Технологии виртуализации в России сегодня и завтра

АНДРЕЙ КОЛЕСОВ

ОБЗОРЫ

Виртуализация информационно-вычислительных ресурсов — одна из фундаментальных тенденций в сфере ИТ. Современный этап развития средств виртуализации связан в основном с их использованием применительно к архитектуре x86 и продолжается с конца 1990-х. Начавшись с виртуализации рабочих станций, процесс затем сместился в серверную сферу, но сегодня мы опять отмечаем повышение значимости клиентской составляющей, причем преимущественно для широкого класса мобильных устройств.

Именно виртуализация стала технологической основой облачных вычислений, которые, в свою очередь, послужили причиной структурной трансформации как ИТ-систем предприятий, так и ИТ-рынка в целом (речь идет не просто о технологических инновациях, а об изменении взаимоотношений между участниками рынка, в том числе о перераспределении функций между ИТ-поставщиками и ИТ-заказчиками). Можно уверенно говорить, что сегодня идеи и технологии виртуализации пронизывают всю проблематику ИТ.

Хотя в последние годы тематика ИТ-виртуализации в значительной мере ушла из поля публичного внимания, это вовсе не значит, что она утратила свою актуальность. Фактически в этой сфере уже состоялся переход от дискуссий и маркетингового продвижения технологий к их широкому практическому применению.

Вместе с тем технологии виртуализации и методы их применения не стоят на месте. Здесь появились новые продукты, новые инструменты, новые векторы развития. Изменилась и конкурентная ситуация на рынке. И ее понимание, верная оценка перспектив развития данного направления имеют важное значение для всех участников рынка с точки зрения выстраивания стратегии развития собственных ИТ. Особенно это важно для тех заказчиков, которые еще только присматриваются к возможностям, которые для них открывает виртуализация.

Обсудить текущее состояние и перспективы этого важного направления корпоративного ИТ-рынка мы предложили экспертам из числа ведущих отечественных игроков.

Общее состояние рынка

В общей оценке ситуации мнение экспертов едино: серверная виртуализация стала неотъемлемой частью ИТ-инфраструктуры предприятий независимо от их масштаба. Заказчиков не нужно убеждать в эффективности и надежности этих технологий, на рынке нет былого монополизма с точки зрения поставки решений, а у клиентов есть достаточно высокая компетенция, чтобы самостоятельно формулировать требования и выбрать нужного им вендора. Аналитики говорят о значительных абсолютных объемах рынка и очень высоких темпах его роста. По данным VMware, уровень виртуализации серверов в России вырос с 15% в 2011 г. до 30% в 2014-м. При этом все эти годы отмечается повышение темпов роста рынка средств виртуализации (вплоть до 80% в 2016-м). Директор департамента комплексного пресейла компании "Ай-Теко" Владимир Щетинин отмечает также рост коэффициента загрузки серверов за счет виртуализации, который превысил 50% и, по разным оценкам, составляет от 50 до 80%.

Ссылаясь на данные Forrester, директор департамента системной интеграции компании "Инлайн Групп" Андрей Кондратьев приводит такие данные: объем российского рынка виртуализации в 2015 г. может составить 500 млн. долл., что в десять раз превышает цифры начала 2014-го. Конечно, грянувший кризис скорректирует этот прогноз, но, по его мнению, существенного падения не будет. Изменился сам характер процесса внедрения виртуализации: если раньше это были самостоятельные проекты, то теперь виртуализация присутствует при решении практически любых ИТ-задач, в том числе при внедрении прикладных решений.

Актуального вопроса пятилетней давности: "Нужно ли использовать виртуализацию?" — уже нет, но есть более сложный: "Как эффективнее ее использовать?". Развивая этот тезис, ведущий эксперт Центра проектирования вычислительных комплексов компании "Инфосистемы Джет" Андрей Коновалов отмечает, что именно применение виртуализации стало необходимым этапом к началу использования частной облачной инфраструктуры и аренды вычислительных ресурсов у сервис-провайдеров.

Интересен и такой момент: признавая возможность повышения эффективности использования вычислительных ресурсов за счет виртуализации, часто говорили, что это достигается в ущерб надежности и безопасности. Сейчас, по мнению Андрея Кондратьева, виртуализация все чаще ассоциируется с повышением в том числе надежности, непрерывности, безопасности предоставляемых ИТ-услуг.

Однако директор по развитию продуктов компании "Код Безопасности" Константин Пичугов считает, что уже можно говорить об определенном уровне насыщения рынка средствами виртуализации, поэтому вендоры и их партнерские сети будут сейчас перефокусироваться на смежные сегменты: виртуализация рабочих мест, средства автоматизации управления виртуальными инфраструктурами и пр.

Технический директор VMware в России и СНГ Владимир Ткачев видит ключевые изменения на рынке виртуализации за последние пару лет в начале перехода от базовой виртуализации серверов к виртуализации других элементов ЦОД — сетей, систем хранения данных, рабочих столов. На это же обращает внимание руководитель направления инфраструктурных решений компании "КРОК" Иван Шумовский: "Средства виртуализации систем хранения и сетевых функций позволяют превратить обычный сервер, например, в узел хранения, при этом повысить степень автоматизации и использовать единообразное управление для всех типов узлов. Такой подход повышает модульность, степень устойчивости и управляемость соответствующих систем".

Но некоторые представления о возможностях виртуализации оказались или преувеличенными, или просто мифами. В частности, ведущий архитектор департамента аппаратных средств IBM в России и СНГ Владимир Сергиенко говорит о том, что не сбылись предсказания по поводу мгновенного экономического эффекта. Виртуализация требует серьезных инвестиций; экономия, причем значительная, достигается в долгосрочной перспективе. Но что важно, сегодня при принятии решения о переходе на виртуализацию главным доводом является все чаще не экономия на ИТ, а повышение скорости ввода в эксплуатацию новых прикладных решений, то есть получение выигрыша на уровне бизнеса компании.

VDI — всё еще впереди

На протяжении ряда лет аналитики прогнозировали активный рост направления инфраструктуры виртуальных десктопов (VDI). Но практика показала, что, несмотря на ряд позитивных примеров применения этой технологии, ее продвижение в жизнь оказалось намного более сложной задачей, нежели ожидалось. "Долгое время эта технология позиционировалась как решение всех проблем, возникающих при управлении физическими рабочими станциями, да к тому же более экономичное, — отмечает Андрей Коновалов. — В действительности же при сравнении "в лоб" VDI обходится дороже, к тому же требует пересмотра существующих бизнес-процессов в организации. Лишь недавно у заказчиков появилось понимание, как правильно позиционировать VDI и на какие сильные стороны технологии стоит опираться. VDI может очень пригодиться для реализации набирающей популярность концепции BYOD".

Основные причины того, что ожидания в отношении VDI не оправдались, Владимир Сергиенко видит в технических сложностях при внедрении технологии и отсутствии полноценных коробочных решений (несмотря на заявления ведущих производителей). Кроме того, как отмечает Константин Пичугов, "модель VDI уступает по стоимости терминальным подключениям с точки зрения затрат не только на хранение данных, но и на программные лицензии".

Вместе с тем наши эксперты сходятся во мнении, что данное направление развивается и имеет хорошие шансы в будущем. "На Западе технология VDI уже достаточно широко распространена, в России она также демонстрирует рост, — констатирует Владимир Ткачев. — Сейчас VDI особенно востребована в банковской, страховой и телекоммуникационной отраслях".

Уходят в прошлое и некоторые мешавшие внедрению VDI факторы. Так, по словам экспертов, недостатком VDI являются высокие требования к объемам хранимых данных, но сейчас появляются решения этой проблемы в виде использования новых экономичных СХД. Не столь остро стоит сегодня проблема пропускной способности каналов связи, а сами VDI-решения от разных вендоров стали более совершенными.

Тем не менее, считает Андрей Кондратьев, "в ближайшей перспективе прорыв в области VDI вряд ли возможен, но эта технология станет весьма востребованной, когда рабочие места массово переместятся в облака с доступом к ним с любого клиентского устройства".

Главным же сдерживающим фактором для распространения VDI может оказаться заметное падение значимости полноценного "толстого" клиента, переход к широкому использованию онлайновых облачных сервисов, превращение обычного браузера практически в исполняющую среду или даже некую платформу, как в случае с Chromebook. Говоря об этом, Иван Шумовский отмечает, что такая же тенденция наблюдается в корпоративных приложениях, хотя в настоящее время большинство корпоративного ПО существуют в виде "толстых" клиентов, нуждающихся в классической операционной системе для рабочих станций.

Разработка прикладного ПО и средств безопасности для виртуальных сред

Начальное продвижение виртуализации шло под лозунгом: "Просто перемести то, с чем ты работаешь сейчас, в виртуальную машину, и получай прибыль от снижения затрат на серверное оборудование". Но довольно быстро выяснилось, что снизить затраты на "железо" не так просто, а для эффективной работы в виртуальных средах нужно модернизировать прикладное и служебное ПО. Помимо этого оказалось, что традиционные средства защиты на уровне виртуальных машин забирали много ресурсов. Возникла необходимость в новых средствах обеспечения безопасности, ориентированных именно на виртуальные среды (в частности, основные механизмы защиты, например, антивирусное ПО, должны работать на уровне гипервизора, а не прикладной ОС).

К слову, изначально главными преимуществами виртуализации считались повышение эффективности загрузки серверов и, как следствие, возможность экономии аппаратных ресурсов. При этом вполне ожидаемыми были проблемы с надежностью функционирования приложений, использовавшихся на одном физическом сервере. Но практика показала, что все обстоит почти наоборот: затраты на "железо" часто даже возрастают (требования к его качеству повышаются), а вот отказоустойчивость и, что очень важно, масштабируемость решений возрастают благодаря возможности быстрой переносимости приложения (даже без его остановки) на другой узел серверного кластера, в том числе в автоматизированном режиме.

Говоря об этих достоинствах виртуализации, Андрей Коновалов отмечает, что разработчики средств ИБ предлагают решения, которые интегрируются со средствами виртуализации. Более того, сами средства защиты информации порой становятся виртуальными устройствами в составе платформы виртуализации.

Любые новшества наряду с достоинствами имеют, разумеется, и недостатки, причем порой совершенно неожиданного плана. В частности, Андрей Кондратьев напоминает, что виртуальная среда не только облегчает работу администраторам, но и дает новые возможности для злоумышленников — осуществить кражу виртуальной машины гораздо легче, чем физического сервера. В целом же он считает, что с большинством приложений (например, со стандартным офисным ПО) проблем при переносе в виртуальные среды не будет, трудности возникают обычно, если приложения используют напрямую ка-

Наши эксперты

АНДРЕЙ КОНДРАТЬЕВ, *директор департамента системной интеграции, "Инлайн Групп"*

АНДРЕЙ КОНОВАЛОВ, *ведущий эксперт Центра проектирования вычислительных комплексов, "Инфосистемы Джет"*

КОНСТАНТИН ПИЧУГОВ, *директор по развитию продуктов, "Код Безопасности"*

ВЛАДИМИР СЕРГИЕНКО, *ведущий архитектор департамента аппаратных средств, IBM в России и СНГ*

ВЛАДИМИР ТКАЧЕВ, *технический директор, VMware в России и СНГ*

ИВАН ШУМОВСКИЙ, *руководитель направления инфраструктурных решений, "Крок"*

ВЛАДИМИР ЩЕТИНИН, *директор департамента комплексного пресейла, "Ай-Теко"*

Защита информации от несанкционированного доступа согласно требованиям ФСТЭК России

ИВАН БОЙЦОВ

В феврале 2013 года ФСТЭК России выпустил два приказа (№ 17 и № 21), регулирующих защиту персональных данных в ИСПДн и защиту информации в государственных (и муниципальных) информационных системах (ГИС). В 2014 году список аналогичных документов дополнил приказ ФСТЭК России от 14.03.2014 № 31, в котором сформулированы требования к защите информации в автоматизированных системах управления технологическими процессами (АСУ ТП). В данных приказах приводится перечень базовых мер защиты, которые регулятор требует выполнять с помощью сертифицированных средств защиты информации (СЗИ).

Большинство указанных мер выполняются классическими средствами защиты информации от несанкционированного доступа (СЗИ от НСД). Далее мы рассмотрим, как реализовать набор мер, обязательных для применения в системах 1-го класса (уровня защищенности), с помощью механизмов защиты, реализованных в СЗИ от НСД Secret Net 7.

Идентификация и аутентификация субъектов доступа и объектов доступа

Secret Net заменяет стандартный механизм операционной системы по авторизации пользователей и позволяет проводить аутентификацию как по паролю, так и с использованием аппаратных средств усиленной аутентификации и стандартных сертификатов. Возможно и комбинирование способов аутентификации для достижения двухфакторной (многофакторной) аутентификации. Парольная информация защищена от перехвата как при локальном вводе (маскировка вводимых символов путем замены на "*"), так и при сетевой передаче.

Аутентификация устройств относится к сетевым мерам и реализуется средствами защиты других классов (например, с помощью АПКШ "Континент" или МЭ TrustAccess).

Управление идентификаторами и средствами аутентификации реализовано в Secret Net в программе управления пользователями и в расширениях стандартных оснасток управления Windows, настройки устанавливаются с помощью механизма политик. Гибкие настройки политик аутентификации позволяют настроить режимы аутентификации, задать условия блокировки учетных записей и сеансов пользователей, требования к стойкости парольной информации и другие параметры.

Управление доступом субъектов доступа к объектам доступа

Управление учетными записями в Secret Net осуществляется так же, как и управление аутентификационными данными — в программе управления и расширении оснасток Windows. Пользователи и администраторы в системе разделены с помощью ролей и полномочий.

В Secret Net реализованы собственные механизмы мандатного и дискреционного управления доступа к файлам, директориям и устройствам. Правила разграничения доступа к объектам файловой системы настраиваются в расширениях стандартных механизмов управления Windows, а для настройки доступа к устройствам используется механизм политик.

Доверенная загрузка может выполняться средствами модуля защиты диска, входящего в состав Secret Net, или с помощью аппаратного решения ПАК "Соболь", который интегрируется в Secret Net по управлению и аудиту. Интеграция с ПАК "Соболь" в централизованном режиме управления Secret Net позволяет контролировать доверенную загрузку централизованно, из программы управления Secret Net.

Управление сетевыми потоками, контроль удаленного и беспроводного доступа осуществляются средствами сетевой защиты и выходят за рамки функциональности СЗИ от НСД, но Secret Net способен разрешать или запрещать работу сетевых интерфейсов в зависимости от их типа и, в некоторых случаях, реализовывать данные меры.

Ограничение программной среды

Базовые меры по ограничению программной среды реализуются с помощью механизма замкнутой программной среды Secret Net. Данный механизм позволяет настроить список разрешенных к запуску приложений и модулей, все остальные исполняемые файлы и их компоненты пользователи запустить не смогут. Дополнительно возможна настройка контроля целостности исполняемых файлов, гарантирующих неизменность разрешенных к запуску программ. Если исполняемый файл обладает доверенной электронной цифровой подписью издателя, может быть настроено автоматическое обновление контрольной суммы при установке обновлений, что позволяет проводить плановую установку обновлений программного обеспечения без необходимости перенастройки ЗПС и ручного перерасчета контрольных сумм.

Защита машинных носителей персональных данных

Учет и управление доступом к машинным носителям выполняется в механизмах контроля устройств СЗИ Secret Net. Администратор с помощью политик безопасности может управлять устройствами как на уровне классов и моделей, так и на уровне отдельных устройств. Secret Net контролирует устройства USB, PCMCIA, IEEE1394, внешние диски, SD-карты, сетевые интерфейсы и другие типы устройств. В контроле устройств поддерживается полномочное (мандатное) управление доступом, позволяющее разграничить доступ к оборудованию в зависимости от текущего уровня доступа пользователя.

В состав Secret Net входит модуль гарантированного уничтожения удаляемой информации. При обычной работе данные удаляемых файлов остаются на жестких дисках. Сектора, в которых они хранились, лишь помечаются как свободные области и могут быть перезаписаны позднее, при новых операциях записи на диск. При включении модуля Secret Net удаляемые файлы автоматически затираются с помощью случайной информации и не могут быть в дальнейшем восстановлены. Для обеспечения дополнительных гарантий поддерживается несколько циклов затирания.

Регистрация событий безопасности

Secret Net генерирует события безопасности для всех аспектов защиты, все данные аудита сохраняются на компьютере и доступны для просмотра в локальных журналах. При централизованном режиме работы локальные журналы со всех компьютеров собираются в общую базу данных и доступны к изучению в общей программе управления.

Для регистрации событий используется системный таймер, внутренние системные часы информационной системы. Все журналы защищены от несанкционированного доступа и изменений.

Поддерживаются механизмы квитирования событий НСД в централизованном режиме, для каждого события можно отметить их обработку. При просмотре событий поддерживаются различные способы фильтрации данных.

Обеспечение целостности информационной системы и персональных данных

Контроль целостности в Secret Net выполняется для настраиваемых администратором списков файлов, директорий и данных реестра Windows. Поддерживаются различные действия при обнаружении изменения в контрольной сумме — от выдачи уведомления до блокировки рабочей станции. Можно контролировать целостность как системных файлов операционной системы, так и любых других файлов — приложений, данных, документов и так далее.

Восстановление Secret Net в случае повреждения служебных файлов может быть выполнено через программу установки. Поддерживается экспорт и импорт конфигурации для возможности резервного копирования настроек СЗИ.

Заключение

СЗИ Secret Net позволяет реализовать широкий набор обязательных базовых мер по защите информации в ИСПДн, ГИС и АСУ ТП. Однако классическое СЗИ от НСД не реализует меры, относящиеся к антивирусной защите, обнаружению вторжений, сетевой защите, защите технических средств, резервному копированию и защите виртуализации. Для выполнения этих мер существуют другие классы средств и организационные мероприятия, которые в совокупности позволяют обеспечить высокий уровень защиты в соответствии с требованиями регуляторов.

Автор — менеджер по продукту компании "Код Безопасности".

кие-то аппаратные средства (графические ускорители, ключи защиты и т. д.). Сейчас многие разработчики прикладного ПО выпускают новые версии софта с поддержкой виртуализационных сред, но в любом случае при переносе в виртуальную машину ПО, отлично работавшего в физической среде, нужно проводить дополнительное его тестирование на предмет адекватной работы.

Продолжая эту тему, Константин Пичугов напоминает, что соль виртуализации заключается в полном разрыве связи между аппаратным обеспечением и прикладным ПО (чего не было в традиционных ОС). Если приложение не имеет никакой привязки к конкретному "железу" (к тем же физическим токенам), то влияние виртуализации на его функционирование обычно минимально.

Что же касается информационной безопасности, то в виртуальной среде есть свои особенности, в том числе в виде новых угроз. В качестве примера он приводит возможность несанкционированного копирования данных, обрабатываемых в виртуальной машине (включая данные в ОЗУ). Эту угрозу нельзя нейтрализовать только с помощью ПО, размещенного в виртуальной машине, — нужно контролировать всю среду. Сейчас такие решения есть. Есть и методические рекомендации и требования по защите виртуальных сред, сформулированные международными организациями и нашей ФСТЭК.

Нужно исходить из того, что виртуализация стала технологическим стандартом, а потому наличие проблемы в данной сфере — это не повод для отказа от виртуализации как таковой (хотя применять ее нужно не всегда).

Чтобы оставаться конкурентоспособными, абсолютно все компании-разработчики должны принимать во внимание этот факт и адаптироваться к новой реальности, что они, собственно, и делают. Сказав об этом, Владимир Сергиенко отмечает, что основные проблемы с безопасностью лежат не в технической, а в организационной плоскости. В частности, много споров идет по поводу ответственности за управление виртуализированной средой. Кроме того, сохраняется такое явление, как беспорядочный рост числа виртуальных машин (VM sprawl). В совокупности с несовершенством процессов разграничения ответственности за виртуальную среду это создает много проблем для специалистов по безопасности. Но, по мнению эксперта, эти проблемы решаются путем применения эффективных процессов и инструментов управления виртуальной средой. А лучшим вариантом с точки зрения управляемости и, как следствие, безопасности может стать переход на использование облачной модели IaaS.

Исторически виртуализация x86-систем появилась как средство упрощения процессов разработки и тестирования ПО, напоминает Владимир Ткачев. Эта функция остается очень важной, если мы говорим о достоинствах виртуальных сред. "Одна из основных тенденций, которая оказывает значительное влияние на всю ИТ-отрасль, — рост требований со стороны бизнеса к ИТ, — подчеркивает он. — Виртуализация помогает справиться с этим, и это может быть даже важнее, чем экономия на эксплуатации ИТ". Сокращение времени на развертывание сервиса происходит на всех этапах — при разработке приложений, их тестировании и переносе в продуктивную среду. Последний процесс обычно связан со значительными сложностями, так как требования к производительности, надежности и безопасности в ней намного выше, чем в тестовых средах. Поэтому обычно уходит немало времени на тонкую настройку приложений, проверку их защищенности и соответствия нормативным требованиям, что требует привлечения большого количества специалистов для рутинных и однотипных операций.

"Виртуализация позволяет без привлечения дополнительных ресурсов (специалистов) быстро создать среду разработки и тестирования ПО и легко ею управлять, — подчеркивает и Иван Шумовский. — Практика подтверждает, что цикл тестирования и перевода приложений в промышленную эксплуатацию заметно ускоряется".

Говоря о новых угрозах, привносимых виртуализацией, он обращает внимание на ряд аспектов: "Настройка вычислительной среды производится проще. Но и несанкционированным образом это сделать становится проще, что вынуждает усиливать механизмы контроля за процессом настройки. Технологии, ответственные непосредственно за виртуализацию, развиваются достаточно быстро, но, к сожалению, средства защиты несколько отстают. Возможно, дело в отсутствии массового рынка, а может быть, в отсутствии громких инцидентов".

К главным проблемам виртуализации в плане безопасности он относит, во-первых, потенциальную возможность компрометации всей виртуальной среды при компрометации гипервизора, а во-вторых, весьма ограниченный выбор механизмов защиты виртуальной среды, вплоть до того, что для некоторых гипервизоров средств защиты практически не существует. Кроме того, есть потенциальная возможность компрометации гипервизора посредством компрометации виртуальной машины, работающей на данном гипервизоре. Поэтому при использовании виртуализации нужно тщательно анализировать возможные угрозы и учитывать их при реализации соответствующих мер защиты.

Конкурентная ситуация на рынке средств виртуализации

Тема эта имеет два аспекта — конкуренция среди поставщиков продуктов (вендоров) и среди поставщиков услуг по внедрению (системных интеграторов). Но про оба направления можно сказать вполне определенно: идет жесткое соревнование, у заказчиков есть выбор.

Прежнее фактически монопольное положение на рынке компании VMware ушло в прошлое. Компания продолжает быть признанным лидером, но уже не единоличным. Многие годы интрига заключалась в погоне Microsoft за лидером, но, по мнению наблюдателей, с выходом Windows Server 2012 R2 Редмонд в целом догнал VMware в технологическом плане, хотя и не достиг того же положения на рынке. Помимо этих двух гигантов на рынке серверной виртуализации присутствуют еще игроки, делающие ставку на технологии Open Source. Надо также отметить, что в нынешнем году Gartner впервые включила в свой магический квадрант по серверной виртуализации китайскую компанию Huawei.

"На рынке производителей виртуализационных решений пока не так много игроков, и у каждого есть своя ниша, — считает Иван Шумовский. — Поэтому конкуренция пока не столь сильна, но в связи с ухудшающейся экономической ситуацией она будет усиливаться. Среди классических гипервизоров на российском рынке лидирует VMware, но в последнее время растет число внедрений гипервизора Microsoft, поскольку большинство компаний используют ее серверы, операционные системы и приложения и получают возможность сэкономить на лицензиях. Растет и число внедрений на базе гипервизоров, поддерживаемых Citrix и Red Hat. Кроме того, сейчас практически у всех производителей классических гипервизоров есть средства для автоматизации и конвертации образов виртуальных машин, облегчающих переход с одних решений на продукты конкурентов".

Его дополняет Владимир Щетинин: "Технологически рынок развивается

ПРОДОЛЖЕНИЕ НА С. 15 ▸

Технологии...

ПРОДОЛЖЕНИЕ СО С. 13

во многом благодаря усилиям традиционных лидеров — VMware и Microsoft, постоянно расширяющих функциональность существующих решений и предлагающих новые продукты. Не отстает и "группа преследования", в которой я бы выделил Red Hat. Не оправдался, на мой взгляд, прогноз о выравнивании присутствия на рынке решений VMware и Microsoft. Да, продукты последней стали более популярны, но наиболее крупные внедрения, по крайней мере в сегменте корпораций, по-прежнему осуществляются на базе продуктов пионера в сфере виртуализации". Он считает, что конкуренция среди интеграторов высока в традиционном сегменте серверной виртуализации. Но в области виртуализации рабочих мест, СХД или приложений конкуренции значительно меньше. Не высока конкуренция в сегментах мониторинга, управления и автоматизации виртуальных сред. И совсем новая область, в которой, пожалуй, мало кто имеет экспертизу в России, — это виртуализация сетей.

Что касается услуг по внедрению средств виртуализации, то их уже давно предлагают практически все интеграторы. Андрей Коновалов считает, что сегодня многие ИТ-компании обладают высоким уровнем компетенций. Он дает простые рекомендации: выбирайте проверенных поставщиков, которые имеют опыт и компетенции в реализации подобных кейсов, а также готовых выполнять пилотные проекты и поддерживать уже внедренные решения. Если поставщик планирует долгое и взаимовыгодное сотрудничество, он не станет завышать цену и сделает конкурентоспособное предложение.

Владимир Сергиенко рекомендует выбирать интеграторов, которые пропагандируют комплексный подход, имеют необходимые опыт и навыки внедрения подобных решений на разных платформах виртуализации, имеют взаимоотношения с несколькими вендорами. Это важно с точки зрения правильного выбора поставщика виртуализационного решения. Каждое решение имеет свою специфику. Поэтому интегратор должен иметь возможность предложить то, что лучше всего подходит под конкретную задачу заказчика.

"Работайте с теми компаниями, с которыми у вас уже сложились партнерские взаимоотношения и которые уже подтвердили свой профессионализм и экспертизу, — такой совет заказчикам дает Владимир Ткачев. — Если таких партнеров еще нет, то, возможно, в первую очередь следует обратить внимание на опыт компании в реализации схожих проектов и её возможности по построению комплексного и законченного решения".

"Идеальный системный интегратор — это компания с большим опытом соответствующих внедрений и профессиональной командой сертифицированных специалистов, — делится своим опытом Иван Шумовский. — У большинства производителей средств виртуализации помимо общих сертификаций появляется все больше узкопродуктовых специализаций, которые можно однозначно отнести к решению каких-то узких задач, таких, например, как построение резервного ЦОДа. Поэтому если перед заказчиком стоит задача реализации проекта именно в узкоспециализированной области и на примете есть компания с соответствующими специалистами, сертификациями и опытом непосредственно в данной конкретной области, логично сделать выбор в ее пользу".

При выборе решения нужно анализировать задачу в комплексе, принимая во внимание все факторы: зрелость технологии, наличие специалистов, имеющееся оборудование и лицензии, планы по развитию и т. д., уверен Владимир Щетинин. При прочих равных условиях, конечно, лучше обращаться к интегратору, который имеет экспертизу по нескольким вендорам, работающим в сфере виртуализации: VMware, Microsoft, Citrix, Red Hat. Полезной окажется также экспертиза по оборудованию, которое планируется использовать в проекте по виртуализации.

Актуальные направления развития виртуализации

Из ответов экспертов можно выделить два основных направления развития виртуализации. Первое — это углубление виртуализации ИТ-инфраструктуры с переходом ко "всеобщей виртуализации" (серверов, систем хранения, сетей, клиентского оборудования). Второе — переход к более широкому использованию облачных услуг и общее смещение рынка от модели продажи ПО и оборудования к сервисным отношениям между ИТ-поставщиками и ИТ-заказчиками.

Владимир Щетинин считает, что в ближайшее время можно ожидать прорыва в сфере виртуализации сетей: "В последние два года ряд ведущих вендоров, включая Cisco и HP, продвигают решения для этого сегмента, пока, правда, без особых успехов. Тем не менее есть ощущение, что набирается критическая масса наработок и в течение двух-трех лет интерес к SDN заметно вырастет, начнутся внедрения. Крайне интересной представляется предложенная VMware идея создания привычных для телеком-специалистов сущностей (коммутаторов, маршрутизаторов, файерволов) в виде виртуальных машин, которые берут на себя все интеллектуальные функции, оставляя оборудованию роль набора портов для подключения. Думаю, что операторы и корпоративные клиенты со временем оценят те преимущества в гибкости работы с инфраструктурой, которую дает виртуализация сети".

С ним солидарен Андрей Кондратьев: "В сетевой области произойдет то же, что с серверами. Сейчас виртуальные машины могут работать на аппаратных серверах различных производителей. Точно так же сеть станет объединением программных коммутаторов и аппаратных сетевых компонентов различных производителей, на котором будут строиться виртуальные сети (не путать с VLAN) и в них же будут создаваться виртуальные системы безопасности: межсетевые экраны, системы обнаружения вторжений и т. д." Что же касается вычислительной среды, то, по его мнению, в ней продолжится переход от уникальных сложных серверных систем к работе в виртуальных средах на простых вычислителях. Эта тенденция поддерживается и разработчиками ПО. Также сохранится тенденция развития средств автоматизации управления виртуальными средами для того, чтобы в дальнейшей перспективе сделать потребителями систем виртуализации самих пользователей, а не администраторов.

Владимир Сергиенко считает, что будет расти значение решений на базе открытого кода. Но при этом он упоминает и о стоящих на этом пути проблемах. "Главным фактором, мешающим более широкому распространению облачных технологий и соответственно технологий виртуализации, по-прежнему остается недоверие к поставщикам, — констатирует он. — А вызвано оно в том числе и отсутствием необходимой законодательной базы. Поэтому сейчас, на мой взгляд, основные усилия должны быть сконцентрированы именно в этой области".

Акценты начинают смещаться от задач по консолидации второстепенных нагрузок в сторону повышения доступности и непрерывности работы бизнес-критичных приложений. Всё больше компаний предпочитают размещать наиболее критичные для бизнеса нагрузки в виртуальных машинах на стандартных серверах архитектуры x86, что позволяет обеспечить высокую производительность приложений и значительное повышение их доступности. Таковы наблюдения Владимира Ткачева, который считает, что всё более горячими темами становятся вопросы виртуализации хранилищ, сетей и рабочих мест конечных пользователей.

По мнению Ивана Шумовского, сейчас в кризисный период компании с особой тщательностью будут пытаться снизить издержки, а виртуализация — как раз одна из тех технологий, которая помогает это сделать. Но при этом он считает, что нужно дополнительно прорабатывать вопрос ИБ, хотя на нормативно-правовом уровне он уже активно решается. Государство также идет по пути построения всей цепочки ИТ-услуг на сервисных принципах, что просто невозможно без виртуализации и облаков. Однако развитие сервисных отношений между поставщиком и заказчиком потребует развития средств автоматизации управления всеми виртуализированными компонентами для более точного биллинга и мониторинга сервисов, предоставляемых виртуализированными элементами.

Заказчики будут переходить от виртуализации своей внутренней ИТ-инфраструктуры к использованию публичных облачных сред, уверен Андрей Коновалов. На Западе этот процесс уже идет, у нас он пока в самой начальной фазе. Г-н Коновалов согласен с тем, что главными факторами, сдерживающими развитие рынка в нашей стране, являются российское законодательство, предъявляющее жесткие требования к обработке и хранению персональной информации, а также боязнь компаний отдавать свои данные на сторону.