Linxdatacenter: "потеря данных - это потеря бизнеса"

Несмотря на то, что Россия, образно говоря, - это "страна операторских и корпоративных ЦОДов", аутсорсинговые проекты постепенно "пробивают" себе дорогу. Их не так много в абсолютных цифрах, но подобные проекты выигрывают за счет широкого спектра услуг и сетевой нейтральности, предоставляя клиентам выбор из десятков операторов связи для телекоммуникационных услуг. Кроме того, большинство подобных проектов построено "с нуля" за последние несколько лет, что дает им возможность использовать самые технически современные решения и новации последнего времени. О своем взгляде на российский рынок дата-центров, функционале безопасности, требованиях иностранных компаний, резервных офисах и услугах репликации нам рассказали Владимир Лобанов, Директор по развитию бизнеса и Борис Гехтман, Архитектор комплексных инфраструктурных решений компании Linxdatacenter.

Непростой рынок

Как показывает практика, российский рынок ЦОДов достаточно трудно подсчитать: кроме коммерческих проектов различного масштаба в большом количестве присутствуют ведомственные ЦОДы, которые нигде не заявляют своих параметров. Обычно они создаются "с нуля" под какой-то конкретный заказ - оборудование поставляется, монтаж заканчивается и все: о том, что происходит с его модернизацией знает только владелец компании. К примеру, все ЦОДы "Сбербанка", которые монтировали специалисты "Айтеко" проходят именно по этой категории. Вообще, нишевые интеграторы в России занимают значимую долю рынка, к примеру, в таких отраслях экономики, как энергетика (различные "придворные" компании, в названиях которых есть слова "сеть", "строй", "связь" и "проект" или их сочетания) или банковский сектор, а также государственное управление. Любой из ТОП-10 российских интеграторов ("Микротест", "Инлайн", "Крок" и т.д.) с подобными задачами сталкивается регулярно. Причем, как неоднократно отмечали мои собеседники у меня в блоге, «бюджет денег особенно не считает», поэтому проекты там богатые и хорошо, если мощность поставленного оборудования используется хотя бы на две трети от их возможностей.

Правда, аутсорсинговые ЦОДы выигрывают тем, что искренне исповедуют принцип сетевой нейтральности площадки, когда любой игрок, даже небольшой, может организовать подключение своих каналов связи и предложить свою цену корпоративному клиенту. "Сейчас в нашем российском ЦОДе на севере Москвы клиенту доступно порядка тридцати операторов связи - некоторые операторы имеют по 256 волокон. При необходимости увеличить мощность каналов связи клиенты устраивают тендер самостоятельно или обращаются к нам за советом. Особенно по резервным каналам связи. К примеру, у иностранных компаний по правилам их должно быть не 2, а 3, причем по территории страны эти сети должны идти разными и не пересекающимися маршрутами как на магистралях так и на уровне «последних миль», - говорит Владимир Лобанов. - Кроме того, в нашей стране есть реальный дефицит телехаузов, где размещаются исключительно операторы связи. Там предоставляются не только услуги хостинга, но и работает биржа обмена трафиком, заключаются пиринговые контракты. Фактически, ниша ЦОДов, где работали бы исключительно операторы связи, в нашей стране практически не развита, за исключением М9, наверное. А ведь при хорошей сети подобных проектов, клиенту становится важным не то, какое количество операторов связи может прийти в конкретный ЦОД, а скорость канала, которую ЦОД может обеспечить до такого телехауза, где выставлено оборудование крупных магистральных игроков рынка. Кроме того, на площадках подобных проектов в той же Европе или США можно получить хорошие условия для размещения "тяжелого" и нестандартного оборудования - обычно с ним всегда возникают проблемы у небольших проектов".

Резервные офисы

"Пока что российские операторы связи готовы, с нашей помощью, только выставлять свои узлы в подобных телехаузах в Западной Европе, но не участвовать в аналогичных проектах на территории РФ, - добавляет Владимир Лобанов. - К примеру, мы достаточно часто организуем сетевые выносы в том же Франкфурте, которые находятся под полным управлением российского оператора связи (типично востребованные типы услуг в таком случае - терминация международных каналов связи, управление трафиком, подключение к биржам трафика, подключение к голосовым операторам связи и т.д.)". В результате оператор, расположенный в России (к примеру, "Комстар-ОТС", "Синтерра", "Акадо" и т.д.), может напрямую работать с крупными операторами фиксированного ШПД всего мира.

Правда, подключение к таким мощным площадкам напрямую имеет смысл только в том случае, если внешний трафик явно приближается к 10 Гбит/с именно на внешние аплинки зарубеж. "Только в таком случае стоимость подключения будет более-менее разумной, - говорит Владимир Лобанов. - Заметных проектов, которые бы агрегировали меньшие полосы пропускания в таком режиме, на российском рынке пока особенно не отмеченно. Хотя, опыт того же "Айхоум", который анонсировал подобную систему, узнать было бы интересно".

Типовой набор сервисов

Кроме сетевой нейтральности, операторские и аутсорсинговые ЦОДы отличаются набором услуг - между подобными проектами, конечно, присутствует конкуренция, но пока что это схватка за разных клиентов. "Операторские ЦОДы, в основном, предлагают клиентам базовые наборы услуг, не развивая дополнительные сервисы, интересные корпоративным клиентам, - отмечает Владимир Лобанов. - Колкейшен, поюнитное размещение, нормальные энерговводы для стандартных стоек, а также каналы связи. Вот, в целом-то, и все их возможности. Основной бизнес у владельцев таких ЦОДов в телекоме, поэтому ЦОДы работают либо "по остаточному принципу", либо просто "для галочки". Все-таки 95% поступлений их владельцы "отбивают" именно на телекоммуникационных услугах, а на все запросы корпоративных клиентов, связанные с хостингом и т.д. приходится всего 5% оборота таких компаний". Причем, с покупкой "Голден Телекома" компанией "ВымпелКом", объединением "Комстар-ОТС" и МТС, а также приобретением "Синтерры" оператором "МегаФон" ситуация кардинально пока что не меняется - новые собственники только закрепляют уже устоявшуюся ситуацию и ничего особенно не добавляют к подобному участию

компании на рынке: часто она просто консервируется в своем развитии до окончания всех «разборок» и «зачисток» с персоналом.

"Аутсорсинговые же ЦОДы нужны, в основном, тем компаниям, ИТ-руководство которых осознает, что помимо базового набора им требуется резервное копирование, защищенные центры хранения данных, резервные офисы, более мощные системы безопасности и т.д., - уверен Борис Гехтман. - Обычно в российских условиях это компании финансового сектора и иностранные торговые компании, у которых есть не просто четкое представление о спектре необходимых услуг, а давно прописанные регламенты взаимодействия с ЦОДами, которые учитывают весь спектр потребностей от поведения в кризисных ситуациях до конкретного перечня качества сервисов, которые "забиваются" в SLA для поставщика услуги".

Чаще всего стандартных SLA по различным типам услуг в аутсорсинговых и операторских ЦОДов просто нет. Есть набор услуг и ключевые параметры их функционирования, исправления в случае аварий. Компания просто определяет за что именно она готова платить, исходя из своего бизнес-плана, и по этому направлению для нее собирается отдельное предложение из "кубиков" с показателями надежности услуг и скорости реакции хостинговой площадки, а также операторов связи.

Причем, интересная специфика: к примеру, клиентам в последнее время очень интересны расширенные функции безопасности от установки своих камер слежения до возведения капитальных выгородок, за которыми бы размещалось их оборудование. Кроме того, все возрастающим спросом пользуется услуга резервного офиса на территории ЦОДа. Это, конечно, индивидуальные и дорогостоящие услуги, но они позволяют сохранить непрерывность бизнеса компании практически в любых условиях. "Резервные площадки, кстати, у нас заказывают регулярно, - отмечает Владимир Лобанов, - обычно это помещения от 20 кв. м на 2-3 рабочих места: либо пустое пространство с коммуникациями, либо все уже оборудовано "под ключ". Хотя, есть реальные заказы на размещение пятидесяти сотрудников и в таком случае необходимо регулярно проводить учения, когда осуществляется их разовое или поэтапное перемещение из основного офиса в резервный. Отмечу, что это весьма непростая логистическая операция - все ведь должно происходить быстро и без лишнего простоя. Максимальный запрос с реальным числом резервных рабочих мест, который мы обрабатываем, на 100 человек персонала". Причем, в основном такие масштабные проекты реализуют иностранные компании, у которых обширная "генетическая память" проблем, которые возникли 11 сентября 2001 года: ведь из-за катастрофы в WTC в США разорилось более 14 тыс. коммерческих компаний. Большинство из-за того, что потеряли безвозвратно свои данные и не смогли оперативно из восстановить.

Часть системы охлаждения

Из-за рейдеров, различных проектов типа "маски-шоу" и других опасений коммерческих компаний, российским клиентам интересны и услуги репликации: когда по запросу осуществляется "перегонка" всех его данных на резервное оборудование, размещенное за пределами России. "Причем, эта услуга возможна в нескольких вариантах. Самый простой и недорогой по стоимости "входного билета" и эксплуатационных расходов - это копирование по запросу. В таком случае, "на том конце провода" клиенту необходимо держать только сервер, систему хранения и канал связи, - говорит Владимир Лобанов. - Их использование фрагментарно, если вообще случится (хотя все оборудование находится в режиме ожидания). Второй вариант более адаптивный: когда основная обработка осуществляется в нашем ЦОДе в России, а в конце рабочего дня данные копируются зарубеж: это подходит для российских представительств иностранных компаний. И третий, наиболее затратный вариант - когда вся работа происходит удаленно: данные находятся исключительно на иностранном хостинге зарубежом. При этом, на локальных компьютерах может быть даже запрещено сохранение файлов - все действует по модели "тонкого клиента".

Стойки, готовые к размещению оборудования

Специальные клиенты

Наиболее требовательные клиенты - это, конечно, иностранные компании и службы безопасности российских ФПГ. Для них важно не только что за услуги будет предоставлять компания, а насколько ее деятельность законна, какие "соседи" будут размещены в одном с ними помещении, насколько стабильно тот или иной ЦОД работает на российском рынке. Интересная тенденция последнего времени - такие заказчики готовы работать только с прозрачными компаниями. И именно с такими исполнителями в России традиционно проблемы. Кстати, что приятно наблюдать - так это стандартные технические требования от иностранных компаний: скорости каналов, марки оборудования, устанавливаемое ПО. Обычно все это единообразно в любой части света.

Именно поэтому ИТ-специалисты крупных компаний достаточно пристально изучают исполнителей, к примеру, сможет ли ЦОД по своим техническим характеристикам соответствовать той политике безопасности, которая уже зафиксирована в документах заказчика. «Ведь когда объявляется тендер крупной компании или банка, который открывает локальный офис в России, им совсем не все равно, куда ставить оборудование в нашей стране, - уверен Владимир Лобанов. - В этой связи отдельно хотелось бы сказать про классификацию Tier Standard: Topology, согласно которой существуют четыре уровня надежности ЦОД. Данная сертификация важна на этапе стартапов, для новых дата-центров, когда нужны некоторые доказательства надежности и уровня ЦОД. Де-факто мы соответствуем Tier III, но сертификация по этому параметру - это просто красивая упаковка того, что и так присутствует. В нашем случае для клиента более важен 10 летний опыт бесперебойной работы, но если для конкретного случая потребуется сертификация и клиенты окажутся готовыми платить за это – будем сертифицироваться. Другой момент... в России есть десяток проектов (не ведомственных, ведомственных больше) которые говорят, что соответствуют такому же классу, но все забывают, что строительство такого ЦОДа - это серьезная заявка на серьезных клиентов. А если в ЦОДе Tier III - дешевые услуги и всего-то стандартный минимум сервисов, то он просто никогда не окупиться. По европейскому опыту Tier III - это ЦОД для крупных и требовательных заказчиков, компаниям СМБ он просто не по карману. Кроме того, не будем забывать специфику рынка: к примеру, по классификации у ЦОДа должна быть минимум пара генераторов. Но кто гарантирует, что их регулярно запускают в работу для тестирования? Или что вводы энергопитания действительно не только независимо входят в помещение, но и в сам защищенный периметр дата-центра? Хорошо, если тот же Tier III строят правильно "с нуля", но когда о такой классификации говорят применительно к реконструируемым зданиям - это сомнительно».

Холодный коридор отгорожен пластиком

Вдобавок, переход от собственных решений по принципу "все мое" к сдаче своего ИТ-хозяйства в аутсорсинговых ЦОД - это, отчасти, проблема с инертностью мышления. "В России всегда традиционно была хорошая техническая экспертиза. Для компании с разумным бюджетом найти ИТ-специалистов к себе в штат было возможно без особых затруднений, такие кадры всегда были на рынке труда. И было много оборудования, которое можно было купить и настроить под себя. Кроме того, бизнес развивался постепенно, поэтому был отягощен "лоскутными" решениями, которые постепенно превращались в очень обособленную ИТ-инфораструктуру, понятную только тем, кто ее создавал. Соответственно, любая российская компания имеет груз уже решенных проблем, а также персонал, который сопротивляется потере работы. Кроме того, по офисам раскидано огромное количество "железа", которое надо объединять, ломая привычные, хоть и "кривые" по исполнению бизнес-процессы. Делать это многие просто не готовы. Не будем сбрасывать со счетов и очень подозрительные, порой, запросы службы безопасности - часто они выставляют такие жесткие требования к ЦОДам, что по бюджету внедрения перенос узлов связи туда просто невозможен: слишком дорого для заказчика".