Телеком растет вопреки рынку

С 15 октября по 13 ноября на отечественном фондовом рынке наблюдалась преимущественно «медвежья» динамика, обусловленная коррекционными настроениями на мировых инвестиционных площадках. При этом, несмотря на высокую волатильность, наблюдаемую на глобальных сырьевых площадках, нефть марки Brent показала небольшой прирост – на уровне 0,29%, до $76,32 за баррель.

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

Индекс ММВБ за рассматриваемый период снизился на 2,34%, до 1310,27 пункта, индекс РТС также продемонстрировал негативную динамику на уровне 1,23%, откатившись к уровню 1416,75 пункта. Вопреки общерыночной ситуации котировки акций телекоммуникационных компаний увеличили свою капитализацию. Так, отраслевой индекс «ММВБ Телекоммуникации» (MICEX TLC) за месяц увеличился на 3,91% (до 1615,27 пункта), индекс «РТС Телекоммуникации» (RTStl) – увеличился на 4,33% (до 172,87 пункта).

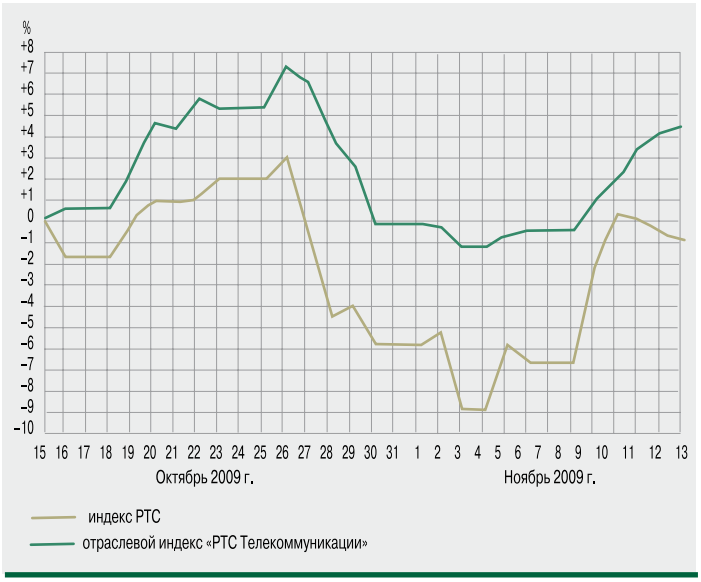
Основным генератором новостей в телекоммуникационном секторе, как и прежде, оказался «Связьинвест». С одной стороны, поступающая на рынок информация касалась внутрикорпоративного конфликта менеджмента данной компании, с другой – появились новые данные относительно реформирования телекоммуникационного холдинга.

Конфликт менеджмента «Связьинвеста» начался с письма (автором которого считается Леонид Рейман, председатель совета директоров компании), где были подвергнуты критике цели и задачи генерального директора Евгения Юрченко. Продолжением темы стала прошедшая в СМИ информация о том, что в ближайшее время возглавить совет директоров «Связьинвеста» может глава Минкомсвязи Игорь Щеголев, сместив на этом посту Леонида Реймана. Такая перестановка объясняется необходимостью изменения совета директоров, так как АФК «Система» перестанет в ближайшем будущем являться акционером компании и потеряет право выдвигать членов совета директоров. Несмотря на логичность назначения г-на Щеголева в «Связьинвест» с точки зрения расстановки властных сил, мы полагаем, что это событие может рассматриваться как ответ на критику, возможно, Леонидом Рейманом, генерального директора холдинга. Впрочем, мы не считаем, что это негативно скажется на эффективности работы самого холдинга и на его реформе.

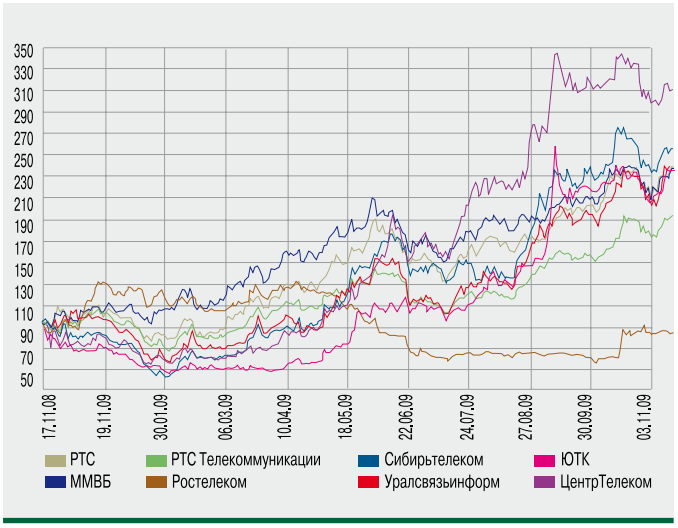
Касаясь темы реформирования «Связьинвеста», следует отметить информацию об обмене привилегированных акций МРК на обыкновенные акции «Ростелекома». Полагаем, что данная новость может подогреть интерес к «префам» последнего. При этом, вероятнее всего, дивидендные выплаты «нового» «Ростелекома» значительно вырастут на фоне неизменного количества его привилегированных акций. Вкратце также обозначим, что «КИТ Финанс» выдвинул альтернативный вариант реформы «Связьинвеста», который, однако, не был поддержан на надлежащем уровне – он чрезмерно сложен, долог, и, как результат, интересы государства могли пострадать за счет неподобающе низкой оценки самого «Связьинвеста» как имущественного вклада в «Ростелеком».

На этом фоне обыкновенные акции «Ростелекома» продемонстрировали существенный прирост: на ММВБ они подорожали на 30,73%, достигнув уровня 186,95 руб. Позитивной динамике бумаг компании не помешала даже плохая отчетность по МСФО за 1-е полугодие 2009 г.: выручка от основных услуг упала, расходы росли опережающими темпами, рентабельность по OIBDA снизилась до 17,5%, а чистая прибыль уменьшилась в 7 раз. Впрочем, инвесторы в акции «Ростелекома» вклады-

Динамика индексов и инструментов РТС



Динамика индексов РТС и телекоммуникационных компаний в период с 17 ноября 2008 г. по 3 ноября 2009 г.



ваются с расчетом на реформу «Связьинвеста», а дела у МРК идут вполне приемлемо.

Акции большинства межрегиональных компаний в течение месяца демонстрировали восходящую динамику. Основным поводом для этого стала информация о том, что тарифы МРК (а точнее, операторов, занимающих более 25% рынка) могут вырасти в отдаленном будущем. Возможное смягчение тарифного регулирования МРК способно привести к росту выручки практически всех компаний и сделать тарифы на услуги местной связи более справедливыми для операторов. На указанном фоне акции «ВолгаТелекома», «Северо-Западного Телекома», «Уралсвязьинформа» выросли на ММВБ на 10,12% (до 69,43 руб.), 5,68% (до 13,95 руб.) и 3,75% (до 0,775 руб.) соответственно. Акции «Дальсвязи» подорожали на 3,62% за акцию (до 92, 64 руб.), при этом основной корпоративной новостью стала отчетность компании за 9 месяцев 2009 г. по РСБУ. Основной бизнес оператора не принес сюрпризов по итогам работы трех кварталов – выручка незначительно выросла, а рентабельность практически не изменилась.

В минусе торговались акции «ЦентрТелекома», «Сибирьтелекома» и ЮТК, акции которых подешевели на 11% (до 14,15 руб.), 10,8% (до 1,024 руб.) и 0,95% (до 2,179 руб.) соответственно. Причиной снижения капитализации «ЦентрТелекома» стало вынесение предписания Федеральной антимонопольной службы о наложении в отношении оператора штрафа в размере 8,3 млн руб. за нарушение закона о конкуренции и подтверждение судом законности действий антимонопольщиков. Среди позитивных для «ЦентрТелекома» новостей можно выделить хорошую отчетность по РСБУ за 9 месяцев 2009 г., а также повышение долгосрочного кредитного рейтинга компании агентством S&P. Снижение стоимости акций «Сибирьтелекома» мы связываем с плохой отчетностью по РСБУ за 9 месяцев 2009 г., согласно которой чистая прибыль компании снизилась за период в полтора раза, до 1 млрд 737,2 млн руб. В свою очередь, снижение котировок ЮТК объясняется нейтральной отчетностью по РСБУ за 9 месяцев 2009 г. (чистая прибыль за 9 месяцев выросла на 10,7%, достигнув 1 млрд 313,38 млн руб., выручка увеличилась на 5%, до 16,2 млрд руб.), а также претензиями к компании со стороны ФАС за неконкурентные действия в отношении «ВымпелКома».

В мобильном сегменте наблюдался уверенный рост капитализации. Акции МТС подорожали на 3,95%, до 220,8 руб. Причины стабильности – в спокойной отчетности компании по US GAAP за 9 месяцев 2009 г.: выручка росла с запланированным темпом, рентабельность по OIBDA превысила прогноз, но доходы от ритейла значительно отстают от ожидаемых, а капитальные затраты за три квартала оказались выше докризисных трех кварталов прошлого года. Важным негативным моментом отчетности нам видится высокий уровень капитальных вложений МТС: по итогам кризисных 9 месяцев 2009 г. он составил $1,597 млрд, что на 3% выше чрезвычайно успешных 9 месяцев 2008 г. В свою очередь, интерес к акциям «ВымпелКома» на РТС был по-прежнему минимальным, что выразилось в отсутствии сделок на указанной бирже.

Акции АФК «Система» за месяц подорожали на 8,47%, до 20,5 руб. Основной причиной такой динамики, очевидно, стали заявления менеджмента компании относительно ожидаемого им двухзначного роста выручки на большинстве рынков присутствия. Также были озвучены планы «Системы» о продаже «Башнефти» контрольных пакетов предприятий Башкирского ТЭК на общую сумму более 41 млрд руб. Среди других корпоративных новостей можно отметить подтверждение S&P кредитных рейтингов МТС и «Системы». ИКС

Информация об обмене привилегированных акций МРК на обыкновенные акции «Ростелекома» может подогреть интерес к его «префам»

Опасные догмы анализа инвестиций

При экономическом анализе инвестиционных проектов на практике достаточно часто используется метод дисконтирования денежных потоков. Насколько корректно его применение?

Александр ЩЕРБАКОВ, ведущий бизнес-аналитик ЗАО «Бизнес Компьютер Центр», канд. техн. наук

Принятию решения об осуществлении того или иного инвестиционного проекта всегда предшествуют комплексный анализ основных проблем его реализации и оценка ожидаемых результатов. И если одной из главных целей проекта является извлечение прибыли, то непременно производится оценка его ключевых экономических показателей, среди которых должны быть:

- сгенерированная проектом чистая прибыль нарастающим итогом во времени;
- чистый денежный доход, под которым понимается сгенерированное проектом приращение денежных средств компании (сумма денежных потоков по проекту);
- срок окупаемости проекта, т.е. срок, по истечении которого величина чистого денежного дохода примет положительное значение;
- рентабельность инвестиций (как мерило их экономической эффективности) – отношение сгенерированной проектом чистой прибыли нарастающим итогом во времени к инвестициям.

Поскольку у любого инвестиционного проекта, нацеленного на извлечение прибыли, всегда есть банальная альтернатива, а именно «абсолютно безопасное» вложение имеющихся свободных денежных средств в банковский депозит, то каждого инвестора, естественно, интересует вопрос, какая из этих альтернатив предпочтительней.

Ответ может быть получен путем расчета следующих экономических показателей:

- срока, по истечении которого сумма наращенного возврата денежных средств от проекта (рассматриваемых в качестве средства накопления) превысит сумму денежного возврата от вложения в банк при текущей ставке депозита средств, требуемых для осуществления проекта. Назовем этот срок сроком достижения большей денежной возвратности проекта.
- Изменения во времени разницы между двумя указанными выше суммами возвратов денежных средств. Назовем этот показатель наращенным чистым денежным доходом.

Между тем практика непосредственного взаимодействия со многими хозяйствующими субъектами в России, в том числе компаниями телекоммуникационного сектора, показала, что при проведении экономического анализа инвестиционных проектов основное внимание уделяется трем другим экономическим показателям, опирающимся на метод дисконтирования денежных потоков, а именно:

- дисконтированному чистому денежному доходу, определяемому как сумма всех денежных потоков по проекту, приведенных в соответствие с канонами теории временной стоимости денег к моменту начала проекта с помощью ставки дисконтирования;
- дисконтированному сроку окупаемости проекта (т.е. сроку достижения положительного значения величины дисконтированного чистого денежного дохода);
- индексу рентабельности инвестиций.

Последний из этих показателей рассматривается как индикатор экономической эффективности инвестиционных проектов и определяется как отношение дисконтированного чистого денежного дохода по проекту к дисконтированной стоимости инвестиций.

При этом совершенно упускается из вида то обстоятельство, что получившая широкое распространение формула для вычисления величины дисконтированного чистого денежного дохода есть ни что иное, как математически преобразованное соотношение для определения разницы между суммой наращенных возвратов денежных средств от проекта и величиной денежного возврата от вложения средств, требуемых для осуществления проекта, в банковский депозит при допущении, что прибыль от такого вклада налогом не облагается.

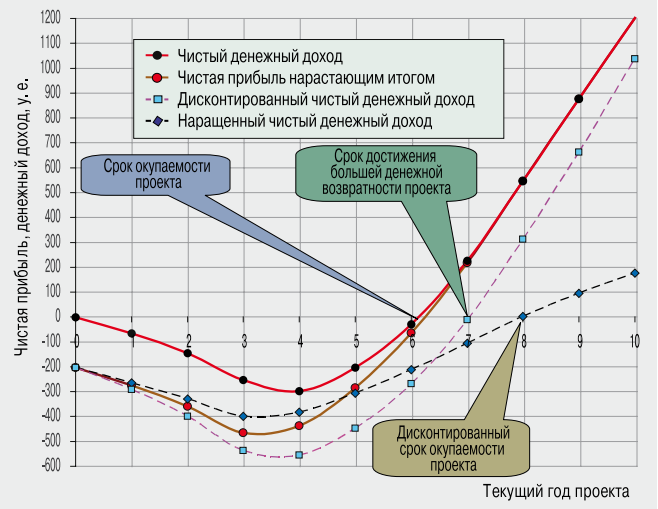
Как следствие, дисконтированный чистый денежный доход не дает адекватного представления ни о чистой прибыли по проекту, ни о приращении оборотных средств компании, сгенерированном проектом, ни тем более о разнице между суммой наращенных возвратов денежных средств от проекта и величиной денежного возврата от вложения средств, требуемых для осуществления проекта, в банковский депозит. А дисконтированный срок окупаемости искажает представление как об ожидаемом сроке окупаемости, так и о сроке достижения большей денежной возвратности проекта (рис. 1).

Это обстоятельство особенно наглядно проявляется тогда, когда инвестиционный проект предусматривает разнесение капитальных затрат во времени, а срок его окупаемости измеряется несколькими годами.

Использование же вместо рентабельности инвестиций индекса рентабельности приводит к существенному занижению оценки экономической эффективности проекта (рис. 2).

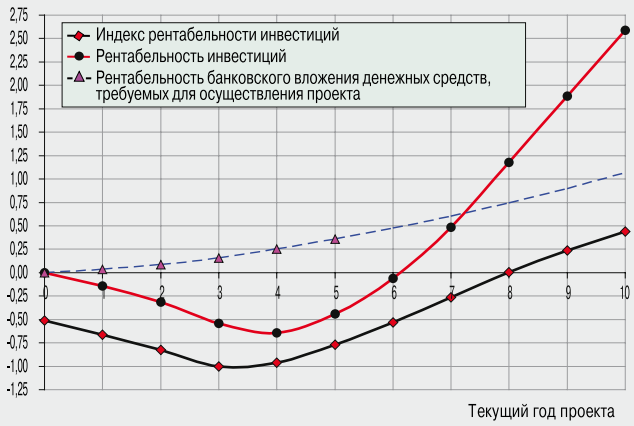
Относительно широко применяемой формулы для оценки дисконтированного чистого денежного дохода следует признать, что она была получена вовсе не для пересчета будущих денежных потоков по проекту в обратное временно́е измерение, как это часто интерпретируется, а для упрощения математических выкладок при определении (с некоторой погрешностью) срока достижения большей денежной возвратности проекта.

Рис. 1. Чистая прибыль и денежные доходы по проекту*



* Данные получены в результате анализа реального инвестиционного проекта в области телекоммуникаций.

Рис. 2. Изменение показателей экономической эффективности инвестиционного проекта*



* Данные получены в результате анализа реального инвестиционного проекта в области телекоммуникаций.

Погрешность вычисления срока достижения большей денежной возвратности проекта методом дисконтирования тем выше, чем больше срок окупаемости, выше ставка налога на прибыль и больше разница между ставками дисконтирования и банковского депозита.

Следует особо отметить, что величина дисконтированного чистого денежного дохода зависит от периода дискретизации исчисления и последующего дисконтирования денежных потоков, а само выражение для определения дисконтированного чистого денежного дохода, как результат математического преобразования исходной функции наращенного чистого денежного дохода, не имеет физического смысла (в прикладных науках, да и в самой мате-матике, преобразования функций достаточно часто используются для достижения конкретной цели. Например, прямое преобразование оператором обыкновенного дифференциального уравнения Лапласа не имеет никакого физического смысла, а служит лишь инструментом решения исходного уравнения).

В практической деятельности сосредоточение основного внимания на трех экономических показателях, опирающихся на метод дисконтирования денежных потоков, без должного понимания их сущности и очевидных недостатков зачастую приводит к следующему:

- отказу от реализации инвестиционного проекта в пользу, например, банковского размещения инвестиций;
- искусственному занижению оценки потребного объема инвестиций, что вынуждает подрядчиков либо работать себе в убыток, либо настаивать на снижении требований к проекту, либо вовсе отказаться от его выполнения;
- экономическим неудачам в осуществлении проекта в связи с некорректным выбором ценовой политики и др. ИКС

Организаторы

ГОД БЕЗОПАСНОГО ИНТЕРНЕТА В РОССИИ

издается с 1992 года ИКС www.iksmedia.ru

.RU Координационный центр национального домена сети Интернет

Партнеры

COMSTAR МГТС

Поддержка

CISCO

Осторожно: дети в Интернете!

Интернет, ставший глобальным информационным и социальным феноменом, вобрал в себя все достоинства и недостатки реального мира. Ведя ребенка по жизни и ограждая его от опасности, мы должны помнить и об угрозах, исходящих от Всемирной паутины. Безопасность Сети и ее пользователя – проблема государства, общества, родителей и тех, кто доставляет виртуальный мир в реальную жизнь человека.

Технические и организационные проблемы выстраивания барьеров на пути противоправного интернет-контента, вирусов и спама за круглым столом «Осторожно, дети в Интернете! Технологии безопасности по всему фронту», организованным Оргкомитетом по проведению Года безопасного Интернета в России, Координационным центром домена RU и журналом «ИКС» при партнерстве компаний «КОМСТАР-ОТС» и МГТС и поддержке Cisco, обсуждали:

Павел АНТОНОВ, технический консультант, **Cisco**
Евгений БЕСПАЛОВ, гендиректор, **Фонд «Дружественный Рунет»**
Максим БОБИН, вице-президент по правовым вопросам, **Mail.Ru**
Наталия МАКАРОВА, менеджер по развитию, **Фонд развития Интернет**
Мария МАЛЫШЕВА, заместитель начальника юридического отдела, **.masterhost**
Дмитрий МЕДВЕДЕВ, директор по информационным технологиям, **МГТС**
Юлия ОВЧИННИКОВА, член Совета **Координационного центра домена RU**, сопредседатель Оргкомитета Года безопасного Интернета;
Игорь ПОЛЯКОВ, гендиректор, **Центр анализа интернет-ресурсов (ЦАИР);**
Елена СЕРЕГИНА, директор по связям с общественностью, **Группа компаний «КОМСТАР-ОТС»;**
Андрей ЯРНЫХ, начальник отдела интернет-решений, **«Лаборатория Касперского».**

Круглый стол вела главный редактор журнала «ИнформКурьер-Связь» **Наталия КИЙ.**

Наталия КИЙ: Научить детей гигиене общения с виртуальным миром – новая задачка для родителей

Н. КИЙ: В теме «Дети в Интернете» сошлось несколько векторов. Во-первых, это тема общественного и государственного звучания. Во-вторых, это тема нашего телеком- и ИТ-сообщества. В-третьих, это тема личная, поскольку большинство из нас родители, которые должны привить своему ребенку не только привычку чистить зубы по утрам, но и научить его гигиене общения с виртуальным миром. Для начала: по данным исследования Symantec, в десятке самых популярных детских поисковых запросов фигурируют слова «секс» и «порнография».

Е. СЕРЕГИНА: Интернет открыл в наши дома двери и окна, через которые в семьи попадает не только хорошее, но, увы, и плохое тоже. В Группу «КОМСТАР-ОТС» входят два интернет-провайдера СТРИМ и МГТС. Мы понимаем, что Интернет не так безопасен для наших детей, как нам всем хотелось бы. Поэтому в рамках своей политики корпоративной социальной ответственности мы реализуем программу в сфере безопасного использования Интернета: поддерживаем горячую линию Фонда «Дружественный Рунет», проекты

Елена СЕРЕГИНА: Кроме технологических проблем фильтрации интернет-контента, есть и этические проблемы

Года безопасного Интернета в России, детский творческий конкурс «Интернешка», а во Всероссийском конкурсе дизайнерских и фоторабот «КРУПНЫМ ШРИФТОМ», посвященном социальной ответственности бизнеса, мы учредили специальную номинацию «Полезный Интернет. Безопасный Интернет». Мы готовы и к другим проектам и хотели бы обратиться к бизнесу и широкой общественности: безопасность детей в Интернете – это та тема, которую нужно поддерживать.

«ИКС»: Давайте определимся: какие угрозы, идущие из Интернета, наиболее опасны для детей?

Павел АНТОНОВ: Самое опасное, когда ребенок натыкается на неподобающий контент вне зависимости от своего желания

П. АНТОНОВ: Я бы выделил два класса угроз: вредоносный код, или вирусы, и неподобающий, вредный для психики детей контент. Хотя первый представляет опасность прежде всего для компьютера, но бывают случаи, когда после заражения ПК на экране появляются всплывающие окна, ведущие на порносайты, а за монитором может сидеть ребенок. Самое опасное, когда ребенок натыкается на такой контент вне зависимости от своего желания.

А. ЯРНЫХ: Дети – самые уязвимые пользователи Интернета, так как у них нет опыта противодействия вредоносному коду. Раньше мы могли говорить неопытным пользователям: не ходите на незнакомые сайты! Но сейчас угрозу могут представлять посещения даже, казалось бы, доверенных зон. Поэтому очень важно на самом раннем этапе приобщения к Сети рассказать детям, что Интернет является дружественным и открытым лишь в очень небольшой своей части, а в основном это довольно агрессивная среда, и важнейшим элементом защиты служит специальное ПО, без которого даже опытный пользователь окажется мишенью для атак злоумышленников.

Е. БЕСПАЛОВ: Есть и другие опасности. Они связаны с тем, что наши дети активно общаются в социальных сетях, причем далеко не всегда в детских, в чатах и других интернет-сервисах. Там они рискуют стать жертвами мошенников или людей, имеющих сексуальный интерес к детям. Но бывает и так, что дети, не зная основных правил правильного и безопасного поведения в Сети, могут сами нарушать те или иные законы.

М. БОБИН: Неподобающая информация распространяется не только через чаты, блоги, сервисы видео- и фотохостинга, но и через онлайновые компьютерные игры, где есть и текстовые, и голосовые чаты, которые вообще никак не контролируются, и там может происходить все что угодно.

Максим БОБИН: На любом из сервисов Mail.Ru есть кнопка «Пожаловаться модератору» и работает круглосуточная служба модерации

«ИКС»: Прежде чем попасть к человеку за компьютером, контент, как правило, проходит долгий путь. В его создании и доставке пользователям участвуют контент-провайдеры, интернет-регистраторы, хостинг-провайдеры, магистральные операторы, ISP. Что может сделать каждый из участников этой цепочки для защиты малолетних интернетчиков?

А. ЯРНЫХ: Мы считаем, что наиболее эффективный механизм противодействия угрозам – эшелонированная защита, установленная и на магистральных сетях, и у интернет-провайдеров, и на ПК пользователей. Такие многоуровневые фильтры в максимальной степени отсекают вредоносный контент. В наши средства комплексной защиты встроен и модуль «родительского контроля», который позволяет фильтровать контент и по возрастному, и по тематическим признакам.

Д. МЕДВЕДЕВ: Нам как оператору, предоставляющему ту самую магистраль, по которой наши чада попадают в Интернет, небезразлично, что там происходит. Согласен, что для защиты абонентов от негативной информации из сети Интернет нужна эшелонированная оборона Но эта оборона не должна ограничивать права пользователей. Для этого мы еще в 2008 г. создали услугу «Родительский контроль», позволяющую родителям составить для своих детей расписание доступа в Интернет. При этом управление доступом осуществляется с сервера провайдера, а на самом клиентском компьютере не устанавливается никакого ПО, которое современные продвинутые дети смогли бы обойти или отключить.

Дмитрий МЕДВЕДЕВ: Наша услуга «Родительский контроль» позволяет родителям составить для своих детей расписание пользования Интернетом

П. АНТОНОВ: Законодательства некоторых стран обязывают операторов связи блокировать доступ к сайтам с незаконным контентом, в частности с детской порнографией, независимо от желания пользова-

теля. Выявлением таких сайтов занимаются специализированные организации. Например, в Великобритании это делает фонд Internet Watch Foundation.

М. МАЛЫШЕВА: Хотелось бы обратить внимание на тех лиц, которые размещают нежелательный контент с помощью наших услуг – услуг регистраторов доменов и хостинг-провайдеров. В борьбе с детской порнографией нам очень помогает Фонд «Дружественный Рунет». К его экспертам мы обращаемся, если нужно классифицировать контент, на который поступают жалобы пользователей. Если контент оказывается незаконным, мы блокируем к нему доступ. Но что делать с абонентом, нарушившим закон? Мы готовы сотрудничать с правоохранительными органами, чтобы эти правонарушители были пойманы и наказаны. Возможно, имеет смысл создавать базы данных лиц, публикующих на своих сайтах незаконный контент, и обмениваться ими с другими хостинг-провайдерами, чтобы этот контент не кочевал по Интернету. Так мы могли бы бороться с правонарушителями, а не только защищаться от них.

Мария МАЛЫШЕВА: Если контент оказывается незаконным, мы блокируем к нему доступ

М. БОБИН: На любом из сервисов Mail.Ru есть кнопка «Пожаловаться модератору» и работает круглосуточная служба модерации. В этом году мы хорошо «почистили» наш сервис бесплатного хостинга Видео@Mail.Ru, и теперь, я думаю, там стало гораздо меньше неприятного контента. У нас также есть служба безопасности, которая активно сотрудничает с правоохранительными органами и доводит до их сведения выявленные факты публикации незаконного контента.

Е. БЕСПАЛОВ: В мировой практике уже выработана модель безопасного Интернета для детей, которая предполагает удаление и блокирование негативного контента, создание позитивного контента и обеспечение безопасного поведения детей в социальных сетях и сервисах. В России работает несколько горячих линий, финансируемых интернет-сообществом и компаниями интернет-отрасли, куда можно сообщить о противоправном контенте. Это говорит о становлении системы саморегулирования в России. Да, в борьбе с противоправным контентом нужно развивать законодательство, но практика ведущих стран мира показывает, что наиболее действенным является саморегулирование интернет-отрасли, которая сама вырабатывает механизм противодействия и подключает государственные ведомства для наведения порядка.

Евгений БЕСПАЛОВ: Бывает и так, что дети, не зная основных правил правильного и безопасного поведения в Сети, могут сами нарушать те или иные законы

Ю. ОВЧИННИКОВА: С формальной точки зрения Координационный центр домена RU не обязан заниматься обеспечением безопасности детей в Интернете, но в его задачи входит разработка правил и регламентов работы с регистраторами. Недавно были разработаны новые правила регистрации имен в домене RU и в новом кириллическом домене РФ, где серьезное внимание уделено безопасности всего Интернета. Кроме того, КЦ поддерживает горячие линии по борьбе с противоправным контентом, проекты по стимулированию позитивного контента в Интернете (викторины «Твиди», «Интернешка», конкурс «Позитивный контент»), а в Оргкомитете Года безопасного Интернета в России КЦ выступает в роли объединяющей общественность площадки.

Игорь ПОЛЯКОВ: Контентный фильтр на основе наших решений в пакете ПО «Первая помощь 1.0» поставлен в каждую школу РФ

И. ПОЛЯКОВ: ЦАИР занимается разработкой программных решений по управлению доступом к интернет-ресурсам (контентная фильтрация). Мы предлагаем решения как для провайдеров и операторов связи, так и для конечных пользователей. Контентный фильтр на основе наших решений в пакете ПО «Первая помощь 1.0» поставлен в каждую школу РФ, наши фильтры используют более 500 тыс. пользователей в 51 стране мира.

Мнение МВД: детей – в интернет-лягушатник!

Участники рынка, как мы видим, готовы сотрудничать с правоохранительными органами в деле обеспечения безопасности детей в Интернете. Ну а что же само МВД, а точнее, его Бюро специальных технических мероприятий (БСТИ, оно же Управление «К»), специализирующееся на борьбе с преступлениями в сфере информационных технологий? Оно приветствует идею саморегулирования интернет-отрасли в этом вопросе, но считает, что для настоящего саморегулирования игрокам этого рынка следует разработать корпоративные этические нормы и строго придерживаться их. МВД активно поддерживает и работу горячих линий по приему сообщений о детской порнографии и другом негативном контенте в Интернете. Благодаря им возросла раскрываемость преступлений в этой сфере. Правда, и правонарушители не дремлют: открывают новые сайты взамен закрытых, уходят на хостинг за границу и т.п., но на этот случай у БСТИ налажены связи с зарубежными коллегами.

Очень беспокоит МВД и ситуация с интерактивными сервисами и социальными сетями, поскольку пока в российском законодательстве нет норм, обязывающих владельцев этих ресурсов заниматься модерацией контента, публикуемого пользователями, блокировать или удалять его. Наши правоохранители поддерживают идею фильтрации контента и считают, что эту услугу надо активно предлагать пользователям, а в некоторых случаях даже навязывать. Кроме того, для детей нужно создавать в Сети специальные доверенные зоны с позитивным контентом и до определенного возраста не выпускать их в свободное плавание в океан по имени Интернет.

«ИКС»: Насколько эффективны современные технологии фильтрации контента?

Е. СЕРЕГИНА: Сейчас мы можем отфильтровать ресурсы, о которых заведомо известно, что они являются вредоносными. Но есть сайты с неоднозначным контентом и возникает вопрос: где критерий, который позволит категоризировать эти ресурсы? На этот счет нет ни регуляторных правил, ни органа, который мог бы этим заняться. В блогах, на форумах и в социальных сетях существуют свои форматы общения. Там можно встретить контент, который вроде бы разрешен (это же свободное общение в соответствии с конституционным правом каждого высказывать свое мнение), но, наверное, ни один родитель не хотел бы, чтобы на подобный форум попал его ребенок. Так что, кроме технологических проблем фильтрации, есть и этические проблемы.

А. ЯРНЫХ: Борьба за чистоту Интернета – это фактически поединок снаряда и брони. Фильтры отсеивают значительную часть вредоносного контента, но меньше его не становится. Улучшаются средства распознавания, но вслед за этим злоумышленники разрабатывают новые механизмы обхода всевозможных фильтров. Источники спама, вирусов и противоправного контента, закрытые в одном месте, быстро находят убежище в других странах. К сожалению, имеет место динамическое равновесие.

Андрей ЯРНЫХ: Без специального ПО даже опытный пользователь окажется мишенью для атак злоумышленников

«ИКС»: Важно ведь не только закрыть доступ к неподобающему контенту, но и предложить детям что-то интересное и позитивное.

Н. МАКАРОВА: В рамках Года безопасного Интернета компания RU-CENTER, Фонд развития Интернет и КЦ национального домена RU организовали конкурс на лучший интернет-ресурс с позитивным контентом, для детско-юношеской аудитории. Заявок много, но действительно позитивного контента и достойных сайтов для детей недостает.

М. МАЛЫШЕВА: Не могу согласиться. Наша компания с 2005 г. поддерживает образовательные интернет-ресурсы, в том числе сайты студентов или школьников.

Наталия МАКАРОВА: Действительно позитивного контента и достойных сайтов для детей явно недостает

Мы видим их большое желание создавать в Сети что-то интересное и позитивное, и ресурсов этих довольно много.

Е. БЕСПАЛОВ: Нужны исследования того, что дети ищут в Сети, что находят, насколько они этим удовлетворены и насколько удовлетворены их родители и учителя. Пока таких данных нет. Очень надеемся, что Фонд развития Интернет в рамках Года безопасного Интернета возьмется за такие исследования. Подождем результатов.

«ИКС»: В доме, где есть дети, появляется компьютер. Что можно и нужно сделать родителям?

Д. МЕДВЕДЕВ: Если родители – продвинутые пользователи, то они, конечно, могут сконфигурировать ограничения для ребенка на уровне операционной системы, но таких родителей очень мало. Мы все-таки обсуждаем несколько другой аспект этой темы. Родителям хотелось бы, чтобы их ребенок получал в Сети полезную информацию и общался со сверстниками, но им нужно знать, как оградить его от неподобающего контента. Эти вопросы касаются уже не только технарей, но и всего общества.

Е. БЕСПАЛОВ: Полагаю, что родителям и педагогам следует обратить внимание детей на детский конкурс «Интернешка», который организован как раз для того, чтобы стимулировать детей знакомиться со способами безопасного использования Интернета. Кстати, самой посещаемой страницей сайта этого конкурса является страница с рекомендациями для детей по интернет-безопасности.

М. БОБИН: Я бы посоветовал родителям больше общаться со своими детьми, чтобы знать, что они делают Интернете и куда они там ходят. И, соответственно, учить их не поддаваться на провокации, которые там бывают.

П. АНТОНОВ: Родителям надо как минимум интересоваться проблемой интернет-безопасности, быть активнее, высказываться на форумах, обращаться к своим операторам связи по поводу блокировки интернет-контента и т.д. Только активная дискуссия в обществе позволит выработать наиболее продуктивные решения.

Ю. ОВЧИННИКОВА: Надо дружить со своими детьми. Только тогда они нам будут доверять и мы сможем им объяснить, чего надо и не надо опасаться, что надо делать и чего не надо, и научить их критически относиться к любой информации, в том числе и полученной из Интернета.

Юлия ОВЧИННИКОВА: Мы должны научить наших детей критически относиться к любой информации, в том числе и полученной из Интернета

«ИКС»: А что следует делать государству, чтобы Интернет стал безопасным пространством для ребенка?

Е. БЕСПАЛОВ: Совет государству простой: поддержать инициативы общественности и интернет-индустрии, ведь общество быстрее найдет нужные инструменты и механизмы, чем государство сможет их придумать и зафиксировать в нормативных актах. И еще государству стоит заняться серьезной проблемой низкой интернет-грамотности учителей в школах. Встречаются вопиющие случаи, когда учителя велят детям зарегистрироваться во взрослой социальной сети и выполнять там домашние работы по информатике. Поэтому я предложил бы Оргкомитету Года безопасного Интернета обратиться к Минкомсвязи и Минобрнауки с инициативой посвятить 2010 год безопасности современных инфокоммуникаций в школе.

Е. СЕРЕГИНА: Тема безопасности в Интернете периодически обсуждается в Государственной думе и в других ведомствах. Там есть и сторонники жесткой регуляторики, и те, что поддерживают либеральное отношение к Интернету. Чем больше компаний интернет-отрасли будут обращаться к этой теме, тем быстрее на государственном уровне будут предприниматься какие-то действенные шаги, которые позволят нам обеспечить безопасное общение с Интернетом наших пользователей и их детей, не ограничивая свободы доступа к информации

Подготовила
Евгения ВОЛЫНКИНА

ПОЛНЫЙ ТЕКСТ КРУГЛОГО СТОЛА на www.iksmedia.ru

Чем полезен потребитель

Потребитель стал играть активную роль не только в процессе потребления, но и в разработке продукта, формировании рекламной концепции и продвижении. Компании включают потребителей в свои корпоративные сети, создавая среду для разработки передовых продуктов.

Наталья КОРОТКОВА,
ГУ-ВШЭ

Обычно пользователи совершенствуют продукт своими силами, если он по тем или иным причинам не удовлетворяет их потребности. Вспомним, как в эпоху дефицита молодежь варила в хлорке новые джинсы, чтобы придать им модный в ту пору потертый, умеренно поношенный вид. Сегодня, в эпоху консьюмеризма, компании стремятся предоставить товар, максимально отвечающий требованиям клиента, но в случае радикальных инноваций в продукте пользователи не всегда могут сформулировать свои ожидания. Кроме того, между производителем и потребителем может существовать значительная когнитивная (понятийная) дистанция, затрудняющая сбор, анализ и интерпретацию данных о потенциальном спросе и использовании продукта. В результате эффективность традиционных методов исследования рынка снижается: они лишь сканируют поверхностную информацию о потребностях, но не позволяют потребителям предложить что-то свое или внести изменения в тестируемую концепцию или прототип.

Бывает, что неудачный продукт все-таки проникает на рынок и наиболее креативные потребители начинают собственный инновационный процесс. Подобных случаев стало так много, что маркетологи выделили специальный статус потребителей-инноваторов – лид-юзер (lead user) и определили его как «пользователя, находящегося в авангарде и ищущего способы улучшить или модифицировать существующие продукты, чтобы они приобрели новые функции»*. Лид-юзеры – это изобретатели-авангардисты. Они чувствуют потребности рынка раньше среднестатистического потребителя и склонны приобретать новые продукты на ранней стадии жизненного цикла. Это позволяет предприятиям рассматривать их как целевой сегмент на ранних этапах диффузии новых продуктов.

Откуда идеи? От спроса, вестимо...

Идеи инноваций возникают как ответ либо на неудовлетворенный спрос, либо на некую общую тенденцию отрасли. Есть и так называемые изобретения-озарения, когда новое решение появляется в ходе внутреннего когнитивного процесса, а не вследствие внешних стимулов.

При создании нового продукта на этапе генерирования идей предприятия прибегают к таким инструментам, как рыночные исследования, опросы, книги предложений. Источниками идей могут быть прямые контакты с потребителями и их жалобы, исследования клиентской базы, маркетинговые исследования, конкурентный анализ и т.д.

Но идей может быть много, поэтому существует этап фильтрации, когда сотрудничество с пользователями может принимать форму фокус-групп (реальных или виртуальных). К сожалению, практика показывает, что на этом этапе предприятия мало используют инструменты взаимодействия с потребителем, часто по причине чрезмерного контроля процесса создания нового продукта.

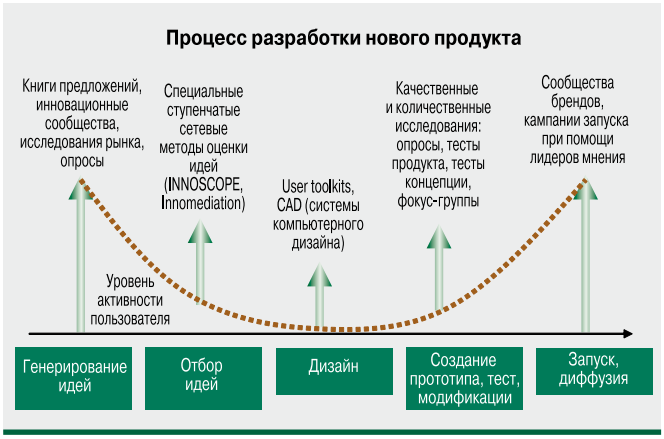
Между тем виртуальная среда позволяет вовлечь пользователей в генерирование и фильтрацию идей при минимальных затратах. Например, метод Branddelphi tm предлагает посетителям сайта www.branddelphi.com проявить креативные способности и вначале сгенерировать идеи относительно предложенной категории товаров, а затем оценить идеи предшественников.

Точки приложения сил

Анализ процессов разработки на предприятиях показывает, что наиболее активно сотрудничество с пользователями протекает на начальных и финальных этапах инновационного процесса и носит в основном информационный характер. На этапах отбора идей и дизайна предприятия опираются главным образом на внутренних и внешних экспертов или на сотрудников отдела разработки. На этапе тестирования прототипа взаимодействие с потребителями имеет в основном пассивный характер: пользователи могут одобрить или отвергнуть предложенный ими прототип, но лишены возможности привнести свои идеи или модифицировать прототип.

Участие потребителей в процессе разработки продукта можно разделить на две категории: информационное

Сотрудничество с потребителями в процессе инновации



* Von Hippel E. (1986) Lead Users: a Sourse of Novel Product Concepts, *Management Science*, July1986, vol. 32, 7, c. 791.

сотрудничество (генерирование идей, участие в фокус-группах или мозговом штурме); совместная разработка (как правило, эта категория возможна при наличии у потребителя материально-технических ресурсов для исследования и/или производства).

Совместная разработка предполагает высокий уровень взаимодействия между производителем и потенциальным потребителем и позволяет последнему влиять на принятие технических и маркетинговых решений на любом этапе создания нового продукта. Часто она ассоциируется с созданием ПО open source, а также с бета-тестированием, но применяется и в других отраслях. Так, например, однажды в рамках исследовательского проекта покупателям профессиональных спортивных товаров Adidas было предложено поучаствовать в создании (в том числе в дизайне) спортивной обуви на специальном портале, где можно было «спроектировать» кроссовки (при покупке вместе с чеком выдавался код доступа). Автора лучшего предложения ждал приз. К удивлению организаторов, порядка 80% покупателей, получивших код, внесли свои предложения, 20% из них были оценены как очень перспективные и инновационные.

Основным барьером, препятствующим привлечению потребителей к процессу создания и технического воплощения новых продуктов, являются технические ресурсы фирмы. В таких отраслях, как химия, медицина, автомобилестроение, участвовать в инновационном процессе могут только квалифицированные специалисты в данной области. В отличие от начальных этапов (когда от потребителя по большому счету требуется только вовлеченность, мотивация и креативность), в создании технического прототипа нового продукта необходима специальная квалификация и знание предметной области.

Между тем участие лид-юзеров на этапе дизайна продукта может быть организовано с помощью специальных инструментов взаимодействия – user toolkits. С их помощью можно установить обратную связь с потребителями и учесть их предпочтения на этапе дизайна.

Известным и успешным примером совместной разработки является сетевое сообщество InnoCentive (www.innocentive.com), созданное фармацевтической компанией Eli Lilly в 2001 г. Средняя стоимость разработки нового препарата составляет $500 млн, а время его создания от начала исследований до получения патента иногда превышает 15 лет. Чтобы ускорить этот процесс, компания решила привлечь пользователей, определив вознаграждение в $25 тыс. специалисту, который предложит оригинальное решение для создания нового лекарства. Решение было найдено достаточно быстро.

А InnoCentive преобразовался в портал, где фармацевты из разных стран обмениваются мнениями по поводу использования новых лекарств, а также вносят свои предложения или участвуют в разработках по запросам различных фармацевтических компаний. Уже через год на этом портале зарегистрировалось более 10 тыс. добровольцев-разработчиков, причем, как признаются сами пользователи-исследователи, они получают удовольствие от самого факта причастности к разрешению сложных медицинских проблем. Бóльшая часть участников сообщества – это вышедшие на пенсию исследователи, преподаватели медицинских вузов, специалисты фармацевтической отрасли и врачи.

Векторы интересов потребителя

Участие потребителей в создании новых продуктов наиболее эффективно в следующем контексте:

- ✓ если спрос на продукт/услугу является гетерогенным;
- ✓ если знания представляют основной источник формирования экономической стоимости (так называемая наукоемкая продукция);
- ✓ на фрагментированных рынках спроса и предложения (например, продукты длительного пользования);
- ✓ на рынках B2B, где прикладными навыками (tacit know-how) обращения с продуктом владеет покупатель (фармацевтическая отрасль, разработка ПО);
- ✓ на формирующихся рынках, где важны предпочтения потребителя и кастомизация (например, мобильная связь);
- ✓ в «гедонических» отраслях, относящихся к стилю жизни, моде, где при создании товара важны социальные аспекты.

Не хлебом единым...

Участие пользователей в разработке новых решений определяется не только и не столько обещанным вознаграждением, сколько любознательностью, удовольствием от общения с другими инноваторами, интересом к продукту, желанием стать первым обладателем эксклюзивной информации, ну и, конечно, возможностью самоутвердиться.

Нередко креативные пользователи бескорыстно делятся идеями со своим окружением, а иногда даже с предприятием. В маркетинговой литературе таких потребителей называют хоббистами: они настолько увлечены продуктом, что готовы вкладывать свое время и силы, а иногда даже материальные средства в его усовершенствование и совершенно безвозмездно делиться идеями. Хоббистов можно встретить в сообществах, посвященных компьютерным играм, мотоциклам, серфингу, походному инвентарю и прочим «увлекательным продуктам». Иногда идеи, исходящие от пользователей, стимулируют создание коммерческих продуктов, поэтому производители спортивного инвентаря с интересом читают форумы, подобные www.backpackinglight.com, и сотрудничают с авторами наиболее интересных идей.

Практика показывает, что у идей, создаваемых пользователями на независимой основе или в сотрудничестве с предприятиями-производителями, высокий потенциал. Часто эти идеи дают жизнь не только одному продукту, но и ложатся в основу целой серии. Однако российские предприятия при разработке продуктов прибегают к сотрудничеству с потребителями в основном в форме маркетинговых исследований (опросов, фокус-групп), не давая потребителям возможности предложить собственные идеи. Интеграция потребителя в полный цикл работ по созданию продуктов, а также в создание и развитие виртуальных инструментов сотрудничества с продвинутыми пользователями позволят российским предприятиям повысить конкурентоспособность новых продуктов. ИКС

Как разгрузить маршрутизаторы ядра IP-сети

Объем интернет-трафика удваивается ежегодно, а производительность маршрутизаторов повышается вдвое только раз в полтора года. Сегодня уже очевидно, что производительность, стоимость и энергопотребление маршрутизаторов уровня IP-ядра становятся главными сдерживающими факторами развития сетей связи и ИТ-индустрии в целом. Как их нейтрализовать?

Алексей ШПАК,
заместитель директора отдела оптических сетей Huawei CIS

Современная опорная IP-сеть крупных операторов связи строится по так называемой dual-homing-топологии, т.е. путем подключения граничных маршрутизаторов (PE) к двум маршрутизаторам ядра (P). Маршрутизаторы уровня ядра занимаются транзитом и маршрутизацией между граничными маршрутизаторами. Анализ трафика опорных IP-сетей показал, что около половины трафика, обрабатываемого P-маршрутизатором, является транзитным, вследствие чего ресурсы дорогостоящих линейных плат маршрутизаторов используются не по прямому назначению. Это серьезно снижает эффективность функционирования оборудования и увеличивает стоимость сети и ее энергопотребление. Сократить или исключить эти издержки – важная цель операторов и производителей оборудования.

По оценкам зарубежных экспертов, производительность узлов опорной IP-сети в ближайшие годы будет измеряться терабитами в секунду. Экстенсивное наращивание производительности одного устройства в таких условиях неэффективно и труднореализуемо. С другой стороны, решения для оптических транспортных сетей (OTN) уже сейчас поддерживают мультитерабитную емкость коммутации на оптическом (ROADM) и электрическом (ODU) уровнях, равно как и традиционные преимущества WDM (емкость и дальность передачи) и SDH (механизмы управления и защиты). Однако в одиночку они не могут обеспечить всю функциональность, требуемую современной IP-сетью.

Основная техническая задача на сегодняшний день – реализация оптимального взаимодействия между оптическими и IP-сетями, что поможет разгрузить маршрутизаторы в ядре IP-сети путем передачи функций по диспетчеризации высокоскоростного транзитного трафика оптической сети. Это позволит минимизировать капитальные и операционные затраты, гарантируя качественное предоставление телекоммуникационных услуг.

Варианты взаимодействия оптического и IP-уровней

Традиционная двухуровневая модель работы IP/MPLS over WDM предполагает, что маршрутизаторы связаны логическими соединениями, а WDM создает эти соединения на физической топологии без дополнительных волокон, обеспечивая необходимую емкость и дальность передачи (рис. 1). Благодаря этому маршрутизаторам не требуется обрабатывать транзитный трафик, он доставляется напрямую по оптической сети. Для расширения емкости соединения между маршрутизаторами на WDM-уровне добавляется соответствующее число каналов.

Однако IP-сеть ничего не знает о топологии и возможностях защиты оптической сети, равно как и оптический уровень не знает о динамическом предоставлении сервисов в IP-сети. Кроме того, вся нагрузка по диспетчеризации трафика остается на маршрутизаторах ядра сети.

Рис. 1. Двухуровневая модель

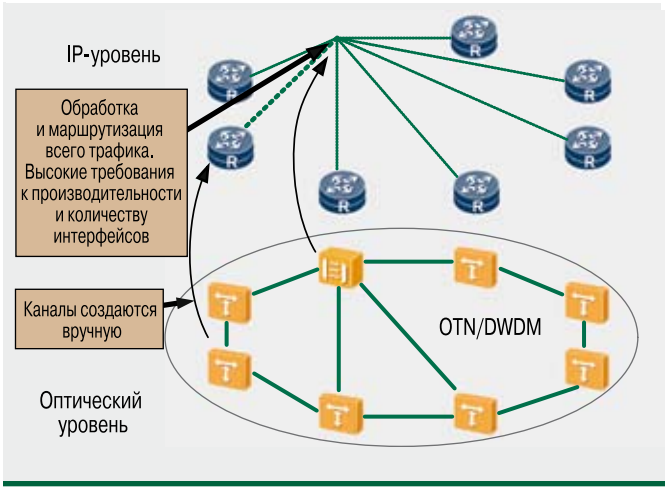
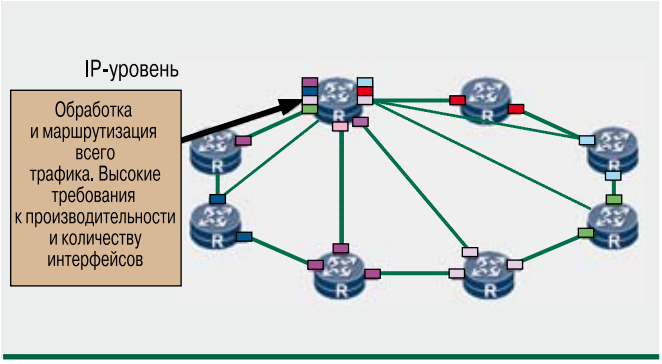


Рис. 2. Окрашенные интерфейсы на IP-оборудовании



Таким образом, двухуровневая модель лишь отчасти способна решить поставленную задачу.

Другой реализацией сети IP/MPLS over WDM является установка окрашенных линейных интерфейсов WDM непосредственно в маршрутизаторы (рис. 2). Такой подход позволяет сократить количество оптико-электрических преобразований и естественным образом решает проблему взаимодействия оптического и IP-уровней сети.

К сожалению, и этот вариант не решает главную задачу – снизить нагрузку на маршрутизаторы ядра IP-сети с их высокой стоимостью и энергопотреблением. Кроме того, из-за серьезных ограничений на использование оптических технологий применить это решение можно лишь для небольших сетей.

Третий вариант – единый уровень управления GMPLS. Предполагается, что IP- и оптическая сети поддерживают GMPLS, благодаря чему они могут полноценно взаимодействовать в едином домене управления. Данные о топологии рассылаются на все узлы посредством протоколов маршрутизации, благодаря чему они получают одинаковую информацию о структуре сети. Оптический уровень OTN/DWDM осуществляет диспетчеризацию высокоскоростного трафика и защиту на физическом уровне, IP-сеть занимается обработкой сервисов и их защитой.

Это решение – идеальное, однако реализовать его в ближайшем будущем не представляется возможным из-за отсутствия оборудования и окончательно утвержденных стандартов. Также очевидно, что для IP-сети такое взаимодействие породит множество трудностей, связанных с безопасностью, управлением и масштабируемостью.

Оптимальное решение

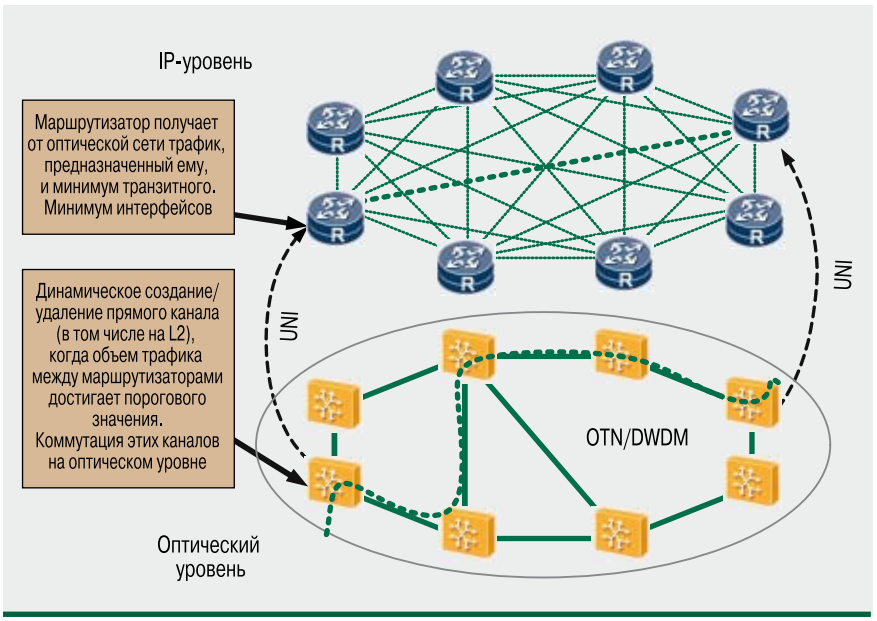
Оптимальным и реальным вариантом решения проблемы взаимодействия оптической и IP-сетей является организация обмена сигнальной информацией между уровнями управления оптического (GMPLS) и IP (MPLS) доменов посредством интерфейса GMPLS UNI (рис. 3). Для такого взаимодействия требуется, чтобы оборудование оптических и IP-сетей поддерживало GMPLS UNI-интерфейсы, которые уже стандартизованы и выпускаются производителями. Это позволит решить две главные задачи.

1 Динамически устанавливать или удалять логический канал между маршрутизаторами, когда объем трафика между ними достигает порогового значения. Маршрутизаторы, лежащие на пути следования трафика, проходятся им транзитно на оптическом уровне для оптимального распределения нагрузки между оптической и IP-сетями.

В этом решении отслеживается трафик между двумя граничными маршрутизаторами и используется информация о сервисах и нагрузке каждого PE-маршрутизатора. При достижении определенного объема трафика между PE-маршрутизаторами по специальному алгоритму выбираются начальная и конечная точки создаваемого или удаляемого логического канала. Информация об этом передается на соответствующие маршрутизаторы, которые посредством GMPLS UNI-интерфейса запрашивают ресурсы в оптической сети для создания или удаления логического канала. Маршрутизатор упаковывает трафик для передачи в канализированный спектральный подканал оптической сети (например, в ODU1 или GE). Оптическая сеть осуществляет коммутацию и передачу созданного канала, опираясь на данные о начальной и конечной точках. В этом варианте использования интерфейса GMPLS UNI от маршрутизаторов требуется поддержка канализированных OTN-интерфейсов.

Оптическая сеть может передавать транзитный трафик, основываясь на идентификаторах второго уровня L2 (например, на тэге S-VLAN). В этом случае оборудование OTN/DWDM должно поддерживать работу на втором уровне, что его усложняет, однако повышает эффективность всей сети. К тому же создание динами-

Рис. 3. Оптимальная модель взаимодействия оптической и IP-сетей для снижения нагрузки на маршрутизаторы IP-ядра



ческого канала на втором уровне не требует выделения дополнительных портов на маршрутизаторе.

2 Использование интерфейса GMPLS UNI дает возможность разделить защиту узлов маршрутизации IP-трафика и защиту волокна (по статистике, из-за обрыва волокна происходит 60–70% аварий на опорных сетях). Маршрутизатор будет резервировать сервисы, а OTN/DWDM – волокна. Повторное срабатывание защиты предотвращается путем внесения задержки в реагирование IP-сети. При получении сообщения о потере сигнала (LOS), связанного с обрывом волокна, сеть OTN/DWDM GMPLS мгновенно запускает защитное переключение, которое срабатывает за 50 мс. Маршрутизатор также фиксирует обрыв волокна с помощью BFD, но не реагирует на него в течение 50 мс. Получив BFD с данной линии повторно, маршрутизатор обнаруживает, что неисправность уже устранена. Таким образом, с точки зрения IP-сети никакой аварии нет. А значит, нет необходимости поддерживать низкое заполнение каналов IP-сети на случай защитной перемаршрутизации при обрыве физической линии. Более того, сеть останется работоспособной даже при многократных обрывах линий. Надежность единой оптической и IP-сети повышается, а затраты на ее строительство, расширение и обслуживание снижаются.

Современный уровень развития оптических и IP-технологий позволяет уже сегодня реализовать интегрированную сеть, в которой диспетчеризацией основной массы трафика и резервированием оптики будет заниматься оборудование OTN/DWDM. IP-оборудование имеет возможность динамически запрашивать необходимую полосу пропускания у оптической сети через GMPLS UNI, не заботясь о реальной топологии сети и защите от обрывов волокна.

Использование динамической передачи транзитного трафика с помощью оптического оборудования приведет к тому, что начиная с некоторого момента увеличивать производительность маршрутизаторов вслед за ростом трафика более не потребуется. Здесь уместно сравнение с организацией дорожного движения: в городе строятся скоростные магистрали, напрямую связывающие удаленные районы, благодаря которым можно миновать переполненный центр и не загружать его еще больше. Съезжать с хайвэя будут только машины, направляющиеся непосредственно в центр города, а их доля не слишком велика и растет значительно медленнее общего потока машин.

По оценкам операторов, переход к взаимодействию оптической и IP-сети через UNI может снизить требования к производительности маршрутизаторов в ядре IP-сети на 25–50%. Стоимость же оптического оборудования и его энергопотребление на бит предаваемой информации в 3–5 раз меньше, чем у IP-оборудования. Считайте сами. ИКС

Персональным данным требуется отсрочка?

Эксперты в один голос говорят о противоречивости российской нормативной правовой базы по персональным данным, сложности внесения изменений в существующие информационные системы с целью приведения их в соответствие новым требованиям и ограниченности установленных законом сроков. Могут ли многочисленные операторы персональных данных рассчитывать на перенос этих сроков?

Александр ВАСЮНИН,
компания «Информзащита»

Европейский опыт

Для понимания контекста проблемы вспомним основные этапы становления законодательства о персональных данных (ПД) за рубежом.

Европейское законодательство в этой сфере уходит корнями в принятую в 1948 г. Генеральной Ассамблеей ООН «Всеобщую декларацию прав человека», ст. 12 которой гласит, что «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

В 1981 г. Совет Европы принял Конвенцию о защите физических лиц при автоматизированной обработке ПД, которая исходит из того, что права и интересы личности в условиях применения новейших информационных технологий могут быть нарушены в результате несанкционированных сбора, обработки, хранения и распространения сведений персонального характера. Евросоюз стремился к тому, чтобы субъекты ПД имели четко определенные права и возможность обратиться к должностному лицу или органу, который обязан предпринять действия для их защиты. Каждой стране-члену ЕС было рекомендовано создать институт уполномоченного по защите ПД.

Следующим шагом стала Директива 95/46/ЕС Европарламента и Совета ЕС от 24.10.1995 о защите прав частных лиц применительно к обработке ПД и о свободном движении таких данных. Здесь стоит особо отметить, что Директива 95/46/ЕС рекомендует учитывать отраслевую специфику при исполнении ее требований.

В целях углубления отраслевого принципа защиты ПД, провозглашенного Директивой 95/46/ЕС, была утверждена Директива 97/66/ЕС Европарламента и Совета ЕС от 15.12.1997 об обработке ПД и защите неприкосновенности частной жизни в сфере телекоммуникаций. Она дополняет и конкретизирует правила обработки данных в информационных системах, которые собираются операторами в ходе предоставления услуг связи. Позже появилась Директива 2002/58/ЕС Европарламента и Совета ЕС от 12.07.2002 относительно обработки личных данных и защиты личной тайны в сфере электронных коммуникаций, заменившая Директиву 97/66/ЕС, которая регулировала схожую сферу отношений, но не учитывала современное состояние электронной связи.

Таким образом, европейское законодательство в области ПД идет параллельно с техническим прогрессом и учитывает современные тенденции в области технологий.

А что у нас?

В России основными побуждающими мотивами принятия закона о персональных данных явилось стремление развить положения Конституции РФ о личной тайне и неприкосновенности информации о частной жизни физического лица, а также осознание необходимости в более тесной интеграции страны в мировое и европейское сообщество.

Так, в 2005 г. Россия ратифицировала Конвенцию о защите физических лиц при автоматизированной обработке ПД и во исполнение взятых на себя обязательств в 2006 г. приняла Федеральный закон № 152-ФЗ «О персональных данных». В дополнение к закону в 2007–2008 гг. был принят целый ряд нормативных правовых актов и методических документов, после выхода которых разгорелась нешуточная дискуссия как в экспертном сообществе, так и среди представителей различных ветвей власти.

Нормативные правовые акты о персональных данных

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утверждено Постановлением Правительства РФ от 17.11.2007 № 781).
- Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (утверждены Постановлением Правительства РФ от 06.07.2008 № 512).
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено Постановлением Правительства РФ от 15.09.2008 № 687).

В октябре нынешнего года прошли парламентские слушания на тему «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных», на которых были зафиксированы глубокие системные проблемы и противоречия в нормативной правовой базе, а также противоречия между государственными регуляторами и операторами ПД.

Участники слушаний указали на ориентированность нормативных правовых документов на защиту собственно ПД, а не прав граждан при их обработке в информационных системах, что противоречит Конвенции Совета Европы и закону «О персональных данных», которые в качестве своих целей устанавливают обеспечение защиты прав и свобод человека и гражданина при обработке его ПД.

Вторая проблема связана с высокими требованиями ФСТЭК России по защите информационных систем персональных данных (ИСПД), что также противоречит европейскому опыту. В частности, ст. 17 Директивы 95/46/ЕС прямо увязывает необходимые меры со стоимостью их реализации: «Государства-участники обеспечат, что контролер должен будет реализовать надлежащие технические и организационные меры для защиты персональных данных от случайного или незаконного уничтожения или случайной утраты, изменения, неправомерного раскрытия или доступа, в частности когда обработка влечет передачу данных по сети, а также от всех иных незаконных форм обработки. С учетом состояния и стоимости их реализации такие меры должны обеспечить надлежащий уровень безопасности для рисков, представленных обработкой и природой защищаемых данных».

Требования же ФСТЭК по защите ПД во многом повторяют требования по защите сведений, составляющих государственную тайну, вследствие чего операторы персональных данных должны нести серьезные расходы. К тому же методические документы ФСТЭК имеют гриф «Для служебного пользования» и не находятся в открытом доступе, что было признано неконструктивным.

Еще один момент, на который обратили внимание участники слушаний, – отсутствие учета отраслевой специфики, из-за чего многие компании, основная деятельность которых связана с использованием больших объемов ПД, например организации телекомсектора, попадают в сложное положение. Поэтому получила положительную оценку ведущаяся при участии «большой тройки» работа Инфокоммуникационного союза над проектом отраслевого стандарта по защите персональных данных в ИСПД операторов связи.

Было выдвинуто предложение внести изменения в Федеральный закон № 128-ФЗ «О лицензировании отдельных видов деятельности» для исключения необходимости получения лицензии на техническую защиту конфиденциальной информации при обработке такой информации для собственных нужд.

Но одним из главных вопросов слушаний, безусловно, была возможность переноса на год или даже на два срока приведения ИСПД в соответствие требованиям закона «О персональных данных» (согласно п. 3 ст. 25 данного закона это должно произойти 1 января 2010 г.). Аргументация понятна – методические документы государственных регуляторов были выпущены не так давно, а времени на их реализацию уже практически не осталось. Тем не менее Роскомнадзор официально заявил, что настаивает на нецелесообразности изменения срока приведения ИСПД в соответствие с законодательством. Конечно, не до конца понятны критерии, по которым регуляторы будут определять степень вреда, нанесенного субъектам ПД, однако надо отметить, что именно их обращения являются основным поводом для проверок, а статистика показывает, что число таких обращений с каждым годом неумолимо растет.

■ ■ ■

В сложившихся непростых условиях операторам ПД можно порекомендовать не игнорировать требования по защите персональных данных, ведь полное бездействие в надежде на то, что проверяющие не придут, связано с принятием повышенных рисков, а сам факт проведения работ по защите ПД и аргументированная позиция по возможным спорным вопросам помогут до некоторой степени себя обезопасить. ИКС

- Порядок проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК РФ, ФСБ РФ, Мининформсвязи РФ от 13.02.2008 № 55/86/20).

Методические документы ФСТЭК РФ (с грифом ДСП)

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические документы ФСБ РФ:

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

Когда верстался номер, стало известно, что в Госдуму внесен законопроект, предлагающий перенести срок вступления в силу п. 3 ст. 25 закона «О персональных данных» на год.

VAS-мошенничество
Как защитить свои доходы

На мировом рынке телекома все более активно проявляется бизнес-модель под названием Telco 2.0 (Web 2.0, Mobile 2.0, Business 2.0, Advertising 2.0.). Главная ее особенность – две цепочки создания стоимости: оператор получает прибыль и от своей абонентской базы, и от провайдеров услуг.

Дмитрий КОСТРОВ,
департамент информационной безопасности ОАО «МТС»

Если в классической бизнес-модели оператор выступает в качестве pure merchant («чистый торговец»), то в Telco 2.0 – в качестве pure platform, платформы предоставления сервисов в обе стороны. Согласно этой модели почти все услуги, предоставляемые оператором, относятся к категории VAS (Value Added Services), т.е. услуг, приносящих дополнительный доход с помощью дополнительных платформ. Яркий пример VAS-услуг – SMS, созданная как составная часть стандарта GSM Phase 1.

Следуя данной стратегии, специалист рассматривает клиентскую базу операторов сотовой связи как актив, а управление VAS строит с учетом потребностей абонентов. Услуги с добавленной ценностью становятся для операторов основным источником обеспечения устойчивого роста бизнеса.

Сегодня телеком-рынок, да еще оказавшийся в условиях финансового и экономического мирового кризиса, зашел в тупик. Сложность внедрения новых технологий, новых услуг, а также недостаточная гибкость телекоммуникационных компаний ведут к снижению прибыли. Дополнительная прибыль уходит к компаниям, которые расширяют спектр услуг VAS. В цепочке стоимости контент-услуг более 50% денег, поступающих от конечного потребителя, идет производителю контента. Остальным участникам цепочки – провайдерам доступа, транспортной сети, сервис-провайдерам и др. – достается всего по 7–10%. Вывод: для того чтобы зарабатывать больше, надо контролировать несколько элементов value chain – цепочки создания стоимости. «Захватить цепочку» – купить ее участников или заключить с ними партнерство – может как оператор, так и производитель контента. На сегодняшний день расклад сил явно не в пользу операторов, которые фактически становятся транспортной сетью, уступая свою долю в value chain другим игрокам. Единственный выход для телекомкомпаний – преобразовать свой бизнес в соответствии с «философией» Telco 2.0.

Основываясь на опыте ведущих игроков интернет-рынка (Google, eBay, Amazon и др.), операторы связи предпринимают попытки реализовать новые стратегии, классифицируемые как Mobile 2.0 и Telco 2.0. France Telecom, например, опубликовала интерфейсы доступа к услугам, а также к блогам Orange – теперь в создании контента принимают участие пользователи. Кроме того, компания разрабатывает малые приложения (так называемые widgets), которые могут выполняться на компьютерах и мобильных телефонах и способствуют конвергенции фиксированных и мобильных сетей. Цель – привлечь пользователей к развитию сервисов, предлагаемых компанией, и построить некое подобие экосистемы, способствующей созданию совместно с пользователями новых сервисов.

Типы и формы SMS-спама/фрода

Однако переход на новую модель, стремление получить дополнительный доход с помощью VAS, в частности SMS, сталкивается с необходимостью противодействовать атакам на сеть сигнализации SS7, а также с проблемой SMS-фрода.

SMS-фрод (fraud) и SMS-спам (spam) проявляются в различных формах и представляют большую опасность как для пользователей, так и для операторов связи.

Обычно выделяют 8 типов SMS-спама/фрода:

1. Spamming – пересылка нежелательных сообщений абонентам. Может привести к оттоку абонентов, снижению пропускной способности сети. Опасна спам-пересылка при интерконнекте.
2. Flooding – рассылка удаленной системой огромного количества сообщений абоненту или другой системе. Приводит к перегрузке сигнальных линков (SS7). Оператор домашней сети вынужден оплачивать расходы присоединенной сети.
3. Mobile Terminated Faking (MT faking) – использование удален-

ной системой идентификатора реального разрешенного SMS-центра. Оператор домашней сети не может получить плату за терминацию трафика.

4 Mobile Originated Spoofing (MO spoofing) – нелегальная рассылка сообщений путем эмуляции абонента, находящегося в роуминге. Абоненты получают счета за сообщения, которых не отсылали, и, возможно, за контент.

5 Smishing – рассылка сообщений от якобы легальной компании для получения информации об абоненте. Возможны потенциальная рассылка вирусов, что приводит к спаму, и проблемы с биллингом.

6 Viruses – рассылка сообщений специальными «движками» злоумышленников с целью вынудить абонента загрузить с сайта вирус. Заражение абонентского устройства (смартфона) может привести к проблемам с сервисом, а также к рассылке спам-сообщений.

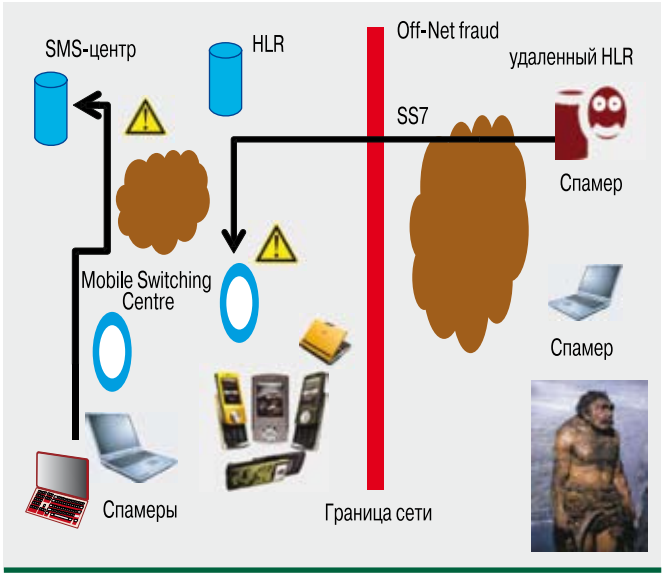
7 GT-Scanning – определение для абонента-получателя короткого сообщения адреса получателя (SCCP CdPA) с помощью специальных транзакций протокола MAP, в которых подменены адрес отправителя (SCCP CgPA) и/или адрес SMS-центра отправителя для транзакции MAP_SEND_ROUTING_INFO_FOR_SM. Чтобы подключиться к сети сигнализации SS7, имеющей выход в межоператорскую сеть SS7 MAP, надо зарегистрировать на STP собственный MTP3 Point Code – PC и SCCP Global Title – GT или контролировать сигнальные линки для зарегистрированных MTP3 PC и SCCP GT. После этого необходимо получить из HLR домашней сети Protected PLMN абонента «B» информацию о коммутаторе (MSC) и/или визитном регистре (VLR), обслуживающем в данный момент абонента «B» (узнать GT MSC/VLR, обслуживающего MSISDN абонента «B»). Ущерб: полученные данные могут использоваться в SMS-spoofing, SMS-faking, SMS-spamming и других видах мошенничества. Провайдеры сигнальных линков требуют с оператора домашней сети абонента «B» плату за трафик от HLR.

8 IWSMS-Charging – выставление счета оператором, обслуживающим получателя короткого сообщения от абонента «A», оператору домашней сети абонента «A» (по соглашению между ними) за доставку короткого сообщения. Оператор, обслуживающий получателя короткого сообщения, должен регистрировать и корректно тарифицировать каждое короткое сообщение, полученное сетью оператора из чужого SMS-центра. При сбое в регистрации или при некорректной тарификации коротких сообщений он может недополучить доход или вступить в конфликт с другими операторами.

Решения для защиты от SMS-спама/фрода

Появление в сетях оператора SMS-спама/фрода может нанести его бизнесу серьезный ущерб. Во-первых, это «удар по бренду», способный привести к снижению лояльности клиентов и отказу их от новых услуг (разрушение бизнес-планов по доходам в mobile advertising mobile и m-commerce). Во-вторых, из-за огромного количества нелегальных сообщений (DoS network attack) увеличиваются расходы оператора на поддержку и обслуживание абонентов, а также падают доходы при интерконнекте (termination fee).

SMS-spam и fraud в незащищенной сети



Чтобы защитить от SMS-спама/фрода каждое SMS-сообщение, которое появилось в домашней сети или пришло от присоединенной сети по SS7, необходимо выяснить: пришло ли оно от авторизованного или нелегального источника (MT faking/MT spoofing), не содержит ли вредоносного контента (smishing, viruses, unauthorised content), не состоит ли источник в «черном списке», не является ли он частью DoS-атаки на пользователя, отдельный узел или сеть.

Сегодня на рынке для защиты от мошенничества представлены два решения: решение с единой точкой – Point Code Based Approach и решение SMS Defence Solution.

Решение Point Code Based Approach основывается на маршрутизации всех сообщений на специальное устройство – Point Code Based Anti-Spam Solution. Минусы этого решения:

- все сообщения, относящиеся к Off-Net mobile-to-mobile SMS spam/fraud, передаются в сигнальную сеть без проверки и занимают ресурсы STP;
- каждое сообщение в режимах Off-Net и On-Net должно быть маршрутизировано в PCB node перед пересылкой в SMS-центр, усиливая поток трафика в сигнальной сети и снижая ее производительность;
- данное решение требует подсоединения к SS7 point code, поэтому оператор обязан провести реинжиниринг сигнальной сети, внедрить систему маршрутизации.

Решение SMS Defence Solution обеспечивает прозрачную фильтрацию трафика SS7. Off-Net SMS spam/fraud могут быть остановлены, перед тем как дойдут до сигнальной сети (граничный STP). При использовании этого решения отпадает необходимость проводить реинжиниринг сигнальной сети, а оператор имеет возможность выбирать место установки устройства в местной сигнальной сети – Radio Access Network или Access Edge (на линках BSC-MSC). ИКС

Корпоративная мобильность растет быстрее ИТ-рынка

Как считает Бхаскар БАГЧИ, директор по продажам Motorola Enterprise Mobility, в России именно мобильные технологии позволяют бизнесу повысить эффективность бизнес-процессов.

Бхаскар БАГЧИ

– Как изменилось понятие «корпоративная мобильность» со времени появления этого термина в 2002 г.? Какие сферы и решения включает этот термин в настоящее время?

– Российский рынок корпоративных мобильных решений начал формироваться немного раньше, во второй половине 90-х. Тогда первыми потребителями стали крупные российские предприятия и розничные сети. К 2006 г. формирование рынка завершилось. В таких отраслях, как розничная торговля и логистика, мобильные технологии стали неотъемлемой частью бизнеса.

Сегодня ситуация в России благоприятствует проникновению мобильных решений в те сферы, где ранее они не получили широкого распространения. Мобильные технологии позволяют повысить прозрачность бизнеса, в первую очередь там, где задействовано большое количество «полевых» сотрудников, существует необходимость передавать информацию в режиме реального времени или повысить точность учета и управления различными активами. Такие проекты не требуют больших ресурсов и зачастую окупаются за три-четыре месяца.

– Как бы вы охарактеризовали идеальное мобильное предприятие? Каким требованиям оно должно отвечать и какими возможностями обладать?

– В идеальном мобильном предприятии все подразделения, инфраструктурные единицы и сотрудники объединены единой системой передачи данных. В таком предприятии информация в режиме реального времени и без искажений передается заинтересованным пользователям, что обеспечивает своевременное принятие решений и высокую эффективность бизнес-процессов.

– Каков технологический арсенал современного мобильного предприятия?

– Основа мобильного предприятия – единая унифицированная корпоративная платформа. В ее составе можно выделить три компонента. Во-первых, это единая, целостная беспроводная инфраструктура. Мобильные решения обеспечивают беспрепятственную передачу информации между различными, зачастую весьма удаленными друг от друга, подразделениями, каждое из которых может использовать свой специфический набор приложений. Во-вторых, мобильному предприятию необходим мощный пакет программных решений, обеспечивающих взаимодействие различных приложений и облегчающих пользователям работу с корпоративными ресурсами. Третий, не менее важный компонент – предназначенные для функционирования в жестких условиях эргономичные и надежные мобильные устройства, позволяющие осуществлять сбор, обработку и передачу информации в режиме реального времени в точке выполнения работ.

– На каких вертикальных рынках предприятия наиболее широко внедряют и используют мобильные решения?

– Традиционно нашими заказчиками являются предприятия розничной торговли, транспортно-логистические компании. Это связано с тем, что у них большой и быстрый товарооборот. Есть успешные проекты в нефтегазовой сфере, активно развиваются медицинское направление и сегмент hospitality (индустрия гостеприимства). Решения по автоматизации бизнес-процессов становятся известными и среди ведомственных заказчиков, особенно в связи с курсом на е-правительство. Также интересны приложения для мониторинга и обслуживания объектов стратегической инфраструктуры.

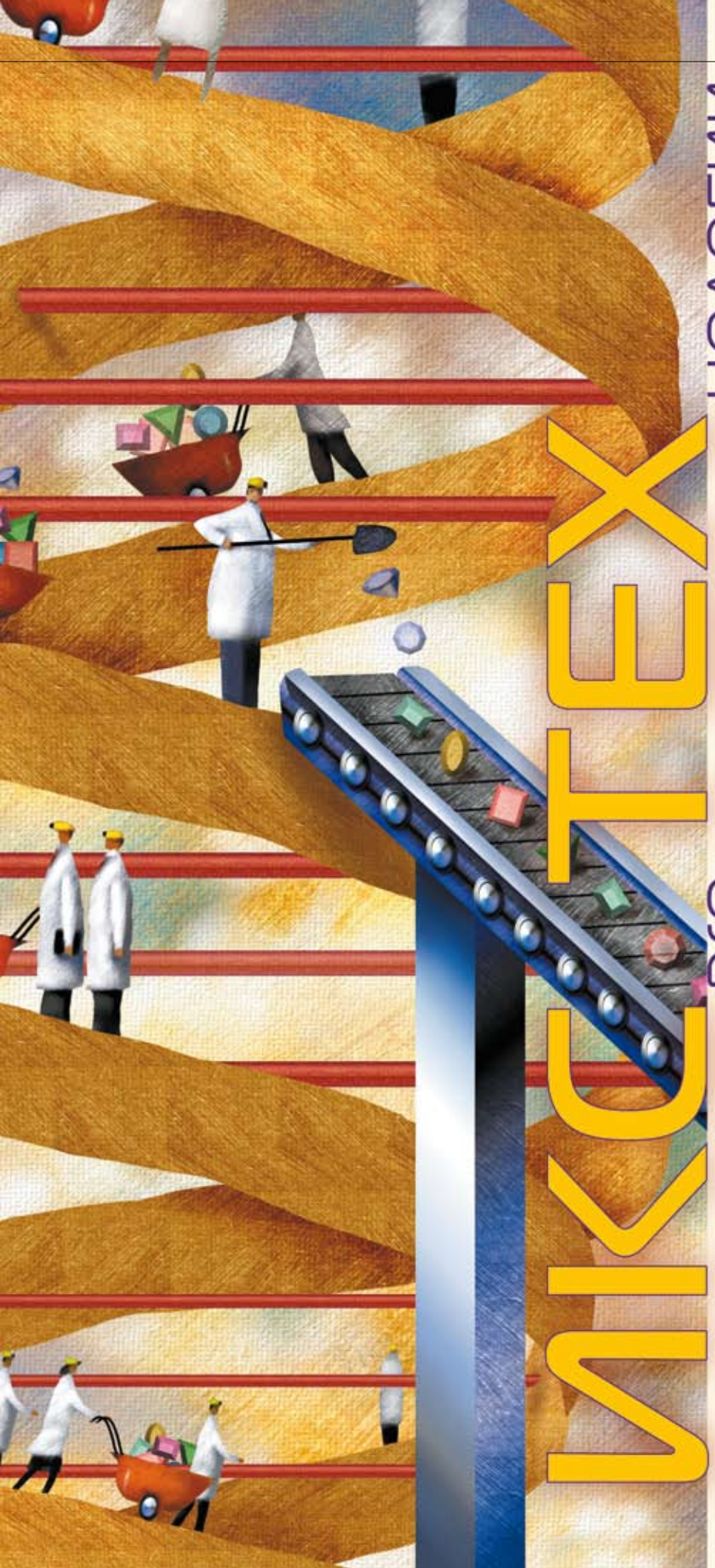
Иными словами, мобильные решения сегодня просто необходимы для крупного бизнеса вне зависимости от его отраслевой специфики. Темпы роста рынка мобильных информационных технологий намного опережают темпы роста рынка ИТ в целом. В этом с нами согласны ведущие аналитические агентства, такие как Gartner и IDC, констатирующие, что мобильные решения все более востребованы бизнесом.

– По вашим наблюдениям: как повлиял экономический кризис на мобильное оснащение предприятий – иначе говоря, как изменились продажи корпоративных мобильных решений?

– С конца 3-го квартала 2009 г. мы отмечаем на рынке существенную положительную динамику.

Очевидно, что за прошедший год российскими компаниями были предприняты все привычные меры по снижению издержек, включая и сокращение ИТ-бюджетов, однако производительность предприятий остается по-прежнему невысокой. Сокращаться больше некуда – настало время подумать о том, каким российский бизнес выйдет из кризиса. Мобильные решения создают возможности для предприятий стать более эффективными, в том числе и в экономически сложных условиях.

Вопросы задавала Наталия КИЙ



ИКС-Тех про технологии

Что должен держать в голове заказчик дата-центров? И почему не стоит обращать внимание на некоторые требования стандарта TIA-942? Зачем телекоммуникационному оператору ввязываться в бизнес ЦОДов?

Это малая толика вопросов, ответы на которые находили участники конференции «ЦОД 2009: проектирование, построение, эксплуатация». В этом номере мы завершаем публикации о дискуссиях вокруг индустрии дата-центров на осенней конференции «ИКС» и анонсируем конференцию «ЦОД 2010». Ее программу «зададут» технологии, рынок и ваши, уважаемые читатели и участники, усилия по его развитию.

«Какими средствами администрировать СКС?» – своей компетенцией вновь поделится с читателями один из ведущих экспертов рынка структурированных кабельных систем.

Соревнование между брендами – примета не только современного операторского рынка, но и рынка оборудования, в том числе систем бесперебойного электроснабжения. Бог, как известно, в деталях. В нашем случае – обзора новинок ИБП.

SOS! – взывают владельцы сетей широкополосного доступа FTTx. Повреждение, хищение оборудования и другие нештатные ситуации на узле доступа, создание необходимых климатических условий для его функционирования и многое другое ложатся на плечи оператора. Сохранить и защитить построенное поможет антивандальный телекоммуникационный шкаф. Основные требования к нему – в одной из статей раздела.

Остается пожелать, чтобы сигнал «спасите наши души» звучал только в потрясающей по силе воздействия песне Высоцкого и никогда не считывался с морзянки вашего бизнеса.

Наталия Кий,
главный редактор «ИКС»

ЦОДы: в вычислительных «облаках» и на земле

Алексей НОВИЧКОВ

Сегодня в России ЦОДы представлены во всем многообразии – корпоративные и коммерческие, базовые и резервные, мобильные и капитальные... Самые разные технологические и экономические аспекты их создания и функционирования обсуждались на конференции «ЦОД-2009: проектирование, построение, эксплуатация», обзор которой мы продолжаем в этом номере*.

Метод проб и ошибок при проектировании и строительстве ЦОДов уходит в прошлое. Появились эксперты, которые заранее могут сказать, на чем можно сэкономить, где следует строго следовать стандартам, а какие из разделов спецификаций относятся к категории заморской экзотики (например, не раз в ироническом ключе упоминавшаяся на конференции прописанная в стандарте TIA-942 высота забора на клиентской парковке).

Но есть вещи, которые заказчик дата-центра без всяких экспертов должен держать в голове. В частности, такой показатель, как предсказуемое время непрерывной доступности сервисов, или, как определил его Максим Иванов, гендиректор проектной компании ADM Partnership, «функциональная устойчивость». Вы не сможете ее обеспечить, даже выбрав абсолютно надежное оборудование, если упустите из виду вынужденные простои ЦОДа по причине выполнения штатных регламентных работ (и неважно, в отношении каких составляющих ЦОДа – здания, инженерной системы, ИТ- или телеком-оборудования – эти работы проводятся).

Рис. 1. Факторы, влияющие на «функциональную устойчивость» ЦОДа

Впрочем, любые ошибки на этапе проектирования обходятся дорого. Предположим, вы выбрали достаточно производительное оборудование, но если совокупная стоимость владения им запредельно высока, то его эксплуатация может свести на нет все доводы в пользу обеспечиваемого этим оборудованием сервиса. Все многообразие факторов, влияющих на функциональную устойчивость ЦОДа, М. Иванов представил в виде пирамиды (рис. 1). Схожую иерархическую модель оценки рисков эксплуатации различных компонентов ЦОДа предложил консультант по управлению ИТ-рисками компании Symantec Константин Смирнов. В основании его пирамиды факторов риска также лежат здание ЦОДа, ИТ- и инженерная инфраструктура, а на вершине – бизнес-процессы и формализованные критерии успешности всего предприятия.

Не последнее место в этой пирамиде рисков, как отметил К. Смирнов, занимает человеческий фактор, поскольку персонал ЦОДа задействован практически во всех производственных цепочках, ведущих от конкретных технологических операций к бизнес-целям компании. Типичный пример – уход сотрудника, обладающего ключевыми знаниями, критичными для одной из технологических областей (скажем, уникальной компетенцией в области ИТ- или инженерной инфраструктуры). Потеря такой информации, находящейся лишь в голове конкретного работника и отсутствующей в проектной или эксплуатационной документации, часто бывает равнозначна отказу соответствующей системы.

К. Смирнов подчеркнул важность наличия инструментальных средств, позволяющих выстраивать цепочки влияния факторов риска нижних уровней пирамиды на целевые показатели бизнеса. Это могут быть как сложные, специализированные средства, так и более простые (вплоть до электронных таблиц Excel). В любом случае для построения таких моделей требуются высококвалифицированные специалисты, совмещающие знания в области ИТ-инфраструктуры и бизнес-процессов компании.

Наличие автоматизированных средств моделирования и разработки (для построения ли модели рисков или термодинамических процессов в ЦОДе) является, по мнению М. Иванова, одним из критериев подбора консультантов и проектировщиков. Так, использование проектной организацией САПР, с одной стороны, резко сокращает число ошибок и дает возможность

*Начало см. в «ИКС» № 11'2009, с. 72.

восстановить часть утерянной проектной документации на уже существующем объекте, а с другой – помогает ускорить ввод ЦОДа в эксплуатацию: современные САПР позволяют представлять проекты в наглядных трехмерных картинках, что особенно выручает на этапе строительства и монтажа оборудования при дефиците квалифицированных исполнителей. А при моделировании процессов теплоотвода в ЦОДе можно заранее «проиграть» все конфигурации вычислительного оборудования, вместо того чтобы экспериментировать на работающем объекте.

К экономии через виртуализацию

Важной особенностью сегодняшнего развития ЦОДов, которую отметил Алексей Грачев, руководитель направления консалтинга EMC в России и странах СНГ, становится возможность постепенного перехода от модели традиционного ЦОДа к корпоративным облачным вычислениям. Преимущества традиционной модели корпоративного ЦОДа состоят в том, что его компания-владелец использует проверенные временем и полностью подконтрольные ей решения и сама обеспечивает физическую и информационную безопасность ИТ-систем.

Технология коммунальных, или облачных, вычислений развивается на протяжении 15 лет, и главное ее достоинство – динамичность и гибкость, возможность получать необходимые информационные ресурсы по требованию из удобного места, не заботясь о том, на какой физической системе они расположены. Сегодня многие компании пользуются услугами внешних провайдеров по принципу облачных вычислений,

По словам А. Грачева, переход от традиционного корпоративного ЦОДа к виртуальному («внутреннему облаку» – private cloud) заключается в предварительной консолидации среды хранения данных и последующем ее разделении на уровни обслуживания (в модели, предлагаемой EMC, таких уровней пять). Управление новой виртуализированной структурой производится, в частности, благодаря специальным программно-аппаратным средствам консорциума VCE (VMware, Cisco и EMC), которые позволяют значительно упростить хранение корпоративных данных. Новая модель так называемого корпоративного облака, состоящего из виртуального корпоративного ЦОДа («внутреннего облака») и традиционного аутсорсингового «внешнего облака» (рис. 2), совмещает в себе обе модели получения информационных сервисов в компании.

Наступление виртуализации вычислительных ресурсов идет широким фронтом на всю ИТ-инфраструктуру, и если этот процесс начался с виртуализации серверов и систем хранения, то сегодня набирает силу виртуализация рабочих станций и ПК. Это направление – относительно новое не только для России, но и для остального мира. Впрочем, по прогнозам Gartner, глобальное число виртуальных станций к концу 2009 г. должно достичь 4 млн штук. По оценкам другого аналитического агентства – The 451 Group, потенциально

Рис. 2. Принципы функционирования корпоративного «облака» по версии компании EMC

этот рынок в 20 раз больше рынка виртуализации серверов. Российская инжиниринговая компания Radius Group, как сообщил ее коммерческий директор Сергей Черепов, уже год занимается виртуализацией ПК и реализовала в этом направлении несколько проектов.

Важный аспект виртуализации рабочих станций – это энергосбережение в офисах компаний. С. Черепов обратил внимание на то, что компьютеры и другое ИТ-оборудование, размещенное в офисах, потребляют порядка 40–60% электроэнергии, расходуемой всем ИТ-оборудованием компании. Этот факт обычно остается незамеченным, поскольку энергопотребление офисного оборудования часто включают не в ИТ-бюджет, а в офисные расходы, в то время как объемы энергозатрат сопоставимы с аналогичными показателями ЦОДов.

Перенос вычислительных мощностей с настольных систем в ЦОДы позволяет существенно сократить затраты на энергопотребление офисов. Но не это в технологии виртуализации ПК главное. Согласно опросу самой Radius Group, российские менеджеры, решившиеся на внедрение виртуальных ПК, в первую очередь делают ставку на централизацию и защиту информации, которая в противном случае часто «размазана» по настольным ПК множества филиалов, а поэтому уязвима как для безвозвратной потери (кражи, пожары и т.п.), так и для банальной утечки. Кроме того, при централизации бизнес-информация становится более доступной для операционной деятельности всей компании. Другой важный аспект – это сокращение расходов на администрирование и поддержку офисного компьютерного оборудования, которые сегодня составляют львиную долю всех текущих затрат ИТ-отделов.

ЦОД как услуга

Отвечая на собственный риторический вопрос «Зачем телекоммуникационному оператору ввязываться в бизнес ЦОДов?», Вадим Ваньков, заместитель генерального директора по коммерческой деятельности ОАО «Комкор» (торговая марка «АКАДО Телеком»), подчеркнул, что темпы роста традиционных видов телеком-

муникационных услуг с каждым годом уменьшаются и операторы заглядываются на новый перспективный «попутный» бизнес. По оценкам консалтинговой компании J'son & Partners, рынок услуг коммерческих ЦОДов в России в 2008 г. составил $160 млн и в ближайшие несколько лет, даже при пессимистическом сценарии развития экономики страны, будет расти минимум на 10% в год. Для «Комкора» недавно построенный коммерческий ЦОД стал третьим по счету. Бизнес компании на ниве ЦОДов ориентирован пока на два типа услуг – базовые (co-location, или размещение клиентского оборудования на площадях ЦОДа, и dedicated – аренда выделенных серверов) и телекоммуникационные. По оценке аналитиков, эти услуги приносят владельцам российских коммерческих ЦОДов львиную долю их доходов (в среднем по отрасли соответственно 75 и 11%).

В принципе же, как считает В. Ваньков, для привлечения клиентов сегодня уже недостаточно предоставления «простых» услуг (аренды площадей/энергомощностей/коммуникаций). Клиенту требуется комплексное решение его проблем с гарантией качества, зафиксированного в SLA (Service Level Agreement). Только в этом случае бизнесу коммерческих ЦОДов может сопутствовать успех. Поэтому в перспективе компания возлагает большие надежды на дополнительные виды услуг, включающие в себя аутсорсинг ИТ-инфраструктуры.

А КРОК, вышедший в этом году на рынок коммерческих ЦОДов, изначально делает ставку на разнообразные услуги аутсорсинга. Как сообщил руководитель аутсорсингового ЦОДа компании КРОК Дмитрий Хороших, сейчас его емкость составляет 70 стойко-мест, а к 2011 г. компания планирует довести этот показатель до 700.

Естественно, что услуга co-location и здесь составляет значительную долю бизнеса. Впрочем, она всегда будет востребована, ведь части клиентов обязательно понадобится то или иное уникальное вычислительное оборудование, которого нет на рынке аутсорсинга. Тем не менее, чтобы в полной мере реализовать свое преимущество как системного интегратора, КРОК заинтересован в моделях аутсорсинга с высокой добавочной стоимостью. В первую очередь это аренда уже имеющегося в ЦОДе ИТ-оборудования, т.е. серверов и систем хранения данных вкупе с коммуникационной «обвязкой». В настоящее время это синонимично аренде виртуального оборудования: современные держатели коммерческих ЦОДов с самого начала ориентируются на виртуализированную вычислительную среду.

К аутсорсингу более высокого уровня относятся услуги типа SaaS (Software as a Service), например популярная среди российских клиентов аренда сервера MS Exchange, которую, кстати, давно практикует КРОК. Другими предложениями могут быть корпоративные автоматизированные системы (CRM, ERP и т.п.). Конечно, высший пилотаж в этом бизнесе – передача всех ИТ-сервисов компании-клиента на аутсорсинг. Если же говорить реально, то для России, по мнению Д. Хороших, в этом спектре услуг пока актуально развертывание у аутсорсера полностью арендуемого резервного ЦОДа.

Такой замечательный клиент

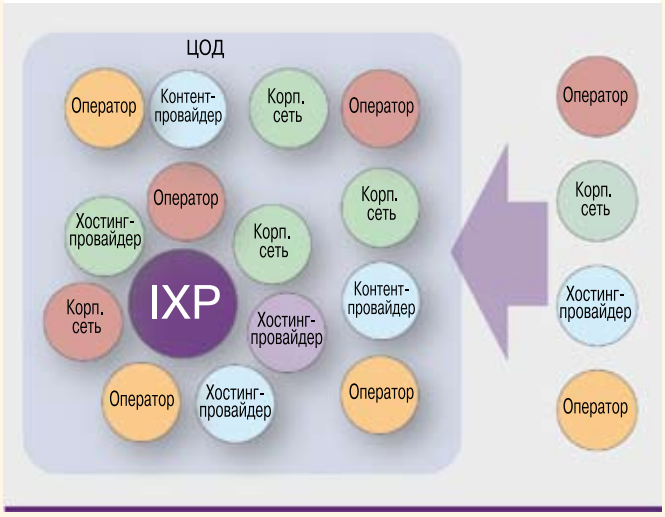
К сожалению, как отметил Сергей Зайцев, директор управления развития компании Stack Group, Россия сегодня не на проценты, а в разы отстает от Запада в развитии услуг аутсорсинга. И такое отставание с годами, увы, не сокращается. Причину этого явления С. Зайцев видит не в характеристиках ИТ-систем или инженерного обеспечения, а в отсутствии гарантий обеспечения качества обслуживания.

Ключевым моментом при составлении SLA должна быть ориентация на бизнес-процессы заказчика, ведь конечная цель последнего – поддержание непрерывности своего бизнеса, а не аренда стоек или мощностей. Но нахождение компромисса в виде SLA требует определенной компетенции в используемых технологиях у обеих договаривающихся сторон. Как убежден С. Зайцев, заказчик для составления договоров на обслуживание должен привлекать экспертов, которые хорошо знают его бизнес-процессы и могут сопоставить их с возможностями, предоставляемыми аутсорсером.

Ведь часто для обеспечения приемлемого уровня цен на свои услуги аутсорсер вынужден прибегать к найму внешних подрядчиков, например при обслуживании той же инженерной инфраструктуры или предоставлении каналов связи. Но такие подрядчики пока не готовы разделить ответственность за нарушение бизнес-процессов конечного клиента наравне с самим аутсорсером. Для преодоления этого противоречия Stack Group, например, сформировала собственные сервисные бригады для поддержки оборудования, которые укладываются в нормативы, предусмотренные в SLA.

Точку зрения клиента на требования к услугам, предоставляемым коммерческими ЦОДами, изложил Константин Чумаченко, заместитель директора Московского Internet Exchange (MSK-IX). Надо, правда, отме-

Рис. 3. IXP образует в ЦОДе экосистемное партнерство, способное привлекать новых клиентов



тить, что оператор обмена интернет-трафиком (Internet eXchange Provider, IXP) – не совсем обычный потребитель услуг ЦОДа, поскольку выступает в некотором смысле бизнес-партнером последнего.

Будучи посредником в обмене трафиком между операторами различных услуг связи (включая интернет-провайдеров, поставщиков контента и SaaS-приложений, хостинг-провайдеров, корпоративные сети и т.п.) и располагаясь на территории конкретного ЦОДа, IXP образует вокруг себя некое системное сообщество, как назвал его К. Чумаченко, – «экосистемное партнерство» (рис. 3). Такой конгломерат клиентов, в свою очередь предоставляющих не конкурирующие между собой услуги, может привлекать в ЦОД новых клиентов, что и является для ЦОДа основным стимулом к размещению IXP на своих площадях.

В то же время, чтобы привлечь к себе оператора обмена интернет-трафиком в качестве клиента, ЦОД должен удовлетворять ряду требований, в частности предъявить достаточную базу операторов-участников, заинтересованных в услугах IXP (и при этом не быть ангажированным одним из таких операторов), иметь достаточный объем канальной емкости и предоставить IXP возможность масштабировать свою коммуникационную инфраструктуру, чтобы не ограничить его бизнес на взлете.

Однако основные клиенты, как говорит С. Зайцев, в расчете на которых строятся ЦОДы с уровнем надежности Tier III и выше, – это высокодоходные крупные заказчики из финансового, страхового или телекоммуникационного секторов. И препятствием к использованию такими клиентами услуг аутсорсингового ЦОДа часто является стандартный «копеечный» штраф в размере 1/720 стоимости месячного обслуживания, который предлагается в качестве компенсации за простой, в то время как клиент теряет миллионы. Именно отсутствие приемлемых условий в SLA толкает сегодня многие богатые компании на строительство собственных ЦОДов.

Пусть маленький, но свой

Реализация серверной комнаты в виде перевозимого контейнера – один из вариантов организации собственного ЦОДа, который регулярно обсуждается на каждой конференции. Однако стоит ли в принципе покупать контейнерный ЦОД в корпоративных целях, если удельная стоимость такого вычислительного комплекса на одну стойку часто проигрывает обычному стационарному ЦОДу в капитальном здании? Андрей Фокин, менеджер по системам хранения данных компании Huawei Symantec Technologies, считает, что стоит. Ведь при поэтапной реализации проекта развертывания крупного ЦОДа с разделением на несколько очередей ввода в эксплуатацию для обеспечении окупаемости проекта на начальной его стадии гораздо эффективнее использовать небольшой контейнерный ЦОД, чем сразу строить/перепланировать большое здание, в котором продолжительное время под реально функционирующее оборудование будет занята лишь небольшая его часть.

Кроме того, иногда контейнерные реализации ЦОДов имеют дополнительные конкурентные преимущества. Например, в мобильном ЦОДе (МЦОД) от Huawei Symantec внешняя обшивка контейнера используется в качестве теплообменника: отработанный горячий воздух из стоек прогоняется вдоль внутренней стороны металлической стенки контейнера, в то время как наружные вентиляторы продувают атмосферный воздух вдоль ее внешней стороны.

Правда холодопроизводительность этой системы имеет жесткие физические ограничения. По словам А. Фокина, она позволяет отводить в 6-метровом ISO-контейнере лишь 50 кВт тепла, поэтому компания предлагает такой ЦОД в компоновке с пятью-шестью стандартными стойками высотой 42U. Эти контейнеры все-таки комплектуются внешним кондиционером, который поставляется в виде отдельного модуля. Кондиционер может подключаться поочереди к нескольким контейнерам и, как правило, используется на начальном этапе их запуска в работу, чтобы нормализовать влажность в герметично замкнутом пространстве МЦОДа. В 12-метровом ISO-контейнере предлагаемая схема позволяет поддерживать работу уже до 10 стоек с активным оборудованием, однако при большем числе стоек Huawei Symantec комплектует свои МЦОДы системами встроенного кондиционирования с внешним водяным контуром.

> Ключевое условие при составлении SLA – ориентация на бизнес-процессы заказчика, поскольку его цель – поддержание своего бизнеса, а не аренда вычислительных мощностей

О контейнерном ЦОДе с внешней инфраструктурой кондиционирования рассказал и Сергей Члек, руководитель направления BladeSystem HP в России. Это решение HP получило название Performance Optimized Datacenter (POD). Для достижения высокой плотности компоновки в 12-метровом ISO-контейнере разработчики HP разместили 19-дюймовые стойки собственного производства с глубиной 1000 мм и нестандартной высотой 50U. POD вмещает в себя 22 (!) таких стойки, образующие сплошной ряд, который делит контейнер на два «герметичных» коридора – горячий и холодный. В результате емкость контейнера составляет 1100U. За счет применения водяного охлаждения с многочисленными теплообменниками, расположенными под потолком, контейнер способен отводить до 27 кВт тепла от стойки (теоретически до 35 кВт), а в общей сложности – до 600 кВт. При этом ЦОД показывает высокую эффективность энергопотребления: заявленный компанией коэффициент PUE (power usage effectiveness) равен 1,25 при среднем значении по отрасли – больше двух.

В контейнере POD можно расположить, например, выносной высокопроизводительный серверный кластер для корпоративного ЦОДа или устроить резервный ЦОД для катастрофоустойчивых конфигураций. Однако надо помнить о том, что POD практически не содержит инженерной инфраструктуры – подача охлажденной воды для теплоотвода, как, впрочем, и бесперебойное электроснабжение, обеспечивается за счет внешних систем.

Тенденции комплектования и управления

Как это ни удивительно, но ИТ-наполнение современных российских ЦОДов уже во многом отечественное. Виктор Урусов, директор по продуктовому маркетингу и системной интеграции компании DEPO Computers, отметил, что половина производимых ими серверных систем закупается российскими ЦОДами, а, по данным аналитиков (Gartner и IDC), в первой половине 2009 г. этот производитель по числу поставляемых на российский рынок серверов вышел на второе место.

Выбор ИТ-систем для ЦОДов имеет свои особенности. Если для обычных корпоративных клиентов главный критерий выбора – отношение цена/производительность, то, как подчеркнул В. Урусов, для крупных ЦОДов таким критерием является отношение производительности к единице занимаемого в стойке объема (1U) или же удельное тепловыделение на 1U. По его словам, до настоящего времени 80% всех установленных серверов в российских ЦОДах составляют обычные двухпроцессорные 1U-серверы. Однако тенденция постепенно меняется и все большим спросом пользуются так называемые twin-системы высотой 1U или 2U, в чьи корпуса вставляются соответственно две или четыре материнские платы. Это своего рода компромисс, переходная форма между классическими и блейд-системами.

Производительность серверной «начинки» также с каждым годом растет по всем направлениям, и отправной здесь точкой является выпуск новых семейств процессоров (серверы DEPO Computers сегодня комплектуются новым семейством процессоров Intel с архитектурой Nehalem). А это влечет за собой и новые требования к ОЗУ серверов, устройствам ввода-вывода, накопителям на жестких дисках, системам коммутации и т.п. Кстати, именно Ethernet-коммутаторами DEPO Computer в этом году собирается пополнить комплекс своих решений для ЦОДов.

Собственно, суть ЦОДа изначально и составляла эта триада ИТ-оборудования – серверы, системы хранения данных и сетевые коммутаторы. Владельцы же крупных ЦОДов сталкиваются с проблемой согласованного управления всеми этими тремя «доменами» ИТ-инфраструктуры, поскольку нередко они находятся в ведении разных ИТ-специалистов или их команд. Очень часто такое управление осуществляется вручную с помощью консольных средств, а документирование и протоколирование ведутся в виде электронных таблиц или даже обычных текстовых файлов. Данный подход связан с большой вероятностью внесения ошибок при конфигурировании систем, а также с пло-

хой прогнозируемостью доступных вычислительных и сетевых ресурсов.

Один из подходов к этой проблеме разрабатывает HP. Как рассказал технический консультант департамента программных решений HP в России Константин Васильев, для унификации управления компания предложила программный комплекс Datacenter Automation, который включает в себя компоненты для управления серверами, системами хранения и сетевой средой, а также некий интегрирующий инструмент HP Operation Orchestration – визуальную среду программирования «кроссплатформенных» и «кросс-доменных» потоковых операций для автоматизации рутинных процедур в ЦОДах. Такой комплекс позволяет автоматизировать управление не только в чисто технологических «доменах», но и в смежных ИТ-системах, включая базы данных, службы каталога, почтовые серверы и т.п.

Особое внимание на проблему управления оборудованием в ЦОДе, связанную с отслеживанием доступных ресурсов, обратил Дмитрий Петров, инженер инфраструктурных проектов компании Complete. Например, для сбора информации в стойках ЦОДа о возможности резервирования оборудования по питанию, о доступных энергоресурсах (по потребляемой мощности и по физической доступности розеток), ресурсах охлаждения, да и просто о свободном пространстве для размещения оборудования, Complete предлагает использовать модуль Capacity Manager в составе комплексной системы мониторинга InfraStruXure Central Enterprise компании APC. Эта система ведет собственную инвентаризационную базу данных и способна в интерактивном режиме отслеживать, например, потребляемую оборудованием мощность благодаря интерфейсу с интеллектуальными PDU-системами.

Другой модуль той же системы – Change Manager – позволяет держать под контролем перемещение оборудования при внесении изменений в инфраструктуру ЦОДа. Это особенно актуально в крупных ЦОДах, где из-за большого объема инсталлированного оборудования после нескольких перемещений бывает трудно определить, в какой стойке установлен тот или иной сервер. Автоматизация учета оборудования производится с помощью штрих-кодов, наклеиваемых на стойки и серверы, и последующего их считывания сканером и занесения в инвентаризационную базу данных. Хранимая в базе данных информация отображается в графическом интерфейсе, и администратор может сразу определить, в какой стойке какое оборудование установлено.

Как мы видим, ЦОДы сегодня превращаются в место невиданной доселе концентрации разнообразного оборудования и систем, вследствие чего возникает новый уровень сложности управления, ответом на который становятся средства виртуализации ресурсов, организации облачных вычислений и централизации управления инженерной и ИТ-инфраструктурой. Очевидно, что спрос на эти технологии, все еще редкие для России, с каждым годом будет только возрастать. ИКС

Системы электроснабжения: что нового?

Алексей НОВИЧКОВ

Соревнование между брендами в отрасли систем бесперебойного электроснабжения сегодня идет в нюансах энергоэффективности, масштабируемости, удобства и простоты обслуживания, эргономики, систем управления, а также в деталях предоставляемого сервиса.

Принципы построения ИБП не могут меняться каждый год, а сами устройства разных поставщиков по мере развития рынка все больше сближаются по своим характеристикам. Крупные производители выпускают мало отличимые друг от друга серии продуктов, чему способствуют многократные слияния компаний, в ходе которых гранды индустрии докупают недостающие их ассортименту линейки.

Эффект масштаба

В новых моделях ИБП очевидно выделяется такое их качество, как модульность. Один из поставщиков – компания Chloride в своей серии продуктов Trinergy разработала даже специальную классификацию модульности: деление ее на вертикальную, горизонтальную и ортогональную. Первая означает функциональную модульность, повышающую ремонтопригодность устройства (по сути – быстрая замена специализированных модулей ИБП). Два других типа модульности характеризуют способ масштабирования мощности: горизонтальная – за счет добавления в ИБП новых модулей-шкафов; ортогональная – за счет параллельного подключения «цельных» ИБП-систем. Таким образом, мощность ИБП Trinergy может масштабироваться модулями по 200 кВт до 1,2 МВт, а целыми установками – до 9,6 кВА (до 8 параллельных систем). Сразу отметим, что этим принци-

пам масштабирования сегодня следуют практически все основные игроки рынка ИБП.

Недавнее предложение Chloride – продукты 80-Net MPR 30–40 кВА и 80-Net 60–200 кВА. ИБП этих серий могут объединяться в параллель без дополнительного контроллера: настройка одиночной системы для параллельной работы осуществляется посредством специализированного ПО. Добавим, что ИБП серии 80-Net могут быть оснащены встроенным трансформатором, обеспечивающим гальваническую развязку по току, необходимую для некоторых типов нагрузок.

На наличие трансформатора в своих схемотехнических решениях указывает и фирма GE Consumer & Industrial, российским партнером которой является компания «Абитех». Так, специалисты последней рекомендуют новый ИБП SG PurePulse этого поставщика для использования в ИТ- и телекоммуникационных отраслях. В настоящее время данная линия продуктов состоит из 10 моделей, мощность которых варьируется от 60 до 250 кВА.

Модульность – характерная черта современных ИБП, таких как устройства серии NH plus фирмы Delta Power Systems

Несмотря на то что сегодня многие производители фокусируются на бестрансформаторных решениях, позиционируя их как более легкие и компактные, компания GE Consumer & Industrial в серии SG PurePulse предлагает двухконтурную схему на IGBT-транзисторах с трансформатором на выходе, делая акцент на повышенной безопасности системы за счет гальванической развязки между шиной постоянного тока ИБП и нагрузкой. При этом устройство удалось сделать относительно компактным (по крайней мере по сравнению с предыдущими аналогичными моделями того же поставщика) и эргономичным: при мощности 500 кВА ИБП занимает площадь 1,7 м² (950 × 1800 мм), в сумме с площадью для обслуживания – 3,15 м² (доступ для сервисных операций осуществляется спереди).

Если вернуться к вопросу масштабируемости мощности за счет модульности, то весьма выгодно с этой точки зрения выглядит система Symmetra PX 250/500 кВт компании APC (в составе концерна Schneider Electric). Эта модель, выпущенная на рынок в 2009 г., рассчитана на ЦОДы малого и среднего размера, и ее мощность может наращиваться от 25 до 500 кВт с шагом 25 кВт.

Что касается «ортогональной» масштабируемости, то разработчики говорят об установке до четырех систем PX в параллель (появление опции ожидается в ближайшее время при выходе новых версий прошивок для управляющего модуля). Другие существенные характеристики ИБП – высокий КПД (96%, причем при загрузке от 35%), резервирование основных блоков, включая модуль управления, высокая компактность и как следствие – энергетическая плотность. Так, установка на 250 кВт вместе с аккумуляторными батареями (АКБ) размещается на площади 3,3 м², а аналогичный параметр для 500-кВт установки равен 5,7 м².

Не отставая от конкурентов в отношении масштабирования, компания Delta Power Systems предлагает ИБП серии NH plus мощностью 20 до 120 кВА. Наращивание мощности здесь так же может осуществляться и на основе установки дополнительных модулей, и путем параллельного подключения ИБП до 480 кВА (4 х 120 кВА). ИБП данной серии позволяют строить различные схемы резервирования как на модульном уровне, так и в параллельном подключении.

Бережливость, совместимость, управляемость

На высокую энергоэффективность своих новых ИБП серии Green Power мощностью от 100 до 200 кВА дела-

ет ставку и компания Socomec. По данным последней, их КПД также составляет 96% – величину, подтвержденную сертификационным агентством TUV SUV (правда, на графике, предоставляемом самой Socomec, заметно, что этот показатель немного падет при загрузке ИБП ниже 50%). Другой важный аспект, на который производитель обращает внимание, – это системы управления зарядом батарей (Expert Battery Service) и их мониторинга (Battery Health Check), позволяющие максимально продлить срок жизни АКБ.

При разработке ИБП нельзя забывать и о «комфорте» питающей электросети или дизель-генераторных установок (ДГУ), для обеспечения совместимости с которыми требуется поддерживать в заданных пределах ряд важных входных параметров ИБП. Компания «НойХаус Групп» объявила о доступности для заказа новых ИБП серии Power System Partner мощностью 100 и 120 кВА. Это трехфазные по входу и выходу системы, построенные с использованием IGBT-транзисторов. По своим характеристикам они стоят в ряду новинок с низким коэффициентом нелинейных искажений входного тока (< 3%) и высоким входным коэффициентом мощности (0,99). Они также наделены функциями плавного старта и запаздывания при включении в случае повторного пуска выпрямителя после возврата напряжения.

Бережная работа с питающей сетью и ДГУ – отличительная особенность ИБП Power System Partner фирмы «НойХаус Групп»

В сравнении с системами переменного тока ИБП постоянного тока намного компактнее, что делает их весьма привлекательными для использования совместно с вычислительным и телекоммуникационным оборудованием. По словам Виталия Синякова, председателя совета директоров ГК «Штиль», для выносных телекоммуникационных узлов, расположенных вне помещений, сегодня все чаще используют климатические шкафы, которые предъявляют довольно жесткие требования к размерам устанавливаемой в них «начинки». Поэтому разработчикам ИБП приходится стремиться к уменьшению размеров своих изделий.

Так, ГК «Штиль» в 2009 г. начала выпуск новой серии систем электропитания постоянного тока в виде блоков высотой 1–2U и мощностью от 350 Вт до 10 кВт. В качестве примера В. Синяков привел компактную модель ИБП постоянного тока «Штиль»

PS48-0030 (2/0800 1U) высотой 1U и глубиной 310 мм с выходным напряжением 48 В, обеспечивающую подключение нагрузки мощностью до 1600 Вт. В размер 1U укладывается и более мощная модель на 3600 Вт («Штиль» PS48-0070). Все ИБП данной серии оснащены аппаратами токовой защиты (выключателями защиты нагрузки и АКБ) и имеют встроенный контроллер с русскоязычным интерфейсом для локального и удаленного управления.

Если говорить о небольших ИБП переменного тока, то стоит отметить анонсированный компанией Tripp Lite ИБП SmartOnline SU10KRT3/1x мощностью 10 кВА/7 кВт с трехфазным подключением на входе и однофазным – на выходе. При его использовании мощность системы может наращиваться до 40 кВА путем подключения до четырех ИБП в параллельном режиме либо до 30 кВА с резервированием по схеме N + 1. ИБП рассчитан на установку в стандартную стойку и по высоте занимает 6U. Управление устройством может осуществляться через порты RS232, USB и Ethernet с помощью предустановленной платы Web/SNMP-управления. Будучи поставщиком комплексного оборудования электроснабжения, Tripp Lite начала выпуск новых моделей консольных серверов B092/B096, которые, в частности, оснащены встроенными приложениями PowerAlert и Network UPS Tools для централизованного управления распределенными ИБП, а также ПО PowerMan – для управления системами распределения питания (Power Distribution Unit, PDU) и резервными системами питания.

Контроллеры SC200 V3 компании Eaton, предназначенные для операторов связи, обеспечивают управление электропитанием в телекоммуникационных «выносах»

Сервисы и периферия

Очевидно, что дальнейшее развитие систем электроснабжения будет сопровождаться появлением новых сервисных функций ИБП или специализированных устройств, обеспечивающих интеллектуальное управление питанием.

Так, компания Eaton недавно объявила о выходе новой модели контроллеров SC200 V3 специально для телекомоператоров. Устройство является частью линейки продуктов Smarter Energy и предназначено для снижения энергозатрат.

Контроллер может устанавливаться в выносных узлах связи с разнородным оборудованием и в соответствии с заложенной в него логикой оптимизировать потребление электроэнергии в часы максимальной ее стоимости путем отключения нагрузки, некритичной для работы телекоммуникационного «выноса». В таких узлах контроллер может выполнять и другие сервисные функции (например, выдачу сигналов оповещения). Будучи установленным на узлах, где применяется ДГУ, контроллер SC200 V3 благодаря функции Eaton Fuel Saver позволяет более рационально расходовать топливо путем интеллектуальной задержки включения генератора и использования заряда батарей, для того чтобы поддержать работу систем во время непродолжительного отключения электропитания.

Компания Emerson Network Power предложила на российском рынке системы PDU семейства Liebert MPX и MPH, предназначенные для установки внутри стоек с электронным оборудованием (они дополнили уже имевшиеся у компании аналогичные устройства начального уровня). Отличительная особенность этих линеек продуктов – расширенные возможности мониторинга и управления. Помимо контроля за электрическими параметрами потребления аппаратуры (напряжением питания нагрузки, потребляемым током, коэф-

фициентом мощности и самой потребляемой мощностью в киловатт-часах), эти системы отслеживают еще температуру и влажность. Таким образом, они являются своего рода интегрированными датчиками параметров среды ЦОДа для централизованных систем диспетчеризации оборудования.

> Для выносных узлов вне помещений сегодня все чаще используются климатические шкафы, которые предъявляют жесткие требования к габаритам оборудования, поэтому разработчики стремятся к уменьшению размеров ИБП

Управление нового уровня

Доказательством того, что системы электроснабжения сегодня выделяются в отдельную инфраструктурную отрасль, может служить тот факт, что для них начинают создаваться системы управления по принципу АСУ ТП. Например, системный интегратор TEV (Transfer Equipment Vostok) – совместное российско-французское предприятие – разработал специализированную систему диспетчеризации и удаленного мониторинга гарантированного и бесперебойного электроснабжения ЦОДа для одного из российских сотовых операторов.

Этот программно-аппаратный комплекс построен на базе системы Trace Mode класса SCADA/HMI, поставляемой компанией AdAstra Reseach Group. Система управляет энергетическими установками суммарной мощностью 600 кВА, включающими в себя пять АВР, 10 ИБП и 15 силовых щитов. В реализованной конфигурации предусмотрено два полноценных автоматизированных рабочих места для операторов, обеспечивающих визуализацию состояния системы при помощи наглядного графического интерфейса.

По данным TEV, специализированный сервер Trace Mode GSM MPB+ собирает и анализирует информацию более чем о 2800 параметрах электроснабжения. Он же при помощи специального GSM-модема способен оповещать сотрудников ЦОДа о возникновении тех или иных критических ситуаций посредством SMS-сообщений.

■ ■ ■

Несмотря на то что революции в системах бесперебойного электроснабжения происходят редко, последние изменения в отрасли связаны с процессами интеграции различных технологий, что и создает общую динамичную картину ее развития. Другими словами, передовые разработки возникают на стыке разнородных систем и на основе современных программных средств, в результате чего ИТ-системы выходят на более высокий уровень надежности, а их инженерное обеспечение обретает новое качество. ИКС

Uptime Institute: время сертификации пришло!

Интервью с Максимом ИВАНОВЫМ, генеральным директором ADM Partnership

– Максим, вы уже давно сотрудничаете с Uptime Institute, в чем заключается ваше сотрудничество?

– С Uptime Institute мы сотрудничаем достаточно продолжительное время. Необходимо сначала рассказать о том, какие услуги он предоставляет. Uptime Institute – ведущая мировая организация, которая разрабатывает стандарты, определяющие функциональную устойчивость центров обработки данных (ЦОД), проводит постоянный мониторинг новых технологий и подходов к их строительству, ведет образовательную деятельность и оказывает консультации клиентам в области строительства ЦОДов для повышения их функциональной устойчивости. Одна из самых известных и значимых работ Института – это создание системы классификации ЦОДов по уровням надежности (так называемым Tier), образующей развитую систему оценки параметров, по которой владелец ЦОДа может получить представление о реальном уровне безотказности всего комплекса дата-центра. Институт проводит программу сертификации объектов на соответствие конкретного дата-центра тому или иному Tier, о чем составляется специальное заключение. Кроме того, Uptime Institute имеет большое количество обучающих программ. Наша компания сотрудничает с Институтом по трем направлениям – сертификации ЦОДов, консультациям клиентов и образовательным программам.

– Есть несколько систем, которые описывают уровни надежности ЦОДа. В чем отличие уровней Tier, предлагаемых Uptime Institute?

– В настоящее время наибольшее распространение получили три основных типа систем оценки уровней надежности ЦОДов. Широко используется система уровней Tier, предусмотренная стандартом TIA-942. Эта система достаточно точно формализует, какие уровни резервирования и где должны быть применены, чтобы достичь определенной статистической отказоустойчивости. К недостаткам этой системы можно отнести формальные критерии, удовлетворяя которым можно достичь абстрактной статистической надежности. На этапе проектирования и строительства ЦОДа все требования резервирования и соответствия стандарту могут быть формально соблюдены, но при этом реальная статистика отказов будет отличаться от расчетной. Поясню на примере. Скажем, стандарт предусматривает дублирование некой системы ЦОДа, предположим, системы кондиционирования, что положительно влияет на ожидаемую статистику отказов дата-центра. Но при этом за рамками регулирования остаются вопросы, как часто такая задублированная система может выходить из строя или какое время может пройти между «плановым» статистическим отказом и выводом системы на регламентное обслуживание, когда «часть дублирования» отсутствует, снижая таким образом на время обслуживания надежность системы климата (в нашем примере) и, как следствие, общую надежность ЦОДа.

Для оценки комплексной функциональной надежности, которая реально отвечает конкретной системе, расположенной на конкретной площадке, Uptime Institute разработал свою систему Tier. Сразу хочу заметить, что эта система Tier для уровней функциональной надежности ограничивается рассмотрением инженерных систем, обеспечивающих функционирование ИТ-комплекса ЦОДа, и не рассматривает вопросы ИТ-систем как таковых и их надежности в отдельности. Для более точного определения надежности ЦОДа Uptime Institute вводит понятие функциональной устойчивости, т.е. способности конкретного ЦОДа не терять своей функциональности вне зависимости от плановых или внеплановых событий. Такая система уровней надежности оценивает конкретные технологические решения и, что еще более важно, их реализацию на практике в конкретном ЦОДе.

Третьим вариантом оценки уровней надежности могут служить различные корпоративные стандарты, которые присутствуют во многих крупных компаниях и организациях в мире и активно начинают разрабатываться и внедряться в крупных российских компаниях, использующих ЦОДы как инструмент бизнеса. Это становится особенно актуальным в тех компаниях и организациях, где непрерывность бизнеса является ключевым фактором работы.

– Вы сказали, что Uptime Institute проводит программы сертификации ЦОДов на предмет соответствия тому или иному Tier. Как это происходит?

– Есть два наиболее распространенных сценария, когда клиент-вла-

делец ЦОДа сертифицирует свою систему. Первый, когда в Uptime Institute обращаются для сертификации уже готового дата-центра; второй, когда Институт привлекается на этапе разработке эскизного проекта или даже концепции будущего ЦОДа.

В первом случае с Uptime Institute Professional Services заключается контракт и сотрудники Института при содействии сертифицированных инженеров нашей компании выезжают на сертифицируемую площадку для инспекции проектной документации и оценки реализованных на ее базе технологических решений с точки зрения соответствия тому или иному уровню Tier, о чем и выдается сертификат. Если площадка не соответствует желаемому уровню надежности, то заказчику необходимо произвести технологическую доработку решений для повышения надежности до необходимого уровня. В таком случае мы можем порекомендовать заказчику программу доработки до желаемого уровня.

Второй сценарий гораздо в большей степени гарантирует прохождение сертификации на требуемый уровень. В этом случае предусматривается привлечение Uptime Institute Professional Services на самом начальном этапе, когда составляется концепция будущего ЦОДа, после чего весь объем проектирования выполняется либо силами Института, либо партнерами, которые имеют в штате сотрудников со статусом Accredited Tier Designer. После разработки проектной документации строительство дата-центра ведется под соответствующим технологическим надзором. При таком сценарии количество «сюрпризов» на этапе сертификации стремится к нулю и заказчик получает ожидаемый уровень надежности системы и сертификацию по соответствующему Tier.

– Что дает заказчику сертификация Uptime Institute?

– В получении сертификации ЦОДа есть ряд существенных преимуществ. Оговорюсь сразу, преимущества для корпоративного ЦОДа немного отличаются от преимуществ, которые получает коммерческий ЦОД. Начнем с последнего.

Сертификация коммерческого дата-центра – очень действенный маркетинговый инструмент, сильно выделяющий сертифицированную площадку на фоне конкурентов прежде всего по уровню надежности, который не просто декларируется, но подтвержден самой авторитетной экспертной организацией в мире. Кроме того, в последнее время коммерческие клиенты дата-центров все чаще предпочитают заключать договор с оператором ЦОДа, в котором указываются четкие параметры качества обслуживания (Quality of Service) и штрафные санкции за их несоблюдение. При наличии сертификации Uptime Institute владелец коммерческого дата-центра имеет уверенность в том, что обязательства перед клиентами будут выполнены и обеспечены проверенными техническими решениями.

Для корпоративного ЦОДа, когда основным клиентом и потребителем услуг дата-центра являются внутренние службы владельца, преимущества имеют иной оттенок. Помимо основного фактора – подтвержденной надежности, проверенной независимым экспертом, существенным преимуществом сертификации является фактор защиты инвестиций. Современный ЦОД – сложный инженерно-технический капиталоемкий комплекс. Капитальные затраты на такие системы работают многие годы, и особенно это актуально в части инженерного обеспечения. В идеале, вне зависимости от постоянно меняющейся конфигурации ИТ-системы, инженерный базис дата-центра должен обеспечивать бесперебойное функционирование всего комплекса. Каждый рубль, вложенный в инфраструктуру, должен работать максимально возможное время. На этапе построения идеологии и бизнес-стратегии использования дата-центра необходимо обозначить требуемую надежность системы, которая должна быть реализована в проектном решении. Известно, что любая переделка работающей системы обходится существенно дороже, чем строительство ее с нуля. Поэтому система, правильно спроектированная и построенная с прицелом на требуемую надежность и, как следствие, на сертификацию по конкретному уровню Tier, будет обладать более оптимальной совокупной стоимостью владения.

– Что кроме сертификации получает клиент от сотрудничества с Uptime Institute?

– Институт не является неким закрытым сообществом гуру, которые вещают миру мудрые мысли. Основным, неоценимым источником информации является сообщество владельцев дата-центров, которые общаются и делятся опытом в рамках ряда специальных программ, наиболее популярная из которых – Site Uptime Network. В этой программе участвуют около 100 владельцев крупных ЦОДов, которые постоянно обмениваются опытом, связанным с проектированием, строительством и эксплуатацией дата-центров. В рамках программы участники получают ценную информацию, которую они могут использовать как для эксплуатации и модернизации существующих ЦОДов, так и для строительства новых. Несколько раз в год проводятся представительные форумы, на которые приглашаются не только участники Site Uptime Network, но и ведущие производители технологических решений для дата-центров. Могу сказать с уверенностью, что такие форумы являются наиболее авторитетной площадкой для обмена опытом в индустрии.

– В июне нынешнего года компания ADM Partnership совместно с Uptime Institute Professional Services провела две представительные конференции в Москве и Санкт-Петербурге, которые вызвали большой интерес ИТ-директоров различных компаний. Какова была цель этих мероприятий и будут ли подобные форумы проходить в будущем?

– Вы правы, конференция вызвала большой интерес, в Москве мы даже наблюдали аншлаг, что говорит о востребованности тех идей, которые исповедует Uptime Institute. Основной целью данных мероприятий было более тесное и детальное знакомство с подходами к идеологии, проектированию и строи-

тельству ЦОДов, которые многие годы разрабатываются Институтом и реализуются на практике. Каждая конференция состояла из двух частей – рассказа о теоретических наработках по обеспечению функциональной устойчивости и рассмотрения конкретных практических решений при построении дата-центра. Каждый участник получил уникальный опыт, практические материалы и возможность личного общения с Питом Тернером (Pit Turner), президентом Uptime Institute Professional Services. В наши планы входит продолжить начинание 2009 года. Более того, могу сказать, что как раз после этих конференций в России началась активная работа по сертификации дата-центров.

– Какова сейчас ситуация с сертификацией ЦОДов в нашей стране?

– В настоящее время Uptime Institute при нашем содействии ведет работу с четырьмя компаниями по сертификации их дата-центров. Процесс сертификации занимает некоторое время, так как требуется детальное изучение проектной документации, уточнение ряда вопросов с заказчиком (здесь важный момент – обеспечение правильного технического понимания проектной документации, сделанной по российским нормам, специалистами Uptime Institute, которые привыкли к другой системе проектной документации. В этом наша компания оказывает существенное содействие и является интерфейсом между клиентом и Институтом) и инспекционный визит на конкретную площадку.

Кроме того, сейчас строится не менее пяти ЦОДов, владельцы которых уже на этапе проектирования взяли курс на получение сертификатов.

– Могли бы вы назвать эти компании?

– Следите за новостями на страницах «ИКС»! Могу только сказать, что среди упомянутых мной проектов по крайней мере один может быть сертифицирован по уровню Tier IV, не менее трех будут соответствовать уровню Tier III. В целом считаю такой интерес к сертификации достаточно убедительным фактором становления российского рынка дата-центров.

– Кого больше интересует сертификация – владельцев корпоративных дата-центров или коммерческих?

– К моему удивлению, среди упомянутых компаний наблюдается паритет. Половина – это корпоративные клиенты, половина – коммерческие ЦОДы. Последнее особенно отрадно. Не секрет, что в период становления рынка коммерческих дата-центров первые (да и многие последующие) проекты строились в условиях очень ограниченных бюджетов и для инвесторов вложения в такие проекты были часто рискованными. Как следствие, требовалась максимально быстрая окупаемость, что, в свою очередь, приводило к максимальной экономии на всем. В последние пару лет и сегодня, даже несмотря на текущие кризисные времена, наблюдается тенденция строительства реально качественных площадок. Увеличивается спрос на более цивилизованные услуги, а это как раз и определяет желание сертифицировать свои площадки для получения серьезных клиентов. Хотя это не исключает и продолжение развития и увеличения количества простых площадок, которые могут быть сертифицированы по Tier I и Tier II. Главное, чтобы каждый клиент имел ЦОД именно того качества, которое ему требуется.

– Не считаете ли вы, что девять сертифицированных ЦОДов – это не так много в масштабах нашей страны?

– Проектирование и сертификация ЦОДов – это область, где олимпийский принцип «главное – не победа, а участие» во многом работает. Несмотря на то что для Uptime Institute и нашей компании консультации по проектированию надежных дата-центров и их сертификация являются бизнесом, основной момент в этой деятельности – обмен опытом, который нацелен на создание функционально устойчивых ЦОДов. Никто не гонится за количеством сертифицированных площадок. Важнее, чтобы владельцы дата-центров, обмениваясь информацией, строили наиболее правильные для себя системы. В этом плане можно перефразировать известную крылатую фразу: сертификация – дело добровольное! Если компания или организация не имеет планов по сертификации площадки, то наработанный опыт может быть с успехом применен в составлении корпоративных стандартов для ЦОДа. В нашей практике есть ряд примеров, когда на базе знаний и идеологии Uptime Institute были разработаны и очень успешно внедрены корпоративные стандарты для крупных заказчиков, которые имеют сети ЦОДов, распределенные по всей стране и работающие как единая функционально устойчивая система.

– Расскажите о компании ADM Partnership.

– Мы являемся инжиниринговой компанией, специализирующейся на проектировании и управлении сложными инженерными проектами. Центры обработки данных – одно из наших главных направлений работы. Мы успешно сотрудничаем со многими ведущими системными интеграторами в области комплексного проектирования и строительства вычислительных комплексов. Нашей компанией накоплен более чем 15-летний опыт в области проектирования и создания инженерных систем различного назначения. ADM Partnership спроектировала в совокупности свыше 40 вычислительных центров суммарной мощностью более 200 МВт. Объединяя наш опыт, знания Uptime Institute и возможности ведущих системных интеграторов, заказчики могут создавать самые надежные вычислительные комплексы для решения широкого спектра задач.

– Спасибо.

Какими средствами администрировать СКС?

Физической основой подавляющего большинства современных информационно-вычислительных систем являются структурированные кабельные системы. По статистике, конфигурация ИВС в отношении конкретного пользователя изменяется каждые полтора года, а то и раз в полгода, причем зачастую требуется переключение на уровне СКС. Этот процесс необходимо держать под контролем – с помощью систем управления.

Андрей СЕМЕНОВ, директор по развитию «АйТи-СКС»

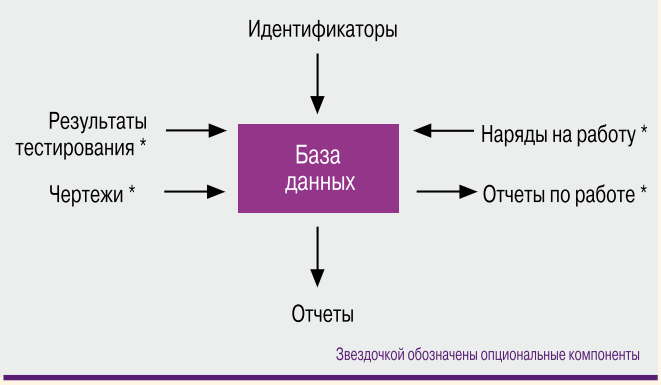
Схема построения системы администрирования

Изменение конфигурации СКС традиционно называется администрированием. Соответствующие процедуры детально регламентированы стандартами TIA/EIA-606-A и ISO/IEC 14763-1, что свидетельствует об их важности.

Центральным элементом концепции администрирования независимо от формы ее реализации является специализированная база данных (рис. 1), которая может существовать как в электронной форме, так и на бумажных носителях (TIA/EIA-606-A допускает применение последнего варианта БД для небольших сетей). База данных строится вокруг определенного реперного элемента. Для формирования маркирующего индекса используется подробно описанная в стандартах система суффиксов и префиксов требуемой глубины, которыми в обе стороны наращивается обозначение реперного элемента. В зависимости от области применения реперным элементом может служить шкаф (ANSI/TIA-942), техническое помещение (TIA/EIA-606-A) или даже целое здание.

Естественное стремление к использованию преимуществ современных средств обработки данных привело к тому, что наибольшее распространение получили электронные варианты баз данных систем администрирования СКС. Европейский стандарт EN-50174-1 дополнительно подчеркивает целесообразность применения при построении крупных СКС (с количеством портов более 10 тыс.) оборудования интерактивного управления, в котором БД является одной из двух главных составных частей.

Рис. 1. База данных как центральный элемент системы администрирования СКС (по ISO/IEC 14763-1)



Основная проблема администрирования СКС

В составе канонической СКС нет никакого штатного источника энергии. Поэтому при изменении конфигурации ИВС на физическом уровне приходится выполнять большой объем ручных работ. Системному администратору – главному действующему лицу в данном процессе – даже при элементарном переезде пользователя в соседнее помещение требуется осуществить многоступенчатую процедуру, результаты которой в

обязательном порядке нужно отразить в эксплуатационной документации.

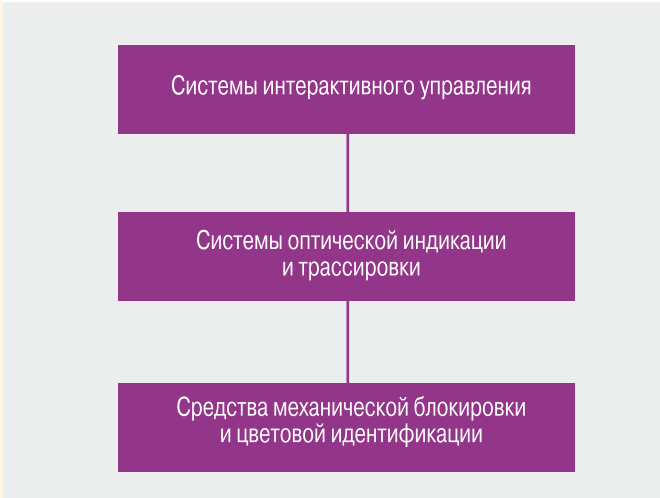
Эффективность управления СКС в немалой степени зависит от того, насколько точно база данных администрирования отражает фактическую конфигурацию кабельной системы. В таких условиях резко возрастает значение человеческого фактора. Попытки преодолеть негативные последствия наличия этого слабого звена вызвали к жизни разнообразные системы более или менее глубокой автоматизации рутинных операций администрирования.

Разновидности технических средств администрирования СКС

База данных системы администрирования может быть самостоятельным продуктом или же, что встречается чаще, входить в состав системы интерактивного управления. Поэтому, чтобы обеспечить единство терминологии, самостоятельные БД администрирования нередко называют системами неинтерактивного управления СКС.

Для повышения (часто весьма существенного) эффективности администрирования, кроме чисто программных средств, в инженерной практике широко используются многочисленные программно-аппаратные и аппаратные решения, хотя они не упоминаются в действующих и перспективных редакциях основных нормативных документов по СКС. К категории таких продуктов относятся коммутационные шнуры с опцией оптической индикации и трассировки, а также элементы механической блокировки некорректного подключения и ошибочного отключения (рис. 2).

Рис. 2. Иерархия технических средств поддержки администрирования СКС



Немалый вклад в увеличение эффективности администрирования может внести и системный интегратор, создающий кабельную систему. Для этого в его распоряжении имеется целый ряд проектных приемов, позволяющих обойтись серийной элементной базой и не требующих новых разработок. В перечень таких приемов входят: конструктивная неоднородность, формирование коммутационного поля в виде отдельных функциональных секций, использование панелей и розеточных модулей с различной окраской и т.д.

Программные продукты для неинтерактивного управления СКС

Как отмечалось выше, продукты этой категории представляют собой специализированные базы данных. В настоящее время на отечественном рынке присутствует несколько программных систем администрирования СКС (Crimp for Windows, Cable System Manager, CableScout и некоторые другие). Они достаточно близки по функциональным возможностям и, помимо графического пользовательского интерфейса, отличаются от друг друга главным образом набором выполняемых функций. Полностью заполненная и готовая к передаче в эксплуатацию БД системы администрирования также может быть получена в результате работы системы машинного проектирования кабельной системы (отечественная разработка nanoCAD).

Специализированные БД для неинтерактивного управления СКС имеют общие отличительные особенности:

- функционируют на выделенном сервере и при наличии соответствующих допусков обеспечивают чтение и запись информации по ЛВС или даже через Интернет;
- вследствие большого объема содержащейся в них информации, а также развитой графической системы представления информации, предъявляют высокие требования к станции управления сетью и к пропускной способности канала связи;
- в них поддерживается интуитивно понятный пользовательский интерфейс и ряд широко распространенных функций, таких как перетаскивание объектов, переход между уровнями с помощью древовидного представления структуры и т.д.;
- в ряде случаев предоставляется возможность управления не только кабельной системой здания, но и активным сетевым оборудованием ЛВС, сетей доступа и даже сетей связи общего пользования;
- обеспечивается доступ к вспомогательной информации – протоколам измерений конкретной линии, индивидуальным пользовательским данным, параметрам эксплуатируемого оборудования – с возможностью инвентаризации имеющихся ресурсов.

Специализированный характер БД проявляется в наличии встроенной в нее развитой системы контроля и проверок, а также защиты от некорректных и несанкционированных действий администратора. Одно из возможных средств контроля, например, – деление всех нарядов на работы на срочные, текущие, незавершенные и выполненные и генерация предупреждающих сообщений в случае отсутствия отметки о выполнении в заданные сроки. Наиболее очевидная функция защиты – запрет попытки прямого соединения оптических и симметричных трактов передачи без использования преобразователя среды, блокирование под-

ключения одномодовой стационарной оптической линии к многомодовой и т. п.

Особенность системы неинтерактивного управления, интересная и полезная с практической точки зрения, – простота включения в область ее действия активного сетевого оборудования. Для этого любая аппаратура (коммутатор ЛВС, станция РЛЛ, система спектрального уплотнения и т.д.) описывается в системе не в виде точки, а в форме «протяженного» объекта, имеющего вход и выход, что позволяет применить для его описания тот же подход, что и для кабеля. В результате в процессе поиска маршрутов формирования каналов система управления БД получает возможность выйти за пределы пассивной части сети и включить в список анализируемых вариантов и те из них, которые создаются на более высоких уровнях модели открытых систем.

Распространение системы неинтерактивного управления на активное сетевое оборудование существенно упрощает многочисленные вспомогательные процедуры, которые должны выполняться в процессе эксплуатации сети, – инвентаризацию ресурсов, балансировку трафика, построение обходных маршрутов в аварийных ситуациях, формирование резервных трактов при повышенных требованиях к отказоустойчивости сетей и т.п.

Общий принципиальный недостаток неинтерактивных программных систем – необходимость жесткой пользовательской дисциплины: все изменения обязательно должны отражаться в БД. Практика эксплуатации СКС свидетельствует о том, что именно с этим возникают серьезные проблемы, в том числе из-за того, что конфигурация СКС меняется относительно часто (0,5–1,5 раза в год в пересчете на одну пользовательскую информационную розетку). Поэтому, хотя многие производители СКС периодически предлагают подобные продукты, широкого распространения они не получили.

Оборудование интерактивного управления СКС

Такое оборудование впервые появилось на рынке еще в начале 90-х годов прошлого столетия (система PatchView израильской компании RiT Technologies). В настоящее время практически все ведущие производители СКС имеют в составе своих продуктовых линеек оборудование данной категории. Эти решения представляют собой программно-аппаратный комплекс и внедряются в существующую или вновь создаваемую СКС методом наложения, что дает возможность не нарушать фундаментальное положение базовых стандартов о запрете параллельного подключения к цепям передачи в пределах стационарной линии.

Программная часть комплекса – это опять же специализированная БД. Аппаратная часть включает в себя управляющий контроллер и датчики подключения коммутационных шнуров к розеткам коммутационных панелей, а также элементы оптической и текстовой поддержки изменения конфигурации СКС.

Оригинальные системы интерактивного управления в СКС на базе датчиков собственной разработки

Тип СКС	Компания-производитель	Торговая марка системы управления	Тип датчика подключения
Smart	RiT Technologies (Израиль)	PatchView	Контактный (10-контактная вилка)
–	Data-complex (Германия)	.max	Бесконтактный (RFID-метка)
Systimax	Commscope (США)	iPatch	Бесконтактный (световой затвор)
–	TKM (Германия)	Future-Patch	Бесконтактный (RFID-метка)
PowerCat	MolexPN (США)	MIIM	Бесконтактный

Общее количество портов СКС, которое потенциально может быть охвачено системой интерактивного управления, оказывается сравнительно небольшим из-за разового характера инсталляций. В связи с этим для производителя СКС данное направление бизнеса не является приоритетным, несмотря на маркетинговую значимость крупных проектов. Такое положение дел не способствует проведению масштабных НИОКР и приводит тому, что на открытом рынке предлагается относительно немного оригинальных продуктов (см. таблицу). При этом даже ведущие мировые производители СКС довольно охотно идут на заключение OEM-контрактов с компаниями, которые (за исключением RiT Technologies) занимаются исключительно разработкой оборудования интерактивного управления.

Представленные в настоящее время на рынке продукты относятся уже к третьему поколению систем интерактивного управления СКС. Их основные характерные черты таковы:

- архитектура клиент–сервер;
- отказ от использования двух разновидностей сканеров в пользу однотипных устройств, более удобных с эксплуатационной точки зрения;
- переход на бесконтактные датчики подключения, что позволяет существенно более простыми средствами обеспечить для системы управления ту же продолжительность гарантийной поддержки, что и для самой СКС;
- использование в качестве средства поддержки процесса изменения конфигурации СКС светодиодов, индивидуальных для каждого порта.

Большое внимание разработчики уделяют простоте внедрения системы интерактивного управления в построенные ранее СКС. В связи со все более широким распространением СКС, реализованных на базе моноблочных панелей, используются преимущественно различные накладки на лицевую пластину этого коммутационного элемента. Накладка может как плотно прилегать к панели (продукты RiT, Tyco Electronics), так и выполняться в форме козырька, нависающего над отдельными портами (TKM и Data-complex). Соответственно, в первом случае подключение к сканеру выполняется с помощью ленточного кабеля, разъем которого находится с задней стороны панели. Во втором случае применяется вертикальная боковая планка, устанавливаемая на монтажном рельсе 19-дюймового конструктива.

Принцип предварительной подготовки оборудования к внедрению системы интерактивного управления может быть распространен также на коммутационные шнуры. Для этого их вилки могут снабжаться внешними кармашками, куда при необходимости вставляется RFID-метка (хвостовик типа «кенгуру»).

Еще одна тенденция современных систем интерактивного управления СКС – миниатюризация сканеров, которая позволяет экономить обычно дефицитные посадочные места в шкафах и стойках. Часто они выполняются в виде блока размером чуть больше пачки сигарет и монтируются в центральную часть коммутационной панели (решения компаний Panduit и Siemon).

Особняком от других систем интерактивного управления пока стоит продукт MIIM компании Molex. В нем, как и в продукте iPatch, используются обычные коммутационные шнуры. Однако установка на линейный кабель панельного компонента чувствительного элемента датчика подключения, выполненного в виде скобы, производится в этой системе не только в коммутационной панели, но и в пользовательской розетке. Это позволяет расширить область действия системы за пределы коммутационного поля в техническом помещении и контролировать всю стационарную линию. При синхронизации баз данных систем управления СКС и ЛВС осуществляется полный контроль нижних уровней информационной инфраструктуры.

Дополнительно отметим, что БД системы интерактивного управления СКС по своим функциональным возможностям обычно несколько уступает конкурирующим продуктам неинтерактивного типа. Обусловливается это ограниченным количеством тех компонентов СКС и сопутствующей инфраструктуры, на которые могут быть установлены чувствительные элементы. Базы данных обеих разновидностей сразу или после минимальной адаптации, выполняемой сотрудниками отдела автоматизации, легко могут быть интегрированы в общую систему управления предприятия.

■ ■ ■

Администрирование современной СКС подробно описано профильными американским и международным стандартами. Центральный элемент системы администрирования – классическая база данных. Если она реализована в форме специализированного программного продукта, появляется возможность задействовать в этом процессе все достижения современных аппаратных и программных средств электронной обработки данных. Наибольшая эффективность администрирования достигается при применении системы интерактивного управления СКС. Имеющиеся на рынке продукты этой категории отличаются хорошими функциональными возможностями и в ряде случаев могут быть без серьезных проблем внедрены в построенную ранее кабельную систему. ИКС

SOS! Как защитить оборудование FTTx?

Михаил РАПОПОРТ,
заместитель гендиректора по развитию компании «Пауэр Инжиниринг»

FTTx сегодня – одна из наиболее популярных технологий создания сетей широкополосного доступа. Но построить сеть – только часть задачи. Необходимо также обеспечить гарантированное электропитание активного оборудования, его сохранность и своевременное оповещение оперативного персонала провайдера услуг о возникающих нештатных ситуациях на всех элементах сети.

Сети оптического доступа позволяют протянуть симметричные широкополосные каналы связи непосредственно в дома и квартиры пользователей. Следствием такой возможности является необходимость размещения активного телекоммуникационного оборудования в непосредственной близости от абонента, т.е. на чердаках, в подъездах, подвалах и других технологических помещениях многоквартирных жилых домов и производственных зданий.

Однако эти площадки зачастую абсолютно не охраняются и перед провайдером встает не только вопрос «где установить оборудование?», но и ряд других, не менее важных:

- ✓Как не допустить повреждения или хищения оборудования?
- ✓Как создать необходимые климатические условия для его функционирования?
- ✓Как обеспечить независимость работы элементов сети от нестабильности сети первичного электроснабжения, к которой оборудование подключается, от импульсных и наведенных помех?
- ✓Как своевременно известить оперативный персонал оператора связи о нештатной ситуации на узле?

Ответы, казалось бы, лежат на поверхности...

Для обеспечения сохранности оборудования удаленного абонентского узла надо поместить все активное и вспомогательное оборудование в некоторый шкаф, который поможет предотвратить несанкционированный доступ, порчу или хищение установленных внутри компонентов узла. Для защиты от помех и перебоев в энергоснабжении смонтировать в шкафу систему бесперебойного электропитания, а для контроля за объектами и элементами сети – предусмотреть систему мониторинга.

Но какие конкретно параметры должны быть у этого шкафа и сопутствующих ему систем жизнеобеспечения? Стремясь разработать оптимальное решение по строительству узлов удаленного доступа, компания «Пауэр Инжиниринг» проанализировала ряд уже действующих сетей FTTx и провела опрос клиентов на предмет определения наилучших вариантов защиты оборудования.

Антивандальность

Провайдеры сошлись во мнении, что стенки металлического антивандального шкафа, монтируемого в помещении со свободным доступом, должны быть толщиной 1,5–2 мм. Дверцу необходимо оборудовать замком с трехточечной фиксацией и скрытыми от доступа извне петлями; конструкция дверцы должна исключать возможность ее вскрытия путем отжимания со стороны петель. Также необходим дополнительный силовой элемент по периметру. Кроме того, есть смысл защитить замочную скважину отдельно фиксируемой шторкой для предотвращения засорения личинки замка и вывода его из рабочего состояния.

Поскольку невозможно предугадать, с какой стороны в месте установки шкафа будет удобнее заводить внутрь силовые, оптические и Ethernet-кабели, логично обеспечить возможность ввода/вывода кабелей со всех четырех сторон и при этом обязательно снабдить эти технологические отверстия стальными легкосъемными заглушками.

В зависимости от комплектации и места установки шкафы могут иметь высоту от 6U до 15U полезного пространства для размещения оборудования и глубину 400–600 мм.

При проработке организации внутреннего пространства шкафа стоит предусмотреть место для хранения технологического запаса кабелей между одной из боковин шкафа и направляющими 19-дюймового конструктива, так как при строительстве сети кабели прокладываются, как правило, с некоторым запасом.

Рис. 1. Антивандальный телекоммуникационный шкаф (серия ME Y)

Система вентиляции

Одно из ключевых условий работы электронного оборудования – тепловой режим. Для определения параметров системы вентиляции и предотвращения перегрева оборудования необходимо провести тепловые расчеты шкафов узлов доступа. При этом надо ориентироваться на самый неблагоприятный режим функционирования оборудования, т.е. когда его тепловыделение максимально: источник бесперебойного питания работает от аккумуляторов, а Ethernet-коммутаторы загружены на 100%. При проведении расчетов можно исключить из рассмотрения пассивные элементы, а также пренебречь выделением тепла в электрическом счетчике, автоматическом выключателе и блоке розеток.

Вычисления производятся путем решения системы уравнений, описывающей теплопередачу в стационарном режиме и включающей в себя: уравнение теплоотдачи от поверхности оборудования к воздушному пространству внутри шкафа; основное уравнение теплопередачи от воздушного пространства внутри шкафа через стенку в окружающую среду (с учетом вентиляционных отверстий и воздушных потоков в шкафу); уравнение неразрывности теплового потока. Решение осуществляется, например, с применением программного пакета MathCad. В результате расчета получаем значения средних температур поверхности оборудования, воздушной среды внутри шкафа и поверхности стенки шкафа. И эти значения должны удовлетворять требованиям функционирования оборудования.

Обеспечение бесперебойного питания

Комплектовать шкаф узла удаленного доступа предпочтительнее источником бесперебойного питания форм-фактора 19". Для удобства эксплуатации, особенно в условиях ограниченного пространства, вся коммутация ИБП должна выводиться на лицевую панель. Как вариант – система питания может дополнительно оснащаться встраиваемым SNMP-адаптером, что позволит дистанционно контролировать работу устройства и управлять им.

Контроль системы питания может осуществляться как посредством штатной системы мониторинга производителя ИБП, так и путем интегрирования ее в существующую систему мониторинга объекта в целом.

По оценке провайдеров, ИБП должен обеспечивать электроснабжение объекта в течение как минимум 30 минут.

Мониторинг узла удаленного доступа

При эксплуатации разветвленной по территории населенного пункта сети широкополосного доступа очень важно, чтобы диспетчерская служба провайдера могла непрерывно дистанционно контролировать все узлы сети и получать оперативную информацию о возникающих нештатных ситуациях (попытках несанкционированного вскрытия, перебоях в сети внешнего энергоснабжения, попадании воды внутрь шкафа в результате аварии магистралей тепло- или водоснабжения в сооружениях, где установлено оборудование, возгорании или задымлении и т.д.).

Несомненным достоинством такой системы будет наличие возможности осуществлять контроль как с помощью специального ПО, так и по открытому протоколу SNMP, что позволит интегрировать систему мониторинга узла удаленного доступа в уже существующую систему наблюдения за телекоммуникационным оборудованием на базе единого программного обеспечения, установленного у провайдера.

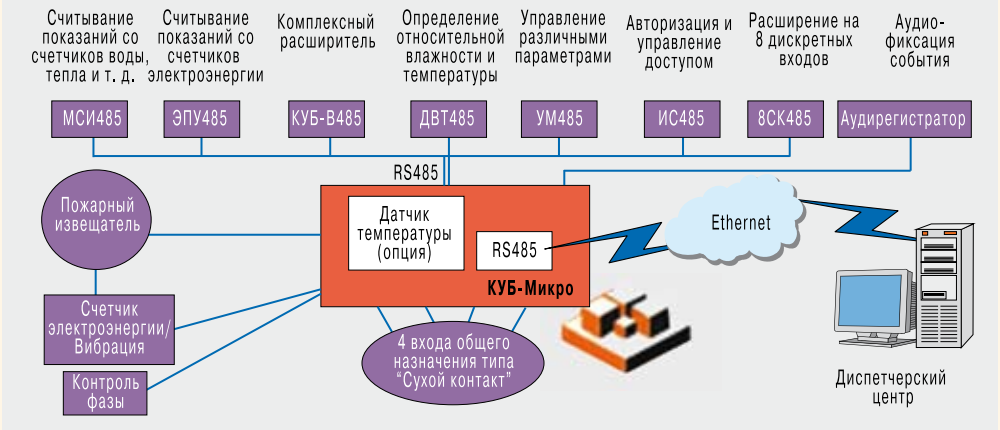
В качестве примера можно привести систему мониторинга, выполненную на основе контроллера «КУБ-Микро» (рис. 2), обеспечивающую контроль объекта в режиме реального времени и передачу сообщений оперативному персоналу о возникающих аварийных ситуациях (открытии дверцы, попытке взлома, выходе значений температуры и влажности внутри шкафа за установленные пределы, затоплении и пожаре, пропадании внешнего электропитания и пр.).

■ ■ ■

Итак, резюмируем: для обеспечения максимальной защиты оборудования дверцы антивандальных шкафов должны иметь замок с фиксацией в трех точках, скрытые петли, конструкцию, затрудняющую «отжимание» дверцы со стороны петель и дополнительный силовой элемент по периметру.

Узел доступа оснащается вспомогательным оборудованием. Шкаф должен быть укомплектован: вводно-распределительным устройством с установленным на нем прибором учета электроэнергии, поддерживающим возможность дистанционного снятия показаний; вводным автоматом защиты, блоком розеток и пакетным переключателем; источником бесперебойного питания со встроенной аккумуляторной батареей; системой мониторинга; оптическим кроссом и опционально распределительным устройством для кабелей UTP и кабельным органайзером. ИКС

Рис. 2. Система мониторинга на основе «КУБ-Микро»



CBOSSdm – система интеллектуальной поддержки CRM-проектов

Решение CBOSSdm создано специально для отделов маркетинга и продаж телеком-операторов.

Пользователи системы могут проводить сложные маркетинговые исследования абонентской базы, сегментировать ее по критериям ценности и доходности, разрабатывать оптимальные тарифные планы, определять профили потребления услуг абонентами, анализировать потребительскую корзину пользователей, составлять перечень активных абонентов, склонных к смене оператора, рассчитывать вероятный отток по всей базе или выделенному сегменту и предлагать комплекс мер по его снижению.

В результате оператор получает возможность:

- увеличить «стаж» абонентов и повысить их удовлетворенность услугами компании;
- снизить потери от блокировок и ухода абонентов;
- сократить затраты на продвижение и ускорить ввод в эксплуатацию новых услуг;
- снизить издержки на продажи и маркетинг за счет автоматизации рутинных процессов компании.

Реальная практика применения CBOSSdm показывает, что с помощью системы можно сохранить до 80% абонентов из числа тех, кто мог отказаться от услуг компании.

Одно из преимуществ решения – дружественный и эргономичный интерфейс, ориентированный на бизнес-пользователей. Для работы с CBOSSdm не требуется привлекать ИТ-специалистов или обладать глубокой технической подготовкой. Оператору системы не приходится иметь дело со сложными математическими методами и алгоритмами интеллектуального анализа данных (data mining) – он видит только исходные данные и результаты, необходимые для принятия решения.

При обращении к CBOSSdm пользователь просто выбирает задачу, которую необходимо решить, например спрогнозировать возможный отток абонентов. В диалоговом режиме он определяет настройки отбора информации, период времени, за который проводится анализ, а также степень детализации результатов. После этого система производит обработку данных и с заданной вероятностью формирует список абонентов, которые в течение ближайшего времени могут отказаться от услуг компании.

CBOSSdm обеспечивает высокое качество принимаемых решений. Система дает возможность оперировать наглядными списками абонентских номеров, в которых отражены такие важные параметры, как:

- ценность клиента для оператора;
- доходность;
- предпочтения в использовании услуг;
- принадлежность к маркетинговым сегментам;
- склонность к смене оператора.

CBOSS®

Дополнительная информация на сайте www.cboss.ru

Протокол-тестер

LTS5100 – решение операторского класса для тестирования сетей классической, мобильной и IP-связи. Устройство поддерживает 3G- и LTE-интерфейсы, позволяет контролировать конвергентные сервисы, а также облегчает создание и отладку новых услуг.

Особенностью LTS является возможность проведения тестов как в режиме мониторинга, так и в комбинации с генерацией трафика, симуляции работы элементов сети.

Некоторые из вариантов использования прибора:

- мультипротокольный мониторинг, контроль конвергентных сервисов;
- тестирование качества услуг;
- тестирование взаимодействия оборудования различных производителей;
- функциональное тестирование оборудования и приложений;
- отладка новых услуг перед запуском в коммерческую эксплуатацию;
- стрессовое тестирование (для SS7 – 600 CPS на 1 поток E1, для SIP – до 15 тыс. CPS);
- проверка сетей на уязвимость;
- имитация DDoS-атак – до 12 тыс. соединений/с;
- тестирование на соответствие тому или иному протоколу.

Поддерживаемые протоколы: SIP, SDP, RTP, RTCP, Skinny, MEGACO, MGCP, H.323, H.248, DIAMETER, RADIUS, FTP, TELNET, SSH, DHCP, IMAP, CIFS, POP3, NETBIOS, M3UA, M2UA, M2PA, SUA, DUA, IUA, SCTP, GSM MAP, IS-41, RANAP, ALCAP, NBAP, LTE S1AP, LTE X2AP, GTP, TCAP, SCCP, INAP, CAMEL, WIN, GTP, SNDCP, TOM, Gb NS, Gb LLC, BSSGP, BSSAP, BSSMAP, DTAP, MM/CC/SM, TOM, GSM Radio L3, GSM Radio SS, GSM Radio GMM/SM, GSM Radio LCS, GSM Radio SM-CP, SS7 ISUP, MTP, DSS1, QSIG, DPNSS, V5.2, V5.1, LAPD, LAPF, HDLC, R1, R1,5, R2 и т.д.

Поддерживаемые кодеки: G.711, G.723, G.729, 3GPP 06.10, LPC-10, GSM FR, GSM EFR, AMR (со скоростью 12,2, 10,2, 7,95, 7,4, 6,7, 5,15 и 4,75 кбит/с).

Программное обеспечение и документация русифицированы.

Linkbit: (495) 361-2000

Камеры видеонаблюдения
с интеллектуальным детектором движения

Семейство аналоговых камер видеонаблюдения с технологией Super Dynamic 5 (SD5) объединяет серию WV-CP500 в стандартном корпусе и вандалозащищенные фиксированные купольные камеры серии WV-CW500.

Технология SD5 обеспечивает высокую чувствительность (0,3 лк в цветном режиме), высокое разрешение (650 ТВЛ в цветном режиме), 3-D-оптимизацию цвета, цифровое шумоподавление и увеличенный в 128 раз динамический диапазон по сравнению со стандартным режимом. Также в камерах используется технология Adaptive Black Stretch (ABS) для «вытягивания» изображения в затемненных областях и интеллектуальный детектор движения (i-VMD), который определяет, был ли объект удален или оставлен в определенной зоне, и выдает тревожный сигнал при попытках расфокусировать или закрыть камеру.

Обе модели оснащены функцией заднего фокуса (ABF) для настройки точной фокусировки путем коррекции положения CCD-матрицы при переключении режимов день/ночь.

Функция автоматической стабилизации изображения дает возможность установить камеру в местах с вибрацией или сильными порывами ветра.

Вандалозащищенные фиксированные камеры серии WV-CW500 оснащены водо- и пыленепроницаемым куполом класса IP66. Устройство удаления влаги позволяет использовать камеру в различных погодных условиях, дополнительный обогреватель поддерживает необходимую рабочую температуру.

Panasonic Corporation: (495) 739-3443

Угловая патч-панель

RiT SMART CLASSix 48 UTP – патч-панель, соответствующая стандартам категории 6 и предназначенная для высокоскоростных приложений, таких как ATM 622 Мбит/с, Gigabit Ethernet 1000 Мбит/с и т.д.

Панель удобна для монтажа и терминации. Наличие угла в 130˚ дает возможность увеличить плотность монтажа в стойке за счет увеличения радиуса изгиба патч-кордов и использования вертикальных кабельных органайзеров вместо горизонтальных. Для заделки кабеля в патч-панели используется стандартный инструмент для разъемов типа 110 или Krone.

Панель поставляется в двух вариантах: для обычных СКС и для управляемых сетей. Управляемая версия оснащена светодиодными индикаторами (LED), позволяющими сократить время работы на кроссовом поле, уменьшить число ошибок и повысить производительность труда ИТ-персонала.

Основные характеристики:

- поддержка 48 портов в 2U;
- соответствие стандартам ANSI/TIA/EIA-568-B.2-1, ISO/IEC11801 2-я редакция (2002) и CENELECEN50173 (2002) для категории 6/класс E;
- обратная совместимость с категорией 5e;
- поддержка горизонтального кабеля 22-24 AWG и 24-26 AWG патч-кабеля;
- цветная маркировка для расшивки кабеля соответствует стандартам T568A и T568B.

Патч-панель доступна как с поддержкой PatchView, так и без нее.

RiT Technologies: (495) 684-0270

Установка электропитания «Штиль» PS48042T-2.01

Мобильная установка электропитания предназначена для применения в качестве резервного источника питания при проведении ремонтных и профилактических работ основной системы электропитания объекта связи, а также в качестве временного основного источника питания телекоммуникационного оборудования при выходе из строя базовой системы электропитания.

В комплект поставки входят два переносных модуля с аккумуляторными батареями 48 В, 26 А·ч. Общий вес УЭП с аккумуляторными модулями – 37 кг, что позволяет доставлять их к месту ремонта на автомобиле или даже вручную. Установка электропитания поддерживает все необходимые сервисные функции по работе с аккумуляторными батареями, включая защиту от глубокого разряда.

Входные характеристики:

- тип входной сети: однофазная, 220 В, 50 Гц;
- диапазон входного напряжения: 150–300 В;
- коэффициент мощности: 0,98 при нагрузке более 50%.

Выходные характеристики:

- номинальное выходное напряжение: 48 В;
- выходная мощность – 3600 Вт;
- выходной ток на нагрузку – 70 А;
- КПД – 90%.

УЭП может штатно работать при температуре окружающего воздуха от 0 до +40 °С. Основные параметры установки электропитания доступны для мониторинга и контроля как непосредственно на месте, так и удаленно – с помощью входящего в состав установки питания контроллера «Штиль» с русскоязычным интерфейсом.

Группа компаний «Штиль»: (495) 788-8291

Сервер конференц-связи операторского класса

Polycom RMX 4000 – сервер многоточечной конференц-связи, предназначенный для крупных предприятий или операторов связи. Он поддерживает до 80 HD-портов (или до 320 видеопортов с разрешением CIF или 1600 аудиопортов) в одной конференции. Благодаря «горячему» резервированию источников питания система отличается повышенной надежностью.

RMX 4000 имеет модульную архитектуру, поддерживается «горячая» замена модулей. В сервер можно установить до четырех карт MPM+. В нем использованы шасси архитектуры ATCA и высокоскоростная шина. Устройство может быть смонтировано в стандартную телекоммуникационную стойку и занимает 6 юнитов.

Сервер RMX 4000 поставляется вместе с версией программного обеспечения 5.0 для платформы RMX. В числе новых возможностей ПО – поддержка IPv6.

Avicon: (495) 788-3184

Системы экономии энергии и адаптивного управления модулями

реализовала компания Eaton в ИБП моделей 9395 и 9390.

Система экономии энергии (Energy Saver System, ESS) позволяет ИБП работать с КПД, равным 99%, во всем диапазоне нагрузки от 0 до 100%. В режиме энергосбережения система работает на внутреннем статическом байпасе, следя за качеством внешнего питания. При этом все внутренние энергопотребители ИБП переведены в спящий режим. Когда сетевое питание отключается или параметры сети выходят за допустимые пределы, ИБП менее чем за 2 мс переходит в стандартный режим двойного преобразования (от сети или от батарей) и возвращается обратно в ESS, как только заданное качество сети восстановится. Если же ИБП в течение часа детектирует три возмущения внешней сети, то система безусловно переходит в режим двойного преобразования также на 1 час. Если в течение этого часа не обнаруживается каких-либо проблем с питающей сетью, то ИБП вновь возвращается в экономичный режим. Параметры перехода в режим двойного преобразования могут настраиваться в зависимости от требований потребителей и защищаемой нагрузки. В режиме экономии ИБП также способен определять, что является причиной сбоя выходного питания – питающая сеть или нагрузка. При сбое сети происходит немедленное переключение на инвертор, если же сбой связан с нагрузкой, ИБП продолжает работать в режиме экономии.

Технология Eaton адаптивного управления элементами модульных и параллельных систем Variable Module Managenent System (VMMS) помогает повысить эффективность ИБП (или параллельной системы ИБП) при низкой загрузке. Режим VMMS позволяет оценивать степень загрузки ИБП и отключать часть модулей (ИБП 9395) или часть ИБП параллельной системы (ИБП 9390 и 9395), тем самым повышая общую эффективность работы системы. В случае увеличения нагрузки система подключает дополнительные модули (и ИБП) менее чем за 2 мс. Степень избыточности системы в режиме VMMS задается пользователем.

Eaton: (495) 981-3770

Блог, еще раз блог!

Наталия КИЙ

Прямо по Штирлицу. Инфа к размышлению

>>>> Как считают военные, в 2006 г. было принято ошибочное решение о принятии стандарта UMTS (2,1 ГГц) в качестве стандарта 3-го поколения сотовой связи.

Причина – близкое нахождение в частотном спектре космических станций военного назначения, что привело к известным частотным проблемам в московской зоне (радиус 300 км) и на Дальнем Востоке. Наличие подобной системы в США, по мнению начальника войск радиоэлектронной борьбы ВС России Олега Иванова, заставило американцев в свое время принять стандарт CDMA2000. «Перевести «ту» систему в другой диапазон частот невозможно. Аналогичная система в США использует те же частоты, – заявил представитель Вооруженных сил страны. – Два года операторы думали: не снимут ли военные ограничения?». Два с лишним года расхлебывали частотные проблемы 3-го поколения. А на пороге 4-е...

На конверсию нужны серьезные средства и много времени – сходятся все участники рынка. А начальник войск радиоэлектронной борьбы на межведомственном совещании предлагает: «Мы идем в хвосте, мы не разрабатываем стандарты, не пытаемся опередить. Может быть, нужны свои стандарты? И предложить провести конверсию коллегам из других стран?».

Он не скрывает, что это прямо по Штирлицу: последняя фраза запоминается лучше всего.

Поскольку наши стандарты сначала создать, а потом навязать миру вряд ли удастся (посмотрим, что получится с цифровым радио РАВИС), то при таком подходе остается одно – железный занавес.

комментировать

Алексей МИШУШИН

Шпаргалка по авторскому праву

>>>> Иной раз полезно повыдергивать из 600-страничного Гражданского кодекса РФ информацию по определенной теме и свести ее в лаконичную систему. Сделать некую шпаргалку на каждый день, чтобы не разыскивать всякий раз необходимое. Решил я систематизировать перечень условий, обязательных для договоров на создание авторского продукта, например программного обеспечения.

Хотите поручить софтверной компании разработку компьютерной программы? Заказываете создание веб-портала или дорогостоящей ERP-системы? Нет ничего проще. Только не забудьте в договоре с разработчиком оговорить важнейшие для такого рода соглашений условия. Чтобы создали то, что заказываете, а права на продукт вы получили те, что ожидаете.

В силу того что итоговый перечень актуален для договоров не только в отношении любого ПО, но и иных продуктов (литературных, музыкальных, аудиовизуальных, фотографических и др.), я использую аббревиатуру РИД – Результат Интеллектуальной Деятельности. Если же вы заказываете разработку программы, то для простоты мысленно заменяйте это абстрактное понятие сущей конкретикой – софт. Ошибки не будет.

комментировать

Александра КРЫЛОВА

Кому нужен закон «Об электронных деньгах»?

>>>> Год назад появилась надежда, что проблема отсутствия регулирования систем электронных денег решится в рамках разрабатываемого Минфином РФ, Банком России и Минкомсвязи РФ законопроекта «О национальной платежной системе». По крайней мере А.С. Обаева, зам. директора департамента расчетов ЦБ РФ, с трибуны первой международной конференции «Мобильная коммерция-2008», говорила о том, что в этом документе будут даны юридические определения понятий «платеж», «перевод», «система перевода», «платежные системы», а также появится такой новый субъект регулирования, как «небанковский оператор платежной услуги».

Однако представители компаний «Яндекс.Деньги» и WebMoney, а также НАУЭТ признались: несмотря на то что работа над законопроектом близка к завершению, его основные положения для них тайна за семью печатями.

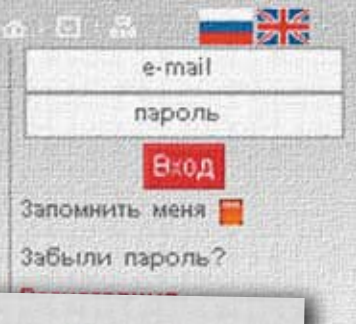
Словом, для того, чтобы обратить на себя внимание государства как на рынок, нуждающийся в регулировании, компаниям, занимающимся интернет- и мобильными платежами, кажется необходимым разработать и принять ФЗ «Об электронных деньгах».

Но если банки и игроки рынка электронных денег и сегодня партнеры, зачем последним нужно отдельное регулирование?

комментировать

IKS-статистика
IKS-рейтинги
Профили
IKS-презентации
IKS-индикатор

Шпаргалка по авторскому праву, инфа к размышлению, где VSAT'ам искать свое счастье, перевод статьи Тима О'Рейли… Признаться, блоги на IKSMEDIA.RU – полезное чтение.



Петр ДИДЕНКО

The War For the Web

>>>> Наткнулся на очень интересную статью «Война за Веб» самого Тима О'Рейли, интернет-ветерана и основателя O'Reilly Media – лучшего издательства компьютерных книг в мире. Он рассуждает о будущем Интернета, как ему и положено по статусу ☺ По-моему, он видит очень интересные тенденции, и его мнение я полностью разделяю. Более того, в своем блоге я, как и многие другие наблюдатели за веб-рынком, отмечаю то же самое: готовится война против веба, грядут новые мерзкие монополии.

Apple iPhone – крутейшее устройство для доступа к вебу, и, как и Facebook, когда речь идет о вебе, работает по правилам, отличающимся от общепринятых на рынке. Кто угодно может сделать веб-сайт или выпустить новое Windows-, MacOS- или Linux-приложение без чьего-либо разрешения. Но что произойдет, когда вы попытаетесь сделать приложение для iPhone? Это требует высочайшего благословения со стороны Apple.

Конечно, есть шикарная лазейка: можно написать веб-приложение, которое пользователь может сохранить как запускаемую программу на своем телефоне. Но такие веб-приложения имеют жесткие ограничения – ключевые возможности телефона недоступны веб-приложениям. Стандарт HTML 5 может предлагать какие угодно новые фичи, похожие на функции обычных программ, но они будут работать только в веб-приложениях и не получат доступа к ключевым функциям телефона – так, как это задумал Apple. И как мы видели ранее в этом году на примере отказа в приеме приложения Google Voice, Apple не стесняется блокировать приложения, которые, как считают специалисты компании, наносят потенциальный вред их бизнесу или бизнесу партнеров Apple.

Прямо сейчас мы наблюдаем очередную войну против принятых правил прозрачности веба – угрозу Р. Мердока удалить данные Wall Street Journal из поискового индекса Google. Притом что большинство людей повторило очевидную истину «сделать это будет равно суициду для журнала», несколько несогласных обозревателей отметили и сильные стороны решения Мердока. Mark Cuban заявляет, что Твиттер сейчас превосходит Google по части поиска информации о происходящих прямо сейчас новостях. Jason Calacanis выступил еще более провокационно, предложив (за несколько недель до заявления Мердока) всем крупным СМИ, которые хотят избавиться от Google, паразитирующего на их эксклюзивной информации, заблокировать индексацию Google и заключить сделку с Microsoft, чтобы их информация находилась только поисковиком Bing.

Конечно, Google этого просто так не оставит и, возможно, предложит газетам собственные условия, что приведет к войнушке, по сравнению с которой даже браузерные войны 90-х покажутся сущей ерундой.

комментировать

Евгения ВОЛЫНКИНА

VSAT-счастье уже на горизонте?

>>>> К 2015 г. согласно планам государства на каждые 100 жителей страны будет приходиться 60 линий широкополосного доступа в Интернет. Причем около 2 млн российских абонентов будут иметь ШПД, использующий спутниковые системы связи. Обеспечить это планируется с помощью открытия нового высокочастотного Ka-диапазона и 3 легких спутников, которые должны быть выведены на орбиту к 2015 г. Зоны их покрытия должны охватить всю территорию России. И в итоге упомянутые 2 млн пользователей получат спутниковый ШПД по (*цитирую*) «достаточно низким ценам». Как сказал Н.С. Мардер, государство планирует взять на себя как минимум четверть затрат на реализацию этого проекта, так как он связан с запуском ракет и выводу спутников на орбиты. Остальное, по всей видимости, должны будут вложить игроки VSAT-рынка.

…Во всяком случае, на уровне деклараций какая-то надежда на относительно недалекое VSAT-счастье появилась.

комментировать

Дмитрий КУТЯВИН

Телевизор и/или компьютер?

>>>> ТВ по-прежнему занимает главное место в гостиной, так как большинство людей выросли за просмотром телевизора и имеют привычку проводить так свободное время. Тем не менее традиционное ТВ в эпоху Интернета, являясь устройством, вещающим в одностороннем порядке, противоречит интерактивным возможностям Сети. Люди, знакомые с цифровыми возможностями, а также новое поколение уже меньше проводят времени перед телевизором, хотя старшее поколение по-прежнему не отрывается от экранов. Ежедневные газеты и журналы резко изменились из-за Интернета, а изменения в ТВ только начинаются. Что в ближайшем будущем заменит телевизор, который является основным источником развлечений? Поколение домашних «коробочек», компьютеров и игровых приставок готовится стать главным источником развлечений. А может быть, сервисы «видео по запросу» и возможности IPTV позволят сохранить популярность телевизора?

комментировать

Реклама в номере

АЙТИ
Тел.: (495) 974-7979
Факс: (495) 974-7980
E-mail: info@it.ru
www.it-scs.ru . . . . . с. 75

ДЖЕНЕРАЛ ДЕЙТАКОММ
Тел.: (812) 325-1085
Факс: (812) 325-1086
E-mail: info@gdc.ru
www.gdc.ru . . . . . с. 21

ИСКРАУРАЛТЕЛ
Тел. (3432) 10-6951
Факс: (3433) 41-5240
E-mail: sales@iskrauraltel.ru
www.iskrauraltel.ru . . . с. 27

ЛАБОРАТОРИЯ КАСПЕРСКОГО
Тел./факс: (495) 797-8700
E-mail: sales@kaspersky.com
www.kaspersky.ru . . . . с. 59

РОСТЕЛЕКОМ
Тел.: (499) 972-8283
Факс: (499) 972-8222
E-mail: info@rt.ru
www.rt.ru . . . . . с. 11

РУСАТ
Тел.: (495) 933-1614
Факс: (495) 933-1625
E-mail: rusat@rusat.com
www.rusat.com . . . . . с. 17

ШТИЛЬ ГК
Тел./факс: (495) 788-8291
E-mail: mosoffice@shtyl.ru
www.inels.ru. . . . . с. 81

ADM PARTNERSHIP
Тел.: (495) 958-5665
Факс: (495) 958-5675
E-mail: business@admpartnership.ru
www.admpartnership.ru с. 82-84

ANCOTEL GMBH
Тел.: +49 69 750013-200
Факс: +49 69 750013-215
E-mail: future@ancotel.de
www.ancotel.com . . . . с. 45

CBOSS
Тел.: (495) 363-4460
Факс: (495) 363-4461
E-mail: email@cboss.ru
www.cboss.ru . . . . . с. 91

DISSOLT
Тел./факс: (495) 783-6822
E-mail: info@dissolt.ru
www.dissolt.ru. . . . . с. 80

EMERSON NETWORK POWER
Тел.: (495) 981-9811
Факс: (495) 981-9810
E-mail: sales@emerson.com
www.emersonnetworkpower.ru . . . . . с. 78

LINKBIT
Тел: (495) 361-2000
E-mail: sales@anytest.su
www.anytest.su . . . . . с. 14

LINXTELECOM
Тел.: (495) 797-9160
Факс: (495) 797-9161
E-mail: info@linxtelecom.com
www.linxtelecom.com . . с. 13

PANASONIC
Тел.: (495) 739-3443
E-mail: office@panasonic.ru
www.panasonic.ru . . . . с. 25

POWER ENGINEERING
Тел./факс: (495) 663-3250
www.e-pwr.ru . . . . . с. 19

QTECH
Тел./факс: (495) 797-3311
www.qtech.ru . . . . . с. 15

RIT
Тел./факс: (495) 684-0319
E-mail: marketing@rit.ru
www.rit.ru . . . . . с. 85

TELLABS
Тел.: (495) 737-5408
Факс: (495) 737-0086
www.tellabs.com . . . . 4 обл.

EATON
Тел.: (495) 981-3770
Факс: (495) 981-3771
E-mail: UPSRussia@eaton.com
www.eaton.ru . . . . . с. 79

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.