

Стратегические ЦОД-технологии

ВАЛЕРИЙ ВАСИЛЬЕВ

За последнее десятилетие роль ЦОДов как основы ИКТ-инфраструктуры современных предприятий и организаций существенно возросла. Вместе с тем известно, что ЦОДы стоят дорого. Именно поэтому в настоящее время разрабатываются и внедряются технологии, позволяющие снизить капитальные и операционные расходы, связанные с построением, развитием и эксплуатацией ЦОДов, а также расширить их функциональные возможности в соответствии с растущими требованиями к их надежности, гибкости и производительности предоставляемых сервисов.

Какие новейшие технологии имеют стратегически важное значение для построения ЦОДов сегодня и в ближайшем будущем, каковы их эффективность и уровень готовности к внедрению, с какими проблемами сталкиваются или могут столкнуться заказчики при внедрении этих технологий — эти и другие смежные вопросы мы постарались осветить в нашем тематическом обзоре.

Современные драйверы ЦОД-технологий

Мощным драйвером развития рынка ЦОДов в нашей стране, как отметил Владимир Кондаков, выступает государство, реализующее свои электронные программы и национальные проекты, которые уже являются стабильным источником спроса на ЦОД-услуги, и в дальнейшем этот спрос со стороны госсектора будет только расти.

Сюда же следует отнести масштабные интернет-проекты — поисковые системы, информационные и торговые интернет-порталы, социальные сети, которые генерируют большой объем трафика и имеют много пользователей, что побуждает их владельцев размещать свои ресурсы ближе к конечному потребителю с целью удешевления стоимости передачи данных. Это, по мнению г-на Кондакова, стимулирует строительство ЦОДов в регионах.

Как отметил Николай Гришин, клиенты хотят получать ИКТ-услуги более высокого качества по возможности за меньшие деньги. Для владельцев и операторов ЦОДов есть два (взаимосвязанных) пути выполнения этих требований: повышение эффективности и снижение затрат при использовании вычислительных ресурсов, хранении данных, администрировании.

Выполнять эти требования, как заметил Николай Кузнецов, приходится в условиях ухудшения экономической ситуации и финансового положения, что ведет к ужесточению требований к ключевым экономическим показателям ЦОДов — совокупной стоимости владения (ТСО) и возврату инвестиций (ROI), а это, в свою очередь, повышает интерес к услугам коммерческих ЦОДов.

Рост интереса к коммерческим ЦОДам, полагает Денис Сивцов, обостряет конкуренцию среди их владельцев, стимулирует их оптимизировать расходы и повышать эффективность своего бизнеса — в первую очередь снижать операционные затраты, которые г-н Сивцов напрямую увязывает с энергоэффективностью ЦОДов.

В повышении эффективности и снижении затрат (в том числе и на энергоресурсы) технологии играют первые роли. Например, по оценкам экспертов компании Gartner, повышение допустимой температуры рабочей среды в ЦОДе на 5°C позволяет сэкономить до 27% затрат на его охлаждение.

Более высокая энергоэффективность современных ЦОДов вынуждает владельцев ЦОДов, сланных в эксплуатацию пять-семь лет назад (в нашей стране это в основном корпоративные ЦОДы), ре-

шать задачу повышения энергоэффективности наложенными средствами (организационными и техническими) или переносить расходы на электроэнергию (и другие ресурсы) на клиентов, тем самым проигрывая в конкуренции.

Однако риски, связанные с невыполнением регулятивных требований (compliance) к снижению загрязнения окружающей среды, подчеркнул Алексей Шалагинов, перенести на клиентов невозможно, поэтому владельцы ЦОДов вынуждены использовать “зеленые” технологии.

Технологический вызов в сфере строительства ЦОДов представляют, по мнению г-на Гришина, задачи хранения данных и резервного копирования в связи с экспоненциальным ростом объемов обрабатываемых данных (в первую очередь неструктурированных, так называемых больших данных) и, как следствие, повышением требований к производительности и надёжности систем хранения данных (СХД).

Важным технологическим трендом в строительстве ЦОДов Сергей Андронов назвал возможность (благодаря виртуализации) формировать единые вычислительные пулы, объединяющие множество виртуальных машин (VM), способных без прерывания работы и незаметно для пользователей мигрировать между физическими серверами. Значимой, по его мнению, стала также вытекающая из этого тренда концепция логической консолидации ЦОДов, позволяющая не разделять их на основные и резервные.

Особенно высокие показатели такая консолидация обещает для территориально разнесенных ЦОДов. После того как в нашей стране будут преодолены ограничения, накладываемые каналами связи (что, по его наблюдениям, не требует много времени), применение виртуализации позволит создавать единые территориально распределенные ЦОДы. Максимально эффективное использование их ресурсов достигается за счет перемещения VM между образующими их физическими площадками. Так, если такие площадки расположены в разных часовых поясах, можно использовать разницу суточных тарифов на электроэнергию.

Мировым трендом стало укрупнение ЦОДов. В России (где в Москве, по оценкам некоторых экспертов, сосредоточено более 80% всех ЦОДов страны) это станет дополнительным стимулом строительства ЦОДов в других регионах, поскольку в Москве трудно построить мощный ЦОД из-за действующих ограничений по подключению к энергосетям и дороговизны землеотвода.

Фокус инноваций в строительстве ЦОДов

Руслан Чиняков считает, что инновации относительно равномерно распределяются по всем компонентам ЦОДов и реализуются в основном через ПО, которое становится основой любого компонента.

Инновации в компоненты инженерной инфраструктуры г-н Чиняков разделяет на две группы: компоновочные и технические. К первым он причисляет disaggregation серверов (формирование общего пула ресурсов) — диски, процессоры, оперативная память физически разносятся по отдельным зонам ЦОДа, что позволяет эффективно охлаждать и распределять электропитание для каждой зоны.

Из технических новинок г-н Чиняков особое внимание обращает на новые способы жидкостного охлаждения серверов (погружное, иммерсионное и адиабатическое) и фрикулинг. Рыночным сегментом, на котором сфокусированы эти инновации, как считает (в отличие от некоторых других наших экспертов) г-н Чиняков, являются корпоративные ЦОДы. Владельцы коммерческих ЦОДов,

по его мнению, озабочены удешевлением стоимости стартовых затрат, особенно на инженерные системы. Он отметил, что это действительно сокращает ROI, однако может отрицательно сказаться на стоимости ЦОДа на всем его жизненном цикле (ТСО).

Иное видение ситуации у Дениса Сивцова. Он считает, что при строительстве новых ЦОДов основное внимание их владельцы уделяют инженерной инфраструктуре, по его мнению, именно она определяет основные характеристики ЦОДа, а также последующие операционные затраты. Инновации в области ИКТ-инфраструктуры ЦОДов (вычислительной, сетевой, СХД) в данный момент он определяет как эволюционные: постепенное улучшение существующих технологий, нацеленное на рост производительности, уменьшение размеров и повышение плотности оборудования.

Технологические инновации в ЦОД-строительстве, считает г-н Сивцов, связаны в основном с коммерческими ЦОДами, которые сегодня оказались основными игроками на рынке ЦОД-услуг. Эти инновации направлены на повышение энергоэффективности и надежности. Что же касается корпоративных ЦОДов, то, по его оценкам, их начали строить ранее коммерческих, и их владельцам вскоре предстоит сосредоточиться на технологиях модернизации.

По мнению г-на Андропова, сегодня при строительстве и развитии ЦОДов руководствуются конкретными обстоятельствами (принцип case-by-case), а не закладывают, как ранее, изначально максимально возможную для заказчика избыточность ресурсов. Так, если раньше преобладали мощные (по 80—100 кВт) напольные системы кондиционирования, располагавшиеся по периметру чистого зала, то сейчас используются межрядные (InRow) кондиционеры, позволяющие охлаждать конкретную группу стоек. Такой подход к построению инженерной инфраструктуры ЦОДов отвечает запросам российских провайдеров ЦОД-услуг (у которых преобладает аренда площадей). Это побудило производителей инженерной инфраструктуры перейти к модульным, хорошо масштабируемым предложениям. Г-н Андронов считает, что к модульному подходу положительно относятся владельцы как коммерческих, так и корпоративных ЦОДов.

Алексей Шалагинов обратил внимание на то, что сегодня ЦОД помимо типовых может содержать и некоторые другие специализированные программно-аппаратные подсистемы, востребованные заказчиком. Например, внутри ЦОДа может быть развернут ситуационный центр для информационно-аналитической системы “Безопасный город”. Поэтому в числе трендов в ЦОД-разработках он назвал построение конвергированных инфраструктур, которые предусматривают вертикальную интеграцию приложений и инфраструктуры ЦОДа.

Николай Кузнецов отметил успехи (пока, правда, скромные) в управлении ЦОДами, достигнутые благодаря движению от отчуждения логики управления от оборудования и ее реализации на программном уровне, а также благодаря стандартизации компонентов ЦОДов и сближению функциональных характеристик предлагаемых разными вендорами продуктов, что обеспечивает заказчиком независимость от разработчиков.

Трудно не согласиться с большинством наших экспертов, настаивающих на неотделимости аппаратной части ЦОДов от программной, на их тесной взаимодополняемости. Тем не менее некоторые из них указали на такие особенности развития ЦОДов, которые четко свидетельствуют о том, что разработчики ком-

Наши эксперты



СЕРГЕЙ АМЕЛЬКИН,
менеджер по продукции
направления
“Качественное
электропитание”, Eaton
в России



СЕРГЕЙ АНДРОНОВ,
директор центра сетевых
решений, “Инфосистемы
Джет”



НИКОЛАЙ ГРИШИН,
ведущий консультант
по бизнес-приложениям,
Fujitsu в России и странах
СНГ



НИКОЛАЙ КУЗНЕЦОВ,
директор департамента
комплексных проектов,
“Борлас”



ВЛАДИМИР КОНДАКОВ,
руководитель отдела
серверных решений
и СХД, центр разработок
ПК “Аквариус”



ДЕНИС СИВЦОВ, менеджер
проектов подразделения
IT Business, Schneider
Electric



КИРИЛЛ ТЕРЕШЕНКО,
руководитель группы
технических экспертов
IBM PureSystems, IBM
в России и СНГ



РУСЛАН ЧИНЯКОВ,
вице-президент, OCS
Distribution



АЛЕКСЕЙ ШАЛАГИНОВ,
директор по отраслевым
решениям департамента
по работе
с корпоративными
заказчиками, Huawei

понентов ЦОДов фокусируются именно на программном компоненте.

Сегодня на слуху такие термины, как программно-конфигурируемые ЦОДы (SDDC), сети (SDN) и СХД (SDS), которые выражают тенденции к созданию программного слоя между ИКТ-инфраструктурой и поддерживаемыми ЦОДами приложениями. Этот слой должен обеспечивать гибкое и оперативное предоставление ИКТ-ресурсов работающим поверх них приложениям и эффективное централизованное управление всей инфраструктурой ЦОДов в целях бесперебойного предоставления этих ресурсов клиентским приложениям.

Современные ЦОДы, по выражению Сергея Амеликина, должны поумнеть. Достигается это повышением уровня интеллекта, заключенного именно в ПО компо-

ЦОД для энергосбыта: миллион счетов за час

Свыше 1,3 млн. частных потребителей и почти 39 тыс. юридических лиц в Челябинской области являются клиентами ОАО «Челябэнергосбыт» — гарантирующего поставщика электроэнергии в этом регионе. Ежедневно в филиалы компании стекаются 76 тыс. показаний от систем учета, сетевых организаций, контроле-



Аркадий Карев: «Оборудование подобрано с запасом по многим параметрам, поэтому его возможности и мощность могут быть без труда увеличены»

ров, данных квитанций, СМС-сервисов, а также из личных кабинетов потребителей. Общий объем корпоративных данных достигает 40 Тб. Большая часть из них обрабатывается двумя ключевыми приложениями: системой управления энергоданными Oracle Utilities Meter Data Management и системой биллинга Oracle Utilities Customer Care & Billing. Они отвечают за коммерческий учет поставленного электричества, расчеты и выставление счетов, а значит, именно их скорость работы и надежность имеют ключевое значение для бизнеса компании и энергоснабжения потребителей. Учитывая критическую важность этих систем, создание надежного и мощного центра обработки данных (ЦОД) для их размещения стало нетривиальной задачей, стоящей перед ИТ-блоком. Для ее решения совместной командой специалистов «Челябэнергосбыта» и компании «Борлас» были применены передовые подходы к созданию инженерной инфраструктуры и развертыванию вычислительных мощностей. Это позволило повысить скорость обработки данных и производительность используемых «Челябэнергосбытом» приложений в 2—11 раз в зависимости от типа выполняемых операций.

Расположенный в центральной части офиса компании в Челябинске ЦОД изначально был спроектирован с учетом необходимости выдерживать пиковые нагрузки при закрытии расчетного периода. Кроме того, он предусматривает и возможный рост объема обрабатываемых данных в будущем. Проектная мощность ЦОДа

по электропотреблению составляет 107 кВт. Обеспечивают его бесперебойную работу современные инженерные системы. Так, система кондиционирования, построенная с использованием оборудования Emerson, гарантирует круглосуточную и круглогодичную работу ЦОДа даже при критических нагрузках. Для этого используются

два чиллера в режиме ротации с максимальной холодопроизводительностью 100,5 кВт каждый. Непосредственно для охлаждения оборудования применяются четыре прецизионных кондиционера стоечного исполнения. Система кондиционирования имеет необходимый запас производительности, что позволяет «Челябэнергосбыту» при необходимости наращивать вычислительные мощности. Система питания

выполнена с использованием двух источников бесперебойного питания Chloride 80-NET мощностью по 120 кВт каждый, она защищает ЦОД в случае перебоев подачи электричества. Безопасность объекта обеспечивают система мониторинга, охранная сигнализация, системы видеонаблюдения, контроля и управления доступом. Традиционная пожарная сигнализация дополнена системой газового пожаротушения.

Начинка ЦОДа также отвечает передовым требованиям. В качестве основы вычислительной инфраструктуры ЦОДа используются интегрированные программно-аппаратные комплексы Oracle Exadata Database Machine и Oracle Exalogic Elastic Cloud. Они дают преимущества по производительности и надежности работы за счет того, что все их компоненты изначально настроены и оптимизированы для достижения наибольшей скорости, а самые высокие результаты достигаются именно при работе с базами данных и приложениями Oracle.

«В таких проектах особенно важно найти и предложить лучшие решения в каждом конкретном

случае. Так, по результатам тестирования для ЦОДа были выбраны оптимизированные комплексы Oracle, которые прекрасно работают в связке с приложениями этого поставщика и позволяют достичь выдающейся производительности. Важно также, что оборудование подобрано с запасом по многим параметрам, поэтому его возможности и мощность могут быть без труда увеличены, если этого потребуют развитие бизнеса и рост объема данных», — отметил вице-президент консалтинговой группы «Борлас» Аркадий Карев, участвовавший в проекте.

В качестве сервера баз данных «Челябэнергосбыт» использует Oracle Exadata Database Machine (в конфигурации Half Rack). Данная конфигурация Exadata содержит четыре сервера СУБД Oracle и семь серверов хранения данных. Специальное программное обеспечение Exadata позволяет прямо на серверах хранения выполнять множество операций, традиционно работающих на серверах СУБД. Это обеспечивает многократное увеличение производительности для разного типа запросов и операций по сравнению с обычными аппаратными конфигурациями. По данным тестирования Oracle, проведенных ранее с использованием данных среднестатистической энергопоставляющей компании, в системе Oracle Utilities CC&B на Oracle Exadata Database Machine за 1 мин было оформлено 16 500 счетов на оплату, что равняется почти 1 млн. счетов в час.

В качестве сервера приложений применен еще один представитель семейства Oracle Engineered System — Oracle Exalogic Elastic Cloud (в конфигурации Quarter Rack). Комплекс оптимизирован для работы с Java-приложениями разных типов. Включает в себя восемь вычислительных узлов, содержащих по два шестиядерных процессора и 96 Гб оперативной памяти каждый, и систему хранения ZFS 7320 Storage Appliance

(40 Тб дискового пространства). Совместная работа сервера баз данных и сервера приложений, подключенных при помощи сетевой инфраструктуры InfiniBand, дала возможность расширить «узкие места» и добиться комплексного роста производительности информационных систем. Сопровождение перевода баз данных и приложений



Павел Киселев: «Мы получили ИТ-поддержку, соответствующую лучшим мировым стандартам, что обеспечивает бесперебойное функционирование внутренних систем и процессов компании»

на новое оборудование также выполнялось совместно «Челябэнергосбытом» и специалистами «Борласа», уже имеющими подобный опыт. Это позволило сократить время простоя промышленной системы и быстрее начать эксплуатацию нового оборудования.

Новый ЦОД вывел производительность и надежность ИТ-инфраструктуры «Челябэнергосбыта» на новый уровень, что особенно важно — было ускорено выполнение важнейших бизнес-процессов компаний. Загрузка показаний приборов учета ускорена в шесть раз, а их обработка — в 11 раз. Время расчета потребления и начислений сократилось в 2,5 раза, а выгрузка соответствующего файла с квитанциями стала быстрее в 7,5 раз. В целом аналогичные положительные результаты были получены для различных операций, выполняемых системами управления энергоданными и биллинга.

«В своей работе мы используем мощные программные приложения. Естественно, что им нужна адекватная по масштабируемости и отказоустойчивости инфраструктура. Именно для этих задач был развернут новый ЦОД, — прокомментировал генеральный директор «Челябэнергосбыта» Павел Киселев. — В результате мы получили ИТ-поддержку, соответствующую лучшим мировым стандартам, что обеспечивает бесперебойное функционирование внутренних систем и процессов компании, а значит, надежность поставок электричества, точность и своевременность выставления счетов для потребителей на Урале».

Стратегические...

ПРОДОЛЖЕНИЕ СО С. 23

ментов, блоков и узлов. Этим требованиям соответствует большинство появляющихся сегодня на рынке продуктов для ЦОДов. Наиболее передовые ИКТ-разработчики организовали и поддерживают цикл переноса устойчивых фрагментов программного интеллекта в аппаратную часть — в специализированные интегральные схемы (ASIC), добиваясь тем самым от своих продуктов рекордных для рынка эксплуатационных характеристик.

Актуальные проблемы ЦОДостроительства
Руслан Чиняков считает российский рынок ЦОДов уже сформировавшимся: игрокам рынка, по его мнению, понят-

ны основные технологии, их достоинства и недостатки. Однако в отличие от рынков ЦОДов экономически развитых стран наш рынок отстает в востребованности сертификации и аудите существующих ЦОДов на уровне Tier III и IV. Потребность в ЦОДах такого качества, по его оценке, появилась в нашей стране только год назад. Он увязывает это с ожидаемым в России ростом спроса на услуги коммерческих ЦОДов. Подобный рост, кстати, по данным DCD Intelligence, аналитического подразделения компании DCD, имеет место во всем мире. Аналитики связывают его с усложнением корпоративной ИКТ-среды, а также, как упоминалось выше, с тем, что в трудные для экономики времена заказчики заинтересованы в уменьшении капитальных затрат.

Хотя в России доступны те же оборудование и технологии для ЦОДов, что и за рубежом, и некоторые эксперты оценивают данный сегмент рынка как сформировавшийся в нашей стране, считает Николай Кузнецов, еще не хватает экспертизы для реализации сложных, рекордных проектов, подобных тем, которые реализуют такие компании, как Google, Facebook, Amazon.

Экспертизы не хватает не только на уникальные проекты. Российские заказчики ЦОДов, согласно наблюдениям Дениса Сивцова, продолжают экономить на проектировании, планировании и управлении строительными работами (включая услуги проектных и инженеринговых компаний), несмотря на негативные последствия этой экономии — задержки и незапланированные траты

в процессе строительства, снижение надежности и энергоэффективности сдаваемых объектов. Однако он надеется, что вскоре на нашем рынке появятся экспертные компании, которые будут в состоянии разрабатывать проекты эффективных и надежных ЦОДов, а заказчики будут готовы адекватно оплачивать их услуги.

Одной из наиболее актуальных задач, стоящих сегодня перед владельцами ЦОДов, Сергей Андронов считает задачу максимальной утилизации инженерной инфраструктуры, решить которую можно с помощью ее детального мониторинга. Для этого разработаны специальные системы — Data Center Infrastructure Management (DCIM), потребность в которых особенно возросла с переходом к практике наращивания мощностей ЦОДов по мере необходимости.

Как построить систему защиты для ЦОДа?

АЛЕКСАНДР ЗАЙЦЕВ

Многие компании сегодня переносят свою ИТ-инфраструктуру и бизнес-приложения в ЦОД. В данной статье мы рассмотрим подходы к построению системы защиты ЦОДа.

ЦОД представляет собой сложную систему, состоящую из множества элементов. Архитектура ЦОДа — это сочетание физических и виртуальных серверов, различных систем, сервисов и приложений, предназначенных для обслуживания пользователей (внутренних, внешних, мобильных и др.). Поэтому при построении системы защиты ЦОДа необходимо учитывать особенности его архитектуры, а также специфические требования к обеспечению его надежности, доступности и производительности.

Для организации информационной безопасности (ИБ) ЦОДа необходимы несколько подсистем защиты, которые бы учитывали сетевую архитектуру, серверную (в особенности архитектуру виртуальных серверов), а также архитектуру сети хранения данных.

Можно выделить следующие элементы обеспечения ИБ ЦОДа:

- защита периметра ЦОДа;
- защита инфраструктуры ЦОДа (виртуальной и физической).

При этом используемые средства защиты ЦОДа должны соответствовать требованиям регуляторов. Поэтому при выборе СЗИ для ЦОДа необходимо обращать внимание на наличие у них действующих сертификатов ФСБ и ФСТЭК.

Защита периметра ЦОДа и безопасный удаленный доступ

Для построения системы защиты периметра ЦОДа, как правило, применяются традиционные подходы к обеспечению сетевой безопасности. Такая система строится по принципу эшелонирования и обычно предполагает использование пограничного

межсетевых экранов (МЭ), средств построения VPN-туннелей, системы обнаружения и предотвращения вторжений (IPS).

Для разграничения доступа между виртуальными сегментами можно использовать специализированные виртуальные МЭ, работающие на уровне гипервизора, или выделенный физический МЭ, через который будет маршрутизироваться сетевой трафик защищаемых виртуальных сегментов. Еще одним вариантом является работа выделенной высокопроизводительной платформы, на которой разворачиваются виртуальные МЭ (виртуальные контексты). Использование виртуальных МЭ на базе одной аппаратной платформы позволяет, с одной стороны, легко масштабировать систему, с другой — не требует приобретения дополнительных аппаратных средств, так как при необходимости можно создать дополнительный виртуальный МЭ на базе существующей аппаратной платформы. Для организации VPN-туннелей в ЦОДе применяются криптошлюзы, которые не только обеспечивают шифрование трафика, но и могут являться дополнительным межсетевым экраном. Среди отечественных продуктов, сертифицированных в ФСТЭК и ФСБ России, для этих целей можно использовать АПКШ “Континент” компании “Код Безопасности”.

Защита виртуальной инфраструктуры ЦОДа

Зачастую все информационные сервисы и бизнес-приложения компании разворачиваются в ЦОДе на базе виртуальной инфраструктуры (ВИ). Соответственно говоря о защите инфраструктуры ЦОДа, мы должны подразумевать в первую очередь защиту виртуальной среды ЦОДа.

Система защиты виртуальной среды ЦОДа должна обеспечивать:

- защиту информации, обрабатываемой в виртуальной инфраструктуре;
- защиту элементов управления виртуальной инфраструктурой.

Вопросы защиты информации, обрабатываемой непосредственно на виртуальных серверах и рабочих станциях, в принципе, очевидны. Как и в случае с физическими серверами, необходимо обеспечивать защиту информации от несанкционированного доступа (НСД), антивирусную защиту и шифрование информации.

Если говорить о защите управления ВИ, то многие компании не уделяют должного внимания данной проблеме. Однако появление такого элемента, как виртуальная среда, несет с собой новые угрозы, не всегда свойственные классическим автоматизированным системам. К таким угрозам относятся:

- угроза компрометации гипервизора (Microsoft Hyper-V, VMware vSphere Hypervisor) как нового по сравнению с физической средой элемента управления инфраструктурой;
- угроза утечки данных вследствие злонамеренных или непреднамеренных действий системного администратора, получающего доступ к данным и к инфраструктуре;
- консолидация нескольких серверов на одном аппаратном комплексе, что приводит к повышению риска компрометации консолидированного хранилища данных;
- угроза несанкционированного доступа администратора ВИ к настройкам и правам пользователей на серверах виртуализации;
- угроза нарушения целостности виртуальной машины;
- невозможность контролировать все события информационной безопасности и расследовать инциденты информационной безопасности в случае их возникновения.

Данные угрозы актуальны как для коммерческого ЦОДа, где арендуются ресурсы, так и для корпоративного.

Чтобы свести эти угрозы к минимуму, рекомендуется использовать встроенные в платформу виртуализации механизмы защиты гипервизора, а также специализи-

рованные средства защиты. Кроме того, если в виртуальном ЦОДе обрабатываются персональные данные, гостайна или другая информация ограниченного доступа, то для защиты виртуальной среды должны применяться только сертифицированные по требованиям безопасности информации средства защиты. Специализированных средств защиты для виртуальных инфраструктур, прошедших сертификацию в ФСТЭК России, на сегодняшний день не так много. Одним из таких средств является СЗИ от НСД vGate R2 для защиты виртуальных инфраструктур VMware.

СЗИ от НСД vGate обеспечивает комплекс мер по защите виртуальной инфраструктуры, а именно:

- разделение прав на управление виртуальной инфраструктурой и на управление безопасностью виртуальной инфраструктуры;
- усиленную аутентификацию администраторов виртуальной инфраструктуры и администраторов информационной безопасности;
- полномочное управление доступом к конфиденциальным ресурсам;
- контроль целостности конфигурации виртуальной машины (VM) и файлов гостевых систем VM, доверенную загрузку;
- централизованное управление и аудит событий безопасности;
- регистрацию событий;
- подготовку отчетов о состоянии и событиях информационной безопасности.

Практика показывает, что многие компании недооценивают сложность задач защиты ЦОДа. Успешность проекта по защите ЦОДа напрямую зависит от того, насколько тщательно будут проработаны не только вопросы технической защиты, но и организационные вопросы по обеспечению ИБ в ЦОДе. Начинать проект по защите ЦОДа лучше всего с разработки модели угроз, которая позволит выявить актуальные для бизнеса угрозы, после этого можно переходить к проработке технических и организационных решений.

Автор статьи — менеджер проектов компании “Код Безопасности”.

Ключевой функционал DCIM нацелен на автоматизацию инвентаризации физических ресурсов ЦОДов — оперативное выявление незанятых площадей, свободных юнитов в стойках, определение мощности электропитания и охлаждения (приходящихся на помещение в целом и на каждую стойку), количества модулей распределения питания, мощности перекрытий и фальш-полов и т. п. На основе полученной информации можно планировать размещение нового оборудования, вести статистику заполнения места в залах и стойках, энергопотребления, тепловыделения, прогнозировать темпы и направление развития ЦОДов, ожидаемые потребности в электричестве и теплоотводе, моделировать инфраструктурные потребности ЦОДа при различных вариантах его заполнения.

Сегодня разработчики ищут решение задачи стыковки управления и инженерной и вычислительной частей инфраструктуры ЦОДа, основная сложность которой заключается в том, что динамика изменения физической и виртуальной сред сильно различается. Инженерная инфраструктура, контролируемая с помощью DCIM, относительно стабильна и допускает управление в полупручном режиме. Иное дело ИТ-среда ЦОДа, тем более виртуализованная, тем более построенная по облачной архитектуре.

Как заявил Сергей Андронов, ни одна из представленных в настоящее время на рынке систем DCIM не позволяет обеспечить скорость управления изменениями, характерными для VM. Некоторые ИТ-вендоры пытаются решить задачу выделения для VM не только необходимой вычислительной мощности, но и ресурса электропитания и охлаждения, т. е. управлять инженерным и ИТ-оборудованием как единым пулом ресурсов. Для этого базу данных виртуальных и физиче-

ских ресурсов ЦОДа надо вести в одной системе. Но пока таких решений нет, хотя уже года через два-три потребность в них будет очень актуальна.

Перспективы ЦОД-технологий

С одной стороны, отметил Руслан Чиняков, на рынке имеется полный спектр продуктов, необходимых для создания продвинутых ЦОДов, но с другой — каждый из них реализует только часть полного функционала ЦОДа. Комплексные же решения, согласно его наблюдениям, пока единичны, их предлагают партнерские союзы разработчиков-лидеров. Однако подобные решения в основном закрыты архитектурно и не допускают использования компонентов других производителей.

Алексей Шалагинов вообще считает, что время “продуктовых предложений” для ЦОДов проходит. Интегрировать ЦОД из компонентов, по его мнению, сложно, долго и неэффективно даже при участии системных интеграторов — слишком велики риски нестыковок интерфейсов, несовместимости протоколов, появления других узких мест. Экономия на капитальных затратах при строительстве ЦОДа из набора “продуктовых предложений” неизбежна, подчеркнул он, “съедается” необходимостью устранения нестыковок и доработок. Поэтому сегодня компании предпочитают либо отдавать свои ИТ-системы на аутсорсинг облачным провайдером, либо приобретать готовые законченные решения для корпоративного ЦОДа.

К одному из важных направлений развития российского и мирового рынков ЦОДов Руслан Чиняков относит мобильные ЦОДы. Считается, что мобильные ЦОДы позволяют экономить на капитальных затратах (поскольку не требуют подготовки помещений и стоят в два-три раза меньше, чем стационарные аналоги), они

легче масштабируются, быстро развертываются, при необходимости их можно переместить в другое место и даже продать.

Вместе с тем контейнерные (мобильные) ЦОДы не являются конкурентами стационарным: такое решение эффективно, когда у заказчика есть необходимость обеспечить надежную инфраструктуру на удаленных территориях, в ограниченных пространствах внутри офисного здания или оперативно развернуть ИКТ-инфраструктуру (например, в полевых условиях).

Родственными модульным ЦОДам являются “ЦОДы в коробке”. Как пояснил Кирилл Терешенко, “ЦОД в коробке” представляет собой стандартизованное решение с современными серверами, высокопроизводительным сетевым оборудованием, интегрированной в шасси СХД, позволяющей виртуализовать все СХД заказчика и управлять ими как единым пулом хранения информации. Такой ЦОД предоставляет владельцу сотни готовых шаблонов для быстрого развертывания приложений (с возможностью разработки своих собственных), ПО для создания гетерогенной облачной среды, централизованную консоль управления всей инфраструктурой, упрощающую установку средств виртуализации, развертывание операционных систем и приложений, управление сетями, СХД и облачными средами. Кроме того, он умеет автоматически обнаруживать назревающие аппаратные проблемы.

Как считает Денис Сивцов, были и останутся актуальными технологии, позволяющие повышать энергоэффективность инженерной инфраструктуры. Так, сегодня востребованы технологии, увеличивающие эффективность классических систем охлаждения ЦОДа, — использование высокоэффективных систем периметрального охлаждения на прецизионных кондиционерах и высокоэффективных чиллеров.

Интересны для заказчиков системы кондиционирования, построенные на модульных экономайзерах косвенного испарительного охлаждения воздуха, позволяющие (в определенных условиях) значительно повысить эффективность системы охлаждения ЦОДа. В будущем достаточно перспективным, по мнению г-на Сивцова, станет построение систем кондиционирования на базе технологии жидкостного охлаждения ИТ-оборудования.

По мнению Николая Кузнецова, актуализируются задачи обеспечения безопасности ЦОДов, как физической, так и информационной. Он предполагает, что в ЦОДах найдут применение продвинутые методы шифрования, несмотря на то что это потребует увеличения производительности ЦОДов.

Алексей Шалагинов отметил тенденцию к переходу на твердотельные накопители в СХД. Они не уступают по емкости и надежности дисковым, значительно превосходя их по скорости ввода-вывода (IOPS), и могут повысить показатель IOPS до 20 крат. Однако они еще достаточно дороги (хотя цены на них быстро падают). Все большую актуальность, согласно его наблюдениям, приобретают СХД для больших данных, к которым предъявляются высокие требования: производительность до 5 млн. IOPS при емкости до 100 Пб и полосе пропускания системы коммутации до 170 Гбит/с.

Учитывая нынешнее концептуальное разнообразие в подходах к строительству ЦОДов, Руслан Чиняков склонен оценивать рынок ЦОДов далеким от зрелости. По его мнению, рынок находится на новом витке спирали развития. Появляются новички, которые теснят вчерашних лидеров. Предлагаются новые наборы “открытых” интерфейсов, сталкиваются кардинально противоположные стратегии развития ЦОДов.