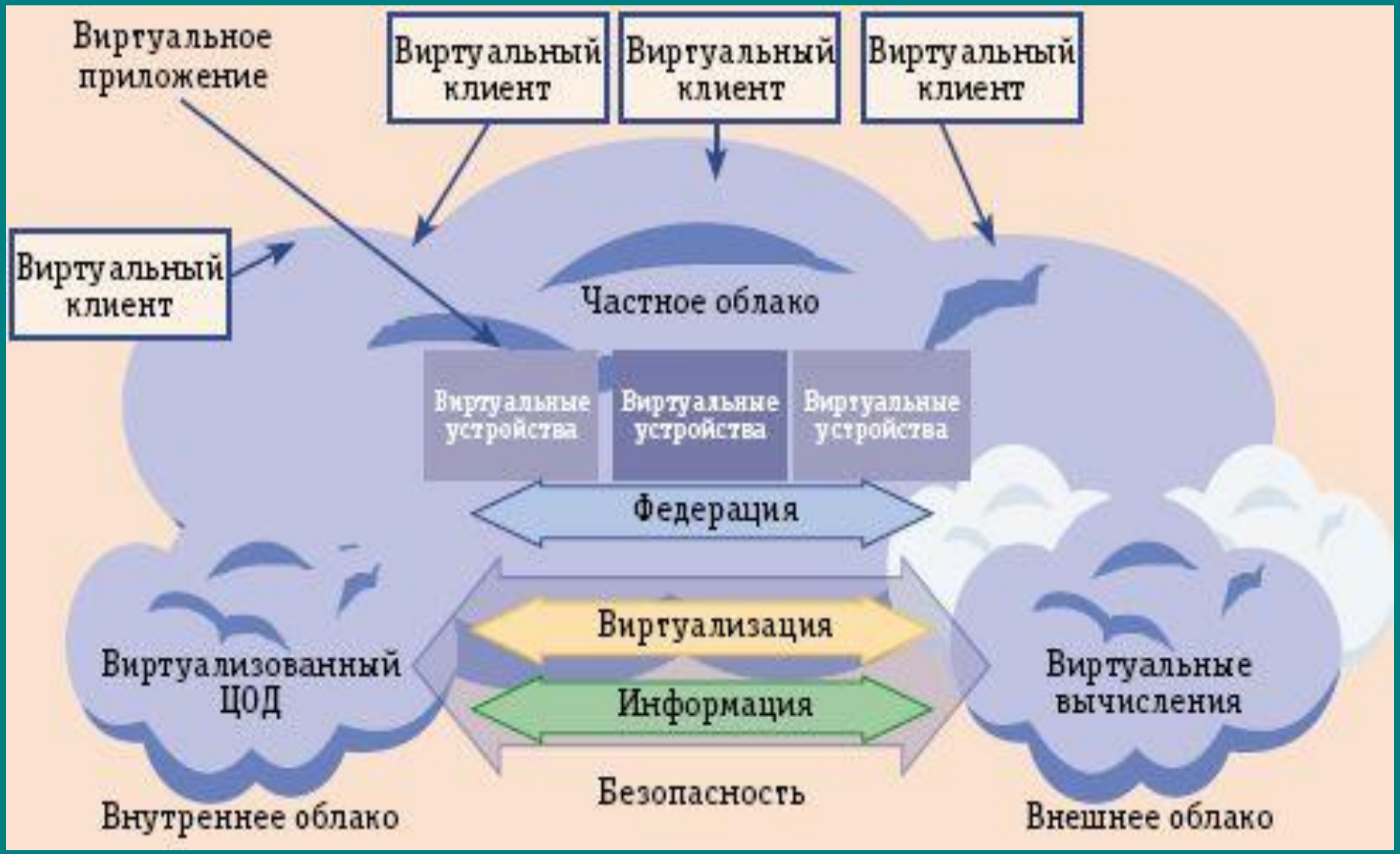
Измерение 3. Наличие периметра (Perimeterised/De-perimeterised). В случае существования периметра могут быть использованы традиционные средства обеспечения безопасности, в противном требуются информационно-центричные технологии защиты.

Измерение 4. Собственная поддержка или внешняя (Insourced/Outsourced). Определяет персонал, обслуживающий облако, собственный или сторонней организации.

Кубическая модель облаков

«ИДЕАЛЬНОЕ ВИРТУАЛИЗАЦИОННОЕ ОБЛАКО» (совокупность технологий IaaS)

Корпоративная ИТ-система на основе «облачной» модели



Преимущества корпоративной ИТ-системы на основе «облачной» модели

«Облака», в отличие от ЦОД, мэйнфреймов или мощных Unix-серверов (мидфреймов), являются динамической структурой. Все ресурсы «облака» могут использоваться с большей эффективностью, т.к. не требуется заранее для каждого приложения резервировать серверную нагрузку, область хранения и пропускную способность сети – они могут быть выделены «по требованию», а приложение может использовать ровно столько ИТ-ресурсов, сколько ему нужно, из общего пула. «Облака» позволяют совместить преимущества централизованной модели с достоинствами распределенной, обеспечивая тем самым динамическое управление ресурсами (Dynamic Resource Scheduling, DRS).

Результатом «облачной» конвергенции может стать КИС, построенная как частное «облако» (private cloud). Виртуальные устройства, в зависимости от необходимости, могут находиться во внешнем или во внутреннем облаке, а место выполнения приложения диктуется наличием ресурсов и требованиями безопасности.

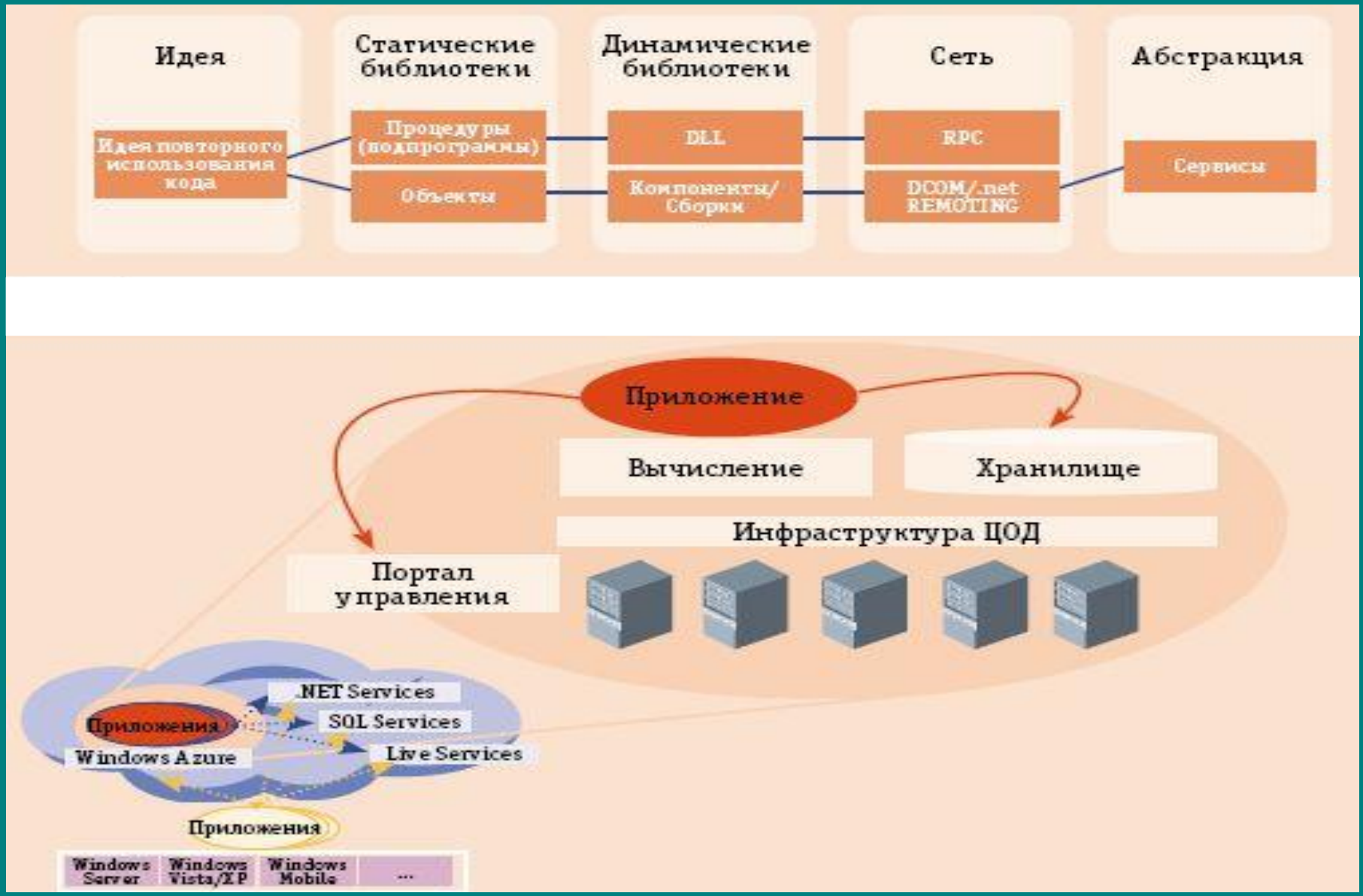
Внутреннее «облако» есть корпоративная система, построенная на базе динамического ЦОД, которая, кроме использования собственных ресурсов, может заимствовать их из внешнего «облака», создавая частное «облако». Внутреннее облако позволяет собрать в единый пул разнородные информационные ресурсы предприятия, чтобы потом распределять их «на ходу», по мере возникновения потребностей, что в конечном итоге приводит к более разумному использованию ресурсов и повышению эффективности.

Группы платформ для реализации «облаков»

Application Platform. В эту категорию попадают компании, первыми вышедшие на рынок SaaS, прежде всего, Webex, Netsuite, Salesforse.com. Они перекрывают всю нишу, предоставляя возможность использования только API или же завершенную среду для разработки и внедрения приложений.
Deployment Platform. Поставщики, занимающие эту нишу, предоставляют платформу для внедрения приложений, а все остальное отдают на откуп пользователям. Основные поставщики в этом сегменте Cloud Computing — Amazon и Google, а в сегменте, который называется Managed Hosting («управляемый хостинг») — Opsourse, IBM, Rackspace, Savis.
Development Platform. В дополнение к платформам для внедрения должны появляться и платформы для разработки приложений, занимающие верхний уровень в модели PaaS. Вендоры этой категории предоставляют интегрированные средства для разработки и возможности размещения своих приложений на платформе внедрения. Для создания и внедрения приложений могут использоваться классические технологии Java и .Net, а также технологии, специально ориентированные на разработку «облачных приложений». Группа компаний, предоставляющих технологии для разработки приложений такого рода, пока немногочисленна; ее составляют Bungee Labs, Comrange (Opsource), IT Factory и Coghead.

Рыночные ниши SaaS

«Облачная» архитектура в среде Windows

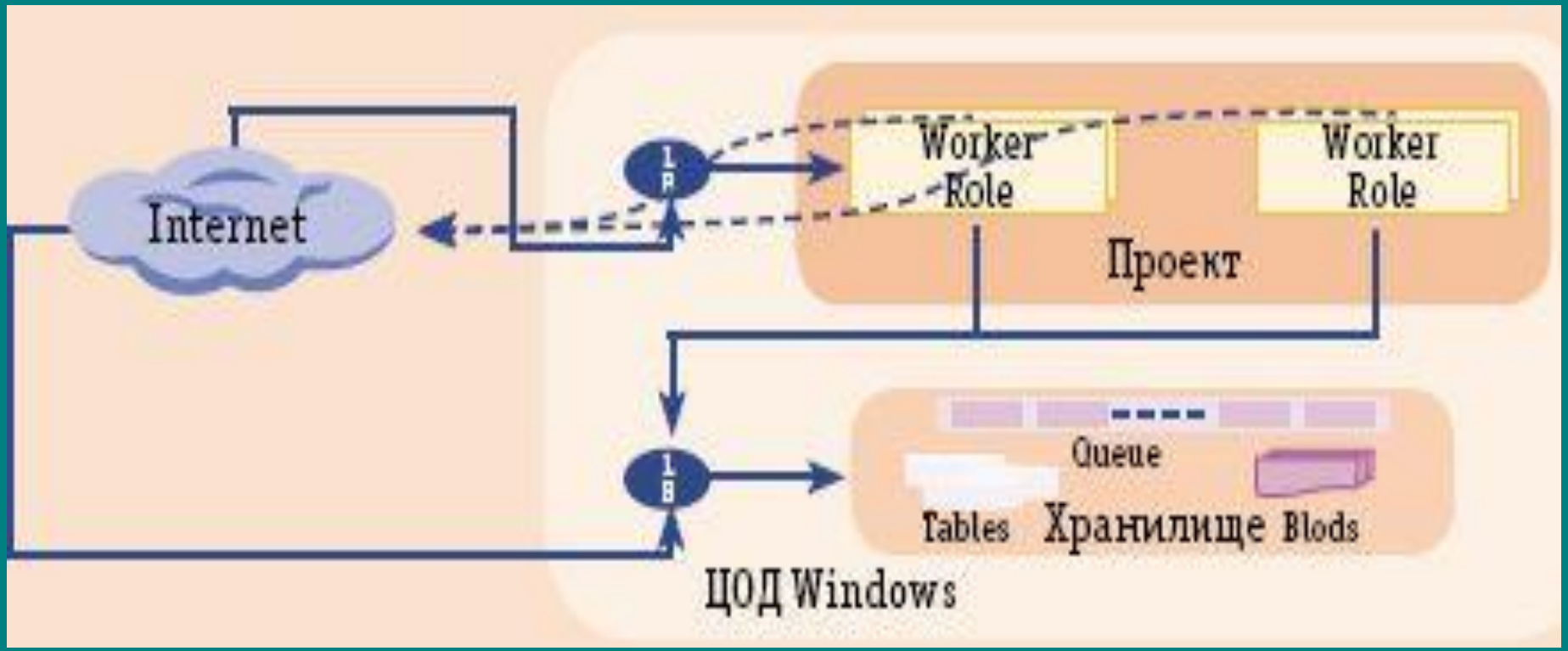


«Облачная» платформа Windows Azure

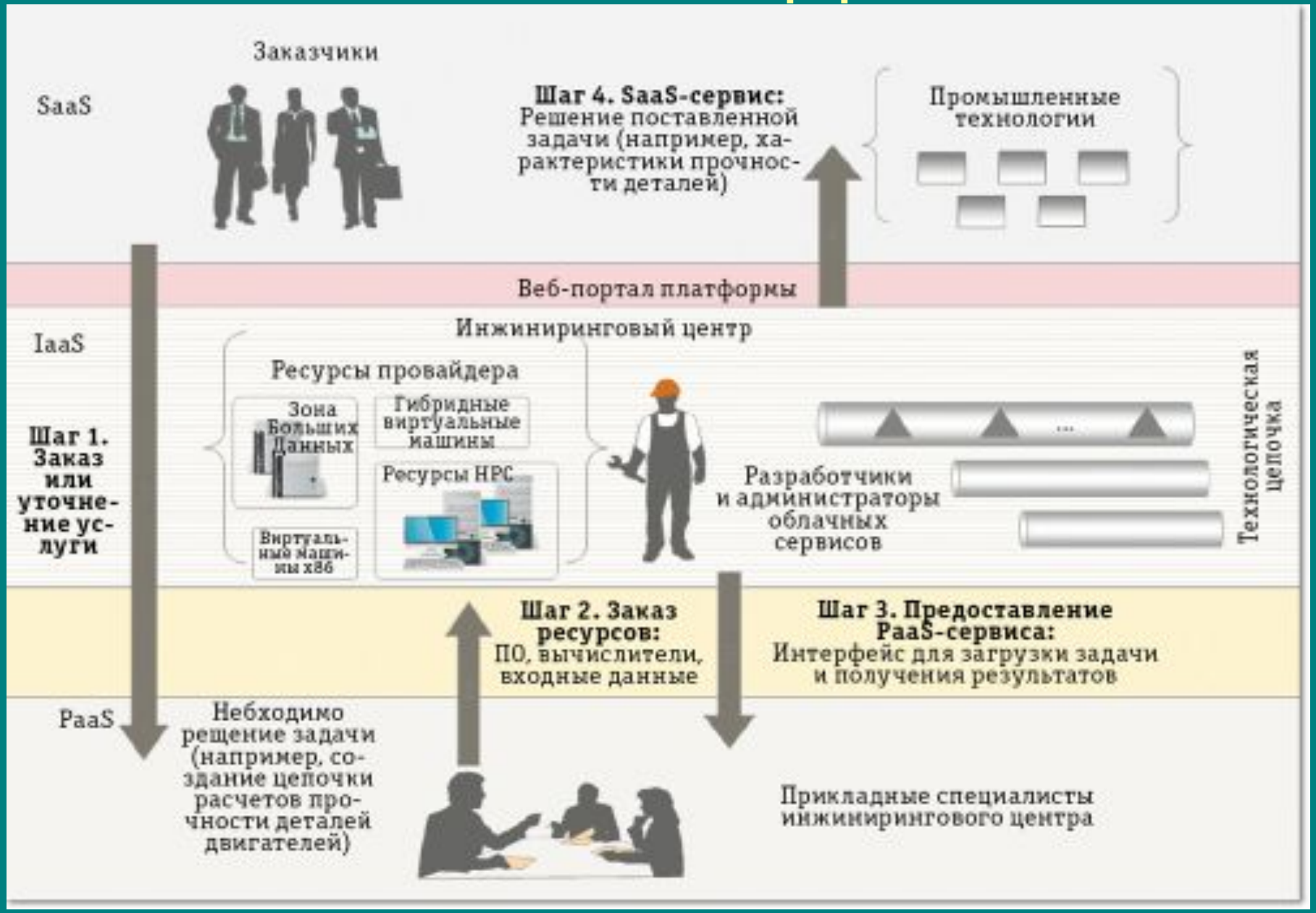
Платформа Windows Azure предоставляет: инструменты для разработки сервисов или сайтов; Центр обработки данных, исполняющий код разработанного решения; масштабируемое хранилище данных; локальную эмуляцию сервиса, позволяющую полноценно отлаживать приложения на локальной машине; портал, на котором можно разворачивать разработанные решения, управлять выделенными мощностями и на ходу менять конфигурацию сервисов. Масштабируемые сервисы часто имеют модульную структуру, состоящую из «фасада», хранилища данных и портала для управления мощностями сервиса в зависимости от нагрузки.

«Фасад» (front-end) обрабатывает Web-запросы, причем высоконагруженный сервис может потребовать несколько экземпляров «фасада», поэтому должна использоваться балансировка нагрузки. Отсюда следует, что необходимо отдельное от «фасада» хранилище данных, при этом «фасад» не должен сохранять состояние. В случае, когда требуется запуск сложного приложения, необходима возможность запуска кода в фоновом режиме (отдельные сервисы, процессы, демоны, потоки, нити). На сладе приведена схема типичного решения на Azure.

Типичная архитектура «облачного» сервиса на платформе Windows Azure



Функциональная модель использования «облачной» платформы



Проблемы «облачных» вычислений

«Вычисления в облаке» сталкиваются с теми же проблемами, что и другие современные информационные и сетевые технологии: безопасность, производительность, устойчивость к сбоям, интероперабельность, перенос данных и работа с унаследованными системами.

Провайдеры, пользователи и федеральные структуры согласны с тем, что сегодня важнейшей задачей является обеспечение информационной безопасности. Учитывая серьезность угроз, исходящих из разных источников, снизить такой риск можно только объединенными усилиями провайдеров сервисов «в облаке», сетевых провайдеров, корпоративных ИТ-отделов и пользователей всех категорий.

Измерение производительности «облачных» сервисов остается серьезной проблемой, главным образом из-за отсутствия соответствующих стандартов. Параметры оценки производительности для сервисов в облаке далеко не столь совершенны, как соответствующие показатели для телекоммуникационных сетей, где, например, такие метрики, как готовность, задержка и джиттер хорошо определены и понятны как пользователям, так и сетевым провайдерам. Для вычислений «в облаке» методы определения производительности и стандарты расчетов серьезно разнятся даже среди провайдеров, предлагающих аналогичные сервисы.

Наконец, пользователи и провайдеры в равной степени сталкиваются с дополнительными трудностями, связанными с переходом на новые решения и переносом данных с унаследованных систем «в облака», а также с интер-операбельностью «облачных» сервисов и унаследованными системами.

Уязвимости «облачной» инфраструктуры

Несанкционированное взаимодействие между виртуальными машинами и хостами. Инфраструктура «облака» должна исключать любое взаимодействие между отдельными виртуальными машинами (ВМ) или ВМ и физическими машинами, на которых они работают. Однако подобного рода взаимодействие возможно через общие области обмена данными (shared clipboard), оставляющие лазейку для распространения паразитных кодов.

«Побег» виртуальной машины. При недостаточной изоляции от хоста специально созданная злонамеренная ВМ может «совершить побег» (VM Escape) – «пройти» сквозь гипервизор и захватить управление хостом. В случаях, когда целью побега является захват других ВМ, это явление называют «перескакиванием» (VM Hopping).

Слежение со стороны хоста. По определению ВМ работает на хосте и под его управлением, и если не создать специальные барьеры, то хосту могут стать известны все секреты ВМ. Такая ситуация недопустима, она создает условия для тотальной слежки в «облаке».

Слежение со стороны виртуальной машины. Современные гипервизоры и процессоры со встроенной защитой памяти исключают взаимное наблюдение между ВМ, но изолированность может пострадать на уровне сетевого трафика, если машины используют «виртуальный коммутатор». В таком случае возможно хищение или переадресация передаваемых пакетов данных.

Уязвимости «облачной» инфраструктуры (окончание)

Атаки в «облаке». При недостаточной изоляции в «облаке» можно создать DoS-атаку, которая выведет из строя все «облако», или же реализовать локальную атаку одной ВМ на другую.

Внешние модификации. Целью атак такого рода может быть изменение кодов гипервизора и приложений, работающих на виртуальных машинах.

Перечисленные угрозы прежде не возникали, поэтому их невозможно устранить существующими технологиями или процессами, нет также единого решения по борьбе с ними, которая требует целенаправленных усилий производителей всех технологий, применяемых в «облаках», – аппаратного и программного обеспечения, сетевого оборудования и средств защиты.

Перспективные технологии повышения надежности идентификации в «облаках»

В «облачных» условиях не теряет своего значения направление, называемое *управлением идентификацией и доступом* (Identity Management, IdM), а также решения более широкого класса – обеспечения *безопасности на основе контроля за идентификацией* (Identity-Based Security, IBS).

Обеспечение сквозных (end-to-end) процедур управления идентификацией, аутентификация услуг, предлагаемых третьей стороной, и федеративная, охватывающая разные системы, проверка идентичности должны стать ключевыми компонентами «облачной безопасности». Решения категории IBS позволяют сохранить целостность и конфиденциальность данных, допуская при этом возможность для доступа к ним со стороны множества пользователей и приложений.

Этот класс технологий базируется на технологиях т.н. *сильной аутентификации* (strong authentication): многофакторная аутентификация; однократные пароли; аутентификация на основе рисков (risk-based authentication), учитывающая предшествующую историю, текущий контекст и другие факторы риска, сопровождающие тот или иной запрос к данным.

Аутентификация должна делиться на уровни, предусмотренные в соглашении об уровне обслуживания, а процедуры авторизации, то есть наделения правами, должны стать более гранулированными (granular authorization) – полномочия должны даваться только в ограниченных пределах, задаваемых выполняемыми ролями и функциями.

Должны также получить развитие такие технологии, как управление доступом на основе ролей (Role Based Access Control, RBAC), управление правами на информацию (Information Rights Management, IRM) и избирательное управление доступом (Discretionary Access Control, DAC).

Усиление защищенности данных

В традиционных ЦОД защита данных строится на основе физической защиты доступа к аппаратным или программным ресурсам, но в облаке происходит то, что называют депериметризацией, – все расставленные по периметру барьеры теряют смысл. Чтобы сохранить защищенность, соответствующие методы должны стать *информационно-центричными* (information-centric). Такого рода секретность предполагает перенос методов защиты непосредственно к данным.

В распределенных средах, обладающих качествами multi-tenancy (коммунальности, позволяющей нескольким пользователям независимо разделять один и тот же ресурс) и multi-instancy (индивидуальности, позволяющей каждому пользователю владеть частью «облака» для выполнения своих приложений), данные защищены с предельной возможностью.

Обеспечение защиты, как и аутентификации должно быть более гранулярным, нацеленным на более мелкие порции данных и меньшие по размерам группы пользователей. В нынешних условиях представления о гранулярности сформировались исходя из того, что данные находятся в пределах защищаемого периметра, но если данные «лежат» в некотором «облаке», то организации средств защиты может потребовать не только файл в целом, но и, например, отдельное поле или блок.

Работа «в облаке» может потребовать согласованной защищенности данных, различной для разных групп пользователей, например при обмене между «своими» и теми, кто вовне. Вместе с тем, распределение грифов секретности должно быть таковым, чтобы не снижать общей производительности, а для этого нужно ранжировать данные по степени их важности и величине рисков. IRM обычно распространяют только на управление идентификацией и доступом, но в условиях облаков права должны быть доведены до уровня данных.

Организация защищенных сегментов в среде «облачных» вычислений