Позитив возвращается

Достигнув минимальных годовых значений после продолжительной весенней коррекции в конце мая, российские площадки в июле начали восстанавливаться. Неплохая отчетность и ожидания важных событий на рынке повысили привлекательность бумаг телеком- и ИТ-компаний.

Анна ЗАЙЦЕВА,
аналитик УК «Финам Менеджмент»

Впрочем, был и целый ряд факторов, препятствовавший росту отечественных бирж. Основным из них стало обострение долгового кризиса еврозоны: противоречивые заявления официальных лиц ЕС по поводу финансовой помощи Греции, неоднократно отложенное принятие окончательного решения по этому вопросу, снижение кредитных рейтингов проблемных европейских стран. Все это сдерживало активность инвесторов на фондовых площадках. Однако в конце июня ситуация с долговой проблемой Греции разрешилась: ЕС и МВФ все-таки предоставили стране очередной транш финансовой помощи.

Волатильности рынков способствовала и неопределенность в США, но содержание комментариев главы ФРС Бена Бернанке в целом совпало с ожиданиями игроков (подтверждение завершения программы QE2 и сохранение ставок на низком уровне на неопределенно долгое время). Тем не менее заявление Бернанке о том, что ФРС может принять дополнительные меры поддержки экономики, инвесторы восприняли настороженно. В этой ситуации российский рынок чутко реагировал на внешнюю конъюнктуру, в том числе на динамику нефтяного рынка. В течение месяца стоимость нефти марки Brent снижалась, дойдя к концу июня до отметки $105 за баррель.

«Ростелеком» набирает силу

Бумаги «Ростелекома» в очередной раз выступали в роли «защитного актива» на российском рынке. И если вторую половину мая акции компании торговались в узком боковом ценовом коридоре (160–165 руб.), то уже в июне они почувствовали в себе силу и начали стремительно покидать непривлекательный для них диапазон.

Своего пика обыкновенные акции «Ростелекома» достигли 17 июня, прибавив за день около 25% – с 173,96 до 217,36 руб. за акцию. Столь мощному скачку способствовал целый ряд новостей. В первую очередь, инвесторы позитивно оценили новость о включении акций «Ростелекома» в базу расчета индекса РТС, которая будет действовать в период с 16 июня по 15 сентября. На этом фоне снова усилились ожидания, что бумаги оператора в ближайшем времени войдут в расчет индекса MSCI. Напомним, что MSCI допускала возможность включения акций компании в свои индикаторы еще в июне, однако решила повременить до августа – до объединения всех выпусков «Ростелекома». Основным же катализатором роста послужило заявление Министерства экономического развития РФ о возможной приватизации укрупненного «Ростелекома».

Однако в дальнейшем на фиксации прибыли акции «Ростелекома» нивелировали весь свой рост, опустившись по итогам июля к отметке 188,39 руб. за акцию, – таким образом, за рассматриваемый период они прибавили 6,73%.

МТС: отчетность лучше ожиданий

Весьма волатильно проходили торги акциями сотового оператора МТС, которые по итогам отчетного периода по-

Справка ИКС

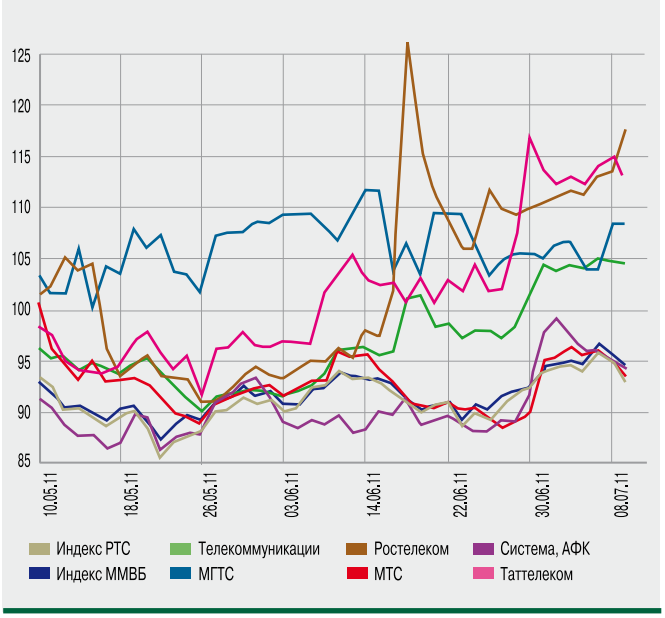
В период с 15 мая по 30 июня индекс ММВБ прибавил 2,11%, достигнув уровня 1666,59 пункта; индекс РТС вырос на 2,16% – до 1906,71 пункта. Рост продемонстрировал и отраслевой индекс «ММВБ телекоммуникации», прибавив 2,63% – до значения 2468,47 пункта.

теряли 2,52%, остановившись на отметке 230,05 руб. Не стала драйвером роста для бумаг компании и отчетность по US GAAP за I квартал 2011 г., которая, между прочим, оказалась несколько лучше ожиданий. Так, консолидированная выручка группы МТС по US GAAP выросла в I квартале на 12,2% по сравнению с I кварталом прошлого года – до $2,934 млрд. Консолидированный показатель OIBDA по группе МТС уменьшился в годовом исчислении на 2,7% – до $1,126 млрд, маржа OIBDA составила 38,4%. Консолидированная чистая прибыль группы МТС в I квартале равнялась $322 млн, сократившись на 16,1%. Чистый денежный поток компании за первые три месяца 2011 г. составил $621 млн. В России, на основном рынке группы МТС, выручка за I квартал выросла в годовом исчислении на 14% – до 74,3 млрд руб., при этом выручка от услуг передачи данных составила 5,5 млрд руб., увеличившись в полтора раза.

ИТ-сегмент подводит итоги

Неплохо выглядели на российском рынке акции АФК «Система», которые за рассматриваемый период прибавили 5,06%, до отметки в 31,2 руб. за акцию. Среди корпоративных новостей компании стоит отметить публикацию отчетности по US GAAP за I квартал 2011 г., результаты которой были вполне ожидаемы рынком. Так, выручка АФК «Система» выросла на 25,8% по сравнению с аналогичным периодом предыдущего года и составила $7,8 млрд. Показатель OIBDA увеличился на 13% – до $1,9 млрд, маржа OIBDA достигла 23,7%. Операционная прибыль компании прибавила 10,6% по сравнению с аналогичным периодом предыдущего года – до $1 млрд, операционная маржа составила 13,2%. Чистая прибыль в доле группы после корректировок выросла до $102,3 млн – на 30,5% по сравнению с $78,4 млн в I квартале 2010 г. Чистый долг на уровне корпоративного центра сни-

Динамика индексов РТС и телекоммуникационных компаний в период с 10 мая 2011 г. по 8 июля 2011 г.



зился на 38,5% относительно аналогичного периода предыдущего года: с $1922,3 млн до $1182,8 млн.

Основным же поводом для роста бумаг АФК «Система» стали сведения о дальнейших планах компании, направленных на развитие и укрупнение бизнеса на основе сделок M&A. В середине июня представители «Системы» заявляли, что компания собирается сформировать третий актив в группе базовых (сейчас у нее есть МТС и «Башнефть»), который был бы соизмерим по стоимости с остальными (доля «Системы» и в МТС, и в «Башнефти» – около $10 млрд).

Капитализация акций ОАО «РБК» выросла на 9,65%, составив 36,8 руб. Напомним, что 31 мая был успешно завершен обмен акций «РБК Информационные Системы» на акции ОАО «РБК», свои бумаги предъявили к обмену примерно 90% их держателей. Обмен осуществлялся в соотношении 1,116 акции РБК за акцию РБК ИС.

Среди новостей компании стоит отметить публикацию финансовой отчетности за I квартал 2011 г., которая так и не стала драйвером для роста котировок РБК, поскольку результаты говорят о том, что компания неактивно увеличивает свою стоимость для акционеров. Согласно отчетности, совокупная выручка РБК в I квартале увеличилась на 31% – до 853 млн руб. Выручка от продажи рекламы выросла на 47% – до 618 млн руб. Интернет-аудитория РБК составила 56 млн пользователей на конец марта (прирост на 22% за год). Аудитория РБК-ТВ в России достигла своего исторического максимума в феврале – 17,7 млн зрителей. Показатель EBITDA в I квартале был близок к точке безубыточности и составил –88 млн руб.

Акции «Ситроникса» подешевели на 8%, до $0,69. В начале июня бумаги компании подобрались к максимальным значениям года – февральским уровням в $0,9 за акцию, но неудачная отчетность по US GAAP потянула их вниз. Согласно отчетности, ОАО «Ситроникс» в I квартале 2011 г. получило $12,7 млн чистого убытка, таким образом уменьшив размер убытка, полученного годом ранее, в два раза. Выручка выросла на 46% и составила $277,6 млн. Показатель OIBDA снизился с $7,4 млн до $5,8 млн, рентабельность сократилась с 3,9 до 2,1%. Негативом выступила высокая долговая нагрузка компании, которая препятствует росту стоимости акционерного капитала.

Акции IBS Group прекратили понижательный тренд, прибавив за рассматриваемый период 2,44% – до уровня $22,64. Акции Mail.ru Group на Лондонской фондовой бирже (LSE) за то же время потеряли 5%, снизившись в цене до $33,22 за одну GDR. Торги акциями проходили весьма волатильно. На динамику котировок сильное влияние оказывали поступающие новости об IPO. Успешное размещение «Яндекса» затмило у инвесторов интерес к акциям Mail.ru Group, акции последней не поддержали даже планы «Вконтакте» и Facebook также выступить с первичным публичным размещением (напомним, что Mail.ru Group владеет долями в обеих социальных сетях). ИКС

Земля по праву,
или Как защитить имущество операторов связи

Противоречия между действующим земельным законодательством и правилами эксплуатации сетей связи создают операторам существенные проблемы в эксплуатации линейно-кабельных сооружений. Для их разрешения потребуются изменения в гражданском и земельном законодательстве.

Екатерина КОВАЛЬ,
начальник отдела правового обеспечения проектной деятельности, макрорегиональный филиал «Центр» ОАО «Ростелеком»

Предоставление качественных услуг связи предполагает сохранность линий и сооружений связи, которая обеспечивается проведением охранно-предупредительной работы (ОПР). Однако нормативно-правовые акты, регулирующие проведение ОПР*, были приняты довольно давно и на данный момент, учитывая существенные изменения в гражданско-правовых отношениях и порядке их регулирования, они не в полной мере соответствуют действующему законодательству.

В настоящее время подавляющее большинство земельных участков, на которых расположены объекты линейно-кабельных сооружений (ЛКС), не имеет соответствующего правового режима и используется на основании фактически устоявшегося порядка, юридическая основа которого была заложена еще до введения в действие Земельного кодекса РФ пунктом 38 Правил охраны линий и сооружений связи, установившим известные ограничения на земельных участках охранных зон. Следует отметить, что Земельный кодекс имеет бóльшую юридическую силу, чем нормы указанных Правил, регулирующие земельные правоотношения (ст. 2 Земельного кодекса). Это означает, что правовой режим земель охранных зон в любом случае должен быть установлен в соответствии с нормами Земельного кодекса РФ; «охранные зоны» не входят в число вещных прав на землю. К тому же статьей 7.1 Кодекса об административных правонарушениях РФ закреплена административная ответственность за использование земельного участка без оформленных в установленном порядке правоустанавливающих документов на землю (штраф для юридических лиц – от 10 тыс. до 20 тыс. руб.).

Таким образом, существующий сегодня комплекс мероприятий ОПР, в частности правовой механизм его реализации, не позволяет должным образом обеспечить сохранность линий и сооружений связи. Проблемы здесь состоят в следующем. Во-первых, собственники земельных участков, на которых расположены ЛКС операторов связи или иных владельцев, отказываются выполнять требования специалистов технических служб операторов связи, эксплуатирующих ЛКС, касающиеся осуществления (или неосуществления) определенных действий в охранной зоне линии связи. Более того, они чинят препятствия сотрудникам операторских компаний в проведении эксплуатационных мероприятий, объясняя это отсутствием указаний об обременении земельных участков.

Во-вторых, при выдаче соответствующих разрешений на строительство или ремонт объектов капитального строительства местные (муниципальные) органы власти не требуют от застройщика согласования проектной документации с представителями оператора связи (оно предусмотрено Правилами проведения земляных работ, утвержденными в некоторых субъектах РФ), а также заключения на проектную документацию и иных документов. При этом они вполне правомерно ссылаются на нормы

* ОПР – составная часть технического обслуживания линейно-кабельных сооружений, которая регламентируется Правилами охраны линий и сооружений связи (утверждены Постановлением Правительства РФ от 09 июня 1995 г. № 578) и Правилами технической эксплуатации первичных сетей ВСС РФ (утверждены приказом Госкомсвязи России от 19 октября 1998 г. № 187).

Градостроительного кодекса РФ от 29 декабря 2004 г. № 190-ФЗ (которым такое согласование не предусмотрено), а также аргументируют это тем, что вся информация об ограничении права пользования – обременении земельного участка в границах охранной зоны линии связи, – являющаяся, по сути, исходными данными при проектировании и строительстве, должна присутствовать в государственном кадастре недвижимости. Как следствие, работа застройщиков в соответствии с утвержденной, но не согласованной с владельцем линии связи проектной документацией в большинстве случаев ставит под угрозу сохранность ЛКС.

Какие возможности дает закон

В соответствии с п. 15 Правил охраны линий и сооружений связи порядок использования земельных участков, расположенных в охранных зонах сооружений связи и радиофикации, регулируется земельным законодательством Российской Федерации. Принятый и введенный в действие в 2001 г. Земельный кодекс (№ 136-ФЗ от 25 октября 2001 г.) устанавливает, что в настоящее время собственник линейных сооружений может размещать свои объекты на земельных участках на основании права собственности, аренды либо сервитута (права ограниченного пользования чужими земельными участками), т.е. на основании вещных прав.

Приобретение оператором связи всех земельных участков, используемых для размещения ЛКС, в собственность практически нереально в силу технических и экономических причин: возникают большие трудности с определением размера необходимых участков и их стоимости, уплаты соответствующего налога; выкуп участков у нынешних собственников весьма проблематичен.

Размещение ЛКС на арендуемых земельных участках – тоже не самое простое решение, так как собственники данных участков не обязаны заключать договор аренды, к тому же отсутствует методика расчета арендной платы.

В настоящее время ЛКС располагаются на земельных участках на правах «фактического владения». Таким образом, данные земли используются на основании права ограниченного пользования чужими земельными участками (сервитута). Установление сервитута – его официальное правовое закрепление – представляется одним из наиболее приемлемых вариантов решения проблемы.

Решение найдено?

Сервитут представляет собой ограниченное право пользования чужим земельным участком, незначительно обременяющее права собственника такого участка и не препятствующее дальнейшему использованию участка по целевому назначению. Возможен частный и публичный сервитут; различие между ними состоит в том, что в зависимости от наличия или отсутствия публичного интереса (большой общественной значимости) предусматриваются разные способы обременения права собственности сервитутом. Так, пункт 2 ст. 23 Земельного кодекса РФ предусматривает возможность установления публичного сервитута в целях ремонта коммунальных, инженерных, электрических и других линий и сетей, а также объектов транспортной инфраструктуры.

Договор о **частном сервитуте** – это соглашение, в силу которого одна сторона (собственник) предоставляет в пользование другой стороне (сервитуарию) недвижимое имущество, а другая сторона (сервитуарий) обязуется пользоваться имуществом в соответствии с условиями и прекратить использование при отпадении оснований установления.

В случае частного сервитута презюмируется его платность. Собственник земельного участка, обременяемого частным сервитутом, вправе требовать от лиц, в интересах которых установлен сервитут, соразмерную плату за пользование участком.

Если частный сервитут является примером частноправовых (гражданских) отношений и устанавливается соглашением сторон, то **публичный сервитут** устанавливается решением органа власти – правовым актом РФ, нормативным правовым актом субъекта РФ, нормативным правовым актом органа местного самоуправления (административный метод). В то же время ограничение права касается неограниченного круга лиц и представляет собой определенный правовой режим использования земельных участков или их частей любым лицом независимо от наличия или отсутствия у него прав на земельный участок. Целью ограничения прав (в частности, установления охранных зон линии связи) является охрана объектов, имеющих общественное значение, путем ограничения хозяйственной деятельности.

Таким образом, установление публичного сервитута в интересах оператора связи является наиболее приемлемым, поскольку не влечет за собой соответствующей платы и решает проблему заключения отдельного договора о сервитуте (поиска компромисса) с каждым собственником земельного участка, на территории которого расположены ЛКС.

Юридические проблемы и финансовые следствия

Минэкономразвития России в своем письме от 22 июня 2009 г. № Д23-1850 констатирует, что Правила охраны линий и сооружений связи не являются решением об установлении публичного сервитута, поскольку они не предусматривают закрепления права ограниченного пользования земельным участком, а вводят ограничение прав хозяйствующих субъектов для обеспечения сохранности действующих кабельных, радиорелейных и воздушных линий связи и линий радиофикации, а также сооружений связи, повреждение которых нарушает нормальную работу российской взаимоувязанной сети связи, наносит ущерб интересам граждан, производственной деятельности хозяйствующих субъектов, обороноспособности и безопасности России.

Далее, необходимо подчеркнуть, что правовая конструкция публичного сервитута имеет ряд недостатков, что приводит к затруднениям при его установлении. В частности, публичный сервитут может устанавливаться исключительно для ремонта линейного объекта – для целей строительства и эксплуатации линейного объекта это невозможно. Кроме того, в соответствии с правилами ст. 23 Земельного кодекса РФ при установлении публичного сервитута собственник земельного участка вправе требовать соразмерную плату от органа государственной власти или органа местного самоуправления, установившего публичный сервитут, но не от его пользователя. В результате органы государственной власти и местного самоуправления никоим образом не заинтересованы в установлении публичных сервитутов.

Приобретение оператором связи всех земельных участков, используемых для размещения ЛКС, в собственность практически нереально в силу технических и экономических причин

Пункт 2 ст. 23 Земельного кодекса РФ закрепляет, что при установлении публичного сервитута учитываются результаты общественных слушаний, однако порядок (механизм) их проведения не определен. Тем не менее отметим, что Научно-консультативный совет при Федеральном арбитражном суде Уральского округа (протоколом № 4 от 11 ноября 2005 г.) утвердил рекомендации «По вопросам разрешения споров, связанных с применением норм земельного законодательства». В них даны разъяснения по поводу принципов проведения общественных слушаний при установлении публичного сервитута, которые можно использовать в практических целях.

Существует также немаловажная проблема, связанная с процедурой оформления прав на ЛКС и права пользования земельными участками под ними, обязательность которой определена ст. 12 Федерального закона «О государственной регистрации прав на недвижимое имущество и сделок с ним» от 21 июля 1997 г. № 122-ФЗ и ст. 51 Градостроительного кодекса РФ от 29 декабря 2004 г. № 190-ФЗ. Не сбрасывая со счетов техническую составляющую, можно сказать, что проблема обусловлена в большей степени экономическим фактором: потребуются большие финансовые затраты для подготовки землеустроительной документации, проведения исследовательских и изыскательских работ, межевания и согласования границ земельного участка, перевода земель из одной категории в другую.

Однако в соответствии с действующим законодательством без данных мер не обойтись. При этом п. 9 ст. 23 Земельного кодекса РФ при установлении сервитута также определяет необходимость его государственной регистрации в соответствии с Федеральным Законом «О государственной регистрации прав на недвижимое имущество и сделок с ним», который, в свою очередь, делает обязательным проведение ряда перечисленных выше мероприятий, обременительных с финансовой точки зрения.

Как видно из характера проблем, связанных с использованием земельных участков в целях размещения, строительства, эксплуатации и ремонта ЛКС, их разрешение потребует внести соответствующие изменения в гражданское, земельное и иное законодательство.

Как быть операторам?

Попытки разработать концепцию улучшения законодательного регулирования земельных отношений предпринимаются уже несколько лет. К примеру, два законопроекта подготовило ОАО «Связьинвест», Минэкономразвития России разрабатывало законопроект во множестве редакций, две редакции законопроекта принадлежат ОАО «Федеральная сетевая компания», свой законопроект предлагал депутат С.А. Капков. Но ни одна из предложенных концепций не получила всеобщего (правительственного, ведомственного, научного) одобрения и не была реализована.

НП «ЦИПРТ» и «Связьинвест» взяли на себя инициативу, проведя (совместно с «Газпромом», «Федеральной сетевой компанией», «Транснефтью», Мининформсвязи, Минэкономразвития, ведущими научными организациями и экспертами в области гражданского и земельного права) работу по подготовке изменений в законодательство. В результате этих совместных усилий были разработаны концепция изменений и техническое задание на разработку законопроекта «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием нормативно-правового регулирования сервитутов».

Разработанный проект Федерального закона, как отметило Минэкономраз-

вития России в своем письме от 22 июня 2009 г. № Д23-1850, предполагает значительное упрощение и удешевление доступа соответствующих организаций к земельным ресурсам. Законопроект, в частности, предусматривает, что:

- возможно проведение не только ремонта, но и строительства, реконструкции, эксплуатации линейных объектов на условиях публичного сервитута;
- выполнение работ на условиях сервитута не влечет за собой необходимости изменения категории земельного участка и его разрешенного использования;
- документ, подтверждающий установление публичного сервитута, наряду с иными предусмотренными Градостроительным кодексом РФ требованиями является основанием для получения разрешения на строительство и на ввод объекта в эксплуатацию;
- установление публичного сервитута не требует образования земельных участков и проведения связанных с этим кадастровых работ;
- установление публичного сервитута не требует заявления со стороны линейных организаций о проведении государственного кадастрового учета (сведения о границах действия публичного сервитута вносятся в кадастр как сведения о зонах с особыми условиями использования территории, представляемые органом власти, принявшим решение об их установлении, в порядке информационного взаимодействия);
- не требуется регистрация публичного сервитута в Едином реестре прав на недвижимое имущество и сделок с ним.

На момент подписания письма Минэкономразвития России законопроект находился на стадии согласования с федеральными органами исполнительной власти, однако дальнейшая его судьба неизвестна.

Поскольку описанная проблема для операторов связи – владельцев ЛКС является существенной и актуальной, а ее разрешение требует комплексной глобальной оценки экономических, правовых, административных и иных аспектов, необходимо разработать механизм обеспечения защиты имущественных прав операторов связи на ЛКС, проложенные в земле, провести кадастровый учет в отношении ЛКС операторов связи, государственную регистрацию права собственности на отдельные ЛКС либо на те, которые являются сложной вещью. Необходимо также решить вопрос об установлении ограниченного права пользования на земельных участках, на которых размещаются или планируется размещение ЛКС (в том числе выносок), с учетом предполагаемых изменений в действующем законодательстве. Чтобы снизить расходы на оформление документов, необходимых для кадастрового учета, целесообразно рассмотреть вопрос о создании особого аффилированного лица – специализированной организации для ведения кадастровой деятельности.

Для реализации этих мероприятий операторам связи в первую очередь следует обратить внимание на следующие вопросы. Необходимо изучение и анализ имеющихся проектов изменений в законодательство, касающихся совершенствования нормативно-правового регулирования сервитутов. Эта работа должна включать определение этапа согласования изменений, степени вероятности их одобрения и последующей реализации, составление прогноза развития законодательства о сервитутах.

Далее, потребуется разработка и дальнейшая корректировка соответствующей программы проведения кадастрового учета в отношении ЛКС оператора связи и установления ограниченного права пользования на соответствующих земельных участках. При этом особое внимание следует уделить таким вопросам, как:

- порядок взаимодействия с органами местного самоуправления;
- порядок проведения общественных слушаний;
- подготовка документов, необходимых для государственной регистрации указанных ограничений;
- порядок судебного оспаривания действий (бездействий), связанных с отказом в установлении (регистрации) ограничений пользования земельными участками.

А для более эффективного решения всех рассмотренных вопросов операторам связи, отвечающим за сохранность кабельных линий и сооружений, целесообразно объединить усилия в деле защиты своих интересов. ИКС

ЛКС располагаются на земельных участках на правах «фактического владения» – т. е. данные земли используются на основании права ограниченного пользования чужими земельными участками (сервитута)

Регулирование 2.0
С точки зрения здравого смысла

Настала пора поговорить о регулировании Интернета, из которого поступает ныне большинство инфокоммуникационных сервисов и на котором базируется создаваемое у нас электронное правительство со всеми своими электронными госуслугами.

Александр ГОЛЫШКО,
канд. техн. наук

Интернет наступает

Глобализация стирает все границы на пути к информационному обществу, и уже давно телекоммуникационные решения используются не только для общения. Для телекоммуникационной отрасли это открывает большие возможности, но одновременно таит огромные риски. Операторы замкнуты на своих сетях и своих аудиториях, тогда как интернет-сервисы имеют воистину глобальный охват. Интернет-сервисы методично «вытаптывают поляну», которую телеком-операторы издавна считали своей. Когда-то все началось с интернет-телефонии, имевшей весьма невысокое качество, а сегодня «поговорить по скайпу» – термин, используемый даже менеджментом телефонных компаний и подразумевающий в дополнение неплохую видеосвязь, которая, похоже, уже «убила» рыночные перспективы обычных (не HD и пр.) видеоконференций. Еще в Интернете легко осуществляется переносимость номера и «обходится» роуминг. Благодаря развитию ШПД и «облаков» больше никто не смеется над сервисом YouTube, а Интернет стал напоминать кабельное ТВ (возьмем хотя бы технологию OTT (Over the Top) для качественной передачи ТВ-программ). Но видят ли это телевизионщики, так активно занимающиеся цифровизацией ТВ-вещания? «Эфирных телевизионщиков» хотя бы прилично инвестировало государство (там есть некоторые государственные интересы), но инвестиции в коммерческие сети кабельного ТВ и даже сети IPTV (которых государство как бы не видит в программе цифровизации) также находятся под угрозой. В свете происходящего логично было бы развивать ФЦП «Национальный ШПД», в рамках которой решались бы задачи всех остальных коммуникационных и информационно-технологических ФЦП.

Кстати, КВ-радиовещание уже уходит из эфира в Интернет. И дети больше слушают «мобильник» или iPod (со скачанной из Интернета музыкой), нежели радиоприемник, и больше смотрят компьютер, нежели телевизор. А ведь дети и есть те самые будущие массовые участники процесса коммуникаций, для которых трудится сегодня наша отрасль. И то, что они выберут после «пепси», во многом уже понятно. Их вряд ли заинтересуют правила предоставления услуг телефонной связи, которая, не исключено, станет просто бесплатным приложением к любому сервису или бытовой электронике.

Современные крупные интернет-компании уже практически не видят в операторах связи конкурентов – и по набору сервисов, и по охвату клиентской базы, а иногда и по капитализации. Они искренне считают, что задача телеком-операторов – дать абоненту ШПД и обеспечить хороший транспорт, а все остальное их не касается, потому что с сервисами и доходами интернет-компании разберутся сами. Интернет-компании долго ждали, чтобы операторы поделились с ними доходами от дополнительного трафика, который они помогают сгенерировать. Целое десятилетие операторы не замечали контент-провайдеров сотоварищи и в итоге пришли к безлимитной модели предоставления ШПД, поверх которого теперь идет настоящее цунами трафика от контент-провайдеров. Более того, крупнейших из них операторский транспорт уже перестает удовлет-

ворять, и они начинают строить свои оптические сети доставки контента (CDN), шунтирующие этот транспорт чуть ли не до ближайшего сетевого узла доступа, откуда рукой подать до абонентского ШПД. Куда выходят эти CDN другим концом? К мощнейшим ЦОДам с контентом и облачными сервисами, также закольцованным «оптикой», никак не относящейся к сетям телеком-операторов. Зачем, к примеру, Google несколько лет назад купил алюминиевый завод в Орегоне? Из-за подведенных туда огромных энергетических мощностей, и после того, как все заводское оборудование было оперативно демонтировано, там было размещено 500 тыс. серверов для того, чтобы сервисы Google на нашей планете были быстрее и доступнее. А еще Google строит свои оптические сети и даже реализует проект по подключению граждан со скоростью 1 Гбит/с. Неужели кто-то думает, что подобной деятельностью занимается только Google?

У интернет-компаний, кстати, своя конкуренция, но она мало касается телеком-операторов, у которых есть IMS и которые также начали строить CDN, но все-таки отстают от наступающих интернет-игроков, предоставляющих облачные сервисы (платформа как услуга, сеть как услуга, инфраструктура как услуга). Что же остается тем, кто не успел? Немного. Достаточно сравнить набор операторских сервисов с сервисами Google, Yandex и др. Причем их дополнительно тормозит действующее регулирование. К примеру, платформы IMS, как показала конференция NGN-2011, становятся попросту неэффективными, если их приходится ставить в каждом регионе (согласно действующим «телефонным» нормам), тогда как логика управления сервисами единой IMS в масштабах страны была бы не в пример дешевле и конкурентоспособнее. С глобальным можно конкурировать лишь на глобальном уровне. Однажды при либерализации МГ/МН-связи мы уже заставили наших операторов расставить не очень нужное и недешевое оборудование по всей стране, а в итоге многие тарифоемкие «говоруны» пользуются «скайпом». Но, как говорил Виктор Черномырдин, «отродясь этого не было, и вот опять». Здесь бы очень пригодилось «параллельное» регулирование IP-сетей, о котором мы уже говорили (см. «ИКС» № 1–2'2011, с. 55).

Помимо всего прочего сегодня в индустрии акцент с аппаратных решений смещается на приложения, обеспечивающие потребителям возможность поддерживать связь друг с другом посредством широкого круга устройств, куда входят и многие миллиарды «участников процесса» M2M или так называемого Интернета вещей. Непрерывно выходят новые модели бытовой техники: телевизоры, домашние кинотеатры, игровые приставки с подключением к Интернету. Единственное, что в них отсутствует – это поддержка чисто операторских технологий вроде IPTV. Зато «прямо из коробки» они поддерживают сервисы YouTube, Netflix, Amazon VOD и др. Вот компания CMM заключила соглашение с Samsung о доставке своего контента по технологии OTT. Теперь, подключив телевизор Samsung к Интернету от любого провайдера (нужен лишь доступ по безлимитному тарифу на скорости 1 Мбит/с), пользователь сможет смотреть кино и сериалы, снятые входящей в CMM Russia World Studios, а также видеоматериалы телекомпании «Стрим». Получается, что вопросы качества уже решены, и какие-то особенные операторские ТВ-сети для этого не нужны. Сервисы продвигают технику, техника продвигает сервисы. Компаниям-операторам в этой схеме отведено место арыка, по которому сервисы текут к человеку или устройству. Не видеть этого – самая большая опасность для всей современной отрасли связи, потому что этак «за бортом» скоро окажутся не только наши операторы, заигравшиеся на «битовой трубе» с безлимитными тарифами, но и регулятор, тщательно обдумывающий какие-нибудь новые правила, а, возможно, и правоохранители, использующие СОРМ. Кстати, говорят, что Федеральная комиссия по связи США поставила задачу обеспечить СОРМ в Skype, а затем и в социальных сетях.

Все вышесказанное, несомненно, должно быть осмыслено с точки зрения логики развития отрасли, технологий и человеческих коммуникаций. И проблемы здесь будут не столько техническими, сколько психологическими. Впрочем, отступать, прикрываясь какими-нибудь правилами пользования телефонными или телематическими услугами, некуда – Интернет наступает.

Что есть Интернет?

Интернет одновременно существует в трех лицах: как сеть передачи данных по определенным правилам и протоколам, как источник информационного обмена и как среда для ведения бизнеса. Нетрудно видеть, что к отраслевому регулированию по закону «О связи» полностью относится лишь первое «лицо» – «сеть передачи данных». Второе «лицо» подпадает под закон «Об информации, информационных технологиях и о защите информации» и закон «О персональных данных». Третье «лицо» регулируется всеми рыночными нормами, действующими в стране, и где у них «среда», где «четверг» или «суббота», они прекрасно разбираются без нас.

Так что же такое Интернет? Есть много похожих (причем технических) определений, например:

- Интернет – это глобальная информационная сеть, части которой логически связаны друг с другом посредством единого адресного пространства, основанного на протоколе TCP/IP. Интернет состоит из множества взаимосвязанных компьютерных сетей и обеспечивает удаленный доступ к компьютерам, электронной почте, доскам объявлений, базам данных и дискуссионным группам.
- Интернет – глобальная сеть компьютерных ресурсов с коллективным доступом на основе использования единой стандартной схемы адресации, высокопроизводительной магистрали и высокоскоростных линий связи с главными сетевыми компьютерами.
- Интернет – очень большая информационная система, части которой взаимодействуют между со-

бой с помощью адресного пространства, основанного на протоколе IP, а также его расширений и дополнений. Другими словами, Интернет – это просто большая сеть. Это определение принадлежит Федеральному совету США по информационным сетям.

А у нас в стране есть хотя бы «незаконодательное» определение Интернета?

Интересно, что на самом деле этой сетью никто не управляет в общепринятом смысле слова. Интернет – это, по сути, виртуальная сеть, которая не имеет физического воплощения. Функциональность этого виртуального объекта реализуется с помощью объектов другой природы – за понятием «Интернет» скрываются и телефонная сеть, и сеть мобильной связи, и контент-провайдеры. То есть функциональность Интернета реализуется с помощью множества разных сетей, имеющих разных владельцев, находящихся в разных странах и т.д. И все, кто собирается «подрегулировать» Интернет, попадают в интересное положение, пытаясь придумать новые правила для виртуального объекта, существующего поверх вполне известных материальных объектов, которые уже однажды «отрегулированы». Правда, можно, например, посоветовать национальному регистратору, чтобы он регистрировал новые доменные имена так, а не иначе. Можно поговорить с конкретным сервис-провайдером о том, как он ведет свои отношения с клиентом или контент-провайдером. Можно бороться с «нехорошими» ресурсами, но при этом ясно понимать, что мы боремся с теми, кто разместил эту информацию, а не с Интернетом или его сервис-провайдером, ибо это все равно, что бороться с радиоволнами, потоками фотонов или кабельщиками-спайщиками. Нет никакого особенного терроризма или преступности в Интернете – есть просто терроризм, есть преступность в мире и государстве. Кстати, нет и бизнеса в Интернете, а есть просто бизнес. Разумеется, все это весьма непросто для восприятия, потому что схватить сервис-провайдера гораздо легче, чем изловить какого-нибудь негодяя.

«Большая восьмерка» в 2011 г. включила в финальную декларацию своего ежегодного саммита отдельный раздел о принципах развития Интернета. Там в 22 пунктах излагаются основные положения, касающиеся Сети, которые поддержали руководители стран-участниц. В частности, после констатации важности Сети для современного мира сначала заявляется, что «открытость, прозрачность и свобода Интернета были ключом для развития и успеха Сети. Эти принципы наряду с честным, недискриминационным соревнованием должны оставаться важной движущей силой развития Интернета». Однако в следующем же пункте говорится, что при реализации перечисленных принципов свобода должна все-таки быть ограничена, а именно «включена в более широкие рамки уважения к верховенству закона, правам человека, защите интеллектуальной собственности» и т.д. При этом «в Интернете базовые принципы должны получить ровно ту же защиту и гарантии, что и в любой другой среде». Таким образом, декларация не поощряет, к примеру, свободу деятелей, выкладывающих пиратское ПО в торренты.

Зафиксирована позиция «большой восьмерки» по цензуре: «частичная или полная цензура или ограничение доступа к Интернету противоречат международным обязательствам государств и абсолютно неприемлемы». Кроме того, страны констатировали интерес на высшем уровне к модным сетевым сервисам: «Мы должны использовать растущие возможности облачных вычислений, соцсетей и публикаций граждан». Отмечена важность защиты персональных данных граждан и необходимость совместной международной работы над этим вопросом. Не забыта в документе (в аккуратных выражениях) и безопасность Сети для детей: «Мы будем развивать безопасную среду, повышая грамотность детей через предупреждение о рисках и поощрение родительского контроля, не ущемляющего свободу выражения». Наконец, в декларации говорится о том, что при управлении Интернетом необходимо придерживаться принципов multi-stakeholderism'a (участия многих заинтересованных сторон).

А глава Казахстана Нурсултан Назарбаев, выступая на недавнем юбилейном саммите Шанхайской организации сотрудничества (ШОС), отметил, в частности, что такие явления, как терроризм, сепаратизм, наркобизнес, «используют Интернет для распространения в наших странах и во всем мире». «Этот сетевой деструктив является еще одной общей угрозой. Поэтому страны ШОС должны безотлагательно выставить перед ним общий мощный заслон»,– заявил Назарбаев и добавил, что настало время вводить в международное право новые понятия – «электронная граница», «электронный суверенитет».

На встрече с генеральным секретарем МСЭ Хамадуном Туре премьер-министр РФ Владимир Путин подчеркнул, что «одна из важнейших задач – это интернационализация управления Интернетом при определенной надзорной функции со стороны Международного союза электросвязи». Мы должны запомнить все эти заявления, поскольку они крайне важны для дальнейшего развития Интернета, и не только его.

Два мира. Но не там, где ожидалось

А как можно совместно управлять тем, что принципиально никем не управляется? Как можно вводить границы там, где границ нет по определению? Одно из возможных решений предложил глава МВД Германии, который считает, что «те, кто не курит, должны быть там, где чисто, а те, кто курит, – там, где Интернет». Сие означает, что национальный интернет-ресурс должен состоять из двух частей: особо защищенной и обычного Интернета. Почему?

Как мы уже говорили (см. «ИКС» № 6'2010, с. 59), несмотря на бурное развитие интернет-технологий, никуда не делись законные вопросы к Сети, которая:

- является сетью передачи данных со своей адресацией, ключевые точки управления которой находятся в США. **Так сохранить ли риски зависимости от технических проблем или угроз за рубежом или**

построить полностью управляемый национальный сегмент?

- является бизнес-средой, которая не признает наших границ и в которой так много мошенничества и нарушения прав. **Так сохранить ли высокие риски при работе через Интернет или построить отдельную экосистему с высоким уровнем безопасности?**
- является сетью, в которой оператор не может гарантировать высокое качество услуг. **Так оставить ли доступ в Интернет как в универсальную среду или построить отдельную экосистему с высоким качеством?**

Вот мы создаем так называемое электронное правительство, развертываем доступ к тысячам электронных госуслуг и, как уже понятно, на этом не остановимся – будем строить электронное государство. Если электронное государство представляется в виде обеспечения интернет-доступа к различным серверам, то его жизнеспособность и эффективность – большой вопрос. И оберегая эти ресурсы, мы строим защищенный сегмент сети, сегмент с гарантированным качеством и информационной безопасностью. Причем и тем и другим должен заниматься один регулятор, который должен представлять электронное государство как неотъемлемую (и, очевидно, лучшую) часть отрасли. Ведь создание электронного правительства – это лишь начальный этап развития электронного государства с постепенным расширением функциональности, защиты, сервисов, коммуникативных свойств, существующих поверх создаваемой инфраструктуры All-IP. Возможно, по мере его развития наступит частичное объединение по особым правилам с другими электронными государствами. И очевидно, что электронное государство – это как минимум своеобразная социальная сеть для 140 млн пользователей или электронных граждан, обладающих уникальным идентификатором (номером, адресом). И новая историческая общность, которая в создаваемой коммуникационной среде должна себя чувствовать одновременно и комфортно, и ответственно

Что рано или поздно будет обязательно востребовано? Создание концепции «электронного правительства» как института «электронного государства» для «электронных граждан» на базе облачных вычислений и централизованной базы данных. Развитие данного сегмента информационного общества от чисто информационных функций ко все более полному электронному документообороту, интерактивному (в том числе индивидуальному) диалогу, обслуживанию массовых мероприятий (выборы и опросы) и даже «роумингу» с другими «электронными государствами». Создание соответствующей защищенной инфраструктуры как части общей национальной инфраструктуры. Последнее может подразумевать, к примеру, организацию выделенного сегмента Интернета, обладающего новыми возможностями и свойствами (которыми, кстати, обладают любые защищенные ресурсы). Это отсутствие анонимности пользователя, гарантии информационной безопасности (фроду там будет крайне неуютно), страхование информации, а далее информационный обмен, бизнес и пр. и пр. Отчего бы не выделить электронному гражданину персональный адрес/номер (возможно, первичный по отношению ко всем остальным персональным идентификаторам)? Почему бы в дальнейшем не наполнять этот защищенный сегмент новыми услугами наших операторов и интернет-компаний с гарантиями качества и информационной безопасности? И почему бы не перенести туда эффективные и защищенные платежные системы как важнейший элемент «электронного государства»? И еще много-много «почему»...

В общем, логика нашего движения к так называемому Telecom 2.0 должна заключаться не в тотальном переходе на Web 2.0/3.0 с «арыком» для операторов, а в создании двух связанных через шлюзы сегментов одной сети:

- «супермаркета» с различными гарантиями кибербезопасности и QoS, в который придут госуслуги и добросовестные поставщики сервисов, включая контент-провайдеров и операторов с их NGN, а еще там будут находиться добропорядочные «электронные граждане»;
- «колхозного рынка» в лице «традиционного» Интернета, где, как в Греции, есть абсолютно все, включая облавы на преступников и возможный дефолт по любым обязательствам.

И каждый волен будет выбирать, где ему присутствовать, или присутствовать везде. ИКС

Платформы IMS становятся неэффективными, если их ставить в каждом регионе, тогда как логика управления сервисами единой IMS в масштабах страны была бы не в пример дешевле и конкурентоспособнее

ИТ-специалисты учатся – качество бизнес-процессов растет

Технические вузы не выпускают ИТ-специалистов, готовых к эффективной командной работе, – такова особенность российского высшего образования. Но где бизнесу взять квалифицированных ИТ-сотрудников? Одно из решений проблемы – корпоративное обучение.

Михаил КУМСКОВ,
эксперт Учебного центра Luxoft, д-р физ.-мат. наук, профессор МГУ

Успешность современного бизнеса все больше и больше зависит от ИТ-инфраструктуры. По оценкам экспертов, на сегодняшний день на сопровождение ИТ-приложений для управления бизнес-процессами тратится до 80% бюджета ИТ-службы крупного предприятия. При этом линейка ИТ-решений для разных уровней организации бизнес-процессов – от простейших электронных таблиц до комплексных ERP-систем – с каждым годом пополняется новыми разработками.

Помочь грамотно выстроить отношения бизнеса и ИТ могут лишь специалисты, обладающие достаточной квалификацией. А учитывая стремительное развитие ИТ-отрасли, им приходится постоянно повышать свой уровень компетентности, причем не только накапливая опыт, но и обучаясь новым технологиям. Помимо высокой компетентности в соответствующей сфере ИТ, в числе требований к сотрудникам ИТ-службы зачастую оказываются знания в области системного анализа и управления проектами, навыки эффективных коммуникаций.

Вузы готовят программистов – практика требует эффективных ИТ-специалистов

Многим компаниям нужны не только программисты, но и другие ИТ-специалисты: системные и бизнес-аналитики, тестировщики, специалисты по развертыванию и сопровождению ИС, технические писатели, инженеры по управлению конфигурациями и изменениями, инженеры по постановке и адаптации процессов проекта.

Российских ИТ-специалистов традиционно отличает высокий уровень профессионализма. Доказательством тому служат многочисленные центры исследований и разработок, которые зарубежные компании открывают на территории РФ. Однако ошибочно было бы думать, что экспертную квалификацию отечественные разработчики и аналитики в сфере ИТ приобретают в вузах. Напротив, аналитики рынка труда сходятся во мнении, что российская высшая школа, к сожалению, не дает ИТ-компаниям стопроцентно подготовленных для эффективной командной работы специалистов.

Одним из препятствий на пути развития ИТ-образования, отвечающего требованиям сегодняшнего дня, является структура утвержденных учебных программ для вузов. Дело в том, что традиционно российское техническое образование сфокусировано на фундаментальных основах специальности. Отличительными чертами такого фундаментального подхода являются взаимосвязанность предметов и стремление развить у студентов способность самостоятельно решать задачи. В итоге выпускники технических вузов, как правило, отлично разбираются в законах, которые лежат в основе различных теорий и практик, способны мыслить глобально и анализировать большие объемы информации. Они также умеют эффективно искать и фильтровать данные, самостоятельно выводить используемые в рамках поставленной задачи формулы и решения из базовых постулатов. Из таких молодых специалистов получаются хорошие ученые и исследователи, так как еще с институтской скамьи их ориентируют на нестандартное мышление и поиск инновационных решений. Однако непосредственно в работе над конкретным проектом, да еще и в команде (а ИТ-

проекты чаще всего предполагают работу в команде), выпускнику технического вуза может не хватить практических навыков и умений.

Таковы особенности российского технического образования: при всей глобальности и фундаментальности подхода к обучению ни один вуз не развивает в студентах знания и умения применять новейшие технологии, инструменты и практики. Происходит это по той простой причине, что вузы просто не в состоянии быстро обновлять учебные программы, подстраивая их под стремительно развивающуюся ИТ-отрасль.

ИТ-специалисты должны постоянно повышать квалификацию

Технологии сегодня так быстро приходят на смену друг другу, что специалист, «выключенный» из профессии даже на непродолжительное время, рискует потерять навык и квалификацию. К примеру, как утверждают специалисты по ИТ-рекрутингу, даже самый востребованный на сегодняшний день программист Java через пару лет рискует остаться без работы, если не будет развиваться и осваивать новые технологии. Другой пример, более масштабный: еще несколько лет назад в ИТ-отделах не существовало таких должностей, как системный аналитик или тестировщик, которые сейчас входят в список наиболее актуальных на рынке труда профессий.

Таким образом, сама специфика отрасли диктует ИТ-специалистам необходимость постоянно овладевать новыми знаниями, регулярно обучаться работе с новыми продуктами и технологиями, чтобы соответствовать современным требованиям, предъявляемым как работодателями, так и самим бизнесом.

Обучение сотрудников – часть усовершенствования бизнеса

Информационные системы для бизнеса требуют поддержки, развития, обновления, интеграции с другими системами – а для этого нужна команда профессионалов. Результаты работы такой команды, а значит, и эффективность всего бизнеса напрямую зависят от квалификации персонала. Поэтому повышение квалификации сотрудников должно быть составляющей больших организационных движений. Так, если в компании внедряются новые регламенты ведения бизнес-процессов, то нужно обучить сотрудников работать в соответствии с этими регламентами.

При этом руководство компании, отправляющее своих подчиненных на тренинги, должно четко понимать, зачем это делается. Другими словами, не должно быть обучения «для галочки». Цель учебы не в том, чтобы повысить самооценку и себестоимость сотрудников на рынке труда (а заодно и престиж организации), а в том, чтобы решить конкретные бизнес-задачи. Если сотрудник проходит тренинг, но впоследствии не использует полученные знания на практике, можно считать, что средства, вложенные в его обучение, компания выбросила на ветер. Без непосредственного включения в рабочий процесс полученные на тренингах знания и навыки мгновенно забываются. Поэтому обучение должно позиционироваться не просто как бонус, входящий в соцпакет, или как возможность расширить свой кругозор за счет компании-работодателя, а как неотъемлемая часть процесса повышения эффективности бизнеса и улучшения качества работы конкретной организации.

Корпоративные тренинги как метод гибкого и фокусного обучения

Итак, необходимость регулярного послевузовского обучения ИТ-специалистов очевидна. Возникает вопрос: где, как и у кого учиться?

Существует несколько возможностей: фирма может отправить на тренинги одного или нескольких своих специалистов, а может организовать обучение сразу для всей проектной группы или вообще для всего персонала. Причем оно может проходить как в специализированном учебном центре, так и в офисе компании, «без отрыва от производства», это на самом деле не имеет особого значения. Принципиально важно, насколько тренинг полезен не для каждого отдельного сотрудника, а для компании в целом. К примеру, когда компания выборочно отправляет на обучение нескольких специалистов, то порой между

сотрудниками, побывавшими на тренингах, и остальными членами проектной команды возникает непонимание. Оказывается, что не прошедшие обучение сотрудники попросту не знакомы с теми рекомендациями, которые их коллеги почерпнули на тренингах и теперь стремятся воплощать в действующих проектах. Когда же обучением охвачены все участники команды, это дает дополнительные преимущества. Помимо повышения квалификации, сотрудники на тренингах учатся «говорить на одном языке», лучше понимать друг друга в контексте решения конкретных рабочих задач. Тем самым обучение способствует лучшей коммуникации в команде. Обучаясь в группе и развивая командное мышление, сотрудники получают более четкое представление о том, как применить новые знания и навыки к улучшению бизнес-процессов их организации.

Еще несколько лет назад в ИТ-отделах не существовало таких должностей, как системный аналитик или тестировщик, а сегодня они входят в список наиболее актуальных профессий

Именно поэтому наиболее распространенной формой получения знаний и навыков на сегодняшний день является корпоративное обучение. По динамичности оно не уступает развитию ИТ-отрасли и потому успевает идти в ногу с потребностями каждой конкретной компании. Корпоративное обучение подразумевает серию тренингов для группы сотрудников одной организации. Основная его задача – обеспечить фокусную подготовку специалистов, т. е. обучить их с наименьшим отрывом от производства и за меньшие деньги.

За счет чего обеспечивается **экономия времени?** Во-первых, это формат: время и место проведения тренинга подбирается с учетом производственного расписания сотрудников и их возможностей. Во-вторых, объем материала: программа тренинга корректируется в соответствии с потребностями и пожеланиями слушателей. К тому же тренеры делают выбор в пользу дозированной подачи материала с его поэтапной отработкой на конкретных примерах.

В качестве примеров при корпоративном обучении можно использовать внутренние кейсы компании. В этом состоит следующее его преимущество: **практичность и наглядность.** Теоретические положения и практические советы проецируются на реалии компании. Затем слушатели уже в процессе обучения применяют новые знания для решения своих производственных задач. Так как тренинг проводится только для сотрудников одной конкретной организации, у слушателей есть возможность обсудить с тренером нюансы конкретного проекта, не вынося «внутреннюю» информацию за пределы своей команды.

Это обеспечивает корпоративному обучению и преимущество **гибкости:** преподаватели подбирают наиболее эффективные формы подачи материала, опираясь на специфику конкретной компании. Разрабатывается программа обучения, максимально отвечающая потребностям, опыту и квалификации слушателей. Тренер, кастомизируя обучение, акцентирует внимание на наиболее актуальных для данной организации темах, пропуская те области, которые компания-заказчик в работе не использует.

Ценность такого обучения не только в точной, своевременной и подобранной под нужды производства информации, но и в **«живом» экспертном опыте**. Тренерами в нем выступают не просто грамотные специалисты, но и успешные практики. Преподаватели-теоретики, которые берут опыт исключительно из рассказов своих слушателей, вряд ли могут поспособствовать улучшению качества бизнес-процессов компании-заказчика.

Наконец, корпоративное обучение выгодно и с **финансовой точки зрения**. Многие руководители сходятся во мнении, что компании дешевле обучить сотрудников, которые уже имеют опыт работы в конкретном коллективе и доказали свою личную состоятельность. Приход в команду новых людей, не знающих специфики проекта, всегда связан с определенными рисками.

Разумеется, компании, решившей обучать своих специалистов, нужно быть готовой к определенным затратам. Но обучение — это инвестиция, и, как любая правильно рассчитанная инвестиция, в конечном счете оно повышает производительность труда и качество работы сотрудников, а значит, снижает расходы и/или увеличивает доходы компании.

Как мотивировать сотрудников, как планировать обучение, как оценить его эффективность – в следующем номере «ИКС».

ИКС pro технологии

Виртуализация: курс на синергию технологий

Надежда ПРИВЕЗЕНЦЕВА

В ходе эксплуатации дата-центры быстро достигают пределов своих физических возможностей. Выход – оптимизация ИТ-инфраструктуры ЦОДа путем консолидации и виртуализации.

К концу 2013 г. 50% крупных ЦОДов по всему миру будут испытывать дефицит площадей, питания и охлаждения, предрекает Gartner. Параллельно увеличивается и стоимость содержания разрастающихся систем.

В существующих дата-центрах виртуализация, как правило, начинается с вычислительной инфраструктуры. Но этот процесс требует соблюдения ряда условий и правил.

Эволюция гипервизоров

Начнем с того, что в полной мере воспользоваться преимуществами виртуализации могут лишь обладатели последних поколений серверов. Архитектура процессоров x86 изначально не была рассчитана на виртуализацию, и гипервизорам приходилось вмешиваться в вычислительный процесс, что негативно влияло на производительность виртуальных машин (ВМ). Так, некоторые команды, выполняемые обычными операционными системами, не были разрешены к исполнению внутри ВМ. Чтобы решить эту проблему, гипервизоры «перехватывали» команды гостевой ОС и модифицировали их в разрешенные. Первой компанией, запатентовавшей технологии программной виртуализации, была VMware, а описанный механизм использовался в решении VMware ESX до момента выхода 4-й версии.

С 2006 г. компании AMD и Intel выпускают процессоры x86 усовершенствованной архитектуры – с аппаратной поддержкой виртуализации (технологии AMD-V и Intel VT), в результате чего гостевые системы могут получать прямой доступ к процессорным ресурсам. Аппаратная поддержка освобождает гипервизор от выполнения ряда ресурсоемких задач, благодаря чему виртуализация сделалась более экономичной в плане потребляемых ресурсов. Кроме того, улучшилась изоляция ВМ.

Современные версии гипервизоров ориентированы именно на поддержку виртуализации на уровне процессора. Например, VMware использует возможности аппаратной виртуализации начиная с версии vSphere 4, да и гипервизоры других основных производителей в обязательном порядке требуют наличия в серверах процессоров и BIOS с поддержкой технологии AMD-V или Intel-VT. «Без этих технологий гипервизоры Red Hat KVM и XenServer не работают вообще; применяя Hyper-V, не удастся использовать виртуальные машины Linux, – комментирует Валерий Рыбин из компании «Открытые технологии».

Дальнейшее развитие технологий аппаратной поддержки виртуализации направлено на сокращение потребления ресурсов при доступе к памяти и контроллерам ввода-вывода. Речь идет о таких технологиях, как Intel VT-d и AMD-Vi (виртуализация операций ввода-вывода), Intel VT-c (виртуализация сетевых адаптеров), Intel EPT и AMD RVI (расширение функций управления памятью виртуальных машин) и т.п. Производители гипервизоров стремятся обеспечить поддержку этих технологий в своих продуктах; к примеру, поддержка аппаратных технологий EPT/RVI и VT-d/AMD-Vi есть в большинстве продуктов с гипервизорной виртуализацией.

Вместе с тем процесс «налаживания отношений» между гипервизорами и технологиями аппаратной виртуализации еще не завершен, считает Петр Марков (Fujitsu). В качестве примера он приводит поддержку технологии Intel VT-c и связанную с ней функцию VMDq (технология позволяет обрабатывать параллельные очереди пакетов, перенаправлять их в нужную ВМ на уровне чипсета): для Hyper-V поддержка этого функционала появилась только в 16-й версии драйверов, которая была выпущена в этом году.

Современные гипервизоры: возможны варианты

Как известно, существуют гипервизоры двух типов. Гипервизор первого типа устанавливается непосредственно на аппаратный комплекс, не имеющий ОС (примеры – VMware ESX, Microsoft Hyper-V, Citrix XenServer). Гипервизор второго типа устанавливается в хостовую ОС и работает поверх нее (это, например, VMware Server, Parallels Virtuozzo Containers, а также решения для виртуализации ПК – Microsoft Windows Virtual PC, VMware Workstation и др.). Обе технологии имеют свои плюсы и минусы.

В числе преимуществ гипервизора первого типа Сергей Халяпин (Citrix Systems) называет более высокую производительность системы и полную изоляцию машин друг от друга. Но за это приходится платить, на-

пример, ограниченной совместимостью с аппаратным обеспечением (Hardware Compatibility List). Гипервизор второго типа можно поставить на любой компьютер, где есть хостовая ОС. Установка его гораздо проще, но платой за это будет снижение быстродействия и зависимость от проблем хостовой ОС. «Гипервизор первого типа – для систем, требующих производительности, безопасности, – резюмирует С. Халяпин, – это вариант промышленного (корпоративного) внедрения. Гипервизоры второго типа – для вспомогательных сред (тестирования, обучения), которые предъявляют невысокие требования к квалификации обслуживающего ИТ-персонала».

Виртуализация на уровне ОС (виртуализация на базе хостовой ОС, в терминологии VMware) больше подходит для поддержки некритичных задач, для сред тестирования и разработки, а также для персонального использования, подтверждает Лионель Кавальер из компании VMware. К недостаткам этой технологии он относит то, что виртуальные машины имеют косвенный доступ к аппаратным ресурсам (с многочисленными уровнями перенаправления), что значительно повышает издержки. Кроме того, нет возможности гарантировать производительность работающих виртуальных машин: например, все входящие и исходящие запросы идут через хостовую ОС, делая ее узким местом (подверженным сбоям). Все факторы, влияющие на стабильность хостовой операционной системы, будут влиять и на виртуализованный слой, а значит, на запущенные в нем ВМ.

Программное обеспечение, устанавливаемое непосредственно на аппаратную платформу (на «голое железо»), лучше подходит для эксплуатации в производственных средах для поддержки важнейших приложений и сервисов. В числе плюсов такого решения Л. Кавальер отмечает то, что оно интегрируется, распространяется и поддерживается вместе с серверными системами, дает возможность стандартизовать ПО на множестве серверов разного типа и предоставляет расширенные возможности для организации серверов в пулы. Однако такое решение требует соблюдения определенных условий: необходимы специализированное ПО для управления гипервизором, поддержка независимых поставщиков ПО, а кроме того, применяемый гипервизор «должен доказать свою надежность и стабильность».

Виталий Обернихин (Parallels) полагает, что использование виртуализации на уровне ОС (виртуальных контейнеров) позволяет достичь большей плотности виртуальных сред на одном хосте и их большей производительности. Однако происходит это за счет того, что все виртуальные среды имеют одну ОС – либо Windows, либо Linux. Виртуализация на основе гипервизора, установленного на аппаратный комплекс, позволяет запускать различные ОС на одном хосте, однако необходимо «платить дань» в виде меньшей плотности виртуальных сред и меньшей производительности. «Виртуализацию на уровне ОС имеет смысл использовать везде, где нет необходимости смешивать различные ОС на одном хосте. Кроме того, ОС-виртуализация позволяет гораздо более эффективно использовать имеющееся оборудование, что очень важно, когда вы хотите контролировать расходы на содержание ЦОДа», – констатирует представитель Parallels. Поэтому продукты виртуализации на уровне ОС широко используют, например, хостинг-провайдеры.

Но вернемся к гипервизорам первого типа. Как уже было сказано, они могут быть встроены в серверное оборудование, и основные производители серверов выпускают решения с интегрированными гипервизорами (хотя Валерий Рыбин считает, что применительно к серверам x86 правильнее употреблять термин «предустановленные»). Они представляют собой флеш-карту либо USB-накопитель, который вставляется в разъем на системной плате сервера. В качестве интегрированных гипервизоров на данный момент используются VMware ESXi, Citrix XenServer и Microsoft Hyper-V. «Интегрированные гипервизоры становятся

все более популярными, – говорит Сергей Лисняк из компании «АйТи». – Такой подход позволяет максимально быстро разворачивать виртуальную инфраструктуру, а также сокращать затраты на покупку внутренних дисков для серверов. Производители серверов также «зашивают» в гипервизор дополнительный программный компонент, который позволяет вести постоянный мониторинг физических компонентов сервера».

«Поскольку гипервизор, по сути, является неизменяемой единицей с минимальными настройками, то вполне логично выглядит решение интегрировать его с предлагаемым серверным оборудованием, – подтверждает Владимир Мешалкин (АМТ-ГРУП). – Но в больших корпоративных инфраструктурах со множеством хостов и централизованной системой управления более целесообразной видится загрузка из сети хранения (SAN), что позволяет оперативно управлять всем комплексом, включая обновления и добавление дополнительных хостов».

Первые версии интегрированных продуктов работали не всегда стабильно, но сейчас, по мнению Александра Светлакова (HP Россия), все «детские болезни» излечены. «Функциональные возможности интегрированных гипервизоров точно такие же, как у устанавливаемых на жесткие диски, поэтому нет никаких причин не использовать их на производственных системах, – говорит он. – Многие наши заказчики уже больше двух лет используют гипервизоры, загружаемые с флеш-накопителей».

Главным достоинством интегрированных гипервизоров П. Марков считает снижение TCO: «Диск имеет механическую часть, и это делает высокой вероятность его отказа. Для обеспечения отказоустойчивости требуется минимум два диска и контроллер, который поддерживает функции RAID, а конфигурирование потребует дополнительных знаний и времени».

Что лидер нам готовит?

В отчете Gartner (май 2010 г.) компания VMware с ее платформой виртуализации VMware vSphere названа лидером на рынке виртуализации серверной инфраструктуры на базе x86. Платформа VMware vSphere представляет собой набор продуктов для виртуализации серверов, в который входят гипервизор и инструмент управления VMware vCenter Server. Что касается гипервизора, то на данный момент VMware предлагает два варианта – ESX и ESXi. Основная разница между ними состоит в том, что ESXi представляет собой так называемый тонкий гипервизор размером около 30 Мбайт, который устанавливается непосредственно на сервер. В нем отсутствует встроенная графическая консоль управления vCenter и дополнительные функции. «Благодаря этому, – поясняет С. Лисняк, – почти в 10 раз снижается размер обновлений, скачиваемых с сайта. Все управление производится удаленно, а функционал можно наращивать путем приобретения дополнительных лицензий на те опции, которые необходимы конкретному заказчику».

До последнего времени в VMware vSphere поддерживались оба гипервизора. Однако VMware объявила, что в vSphere 5 останется поддержка только ESXi. В. Рыбин считает такой шаг производителя вполне логичным: «Начиная с 4-й версии VMware vSphere практически полностью готов механизм взаимодействия с гипервизором напрямую, без посредника, которым являлась сервисная консоль. VMware предоставила доступ к API взаимодействия с гипервизором напрямую и дала достаточно времени компаниям-разработчикам, чтобы переписать свое ПО под новую архитектуру». Отказ от сервисной консоли должен уменьшить издержки виртуализации: сейчас сервисная консоль – это фактически виртуальная машина, потребляющая ресурсы. Кроме того, добавляет В. Рыбин, повысится надежность решения: «меньше программного кода – меньше невыявленных ошибок, меньше сложность системы». Сократятся затраты на разработку новых версий ПО и сам цикл разработки.

Ожидается, что VMware предложит и так называемый stateless hypervisor – гипервизор, который не привязан к конкретному серверу и загружается по сети (в режиме PXE). Такой подход Александр Скороходов (Cisco) считает наиболее перспективным: «Как установка гипервизоров на флеш-диск сервера, так и установка на традиционный диск обладают тем недостатком, что привязывают функцию виртуализованного хоста к конкретному экземпляру блейд- или стоечного сервера. Поэтому в ближайшее время мы будем видеть более активное применение схем развертывания гипервизоров без привязки к конкретному серверу, использующих загрузку сервера по LAN или SAN». По мнению представителя Cisco, эта технология обеспечивает более гибкое управление серверными ресурсами и, в частности, позволит более полно задействовать возможности вычислительной платформы Cisco UCS.

Мультивендорная виртуализация

В ходе исследования Virtualization Decisions Purchasing Intentions Survey, проведенного порталом TechTarget два года назад, больше половины респондентов сообщили, что предпочли бы избежать смешанных виртуальных сред, но при этом не исключают использования в своей инфраструктуре платформ разных производителей, поскольку сомневаются, что единственная платформа способна в полной мере обеспечить выполнение всех возможных бизнес-задач. Оправдан ли мультивендорный подход при создании виртуализованной инфраструктуры, применяется ли он сегодня?

«Да, мультивендорные виртуализационные среды используются у многих заказчиков, – отвечает А. Светлаков. – Например, виртуализация серверов выполняется на продуктах одного вендора, а виртуализация персональных компьютеров – на продуктах другого. В крупных компаниях нередки ситуации, когда разные филиалы выбирают разные гипервизоры. Кроме того, иногда компания, внедрившая серверную виртуализацию на продуктах одного поставщика, выбирает для

ЦОД·2011

6-я ежегодная международная конференция

издается с 1992 года
ИКС
www.iksmedia.ru

для профессионалов в области строительства и эксплуатации дата-центров
6 сентября 2011 года, гостиница Holiday Inn Sokolniki, Москва

Цели конференции:

- Обсудить в кругу профессионалов отечественной и зарубежной индустрии цодостроения актуальные вопросы строительства и эксплуатации ЦОДов
- Изучить лучшие зарубежные и российские практики
- Узнать о последних инновационных разработках в области цодостроения
- Рассмотреть эволюцию услуг ЦОДов
- Задать вопросы ведущим мировым экспертам и владельцам ЦОДов

Аудитория конференции: владельцы и руководители ЦОДов, ИТ-директора, директора по строительству, начальники служб эксплуатации, специалисты ИТ и инженерных служб. Всего более 400 участников.

Основные темы конференции

Оборудование и инфраструктура

- Кабельные системы
- Системы электроснабжения
- Климатическое оборудование
- Системы управления и мониторинга
- Системы физической безопасности
- Серверы, системы хранения, сетевое оборудование и ПО
- Виртуализация и консолидация
- ИТ-архитектура
- Информационная безопасность

Услуги

- Облачные сервисы
- ИТ-аутсорсинг
- SLA
- Managed Services

Управление и экономика

- Создание бизнес-концепций
- Типы ЦОДов
- Управление проектами создания ЦОДов
- Стандарты, сертификация
- Модернизация
- Аутсорсинг персонала
- Оптимизация затрат на инфраструктуру и ПО
- Повышение доходов от услуг
- Возврат инвестиций
- Энергосберегающие технологии

Инновации

- Модульные ЦОДы
- «Зеленые» подходы в ЦОДах
- Виртуальный ЦОД
- Новые инженерные решения

По вопросам спонсорского и делегатского участия обращайтесь в коммерческий отдел журнала «ИКС» по телефонам: (495) 229-4978, 785-1490, 502-5080 или факсу (495) 229-4976.

Более подробная информация на портале **http://dcforum.ru**

Организатор – журнал «ИКС»

новых решений другие продукты, чтобы не попадать в зависимость от конкретного вендора».

«Такие подходы используются нашими заказчиками, – подтверждает С. Халяпин. – Например, для работы XenDesktop или XenApp они выбирают решение XenServer, хотя для прочей нагрузки ранее выбрали другой гипервизор. Обычно продукты одного вендора оптимизированы для совместной работы гораздо лучше, чем для работы на стороннем ПО».

Платформы виртуализации разных вендоров могут различаться по цене, функциональности и производительности. Поэтому мультивендорный подход имеет смысл, если желательно предлагать разнообразные виртуализационные решения, считает В. Обернихин. С другой стороны, поддержка решений нескольких вендоров обычно увеличивает количество проблем: требуются надежное решение для управления разными платформами, беспроблемная миграция между виртуализационными продуктами и т. д. «Есть компании, которые на практике используют различные виртуализационные платформы, – замечает г-н Обернихин, – но, как правило, для непересекающихся категорий пользователей».

«Данный подход характерен скорее для крупных организаций или в случае специфических требований уже реализованных проектов виртуализации. В целом экономически целесообразно использовать единую платформу виртуализации», – считает Андрей Кучинский («Verysell Проекты»). С этим согласен и В. Мешалкин: «Обслуживание однотипной инфраструктуры обходится значительно дешевле». При переводе инфраструктуры в виртуальную среду он советует максимально внимательно подойти к вопросу стандартизации: «Выбор поставщика среды виртуализации – это выбор не просто гипервизора, но и системы управления, обеспечения отказо- и катастрофоустойчивости, резервного копирования, а в перспективе и частного облака компании. Поэтому к первоначальному выбору платформы нужно относиться весьма ответственно. Кроме того, практика показывает, что вслед за первоначальным внедрением и апробацией следует масштабирование, т.е. дополнительные траты. Нецелесообразно создавать дублирующие непрозрачные друг для друга системы».

Средства управления – свои или чужие?

Специалисты часто подчеркивают, что при внедрении виртуализации обязательны средства мониторинга и управления, иначе высок риск получить неконтролируемую среду, способную принести больше проблем, нежели пользы. Производители гипервизоров предлагают «фирменные» инструменты управления и планирования нагрузки в виртуализованной среде – VMware vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Citrix XenCenter, Citrix Essentials для управления средами на базе Citrix XenServer и Microsoft Hyper-V. Пакет Citrix Essentials для Hyper-V дополняет собственное решение Microsoft; в свою очередь, компания Microsoft в этом году добавила возможность управления инфраструктурой виртуализации Citrix в SCVMM 2012.

Вместе с тем существуют и продукты сторонних производителей для мониторинга и управления виртуальной средой VMware, Hyper-V или Citrix: их предлагают, например, компании SolarWinds, Veeam, IpSwitch и ряд других. Имеет ли смысл пользоваться ими?

«Продукты сторонних производителей можно и нужно использовать, если функционал, например, vCenter недостаточен, – полагает В. Рыбин. – Обычно такая ситуация имеет место в организациях, где помимо виртуализации существуют еще гетерогенные сети LAN и SAN, компьютеры под управлением UNIX и Linux, почтовые серверы, серверы баз данных, ERP и прочие системы. В этих случаях использование единой системы мониторинга позволяет значительно быстрее выявлять сбои в системе и восстанавливать ее работоспособность». Выбор же конкретной системы во многом зависит от требований заказчика.

«Поставщики средств виртуализации часто сильно заняты концепцией, а об удобстве конечных пользователей задумываются во вторую очередь, – замечает П. Марков. – Именно в этот момент на помощь приходят поставщики дополнительного ПО и сообщество независимых программистов».

«Указанные компании разрабатывают нишевые решения, они создают отличные средства управления, но для строго определенных задач, – отмечает А. Светлаков. – Например, продукты Veeam хорошо дополняют VMware vCenter. Проблема для заказчиков в том, что для управления виртуализированной средой им приходится использовать несколько консолей, а это не всегда удобно. Для управления средой виртуализации использование фирменных средств является обязательным. Другие программные продукты, например HP Virtual Machine Management, могут их дополнять, но не заменять».

У компании Citrix есть развитая экосистема, и партнерские продукты расширяют и дополняют возможности фирменных средств управления и мониторинга. Для управления гипервизором XenServer можно воспользоваться, например, продуктами Servarica WHMCS XenServer Module (SWXSM), Solus Virtual Manager (SolusVM), OpenXenManager (аналог Citrix XenCenter с открытым кодом); XVP (web-менеджер ВМ для Citrix XenServer и Xen Cloud Platform). «Существуют также решения, нацеленные на любые гипервизоры, имеющие ядро Xen, – добавляет С. Халяпин, – ситуация с гипервизором Microsoft аналогичная».

Parallels Automation, стандартная платформа автоматизации бизнеса хостинг/сервис-провайдеров, поддерживает, в частности, Hyper-V.

Классики виртуализации к возможности использования управляющего ПО от сторонних производителей относятся скептически. «VMware как никто другой понимает, что происходит на уровне гипервизора, – говорит Л. Кавальер. – Наши решения созданы в соответствии со спецификой слоя виртуализации («прослойки» между аппаратным уровнем и виртуальными

машинами), который обеспечивает корректное использование памяти, мобильность виртуальных машин, динамичное перераспределение ресурсов и т. д.».

Как правило, для управления всеми функциями VMware достаточно использования стандартных средств. Но периодически у заказчиков возникает необходимость интегрировать средства управления виртуальной инфраструктурой с основным ПО мониторинга и управления, которое используется в компании. «К примеру, – поясняет С. Лисняк, – ПО управления Veeam ONE Solution хорошо интегрируется с такими системами, как HP Operations или Microsoft System Center. В результате заказчик получает единую систему управления, которая охватывает всю ИТ-инфраструктуру предприятия». Того же мнения и А. Кучинский: «Лучше использовать фирменные средства управления. Только в этом случае гарантируется хороший уровень функциональности и надежности. Но можно говорить о применении инструментов комплексной автоматизации управления ИТ-инфраструктурой, где виртуализация – одна из составляющих».

Корпорация NEC предлагает собственное решение для управления виртуализованной средой. «Для предприятий и операторов связи имеет смысл использовать среду управления виртуализацией, способную работать с максимальным числом популярных гипервизоров, включая Xen, Hyper-V, VMware, –считает Николай Ильин («NEC Нева Коммуникационные Системы»). – Таким образом можно выбирать оптимальную среду под приложения и ОС. Например, система NEC Sigma Server Center поддерживает все вышеназванные среды и способна сама создавать, клонировать и переносить между физическими серверами виртуальные машины, созданные в различных средах виртуализации».

Интеграция технологий

Для управления нагрузкой в виртуализованных средах производители серверных систем и систем хранения обычно предоставляют собственные средства. В сущности, речь идет об интеграции средств управления физическими системами (серверами, системами хранения данных, сетевыми устройствами) с ПО управления виртуальными машинами. «Наверное, самое важное преимущество такой интеграции – это возможность определять предсбойные состояния серверов (оперативной памяти, жестких дисков, процессоров) и переносить виртуальные машины на «здоровые» системы», – полагает А. Светлаков.

С. Лисняк отмечает такие средства управления, как IBM Tivoli Dynamic Workload Broker, Dell Management Console (DMC), Fujitsu Resource Coordinator Virtual Edition (RCVE), HP Systems Insight Manager. Все они позволяют передавать рабочие нагрузки наиболее подходящим ресурсам в зависимости от требований нагрузок, бизнес-политик и доступности ресурсов, а также автоматически обнаруживать ресурсы, добавляемые в виртуальную инфраструктуру. Петр Марков также обращает внимание на программный комплекс Primergy ServerView Suite компании Fujitsu Technology Solutions, который, обладая функцией PDA (Pre-Failure Detection and Analysis), уведомляет центр управления виртуализованной средой о возможности аппаратного сбоя, благодаря чему виртуальные машины можно своевременно переместить на соседние серверы.

Упростить управление нагрузкой в виртуализованной среде призваны и решения виртуализации ввода-вывода и приоритизации трафика от виртуальных машин к системам хранения. Эту задачу со своих позиций решают процессорные технологии, виртуализационное ПО и технологии, предлагаемые производителями серверного и сетевого оборудования. Со стороны производителей процессоров это, например, технологии виртуализации сетевого ввода-вывода Intel VMDq и VMDc, AMD IOMMU и пр. Производители виртуализационных решений обеспечивают функционал виртуальных коммутаторов (так, базовый функционал виртуальных коммутаторов vSphere включает выставление гарантированной полосы пропускания, установку лимита полосы пропускания, настройку доли в потоке трафика при 100%-ной утилизации канала). Поставщики оборудования предлагают такие решения, как распределенный виртуальный программный коммутатор Cisco Nexus 1000V или технология VM-FEX, которая работает на базе виртуализованного сетевого адаптера Cisco VIC и поддерживает коммутацию трафика виртуальных машин на аппаратном уровне; конвергентные сетевые адаптеры и модули HP Virtual Connect FlexFabric, обеспечивающие подключение серверов к сетям как LAN, так и SAN без покупки дополнительных адаптеров Fiber Channel и коммутаторов, и целый ряд технологий других производителей.

Одной из самых интересных технологий в области виртуализации ввода-вывода Роман Ройфман («NetApp Россия и СНГ») считает так называемую one wire, когда через один порт передается как блочный трафик (FCoE, iSCSI), так и файловый (NFS, CIFS). Концепция one wire предполагает, что эта технология является сквозной – от сервера и сетевой среды до системы хранения данных. Реализована она, например, во FlexPod и других «коробочных» решениях для облачных вычислений.

■ ■ ■

Подводить итоги развития технологий виртуализации пока рано. Тем более что производители гипервизоров работают на этом поле не в одиночку, а технологии, предлагаемые поставщиками процессоров, серверного оборудования и программного обеспечения, движутся в сторону все более тесного взаимодействия и даже взаимозависимости. К тому же виртуализация на современном этапе охватывает не только вычислительные ресурсы, но и ресурсы хранения, и сетевые технологии – иначе говоря, ИТ-инфраструктуру в целом, выводя ее на концептуально иной уровень работы. ИКС

Не только кондиционер

Основные компоненты систем охлаждения ЦОДов

Петр РОНЖИН,
директор,
ООО «ВЕНТСПЕЦСТРОЙ»

Система охлаждения – это отнюдь не только холодильное оборудование; в ее состав входят и другие компоненты, особенности которых необходимо учитывать при проектировании ЦОДа.

Когда заходит разговор о системах охлаждения в ЦОДе, многие мои собеседники сразу же начинают говорить о чиллерах и кондиционерах той или иной фирмы. Хотя бы уже никому не надо объяснять, что такое «чиллер», и это радует. Еще больше радости приносит то, что сегодня большинство заказчиков понимают разницу между кондиционерами типа «сплит-система» и прецизионными кондиционерами. Безусловно, в сознании людей, которые строят, эксплуатируют, обслуживают дата-центры и пользуются их услугами, за последние два-три года произошел качественный скачок. И если раньше словосочетание «система охлаждения» воспринималось буквально как «прецизионные кондиционеры», то теперь специалисты, умудренные порой негативным опытом, рассматривают это понятие гораздо шире.

Да, кондиционеры, холодильные машины или другие источники холода по-прежнему остаются основными элементами систем охлаждения. Но как организм человека не сводится только к сердцу и легким (хотя это важнейшие его составляющие), так и холодильное оборудование, каким бы оно не было хорошим и эффективным, – это еще не система охлаждения. Более того, забыв или не уделив должного внимания другим элементам системы, мы сильно рискуем получить «колосса на глиняных ногах», который может рухнуть в любую секунду. И даже если последствия недоработанности решения в целом не будут катастрофическими, система окажется крайне неэффективной. А поскольку по потреблению электроэнергии системы охлаждения дата-центров стоят на втором месте после непосредственно полезной ИТ-нагрузки, непроработанная система охлаждения сильно снизит эффективность всего ЦОДа.

Разберемся, из чего состоит система охлаждения ЦОДа, и попробуем сформулировать, на что следует обратить внимание. Прежде всего отметим, что сейчас в ЦОДах используют разные варианты систем охлаждения. На страницах «ИКС» мы рассматривали их классификацию, достоинства и недостатки той или иной схемы*. Настало время более подробно остановиться на компонентах технических решений.

Прецизионные кондиционеры DX

В состав классического варианта системы охлаждения – решения на базе прецизионных кондиционеров с непосредственным расширением (DX) – входит следующее:

1) прецизионные кондиционеры (внутренние блоки) с подачей холодного воздуха вниз и забором теплого воздуха сверху;

2) конденсаторы с воздушным охлаждением (наружных блоков);

3) низкотемпературные комплекты;

4) трубопроводы для жидкого и газообразного фреона;

5) пароувлажнители;

6) трубопроводы подвода воды для пароувлажнителей;

7) трубопроводы отвода конденсата (дренажной системы);

8) гидроизоляция и защита от протечек;

9) фальшпольное пространство;

10) перфорированные панели фальшпола для подачи воздуха в «холодные» коридоры;

11) «холодные» коридоры;

12) «горячие» коридоры;

13) пространство над стойками или воздуховодами для удаления горячего воздуха;

14) система подпора (приточно-вытяжная вентиляция);

15) система электропитания кондиционеров;

16) система управления, мониторинга и диспетчеризации.

Как видно из перечисленного списка, состав самой простой системы охлаждения уже тянет на полтора десятка позиций. Отметим, что пункты списка 5–16 входят и в состав систем охлаждения других типов, поэтому в дальнейшем, характеризуя отдельные системы, мы будем говорить только об «индивидуальных» их компонентах.

Итак, на что же следует обратить внимание при проектировании и строительстве системы охлаждения ЦОДа?

Прецизионные кондиционеры должны не только обладать необходимой холодопроизводительностью в киловаттах, но и обеспечивать соответствующий стойкам расход воздуха и его напор, чтобы преодолеть аэродинамическое сопротивление фальшпольного пространства, перфорированных панелей, стоечного оборудования и воздуховодов. Исходя из этого, высота фальшпола должна быть строго рассчитана, чтобы обеспечить беспрепятственное прохождение воздуха с учетом проложенных кабельных систем, трубопроводов, лотков и т. п. К выбору перфорированных панелей фальшпола стоит подойти с особой тщательностью – они могут оказаться «бутылочным горлышком» системы охлаждения. В своей практике обследования проблемных ЦОДов мы не раз сталкивались с тем, что прекрасная работа кондиционерного оборудования была «помножена на ноль» из-за того, что перфорированные панели в «холодных» коридорах не способны были пропустить необходимое количество воздуха.

Конденсаторы воздушного охлаждения должны соответствовать по производительности внутренним блокам, а самое главное – они должны быть подобраны для работы при экстремальных (максимально высоких) температурах, которые возможны для района размещения дата-центра. Кроме того, существует еще ряд оговоренных производителями оборудования специфических требований, касающихся взаимного расположения внутренних и наружных блоков. Для российских климатических условий прецизионные кондиционеры должны в обязательном порядке оснащаться низкотемпературными комплектами, позволяющими работать при самых низких температурах, когда-либо наблюдавшихся в данной местности.

Отдельных слов заслуживают трубопроводы для газообразного фреона. Существует перечень очень жестких требований к проектированию и монтажу фреонопроводов. Они должны иметь определенное расчетом сечение, быть прочными и герметичными. В современных системах давление опрессовки может составлять 50 бар! Трубопроводы должны быть хорошо теплоизолированы, так как температура медной трубы на выходе компрессора достигает 60–70°C, и иметь небольшой уклон в сторону движения фреона для обеспечения циркуляции масла по контуру. Если наружные и внутренние блоки значительно разнесены по высоте, необходимо предусмотреть специальные маслоподъемные петли. Я не зря так подробно останавливаюсь на этом вопросе, потому что не раз сталкивался с непониманием в этом вопросе: до начала монтажа многие заказчики не вполне представляют себе, что такое фреоновый трубопровод, думая, что его так же легко проложить, как тонюсенький кабель.

«Холодные» и «горячие» коридоры должны быть изолированы друг от друга. Этому вопросу за последнее время было посвящено множество публикаций, доказывающих, что таким нехитрым и недорогим способом можно существенно повысить эффективность работы системы охлаждения.

Пространство над стойками (в ряде случаев применяются воздуховоды для удаления горячего воздуха) играет примерно ту же роль, что и фальшпольное пространство. Эта одна из составляющих контура циркуляции воздуха, о которой не стоит забывать.

Особое внимание надо уделить электропитанию кондиционеров. Для бесперебойной работы дата-центра с рассматриваемым техническим решением системы охлаждения требуется организовать питание наружных и внутренних блоков от ИБП. Причем ИБП должен обеспечивать пуски компрессоров, которые характеризуются высокими значениями пусковых токов.

Система подпора (приточно-вытяжной вентиляции) является отдельной инженерной системой дата-центра.

---

* См. «ИКС» 2010: № 3, с. 80; №5, с. 78; №7-8, с. 70; «ИКС» 2011: №3, с. 76.

Но не зная ее вклада в общее тепловыделение, нельзя рассчитать суммарную холодопроизводительность системы охлаждения. Кроме того, неправильное расположение дефлекторов приточной вентиляции может исказить показания датчиков температур, расположенных в серверном помещении, что приведет к неадекватной работе системы охлаждения.

Теперь, чтобы получить «полноценную» систему охлаждения, остается совсем немного: автоматизировать систему, организовать ее диспетчеризацию, грамотно подвести воду для пароувлажнителей, предусмотреть дренажные трубопроводы, а при необходимости и конденсатные насосы (они должны выдерживать высокие температуры, так как из увлажнителей периодически сливается горячая вода), систему сигнализации об утечках воды, гидроизоляцию пола и т.п. Только проработав в комплексе весь круг вопросов, можно с уверенностью сказать, что система охлаждения ЦОДа будет работоспособной в любой ситуации.

Мы рассмотрели самый простой случай организации системы охлаждения. Как будет изменяться система в других случаях?

Прецизионные кондиционеры DX с водяными конденсаторами и фрикулингом

В этом варианте состав системы охлаждения, помимо типовых компонентов (пункты 5–16 из предыдущего раздела), таков:

- прецизионные кондиционеры (внутренние блоки) с дополнительным теплообменником фрикулинга;
- сухие градирни (наружные блоки);
- трубопроводы холодоносителя;
- гидравлический модуль.

Прецизионные кондиционеры с дополнительным теплообменником фрикулинга в теплое время года охлаждают воздух за счет кипения фреона в основном теплообменнике, так называемом испарителе. В холодное время года используется фрикулинг – холодоноситель, охлажденный в сухих градирнях, поступает для охлаждения в дополнительный теплообменник. Фреоновый контур, а значит, и компрессор, зимой можно полностью выключать.

Сердце данной системы охлаждения – это гидравлический модуль, который должен обеспечить циркуляцию холодоносителя по «кровеносной системе», трубопроводам. Гидравлический модуль, в свою очередь, состоит из основных и резервных насосов, запорно-регулирующей арматуры, обратных клапанов, фильтров, расширительного бака для компенсации изменения объема холодоносителя при разных температурах. Модуль соединяется трубами с кондиционерами и сухими градирнями.

Наиболее распространенная ошибка заказчиков при подготовке технического задания на данную систему охлаждения – не предусматриваются площади для размещения гидравлического модуля. К сожалению, все перечисленное выше требует достаточно много места не только для размещения, но и для обслуживания.

Система электропитания в данном случае должна предусматривать питание от ИБП не только кондиционеров и градирен, но и оборудования гидравлического модуля.

Чиллеры и прецизионные кондиционеры на холодоносителе

В состав таких систем, работающих на холодоносителе, помимо типовых компонентов (пункты 5–16 первого списка), входят:

- прецизионные кондиционеры (внутренние блоки);
- чиллеры;
- трубопроводы холодоносителя;
- гидравлический модуль;
- бак-аккумулятор.

Гидравлический модуль, аналогичный тому, который описан выше, должен обеспечивать циркуляцию холодоносителя от чиллеров к прецизионным кондиционерам и обратно. Главное отличие данной гидравлической схемы состоит в том, что все кондиционеры и чиллеры связаны трубопроводами холодоносителя в единую сеть, посредством которой должны включаться в работу резервные кондиционеры и чиллеры. Однако в дата-центрах класса Tier III и IV для обеспечения необходимого уровня доступности предусматривается несколько независимых гидравлических контуров, объединяющих группы чиллеров и кондиционеров. Более того, резервируются и сами трубопроводы. При проектировании систем охлаждения подобных ЦОДов главную трудность составляет не охлаждение серверного оборудования в штатном режиме, а поддержание высокого уровня доступности сервиса вне зависимости от различного рода обстоятельств.

Бак-аккумулятор является простым, но очень эффективным средством бесперебойного холодоснабжения при авариях систем основного электропитания. Его емкость рассчитывается исходя из времени, необходимого для перехода на резервное питание, запуска и выхода чиллеров на рабочий режим. В принципе, чем больше его объем, тем лучше. Ограничения «сверху» здесь диктуются здравым смыслом, а также стоимостью и возможностями площадки и несущих конструкций.

Система электропитания должна обеспечивать переход на резервное питание чиллеров, кондиционеров, насосов и т. п., но насосы, запорно-регулирующая арматура, кондиционеры и системы управления должны иметь питание от ИБП.

Чиллеры и межстоечные кондиционеры на холодоносителе

По составу эти системы в основном аналогичны предыдущему типу, поэтому остановимся только на различиях.

Сильная сторона внутрирядной системы кондиционирования – отсутствие фальшполов, перфорированных панелей и т. д. Контур циркуляции воздуха гораздо проще: «горячий» коридор – кондиционеры – «холодный» коридор – серверные стойки. Для эффективной работы системы кондиционирования необходимо проработать вопросы изоляции (перекрытия) «холодных» или «горячих» коридоров и «заглушения» незанятых серверами мест в стойках.

В силу архитектуры внутрирядного кондиционирования серьезные проблемы часто создает подвод холодоносителя к кондиционерам и отвод конденсата, так как в большинстве случаев фальшпол отсутствует или его высота не позволяет подвести трубопроводы снизу. Поэтому трубные системы приходится проектировать и монтировать таким образом, чтобы исключить затопление серверов холодоносителем при разгерметизации гидравлического контура.

Стойки с интегрированными модулями охлаждения

Это самое простое решение с точки зрения организации воздушных потоков, так как и серверное оборудование, и охладитель находятся внутри шкафа.

В зависимости от того, что используется, холодоноситель или фреон, проектируется трубопроводная часть и уличные подсистемы (чиллеры или наружные блоки). Принципы их проработки остаются такими же, как и в описанных выше случаях.

Заказчикам, которые предполагают строить свой дата-центр на базе охлаждаемых шкафов, следует уделить особое внимание резервированию серверных мощностей, потому что обычно теплообменник модуля охлаждения не резервируется (есть только резервные вентиляторы) и при его разгерметизации шкаф остается без охлаждения. Выход из данной ситуации – оснащение серверного шкафа двумя модулями охлаждения, но при этом сильно ухудшаются массогабаритные показатели, сводя на нет все изящество и кажущуюся компактность данного решения.

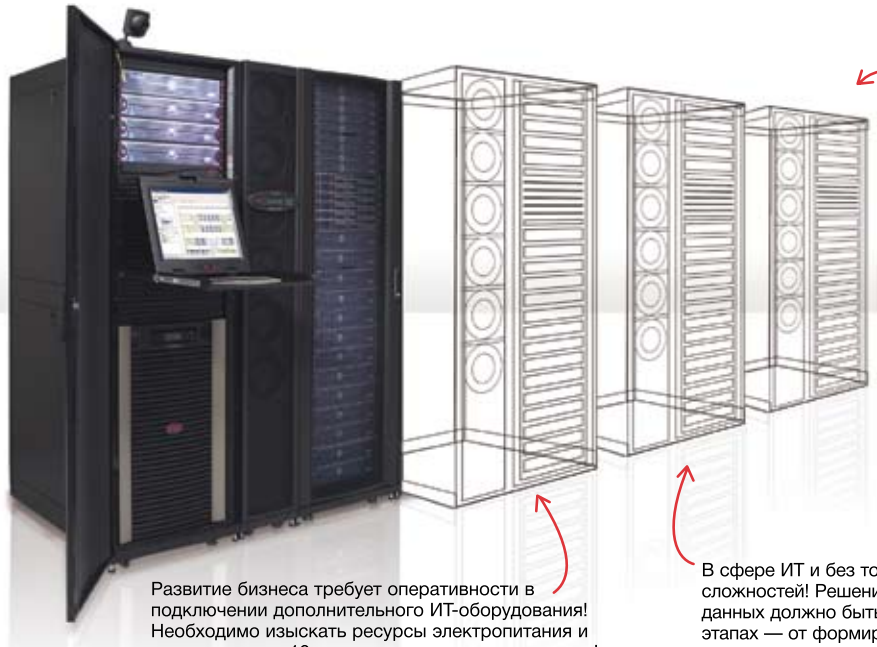
KyotoCooling

Название в данном случае вводит в заблуждение. KyotoCooling – это не холодильное оборудование, а сумма технологий, в том числе охлаждения, которые минимизируют энергопотребление дата-центров, что приводит к уменьшению эмиссии парниковых газов в соответствии с Киотскими соглашениями.

Эффективность охлаждения с помощью KyotoCooling напрямую связана с архитектурой дата-центра. Если вы собираетесь использовать KyotoCooling, сразу откажитесь от мысли приспособить под дата-центр какие-то пустующие площади – в 95% случаев они вам не подойдут. Но решение очень хорошее, если дата-центр будет строиться с чистого листа. Тогда вы сможете нормально разместить охлаждающие модули с роторным рекуператором, обеспечить подвод воздуха к серверному залу и возврат горячего воздуха. Основное внимание и время при проектировании такой системы охлаждения будет уделяться проектированию воздушного контура. При кажущейся простоте (нет труб, высокого давления, холодоносителя) обеспечить нормальную циркуляцию воздуха без образования застойных зон и местного перегрева оборудования – задача непростая, посильная только высококвалифицированным специалистам.

■ ■ ■

Надеюсь, что эта статья вооружит читателей определенными познаниями, так что при выборе системы охлаждения для дата-центра они смогут ориентироваться не только на строчку с указанием стоимости кондиционеров и чиллеров. ИКС



Центр обработки данных должен обслуживать пользователей круглые сутки без праздников и выходных! Необходимы системы электропитания и кондиционирования с резервированием, и чтобы в рамках выделенного бюджета!

Развитие бизнеса требует оперативности в подключении дополнительного ИТ-оборудования! Необходимо изыскать ресурсы электропитания и охлаждения на 10 новых серверов прямо сегодня!

В сфере ИТ и без того достаточно сложностей! Решение центра обработки данных должно быть простым на всех этапах — от формирования концепции до развертывания!

ЦОД не должен сдерживать рост бизнеса!

Только InfraStruxure предлагает тройное преимущество постоянной готовности круглые сутки, без праздников и выходных, высокой оперативности и экономии за счет эффективности

Инженерная архитектура InfraStruxure нового поколения

Центр обработки данных должен служить компании опорой в росте — будь то удвоение продаж или численности персонала — а не становиться препятствием для ее развития. Однако слишком часто бизнес испытывает ограничения ресурсов систем инженерной инфраструктуры. Найдется ли в стойках место для дополнительных серверов? Хватит ли электрической мощности новым ИТ-системам? APC by Schneider Electric удалось решить эти проблемы с помощью проверенной практикой высокопроизводительной, масштабируемой и комплексной инженерной архитектуры ЦОДа InfraStruxure.

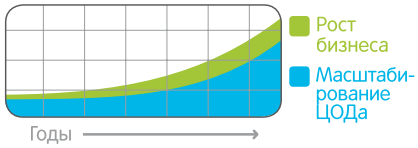
Центры обработки данных InfraStruxure — опора бизнеса!

Мы называем центры обработки данных, построенные на основе инженерной архитектуры InfraStruxure, опорой бизнеса. Что это значит? Все очень просто. ЦОД можно назвать опорой бизнеса, когда он: находится в постоянной готовности круглые сутки без праздников и выходных; постоянно работает на наивысшем уровне характеристик; поспевает за стремительным ростом бизнеса; на каждом этапе — от проектирования до эксплуатации — выходит на все более высокие уровни эффективности использования энергии и способен развиваться в гармонии с основной деятельностью компании. Более того, модульная инженерная архитектура InfraStruxure позволяет спроектировать интегрированное решение, в точности соответствующее требованиям на сегодняшний день и легко адаптируемое к их изменениям в будущем.

Тройное преимущество InfraStruxure

InfraStruxure предлагает тройное преимущество качественного превосходства: высочайший уровень готовности, простоту и оперативность адаптации к изменениям требований бизнеса и экономию за счет эффективного использования энергии. Как можно быть лучшей «опорой бизнеса», не обеспечивая качество, скорость и экономию одновременно?

InfraStruxure



Центры обработки данных InfraStruxure — опора бизнеса!

- Готовность: безостановочная работа круглые сутки без праздников и выходных благодаря лучшим в своем классе системам электропитания ответственного оборудования с модульными блоками распределения питания, системам охлаждения с теплообменниками, максимально приближенным к источникам тепла, а также ПО контроля и моделирования изменений параметров инженерных систем
- Оперативность: простота развертывания инженерной инфраструктуры в сжатые сроки. Все компоненты системы спроектированы с учетом совместной работы, а архитектура в целом рассчитана на любые, самые высокие темпы роста бизнеса.
- Эффективность: благодаря передовым конструктивным решениям, включая трехступенчатые инверторы ИБП и вентиляторы систем кондиционирования с переменной скоростью вращения, достигается настоящая эффективность использования и экономия энергии.
- Управляемость: управляющее ПО InfraStruxure Management Software позволяет отслеживать и управлять свободными ресурсами и уровнем резервирования систем электропитания и охлаждения, а также свободным пространством в стойках для оптимального использования ресурсов инженерной инфраструктуры центра обработки данных.
- Гибкость: начиная с совместимости шкафов с ИТ-оборудованием любых производителей до полной масштабируемости по электропитанию и отводу тепла.

Загрузите БЕСПЛАТНО информационные статьи APC в течение 30 дней, ответьте правильно на вопросы и получите шанс выиграть планшетный компьютер iPad!

Зайдите на сайт www.apc.com/promo и введите код 93237t

APC™
by Schneider Electric

Пусть ваша сеть не угрожает бизнесу

Дмитрий ЮФЕРОВ,
консультант по сетевой безопасности, Landata

Угрозы безопасности несет в себе не Интернет как таковой, а бесконтрольность в использовании его ресурсов. Поэтому основной задачей на сегодня является восстановление контроля над сетью компании.

Доступ в Интернет стал в наше время такой же неотъемлемой частью рабочего места, как телефон или канцелярские принадлежности. Однако Сеть за последние годы превратилась в рассадник вирусов, шпионских программ и прочего вредоносного кода.

Большинство заражений и атак происходит сегодня при использовании сетевых приложений. И в этом плане такой инструмент защиты сети, как межсетевой экран, уже не может ничего противопоставить атакам. Сетевые приложения за последние 15 лет шагнули далеко вперед, а межсетевые экраны принципиально не изменились. Более того, в последнее время появилось множество приложений, способных «обманывать» системы безопасности (работать по нестандартным портам, строить шифрованные туннели и т.д.).

Дисбаланс в развитии сетевых приложений и систем безопасности породил множество «решений-помощников», призванных закрывать дыры в безопасности обычного межсетевого экрана. Это прокси-серверы и IPS- системы, сетевые антивирусы и средства URL-фильтрации, веб-шлюзы и системы защиты от утечки конфиденциальных данных (DLP). Каждая из этих систем решает проблему лишь частично, а использовать их все одновременно, во-первых, дорого, а во-вторых, вносит в работу сети такую задержку, что работа сотрудников превращается в истинное мучение.

Устройства типа «все в одном», или UTM объединяют множество различных «помощников» межсетевых экранов в одном корпусе. Такие устройства экономят электроэнергию и место в стойке, но проблема производительности остается нерешенной – трафик сканируется в каждом блоке заново, так что задержка остается недопустимо высокой.

Межсетевые экраны нового поколения

Новой тенденцией контроля безопасности сетевой инфраструктуры стали межсетевые экраны, в которых все операции выполняются за один проход трафика. Сессия не сканируется каждый раз заново, и это в разы уменьшает сетевую задержку. К тому же эти устройства имеют многопроцессорную архитектуру с большим объемом оперативной памяти, что значительно уменьшает время выполнения таких ресурсоемких операций, как антивирусная обработка и контроль утечек конфиденциальной информации.

Один из самых ярких представителей семейства межсетевых экранов нового поколения – система компании Palo Alto Networks, основанной Ниром Зуком (в середине 90-х именно он разработал технологию контроля состояния соединений – stateful inspection, которая до сих пор лежит в основе работы любого межсетевого экрана).

Комплексные системы Palo Alto, используя сигнатурный и поведенческий анализ, применяют политики безопасности непосредственно к сетевым приложениям и пользователям служб каталогов. Это позволяет разрешить, заблокировать или ограничить функционал приложения даже в случае подмены стандартных портов, а возможность дешифрации SSL-соединений исключает использование шифрованных туннелей для обхода системы безопасности. Еще одной особенностью систем безопасности Palo Alto является механизм их настройки: при включении устройство показывает список всех приложений, работающих в сети, а администратор уже сам решает, какие политики применить к выявленным приложениям. Дополнительно в однопроходной архитектуре Palo Alto реализован функционал сетевого антивируса, IPS, URL-фильтрации и DLP.

Ниже мы покажем, как в Palo Alto реализована защита от основных опасностей Интернета.

Нецелевое использование рабочего времени

Сотрудники даже самых серьезных компаний часто тратят свое рабочее время на веб-почту, игры, просмотр видео, общение в социальных сетях – эта проблема остро стоит перед работодателями по всему миру. Системы безопасности Palo Alto позволяют отслеживать, какими сетевыми приложениями пользуется сотрудник (по количеству сессий, объему загруженных данных и т.д.). Администратор может разрешить или запретить как клиент-серверное, так и любое из распознаваемых приложений: например, ограничить просмотр видеороликов или запретить присоединение к любой файлообменной сети (BitTorrent, eMule, Kazaa).

Иногда администратору системы безопасности не нужно запрещать приложение целиком, достаточно лишь ограничить небезопасный функционал (например, передачу файлов в ICQ, в веб-почте или передачу управления рабочим столом администратору WebEx). К примеру, ограничение функции комментирования в сети «ВКонтакте» уменьшает расход времени на это приложение в 10 раз.

Сетевые угрозы

Интернет несет в себе множество угроз для жизнедеятельности компаний: от увеличения потребления трафика до проникновения вирусных программ в локальную сеть и несанкционированного доступа к корпоративным данным.

В Palo Alto имеется функционал сетевого антивируса и системы предотвращения вторжений. В ходе независимого тестирования компанией NSS Labs IPS-система Palo Alto отразила 93,4% сетевых атак.

Обход систем безопасности

Даже в сети, в которой установлены стандартные средства защиты, как правило, остаются лазейки, позволяющие обойти политики безопасности компании.

Подмена портов. Многие сетевые приложения умеют выходить в Интернет через нестандартные порты. Например, в настройках ICQ можно поменять порт, а в Skype или BitTorrent заложена возможность сканировать открытые порты автоматически. Тот факт, что практически в любом межсетевом экране открыты порты 80 и 443, делает невозможным запрет приложений peer-to-peer стандартными средствами.

Межсетевые экраны нового поколения Palo Alto сегодня распознают более 1300 различных приложений. Таким образом, если администратор применяет политику «запретить BitTorrent», это приложение полностью запрещается в сети, даже если пользователь пытается обмануть систему безопасности, меняя стандартные или используя динамические порты.

Построение шифрованных туннелей. Для обхода системы безопасности используется и шифрование SSL (протокол HTTPs). Пользователь ставит на рабочий компьютер клиент (например, PingFU), который открывает шифрованное SSL-соединение с внешним сервером. Внутри такого соединения можно передавать сетевой трафик любого запрещенного приложения, начиная от ICQ и заканчивая онлайн-играми. Обычный межсетевой экран не может «смотреть внутрь» SSL-трафика и по умолчанию разрешает все шифрованные передачи.

В библиотеке Palo Alto есть и PingFU, и другие приложения, шифрующие пользовательский трафик (Hotspot Shield, Bypass, HTTP-tunnel и т.д.). Таким образом, устройства Palo Alto способны различать легальные и нелегальные SSL-соединения. Запретив в сети шифрующие приложения, администратор исключает возможность обхода системы безопасности при помощи туннелей.

Утечка конфиденциальной информации через веб-почту. Поскольку все соединения с внешней веб-почтой (mail.ru, rambler.ru и т.д.) шифруются, этот неконтролируемый канал также часто используется при утечках конфиденциальной информации.

В Palo Alto имеется настраиваемая функция дешифрации SSL-трафика, что позволяет «заглянуть» в передаваемые почтовые сообщения. С помощью встроенного функционала защиты от утечки информации можно запретить передачу конкретных типов файлов (известные офисные приложения, шифрованные документы Microsoft Office и архивы), а также запретить передачу файлов с определенным содержимым (например, с номерами кредитных карт или содержащие слова «Конфиденциально», «ДСП» и т.д.).

Веб-анонимизаторы. Существует целый класс специализированных сайтов для обхода систем безопасности. Например, сайт https://webvpn.org/, организуя шифрованное соединение HTTPs, перенаправляет запрос пользователя на любой адрес в Интернете, даже если этот ресурс запрещен администратором в сети. На главной странице сайта владельцы без тени смущения пишут: «Анонимайзер, предлагаемый вам, поможет посетить любой сайт, минуя запреты, наложенные руководством или системным администратором вашей фирмы».

Palo Alto, во-первых, может закрыть URL-категорию «веб-анонимизаторы» целиком. При попытке перехода на подобный сайт пользователь получит предупреждение, что все его действия записываются в лог, или сообщение, что доступ на данный сайт запрещен политиками компании. Во-вторых, механизм дешифрации SSL позволяет вскрыть шифрованное соединение и применить политики компании к передаваемому контенту, даже если пользователь пытается его скрыть.

Это далеко не полный перечень лазеек, используемых для обхода обычных межсетевых экранов, работа которых основана на анализе порта TCP/UDP и IP-адреса пакета. Но здесь важно, что системы безопасности Palo Alto применяют политики безопасности не к портам, а **к приложениям**; не к IP-адресам, а **к пользователям служб каталогов** (Active Directory и др.). Такой подход позволяет закрыть присущие обычным межсетевым экранам «дыры» в безопасности.

Дополнительный функционал

При интеграции со службами каталогов (AD, Novell eDirectory, OpenLDAP) Palo Alto позволяет применять политики безопасности к конкретным пользователям и группам (например, «разрешить использовать Skype Иванову И.И.» или «Запретить доступ к приложению odnoklassniki группе Бухгалтерия с 9:00 до 18:00»). Данный функционал является базовым и не требует дополнительных подписок или установки дополнительных устройств.

Интеграция со службами каталогов в совокупности с механизмом распознания сетевых приложений позволяет применять политики качества обслуживания (QoS) к конкретным пользователям и сетевым сервисам. Например, группе «Менеджеры» для работы с приложением SharePoint можно выделить большую полосу пропускания, а для приложений Gmail и ICQ для той же группы ограничить скорость соединения.

Оперировать категориями «пользователь» и «приложение» можно также при маршрутизации трафика (функционал Policy Based Forwarding – PBF). Palo Alto позволяет, например, направить трафик бизнес-приложений по дорогому выделенному каналу, а развлекательных приложений – по более дешевому Интернет-соединению.

Как выбрать лучшее?

Все больше компаний полностью переводят обеспечение безопасности сети на межсетевые экраны нового поколения или используют их в дополнение к классическим решениям. В сфере информационной безопасности существует устойчивая тенденция смещения контроля в сторону уровня приложений, соответственно большинство производителей заявляют о том, что их устройства способны контролировать работу всех сетевых приложений. Лучшим критерием выбора в этой ситуации может стать собственноручное тестирование в собственной инфраструктуре. Компания Palo Alto Networks предоставляет свои устройства на тестирование; установка и настройка системы занимает всего 15 мин. Возможна работа в пассивном режиме, что исключает нарушение работы сети при неправильной конфигурации устройства. Такое тестирование позволит понять, что происходит в сети: какие приложения используются, какие атаки, вирусы, шпионское ПО в ней зафиксированы, использует ли кто-то тактики обхода систем безопасности, передачу конфиденциальной информации или потенциально опасные приложения. А дальше – решать вам.

5-10-15... Сколько киловатт на стойку нужно в ЦОДе?

Спор о том, какую энергомощность подавать в стойку, начался с появлением первого ЦОДа, и до сих пор однозначного решения нет.

Андрей ПАВЛОВ,
генеральный директор
компании «ДатаДом»

Попробуем разобраться в сути проблемы. Во-первых, определимся, у кого ответ на вопрос «сколько вешать в граммах» может вызвать затруднения. По опыту можно сказать, что заказчики корпоративных ЦОДов с той или иной долей уверенности могут определить свою потребность в мощности на основании собственной же статистики и прогнозов развития вычислительной инфраструктуры предприятия. В данном случае вопрос скорее в выбранной ИТ-стратегии, в параметрах помещения под ЦОД и тенденциях производства вычислительной техники.

Сложнее ситуация с операторами коммерческих дата-центров. Как угадать, что потребует рынок через год, два, четыре? На наш взгляд, есть простой алгоритм выбора решения. В условиях конкуренции и рыночных отношений покупатель голосует рублем. При размещении оборудования в аутсорсинговом ЦОДе для заказчика в большинстве случаев нет разницы, будет ли размещено 20 кВт его вычислительной техники в одной стойке или в четырех, стоящих рядом. На практике с точки зрения топологии размещения вычислительной техники в ЦОДе «не все равно» бывает только в случае таких систем, как суперкомпьютеры и кластеры, связность которых имеет первостепенное значение, и телекоммуникационные решения, трассы которых имеют определенную, зачастую ограниченную длину. Исходя из этого предположения, необходимо просто посчитать все капитальные и операционные затраты на одну стойку (исключая энергетику) и определить, по какой цене оператор коммерческого ЦОДа сможет предложить свои услуги клиенту в том или ином случае.

Возможны варианты

Разберем три потенциальных варианта дата-центра:

1) с классической технологией «холодных» и «горячих» коридоров с допустимой нагрузкой 5 кВт на стойку и раздачей воздуха из-под фальшпола (рис. 1);

Рис. 1. Вариант 1: ЦОД из 200 стоек – 5 кВт на стойку

Рис. 2. Вариант 2: ЦОД из 100 стоек – 10 кВт на стойку

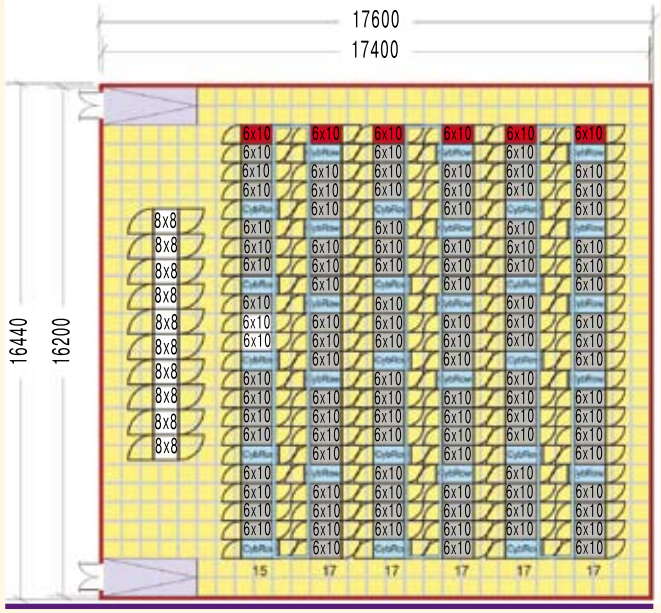
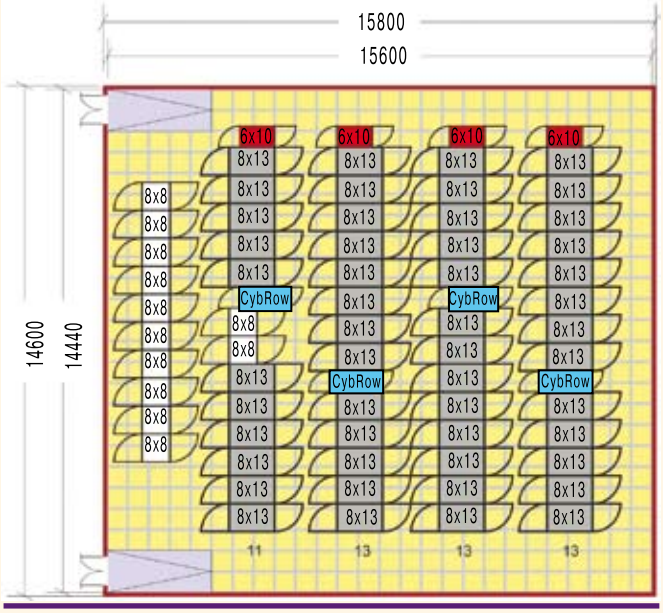


Рис. 3. Вариант 3: ЦОД из 50 стоек – 20 кВт на стойку



2) с аналогичной технологией «горячих» и «холодных» коридоров, но с закрытым «холодным» коридором, с межрядными кондиционерами и допустимой нагрузкой 10 кВт на стойку (рис. 2);

3) с закрытыми водоохлаждаемыми стойками и допустимой нагрузкой 20 кВт на стойку (рис. 3).

Для приведения этих вариантов к единому знаменателю условимся, что мы рассматриваем ЦОД на 1000 кВт общего бесперебойного энергопотребления. Исходя из полученных данных, мы сможем для каждого варианта посчитать удельную стоимость строительства одной стойки и удельную стоимость владения.

На приведенных планировках показаны активные и коммутационные стойки, а также внутренние блоки системы кондиционирования (в случае стоек 20 кВт внутренние блоки кондиционирования размещены в самой стойке). Мы не берем в расчет площади, занимаемые ИБП, дизель-генераторной установкой, ГРЩ и чиллерами, так как для всех трех случаев они будут примерно одинаковыми. Точно так же в расчете капитальных затрат на строительство при сравнении вариантов можно не учитывать стоимости данных инженерных систем, но мы все же приведем ориентировочную стоимость, исходя из средней удельной цены в 20 тыс. евро за одну стойку в ЦОДе.

Существенно будут различаться затраты на строительство для самих монтажных стоек, внутренних блоков системы кондиционирования, системы газового пожаротушения и фальшпола.

При расчете операционных затрат основное различие будет в стоимости аренды помещений. Фонд оплаты труда, цена электроэнергии и расходы на техническое обслуживание инженерных систем будут отличаться незначительно и не внесут весомый вклад в разницу в стоимости этих трех вариантов. Тем не менее в расчете мы сделаем некоторую поправку на бóльшую эффективность систем с межрядным кондиционированием и водоохлаждаемыми стойками.

Для стоек 5 кВт при размере стойки 600×1000 мм (таково среднее значение для коммерческого ЦОДа) площадь помещения под размещение двухсот стоек составляет примерно 29,4×15,6 = 460 кв. м, а в пересчете на одно стойкоместо выходит около 2,3 кв. м. Это хорошо коррелирует с эмпирическими цифрами 2–2,5 кв. м на стойку (в зависимости от размера ЦОДа) при расчете по традиционной схеме холодоснабжения.

Для стоек 10 кВт путем аналогичных расчетов получаем площадь 2,8 кв. м под один монтажный шкаф. Для стоек 20 кВт под один монтажный шкаф требуется примерно 4,5 кв. м.

Беспристрастные цифры

Теперь приступим к расчетам. В примере 1 в зале расположено 15 кондиционеров, и если принять, что систему холодоснабжения мы строим по схеме N+1, то активных кондиционеров будет 14 штук, с мощностью 80 кВт явной холодопроизводительности. Таким образом, мы учитываем небольшой запас по холодоснабжению – около 10%. Также учтем в расчете 200 стоек габаритами 600×1000 мм и высотой 42U. Соответственно потребуется 460 кв. м фальшпола высотой примерно в 50 см.

В примере 2 в зале мы расположим 100 стоек габаритами 600×1000 мм и высотой 42U. Необходимо будет также смонтировать конструкции «холодных» коридоров и установить 30 межрядных кондиционеров полной холодопроизводительностью порядка 40 кВт, что соответствует приблизительно 36 кВт явной холодопроизводительности. И в данном случае у нас получается запас системы кондиционирования около 10%.

В третьем случае мы устанавливаем 50 водяных стоек, каждая из которых может снять с оборудования до 20 кВт тепла, а также четыре резервных шкафных кондиционера, отводящих тепловую энергию, которая выделяется водоохлаждаемыми стойками, и резервирующих ситуацию выхода из строя одной стойки при автоматическом раскрытии ее дверей.

Ориентировочные цены на перечисленное выше оборудование и монтаж приведены в табл. 1.

Данный расчет не претендует на статус абсолютной истины, но он четко отражает основную тенденцию – полная стоимость владения одной высоконагруженной стойкой больше стоимости владения традиционной стойкой 5 кВт пропорционально разнице в электрической нагрузке на них. Заказчику при выборе того или иного варианта необходимо провести детальный расчет всех возможностей в рамках конкретного проекта и на основании этого расчета принимать решение о стратегии развития.

А что на практике?

Опрос, проведенный среди московских игроков рынка ЦОДов, выявил, что в большинстве случаев клиенту достаточно 5–6 кВт на стойку, и даже если он хочет установить оборудование с большим энергопотреблением, фактически данное оборудование расходует не более 70% от заявленной мощности.

Реальные данные о количестве стоек с разным энергопотреблением, полученные у операторов ЦОДов, сопоставлены в табл. 2. Данные приведены с учетом достаточно плотной установки серверного оборудования в стойках – до 35 одноюнитовых серверов и установки блейд-серверов до четырех корзин в одну стойку.

Очевидно, что с развитием облачных вычислений и распространением виртуализации плотность энергопотребления стоек будет расти, но в данный момент стойки с энергопотреблением до 7 кВт являются самыми востребованными. К тому же 7 кВт – это граничное значение, максимум, который при нормальном функционировании оборудования можно снять с использованием традиционной схемы холодоснабжения.

Если же в коммерческом ЦОДе появляется клиент, желающий разместить высоконагруженную стойку, можно установить такую стойку в ряд менее нагруженных, что не слишком существенно повлияет на общий теплообмен ЦОДа, либо разделить данное оборудование на несколько частей, что, как видно из нашего расчета, с экономической точки зрения будет равноэффективно его установке в ЦОДе с возможностью большего среднего теплосъема с одной стойки.

Парадоксальный итог

Исходя из проделанных расчетов, можно однозначно сказать, что на сегодня вполне достаточно строить коммерческие ЦОДы с потреблением до 7 кВт на стойку, что позволит в 90% случаев разместить клиентское оборудование в одной стойке и при этом иметь возможность предоставлять клиентам с высоконагруженным оборудованием ценовую политику не хуже, чем в

Табл. 1. Расчет капитальных и операционных расходов для трех вариантов ЦОДов

	Вариант 1		Вариант 2		Вариант 3	
	Количество	Цена, тыс. евро	Количество	Цена, тыс. евро	Количество	Цена, тыс. евро
Капитальные вложения						
Стойки	200 штук	160	100 штук + коридор	100	50 штук	1350
Кондиционеры	14 штук	350	30 штук	690	4 штуки	92
Фальшпол	460 кв. м	55,2	280 кв. м	36,4	225 кв. м	27
Газ	1600 куб. м	192	1100 куб. м	143	700 куб. м	91
Остальные системы		3250		3250		3250
ИТОГО		4007,2		4219,4		4810,0
На одну стойку		20,036		42,194		96,200
Операционные затраты						
Электричество		1314		1287,72		1278,96
Аренда		138		84		67,5
ФОТ		442,70345		442,70345		442,70345
Техобслуживание		400		400		400
ИТОГО в год		2294,70345		2214,42345		2189,16345
Расходы оператора ЦОДа на одну стойку в год		11,47352		22,14423		43,78327
Расходы оператора ЦОДа на одну стойку в месяц		956,13 евро		1845,35 евро		3648,61 евро
Цена для заказчика за 1 стойку в месяц		1300 евро		2600 евро		5200 евро
Срок окупаемости		4,9 года		4,7 года		5,2 года

Уменьшение затрат на содержание ЦОД и снижение негативного воздействия на экологию.

Высокий КПД ИБП Eaton 9395 и уникальные технологии энергоэффективной архитектуры устройства позволяют значительно уменьшить расходы при эксплуатации ЦОД. Благодаря инновационному дизайну Eaton 9395 и использованию современных экологичных материалов, подлежащих вторичной переработке, снижается негативное воздействие на окружающую среду и расходы на последующую утилизацию. Компактные размеры и малый вес ИБП упрощают его транспортировку и инсталляцию.
Возможность фронтального подключения и обслуживания сводит к минимуму расходы на установку и экономит ценное пространство серверных комнат.

An Eaton Green Solution

EATON
Powering Business Worldwide

www.eaton.ru/ups

Табл. 2. Распределение стоек по энергопотреблению (по данным операторов ЦОДов)

STOREDATA		LOGOL		SAFEDATA	
3–4 кВт	10%	До 5,5 кВт	80%	До 5 кВт	90%
5–7 кВт	80%	До 10 кВт	15%	7–10 кВт	10%
10–12 кВт	10%	Свыше 10 кВт	5%		

ЦОДах с теплосъемом на одну стойку в 20 кВт, при иных вариантах размещения данного оборудования.

Несомненно, на выбор того или иного решения в значительной степени влияют доступные для строительства ЦОДа площади. И если заказчик ограничен в площадях, вероятнее всего, имеет смысл повышать средний теплосъем со стойки, но тенденция развития вычислительной техники такова, что средние значения в 20 кВт на стойку могут быть достигнуты к тому времени, когда инженерное оборудование конкретного ЦОДа необходимо будет полностью менять.

Единственный негативный аспект ЦОДа с низким потреблением на одну стойку – в том, что при недостаточной наполняемости ЦОДа на этапе начальных продаж экономические параметры будут несколько хуже из-за простоя большего количества площадей, взятых в аренду.

Основные выводы таковы: выбирая между площадками под коммерческий ЦОД при определенном бюджете строительства, необходимо учитывать, что разница в экономической эффективности дата-центра с высоконагруженными и малонагруженными стойками может оказаться не столь большой, а вот спрос на стойки в 10–15–20 кВт еще недостаточно велик, чтобы делать на него ставку. ИКС

Ждать ли 100 Гбит/с по меди?

В современных ЦОДах, где протяженность кабельных линий невелика, оптические системы теряют свое основное преимущество – широкополосную «дальнобойность». Но сможет ли СКС на основе симметричных кабельных трактов поддерживать передачу 100-гигабитного потока данных?

Андрей СЕМЕНОВ, директор по развитию «АйТи-СКС»

Владимир РАДЧЕНКО, аспирант Санкт-Петербургского университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Современные информационные системы (ИС) предприятий на физическом уровне в подавляющем большинстве случаев реализованы на основе структурированной кабельной системы (СКС). Стремительное развитие вычислительной техники, рост числа ее потребителей и расширение областей использования предъявляют все новые требования к СКС, и одно из них – увеличение предельной пропускной способности кабельных трактов.

Согласно действующим и перспективным нормативным документам возможно построение структурированной проводки с использованием симметричных и оптических кабелей. При создании кабельной системы основной объем ресурсов направляется на реализацию ее нижнего абонентского уровня (горизонтальной подсистемы в случае офисной СКС). В этой области (в первую очередь из соображений экономического характера) доминируют решения, основанные на симметричном кабеле. Наращивать пропускную способность медножильных кабельных трактов до бесконечности невозможно, а значит, рано или поздно потребуется переходить на новую разновидность кабельных систем.

В настоящее время преемник медножильных трактов фактически известен – это оптические линии. Линии связи в ИС отличаются длительным сроком эксплуатации. В силу этого вполне оправданным выглядит предложение о переходе «на опережение», т. е. уже сейчас, не дожидаясь окончательного морального устаревания электропроводных кабелей.

Задача выбора типа среды передачи с учетом ее перспективы сложна тем, что носит многокритериальный характер. Однако именно многокритериальность позволяет упростить ее решение, по крайней мере в первом приближении. В рамках такой стратегии вполне допустимо вычленить в проблеме главные влияющие факторы и проанализировать каждый из них в отдельности, с последующим выводом уже по всей совокупности полученных результатов. Далее мы воспользуемся именно таким подходом.

Фокусная область применения

Среднестатистический пользователь ИС не в состоянии адекватно, по крайней мере в течение длительного времени, воспринимать информацию, поступаю-

щую к нему со скоростью выше нескольких десятков мегабит в секунду. Это означает, что если рассматривать ИС и основных потребителей ее ресурсов в комплексе, т. е. в форме известной системы человек – машина, то фактором, ограничивающим пропускную способность системы, будет первое звено.

С учетом имеющихся ограничений фокусной областью применения сверхвысокоскоростных трактов станут те составляющие ИС, в которых такие ограничения принципиально отсутствуют: там, где функционируют системы машина – машина. Это магистрали крупных СКС и линии связи ЦОДов. В последних высокоскоростные линии используются для связи серверов с коммутаторами различного уровня и накопителями систем массовой памяти.

Превалирующее значение в свете проблемы, вынесенной в заголовок, будут иметь именно ЦОДы. Этому в первую очередь способствует предельно ограниченное пространство, на котором развертывается ЦОД даже крупного масштаба. В результате средняя протяженность тракта значительно сокращается (с 40 м в офисных системах до менее чем 30 м), т.е. оптическая техника теряет свое главное преимущество – широкополосную «дальнобойность». Одновременно существенно снижается острота проблемы гальванической развязки приемника и передатчика на разных концах.

Разработки элементной базы

В создании техники нового поколения заметную роль играет наличие некоторого задела. В качестве прототипа основного компонента 100-гигабитных симметричных трактов могут быть использованы так называемые мультимедийные кабели, довольно широко представленные на рынке. Достаточно часто для их обозначения пользуются термином «кабель категории 8», хотя категория с таким номером не фигурирует даже в проектах известных нормативных документов.

В области разъемов хороший задел образуют соединители типа Tera и их аналоги с квадрантным расположением пар контактов. Определенную роль в этом вопросе играет их форма, удобная с точки зрения построения коммутационного оборудования, в том числе индивидуальных розеток. Немаловажное значение имеет возможность размещения каждой такой пары контактов в отдельной экранирующей камере, очень эффективной с точки зрения подавления переходных помех.

Стоимость

При прочих равных условиях по затратам на реализацию в случае небольшой протяженности электропроводные линии принципиально превосходят оптические. Тому есть две основные причины: во-первых, в электропроводных линиях отсутствует дополнительная пара преобразования электрического сигнала в оптический и обратно (соответственно на входе и выходе линии). Во-вторых, при скоростях передачи в 40 и 100 Гбит/с структура электропроводных и оптических линий оказывается предельно сходной, так как в их основе лежит схема параллельной передачи.

В 40- и 100-гигабитных оптических линиях СКС из соображений некоторого улучшения стоимостных параметров решения в целом используют дорогостоящие многомодовые световоды категорий OM3 и OM4, причем для создания каждого из субканалов всегда привлекается пара волокон (в симметричных трактах можно ограничиться всего одной парой). Стоимость одного такого волокна по крайней мере соизмерима со стоимостью витой пары категорий 7a и выше, которые могут быть использованы в составе медножильного 40- и 100-гигабитного тракта.

Технические возможности реализации

Сама возможность передачи информационных потоков по медножильным трактам со скоростями 100 Гбит/с определяется их теоретической пропускной способностью. Для симметричных трактов расчет этого параметра упрощается из-за того, что в условиях преобладающего влияния переходной помехи отношение сигнал/шум не зависит от уровня сигнала, а сам шум носит аддитивный характер. Кроме того, некоррелированный характер сигналов, передаваемых по отдельным витым парам и предварительно подвергнутых процедурам скремблирования на передающем конце, позволяет считать шум близким к белому. Таким образом, для оценки пропускной способности можно воспользоваться теорией Шеннона.

Результаты конкретных расчетов показывают, что по крайней мере в первом приближении многочисленные источники шумов, снижающие качество информационного сигнала на входе приемника в симметричном тракте, можно заменить единственным эквивалентным источником. Тогда анализ шумовой составляющей сводится к определению шумов на ближнем конце, а остальные источники учитываются соответствующим поправочным коэффициентом.

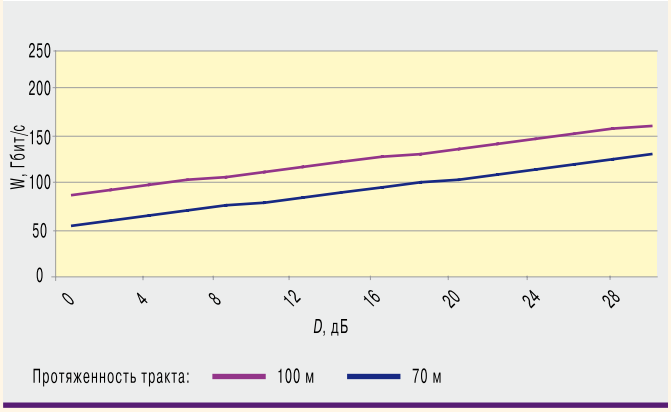
Обработка фирменных спецификаций кабелей категории 8 показала, что описание частотной зависимости PS-NEXT в форме, используемой в действующих и известных перспективных редакциях стандартов, дает очень большую ошибку расчета в сторону занижения пропускной способности *W*. Для ее уменьшения до приемлемого уровня целесообразно применить кусочно-линейную аппроксимацию следующего вида:

$$\text{PS-NEXT}(f) = \text{PS-NEXT0} \qquad f \le f_0$$
$$\text{PS-NEXT}(f) = \text{PS-NEXT0} - k \lg(f - f_0 + 1) \qquad f > f_0$$

где f – частота; f_0, МГц – некоторая критическая частота, при превышении которой начинается «завал» частотной характеристики переходного затухания на ближнем конце; k – крутизна падения частотной характеристики PS-NEXT на частотах выше f_0.

Особенностью аппроксимации является то, что при $k = 15$ и $f_0 = 1$ МГц она переходит в ту, которая используется в действующих нормативных документах, т.е. обеспечена необходимая общность.

Рис. 1. Теоретическая предельная пропускная способность тракта в зависимости от эффективности схемы подавления переходной помехи



Фактические значения параметров для некоторых кабелей, которые после определенного усовершенствования и/или даже обычной пересертификации могут быть задействованы для построения 100-гигабитных симметричных линий, приведены в таблице .

Частотную характеристику затухания как второго компонента, используемого при определении отношения сигнал/шум, вполне можно описать обычным образом.

Результаты расчетов пропускной способности с учетом наших предположений (см. рисунок) свидетельствуют о том, что современная техника СКС вполне обеспечивает решение задачи передачи 100-гигабитных информационных потоков на расстояние вплоть до 100 м с соответствующим эксплуатационным «запасом».

Еще одна важная особенность 100-гигабитных симметричных трактов состоит в том, что их необходимо рассматривать в комплексе с активным сетевым оборудованием. Дело в том, что переходное затухание даже у самых лучших образцов существующих кабелей недостаточно для получения требуемых параметров тракта. Как следствие, для улучшения отношения сигнал/шум на D дБ в обязательном порядке следует применять в приемниках сетевых интерфейсов подавители переходной помехи. Подобные блоки были впервые использованы в интерфейсах 1G Base-T, и за прошедшие почти полтора десятка лет их конструкция хорошо отработана в серийном производстве.

Некоторые параметры мультимедийных кабелей различных производителей

Производитель	PS-NEXT0, дБ	f_0, МГц	k	f_{max}, МГц
Kerpen (Германия)	107	350	11,9	1500
Datwyler (Швейцария)	100	350	6,2	1500
Draka (Норвегия)	112	100	6,6	1500
Nexans (Бельгия)	100	150	3,1	1000
Corning (Германия)	102	100	9,5	1500

Для получения окончательного ответа на вопрос о возможности передачи 100-гигабитного потока по симметричным кабельным трактам необходимо определить верхнюю граничную частоту $f_в$ линейного сигнала. Первичная оценка этого параметра выполняется исходя из следующих соображений. Для симметричных интерфейсов гигабитного диапазона скоростей с целью снижения верхней граничной частоты линейного сигнала используется многоуровневое кодирование вида PAMn, где n = 5 (4), 8, 16, 32 и т.д. Изменение схемы формирования линейного сигнала в интерфейсах новых типов нецелесообразно из-за сложностей обеспечения обратной совместимости с устройствами, функционирующими на более низких скоростях.

Симметричный тракт передачи строится по четырехканальной схеме, верхняя граничная частота входных цепей приемника может быть в два раза ниже значения fв. С учетом этих соображений находим $f_в$, решая уравнение $4 f_в \times m = 0{,}5 \times 160$ Гбит/с, откуда $f_в = 20/m$, где $m = \log_2 n$.

При умеренных значениях m получаем, что верхнюю граничную частоту $f_в$ спектра линейного сигнала не нужно поднимать намного выше значения 2 ГГц, которое в настоящее время уже достигнуто в ряде серийных образцов мультимедийных симметричных кабелей. Работы в этом направлении проводились в процессе адаптации СКС домашних сетей для поддержки систем спутникового телевидения; в частности, с 2007 г. такие кабели серийно выпускает французская компания Acome.

Потеря защищенности сигнала от теплового шума, которую принципиально невозможно устранить методами цифровой обработки, компенсируется увеличением мощности передатчика.

Итак, наши расчеты показывают, что у симметричных кабельных трактов СКС есть вполне конкретные перспективы использования для передачи сигналов сетевых интерфейсов локальных сетей со скоростями вплоть до 100 Гбит/с. Основной областью массового применения 100-гигабитного оборудования могут стать центры обработки данных, в классических СКС его перспективы заметно слабее.

Кабельные тракты 100-гигабитных СКС следует реализовать исключительно на полностью экранированных линейных и шнуровых кабелях со структурой F/FTP или SF/FTP и соответствующем коммутационном оборудовании. Применение неэкранированных изделий на таких скоростях при современном уровне техники не представляется возможным. Эффективность схем подавления переходных помех сетевых интерфейсов должна достигать примерно 23 дБ.

Частотный диапазон нормирования параметров 100-гигабитных симметричных кабелей необходимо расширить по крайней мере до 2–2,5 ГГц. ИКС

ИБП с повышенной энергоэффективностью

Eaton Ellipse ECO – семейство источников бесперебойного питания с топологией офлайн, предназначенных для защиты ПК, рабочих станций, офисных АТС и кассовых терминалов от пропадания, провалов и скачков напряжения. В линейку входят ИБП номинальной мощностью 500, 650, 800, 1200 и 1600 ВА.

Во всех моделях, за исключением самой младшей, имеется порт USB и реализована функция Eco-Control, которая автоматически отключает периферийные устройства при выключении основного оборудования, тем самым обеспечивая до 25% экономии электроэнергии. Эта функция активируется и настраивается с помощью ПО для управления электропитанием Eaton Intelligent Power Software (входит в комплект поставки).

Модели мощностью 500, 650 и 800 ВА оснащены четырьмя розетками Shuko (DIN)/ IEC, три из которых служат для резервного питания оборудования от батарей и для его защиты от скачков напряжения, а одна – только для защиты от скачков напряжения. В моделях мощностью 1200 и 1600 ВА четыре розетки с резервным питанием и защитой от скачков напряжения и еще четыре – только с защитой от скачков напряжения.

По уровню защиты нагрузки от скачков напряжения источники бесперебойного питания Ellipse ECO соответствуют стандарту IEC 61643-1. Во всех моделях предусмотрена защита информационных соединений: Ethernet- и телефонных линий.

В Ellipse ECO используются сменные герметичные свинцово-кислотные батареи, предусмотрен автоматический тест батарей. При необходимости их замены включается светодиодный индикатор и срабатывает звуковой сигнал. ИБП Ellipse ECO отличает эргономичный ультраплоский дизайн, они могут располагаться вертикально, горизонтально, устанавливаться в 19”-стойку или крепиться на стену.

Eaton: (495) 981-3770

ИБП для ЦОДов

Modulys Green Power – линейка модульных ИБП, предназначенных для виртуализованных ЦОДов и критически важного оборудования. Обладает горизонтально-вертикальной модульной структурой, поддерживающей динамическое изменение мощности от 20 до 240 кВА с шагом 20 кВА. Вертикальная модульная структура обеспечивает наращивание мощности до 120 кВА путем подключения к системе дополнительных силовых модулей (мощностью 20 кВА каждый). Горизонтальная модульная структура позволяет увеличить мощность до 240 кВА с помощью соединения двух модульных систем для параллельной работы. Характеристики отдельного модуля: входной коэффициент мощности – 0,99, THDi < 3%, искажения напряжения < 1%, КПД в режиме онлайн – до 96%, в экорежиме – до 98%.

Подключение и замена модулей могут осуществляться в «горячем» режиме. Эксплуатационную готовность системы также повышают наличие двух входов питания (от основной и вспомогательной сетей), регулировка скорости встроенного вентилятора и индивидуальный контроль эффективности воздушного охлаждения.

Возможны конфигурации с двумя типами аккумуляторных шкафов. Первый тип – модульный аккумуляторный шкаф с аккумуляторами малой емкости (до 9 Ач), которые объединяются в цепочки. Второй тип – аккумуляторный шкаф с батареями большой емкости (40 Ач).

ИБП Modulys Green Power имеют многоязычный графический ЖК-дисплей, светодиодную индикацию текущего состояния силовых модулей и встроенную систему дистанционного управления. SNMP-адаптер позволяет осуществлять мониторинг ИБП как обычного периферийного устройства. В случае появления аварийных сигналов адаптер отправляет SNMP-прерывания, мониторинг которых можно вести с помощью ПО управления сетью или через браузер. Также имеются встроенные интерфейс сухих контактов и цифровая система мониторинга параметров окружающей среды, контролирующая температуру

шкафа с ИТ-оборудованием, влажность и наличие аварийных сигналов.

Socomec: (495) 775-1985

Энергоэффективные ИБП

Delta Ultron DPS – это трехфазные ИБП двойного преобразования, с выпрямителем IGBT и трехкаскадным инвертором (TLI). Бестрансформаторная система Ultron DPS Series выпускается мощностью 200 кВА, поддерживается широкий диапазон входного напряжения. В параллель можно подключать до восьми таких устройств, выстраивая системы мощностью до 1,4 МВА (при резервировании N + 1). Параллельное резервирование ИБП Ultron DPS позволяет исключить простои и обеспечить соответствие стандарту TIA-942.

При работе в режиме онлайн КПД системы достигает 95,5% (при 40%-ной загрузке). Особенность Ultron DPS – запатентованная трехфазная топология PFC (Power factor correction), которая улучшает использование переключателей, уменьшает количество компонентов и облегчает мягкий запуск шины постоянного тока (DC-BUS). Входной коэффициент мощности > 99%, коэффициент гармонических искажений входного тока THDi < 3% при 50%-ной загрузке.

Доступ к ИБП организован спереди, что упрощает его обслуживание. Управление системы Ultron DPS полностью цифровое, с многоязычным интерфейсом.

Delta Electronics: (495) 644-3240

Ленточный накопитель четвертого поколения

IBM System Storage TS1140 представляет четвертое поколение систем хранения данных на магнитной ленте корпоративного уровня стандарта IBM 3592. Обеспечивает скорость передачи данных 250 Мбайт/с (650 Мбайт/с с учетом сжатия) и емкость 4 Тбайт (без сжатия), что позволяет сократить окно резервного копирования, количество необходимых картриджей и занимаемое библиотекой место.

По сравнению с системами стандарта LTO-5 (наиболее распространенными сейчас) TS1140 дает выигрыш в скорости в 1,8 раз, в емкости – в 2,8 раз.

Необходимая для корпоративных сред экономичность обеспечивается совместимостью с предыдущими поколениями: кроме возможности чтения и записи картриджей предыдущих поколений, устройство TS1140 поддерживает переформатирование существующих картриджей (с увеличением емкости и скорости).

Для увеличения эффективности записи осуществляется выбор одной из 12 скоростей записи в соответствии со скоростью потока (90–251 Мбайт/с) и технологии «виртуальной перемотки» (SkipSync, FastSync, Backhitchless Backspace). Высокая скорость поиска (12,4 м/с) и наличие каталога высокого разрешения обеспечивает быстрый доступ к данным.

TS1140 поддерживает подключение по двум путям FC 8 Гбит/с с переключением их при сбое. Обеспечивает поддержку всех распространенных корпоративных ОС и приложений.

IBM: (495) 775-8800

Беспроводной ADSL2+ модем-маршрутизатор

DGND3700 – DSL-шлюз для домашней сети, объединяющий в одном устройстве гигабитный двухдиапазонный модем ADSL2+ и усовершенствованную версию беспроводного маршрутизатора Netgear WNDR3700.

Покрытие и емкость сети увеличены благодаря одновременному использованию двух диапазонов 802.11n – 2,4 ГГц и 5 ГГц. DGND3700 оснащен двухъядерным процессором и двумя портами USB. Он поддерживает технологию Netgear ReadySHARE, что дает возможность превратить подключенные к USB-портам внешние жесткие диски в сетевые. Устройство оборудовано отдельным гигабитным портом Ethernet WAN для подключения к высокоскоростному модему кабельной или оптической сети.

DGND3700 позволяет назначать повышенный приоритет потокам видео, играм и другим мультимедийным приложениям, поддерживает создание гостевых сетей (обеспечивает гостям доступ в Интернет, не открывая им пароль от домашней сети). Для контроля потребления трафика имеется счетчик использования широкополосного канала.

Netgear: (495) 799-5610

Платформы поддержки комплектов
подключения сотовой связи и ШПД

образуют программные продукты производства компании «Петер-Сервис».

Биллинговая система (группа продуктов BIS) создает информацию о комплекте подключения сотовой связи, которая транслируется на сервер контроля балансов и управления услугами в режиме реального времени (продукт BRT). После покупки SIM-карты абонент сразу может совершить звонок, который регистрируется в BRT. Регистрация абонента у дилера происходит с помощью ПО, составляющего основу продукта SBMS_ACCOUNT. Регистрация платежа осуществляется с помощью системы приема платежей (продукт SBMS_PAYMENT). Обработка SMS и USSD производится через систему самообслуживания SCC. Информация о действиях абонента поступает в биллинговую систему, которая регистрирует активацию абонента и при необходимости осуществляет подключение недостающих услуг на коммутаторе с помощью продукта HEX (система управления телекоммуникационным оборудованием).

Комплект подключения к услугам ШПД представляет собой scratch-карту определенного номинала, с которой неразрывно связаны логин и пароль пользователя для входа в Интернет. В биллинговой системе заранее создается профиль потенциального потребителя услуг с балансом, равным номиналу карты. Информация о нем размещается в системе онлайн-контроля абонентов BRT и на сервере аутентификации/авторизации, в роли которого выступает продукт BRM. Отличие от мобильного комплекта заключается в том, что вместо номера телефона и SIM-карты для абонента запоминаются его будущие логин/пароль, которые хранятся в специально выделенном хранилище данных продукта GUP. В силу особенностей ШПД помимо идентификационных данных для каждого абонента сразу задаются технические характеристики подключения к сети (в частности, скорость доступа). При подключении абонента к Интернету учетные записи о потребленном объеме трафика поступают в систему, которая в режиме онлайн следит за тем, чтобы этот объем не превышал величину, предусмотренную номиналом карты доступа.

Решение для ШПД также позволяет организовать поддержку «виртуальных» комплектов подключения, т.е. комплектов, не имеющих физического представления и существующих только в биллинговой системе, с нулевым номиналом. Абонент мобильной связи, уже подключенный к сети оператора и зарегистрированный в сети самообслуживания (продукт SCC), может самостоятельно запросить комплект подключения к ШПД, указав в заявке сумму, которая может быть потрачена с его баланса на доступ к услугам ШПД. Такому абоненту выделяется «виртуальный» комплект, на балансе которого фиксируется заявленная сумма (соответственно на эту же сумму уменьшается мобильный баланс абонента).

«Петер-Сервис»: (812) 326-1299

Рис. 1. Платформа поддержки комплектов подключения сотовой связи

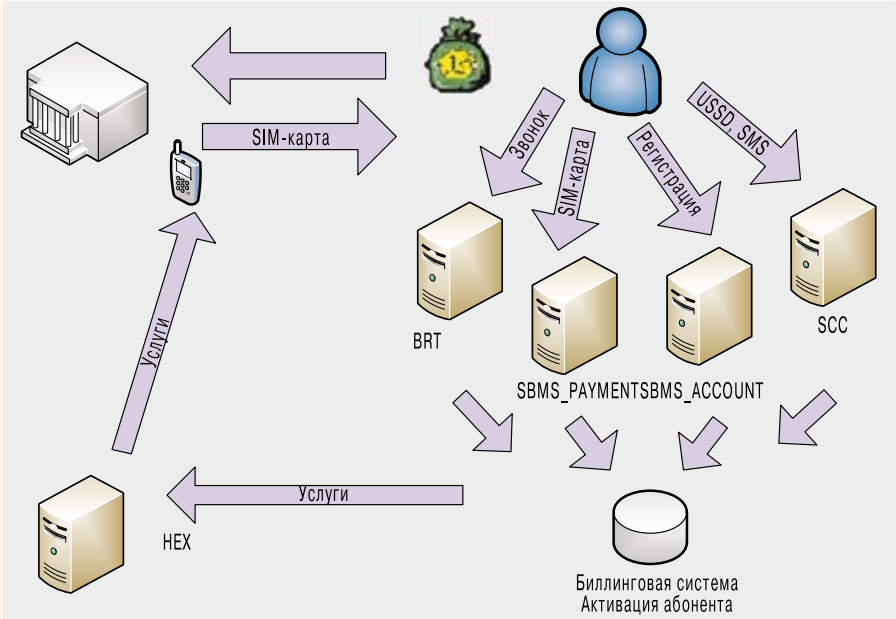
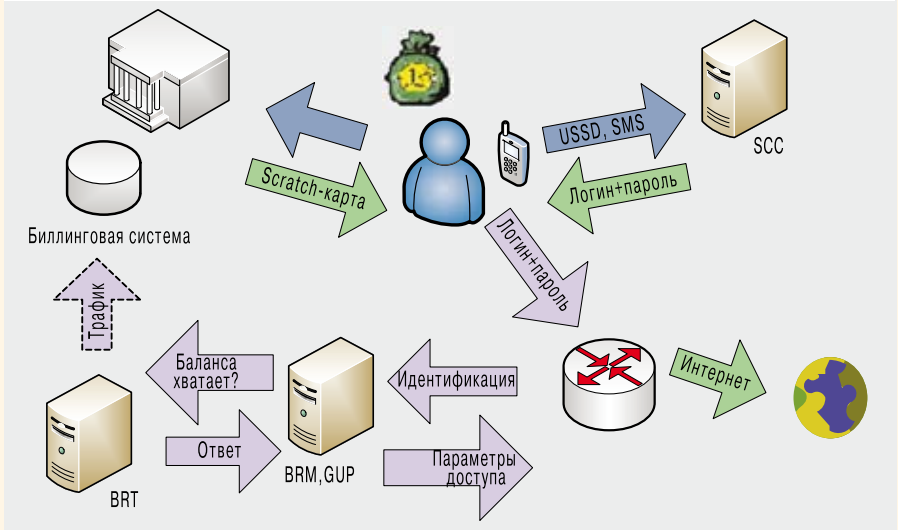


Рис. 2. Платформа поддержки комплектов подключения ШПД



Блог, еще раз блог!

Михаил ЕМЕЛЬЯННИКОВ

Банкомат с детектором лжи

>>>> Прочел про новые банкоматы со встроенными детекторами лжи.

Ужаснулся. Проверил календарь. Не 1 апреля. Огорчился.

А теперь по сути, и к слову для планирующих использовать «банкоматы с детекторами лжи». Принятие решения, порождающего юридические последствия для субъекта персональных данных на основании исключительно автоматизированной их обработки, запрещено ФЗ-152 «О персональных данных», если гражданин не дал письменное согласие на принятие такого решения.

Хорошо бы новому банкомату и письменное согласие у субъекта запрашивать.

Так рождаются сенсации

>>>> Позитивные изменения коснулись и борьбы с незаконным распространением баз данных, которые все эти годы спокойно продавались где угодно, а теперь стали объектом пристального внимания спецслужб. В ходе изъятия баз они активно осваивают возможности PR, предоставляемые Интернетом, а наши журналисты, как обычно, делают из любого маломальски интересного информационного повода «настоящую» сенсацию.

Итак, сенсация. 28 июня, в 10:43 портал Газета.ru огорошил страшным сообщением: «В Москве изъяты более 15 тысяч баз данных, содержащих гостайну». Для тех, кто хоть немного знаком с особенностями охраны государственной тайны, – это новость, сшибающая с ног. Джулиан Ассанж и его Wikileaks стоят рядом и плачут кровавыми слезами зависти к торгашам с радиорынков. 15 тысяч баз с государственной тайной! Такого в России и СССР не было никогда…

…Вот такую нашли журналисты государственную тайну – открытую и общедоступную.

Неужели все-таки услышали?

>>>> Первое совпадение всегда воспринимаешь как случайность. 13 июня запостил недоумение по поводу наличия независимо существующих проекта В.М.Резника и поручения Президента о разработке нового варианта закона «О персональных данных». Ровно на следующий день Дума стремительно выложила законопроект ко второму чтению с рекомендацией принять его 17 июня сразу и в целом. Но о пикантности ситуации задумались, похоже, не только в Думе. И 17 июня законопроект не только не слушали, но решили его не слушать на весенней сессии вообще.

Совпадение, наверное.

Затем 16 июня посомневался насчет эффективности принимаемых мер по борьбе с продажей баз данных о гражданах. И вот уже 25 июня СМИ сообщили о том, что на пресечение незаконной торговли нашими персданными поднялись не только МВД, Роскомнадзор и прокуратура, но и ФСБ, борьбу планируется развернуть не только на четырех московских рынках, но и по территории всей страны.

Опять совпадение – греет. Может, все-таки будем говорить? «Ищите и обрящете, стучите и отверзется вам». Не я это сказал.

комментировать

Владимир ЛИТВИНОВ

«Правое дело» нового «Ростелекома»

>>>> В конце июня состоялось годовое собрание объединенного «Ростелекома» по итогам работы за 2010 г. Должен сказать, что за прошедшие почти двадцать лет жизнедеятельности «Ростелекома» активность акционеров на собрании поменялась кардинальным образом. Концентрация акций в уникальном объеме около 3 млрд штук достигает все больших размеров («Связьинвест», ВЭБ и др.) и, как результат, на собрании отмечается снижение численности и активности акционеров. Думаю, что вместе с многочисленными журналистами и заглянувшими любопытствующими акционерами-пенсионерами присутствовало порядка 200 человек. Миноритарии теряют интерес к деятельности компании, не имея возможности влиять на ее работу. И, возможно, как результат, президент «Ростелекома» Провоторов, не сходя с рабочего места в президиуме, зачитал годовой отчет, который носил достаточно сжатый, поверхностный характер…

Некоторое оживление в зале вызвали выборы нового состава совета директоров. В начале собрания было озвучено обращение министра связи с отказом от участия в выборах в соответствии с последними инициативами Президента России на исключение высших госчиновников из участия в советах директоров акционерных компаний. И тем не менее министр Щеголев был избран – как нас заверили, миноритариями…

В результате намерений приватизации «Ростелекома» акции поднялись в цене на 25% и превысили планку 200 рублей за акцию, что и стало самым положительным событием в объединенном «Ростелекоме» с начала года.

комментировать

Спешите! Последняя вспышка деловой активности этим летом! Персональные данные, связистский чемпион, мошенничество с покупкой авиабилетов в Интернете, риски обладателей интеллектуальной собственности… Всё это в блогах на IKSMEDIA.RU.

Лев АЛАЕВ

Предупрежден – значит вооружен

>>>> Совсем недавно "Яндекс" запустил сервис по поиску авиабилетов. Однако в этой сфере сейчас активно действуют мошенники. Буквально на днях появился живой пострадавший :-(

...Итак, схема мошенничества. Преступник покупает авиабилет по данным чужой кредитной карты и передает данные электронного билета жертве. Жертва проверяет валидность брони и оплату либо на сайте одной из GDS (глобальные системы бронирования), либо позвонив по телефону в авиакомпанию. И только после этого переводит деньги мошенникам. У людей, знакомых с процессингом кредитных карт, может возникнуть вопрос: «А как же антифрод?». Имя на карте не совпадает с именем пассажира, транзакция подозрительная, должен сработать антифрод. Это легко обходится. Приобретается два авиабилета: один на имя жертвы, другой на имя владельца карты.

Откуда берутся данные чужих кредитных карт? Помимо классического воровства есть утечки целых баз данных карточек, которые продаются, в том числе через Интернет...

«Уже слышу крики правозащитников: «Нельзя никого обвинять без доказательств, это клевета». Нет проблем! Пусть подают на меня в суд», – делится со мной в разговоре основатель и руководитель сайта AviaSales Константин Калинов.

комментировать

Андрей СВИРИДЕНКО

Microsoft + Skype против Google и Apple

>>>> Покупка Skype – явный шаг Microsoft в сторону потребительского рынка, несмотря на огромное количество заверений Skype о большой доле корпоративных пользователей. Несмотря на все усилия Skype в сторону корпоративных клиентов, в этом вопросе она явно Microsoft не поможет. Технологически единственное, чего нет у Microsoft, – это технология p2p, но она и не востребована в корпорациях.

Сделка со Skype – это битва Microsoft против Google и Apple за desktop и мобильные платформы. Причем битва, в которой право голоса – у пользователя. Не у разработчика устройств, не у оператора связи, а совершенно конкретно – у абонента. Microsoft усилил свои позиции в ряду гигантов, которые обходят существующую цепочку телеком-услуг: вендор – оператор – абонент, предлагая коммуникационные сервисы напрямую миллионам абонентов. И мы не раз уже говорили о том, что российским операторам связи просто необходимо предлагать пользователям собственные конкурентоспособные сервисы – «Русский Скайп», аналогичные Skype, чтобы не только сохранить, а и усилить свои позиции на рынке.

600 млн пользователей Skype – это и есть главное объяснение, почему Microsoft их купил. И опять-таки, маркетинговая машина Microsoft способна усилить и ускорить замедлившуюся динамику развития Skype, а все это означает и дальнейшее падение голосовых доходов традиционных операторов связи.

Apple Facetime, Google Voice и теперь Microsoft Skype – все это деньги, проходящие мимо операторов.

комментировать

Геннадий ФОКИН

Страхование рисков правообладателей

>>>> Потребность в создании рынка услуг страхования интеллектуальной собственности обусловлена экономическими, правовыми и социальными факторами.

К ним, безусловно, можно отнести востребованность продуктов интеллектуального труда и развитие гражданского оборота интеллектуальной собственности; как следствие — увеличение количества неправомерного использования результатов интеллектуальной деятельности, влекущих за собой нарушение личных неимущественных и/или имущественных прав авторов и правообладателей, судебных споров правообладателей (с авторами, нарушителями, органами государственной власти), а также участившиеся случаи изъятия органами государственной власти материальных носителей, содержащих результаты интеллектуальной деятельности и средства индивидуализации, – например, нашумевший в свое время факт изъятия правоохранительными органами сотовых телефонов, принадлежащих салонам сотовой связи «Евросеть».

Причина, по которой страховщики «избегают» данного вида страхования, кроется в многообразии и «нетипичности» результатов интеллектуальной деятельности и исключительных прав на них (интеллектуальной собственности) как объекты гражданских прав, в незнании страховщиками специфики участия интеллектуальной собственности в гражданском обороте имущества, в сложности определения и отсутствии статистики страховых рисков, подтверждения стоимости страхуемого имущества, а также в существующих проблемах документального подтверждения не только прав на использование результатов интеллектуальной деятельности, но и самого охраняемого законом результата интеллектуальной деятельности, его достоинств, коммерческой значимости и выгод правообладателя.

комментировать

Реклама в номере

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 212; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:
127254, Москва,
Огородный пр-д, д. 5, стр. 3;
тел.: (495) 785-1490, 229-4978.

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка, д. 6/9/20, стр. 1;
тел.: (495) 921-1616.