Ведущая темы
Евгения ВОЛЫНКИНА

ждет ваших комментариев
в своем блоге на
www.iksmedia.ru

Дата-центр (от англ. data center) – специализированное здание (площадка) для размещения серверного и коммуникационного оборудования и подключения к каналам сети Интернет. В русскоязычной терминологии дата центр получил устойчивое название – центр хранения и обработки данных (ЦХОД) либо центр обработки данных (ЦОД). – Википедия

Центр обработки данных – это здание или его часть, первичной функцией которых является размещение оборудования обработки и хранения информации, а также вспомогательных (инженерных) средств, обеспечивающих его работу. – Стандарт TIA/EIA-942

Центрами обработки данных человечество занимается уже почти полвека, однако четкого определения для них так до сих пор и не выработало. Поэтому в угоду моде гордым званием «дата-центр» у нас сейчас величают самые разные объекты, в том числе комнатки размером с кладовку, где стоит подключенный к Интернету сервер и бытовой кондиционер. По этой же причине сложно оценить количество ЦОДов в нашей стране и объемы рынка в деньгах. Все специалисты признают, что есть «серверные комнаты» и есть «дата-центры», но мнения относительно того, где проходит грань между ними, сильно расходятся. Для одних мерило принадлежности «объекта» к категории «дата-центров» – количество занимаемых им квадратных метров, для других – число стоек с компьютерным и телекоммуникационным оборудованием, для третьих – уровень потребляемой электрической мощности, для четвертых – класс используемого оборудования, для пятых – состав этого оборудования (наличие систем резервного электропитания, газового пожаротушения, безопасности, автоматического мониторинга, управления и т.д.).

Но по большому счету любая компания заводит разговор именно о центре обработки данных только тогда, когда ценность этих данных для бизнеса становится настолько высока, что возникает необходимость обеспечить бесперебойное функционирование информационной системы и постоянный доступ к данным. В недостижимом идеале это, конечно же, 24 часа в сутки 365 дней в году, а в реальности – каждой компании приходится определять максимально допустимое для своего бизнеса время простоя и в соответствии с ним строить свой дата-центр или искать провайдера, предлагающего услуги ЦОДа должного уровня. Оба этих пути имеют свои плюсы и минусы и чреваты проблемами для всех участников этого рынка – владельцев, проектировщиков, строителей, системных интеграторов и клиентов ЦОДов, а также производителей оборудования для дата-центров. Попробуем с этими проблемами разобраться.

Погода для ЦОДов
Прогноз благоприятный

Центр обработки данных – совокупность помещений, строений, внешних открытых площадок (анклавов), образующих общее пространство для размещения вычислительной техники, электронных и иных средств приема, передачи, обработки, хранения информации и необходимых инженерных систем, обеспечивающих заданную степень доступности (готовности) среды в заданном режиме функционирования. – **Компания «Датадом»**

фокус

Всеобщая ЦОДофикация

В России дата-центры как направление бизнеса появились в 1999–2000 гг. Пионерами, как и следовало ожидать, стали самые богатые организации – банки, нефтегазовый сектор и госструктуры, начавшие строить ЦОДы для обработки больших массивов собственных данных. ЦОДы для обработки чужих данных, так же как и на Западе, первыми стали создавать интернет-провайдеры, поскольку им надо было где-то размещать сайты своих клиентов и обеспечивать их связь с остальным Интернетом. К тому времени многие пользователи, имеющие собственные сайты или собирающиеся их завести, уже поняли, что самостоятельное обслуживание сайта – занятие довольно хлопотное, которое к тому же не гарантирует нужной скорости доступа, так как для этого требуется очень широкий канал связи с Интернетом, а для обеспечения бесперебойной работы таких каналов должно быть как минимум два, что по карману только какому-нибудь корпоративному монстру. Зато широкие каналы (да еще с резервированием) есть у интернет-провайдеров, которым в принципе несложно поставить у себя несколько серверов для хранения сайтов своих клиентов и заработать на этом дополнительные деньги.

В последние годы информатизация бизнеса и многих услуг идет особенно активно. Автоматизированные системы управления предприятием есть уже не только у всех крупных, но и у многих средних компаний. Документооборот переводится в электронную форму. Повсеместно устанавливаются платежные терминалы для оплаты услуг сотовой связи, доступа в Интернет, ЖКХ. Биллинговые системы крупнейших мобильных операторов обслуживают десятки миллионов абонентов. Информационные системы ритейловых сетей, охватывающих целые регионы страны, должны обрабатывать данные всех кассовых аппаратов, информацию о складских запасах и доставке

Самые распространенные услуги коммерческих ЦОДов

Виртуальный хостинг – размещение веб-сайтов клиентов на серверах дата-центра, подключенных к Интернету.

Dedicated server – аренда у оператора дата-центра выделенного сервера необходимой конфигурации для выполнения приложений одного клиента.

Colocation – размещение в дата-центре физического сервера клиента и подключение его к широкополосным каналам связи. Обычно в состав услуги также входят обеспечение климатического режима, резервированное электропитание, охрана, мониторинг и простейшее техобслуживание оборудования (перезагрузка).

Происхождение вида

Первые дата-центры, или центры обработки данных, появились в 60-х годах прошлого века. Их сердцем были мэйнфреймы. Больше всего наследили в истории мэйнфреймы IBM 360, которые потом у нас решили клонировать, отказавшись от собственных компьютеров БЭСМ-6, «Мир» и др., инженерные решения которых во многом превосходили американские разработки. Так что в эпоху тогдашних дата-центров наша страна вошла с аналогом продукции IBM под названием ЕС ЭВМ. Разные модели этой серии выпускались с 1971 по 1998 г., и ими были оснащены многие советские предприятия и НИИ.

В 60–70-х годах дата-центры использовались главным образом для решения сложных вычислительных задач, под каждую из которых писалась своя программа. Затраты на дорогие мэйнфреймы (они и сейчас недешевы) и на штучную работу по созданию ПО могли позволить себе только крупные богатые компании, и это сдерживало широкое распространение дата-центров. Именно тогда возникла концепция обработки

товаров во все магазины сети. Растет спрос на тяжелый мультимедийный контент. Все это требует централизованной обработки гигантских объемов данных. Причем процесс этой обработки часто должен быть непрерывным, так как, например, даже небольшой простой биллинговой системы грозит оператору серьезными убытками. Компьютерные системы, способные обрабатывать с нужной скоростью такие объемы информации, потребляют столько электроэнергии, что для их нормальной работы уже недостаточно серверной комнаты в офисе. Компаниям приходится либо строить свой ЦОД с соответствующими системами бесперебойного электропитания и охлаждения, что требует колоссальных затрат, либо обращаться к услугам коммерческих дата-центров.

«Самая большая проблема при строительстве ЦОДа – где взять электричество? Все остальное меркнет».
Дмитрий Комиссаров, «Дейтариум»

Аутсорсинг: куда ни кинь...

Но такой аутсорсинг не всем подходит. Иногда политика безопасности компании запрещает передавать данные в чужие руки, хотя современные технологии защиты информации позволяют обеспечить конфиденциальность данных и при их обработке в сторонней организации. Правда, реализовать вариант аутсорсинга сейчас не так-то просто: спрос намного превышает предложение. Коммерческие дата-центры в России строятся довольно активно, но площадей все равно не хватает и места в ЦОДах бронируются задолго до их ввода в эксплуатацию. Неизбежное следствие этого дефицита и ажиотажного спроса – рост цен. За последние три-четыре года стоимость аренды серверной стойки в ЦОДе выросла в пять-шесть раз (!).

Московские цены уже выше среднеевропейских и американских. И ситуация, судя по всему, улучшится не скоро. Хотя оборудование для ЦОДа обходится недешево, немалый вклад в конечную цену проекта вносит стоимость электричества, причем не самих потребленных киловаттов, а фактически только разрешения на подключение к энергосети. Плата за подключение составляет сейчас 100 тыс. руб. за 1 кВт в центре Москвы, до 70 тыс. руб. – на окраине столицы и до 50 тыс. руб. – в коттеджных поселках в ближнем Подмосковье. Но и за такие деньги электричества в Москве практически нет.

В регионы за электричеством

В некоторых районах Московской области, а также в других регионах ситуация с электричеством не столь остра, но любой дата-центр требует толстых каналов связи, а с ними на большей части территории страны большие проблемы. Да и там, где они есть, цены на трафик, как правило, в разы превосходят московские. Правда, есть некоторая надежда на российских магистральных операторов, которые в последние годы активно двинулись в регионы, что способствовало некоторому снижению цен на интернет-доступ. Причем операторы не только потянули туда оптоволокно, но и сами стали строить ЦОДы. Например, недавно «Ростелеком» запустил дата-центры в Новосибирске, Екатеринбурге и Хабаровске, подключив их к своей магистральной сети. Причем в Хабаровске ЦОД располагается на одной площадке с точкой обмена интернет-трафиком РосНИИРОС. Занялись строительством дата-центров в своих регионах и МРК. В сентябре прошлого года «Синтерра» анонсировала программу строительства сети из 40 дата-центров в крупнейших городах России. Двинулись в регионы и корпоративные заказчики. Так, все операторы «большой сотовой тройки» уже имеют там ЦОДы и продолжают их строить: до конца 2008 г. МТС планирует построить пять дата-центров в пяти федеральных округах, а «МегаФон» намерен открыть семь ЦОДов.

«По тому, сколько в стране дата-центров, можно судить о развитости в ней ИКТ-инфраструктуры».
Сергей Лысаков, Stack Group

Перспективным представляется и планируемое строительство дата-центров в открывающихся технопарках. К примеру, анонсированы планы строительства в технопарке подмосковной Дубны двух самых крупных в России дата-центров площадью 10 и 20 тыс. м^2. Правда, скорой реализации этих планов ожидать не приходится (завершение проекта намечено на 2013 г.) и, следовательно, ликвидации дефицита услуг ЦОДов тоже.

информации как централизованного сервиса, предоставляемого вычислительным центром всем остальным подразделениям компании. По нынешней терминологии это внутренний аутсорсинг. Для внешнего аутсорсинга условий тогда не было, поскольку он требует наличия стандартных приложений, пользоваться которыми могут самые разные компании.

Активный рост ЦОДов начался в 80-х годах, когда компьютерное оборудование пошло в массы (пока только западные) и в связи с этим заметно подешевело. Одновременно увеличились мощность компьютеров и объем запоминающих устройств, компании стали создавать для обработки корпоративных данных свои вычислительные центры, а крупные компании, имевшие филиалы в разных городах и странах, соединяли свои дата-центры линиями связи.

Появление Интернета дало мощный толчок развитию дата-центров. До середины 90-х годов Интернет использовался главным образом для обмена электронной почтой и другими данными между пользователями, но со временем компании оценили перспективы Сети как среды ведения бизнеса. Для этого понадобились высокопроизводительные компьютеры и широкополосные линии связи, работающие стабильно и круглосуточно. Чтобы обеспечить такой режим работы мощных компьютеров, нужны были системы, поддерживающие необходимые климатические условия и непрерывную работу, т.е. системы кондиционирования и резервного питания, а также круглосуточная техническая поддержка. В общем-то, это и есть портрет современного дата-центра. ИКС

Мировая мода

Несмотря на столь бурную деятельность, Россия, как водится, заметно отстает в деле ЦОДостроения от развитых стран. Там вокруг дата-центров давно сложилась мощная индустрия, созданы ассоциации владельцев ЦОДов, производителей различного оборудования для них, консалтинговых и специализированных строительных компаний, например Институт профессионалов в области дата-центров (IDCP), Ассоциация менеджеров информационных центров (AFCOM), Американское общество инженеров по отоплению, охлаждению и кондиционированию воздуха (ASHRAE).

С 1993 г. в США действует авторитетная организация Uptime Institute, названная в честь основного критерия качества работы дата-центра – времени доступности сервера (uptime). На основе анализа имеющихся дата-центров, всех их систем и оборудования она вырабатывает рекомендации по обеспечению максимально надежной работы ЦОДов. Именно Uptime Institute предложил классификацию дата-центров по уровням надежности Tier I, II, III и IV (см. таблицу), определяющую среднее время простоя серверов ЦОДа в зависимости от структуры инженерных систем и уровня их избыточности. Есть также принятый в 2005 г. отраслевой стандарт TIA/EIA-942 Telecommunications Infrastructure Standard for Data Center (Стандарт на телекоммуникационную инфраструктуру центров обработки данных), разработанный Ассоциацией телекоммуникационной промышленности США (TIA) и охватывающий многие аспекты создания ЦОДов разных уровней надежности, в том числе принципы построения систем электропитания и кондиционирования, кабельных систем, требования к резервированию отдельных элементов ЦОДа, характеристики помещения, особенности размещения оборудования и многое другое, вплоть до расположения гостевой парковки.

У нас ничего похожего на профессиональные ассоциации пока нет и неизвестно, когда будет. Да, сообщения о создании или планах создания новых российских дата-центров появляются чуть ли не каждую неделю, но круг участников этого рынка остается довольно узким. Даже его старожилы имеют не такой уж большой опыт, а опыта проектирования и построения больших ЦОДов площадью несколько тысяч квадратных метров нет фактически ни у кого. Получить такой опыт на строительстве небольших дата-центров нельзя, так как они требуют оборудования другого класса и других инженерных решений. Так что пока остается смотреть на Запад и перенимать опыт там. Он должен пригодиться уже скоро (на вышеуказанном проекте дата-центров в Дубне).

Характеристики ЦОДов разных уровней надежности

Уровни	Tier I	Tier II	Tier III	Tier IV
Тип резервирования	N	N+1	N+1	N+1(2) или "система+система"
Ввод от электросети общего пользования	1 питающий кабель	1 питающий кабель	2 питающих кабеля (600 В и более)	2 питающих кабеля (600 В и более) от разных подстанций
Коэффициент готовности инженерных систем, %	99,671	99,749	99,982	99,995
Допустимое время простоя за год, ч	28,8	22,6	1,6	0,4
Год постройки первого ЦОДа данного уровня	1965	1970	1985	1995

Проблемы «озеленения»

Мировая индустрия ЦОДостроения сейчас озабочена «озеленением» дата-центров. Недавно Uptime Institute и консалтинговая компания McKinsey & Co представили доклад, в котором утверждается, что к 2020 г. объемы парниковых газов, выбрасываемых дата-центрами в атмосферу, увеличатся в 4 раза и превзойдут объемы выхлопов всех самолетов мира. Там же говорится, что цены на энергоносители растут со скоростью 16% в год, а основной проблемой для дата-центров является резкий рост энергопотребления, который обгоняет рост вычислительной мощности. Компании, строящие и эксплуатирующие дата-центры, обеспокоены тем, что их затраты на электроэнергию сильно выросли за последние годы и продолжают расти. По данным IDC, в 1996 г. на электроэнергию приходилось примерно 15% затрат на эксплуатацию дата-центров, а к 2010 г. ее доля возрастет до 70%. Поэтому около половины опрошенных Uptime компаний собираются в течение ближайшего года модернизировать свои ЦОДы, чтобы снизить энергопотребление их инженерных систем и ИТ-оборудования. Причем заинтересованы в этом прежде всего ИТ-директора, так как электроэнергия для дата-центров на Западе уже давно оплачивается из ИТ-бюджета компании.

Наших владельцев ЦОДов до недавнего времени больше волновал вопрос, где вообще взять электричество, а не его цена. Но теперь мы стараниями наших энергетиков, и в первую очередь почившего в бозе РАО ЕЭС, по стоимости 1 кВт•ч догнали США, а счет энергопотребления нынешних дата-центров идет на мегаватты. К тому же западная практика внесения платы за электричество, потребляемое ЦОДом, в ИТ-бюджет пришла уже и в Россию. Судя по всему, скоро она станет обычной для всех корпоративных дата-центров. И тогда ИТ-директора наших компаний вслед за владельцами коммерческих ЦОДов и всем прогрессивным человечеством должны будут озаботиться проблемами экономии электроэнергии всеми доступными способами. ИКС

Дискуссионный клуб «ИКС»

ЦОД = электрификация + $\sum_{n=1}^{\infty} x_n$

Дата-центры – модная нынче тема. Цены на услуги ЦОДов растут как на дрожжах, но клиенты стойко воспринимают удары судьбы – дефицит-с... Интернетизация и информатизация бизнеса требуют жертв. Ропщут только инвесторы ЦОДостроения. У них свой дефицит – электроэнергии, а аппетиты энергетиков явно зашкаливают. О проблемах и перспективах дата-центров в России - участники дискуссионного клуба «ИКС».

В условиях тотального дефицита

«ИКС»: С мощными стимулами ажиотажного спроса на услуги ЦОДов в общем-то все понятно, а каковы факторы, сдерживающие развитие этого рынка?

В. ВАНЬКОВ, директор по маркетингу, «Комкор»: Основной сдерживающий фактор – дефицит энергоресурсов. Отсюда и наблюдающийся в последнее время рост цен на услуги ЦОДов. Но рынок дата-центров все равно будет развиваться динамично: сейчас потребность в их услугах, по различным оценкам, превышает предложение в 1,5–2 раза и спрос увеличивается в среднем на 30% в год. Растет он в основном за счет клиентов двух типов: контент-провайдеров и крупных корпоративных клиентов (банков, страховых компаний и т.д.). У каждого из них своя специфика и свои требования к услугам. Контент-провайдерам важно обеспечить максимальную доступность своих сервисов для конечных потребителей – пользователей широкополосных сетей. У корпоративных клиентов, особенно у банков, на первое место выходят вопросы безопасности и контроля доступа размещаемого оборудования. Именно по этим причинам такие клиенты часто предпочитают строить собственные ЦОДы.

В. ВАНЬКОВ

А. ПАВЛОВ, генеральный директор, «Датадом»: В столице рост количества коммерческих и корпоративных ЦОДов сильно сдерживается отсутствием электроэнергии. Возможность строить дата-центры на территориях неработающих заводов практически исчерпана, поскольку и самих заводов не так много, и неиспользуемые ими электромощности были отобраны еще в начале 2000-х годов.

А. ПАВЛОВ

С. ЛЫСАКОВ, генеральный директор, Stack Group: Думаю, на данном этапе уместнее говорить не об отдельных сдерживающих факторах, а о высоком пороге вхождения в этот бизнес как о взаимосвязанном комплексе. Сюда входят и затраты на энергоресурсы, и усилия по преодолению кадрового голода, и проблемы правильного проектирования, строительства и эксплуатации дата-центров, и дефицит внимания к вопросам дата-центров в России со стороны государ-

С. ЛЫСАКОВ

ства. Что касается регионов, то там ситуация усугубляется астрономическими ценами на широкополосные каналы связи и полным отсутствием «темной» оптики.


В. КОВАЛЕВ

В. КОВАЛЕВ, начальник отдела ЦОД, «Открытые Технологии»: Рост вычислительных мощностей современного ЦОДа сдерживается недостатком площадей, где можно установить основное серверное оборудование. До недавнего времени ЦОДы размещались в бывших серверных либо машинных залах, рассчитанных на оборудование 10-летней давности. Отдельное здание для дата-центра выделяется редко.

М. ДРЯМИН, руководитель направления развития дата-центров, департамент ИТ-сервисов, «Ланит»: На развитие рынка негативно влияют проблемы информационной безопасности: компании не уверены в сохранности данных, которые будут обрабатываться на оборудовании, размещенном в дата-центре. Часть клиентов просто боится отдать свое оборудование в «чужие руки». Основная причина такого страха – недостаток информации о правильной организации системы информационной безопасности ЦОДа. Вторая причина – отсутствие ГОСТа на проектирование дата-центров. В результате не все ЦОДы соответствуют заявленным уровням надежности и другим не менее важным техническим параметрам.


М. СЕМЕНИХИН

М. СЕМЕНИХИН, ведущий менеджер департамента маркетинга, «РТКомм.РУ»: Для строительства корпоративных ЦОДов сдерживающие факторы – высокая стоимость как оборудования ЦОДа, так и подготовки площадки для него (до 50–60% цены оборудования), а также дефицит высококвалифицированных специалистов технического обслуживания.

Развитие аутсорсинга услуг дата-центров тормозят недостаточная информированность клиентов о его возможностях, малая численность дата-центров в регионах и высокая стоимость междугородных каналов связи для соединения ЦОДа в Москве с офисом в регионе. Кроме того, крупные организации, которые серьезно подходят к защите информации, к аутсорсингу услуг дата-центров, относятся с некоторым скепсисом из-за непроработанности законодательной базы и отсутствия стандартов оказания таких услуг.

Нужен ли ГОСТ для российских ЦОДов?

«ИКС»: Российского ГОСТа, определяющего правила построения и эксплуатации ЦОДов пока не существует, поэтому российские разработчики используют (факультативно) соответствующие американские и европейские документы. Как вы думаете, изменится ли ситуация с качеством дата-центров после принятия такого ГОСТа?


П. ЗЕЛЕНСКИЙ

П. ЗЕЛЕНСКИЙ, системный архитектор, «Инфосистемы Джет»: Не совсем правильно говорить, что российских стандартов нет. Есть целый ряд стандартов, требований и правил, в соответствии с которыми должны строиться ЦОДы на территории РФ: стандарты, определяющие состав документации, санитарные нормы и правила, по которым должны быть построены и оборудованы помещения, правила установки электроприборов, нормы пожарной безопасности, строительные ГОСТы, отраслевые требования по обеспечению безопасности. Другое дело, что нет сводного документа, который отражал бы специфику инженерных систем, необходимых для ИТ-составляющей дата-центра, поэтому в этой части мы сейчас опираемся на западные стандарты. Наличие российского ГОСТа позволило бы заранее определять требования к ЦОДу. Во многих случаях это упростило бы обоснование выбора решения.

А. МАРТЫНЮК, генеральный директор, [dc]^2: У нас есть документ СН-512-78 «Инструкция по проектированию зданий и помещений для ЭВМ». Он хотя и правильный, но старый, и его надо бы обновить. У нас есть переводной очень подробный СНиП по системам заземления, который сделан на основании американского стандарта по заземлению для ЦОДов, но им практически никто не пользуется, потому что это сложно и дорого. Стандарт TIA-942, принятый в США, – это скорее свод рекомендаций, поэтому его каждый трактует, как ему удобно. Отечественного стандарта по ЦОДам нет, но хочется его разработать, чтобы люди понимали, как и что надо делать. Это должно повлиять на качество дата-центров, потому что высокий уровень, задаваемый таким стандартом, будет стимулировать заказчиков и исполнителей следовать правилам. Последние три года мы пытаемся воспитывать заказчиков, и они уже многому научились и по-другому разговаривают с системными интеграторами, подрядчиками и строителями. Но регламентирующий документ им в этом очень поможет. Причем желательно, что-

бы в нем были ссылки на нормы пожарной безопасности, правила устройства электроустановок, строительные ГОСТы. Хочется, чтобы это был детальный и жесткий документ, который не позволял бы никаких вольностей.

С. ШАРАПОВ, заместитель директора по работе с корпоративными заказчиками и развитию рынка, Reichle & De-Massari Russia: Наша страна не является законодательницей мод в информационных технологиях и практически не принимает участия в международных форумах по разработке информационных стандартов. Так о каком же ГОСТе для ЦОДов мы можем говорить? Единственное, что мы можем здесь создать, это какое-нибудь специальное противопожарное требование. Кстати, каждый ли производитель оборудования для ЦОДов имеет сегодня противопожарный сертификат?


С. ШАРАПОВ

В. КУРИЛОВ, технический директор департамента сетевой интеграции, «Ланит»: То, что в России в настоящее время нет никаких документов, определяющих список обязательных инженерных подсистем в составе ЦОДов, – это абсурд. Строить пожароопасные системы, потребляющие значительное количество электроэнергии и выделяющие взамен большое количество тепла, без соответствующих средств защиты – большой риск не только для бизнеса, но и для здоровья окружающих. Конечно же, нужен документ, который регламентировал бы требования к средствам энергообеспечения, пожарной безопасности и физической защиты оборудования при строительстве ЦОДов.


В. КУРИЛОВ

А. СОЛОДОВНИКОВ, директор департамента по работе с корпоративными заказчиками, APC by Schneider Electric: В США и Европе много профессиональных ассоциаций, обладающих опытом, авторитетом и определенными алгоритмами выработки рекомендаций. В такой ситуации можно жить и без ГОСТов. У нас таких ассоциаций пока нет. Но есть книга всех времен и народов под названием «Правила устройства электроустановок». Одна из ее глав подробно описывает, как строить электроустановки для торфоразработок, но вот как организовать электроснабжение узла связи или современного дата-центра, ПУЭ хранит полное и скорбное молчание. А по поводу проектирования систем охлаждения и отвода тепла имеются только документы времен ЕС ЭВМ, т.е. 70-х годов прошлого века. Поэтому путь у нас пока один – перевод на русский язык западных стандартов и их творческая переработка.

«Одной гребенке» – неподвластны...

«ИКС»: В общем, обязательных правил для строительства ЦОДов нет. Существуют ли типовые проекты дата-центров?

А. СОЛОДОВНИКОВ: Думаю, что типового проекта для ЦОДа нет. Решение выбирается всякий раз в результате индивидуального проектирования, потому что в большинстве случаев приходится вписывать дата-центр в существующие помещения, для этого совершенно не приспособленные. И так происходит не только у нас, но и в Европе.


А. СОЛОДОВНИКОВ

В. ПИЛЬКО, директор по маркетингу, «СИТРОНИКС Информационные Технологии»: Типовые проекты, безусловно, существуют. Но это в теории. На практике же очень сложно найти два одинаковых ЦОДа: в любом случае будут разные помещения, разные условия работы и т.п.


В. ПИЛЬКО

С. ШАРАПОВ: В мире строится множество типовых ЦОДов, но надо избегать соблазна. Любой типовой проект ведет к стагнации. Заказчик берет и ставит его, не задумываясь о своем дальнейшем развитии. Другой вопрос, когда производитель предлагает различные варианты решения на базе своей линейки оборудования, адаптируя решение к поставленной задаче.

П. ЗЕЛЕНСКИЙ: До определенного уровня ЦОД типизировать можно, например в части инженерных систем. Можно поделить оборудование на какие-то «строительные блоки» и типизировать их. Но в реальности даже в пределах одной отрасли состав информационных систем ЦОДов сильно различается. Так что нельзя сказать: вот это будет ЦОД для банка или ЦОД для производственного предприятия и повесить на них соответствующие ценники.

И. МЫЗГИН, руководитель отдела инженерных систем, «Ай-Теко»: Типовые проекты инженерной инфраструктуры ЦОДов существуют только до определенного уровня абстракции: ЦОД на фреоне на 5 стоек, ЦОД на воде на 10 стоек. Когда проработка доходит до стадии рабочего проекта, каждый ЦОД уникален, как уникально

каждое здание, которое строится под запросы конечного заказчика. Множество нюансов, связанных с архитектурой здания, со схемами электроснабжения, с географическим поясом объекта, с оборудованием, которое будет в нем размещено, и т.д., приводят к тому, что каждый ЦОД необходимо проектировать заново, хоть и используя опыт предыдущих объектов.


И. МЫЗГИН

М. МИГУНОВ, главный конструктор, Computer Mechanics: Проект каждого дата-центра оригинален и индивидуален по-своему. Типовой ЦОД – это редкость. Многие компании-интеграторы имеют свой набор технических средств и методов для решения задач разного уровня. Это апробированные универсальные кирпичики для построения элементов ЦОДа. Тем не менее для достижения максимальной гибкости, масштабируемости и эффективности каждый проект требует тюнинга решений.


М. МИГУНОВ

...в одной коробке – не согласны

«ИКС»: В последние пару лет на мировом рынке появилось несколько решений, которые можно назвать «ЦОДы в коробке» (Sun Blackbox, InfraStruXure Express от APC и др.). Применимы ли они в российских условиях и найдут ли они спрос?

А. МАРТЫНЮК: Рынок мобильных ЦОДов в России пока только формируется и дозреет года через полтора. С технической точки зрения эти дата-центры у нас вполне применимы – контейнер привезти несложно, но после этого сразу возникают проблемы с инсталляцией и поддержкой. Да и по качеству исполнения мобильные решения заметно различаются. Производители таких ЦОДов должны честно говорить о комплектации своего решения и его функциональных возможностях, о том, что для его работы еще нужны ровная площадка, электроэнергия, каналы связи, вода, канализация, свободные мощности на холодильной машине (а если мобильный ЦОД должен быть отказоустойчивым, то на двух холодильных машинах). Если система рассчитана на другие стандарты электропитания, то нужны и трансформаторы. В общем, получается целый проект внедрения, к которому пока не готовы не только заказчики, но и поставщики таких решений.


А. МАРТЫНЮК

П. ЗЕЛЕНСКИЙ: «ЦОД в коробке» – мобильное решение, обеспечивающее быстрое построение корпоративной ИТ-инфраструктуры, восстановление после катастроф, ввод дополнительной мощности и т.д. Однако, принимая решение о выборе данной технологии, необходимо учитывать, что «ЦОДы в коробках» обычно требуют наличия внешних теплообменников-чиллеров, системы гарантированного электропитания и инфраструктуры связи. Кроме того, такое решение идеально подходит для теплых стран, а в условиях российской зимы для его запуска необходимо вспомогательное оборудование. Отдавая предпочтение «коробочному ЦОДу», нужно быть готовым к взаимодействию с госорганами – как только ЦОД в контейнере снят с прицепа и поставлен на землю, он становится строением, а если его поставили в ангаре, то изменением в конструкции строения. И все эти изменения необходимо регистрировать. Но, несмотря на возможные трудности, область применения мобильного центра обработки данных весьма разнообразна и в ряде случаев использование «ЦОДа в коробке» оказывается единственным верным решением.

Апологет

Наш ответ Sun Blackbox

Недавно московская компания ЧЕРУС представила новую разработку – «Мобильный ЦОД». Как рассказал руководитель департамента информационных технологий ЧЕРУС А. Кормильцев, идея этого решения была позаимствована у компании Sun Microsystems с ее известным дата-центром в контейнере Blackbox (официальное название – Sun Modular Datacenter S20), но конкретная ее реализация учитывает российские реалии. ЧЕРУС позиционирует свое изделие как основной или резервный корпоративный дата-центр, как мобильный офис и как модульное решение для быстрого расширения ИТ-инфраструктуры. По заявлению разработчиков, этот мобильный ЦОД, который может обслуживать предприятие с численностью до 500 человек, обойдется не дороже строительства обычного дата-центра в помещении и позволит даже сэкономить на подключении к более дешевым источникам электроэнергии, а также на арендной плате, поскольку его можно поставить на улице.

Мобильный ЦОД имеет утепленный корпус размером с транспортный 20-футовый контейнер (6056 x 2435 x 2805 мм). В нем можно разместить четыре-пять стандартных 19-дюймовых стоек с компьютерным и сетевым оборудованием. Причем поддерживается оборудование любых производителей, тогда как Sun Blackbox оснащается только оборудованием Sun.

Цена базовой комплектации без серверов и сетевого оборудования – $360 тыс. Комплект сетевого оборудования с двумя маршрутизаторами Cisco2821 добавит к вышеуказанной цене $56 тыс.; шасси HP BladeSystem c7000 с 14 серверами, дисковая система хранения данных на 3,6 Тбайт и ленточная библиотека – $191 тыс.; комплект ПО от Microsoft и VMware – $109 тыс.; система управления и мониторинга – еще $62 тыс. Итого – $778 тыс.

ЧЕРУС берется изготовить такой дата-центр за четыре месяца, монтаж и подключение провести за две недели, и первый заказчик уже есть. ИКС

В. ПИЛЬКО: «ЦОД в коробке» – отличное решение для компаний, столкнувшихся с непредвиденным ростом ИТ-инфраструктуры. Также он актуален в промышленности, если заказчик хочет видеть ИТ-инфраструктуру развернутой уже на этапе начала строительства предприятия.


М. ДРЯМИН

М. ДРЯМИН: Для компаний, чей офис находится за городской чертой, либо при отсутствии проблем с местом для его размещения, мобильное решение вполне оправданно: нет необходимости что-либо проектировать, закупать оборудование, связывать его в единую систему. Кроме того, такой подход позволяет существенно сократить сроки реализации проекта.

Мобилизация для региональной экспансии

«ИКС»: Производители мобильных ЦОДов предлагают разные варианты их использования, в том числе и в труднодоступных районах. Многие наши регионы можно назвать труднодоступными, но ЦОДы там строятся в существенно меньших количествах, чем в Москве. Что мешает?


К. ЕМЕЛЬЯНОВ

К. ЕМЕЛЬЯНОВ, руководитель центра решений, «Стинс Коман»: Ничего не мешает. Регионы отстают от столицы, это так. Но ЦОДы там строятся. Может быть, мешает психология. Регионы изживают психологию «бедности и отсталости». Вот это может мешать. А объективных препятствий нет. Там, где ЦОД выгоден, он обязательно появится.


В. МЕШАЛКИН

В. МЕШАЛКИН, начальник отдела серверов и систем хранения, АМТ: Сейчас многие компании выводят часть своего бизнеса в регионы, и в ряде случаев это экономически оправданно. Однако ЦОД, построенный в регионе, должен использовать каналы передачи данных, при которых его удаленность от центра никак не сказывалась бы на общей производительности компании. Но пока ни один провайдер не может похвастаться пропускной способностью магистральных каналов, конкурирующей с городскими сетями за соизмеримые деньги.


О. КУЩЕВ

О. КУЩЕВ, руководитель проектно-технического отдела, «Трансфер Эквипмент Восток»: Региональные ЦОДы строятся. В отличие от Москвы, где достаточно много дата-центров предназначается для сдачи в аренду, в регионах они строятся под конкретного заказчика или задачу. По мере децентрализации бизнеса и услуг мощность и количество ЦОДов в регионах будет увеличиваться. Многие технические и организационные проблемы строительства ЦОДов там зачастую решаются проще и быстрее. Нет такого, как в Москве, дефицита площадей и мощностей, а взаимодействие с местными властями идет оперативнее.

В. КУРИЛОВ: По-моему, дело в том, что пока не созрело представление о необходимости ЦОДов в регионах. Все понимают, для чего нужна развитая информационная инфраструктура в областных центрах, но многие считают, что такая инфраструктура не требуется в отдаленных регионах. Другой аспект – это стоимость создания равноценных дата-центров в Москве и, например, в Рязани. Стоимость площадей, электроэнергии, содержания самой системы значительно различается, и не в пользу Москвы. Единственный минус региональных ЦОДов – это уровень обслуживающего инженерного персонала, но эта ситуация поправима.


Д. КАЛГАНОВ

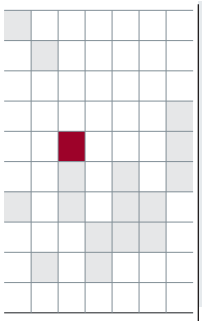
Д. КАЛГАНОВ, директор по производству управления инфраструктуры, ISG: Строительство дата-центров в регионах – довольно рискованное мероприятие. Крайне неравномерное экономическое развитие регионов дает основания полагать, что спрос на подобные услуги по стране будет также неравномерным, а это сильно повлияет на коммерческий успех проекта. Очевидно, что в первую очередь необходимо запускать пилотные проекты в регионах-донорах, где крупные предприятия и развитый вокруг них средний и малый бизнес создадут необходимый для быстрой окупаемости инвестиций спрос.


Р. ЛЕВОЧКА

Р. ЛЕВОЧКА, директор департамента продуктов и маркетинга, «Ростелеком»: Нам ничего не мешает строить дата-центры в регионах. Недавно мы открыли три ЦОДа, и все за Уралом – в Новосибирске, Екатеринбурге и Хабаровске. Это один из этапов реализации нашей стратегической инициативы по развитию инфокоммуникационных технологий в регионах на 2007–2008 гг. Мы и дальше будем развивать дата-центры, поскольку эта услуга популярна и востребована. Уже сегодня ясно, что открываемый нами ЦОД в Новосибирске очень скоро не сможет удовлетворить все потребности региона в услуге обработки данных. Поэтому строительство центров будет продолжено. А пока нам надо приобрести опыт их эксплуатации и предоставления услуг. ИКС

ПОЛНЫЙ ТЕКСТ
Дискуссионного клуба «ИКС» читайте на
www.iksmedia.ru

позиция



Кому в России нужны дата-центры нового поколения?

Уже стало привычным оценивать российский рынок с позиций «мы и они». Причем в большинстве случаев сравнение оказывается не в нашу пользу. К сожалению, не исключение и ситуация с дата-центрами. Как ни парадоксально, дело здесь не в техническом отставании.

Александр МАРТЫНЮК,
генеральный директор
компании [dc]²

Не хуже, чем у других?

Объективный взгляд на российский рынок ЦОДов не оставляет сомнений в том, что по уровню проектов, технических решений и их исполнению российские дата-центры в большинстве своем отстают от того, что делают «они», как минимум на два поколения. Особенно очевиден этот разрыв в секторе операторских и коммерческих ЦОДов. Российские проекты порой не выдерживают никакой критики как в плане подготовки помещения, так и в плане обеспечения заявленной отказоустойчивости. Исключением можно считать разве что действующие дата-центры МТС и Stack Group, при проектировании и строительстве которых были учтены самые современные на тот момент тенденции и концепции. Думаю, что сегодня уровень исполнения этих ЦОДов и есть та планка, относительно которой можно оценивать качество и инновационность других проектов, которые идут сейчас в России, – в большинстве своем громких и амбициозных.

Отрадно заметить: заказчики этих проектов начинают понимать, что, во-первых, использование ИТ-решений высокой плотности не всегда экономически оправданно; во-вторых, для поддержания отказоустойчивости ИТ должна быть создана соответствующая инфраструктура; в-третьих, не стоит ограничивать себя в выборе инфраструктурных решений, предлагаемых международным рынком. Да, есть, конечно, серьезные различия в платформах инженерных систем в США и в России, но это не главное. Например, последние разработки Emerson или APC, которые уже применяются в проектах на территории США, с тем же успехом можно использовать и у нас. Правда, было бы хорошо, если бы владельцы дата-центров руководствовались при этом принципом «лучшее из возможного», а не «не хуже, чем у других».

Возможно лучшее

Основная причина того, что многие новые отечественные дата-центры не соответствуют принятым в мире представлениям о современном ЦОДе, заключается не в техническом отставании российского рынка, а в различии мировоззрений и приоритетов.

Наш нынешний стандартный подход – это применение типовых решений для систем охлаждения и электропитания. В условиях острого дефицита услуг ЦОДов поставщикам этих услуг и их клиентам не до тюнинга – главное как можно скорее нарастить объемы. Редко кто задумывается о том, сколько электроэнергии потребляет климатическое оборудование. Практически никто не пытается всерьез оптимизировать системы охлаждения, чтобы снизить потребление электроэнергии (хотя она у нас довольно дорогая), чтобы получить возможность поставить больше оборудования и применять более сложные решения.

То же самое и с компьютерным оборудованием. Основные энергопотребители в серверах – это жесткие диски, блоки питания и вентиляторы. Чтобы они потребляли меньше энергии, нужно правильно хранить информацию, используя, например, ленточные библиотеки. Нужно устанавливать жесткие диски быстрой доступности и более длительного срока хранения, применять системы управления информацией, исключать реплики, вводить строгую каталожную систему. Какие там «зеленые» ЦОДы? Нам не до этого. Нам элементарно нужна «жилплощадь», а «ремонт» в ней будет делаться позже.

УПРАВЛЕНИЕ МОЩНОСТЯМИ

Интеллектуальное программное решение покажет, где оптимально разместить новые сервера с учетом электропитания, кондиционирования, наличия свободной площади и свободных позиций в шкафах. И все это в режиме реального времени.

НОВЫЙ ПОДХОД К КОНДИЦИОНИРОВАНИЮ

Оптимизируйте эффективность системы кондиционирования с помощью архитектуры охлаждения InRow™. Приближение кондиционеров к источникам тепла сокращает расстояние, преодолеваемое охлажденным воздухом (с 15 до 1,5 метров), предотвращая смешивание горячего отработанного и охлажденного воздуха в помещении. Тем самым организуется более целенаправленное прецизионное охлаждение.

ЭКОНОМИЯ ЭЛЕКТРОЭНЕРГИИ

Традиционные системы расточительно используют энергоресурсы. Воспользуйтесь преимуществами высокой энергетической эффективности, избавившись от избыточного запаса мощности инфраструктуры. Платите только за то, что вам действительно нужно!

Представляем инновационную архитектуру Efficient Enterprise™: больше мощности, больше контроля, больше прибыли

Можно ли сказать то же самое о традиционных системах?

Традиционный подход к кондиционированию заключался в охлаждении всего пространства серверного помещения, однако стремительный рост затрат на электроэнергию делает такие системы экономически невыгодными, а их конструкция с завышенными характеристиками не соответствует требованиям современных сред с высокой энергетической плотностью. Кроме того, неоправданно высокие расходы на электропитание и охлаждение могут стать препятствием к покупке нового ИТ-оборудования. Однако у этой проблемы есть простое решение. Сократив расходы на электропитание и охлаждение, вы можете использовать сэкономленные деньги на приобретение необходимого вам ИТ-оборудования. Согласно исследованию аналитической компании Gartner, 50% всех центров обработки данных, построенных до 2002 года, из-за недостаточной мощности систем питания и охлаждения безнадежно устареют уже к 2008 году. Сложности, связанные с электропитанием и кондиционированием — крупнейшая проблема, стоящая сегодня перед менеджерами центров обработки данных.

На избыток мощности уходит слишком много денег?

Ваш распределительный щит ограничивает количество потребляемой мощности, а бюджет — финансовые ресурсы? Вы вынуждены действовать в жестких рамках этих двух ограничений? Именно поэтому вам необходимо использовать инновационную концепцию APC Efficient Enterprise™!

Решения APC характеризуются модульной масштабируемостью, благодаря которой вы платите только за реально используемую мощность. Кроме того, специализированные системы внутрирядного кондиционирования и изоляции горячих коридоров, входящие в состав решения, улучшают условия охлаждения и обеспечивают стабильность температурных режимов. Применяя концепцию Efficient Enterprise и размещая кондиционеры непосредственно рядом с источниками тепла, вы можете сократить расходы на электроэнергию в среднем на 35%. Наша система способствует увеличению вашей прибыли. Неважно, строите ли вы новый центр обработки данных или анализируете эффективность действующих систем, в любом случае первым вашим шагом должен стать анализ текущей ситуации. Воспользуйтесь аудитом эффективности предприятия в режиме реального времени для того, чтобы наглядно увидеть все преимущества автоматизированной, интегрированной и эффективной системы: больше мощности, больше контроля и больше прибыли.

ИЗОЛЯЦИЯ ГОРЯЧИХ КОРИДОРОВ

Обеспечьте эффективность охлаждения за счет изоляции горячего воздуха и устранения смешивания холодных и горячих потоков воздуха. Наша система изоляции горячих коридоров Hot Aisle Containment System сокращает эксплуатационные расходы до 50% по сравнению с традиционными подходами.

Загрузите **БЕСПЛАТНО** информационные статьи APC в течение 90 дней (на сайте www.apc.com/promo после ввода кода **71134v**) либо заполните купон и пришлите его в офис APC по адресу: 119334, Россия, Москва, 5-й Донской проезд, д. 21Б, стр. 10 (отдел маркетинга) и станьте участником розыгрыша — **выиграйте сумку Power Ready Travel Bag**

Ф.И.О.: _____

Компания: _____

Должность: _____

Адрес: _____

_____

Отрасль: _____

Тел.: _____

E-mail: _____

APC в Москве: 119334, Россия, Москва, 5-й Донской проезд, д. 21Б, стр. 10,
Тел.: +7 495 916-7166, факс: +7 495 620-9180, E-mail: apcrus@apc.com

71134v

APC by Schneider Electric

Все это напоминает ситуацию примерно трехлетней давности, когда в России поднялся ажиотаж вокруг строительства интеллектуальных зданий, а за рубежом уже перешли к «зеленым» домам. Вот и теперь у нас стартовал марафон по созданию дата-центров категории Tier III или Tier IV, а у них тем временем идет горячий обмен мнениями по поводу строительства и эксплуатации «зеленых» дата-центров. Их задача – сделать ЦОДы максимально экологичными и минимально вредными. Они пытаются использовать вместо аккумуляторных батарей маховики, отказываются от дизелей и переходят на газ, строят систему охлаждения так, чтобы она максимально долго работала на внешнем охлажденном воздухе.

Не случайно последние по времени конференции DataCenters World в США были посвящены рассмотрению различных аспектов «зеленых» дата-центров. Причем, если осенью 2007 г. разговор шел на уровне инженерных систем, то весной 2008 г. вопрос «озеленения» изучался уже со стороны ИТ-оборудования. И говорили не только о серверах и мощности процессоров, но и об инженерном оборудовании и грамотном дизайне.

Отчасти в таком положении дел повинен и дефицит информации об аналогичных проектах, реализованных в мире. Причем это касается всех участников проектов – даже внутри одного вендора обмен сведениями о продуктах и решениях не всегда достаточно оперативный и российские подразделения западных поставщиков зачастую оказываются не в курсе достижений собственных головных компаний.

Строительство дата-центра – проект не из дешевых, а создание «правильного» дата-центра – тем более

Что могут системные интеграторы и строители

Чтобы придумывать и реализовывать небанальные технические решения, нужны знания и опыт, которым в России обладают единицы. Это те заказчики и системные интеграторы, которые понимают, что для того, чтобы построить хороший ЦОД, нужно ехать за границу и учиться. Подругому пока нельзя. Российские системные интеграторы, даже лидеры своего сегмента ИТ-рынка, испытывают острый дефицит знаний и специалистов, что не позволяет им спроектировать систему охлаждения или электроснабжения для дата-центра с требуемым уровнем надежности. Поэтому им нужно более тесно взаимодействовать с вендорами, призывая их показывать инновационные технические решения, рассказывать о сделанных проектах, знакомить с «историями успеха». Надеюсь, что в результате этой работы уже в ближайшее время на смену массовым продажам оборудования «с лотка» придет концептуально новый подход к проектам создания ЦОДов – на уровне решений предпоследнего, а то и последнего поколений.

Нередко отечественные системные интеграторы переоценивают свои возможности, пытаясь взять на себя управление проектом. Отсюда и ошибки. Недаром же на Западе сложилось четкое деление: есть консультанты, управляющие компании, координирующие ход проекта, и есть подрядчики по отдельным системам, которые не лезут в чужие разделы проекта. Наши системные интеграторы знают параметры вычислительной техники и хорошо делают СКС, поэтому они могли бы совершенствовать свой профессионализм, занимаясь созданием интегрированных ИТ-решений. А электрикой, климатическим оборудованием и другими инженерными системами должны заниматься специализированные компании. И такие компании в России есть, причем довольно высокого уровня. Они общаются не с российскими, а с зарубежными представительствами вендоров, которые показывают им передовые проекты. Они могут применять эти проектные решения и у нас, и как хорошие технические специалисты, стараются предложить максимально правильное техническое решение, а не продать максимально дорогое оборудование, чем грешат иные системные интеграторы.

Качество строительных работ при создании ЦОДов у нас тоже не блещет. Строительные компании, которые берутся за эти проекты, не видят особой разницы между домом, бизнес-центром и ЦОДом – строят как могут. А ведь ЦОД – это особый объект недвижимости. В нем нет и не может быть мелочей. У нас же в серверных помещениях можно встретить полы из ДСП, фанеры или другого горючего материала, деревянные плинтусы, а на стенах – пластиковые панели, как в обычной поликлинике. Если в ходе подготовки площадки приходится объяснять, что пол должен быть ровным, то рассчитывать на соответствующий ожидаемому уровню качества и надежности результат довольно сложно.

Чего хотят продвинутые заказчики

Некоторые российские заказчики уже осознали, что с системных интеграторов, берущихся строить им ЦОД, нужно требовать законченное комплексное решение, а не просто оборудование, которое можно поставить так, как нарисовано в проспекте производителя. Они ждут от системных интеграторов не предложений, позволяющих решить проблему отвода тепла, но построения дата-центра, который не потеряет своей актуальности и через пять-семь лет. Особенно это касается коммерческих ЦОДов, строящихся для сдачи площадей в аренду. Для них очень сложно заранее спрогнозировать, какое именно оборудование и в каких количествах привезут туда клиенты. Это может оказаться и стойка с небольшим энергопотреблением (например, с одним сервером и ленточной библиотекой), и несколько блейд-серверов, дисковый массив, а то и моноблочная система типа Sun Fire или HP Superdome с тепловыделением 5 или 10 кВт на стойку. Во втором случае оператору ЦОДа придется ставить локальную систему охлаждения или нагнетать в этом месте серверного помещения массу холодного воздуха. Потом придет еще один «горячий» клиент, а свободное место для его оборудования будет только в другом конце зала – и там придется делать то же самое. Но ведь можно создать такой проект, чтобы зал был рассчитан в среднем на 2–5 кВт на стойку, а с помощью шкафного оборудования или трубной разводки позволял отвести до 20 кВт тепла от заданного ограниченного количества стоек. Такой ЦОД в целом будет более экономичен и с энергетической точки зрения более эффективен, чем зал, подготовленный к тому, что в любом

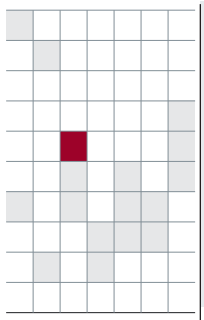
месте может быть установлена высоконагруженная стойка. То есть уровень решений задач может быть разным. Те крупные российские компании, у которых уже есть не один коммерческий дата-центр, сейчас применяют правильные технические решения, можно сказать, предпоследнего американского поколения.

Конечно, строительство дата-центра – проект не из дешевых, а создание «правильного» дата-центра – тем более. Заказчик должен отдавать себе отчет, что, если через два-три года при установке нового ИТ-оборудования потребуются дополнительные дизель-генераторы и переделка инженерных систем, это выйдет дороже, чем строительство инженерной инфраструктуры с нуля. Так что оптимальное решение, сделанное с учетом последующей модернизации дата-центра, может оказаться в итоге заметно дешевле «экономного варианта». Перестраивать же ЦОД придется, поскольку многие компании планируют выходить на IPO, а для этого нужно выполнить определенные требования по ИТ-обеспечению бизнеса. В общем, изменения в сознании заказчиков корпоративных ЦОДов уже идут, и довольно быстро.

По своему опыту знаю, что ряд крупных заказчиков проектов ЦОДов уже лично познакомились с организацией дела в западных дата-центрах. Там они увидели, что «правильный» ЦОД – это 200–300 человек в службе эксплуатации, 7 человек на диспетчерском пульте, 40 охранников, всё под контролем, всё просматривается и записывается, с клиентом заключается соответствующий договор, гарантирующий, например, что вышедшее из строя оборудование заменят со склада в течение получаса. Получить в России такой уровень обслуживания пока очень тяжело, но спрос есть, и компании-операторы ЦОДов вынуждены будут тянуться за такими заказчиками.

Выбирая, как всегда, свой особый путь, мы все-таки постепенно учимся учитывать опыт и ошибки, которые другие уже совершили. Понимаем, что пришло время думать другими категориями, более цивилизованно заниматься бизнесом, больше учитывать интересы заказчика, а не собственные интересы. Потому что в итоге заказчик заботу оценит. ИКС

аналитик



Сколько стоит colocation в регионах?

аналитик

На российский рынок коммерческих дата-центров выходят крупные игроки – телекоммуникационные операторы, специализированные ИТ-компании. Они реализуют проекты, которые предусматривают строительство новых дата-центров не только в Москве и Санкт-Петербурге, но и во многих регионах. С какими тарифами на их услуги придется столкнуться новым участникам региональных рынков?

В.И. ДЕМЧИШИН,
генеральный директор
ЗАО «Современные Телекоммуникации»

А.Г. СВИРИН,
инженер-исследователь
ЗАО «Современные Телекоммуникации»

Для анализа регионального рынка дата-центров* были выбраны города: Екатеринбург, Краснодар, Красноярск, Нижний Новгород, Новосибирск, Пермь, Самара, Ростов-на-Дону и Хабаровск. Основное внимание было уделено дата-центрам, предлагающим услуги хостинга и colocation (аренда стойки либо размещение сервера). В настоящее время наиболее востребована услуга размещения сервера. Тарифы именно на нее мы и рассмотрим в настоящей публикации.

Из чего складывается цена

Цена размещения сервера клиента (т.е. colocation), как правило, включает оплату самого размещения сервера, а также его подключения к Интернету или сети передачи данных. Первый, единовременный, платеж (регистрационный или установочный) оператор дата-центра берет за монтаж

* См. аналитический отчет «Коммерческие региональные дата-центры в РФ: состояние и перспективы развития», 2008 г.: ЗАО «Современные Телекоммуникации».

Рис.1. Средний ежемесячный платеж за размещение сервера (1 Unit)

Источник: "Современные Телекоммуникации"

Рис. 2. Средняя плата за входящий внешний трафик

Источник: "Современные Телекоммуникации"

Рис. 3. Средний ежемесячный платеж за услугу colocation

Источник: "Современные Телекоммуникации"

оборудования клиента в стойку на своей технологической площадке. В дальнейшем за размещение сервера взимается ежемесячная абонентская плата (исходя из места для сервера размером 1U в стандартной 19-дюймовой телекоммуникационной стойке). Иногда вместо ежемесячной оплаты предлагается ежегодная. В таком случае клиент получает скидку, которая может достигать 30% месячного платежа.

При подключении сервера к Интернету клиент единовременно оплачивает инсталляцию Ethernet-порта (full duplex). Стоимость порта зависит от скорости подключения, типовое значение 10 Мбит/с, реже – 100 Мбит/с (подключения со скоростью 1 Гбит/с пока не предлагает практически никто). В комплекте с Ethernet-портом клиент бесплатно получает определенное число IP-адресов (обычно 1–2). Дополнительные IP-адреса оплачиваются клиентом помесячно (в пределах $2–5 за порт). За дополнительную плату также можно подключить добавочный Ethernet-порт.

В дальнейшем оплачивается использование порта и ежемесячный трафик. Здесь операторы дата-центров предлагают различные варианты тарификации. Например, в ежемесячную плату за порт включается определенное количество трафика (обычно это входящий трафик). Тогда оператор тарифицирует превышение лимита трафика, как входящего, так и исходящего. Некоторые операторы тарифицируют трафик по направлениям. Например, компания Orange Business Services берет в Санкт-Петербурге за трафик из Екатеринбурга $28/Гбайт. Иногда плата за порт так высока, что объем трафика не ограничивается.

В последнее время у операторов стал популярен вариант оплаты преобладающего трафика вне зависимости от того, входящий он или исходящий (при погигабайтной тарификации).

Величину ежемесячных платежей за услугу colocation, включая абонентскую плату за размещение сервера и плату за трафик, мы оценивали для модели «один сервер, один порт 10 (100) Мбит/с, два IP-адреса, входящий трафик – 5 Гбайт, исходящий – 15 Гбайт». Именно такое соотношение входящего и исходящего трафика (5/15 Гбайт), по сообщениям представителей региональных дата-центров, наиболее вероятно для одного сервера. И именно такая модель характеризует работу сервера, на котором размещен среднестатистический информационный интернет-сайт, поддерживающий ежедневные обращения десятков абонентов. Естественно, при изменении потребления трафика платежи могут существенно измениться.

Разброс цен велик, но объясним

Изучение стоимости услуг коммерческих региональных дата-центров проводилось в феврале 2008 г. Различия в величине средней ежемесячной платы за размещение сервера (рис. 1*) в исследованных городах составили более 2000 руб. (500%). Это выходит за рамки разумного и может быть обусловлено различиями в тарификации трафика (рис. 2). Действительно, в Ростове-на-Дону максимальная плата за размещение сервера (1U), но плата за 1 Гбайт трафика минимальная. Однако в Перми сравнительно до́роги и трафик, и размещение.

В результате с точки зрения цен на услугу colocation в целом (с учетом абонентской платы за размещение сервера и оплаты трафика по принятой модели) именно Пермь оказалась самым дорогим городом, а Ростов-на-Дону – самым дешевым (рис. 3).

Приведенные цифры говорят, вероятно, о востребованности дата-центров в конкретных городах: чем больше абонентская плата, тем выше потенциальный спрос на их услуги. Отметим, что в шести исследованных городах цена находится в пределах от 7080 руб. (Хабаровск) до 8740 руб. (Краснодар).

Если в качестве опорных точек выбрать 3000 руб. и 6000 руб., то получится, что в 98% региональных дата-центров средний ежемесячный платеж за colocation превышает 3000 руб., а в 73% дата-центров – более 6000 руб. (рис. 4).

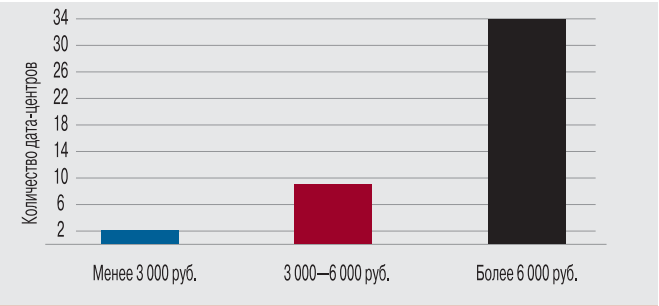
Регионы на фоне столиц

Сравним средние ежемесячные платежи за colocation, полученные в результате исследования рынка региональных дата-центров, с результатами исследования рынка дата-центров Москвы и Санкт-Петербурга (проведенного ЗАО «Современные Телекоммуникации» в мае 2007 г.). За опорные точки также взяты значения в 3000 руб. и 6000 руб. (рис. 5).

Хотя при исследованиях столичных дата-центров была выбрана другая модель потребления трафика (входящий/исходящий трафик – 15 Гбайт/100 Гбайт, а не 5/15 Гбайт, как для региональных рынков), полученные различия подтверждают вывод: на рынке услуг дата-центров, так же как и в ряде других сегментов телекоммуникационного рынка, имеет место существенное **цифровое неравенство** между столичными и остальными регионами РФ.

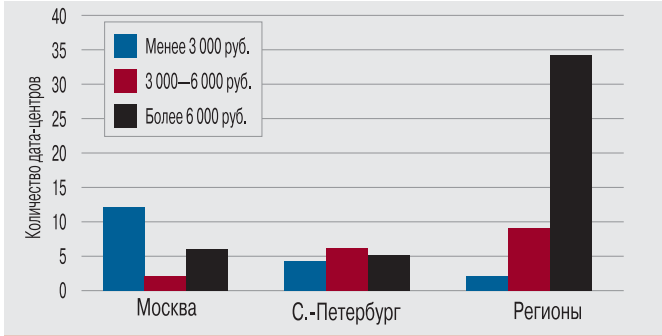
* Цены на рис. 1–3 указаны в рублях с учетом НДС по состоянию на 01.02.2008.

Рис. 4. Распределение среднего ежемесячного платежа за услугу colocation в зависимости от количества дата-центров в городе



Источник: "Современные Телекоммуникации"

Рис. 5. Распределение среднего ежемесячного платежа за услугу colocation в регионах, Москве и С.-Петербурге



Источник: "Современные Телекоммуникации"

Значительно более высокие цены на colocation в регионах (при меньшем объеме трафика) можно объяснить либо дефицитом площадей в региональных дата-центрах, либо дороговизной трафика, а скорее всего, в таком положении повинны оба указанных фактора.

В целом существующие тарифы на услуги дата-центров в российских регионах (в частности, на colocation) говорят о том, что этот рынок пока находится на начальном этапе развития. В дальнейшем, при увеличении предложения, можно ожидать выравнивания тарифов как на размещение, так и на трафик.

Если учесть тарифную политику местных операторов дата-центров, то наиболее привлекательными для создания новых коммерческих ЦОДов выглядят Пермь, Екатеринбург и Краснодар. Однако существуют и другие критерии, которые следует учитывать при выборе городов для строительства дата-центров.

Один из основных факторов, определяющих развитие рынка коммерческих дата-центров в регионах РФ в ближайшей перспективе, включая снижение тарифов и повышение доступности услуг для различных категорий пользователей, – это инвестиционная деятельность федеральных игроков: телекоммуникационных операторов и специализированных ИТ-компаний. ИКС

Сценарий

Эволюция бизнеса:
от непрофильного к профессиональному

С. ЗАЙЦЕВ

Бизнес коммерческих ЦОДов в России делается все более профессиональным. О его эволюционном пути и проблемах рассказывает Сергей ЗАЙЦЕВ, заместитель коммерческого директора, Stack Group.

Коммерческие дата-центры в России начали строить в начале 2000 г. Причем занимались этим в основном телекоммуникационные провайдеры, заинтересованные в развитии пакета услуг, предлагаемых клиентам, и, как следствие, в увеличении объема генерируемого ими трафика. Но, обращаясь к услугам такого дата-центра, клиент попадал в зависимость от одного оператора, который болезненно воспринимал желание клиента получить резервные каналы связи у других операторов. Все это до недавнего времени налагало серьезные ограничения на работу клиентов.

Следующей вехой можно считать 2006 г., когда по времени совпали три процесса. Во-первых, бизнес клиентов дата-центров телеком-операторов заметно вырос и потребовал наращивания компьютерных мощностей; во-вторых, ценовые войны, которые вели между собой интернет-провайдеры, привели к сильному снижению цен на трафик (по крайней мере в Москве); в-третьих, началось бурное развитие крупных интернет-проектов, требующих больших ресурсов и «толстых» каналов связи. Вот тут и выяснилось, что площадок для размещения этих ресурсов катастрофически не хватает.

Общую картину усугубило то, что одновременно пошел в рост корпоративный сектор. Компании, имевшие собственные небольшие серверные в офисах, столкнулись с необходимостью их модернизации. Но новое оборудование, которому нужны более мощные системы электропитания и охлаждения, далеко не всегда могло быть размещено в старых стенах. К тому же не у всех компаний есть возможность, ресурсы и желание заниматься созданием и обслуживанием такого инженерно сложного объекта, как ЦОД. Отсюда – очередь желающих разместить свое оборудование в коммерческих дата-центрах. И это несмотря на активное развитие сети дата-центров SDN, ввод в эксплуатацию московского дата-центра ISG, реализацию «Синтеррой» инициативы «40 x 40».

Причин тому три. Во-первых, строительство дата-центров – это большие инвестиции в инженерные системы, в компьютерное, телекоммуникационное, сетевое и прочее оборудование. Во-вторых, в Москве острый дефицит электрических мощностей, а для серьезного дата-центра нужно как минимум 5 МВт. В-третьих, большой заинтересованности в подобных инвестициях трудно ожидать от операторов связи, которые пока составляют большинство владельцев ЦОДов – для них услуги ЦОДов бизнес отнюдь не основной.

Неудивительно, что появление «неоператорских» дата-центров было с энтузиазмом воспринято корпоративными заказчиками, которые не могут или не хотят работать только с одним оператором и уделяют большое внимание обеспечению непрерывности сервисов дата-центра, влияющих на успешность их бизнеса. Они внимательно следят за анонсами проектов строительства дата-центров в Подмосковье (Дубна, Пущино), регионах («40 x 40», Санкт-Петербург). Но насколько их ожидания будут оправданны, пока неясно, поскольку, во-первых, требования корпоративных заказчиков и владельцев интернет-проектов к ЦОДам сильно различаются, а во-вторых, в России до сих пор нет ни одного системного интегратора и ни одной строительной компании с опытом проектирования и строительства больших и «правильных» дата-центров. Экскурсии на западные ЦОДы, безусловно, полезны, но просто увидеть, как выглядит дата-центр снаружи и даже изнутри, недостаточно, а о тонкостях мало кто рассказывает. Поэтому чем длиннее эволюционный путь компании на рынке услуг дата-центров в России, тем ниже вероятность грубых ошибок (проектных, юридических, эксплуатационных) и, соответственно, выше уровень лояльности к ней клиентов. ИКС

Эволюция технологий:

от мэйнфреймов к автоматической виртуализации

История дата-центров подтверждает, что эволюция идет по спирали. Причем в данном случае старое опять становится новым, не успевая даже хорошо забыться.

Вениамин ИВАНОВ,
менеджер по развитию бизнеса технологии центра обработки данных, Cisco Systems

Концепция ЦОДов 70-х годов, называвшихся тогда вычислительными центрами, очень напоминала нынешнюю. Конечно, возможности самих компьютеров за прошедшие годы изменились кардинально, но общие требования к построению дата-центра остались практически неизменными. Машинный зал представлял собой отдельное помещение (в идеале с ограниченным доступом) с фальшполом и фальшпотолком, где проходили жгуты кабелей, с системами кондиционирования и бесперебойного электропитания. Вычисления были централизованными, т.е. в ВЦ был один мэйнфрейм, на котором одновременно можно было решать несколько задач и выдавать результаты на пользовательские терминалы. Иногда таких компьютеров было несколько и для обеспечения бесперебойной работы они связывались между собой сетью.

Но мэйнфрейм – это дорогая машина, она по карману только крупной и богатой организации. Аутсорсинга вычислительных услуг тогда не существовало, а небольшие предприятия, которым так же, как и крупным, для ведения бизнеса нужны были вычислительные мощности, требовали более дешевого решения своих проблем. Поэтому начался переход от дорогих многозадачных систем к малым машинам, мини-ЭВМ, а затем и к массовому производству персональных компьютеров. Как только появились однозадачные малые машины, стал необходим обмен данными между ними и, соответственно, понадобилась сеть. Тогда же появилась идея сервера как централизованного хранилища информации и места исполнения приложений. Сервер был связан сетью с пользовательскими терминалами, которые уже назывались клиентскими компьютерами. Причем клиент-серверная архитектура предполагала исполнение клиентских и серверных приложений и обмен данными по сети между ними по схеме «запрос-ответ». Таким образом, приложения стали собираться на более мощные компьютеры, а данные записываться на более емкие носители для более эффективного использования. А с ростом количества бизнес-приложений появилась необходимость объединять их в каком-то общем вычислительном ресурсе и сводить данные в общую систему хранения. То есть на следующем витке эволюции вместо децентрализации вычислений на арену вновь вышла централизация.

Это дало новый импульс бизнесу мэйнфреймов IBM. За прошедшие годы многие небольшие компании с ростом своих вычислительных потребностей накупили массу компьютеров и систем хранения. Теперь они обнаружили, что эти огромные ресурсы используются очень неэффективно. На них и ориентирует свои решения IBM, убеждая избавиться от распределенных компьютерных ресурсов, используемых на 15–20%, и объединяющей их сложной сети. Вместо этого предлагается старый добрый мэйнфрейм с логическими разделами для каждого приложения, общая система хранения

также с логическими разделами для приложений и простая сеть для передачи информации на пользовательские терминалы (идея консолидации ресурсов распространилась и на сеть, центром которой стал один большой коммутатор).

Но сейчас идея консолидации перешла на следующий уровень: появилась возможность свести имеющиеся в компании серверы в большой вычислительный кластер, а затем с помощью ПО типа VMware произвести виртуализацию, т.е. логически сегментировать имеющиеся физические ресурсы для более эффективного их использования. Каждому приложению выделяется логический сегмент кластера в соответствии с его потребностями. Такую же операцию можно произвести с системами хранения данных и с сетевой структурой, создав виртуальные сети хранения данных.

Правда, эти процедуры пока предполагают участие человека, который должен определить потребности приложений в тех или иных ресурсах и произвести соответствующее логическое разбиение. Следующим этапом эволюции ЦОДов после виртуализации ресурсов в нем, по идее, должна стать автоматизация предоставления этих ресурсов. Приложения не всегда потребляют одинаковое количество ресурсов – бывают пики и спады. Если приложения начнут «понимать», сколько у них есть доступных ресурсов, использовать ровно столько ресурсов, сколько необходимо именно сейчас, и обмениваться между собой ресурсами, то это не только еще больше повысит эффективность обработки данных, но и позволит удалить из ЦОДа самую ненадежную его часть – человека. ИКС

Дата-центр. Для себя и на продажу

Бизнес дата-центров четко делится на две категории: коммерческие ЦОДы, которые строятся для того, чтобы сдавать мощности и предоставлять услуги сторонним компаниям, и корпоративные дата-центры – исключительно для собственных нужд.

Дмитрий КОМИССАРОВ,
генеральный директор
компании «Дейтариум»

ЦОДы «для себя» строят обычно достаточно крупные компании, имеющие дата-критичный бизнес. Если это не «времянка», а важный для компании проект, то зачастую это более дорогое решение по сравнению с коммерческим ЦОДом, его проектируют с запасом по мощности, надежности и резервируемости оборудования, даже большим, чем реально нужно.

Коммерческие дата-центры рассчитаны, как правило, на небольших корпоративных клиентов и хостинг интернет-сайтов, которым бесперебойность работы менее важна. К тому же это все-таки коммерческий проект, рассчитанный на получение прибыли, и владельцы стараются минимизировать свои издержки, экономя на системах кондиционирования и охлаждения, на резервных дизель-генераторах. Поэтому уровень защищенности от всяческих аварий в коммерческих дата-центрах ниже.

Еще одно важное отличие состоит в том, что у коммерческого ЦОДа обычно огромное число клиентов (десятки, сотни и даже тысячи). В корпоративный дата-центр, по идее, не пускают никого, кроме персонала самого ЦОДа (в некоторых компаниях руководители любят водить в ЦОД клиентов и партнеров, но по правилам делать это категорически запрещено). А в коммерческом ЦОДе бывает два варианта режима: либо в нем все делают только сотрудники дата-центра (но такой порядок очень сложно выдержать), либо доступ к стойкам имеют и сотрудники клиентов, и тогда обеспечение безопасности и разграничение доступа – гораздо более сложная задача.

Аналогичная ситуация с сетевой безопасностью. Оператору коммерческого ЦОДа нужно изолировать каналы связи клиентов друг от друга, иначе при DOS-атаке на один из хостящихся сайтов произойдет отказ в обслуживании у всех остальных клиентов. Закрытый корпоративный дата-центр, где работают серьезные информационные системы и хостится только корпоративный сайт, «чужие» DOS-атаки не беспокоят.

Ситуации с рабочими нагрузками на разные дата-центры тоже различаются. Если ЦОД спроектирован без достаточного резерва для пиковых нагрузок, а это бывает довольно часто из-за экономии на системах жизнеобеспечения (см. выше), то проблемы неизбежны. Какие именно бизнес-приложения работают на серверах корпоративного дата-центра и как в них меняется нагрузка, его администраторам хорошо известно, каких-то резких, непредсказуемых скачков там обычно не бывает. К тому же в частном ЦОДе не может вдруг появиться система с произвольными характеристиками. В коммерческом ЦОДе хозяева, как правило, не знают, какие именно приложения работают на серверах клиентов и чего от них можно ожидать. Если там стоят серверы каких-нибудь информационных сайтов, резкое повышение нагрузки предсказать сложно. Например, произошло какое-то неординарное событие, люди пошли на сайты за информацией, серверы поднялись, диски завертелись, энергопотребление резко возросло. А если в это время на улице +30°С, система охлаждения ЦОДа может не выдержать перегрузки, в результате – перегрев и серверы встали. То же самое может произойти и при виртуальном хостинге серверов.

В общем, требования к надежности и работоспособности коммерческого ЦОДа ниже, но проблем с эксплуатацией больше.

В такой ситуации, на мой взгляд, правильно действуют дата-центры, которые продают клиентам места под стойки с заданным уровнем потребляемой мощности. Таким образом часть проблем перекладывается на клиента. Если его серверы превысили оплаченный уровень мощности (например, 3 кВт), автомат просто отключит такую стойку и остальное оборудование ЦОДа не пострадает. В большинстве же старых дата-центров сделано по-другому. Там определен

максимальный уровень подвода мощности к стойке (например, 10 кВт), и у каждой стойки стоит автомат, который позволяет этот уровень выбрать, но сумма этих максимальных мощностей больше, чем общая мощность, подведенная к залу, и она больше той, на которую рассчитана система охлаждения ЦОДа. Поэтому, если всплеск нагрузки случился одновременно на многих стойках, то дата-центр остановится.

Но клиентам выбирать не приходится. В новых, старых, «правильных» и «неправильных» дата-центрах мест практически нет. Общая потребность в новых мощностях ЦОДов в 2008 г. составляет, по скромным подсчетам, около 3 тыс. стоек, а реально будет введено в эксплуатацию порядка 1 тыс. стоек. И этот дефицит сохранится, на мой взгляд, как минимум до 2010 г. Вот корпоративные клиенты и пытаются строить своими силами, наступая на те же грабли, по которым уже прошлись другие. Ведь в проектировании, строительстве и эксплуатации дата-центров масса тонкостей, известных только специалистам, которых у нас пока немного. Поэтому стоимость корпоративных ЦОДов по отношению к полученному результату очень высока. ИКС

ЦОД: строим сами или?..

На что стоит обратить внимание, приступая к строительству ЦОДа? Всегда ли оправданно «натуральное хозяйство» или же можно найти альтернативные решения?

Денис КАЛИНИН,
генеральный директор
IBS DataFort

Теория и практика

Если у вас нет успешного опыта проектирования ЦОДа, не стоит браться за это самостоятельно. Ведь ЦОД в промышленном исполнении – сложная и точно рассчитанная машина, которая должна максимально надежно обеспечивать оборудование электроэнергией и отводить тепло, постоянно поддерживая требуемые условия эксплуатации вычислительных систем. Незначительные на первый взгляд просчеты в конструкции могут привести к фатальным последствиям и потере ценной корпоративной информации. Имеет значение любая мелочь, вплоть до высоты потолка или глубины фальшпола, и ошибка чревата полной неработоспособностью центра в дальнейшем. Одной теории здесь недостаточно, нужен опыт – опыт строительства и эксплуатации подобных систем. Поэтому лучше обратиться в специализированную организацию.

Второй момент – оборудование и сервис. Одни компании просто строят ЦОД, а потом передают гарантийные обязательства от поставщиков оборудования, а другие берут на себя сопровождение всех систем в будущем. Предпочтение следует отдавать вторым, потому что в противном случае вам придется самостоятельно добиваться решения проблем от поставщиков оборудования.

Подводные камни проекта

Строительство ЦОДов в России из-за неравномерного развития инфраструктуры имеет свои особенности. При выборе места для дата-центра необходимо учитывать климатические условия, возможные проблемы с электричеством, логистикой и транспортной инфраструктурой, необходимой для завоза материалов и доступа персонала, и, безусловно, обеспеченность каналами связи.

Начнем с электроэнергии, стоимость которой весьма высока и продолжает стремительно расти. Электропотребление в ЦОДе необходимо тщательно спланировать, понять, откуда можно взять электропитание, как подвести его к зданию и обеспечить резерв. Требуемые мощности лучше переоценить, чем недооценить. Во втором случае вы столкнетесь с необходимостью полной или частичной перестройки инфраструктуры ЦОДа, которую будет очень трудно, а иногда и невозможно выполнить без остановки оборудования.

Например, на территории Москвы строить ЦОД бессмысленно, поскольку сегодня подключение к энергоресурсам в столице запрещено. Если у вас нет готовой электрической емкости, то цена подключения ЦОДа к сети фактически будет равна стоимости строительства самого центра. В Подмосковье и других субъектах РФ надо учитывать иные аспекты: для кого строится дата-центр (где находится центральный офис), насколько важно нахождение собственной службы на территории ЦОДа и т.д. В настоящее время наилучшее место для ЦОДа предприятия с головным офисом в столице – Подмосковье и города ЦФО, поскольку именно такое расположение обеспечивает надежные каналы связи и хорошие подъездные пути.

При проектировании ЦОДа следует задуматься, как скоро потребуется увеличивать его общую производительность и, самое главное, во сколько обойдется модернизация. Часто, пытаясь сэкономить на начальном этапе, компании ориентируются на дешевые, но плохо масштабируемые решения. Но рано или поздно наступает момент насыщения инфраструктуры и выясняется, что для ее расширения требуются затраты, сопоставимые с первоначальными.

Тернии эксплуатации

Распространенная ошибка – недооценка затрат на обслуживание ЦОДа, которые в период окупаемости проекта могут составить до 80% его стоимости, а могут сделать проект и вовсе убыточным. Подробный анализ этих затрат будет полезен и тем, кто уже эксплуатирует собственный ЦОД, и тем, кто только планирует его построить. Причем сумма, которая закладывается в бюджет, должна позволить масштабировать инфраструктуру как минимум в течение пяти лет.

Эксплуатационные затраты складываются из затрат на амортизацию и сервис оборудования и, конечно же, затрат на персонал, поддерживающий инфраструктуру ЦОДа. Чтобы минимизировать затраты на персонал, в ЦОДе следует предусмотреть эффективную систему мониторинга и централизо-

ванного управления. Дорогостоящее оборудование выдерживает плановые сроки наработки на отказ только при эксплуатации в требуемых условиях. Поэтому каждый случай повышения температуры в помещении ЦОДа из-за отказа системы охлаждения уменьшает срок службы компьютерного оборудования, а значит, увеличивает его амортизацию. Например, недопустимый перегрев среды (до 40°С) практически всегда приводит к выходу из строя жестких дисков в дисковых хранилищах и модулей памяти в серверах (что может привести также к отключению оборудования и потере данных).

Функционирование ЦОДа – это непрерывное поддержание баланса между потреблением энергии и отведением тепла. Поэтому в крупных дата-центрах критическое повышение температуры в машинном зале может произойти всего через несколько минут после аварийного отключения оборудования охлаждения. Следовательно, скорость оповещения персонала и скорость реакции на нештатные ситуации – важнейшие параметры эксплуатации ЦОДа. Наличие у персонала подробных документированных схем электрической сети, оборудования, аварийных планов (Disaster Recovery Plan) кардинально снижает риски потерь.

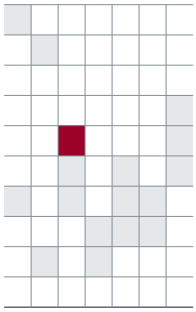
Эксплуатация в основе своей – вопрос организационный. Здесь много специфики, связанной с управлением именно ЦОДом, а не привычной ИТ-инфраструктурой офиса. И имеет смысл оценить, стоит ли компании этим заниматься самостоятельно.

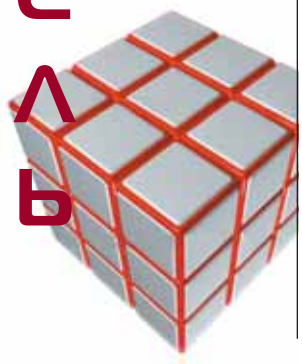
Поиск альтернативы

Наиболее эффективный способ минимизировать затраты и риски на ЦОД – это аутсорсинг. На рынке существует большое количество коммерческих ЦОДов, которые предоставляют в аренду площади под вычислительное оборудование клиентов. Также сейчас можно не просто арендовать полезную площадь, а заказать ЦОД как услугу, передав на аутсорсинг все риски, связанные с эксплуатацией ИТ-оборудования. Если ИТ-процессы в компании достаточно зрелые, то управление информационными системами, включая ERP и CRM, можно передать сервис-провайдеру. Тогда поставщик услуг будет обеспечивать не только размещение этих систем в ЦОДе и их эксплуатацию, но и экономичное развитие.

Правда, спрос на услуги дата-центров сейчас существенно превышает предложение, поэтому места в ЦОДах нужно «бронировать» еще на этапе их строительства. Тем не менее спрос подогрел рынок и 2008 г., очевидно, станет годом бума ЦОДостроительства, что позволяет рассчитывать на общий рост рынка этих услуг. ИКС

Модель





ЦОД, который не боится катастроф

Игорь ЛИТВИНОВ,
руководитель отдела аппаратно-программных комплексов, «Микротест»

Компании все сильнее зависят от своих информационных систем. Для создания катастрофоустойчивых дата-центров крупнейшие корпорации могут позволить себе самые сложные решения и дорогостоящие технологии. Существуют ли катастрофоустойчивые решения для среднего бизнеса и полностью ли они удовлетворяют требованиям российских заказчиков?

Двигатели прогресса

Растущая стоимость корпоративной информации диктует свои требования к конфигурации ЦОДов, заставляя предприятия создавать полноценные решения. Чем дороже данные, тем больше усилий требует их защита.

Второй бизнес-движитель, определяющий облик современного ЦОДа, – необходимость постоянного повышения эффективности использования ИТ-ресурсов. Стоимость эксплуатации ИТ-систем увеличивается год от года и намного опережает рост бюджетов ИТ-подразделений. Руководители ИТ-служб непрерывно предпринимают усилия по сокращению издержек – иначе средств на развитие просто не останется.

Быстро изменяющаяся бизнес-среда – третья тенденция, влияющая на ИТ-инфраструктуру. ИТ-директора озабочены оперативным и качественным обслуживанием запросов бизнес-пользователей. Чем большей гибкостью обладает ИТ-инфраструктура, тем быстрее и проще ее можно перестраивать под изменяющиеся требования бизнеса.

На эти общие движители развития ИТ-инфраструктуры налагаются специфические требования для отдельных отраслей. Характерный пример – розничный банковский бизнес. Предприятия хотят быть ближе к потребителям и поэтому вместо нескольких крупных филиалов открывают множество киосков или точек продаж и обслуживания клиентов. Однако в таких точках нет собственных данных. Это всего лишь киоски, а все данные должны надежно храниться и обрабатываться в ЦОДах, рас-

положенных на центральных технологических площадках. Понятно, что от надежности функционирования такой площадки зависят все бизнес-процессы и в конечном счете сам бизнес организации.

Облик современного ЦОДа

Итак, требования бизнеса в полной мере определяют направления развития современных ЦОДов и всей ИТ-инфраструктуры компании. ЦОД должен:

1. быть **централизованным (консолидированным)**. Защитить информацию, хранящуюся на одной технологической площадке, гораздо проще, чем обеспечить контроль за данными, распределенными по всей компании.
2. быть **гибким и адаптивным**. Инфраструктура должна легко и быстро подстраиваться под требования бизнеса.
3. соответствовать требованиям **экономической эффективности**. Его ресурсы должны утилизироваться, т.е. быть по возможности равномерно и полно загружены.
4. соответствовать требованиям **производительности, масштабируемости и надежности**.
5. обеспечивать **непрерывность бизнеса**. С определенного момента компании становятся настолько зависимыми от своих ИС, что простой ИТ-сервисов приводит в большинстве случаев к недопустимому ущербу.

Выполнение первых четырех требований к ЦОДам способны обеспечить такие инструменты, как консолидация, виртуализация и стандартизация вычислительных ресурсов и систем хранения данных.

Консолидация (объединение ИТ-ресурсов на базе одной технологической площадки или даже одного крупного решения) обеспечивается и на уровне хранения данных, и на уровне вычислительных ресурсов. Примечательно, что если консолидация хранения данных производится заказчиками достаточно давно (масштабные хранилища данных уже созданы в крупных компаниях, операторах связи и банках), то консолидацией вычислительных ресурсов ИТ-руководители предприятий активно занимаются сейчас.

Виртуализация – это средство балансировки нагрузки и, следовательно, повышения утилизации ресурсов. Она подразумевает запуск нескольких виртуальных программных сред или создание на одном реальном физическом устройстве нескольких виртуальных. Если для решения одной бизнес-задачи выделено достаточно ресурсов, а для другой их не хватает, то виртуализация помогает эти ресурсы гибко перераспределять. До последнего времени она активно применялась для повышения гибкости и эффективности использования систем хранения данных, а сейчас – вычислительных систем.

Стандартизация ИТ-ресурсов означает использование при построении ЦОДа решений, основанных на индустриальных стандартах. Это поможет обеспечить необходимую гибкость дата-центра. В случае выхода из строя какого-либо устройства оно без труда может быть заменено на аналогичное.

Несколько сложнее обстоит дело с катастрофоустойчивостью – возможностью оперативного восстановления критически важных ИТ-сервисов и корпоративных данных в случае масштабных аварий на технологических площадках ЦОДов.

Непрерывность бизнеса, или Сохранность яиц в одной корзине

Консолидация ИС, ИТ-сервисов и корпоративных данных в крупных дата-центрах радикально повышает требования к обеспечению непрерывности бизнеса. С одной стороны, консолидация повышает качество предоставления ИТ-сервисов, простоту и эффективность эксплуатации, утилизацию ресурсов, а с другой – компания становится заложником надежности одного ЦОДа. Фактически все яйца кладутся в одну корзину, и если с дата-центром что-нибудь случится (пожар, землетрясение и т.п.), то все данные могут потеряться. Как это предотвратить?

Обеспечивать **сохранность данных** можно посредством их резервного хранения на удаленной площадке. В случае аварии данные уцелеют, но процессы восстановления ИТ-сервисов займут много времени. Компания практически будет простаивать, пока не будет создан новый ЦОД. На это уйдут недели, и далеко не каждое предприятие может это себе позволить.

Для обеспечения **непрерывности бизнеса** необходимо построение полноценной резервной площадки с воспроизведением критически важных сервисов и постоянная репликация данных между основной и удаленной площадками. Именно постоянная репликация и составляет суть катастрофоустойчивого решения – в случае аварии она позволит быстро восстановить критически важные для бизнеса сервисы.

Построение резервной площадки – задача нетривиальная. Для ее решения необходимо проработать множество ответов на вопросы «а что будет, если...?». Ведь может возникнуть неисправность основной системы хранения данных, а серверы продолжат работать, может выйти из строя не основной, а резервный ЦОД или нарушиться канал связи между технологическими площадками и т.д. Каждый

Инфраструктуре ЦОДа – простоту и порядок

Дата-центр – это сердце любой компании, независимо от того, использует она его в качестве собственного корпоративного ВЦ или для предоставления коммерческих услуг обработки данных своим клиентам. Требования бизнеса непрерывно растут, и, чтобы соответствовать им, инфраструктура современных ЦОДов все больше усложняется. ИТ-менеджеры обычно реагируют на проблемы самым простым способом – устанавливают дополнительное оборудование, которого нередко оказывается больше, чем нужно на самом деле, и в результате управлять ИТ-инфраструктурой делается все труднее.

В любом, особенно крупном, дата-центре необходимо вести централизованный мониторинг состояния всех ресурсов (серверов, сетевых коммутаторов, дисковых систем хранения данных, удаленных архивов на магнитных лентах, баз данных, приложений) и осуществлять активное управление работой приложений на десятках и даже тысячах физических или виртуальных серверов. ИТ-подразде-

случай предполагает множество сценариев дальнейшего развития событий, и для сохранения непрерывности бизнеса нужно заранее предусмотреть все варианты.

Какие катастрофоустойчивые решения для крупного и среднего бизнеса чаще всего предлагаются? Как правило, строятся две системы хранения и организуется репликация данных между ними. Выбираются критичные для бизнеса информационные ресурсы, которые должны функционировать при любом развитии событий. Вычислительные ресурсы, необходимые для оказания выбранных ИТ-сервисов, воспроизводятся на удаленной площадке. А далее следует самое важное – настройка логики поведения в той или иной ситуации. Обычно это делается с помощью кластерного ПО. Это может быть ПО производителей серверных решений (например, Sun Cluster, HP Service Guard, IBM HACMP) или продукты независимых вендоров, например Veritas Cluster Server компании Symantec. Кроме того, можно использовать сервисы высокой доступности, заложенные в решении для виртуализации компании VMware. Настройка кластерного взаимодействия между основной и резервной площадкой – достаточно сложный процесс, предполагающий подробное рассмотрение различных вариантов аварий и написание сценариев развития событий для каждого из них. Однако при этом остаются случаи, для которых с точки зрения формальной логики нет рационального решения (например, обрыв канала связи между двумя технологическими площадками) и полная автоматизированность восстановления сервисов достигнута не будет.

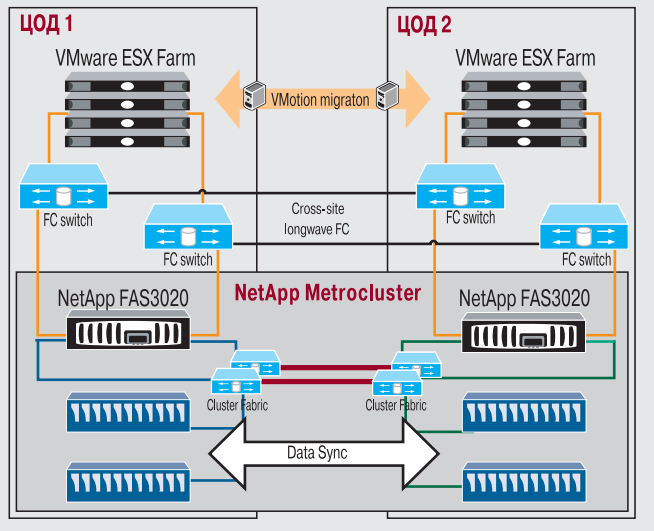
Динамический виртуализованный катастрофоустойчивый ЦОД

При построении катастрофоустойчивого ЦОДа, доступного среднему бизнесу, мы рекомендуем обеспечивать виртуализацию на всех уровнях – как на уровне **систем хранения данных**, так и на уровне **сети хранения** и **вычислительных ресурсов**. Решение, удовлетворяющее этим требованиям и основанное на продуктах NetApp, Dell и VMware, было внедрено у наших заказчиков и доказало свои преимущества.

Динамический виртуализованный катастрофоустойчивый ЦОД (см. рисунок) состоит из вычислительной инфраструктуры под управлением VMware Infrastructure и системы хранения NetApp Metro Cluster под управлением операционной системы Data ONTAP, в которую «зашита» логика работы распределенной системы хранения.

При выборе серверов для построения вычислительной инфраструктуры мы рекомендуем решения Dell. Продукты этой компании еще не достаточно оценены в России, но, по нашему мнению, они наилучшим образом отвечают требованиям стандартизации ИТ-ресурсов. Dell не выпускает уникальных и «закрытых» продуктов, а предлагает массовые тиражируемые решения на основе индустриальных стандартов.

Динамический виртуализованный катастрофоустойчивый ЦОД



Источник: "Микротест"

Для обеспечения виртуализации вычислительной инфраструктуры динамического ЦОДа используются решения VMware, поскольку они поддерживают все современные возможности виртуализации. Так, вычислительная инфраструктура под управлением программного пакета VMware Infrastructure 3.5 независимо от количества используемых серверов представляет собой единую систему. При этом совершенно неважно, на скольких площадках она работает. Сервисы, обеспечивающие высокую доступность и динамическую балансировку нагрузки, функционируют независимо от того, на какой площадке физически расположены серверы. Виртуальные машины могут «перемещаться» с площадки на площадку без остановки сервисов, и на решении задач бизнес-пользователей это никак не отразится.

Для организации виртуализованной системы хранения в случае, если есть возможность использовать две технологические площадки в пределах «городского» расстояния, идеально подходит NetApp MetroCluster. В отличие от схожих решений других производителей, NetApp создает, по сути, единое хранилище данных, которое тем не менее

лению компании нужно не только выявить и учесть все ресурсы, находящиеся внутри дата-центра или связанные с ним, но и повысить скорость реагирования на события. Причем придется обеспечивать работу в неоднородных средах со всеми распространенными платформами и операционными системами (UNIX, Windows, Linux, IBM-AIX, NetWare).

Для того чтобы справляться с этими задачами, могут использоваться самые разные инструменты – от доморощенных решений до промежуточного ПО, привязанного к конкретному оборудованию, и универсальных программ, не зависящих от поставщика. Один из таких инструментов – программный пакет Symantec Veritas Data Center, поддерживающий все основные операционные системы, массивы носителей и серверы. В его состав входят консоль централизованного оперативного управления хранением данных Storage Management в гетерогенных средах, программа Veritas NetBackup для защиты и резервного копирования данных, программа обеспечения непрерывности работы приложений Veritas Cluster Server, ПО для управления гетерогенными и онлайновыми системами хранения Storage Foundation и др. Это решение упрощает инфраструктуру дата-центра и позволяет ИТ-службе сосредоточиться на предоставлении услуг, а не на обслуживании «железа», которое эти услуги предоставляет. ИКС

распределено между двумя технологическими площадками. При этом серверы на технологических площадах ничего «не знают» о том, как на самом деле распределены между ними данные – они работают с единым хранилищем. Это значительно упрощает разработку логики поведения в чрезвычайных ситуациях. Уже не нужно создавать сложные алгоритмы, определяющие приоритетность устройств хранения в том или ином случае, – система хранения только одна и вся логика ее работы «зашита» внутри ее ПО.

Тот факт, что ресурсы на самом деле распределены между двумя технологическими площадками, не оказывает влияния на работу ЦОДа. При выходе из строя любого из серверов на любой из технологических площадок инициируется стандартная процедура обработки сервиса высокой доступности VMware Infrastructure – все виртуальные машины перезапускаются на доступных серверах. В случае выхода из строя всех серверов на одной из технологических площадок виртуальные машины перезапускаются на другой технологической площадке до тех пор, пока там есть свободные вычислительные ресурсы. Поддержание свободных вычислительных ресурсов – задача администратора. При этом различные виртуальные машины имеют различный приоритет, и тем обеспечивается очередность: наиболее важные для бизнеса сервисы будут «подниматься» в первую очередь, а второстепенные – во вторую.

В случае катастрофы на системе хранения мы имеем зеркально реплицированные данные на другой технологической площадке и серверы «не заметят», что одна половина зеркала перестала функционировать. С их точки зрения работа будет продолжаться как и прежде.

Если выйдет из строя технологическая площадка целиком (все серверы и часть системы хранения, расположенные на одной площадке, перестанут нормально функционировать), останутся серверы и зеркальные данные на резервной площадке. Все ИТ-сервисы могут быть быстро запущены на ней по нажатию клавиши администратора системы.

Таким образом, динамический виртуализованный ЦОД, основанный на NetApp MetroCluster и VMware Infrastructure, предоставляет все преимущества, которые дают виртуализация и консолидация ИТ-ресурсов. Он обеспечивает катастрофоустойчивость и, в отличие от стандартных кластерных решений на базе двух отдельных систем хранения, сохраняет простоту настройки и эксплуатации. ИКС

Цена вопроса

Бухгалтерия дата-центра

Во что обойдется строительство ЦОДа и какую прибыль он может принести?

Андрей ПАВЛОВ,
генеральный директор,
«Датадом»

Строительство дата-центра – задача многофакторная, и его стоимость сильно зависит от исходных условий. Первое из них – это требование заказчика к надежности ЦОДа и, соответственно, к его архитектуре. Современная типовая архитектура коммерческого ЦОДа предполагает установку охлаждаемых воздухом монтажных шкафов с энергопотреблением 4–6 кВт. В таком дата-центре на одну стойку приходится 2–2,5 м^2 площади технозоны, включая оборудование систем холодоснабжения и бесперебойного питания, а энергопотребление всех инженерных подсистем и вычислительной техники составляет 3–4 кВт/м^2. Если же в монтажный шкаф установить оборудование, потребляющее более 6–7 кВт, то типовая технология охлаждения из-под фальшпола будет не применима, придется использовать водоохлаждаемые стойки, тепловые доводчики и т.д.

Для высококритичных данных может потребоваться 100%-ное резервирование всех инженерных подсистем ЦОДа по схеме N + N. При более низких требованиях к надежности возможно использование схемы резервирования N + 1. В каждом конкретном случае цена проекта будет своей: для ЦОДа типовой архитектуры со схемой резервирования N + 1 ориентировочная цена составит $10–12 тыс. за 1 м^2 технозоны, или $20–25 тыс. за стойку.

Еще один фактор, влияющий на стоимость строительства ЦОДа,– это наличие на объекте достаточного количества электроэнергии. Если заказчик вынужден покупать электроэнергию по ее полной продажной стоимости, то в Москве каждый киловатт ему обойдется примерно в $3 тыс. Для дата-центра с общим энергопотреблением 1 МВт только за получение технических условий и разрешения на подключение (фактически за бумагу!) придется отдать порядка $3 млн. Так как ЦОД мощностью 1 МВт располагается на площади около 350 м^2, то стоимость типового решения может увеличиться с $10 тыс. до $20 тыс. за 1 м^2.

Сильно влияют на стоимость проекта и технические особенности размещения внешних блоков системы кондиционирования и дизель-генераторов, а также удаленность транс-

форматорной подстанции, к которой необходимо произвести подключение.

Сегодня стоимость аренды стойки составляет $2–2,5 тыс. в месяц, а полная стоимость ее эксплуатации – около $700, т.е. бизнес-модель, подразумевающая предоставление услуги colocation, позволяет ежемесячно получать с одной стойки до $1,8 тыс. прибыли без вычета налогов. Теперь можно рассчитать срок окупаемости ЦОДа типовой архитектуры в пессимистичном варианте: капитальные вложения на 1 стойку ($25 тыс.) делим на ежемесячную прибыль ($1 тыс.), получаем 25 месяцев с начала коммерческой эксплуатации, т.е. два года. В случае покупки электромощностей срок окупаемости увеличивается почти в 2 раза.

Однако мы рассмотрели бизнес-модель предоставления услуги самого низкого уровня. При оказании услуг хостинга, dedicated, remote hands и т.д. эксплуатационные расходы вырастут, но и прибыльность ЦОДа значительно повысится. ИКС

ЦОДы: особенности российской экономии

Конечно, создавая ЦОД, всегда хочется получить решение «числом побольше, ценою подешевле». Но где проходит грань разумной экономии?

Михаил МИГУНОВ,
главный конструктор,
Computer Mechanics

Когда речь заходит о российской специфике построения дата-центров, на ум почему-то приходят в основном негативные примеры. Так, проектирование нового ЦОДа одной достаточно крупной структуры было начато с утверждения строительного плана реконструкции здания. То есть утверждение архитектурного решения, строительных планов, работ и смет, включая отделку, инженерные системы и энергетику, предшествовало проектированию собственно ИТ-инфраструктуры, анализу и аудиту задач, выбору платформ реализации. Каково?! Тут уж, видимо, не до рассуждений о SOA.

Естественно, хороший заказчик должен экономить бюджет, а хороший системный интегратор всячески ему в этом содействовать. Но экономия должна быть осознанной и разумной. Есть некоторый минимум вложений, который делает проект реализуемым. Ниже этого уровня снизить затраты не удастся, задача не будет решена. К сожалению, заказчики иногда допускают типичную ошибку, настаивая по бюджетным соображениям на исключении некоторого элемента инфраструктуры целиком, вместо того чтобы ограничить текущий масштаб этого и других элементов для соответствия бюджету.

Сформулируем так: при корректировке бюджета допустимы любые «урезания смет», если они не нарушают архитектуру решения, не снижают возможностей масштабирования и развития инфраструктуры. Такая рачительность даже полезна, правильное решение всегда можно дооснастить со временем, избегая высоких первоначальных затрат. В противном же случае теряется сам смысл проектирования. ИКС

ПОДРОБНОСТИ

Три кита надежности ЦОДа

Многим известны уровни надежности ЦОДов, так называемые Tier I, II, III и IV, каждому из которых соответствуют свои коэффициенты готовности инженерных систем со своим количеством «девяток». Опираются эти «девятки» надежности дата-центра на трех китов.

Алексей СОЛОДОВНИКОВ,
директор департамента по работе с корпоративными заказчиками, APC by Schneider Electric

«Железо»

Первый – это качественное оборудование, которое служит не ломаясь, с заданным временем наработки на отказ. С этим сегодня проблем нет: есть немало производителей надежного инженерного оборудования для дата-центров, к коим без ложной скромности можно причислить и компанию APC.

Проектирование

Но чтобы обеспечить тот или иной уровень надежности ЦОДа, нужно его вначале грамотно спроектировать. Это второй «кит», и с ним пока есть проблемы. Строительство ЦОДов в России переживает сейчас тот период, который обычная строительная индустрия пережила лет пять назад. Тогда при создании офисных и элитных жилых комплексов много внимания

уделялось отделке, в отличие от инженерных систем. В результате инвестор получал на выходе совсем не то, во что он вкладывал деньги первоначально: например, офисный комплекс класса не «А+», а «В-», который предполагает существенно более низкую арендную плату. И это только из-за того, что не было выполнено полноценное проектирование, требующее по мировым стандартам 5–7% финансирования проекта в целом. Правда, с тех пор многие застройщики поняли, что такая экономия выходит боком, и теперь до начала строительства нанимают консультантов, выполняют проектирование и вкладывают в него серьезные средства.

С дата-центрами, к сожалению, ситуация иная. Многие наши российские заказчики искренне считают, что девять беременных женщин могут за месяц родить одного ребенка. По мировым нормам нужно сначала выделить полгода на проектирование и лишь после этого начинать закупку оборудования, строительство и т.д. Нет, мы сначала размещаем заказы на оборудование и только после этого ищем людей, которые бы все это быстренько «запроектировали». О затратах на проектирование в размере 5–7% стоимости ЦОДа речь вообще не идет: «Да вы что?! 0,5% за глаза хватит! А что там, собственно, проектировать-то? И так все понятно с системами бесперебойного питания и кондиционированием». Конечно, время – деньги, но без некоторых вещей обойтись нельзя, иначе в итоге рождается то, что работает, мягко говоря, не так, как планировалось, или не работает вовсе.

Проблема еще и в том, что у нас мало организаций, имеющих опыт проектирования современных дата-центров, особенно с учетом изменений в инженерных системах, которые произошли за последние 5–7 лет. У традиционных проектировщиков этого опыта просто нет, но кое-какой опыт есть у инжиниринговых компаний и крупных системных интеграторов, у которых за последние годы появились инженерные отделы, занимающиеся проектированием и строительством дата-центров. А без опыта вышеупомянутых «девяток» надежности ЦОДа достичь нельзя. Мало того, рядом с каждым проектировщиком надо сажать по опытному «эксплуататору», ибо проектировщик, даже идеально владеющий теоретической базой, часто не до конца понимает, как его проектные решения будут выглядеть в процессе эксплуатации.

Человеческий фактор

И тут мы подходим к третьему «киту» надежности ЦОДа, а именно к роли человеческого фактора в процессе эксплуатации, а также к наличию (или отсутствию) в дата-центре систем автоматики, которые в критических ситуациях способны принять за оператора единственно правильное решение. Грамотный, обученный персонал, натренированный на отработку нештатных ситуаций, может повысить характеристики дата-центра и сократить среднее время простоя, соответствующее «официальному» уровню ЦОДа, а неграмотные действия службы эксплуатации могут запросто этот уровень опустить. Например, для дата-центра категории Tier III допустимое суммарное время простоя составляет 1,6 часа в год, и тем не менее есть площадки уровня Tier III, которые работают по пять лет без единого сбоя, и это заслуга службы эксплуатации. Нередко крупные западные хостинговые дата-центры проводят профилактические работы чаще, чем рекомендуют поставщики оборудования. Например, батареи ИБП рекомендуется «прозванивать» раз в год, а они делают это дважды в год. Включают резервный дизель-генератор и гоняют его под нагрузкой не раз в полгода, а каждые два-три месяца. Более того, они каждый месяц меняют солярку в баках, потому что при долгом хранении она портится. Есть еще масса вещей, которые надо делать в процессе эксплуатации, чтобы в нужный момент резервное оборудование сработало так, как положено.

В России уже есть компании с большим опытом и грамотной службой эксплуатации именно современных ЦОДов, а не ведомственных машинных залов времен ЕС ЭВМ. Со временем таких профессионалов должно стать больше, а пока самый правильный путь – это использование имеющегося опыта западных компаний, изучение лучших мировых практик и привлечение экспертов наподобие Uptime Institute. Кстати, некоторые российские компании, которые собираются в обозримом будущем строить дата-центры, уже общаются с Uptime Institute и готовы привлекать его специалистов в качестве консультантов для своих проектов. Надеюсь, что это произойдет в ближайшие полгода-год. ИКС

Российские особенности
эксплуатации дата-центров

Обращаясь к услугам коммерческих дата-центров, компании избавляются от необходимости дорогостоящего строительства собственного ЦОДа, а также от немалых расходов и проблем, связанных с его эксплуатацией. Это правильно, поскольку эксплуатация такого сложного объекта, как дата-центр, требует не только финансовых затрат, но и определенных знаний и опыта.

Павел ЗЕЛЕНСКИЙ,
системный архитектор,
«Инфосистемы Джет»

В процессе эксплуатации заказчик может столкнуться с проблемами, решение которых могут предложить только профессионалы.

Зачастую при проектировании объекта заказчик из соображений экономии не включает ряд вспомогательных систем, например систем мониторинга и автоматического управления. Это, по-моему, самая серьезная ошибка при строительстве ЦОДа. Обычно через два-три года работы он убеждается в их необходимости, но происходит это после неоднократных сбоев и аварий.

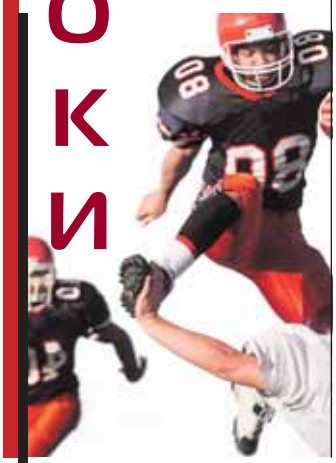
Некоторые недочеты не очень критичны, и их можно устранить с помощью организационных мер. Например, в наших, российских, условиях внешние блоки кондиционеров требуют периодического и сезонного обслуживания. Но иногда они очень неудобно расположены. Не так давно произошла аварийная остановка одного дата-центра. Система охлаждения не справлялась с отводом тепла на улицу – радиаторы кондиционеров оказались забиты тополиным пухом из-за того, что не была предусмотрена возможность быстрой очистки фильтров.

При выборе технического решения необходимо учитывать и особенности российского климата. Далеко не все технологии, которые подходят для более теплых стран, могут применяться у нас без серьезной адаптации. Например, системы кондиционирования, где в качестве теплоносителя используется жидкость, в США могут спокойно стоять на улице круглый год. Но в России, где зимой морозы достигают –30...–40°C, для обеспечения функционирования таких систем нужно либо устанавливать теплообменники внутри помещения, где поддерживается определенная температура, либо разрабатывать системы подогрева теплоносителя.

Нередко многие проблемы в работе дата-центров связаны с неправильно организованным процессом их эксплуатации. Существует ряд методологий, например ITIL, где описаны принципы эффективной организации службы эксплуатации дата-центров. Но даже если процессы эксплуатации инфраструктуры ЦОДа и администрирования информационных систем выстроены с применением лучшего опыта, нельзя исключать влияние человеческого фактора на функционирование центра обработки данных из-за его непредсказуемости. Для того чтобы исключить такие проблемы, необходимо на этапе проектирования и внедрения учитывать специфику эксплуатации и не откладывать на потом внедрение систем и организационных мер, нацеленных на построение качественной службы эксплуатации. ИКС

Дороги, ведущие к ЦОДам

Экономика все больше переходит на информационные рельсы, и дата-центры становятся основой существования и бизнеса. Но сколько существует видов бизнеса, столько и путей достижения заветной цели в виде ЦОДа.



Плохая погода – это счастье для ЦОДа

Марина НИКЕРОВА,
управляющий группой компаний .masterhost

На рынке услуг дата-центров мы работаем почти восемь лет, начав с аренды площадей в чужих ЦОДах. Сейчас мы арендуем площади в пяти ЦОДах, причем сами обслуживаем свое оборудование и заботимся о том, чтобы оно нормально работало. Обычно летом все мечтают о хорошей погоде, а мы хотим плохой, потому что в жару дата-центры перегреваются и начинаются сбои в работе. На что только не приходилось идти, чтобы снизить температуру в машинном зале! Ставили дополнительные кондиционеры, разбрасывали сухой лед, пригоняли пожарную машину и поливали крышу водой из шланга. За эти годы у нас накопился большой опыт, и теперь мы знаем, какие просчеты допускают проектировщики и строители ЦОДов, какое нужно устанавливать оборудование, какие должны быть системы электропитания, кондиционеры, серверные стойки и т.д.

И мы поняли, что гораздо выгоднее, удобнее и надежнее иметь собственный ЦОД, и решили его построить.

Мы долго искали объект, который удовлетворял бы всем необходимым условиям: наличие достаточного количества электрических мощностей, как минимум два электрических ввода в здание, возможность установить альтернативный источник электроэнергии и протянуть качественные оптоволоконные линии связи с резервированием от разных операторов. Наконец на одном из объектов на севере Москвы все совпало.

Для выбора проектировщиков и поставщиков отдельных подсистем ЦОДа мы проводили закрытые тендеры (закрытые, потому что старались до последнего момента скрыть свои намерения, чтобы не увели объект). Проекты выбирали не по цене (заявленные цены были примерно одинаковые), а по качеству и надежности решений.

Сейчас строительство нашего ЦОДа уже заканчивается. В нем два зала общей площадью 1500 м^2. Суммарная электрическая мощность составляет 9 МВт, она будет вводиться в строй в две очереди по 4,5 МВт каждая. Электроэнергия подводится от трех разных источников, а на случай их отключения есть газогенераторная станция. Подаваемая на каждую стойку электрическая мощность рассчитана с запасом, есть запас и у системы кондиционирования. Вводы в здание оптоволоконных кабелей сделаны с четырех разных сторон, так что даже три лихих экскаваторщика не смогут отрезать наш ЦОД от внешнего мира. Поначалу общая пропускная способность каналов связи составит 10 Гбит/с, а к концу 2008 г. мы увеличим ее до 20 Гбит/с.

Сейчас, будучи арендаторами мощностей дата-центров, мы не можем заключать с нашими клиентами настоящий договор об уровне обслуживания. Пока мы подписываем договор на размещение оборудования клиента, где гарантируется только круглосуточный доступ к его интернет-ресурсу по каналу с определенной полосой пропускания, так как это входит в нашу зону ответственности. Никаких параметров качества электропитания и охлаждения в договоре не указывается, поскольку мы сами таких гарантий от владельцев ЦОДов не имеем. Но в нашем новом ЦОДе именно мы будем отвечать за электричество и охлаждение, и мы обязательно будем подписывать с клиентами договор, где все это будет регламентировано.

За восемь лет мы наэксплуатировали немало дата-центров и теперь постараемся учесть весь свой опыт, чтобы наш ЦОД был по-настоящему сервисным. Надеемся, что в начале осени мы сможем перерезать ленточку и войти в наш ЦОД уже вместе с клиентами.

Три точки опоры
Stack Data Network

Сергей ЛЫСАКОВ,
генеральный директор,
Stack Group

Сеть коммерческих дата-центров Stack Data Network (SDN), которую Stack Group развивает с 2004 г., сегодня охватывает три территориально распределенных узла, объединенных в кольцо резервированными оптическими каналами связи. Два из них расположены в разных концах Москвы, а третий, резервный, вынесен за 100 км от МКАД. По состоянию на июль 2008 г. – времени ввода в эксплуатацию третьей очереди Stack M1 – общая площадь SDN превышает 5000 м^2. Здесь расположены серверные залы на 800 стоек, оснащенные в соответствии с требованиями Tier III+, и аналогичные им по отказоустойчивости помещения резервных офисов клиентов.

Хотя жизненный цикл действующих дата-центров SDN рассчитан на 10 лет, уже инициирован процесс предпроектной подготовки новых площадок в Подмосковье, Поволжье, Северо-Западном регионе России, а также в странах ближнего зарубежья. Качественные изменения претерпевает и пакет услуг: если в 2004 г. Stack предлагал физическим лицам и организациям только услуги colocation и dedicated, то сегодня в SDN все бóльшим спросом пользуются консалтинг по вопросам оптимизации затрат на аутсорсинг инфраструктуры дата-центра, а также полное техническое сопровождение отказоустойчивых резервных офисов.

Свой ЦОД
сделали для себя

Константин ЗВЕРЕВ,
директор по информационным технологиям, «ЦентрТелеком»

Наш центр обработки данных создавался прежде всего для решения внутренних задач компании, для консолидации и централизации автоматизированных систем расчетов с абонентами, систем управления предприятием и других корпоративных информационных ресурсов.

Строить свой ЦОД мы начали в 2005 г. Расположен он в Московской области. Основными критериями выбора площадки были наличие свободных технологических площадей, пригодных для размещения оборудования, наличие незадействованных электрических мощностей и каналов связи достаточной пропускной способности. Подрядчика для проектирования и строительства дата-центра выбирали на конкурсной основе, учитывая опыт компании по проектированию и строительству ЦОДов, наличие необходимых лицензий и стоимость предлагаемого решения. Ожидания в целом оправдались, так что своим выбором мы довольны.

Общая площадь серверных помещений в нашем ЦОДе около 300 м^2, подведенная электрическая мощность – 1 МВт (1-я категория электроснабжения). ЦОД оснащен дизель-генератором, источниками бесперебойного электропитания, системами кондиционирования, газового пожаротушения и т.п. Информационная безопасность нашего дата-центра обеспечивается межсетевыми экранами, системами обнаружения и предотвращения вторжений, антиспама и антивирусной защиты, каналы связи защищаются с помощью VPN.

Прибыли как таковой наш ЦОД не дает, но позволяет сэкономить на затратах, поскольку централизованные информационные системы при обслуживании требуют меньше квалифицированного персонала и аппаратных ресурсов, чем децентрализованные.

«Караван» движется к выделенным дата-центрам

Андрей КАСЬЯНЕНКО,
генеральный директор, «Караван»

Услуги виртуального и физического хостинга на базе собственного дата-центра «Караван» предоставляет более 11 лет, а в начале июня мы открыли новую площадку Telehouse Caravan на северной окраине столицы. Во введенной в строй первой очереди дата-центра имеется 6 гермозон на 19 стоек каждая (общая площадь– более 1000 м^2), а всего в ЦОДе будет 12 независимых друг от друга гермозон, оснащенных всеми необходимыми системами жизнеобеспечения, отказоустойчивости и безопасности. К каждой из двух очередей подведена электрическая мощность 1 МВт. Максимальная выделяемая мощность на одну стойку – 30 кВт. По стандарту TIA-942 Telehouse соответствует уровню Tier III+. Опорная сеть имеет многократное резервирование, суммарная пропускная способность межоператорских присоединений превышает 10 Гбит/с. Инвестиции в строительство первой очереди Telehouse составили около $7 млн.

Telehouse Caravan предоставляет услуги colocation, аренду места в стойке и стойки целиком, размещение серверного оборудования и аппаратно-программных комплексов заказчиков. Мы также предлагаем новую для российского рынка услугу аренды выделенного дата-центра, т.е. логически завершенной безопасной площадки для размещения ИТ-инфраструктуры компании.

Основные потребители услуг Telehouse – корпоративные пользователи, телекоммуникационные операторы, контент-провайдеры и сети по доставке контента (CDN), разработчики сервисного ПО, компании финансово-банковского сектора.

ISG пойдет в розницу

Дмитрий КАЛГАНОВ,
директор по производству управления инфраструктуры, ISG

Услуги ЦОДа ISG предоставляет с 2007 г. Для проектирования и создания дата-центра мы объявили конкурс, который выиграла компания «Дата Дом». Инженерная часть ЦОДа рассчитана на подсоединение нагрузки более 2 МВт (1-я категория электроснабжения). Общая полезная площадь модулей гермозоны – 500 м^2, что позволяет разместить более 200 серверных шкафов. Дата-центр имеет собственные ВОЛС до основных московских узлов связи ММТС-9 и ММТС-10. В соответствии с международной классификацией наш ЦОД относится к 3-му уровню надежности (Tier III).

С момента открытия дата-центра мы работали в основном с оптовыми клиентами, предоставляющими услуги хостинга преимущественно для юридических лиц. Им мы сдаем в аренду серверные шкафы и размещаем их оборудование. Эта услуга настолько востребована, что уже через три месяца после открытия ЦОДа нам пришлось отказывать новым клиентам. Чтобы развиваться в условиях недостатка свободных площадей, обеспеченных энергоресурсами, мы собираемся предлагать услуги, связанные с организацией ИТ-сервисов, и выходить на рынок розничных клиентов, которым требуется поддержка операционных систем и приложений.

BCC: наш конек – тяжелые ЦОДы для телекома

Компания BCC имеет опыт создания корпоративных дата-центров для самых разных заказчиков, но своей специализацией считает ЦОДы для телекоммуникационных операторов. Об особенностях работы на рынке дата-центров рассказывает руководитель отдела развития бизнеса BCC Кирилл МИХЕЕВ.

Кирилл МИХЕЕВ

– В чем причина столь значительного спроса на ЦОДы со стороны телекомов?

– Да, этот спрос действительно очень велик и, пожалуй, соизмерим с интересом к ЦОДам во всех остальных «вертикалях», вместе взятых. Причины вполне понятны. Рынок телекоммуникаций – это один из немногих в России высококонкурентных рынков, рынков покупателя. И, как ни банально это звучит, для успеха на нем операторам необходимо предоставлять миллионам абонентов услуги высокого качества, постоянно адаптируя свой продуктовый портфель к изменению спроса. Для этого требуется гибкая, масштабируемая, обеспечивающая высокую степень готовности инфраструктура, одним из ключевых элементов которой является ЦОД. Кроме того, подавляющее большинство операторов связи – это публичные компании, бумаги которых торгуются на бирже. А любая публичная компания должна быть эффективной, иначе снижается ее капитализация, увеличивается стоимость привлечения заемных средств. И поскольку возможности повышения цен на услуги практически отсутствуют, то единственный выход – это снижение издержек. А большие ЦОДы, несмотря на свою высокую стоимость, в сочетании с полноценным использованием технологий виртуализации как раз позволяют весьма существенно снизить операционные издержки оператора и при этом обеспечить высокое качество предоставления услуг.

– Есть ли какие-то особенности у дата-центров для телекоммуникационных компаний?

– Основная нагрузка ЦОДа оператора – это биллинг, или обсчет транзакций. При этом дата-центр должен иметь высокий уровень готовности, что требует построения масштабных катастрофоустойчивых решений с применением кластеров высокой доступности на базе мощных RISC/EPIC-серверов или большого количества серверов стандартной архитектуры. Для коммерческих ЦОДов, используемых операторами для предоставления услуг аутсорсинга, крайне важным аспектом является виртуализация, т.е. возможность исполнения разнородных приложений на одном сервере. Энергопотребление больших операторских ЦОДов может достигать нескольких мегаватт, что в условиях нынешних практически заградительных тарифов на подключение к электросетям (например, в Москве – до $2 млн за 1 МВт) требует от нас максимального использования энергосберегающих технологий и искусства оптимизации при проектировании и строительстве инженерных систем. Весьма сложны такие задачи, как, скажем, отвод тепла, обеспечение электропитания в наших перегруженных сетях, обеспечение технической и информационной безопасности и многие другие.

– Как BCC строит свою работу над проектом?

– Мы считаем, что при проектировании дата-центра надо отталкиваться от бизнес-процессов компании и затем спускаться вниз по пирамиде ИТ-системы через прикладное ПО, вычислительную и телекоммуникационную инфраструктуру к инженерной инфраструктуре и капитальному строительству. Многие заказчики уже оценили этот комплексный подход, поскольку практически каждая динамично развивающаяся компания стремится перейти от «лоскутной» интеграции к проактивному развитию ИТ-инфраструктуры на основе единых принципов. В полной мере это относится к тем решениям, которые предполагают встраивание нового ЦОДа в уже имеющуюся у компании сеть дата-центров. Некоторые такие проекты, выполненные BCC, можно назвать просто уникальными.

– Какие проекты BCC для телекоммуникационных компаний вам хотелось бы отметить?

– К наиболее значимым проектам последних лет я бы отнес дата-центры для биллинга автоматизированной системы расчетов «Курс» Южной телекоммуникационной компании, ЦОД для компании «Уралсвязьинформ» – АСР PETER-SERVICE BIS, ЦОД для «ЦентрТелекома» в Московской области и проекты построения региональных дата-центров в Северо-Западном федеральном округе для МТС и «МегаФона».

– Есть ли у BCC решения для небольших операторов?

– У нас нет жестких ограничений по размеру клиентов и объему проектов. Мы готовы собрать и небольшой ЦОД из набора компонентов, в которых используются общие наработки ранее выполненных проектов, а клиент сам может решить, какое решение для него наиболее приемлемо. Характеристики дата-центра определяются на основе экспресс-анкетирования заказчика. Такой ЦОД очень компактен и экономичен, для его электропитания достаточно кабельной сети обычного офисного здания, а кроме того, он не требует специальной подготовки помещений. В этом случае наши временные и финансовые затраты на проектирование сведены к минимуму, поэтому клиент может приобрести такой ЦОД «из коробки» в сжатые сроки и с немалой экономией средств.

«Синтерра» размером 40 x 40

Когда в сентябре 2007 г. компания «Синтерра» анонсировала программу «40 x 40» по созданию национальной сети коммерческих ЦОДов, аналитики и специалисты отнеслись к ней скептически, говоря, что спрос на такого рода услуги в регионах невелик.

Но за прошедшее время тенденции середины 2007 г. превратились в мощные процессы, связанные с сокращением электронного неравенства между центром и регионами. Развитие информатизации регионов привело к росту потребности в услугах ЦОДов. Стало ясно, что ЦОДодвижение в регионы фактически неизбежно.

Программа «40 x 40» – это строительство в 40 городах России дата-центров, имеющих подключение к национальной магистральной сети «Синтерры» с суммарной скоростью 40 Гбит/с (ширина полосы магистральной сети компании составляет 10 Гбит/с, но в каждом ЦОДе пересекаются два кольца этой сети, так что два входа и два выхода дают в итоге 40 Гбит/с). Даже разработчики программы поначалу считали, что полоса пропускания заявлена с большим запасом, но спрос на «тяжелый» контент растет настолько быстро, что 10 Гбит/с рискуют скоро стать общеотраслевым стандартом. 40 городов для реализации проекта были выбраны на основе оценки потребности в услугах ЦОДов и динамики процесса информатизации в каждом регионе. Также учитывались численность населения и необходимость присутствия дата-центров «Синтерры» во всех федеральных округах России.

Электричество – основа всего

Работы по программе «40 x 40» начались с поиска подходящих помещений, соответствующих всем международным требованиям, предъявляемым к дата-центрам (допустимая нагрузка на пол, определенная высота потолков, возможность расширения и модернизации и т.д.). Одно из самых сложных в российских условиях требований – наличие в здании необходимых электрических мощностей. Под это условие решено было скорректировать бизнес-план всего проекта, поскольку поначалу «Синтерра» рассчитывала главным образом на долгосрочную (15–20 лет) аренду помещений. Как оказалось, «хорошее энергоснабжение» – понятие относительное: потребности оборудования в электричестве постоянно растут, а увеличивать мощность энерговвода в здание проще, являясь его владельцем. Поэтому теперь 95% помещений региональных ЦОДов выкуплены компанией. Однако это несильно повлияло на ранее утвержденный план ввода дата-центров в эксплуатацию. Первая очередь центрального московского ЦОДа уже работает, в июле состоялся запуск дата-центров в Томске и Ставрополе, в сентябре планируется ввести в строй ЦОДы в Казани и Новосибирске.

Не мешай жить другим – и сам будешь в прибыли

Именно такова политика «Синтерры». Очень сложно (и даже практически невозможно) сесть разом на все стулья и «съесть» весь рынок. На этом потерпели фиаско многие некогда большие и могущественные компании. На рынке ЦОДов «Синтерра» выбрала позицию, которая по международной терминологии называется «оператор сервисов нового поколения». Это оператор, который имеет свою магистральную сеть и на базе этой сети и компьютерных мощностей ЦОДа предоставляет услуги поставщикам и агрегаторам контента, операторам связи, хостинг-провайдерам, интеграторам и поставщикам онлайновых программных приложений. Размещение информационных ресурсов в ЦОДах по всей территории России решает важнейший вопрос децентрализации контента, за которым до сих пор все ходят в Москву. Но постоянно «гонять» трафик из Москвы в регионы дорого, и «Синтерра» со своими ЦОДами создала все условия для приближения контента к клиенту. И самое главное – регионы к потреблению этого контента готовы.

«Синтерра» всячески подчеркивает, что в регионах компания не конкурирует с операторами местного доступа и не отбирает хлеб у провайдеров «последней мили». Все вышеуказанные участники «пищевой цепочки», в которую еще стоит включить конечных пользователей, хотят «есть». «Синтерра» предоставляет широкополосный доступ к множеству услуг, оставляя местным провайдерам весь комплекс работ по обслуживанию и развитию их собственной клиентской базы. В отличие от Москвы, где места в коммерческих ЦОДах скупаются на этапе строительства и многие ИТ-проблемы успешно решены, в регионах ситуация иная – ИТ-сервисы «навязчивыми» назвать там нельзя. Поэтому местным заказчикам «Синтерра» предлагает не только телекоммуникационные (дальняя связь, аренда междугородных каналов, услуги на базе сети IP-MPLS, доступ в Интернет, распределенный call-центр, хостинг, colocation и пр.), но и контентно-ориентированные услуги. В частности, в Томске и Ставрополе партнерами «Синтерры» стали Microsoft и хостинг-провайдер Infobox, предложившие проект аренды программного обеспечения «ПО как услуга». Это проект нацелен на компании, которые не хотят или не могут себе позволить единовременно заплатить немалые деньги за ПО. Такая аренда требует широкополосного доступа, что как раз и может предоставить «Синтерра». Позиция компании – не конкуренция, а создание новых возможностей для развития бизнеса всех участников рынка телекоммуникаций.

www.synterra.ru

ракурс

Как хранить ценности

Владимир ИВАНОВ,
консультант Cisco Systems

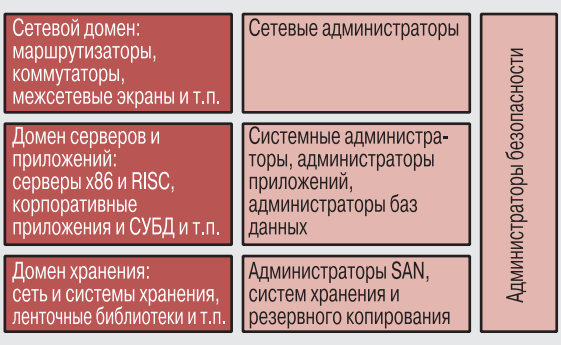
Центр обработки данных – информационное сердце компании: вся информация, которую она хранит и использует, находится именно здесь. Естественно, защита этой ценности должна занимать (и занимает) одну из верхних позиций в списке приоритетов предприятия.

В центре обработки данных принято выделять три инфраструктурные области (домена) – локальной сети, серверов и приложений, хранения (рис. 1). Это разделение влияет не только на проектные решения, принимаемые при создании элементов инфраструктуры, но и на организацию оперативного управления, на административное деление команды ИТ-специалистов, на сферы подчинения и т.п. Вместе с тем информационную безопасность (ИБ) должен обеспечивать комплекс мер, применяемых во всех доменах.

Центр требует централизации

Очевидно, что адекватная информационная защита мультидоменной структуры возможна лишь при выведении службы обеспечения безопасности из структуры общего управления сетью и ее размещении «над» доменами управления. Разумеется, при этом необходимо так разграничить полномочия между администраторами каждого из доменов и службой ИБ, чтобы каждая группа могла выполнять свои обязанности, не мешая другим. Следовательно, системы защиты дата-центров должны поддерживать ролевое управление правами и централизованные средства аутентификации и авторизации.

Рис. 1. Инфраструктура ЦОДа



К настройке элементов инфраструктуры ЦОДа могут иметь доступ разные сотрудники, но при поиске неисправностей или проведении расследований важно знать, кто и когда вносил изменения в конфигурацию. Другими словами, все подсистемы дата-центра должны поддерживать механизмы централизованного учета событий. Для организации оперативного управления важно, чтобы сообщения о действиях администраторов полностью журналировались. Причем журналы событий (системных и связанных с обеспечением безопасности) тоже должны храниться централизованно, чтобы упростить мониторинг и оценку состояния защищенности ЦОДа. Но данные этих журналов будут полезны только в случае, если гарантирована их целостность и полнота.

Другой важный аспект анализа защищенности – возможность корреляции событий, порожденных отдельными системами, которая помогает выявлять скрытые связи между ними. Данные журналов событий должны передаваться в режиме реального времени во внешнюю систему, обеспечивающую их нормализацию (приведение к единому виду), обработку и долговременное хранение. Сроки хранения таких журналов, как правило, определяются внутренним регламентом предприятия, нормативными документами государственных или отраслевых регуляторов. В зависимости от принципов организации управления ИТ, принятых в компании, система консолидированного хранения журналов может находиться в ведении службы информационной безопасности или внутреннего аудита.

Эти компоненты – базовые для любого проекта, связанного с инфраструктурой защиты ЦОДа. Только при наличии централизованных систем аутентификации, авторизации и учета можно переходить к созданию собственно инфраструктуры обеспечения безопасности.

Защитная инфраструктура сети

Конечно, подсистема защиты ЦОДа – не «вещь в себе». Более того, на последней конференции RSA Security было провозглашено, что единичные защитные решения, не являющиеся частью общей информационной системы компании, обречены на вымирание. Подобно тому как производители тормозных систем предлагают свою продукцию не конечному пользователю, а автомобильным концернам, поставщики инфраструктурных ИТ-решений должны включать механизмы обеспечения ИБ в стандартную сетевую или серверную архитектуру, в компоненты систем и сетей хранения, в корпоративные приложения.

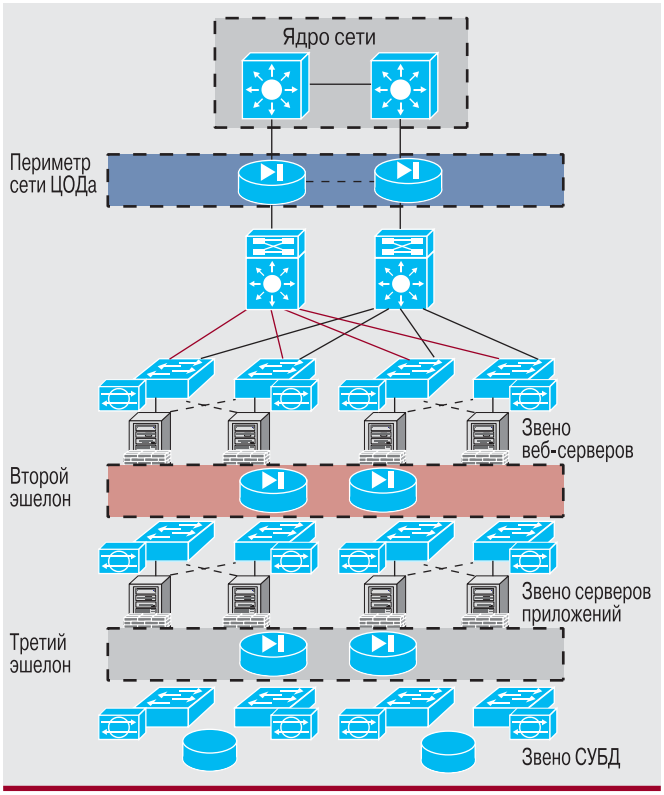
Какой должна быть инфраструктура ЦОДа, способная поддерживать требуемый уровень безопасности? Современная концепция предусматривает использование ряда подсистем защиты, в которых учитываются особенности архитектуры сети передачи данных, серверной фермы и сети хранения, все требования обеспечения ИБ с помощью настроек оборудования и ПО, а также принципы централизованного оперативного управления ИБ.

Эшелонированная сетевая оборона

Методически принято различать ЦОДы, обслуживающие внутренних пользователей (через корпоративную сеть) и внешних (через публичные сети), но с точки зрения защиты их проблемы и решения весьма сходны. При этом во «внутреннем» ЦОДе вероятность атаки на внутренние приложения ниже, чем во «внешнем», а возможный ущерб больше.

В корпоративных веб-приложениях, построенных по принципу трехзвенной архитектуры (рис. 2), с пользователями, по идее, должны работать только серверы первого уровня – web front-end. На практике, однако, потребитель передает данные приложению, установленному на сервере второго уровня, и при недостаточно качественной фильтрации эти данные напрямую попадают в СУБД.

Рис. 2. Архитектура сети и уровни защищенности



При возникновении инцидента в области ИБ и ошибки в приложении, обрабатывающем данные пользователя, не исключено нарушение работоспособности сервера приложений или его захват. А если инцидент сопровождается атакой типа SQL Injection, код атакующего будет выполнен непосредственно на сервере баз данных. Это означает, что ***недоверенными*** следует считать не только трафик, поступающий непосредственно от пользователей к веб-серверам, но и сетевое взаимодействие между серверами.

Для организации глубокой эшелонированной защиты контроль и фильтрация сетевого трафика должны осуществляться как на внешнем периметре, так и между серверами ЦОДа. Трафик между серверами, как правило, ограничен строгими регламентами взаимодействия (параметры даже легитимного трафика пользователей могут иметь большой разброс вследствие различия интерфейсов приложений и версий ОС, местоположения потребителя в сети и т.д.), и их нарушение более подозрительно, чем изменение параметров пользовательского трафика.

В современных ИС серверный и пользовательский трафик может фильтроваться не только на межсетевых экранах, но и средствами коммутаторов, обеспечивающих поддержку списков доступа на портах или VLAN. В идеале фильтр нужно устанавливать максимально близко к источнику трафика, чтобы те пакеты, которые все равно будут отброшены на пути к получателю, не занимали полосу пропускания и ресурсы сетевого оборудования. Это означает: трафик, транспортируемый к отвечающим пользователям серверам, следует фильтровать на границе дата-центра, а трафик между серверами ЦОДа – на порту, к которому подключен сервер-источник. Фильтрация серверного трафика должна быть более жесткой, что вместе с ограниченностью числа протоколов внутри серверной фермы позволит сохранять строгий контроль над ним и наиболее полно использовать системы обнаружения и предотвращения вторжений (IDS/IPS). Разумеется, производительность этих систем необходимо подбирать с учетом предварительных оценок объемов трафика между приложениями.

Наконец, если сложность протокола не позволяет контролировать легитимность информационного обмена между клиентом и сервером, для обеспечения безопасности можно применять фильтрующие прокси-серверы прикладного уровня. Примером сложных, многоуровневых протоколов служит SOAP (Simple Object Access Protocol – простой протокол доступа к объектам). Согласно SOAP общение между сервером (или веб-сервисом) и клиентом происходит с помощью сообщений на основе XML (расширяемого языка разметки). В качестве транспорта для XML-сообщений обычно используется протокол HTTP или HTTPS.

Таким образом, для оценки корректности SOAP-взаимодействия контролирующая система должна:

- проанализировать IP-пакеты и TCP-сегменты, а если в качестве транспорта применяется протокол HTTPS, то выполнить терминирование SSL;
- собрать в памяти полный HTTP-запрос или ответ и проанализировать его на соответствие спецификации HTTP;

➔ проанализировать XML-документ на соответствие XML-схеме;

➔ проанализировать SOAP-сообщение на соответствие спецификации WSDL (языка описания веб-сервисов).

Такой алгоритм оценки делает потоковый (попакетный) анализ, при котором используются некоторые сетевые IDS/IPS-системы, затрудненным или нерациональным. Но контроль можно реализовать и на прикладном уровне, например с помощью промежуточного веб-сервера, который проверяет полностью принятый запрос и, при положительных результатах проверки, передает его «настоящему» веб-приложению. Выделенное устройство контроля над XML-сообщениями не занимается терминированием SSL-соединений или предотвращением вторжений на сетевом уровне, и такое разграничение ролей позволяет добиться высокой производительности.

Идеологически близкая задача – защита веб-приложений, напрямую «общающихся» с клиентом. По данным OWASP (Open Web Application Security Project), наиболее распространенные атаки на веб-приложения – это межсайтовый скриптинг, внедрение кода (например, SQL-инъекция) и неконтролируемое выполнение файлов. Для защиты от них можно использовать комплексы WAF (web application firewall), которые контролируют параметры, передаваемые пользователем с помощью запросов HTTP GET и POST. Параметры запросов, HTTP cookies и URL проверяются на предмет легитимности, отсутствия признаков атак (например, наличия в передаваемом параметре фрагмента SQL-запроса или сценария JavaScript), после чего запрос отправляется «настоящему» веб-серверу.

Средства индивидуальной защиты

Добиться полной защищенности приложений только сетевыми средствами сложно. Необходимо принимать дополнительные меры на уровне серверной операционной системы и установленных на сервере приложений.

Основные причины нарушения режима безопасности – наличие известных и новых уязвимостей ПО, использование небезопасных настроек «по умолчанию» и ошибки в настройке ПО. Как устранить две последние причины, понятно: следовать рекомендациям производителя и никогда не использовать настройки «по умолчанию».

Защититься ***от известных уязвимостей***, как правило, можно путем регулярного обновления операционных систем и приложений. Все основные поставщики ОС общего назначения включают в комплект поставки средства автоматического или автоматизированного обновления программного обеспечения. Однако зачастую темпы обновления корпоративного ПО (такого, как серверы приложений или СУБД) значительно отстают от рекомендуемых производителем.

Администраторы приложений аргументируют такое отставание необходимостью тестирования совместимости серверных компонентов. Чтобы процесс тестирования не ставил под удар безопасность ИС предприятия, необходимо тщательно отработать процедуры проверки обновлений и их установки на работающие системы. Поскольку ответственность за обеспечение безопасности систем возлагается на ИБ-администраторов, а тестировать приложения могут администраторы приложений и внутренние разработчики, имеет смысл ввести формальный процесс контроля над установкой обновлений.

Повысить уровень защищенности от ***неизвестных уязвимостей*** таким способом нельзя, но это можно сделать с помощью программной системы класса HIPS (host intrusion prevention system). Она контролирует системные вызовы, выполняемые приложением, и оценивает информационные потоки между приложениями. В системе HIPS всегда присутствует набор правил, описывающих нормальное поведение корпоративного приложения. Отклонения от этих правил считаются нарушением защиты. Даже если зловредный код, который привел к изменению работы приложения, неизвестен традиционному антивирусу, система его «вычислит». Набор правил-политик, описывающих нормальное функционирование приложений, поставляется производителем такой системы и может быть дополнен специалистами службы ИБ.

Когда сервер управления HIPS получает определенное число сходных уведомлений о подозрительной активности, он расценивает это как атаку неизвестного зловредного кода. Тогда сервер создает сигнатуру, позволяющую IPS предотвратить атаку на уровне периметра сети или ее сегмента.

Защита данных

В домене хранения основное внимание уделяется конфиденциальности данных, которая поддерживается за счет программных систем, работающих на серверах, либо за счет оборудования сети хранения. Основной способ обеспечения конфиденциальности – шифрование.

Наиболее остро стоит проблема ***шифрования резервных копий***, которые в рамках стратегии восстановления системы после катастроф должны быть вынесены с территории организации. Если ленточная библиотека подключена к сети хранения, то шифруется содержимое SCSI-команд в Fibre Channel-трафике, предназначенном для записи на ленту. Но разбор FC-фреймов и шифрование данных внутри команды требуют значительных вычислительных ресурсов. Эта задача обычно выполняется специализированным устройством – кроме тех случаев, когда резервная копия имеет относительно небольшой размер или время, выделенное на резервное копирование, позволяет выполнить шифрование программным способом.

При оперативном хранении данные также могут быть защищены с помощью специального драйвера файловой системы, дискового устройства либо специального устройства в сети хранения. Для инсталляций начального уровня чаще всего применяют программные решения, поскольку выполнение операций на центральных процессорах требует значительных ресурсов. Следует помнить, что при использовании программной криптографической защиты кластерных систем основными проблемами становятся управление ключами и поддержание единого расписания их применения в разных узлах кластера.

■ ■ ■

Защитить дата-центр только сетевым экраном не удастся. Современные угрозы намного сложнее тех, которые подвластны МСЭ. Снизить риски позволяют построение глубоко эшелонированной защиты, правильная организация процессов оперативного управления работой ЦОДа и обеспечение тесного взаимодействия сотрудников. ИКС