# Телеком снижается, но держится

**Акции компаний телеком-сектора во второй половине мая – июне демонстрировали негативную динамику в рамках неблагоприятной рыночной конъюнктуры, однако снижение стоимости бумаг было менее значительным, чем в других отраслях.**

**Анна ЗАЙЦЕВА,**
аналитик
УК «Финам Менеджмент»

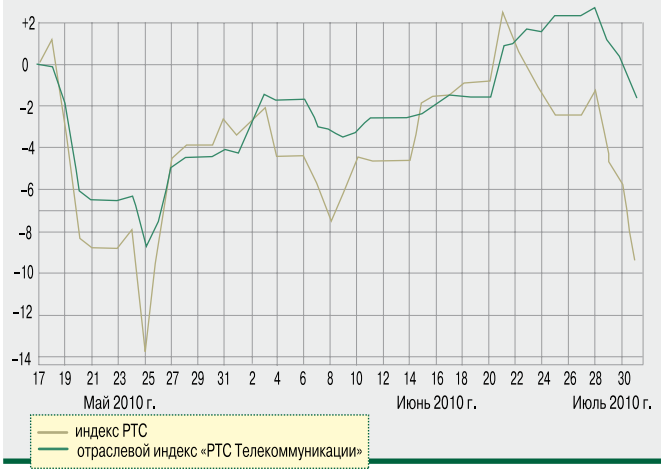
За период с 15 мая по 1 июля индекс ММВБ снизился на 7,2% до 1254,65 пункта, а индекс РТС – на 10,6%, достигнув отметки 1288,72 пункта. Наиболее динамичным для фондового рынка оказался май, когда на российском и мировом рынках господствовали негативные тенденции, обусловленные долговыми проблемами в Греции и других странах еврозоны. На фоне сохраняющихся рисков ухудшения ситуации в мировой экономике не стал позитивным для инвестиционного сегмента и июнь. Так, индекс «ММВБ телекоммуникации» (MICEX TLC) за месяц потерял 2,2%, достигнув отметки 1895,23 пункта, а индекс «РТС Телекоммуникации» (RTStl) подешевел на 2,8% до 197,54 пункта.

Основным событием в секторе стало принятие акционерами «Ростелекома» положительного решения по вопросу реорганизации компании. На годовом собрании акционеры одобрили присоединение к «Ростелекому» семи межрегиональных компаний «Связьинвеста» и «Дагсвязьинформа». Кроме того, за рассматриваемый период в большинстве компаний телеком-сектора были объявлены финансовые результаты по МСФО за 2009 г. и прошли годовые собрания акционеров.

За вторую половину мая – июнь акции «Ростелекома» подешевели на 0,9% до 105,5 руб. Помимо реорганизации, на стоимости акций компании отразился ряд других новостей. В первую очередь, не самая позитивная отчетность по МСФО за 2009 г. Выручка оператора снизилась за год на 2% до 65,5 млрд руб. Операционная рентабельность упала с 10,2% в 2008 г. до 6,5% в 2009 г. Чистую прибыль по итогам 2009 г. компания зафиксировала в размере 3,5 млрд руб., что на 72% ниже показателя годичной давности. Однако чистая прибыль, скорректированная на величину доходов от продажи инвестиционных активов (в 2008 г. «Ростелеком» продал доли в «Голдентелекоме»), уменьшилась всего на 40%. Таким образом, по результатам 2009 г. скорректированная чистая рентабельность составила 5,4% против 8,8% в 2008 г. Что касается выплаты дивидендов за 2009 г., то на выплаты по привилегированным акциям типа А было решено направить 10% чистой прибыли (по 2,1005 руб. на одну акцию), а по обыкновенным акциям – 20% чистой прибыли (по 1,4002 руб. на одну акцию).

Акции «Сибирьтелекома» за полтора месяца подорожали на 5,6%, достигнув отметки 1,784 руб. Поддержку акциям компании оказывала хорошая отчетность. Так, по МСФО за 2009 г. «Сибирьтелеком» по сравнению с 2008 г. увеличил прибыль на 29% – до 1,974 млн руб. А по итогам I квартала 2010 г. прибыль по МСФО увеличилась на 1726 млн руб. и составила 1351 млн руб. Определенное давление на котировки «Сибирьтелекома» оказало решение Арбитражного суда Москвы, который отка-

Динамика индексов РТС и инструментов РТС в период с 17 мая 2010 г. по 1 июля 2010 г.



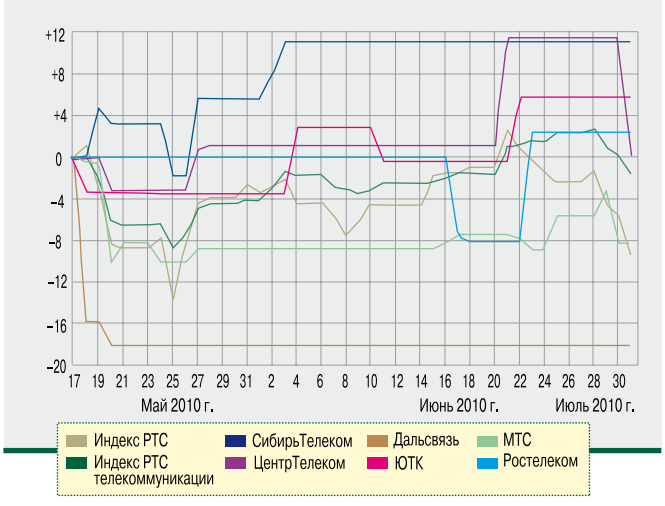
зал оператору в удовлетворении требований о признании незаконным постановления ФАС России о привлечении к административной ответственности и наложении штрафа в размере более 1 млн руб. за нарушение антимонопольного законодательства. На годовом собрании акционеры «Сибирьтелекома» утвердили выплату дивидендов по итогам 2009 г. в размере 0,0589249 руб. на привилегированную и 0,0292878 руб. – на обыкновенную акции. Всего на выплату дивидендов оператор направит 582 090 337 руб.

Капитализация «ЦентрТелекома» повысилась на 7,4% до уровня 21,6 руб. Компания опубликовала позитивную отчетность по МСФО за 2009 г.: чистая прибыль выросла на 39% до 5,868 млрд руб. по сравнению с 2008 г. (4,22 млрд руб.). Выручка увеличилась на 7,2% до 37,3 млрд руб., операционная прибыль – на 15,6% до 10,514 млрд руб., EBITDA – на 26,83% до 16,777 млрд руб., рентабельность по EBITDA – до 44,97% (с 38,02%). Чистый долг компании уменьшился на 30,3% до 16,558 млрд руб. На годовом собрании акционеры «ЦентрТелекома» приняли решение о реорганизации общества в форме присоединения к «Ростелекому», а также утвердили выплату дивидендов за 2009 г.: на одну привилегированную акцию типа А – 0,96 руб., а на одну обыкновенную акцию – 0,48 руб., что практически вдвое выше дивидендов, выплаченных по итогам 2008 г.

Обыкновенные акции «Дальсвязи» подорожали на 1,3% до 88,2 руб. Компания также предъявила хорошую отчетность по МСФО за 2009 г.: чистая прибыль выросла за год на 11,1% и составила 2,518 млрд руб. Выручка увеличилась на 6,8% до 17,197 млрд руб., EBITDA – на 6,6% (до 6,105 млрд руб.). На выплату дивидендов акционеры решили направить 213,5942 млн руб. по привилегированным акциям и 325,7128 млн руб. по обыкновенным акциям.

Акции «Северо-Западного Телекома» прибавили в весе 5,4% до 20,202 руб. Чистая прибыль компании за I квартал 2010 г. в соответствии с МСФО составила 1,452 млрд руб. против убытка в размере 143 млн руб. за аналогичный период прошлого года. Дивиденды на одну привилегированную акцию составят 1,228 руб., на обыкновенную акцию – 0,591 руб.

Динамика индексов РТС и телекоммуникационных компаний в период с 17 мая по 1 июля 2010 г.




Капитализация «Волгателекома» увеличилась на 5,6% до отметки 94 руб. Основная корпоративная новость – сообщение о приобретении «Волгателекомом» 98,19% акций Teleset Networks PCL и планируемый делистинг акций последней на площадке AIM Лондонской фондовой биржи. Дивиденды за 2009 г. будут выплачены в размере 5,1993 руб. на одну привилегированную акцию типа А и 2,5994 руб. на одну обыкновенную акцию.

Стоимость обыкновенных акций «Уралсвязьинформа» выросла на 5%, составив 0,978 руб. Компания подготовила позитивную отчетность по МСФО за I квартал 2010 г., согласно которой выручка от реализации составила 10,6 млрд руб., EBITDA – 5,024 млрд рублей, прибыль от операционной деятельности – 2,853 млрд руб. На годовом собрании акционеры «Уралсвязьинформа» приняли решение направить 75% чистой прибыли на увеличение собственного капитала общества, 10% – на выплату дивидендов по привилегированным акциям и 15% – на выплату дивидендов по обыкновенным акциям. Компания привлекла невозобновляемые кредитные линии ЮниКредитБанка совокупным объемом 3 млрд руб. и возобновляемые кредитные линии от Барклайс Банка и Связь-Банка в размере 1 млрд руб. каждая.

Бумаги МТС подешевели на 7,3% до 227,51 руб. Компания завершила очередной этап работ по запуску в коммерческую эксплуатацию сетей 3G в регионах России. На сегодняшний день сети третьего поколения развернуты более чем в 200 городах во всех субъектах федерации. Среди корпоративных новостей стоит отметить позитивные результаты отчетности по US GAAP за I квартал 2010 г. Чистая прибыль компании составила $381,3 млн, выручка – $2,614 млрд, что на 23,2% больше прошлогоднего результата. Положительный чистый денежный поток компании за первые три месяца 2010 г. достиг $710 млн. Дивиденды за 2009 г. будут выплачены в размере 15,4 руб. на одну обыкновенную акцию (порядка $1,00 на одну АДР). Таким образом, общий размер дивидендов составит 30,70 млрд руб. ($999,3 млрд или 99% чистой прибыли компании за 2009 г. по ОПБУ США или 75% чистой прибыли по ОПБУ США до проведения серии единоразовых списаний).

Цена обыкновенных акций АФК «Система» выросла на 2,8% до уровня 25,3 руб. Финансовая отчетность корпорации по US GAAP за I квартал 2010 г. также позитивная. Более чем вдвое по сравнению с аналогичным периодом 2008 г. увеличились консолидированная выручка (до $6,2 млрд) и операционная прибыль ($956,1 млн). Операционная маржа составила 15,4%. Показатель OIBDA вырос почти в 2 раза и достиг $1,7 млрд, маржа OIBDA – 26,8%. На выплату дивидендов будет направлено 530,75 млн руб., т.е. 0,055 руб. на одну обыкновенную акцию. ИКС

Организатор

Партнер

при поддержке

# КОММУНАЛЬНАЯ СЕТЬ – БУДУЩЕЕ ТЕЛЕКОМА!?

**Сети совместного использования – новая тема российского рынка, пока не приобретшая статус актуального бизнес-направления. Конференции, контракты и сами сети еще впереди. Словцо «шеринг» только начинает мелькать в деловом жаргоне. Пожалуй, первое публичное обсуждение этой темы провел журнал «ИКС» совместно с АРОС на круглом столе «Совместное использование сетей: резервы бизнеса».**

**Первопроходцами в дискуссии вокруг Network Sharing стали:**

**Юрий ДОМБРОВСКИЙ,** президент АРОС
**Шухрат ИБРАГИМОВ,** руководитель департамента стратегии и развития бизнеса РТРС
**Василий ЛЕВЧИК,** руководитель рабочей группы по нормативным правовым вопросам АРОС
**Сергей МИШЕНКОВ,** советник министра связи и массовых коммуникаций РФ
**Александр МЯСОЕДОВ,** директор по продажам Nokia Siemens Networks
**Дмитрий НЕЛЮБОВ,** гендиректор компании «Русские башни»
**Олег НИКОЛАЕНКО,** технический директор компании «МегаФон»
**Сергей ПОРТНОЙ,** директор WiMAX Forum Russia & CIS
**Олег СВИРСКИЙ,** замдиректора бизнес-единицы «МТС Россия» по техническим вопросам
**Сергей СКРИПНИКОВ,** руководитель отдела по работе со СМИ компании «Эрикссон» Восточная Европа и Центральная Азия
Круглый стол вела главный редактор журнала «ИКС» **Наталия КИЙ.**


Н. КИЙ

**Н. КИЙ:** Зрелость рынка сотовой связи, переход конкуренции из области инфраструктуры в сферу брендов, снижение отдачи от инвестиций в инфраструктуру, строительство сетей 3G и перспективы 4G, цифровизация ТВ, экономический спад, стремление поставщиков услуг и акционеров сократить операционные и капитальные затраты – все это предпосылки совместного использования операторами уже действующей сетевой инфраструктуры и «долевого» строительства сетей следующего поколения. Зарубежный опыт Network Sharing (NS) свидетельствует о потенциальном сокращении затрат на 25–50%.

Первые шаги в этом направлении делают игроки российского телекома. Есть примеры совместного использования антенно-мачтовых сооружений (АМС) операторами мобильной связи, они же для размещения своего оборудования арендуют вышки РТРС. Как известно, МТС выступила с предложением о создании в России опытных зон по совместному строительству и использованию сетей операторов. На этот тонкий лед недавно ступила компания с экзотичным названием «Русские башни», которая намерена строить и покупать АМС и сдавать их в аренду операторам радиосвязи.

На начальном этапе речь идет о совместном использовании пассивного оборудования. Но если есть коммунальная башня, то возможна и коммунальная сеть?

Поскольку наш рынок только присматривается к бизнесу на коммунальной сети, разумно поинтересоваться: а как у н и х?

**Ю. ДОМБРОВСКИЙ:** У н и х опыт уже пятилетней давности: в 2006 г. в Швеции две конкурирующие компании – Tele2 и TeliaSonera – ввели в действие совместную сеть UMTS. В Швеции не было аукциона на лицензии 3G, а было условие регулятора: в течение трех лет «покрыть» 98% населения. Два конкурента организо-


Ю. ДОМБРОВСКИЙ

вали совместное предприятие и работают на построенной сообща сети как MVNO – каждая под своим брендом. Экономия капвложений составила около 50%, операционных расходов – примерно 30% ежегодно. Опыт оказался успешным, и в прошлом году Tele2 и Telenor, соединив свои ресурсы в диапазонах LTE и 900 МГц, отдали их компании Net4Mobility и также строят совместную сеть.

Две сотовые компании Китая, China Telecom и China Unicom, скооперировавшись, строят 500 базовых станций 3G в Шанхае, рассчитывают на экономию в $43,9 млн и выполняют жесткое требование регулятора, действующее и в других азиатских странах, о совместном использовании башен и другой пассивной инфраструктуры в сетях 3G.

В Европе максимальное число совместных сетей в Великобритании (четыре), есть такие сети в Италии и Норвегии. Это краткие примеры из зарубежного опыта. Давайте думать, что может произойти в России.

**«ИКС»: В каких единицах (деньги, время, трудозатраты) могут быть измерены резервы Network Sharing? Есть ли опыт в России?**


О. СВИРСКИЙ

**О. СВИРСКИЙ:** Да, опыт есть. С 2005 г. (!) мы начали активно обмениваться башнями с коллегами из «Билайна» и «МегаФона». На 2010 г. у нас свыше 1200 точек совместного стояния. Совместного строительства башен компании не ведут, так как есть определенные сложности с договорами, учетом затрат и т.д. Принцип очень простой: построил один, построил другой. Смотрят, у кого что есть, и договариваются: я тебя пускаю туда, а ты меня пусти сюда. При необходимости производится усиление металлоконструкций. Последние два года при планировании сети предусматриваем будущие обмены местами на башнях с тем, чтобы уже в проекты закладывать повышенную несущую способность металлоконструкций и не тратить время на доработку проектной документации и пр. Строительство 70-метровой башни обходится в несколько миллионов рублей, поэтому разделить эту сумму на двоих или на троих – очень существенная экономия.

Сегодня «большая тройка» начала второй виток соревнования за покрытие территории России – в сети 3G. Но затраты на строительство сети UMTS в диапазоне 2,1 ГГц не сравнимы с затратами на GSM 900 МГц: при ковровом покрытии соотношение 7:1 или 8:1. Вот здесь вырастает потребность в совместном строительстве инфраструктуры 3G и новых предложениях. Рынок к этому готов.

**О. НИКОЛАЕНКО:** Экономия будет – как в деньгах, расходуемых на строительство и эксплуатацию сетей, так и во времени и трудозатратах на развертывание сетей. Оценочно: до 70% CAPEX (при совместном строительстве тремя операторами) и до 50% OPEX.

**Д. НЕЛЮБОВ:** Во времена строительства сетей 2G операторы не считали CAPEX и только на уровне покрытия сельских районов, когда окупаемость стала ниже, начали договариваться о совместном использовании инфраструктуры. Независимая компания «Русские башни», которая финансируется ЕБРР и не принадлежит ни одному из операторов, представляет в России программу совместного использования пассивной инфраструктуры сетей, строит и намерена сдавать в аренду «большой тройке» и другим операторам сетей радиосвязи антенно-мачтовые сооружения, таким образом участвуя в развитии сетей нового поколения.


Д. НЕЛЮБОВ

Мы подтверждаем цифру в 40% экономии капзатрат на башни и сопутствующую инфраструктуру для каждого из операторов сотовой связи.

**С. МИШЕНКОВ:** Несколько лет назад альтернативные операторы решили опутать Московскую область ВОЛС: тебе три нитки, тебе четыре, тебе шесть. Для повышения надежности все волокна надо завести в общие аппаратные, ставить общее станционное оборудование, а потом раздавать – так дешевле. Насколько я знаю, из этой затеи толком ничего не получилось, потому что каждый оператор хотел иметь собственные каналы и аппаратную, которую резервировал. Почему – для меня загадка: это же живые деньги, которые вы тратите! Если вы ставите три аппаратные, их надо обслуживать: вот у вас уже появились три смены и тройные расходы...


С. МИШЕНКОВ

**О. СВИРСКИЙ:** Поддерживаю вас: затраты на эксплуатацию зачастую можно снижать еще более эффективно, чем на развитие. Ситуация: весной в паводок смыло аншлаги (индикаторы прохождения трассы по колхозному полю). Тракторист, не зная о трассе, «пропахал» кабель, по которому проходят волокна трех-четырех операторов. Четыре оператора имеют четыре договора с четырьмя организациями, осуществляющими его техническое обслуживание, и четыре аварийные бригады мчатся к месту обрыва и начинают работать локтями: кто первый заварит волокна своего

заказчика. Здравый смысл подсказывает – инфраструктурный элемент, как сама волоконная линия, так и линейно-кабельное сооружение, должны обслуживаться одной организацией. Общий подрядчик на обслуживание ВОЛС дает экономию от 2 до 4 раз!

**«ИКС»: Какие элементы инфраструктуры сети (пассивные, активные) предназначены для совместного использования? С чего начинать – с фрагментов или со стратегии NS?**


О. НИКОЛАЕНКО

**О. НИКОЛАЕНКО:** Возможно совместное использование как пассивных, так и активных фрагментов: АМС, канализации, оборудования радиосети, ВОЛС (оптических волокон, «лямбды» DWDM), РРЛ (емкости линии). Проще всего начинать, конечно, с пассивных элементов. В настоящее время можно говорить только о фрагментарном совместном использовании сетей. Стратегии Active Network Sharing (ANS) еще нет, она будет прорабатываться в ближайшее время на основе тестового совместного использования радиосети 3G и экономической оценки таких проектов. Далее разработанную стратегию уже можно будет применять при строительстве сетей LTE.

**Д. НЕЛЮБОВ:** Начинать надо с пассивного оборудования: вышек, контейнеров под вышкой, кондиционеров, ИБП, трансформаторов, охраны. Совместное использование активного оборудования – вопрос будущего.

**«ИКС»: В каких формах возможно сотрудничество операторов? Это прямое совместное использование, о котором рассказал представитель МТС? Это СП, подобное Indus Towers, которое учредил в Индии оператор Bharti Airtel совместно со своими конкурентами – Vodafone-Essar и Idea Cellular? Или это создание самостоятельной компании – путь, по которому пошли «Русские башни»?**

**О. СВИРСКИЙ:** С точки зрения рынка должны работать все варианты. Мы исходим из конкретных экономических расчетов.

**Д. НЕЛЮБОВ:** На мой взгляд, у первых двух форм есть недостатки. Допустим, оператор построил башни и предлагает их для совместного использования другому оператору. Кто их будет обслуживать? Тот, кто построил? В результате, я думаю, наши операторы придут к пониманию, что для получения максимальной экономии капитальных и операционных расходов строить пассивную инфраструктуру должны специализированные компании. Мировой опыт говорит о том, что у совместных предприятий, наделенных активами нескольких игроков рынка, тоже есть слабое место. Это проблемы управления, выражающиеся как в разногласиях при установлении цен на аренду и обслуживание, так и при выборе направления развития, строительстве новых объектов. Для российского рынка предпочтительнее независимая компания, которая строит и покупает инфраструктуру в виде башен для самых разных компаний там, где им это требуется.

**Ш. ИБРАГИМОВ:** На текущий момент выбор модели работы ситуационный: решаем на местах. Поэтому на уровне пассивной инфраструктуры превалирует просто аренда. Оборот РТРС по данной услуге на 2010 г. я прогнозирую на уровне $30 млн. 75% в нем занимают сотовики, первая тройка. Большую часть оборудования у нас арендуют в труднодоступных регионах. Инфраструктура у нас имеется, в 2010 г. в соответствии с федеральной программой цифровизации ТРВ будет построена еще почти тысяча объектов, характеристики большей части из них мы согласуем с сотовыми операторами еще на уровне системного проекта. Мы следим за движением рынка и потребностями сотовых операторов.


Ш. ИБРАГИМОВ

**Ю. ДОМБРОВСКИЙ:** Совместное строительство, обмен местами на башнях – это хорошо, это экономия средств. Но это не рынок. Рыночный способ – это специализация: в разных странах, прежде всего в США, есть компании типа «Русских башен», которые обеспечивают экономию средств, ресурсов и времени. Смотрите: несмотря на издержки, нам удалось сделать дешевую мобильную связь – отчасти благодаря тому, что базовые станции «бьют» на 30 км. А вот дешевый мобильный Интернет, который сможет позволить себе наше бедное население, не сделать без кооперации и специализированных компаний.

**«ИКС»: Действующая нормативная правовая база нацелена на стимулирование конкуренции операторов. Возникает новая ситуация – ситуация сотрудничества. Известен приказ Минкомсвязи от 8.08.2005 № 97, который трактуют как запрещающий Network Sharing. Как можно охарактеризовать правовое поле для сетей совместного использования?**

**В. ЛЕВЧИК:** Совместное использование сооружений связи не запрещено – это вопрос договоренности операторов. Не запрещено и совместное использование средств связи, но для телефонных сетей 97-й приказ требует при


В. ЛЕВЧИК

этом физического, технического или программного разделения их узлов. Однако до сих пор не определено, что понимается под таким разделением, поэтому сертификационные испытания на это не проводятся.

Теоретически у регулятора может быть возражение против совместного использования средств связи: возникновение одного общего набора средств связи вместо двух разных не способствует повышению устойчивости функционирования ССОП и доступности услуг связи. Но с антимонопольной точки зрения совместное использование облегчает появление и закрепление на рынке новых игроков.

**О. НИКОЛАЕНКО:** В настоящее время документы, регламентирующие данный вопрос, отсутствуют. Единственное, что можно отнести к этой сфере, приказ Минкомсвязи от 29.12.08 № 116 «Требования к оказанию услуг подвижной радиотелефонной связи при использовании бизнес-модели виртуальных сетей СПР». Но и он носит очень общий характер, детали не проработаны. Поэтому текущая ситуация на правовом поле, как антимонопольное законодательство, так и нормы Минкомсвязи, не способствует бурному развитию ANS.

**О. СВИРСКИЙ.** С точки зрения обмена пассивной инфраструктурой существенных ограничений в нормативной базе не замечено. Как правило, все ограничения вытекают из особенностей заключения договоров и физических возможностей самой инфраструктуры. Сложнее обстоит дело с совместным использованием активного оборудования. Возможность провозглашена, но в очень интересной формулировке: при желании двух операторов использовать одно и то же оборудование оно должно быть сертифицировано как программно-аппаратный комплекс, позволяющий разделить сети связи, программно или аппаратно. По сути, это вопрос сертификации. Но вендорам невыгодно производить оборудование для совместного использования. Представьте: так бы вы купили каждый по коммутатору, а тут один на троих! Но и здесь ситуация меняется – новые технологии уменьшают долю оборудования в стоимости решений, цены снижаются и производители ищут новые источники доходов уже не в продажах «железа», а в предоставлении услуг, в том числе на базе совместного использования операторами их оборудования.

**?→ «ИКС»: ? Мы подошли к больному вопросу Network Sharing – интересам поставщика оборудования. На первый взгляд, он в проигрыше: сокращается объем инфраструктуры сети, необходимого операторам оборудования. Вендор страдает. Это так?**


А. МЯСОЕДОВ

**А. МЯСОЕДОВ:** С одной стороны, для вендора консолидация операторов и уменьшение заказов на строительство сетей – некий минус. С другой, на рынке сформировался новый взгляд на эксплуатацию сетей. И здесь мы видим себя в хорошей позиции: мы могли бы объединять операторов по территориальному признаку, по признаку оборудования, заниматься укрупнением работ по эксплуатации и эксплуатацией сетей сразу нескольких операторов. Для нас это интересно.

Давайте смотреть шире. Совместное использование даже пассивной инфраструктуры высвобождает CAPEX оператора, и эти деньги могут быть направлены на развитие сети и приобретение нового оборудования, которого операторам 3G требуется немало. На развитие могут быть направлены и дополнительные средства, появляющиеся у операторов в процессе совместного использования тех же башен.


С. ПОРТНОЙ

**С. ПОРТНОЙ.** Проблемы нет вообще – вендору по любому выгодно. При пассивном шеринге оператор просто не несет несвойственных ему затрат, в результате больше денег может потратить на свойственные ему затраты, т.е. на базовые станции – он их купит больше. При ANS сложнее, но тоже проигрыша нет. Практика эксплуатации сетей передачи данных показывает, что в отличие от телефонных они заполняются мгновенно, как только тарифы становятся приемлемыми. Если сеть заполнена полностью, ее надо расширять, что и происходит сейчас с WiMAX-сетью Yota (они вынуждены ставить новые базовые станции уже просто для того, чтобы давать большую емкость).


С. СКРИПНИКОВ

**С. СКРИПНИКОВ:** Неправильно воспринимать сегодня вендора исключительно как поставщика «черных ящиков». Мы в Ericsson активно диверсифицируем свой бизнес, и сейчас одним из стратегических направлений для нас стала разработка мультимедиарешений. Операторы, кстати, тоже смещают акцент на сервисную составляющую своего бизнеса. Так что если оператор имеет возможность сэкономить на строительстве сети, у него появляется больше ресурсов для развития новых услуг. Все сегодня понимают, что в сетях 3G и 4G само «протягивание трубы» по сути уже не является бизнес-кейсом: операторы сначала определяют, какие услуги они будут оказывать, и только потом – на какой «трубе». Ну и наконец, успех оператора – это и наш выигрыш тоже как долгосрочного партнера.

Подготовила **Наталия КИЙ**

# Камо грядеши, закон?

**В конце 2009 г., перед самым окончанием срока, отпущенного на приведение автоматизированных систем обработки персональных данных в соответствие с установленными требованиями, резко активизировалась деятельность по изменению законодательства и подзаконных актов, определяющих порядок работы с этой категорией чувствительных сведений. Произошло это не случайно, для изменений были веские основания и глубинные причины. Похоже, это только начало процесса.**

**Михаил ЕМЕЛЬЯННИКОВ,**
директор по развитию бизнеса НИП «Информзащита»

## Что произошло?

Трудно не согласиться с резюмирующей частью пояснительной записки к законопроекту, внесенному в Госдуму В.М. Резником и призванному кардинально изменить регулирование обработки персональных данных: «Практика реализации Федерального закона позволяет сделать вывод о недостижении цели его принятия и создает предпосылки для уточнения его отдельных положений».

Действительно, нелегальных (т.е. созданных вопреки закону) баз данных, содержащих сведения о гражданах, на рынке меньше не стало, скорее наоборот. К ответственности за создание и распространение таких баз никто не привлечен. Ну, прекращена деятельность нескольких интернет-сайтов, наиболее одиозных и нарушавших закон в самой грубой форме. Ощутить на себе бóльшую защищенность прав и законных интересов вследствие применения ФЗ-152 «О персональных данных» российскому гражданину довольно трудно. Зато законопослушные предприятия и организации, которые попытались выполнить требования, установленные регуляторами, в полной мере прочувствовали последствия такого решения. И весьма немалые затраты на создание подсистемы безопасности – отнюдь не единственный побочный эффект реализации требований. Среди прочих и регистрация в качестве оператора персональных данных, фактически являющаяся завуалированным приглашением органам контроля и надзора в рамках плановых проверок ознакомиться с состоянием дел по защите сведений у «легализовавшейся» организации (для справки: уведомление об обработке направили в Роскомнадзор около 100 тыс. операторов, что, по разным оценкам, составляет 1,5–3% общего их количества). И раскрытие сведений о себе как операторе в объеме, превышающем установленный законом (а иначе уведомление к регистрации принято не будет, зайдите на сайт Роскомнадзора и убедитесь в этом сами). И существенное усложнение работы с данными о гражданах в рамках бизнес-процессов организации вследствие ограничений, накладываемых законами и подзаконными нормативными правовыми актами, что отрицательно сказывается на этих процессах и уменьшает доступность информации. И, наконец, значительное усложнение топологии информационной системы и увеличение нагрузки на нее из-за необходимости использования большого количества различных средств защиты информации, функционирование которых требует дополнительных вычислительных ресурсов, средств хранения и повышения пропускной способности сети. В качестве бонуса за эти потери и неудобства – только снижение государственных рисков, в результате которых возможны (но не обязательны!) некоторые, не очень серьезные санкции. Не слишком много...

Подобная ситуация не могла не вызвать противодействия. Усилилось давление на законодателей и регуляторов со стороны бизнеса и его лоббистских структур – различного рода объединений, ассоциаций, союзов. Первым проявлением этих усилий стало утверждение Правительством РФ абсолютно невнятного «Положения об особенностях обработки персональных данных без использования средств автоматизации» (от 15.09.2008 № 687). Приведу для примера только два пассажа из этого постановления, изложенные в первых двух его пунктах:

«1. Обработка персональных данных, содержащихся в информационной системе персональных данных ... считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использова-

ние, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее».

Понять, что имели в виду авторы, решительно невозможно. Руководствуясь этими положениями, любую обработку в информационной системе можно счесть обработкой без использования средств автоматизации. Данные практически всегда вводятся в систему человеком и используются им же, да и классическое определение автоматизированной системы предполагает, что человек является обязательным ее элементом.

Когда большому бизнесу стало ясно, к каким затратам приведет реализация технических требований, которые определены другим постановлением Правительства – от 17.11.2007 № 781, утвердившим «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», в рекордные для наших законодателей сроки в ФЗ-152 были внесены изменения, отодвинувшие на один год дату окончания работ по приведению информационных систем в соответствие закону. Внесению изменений предшествовали парламентские слушания 20 октября 2009 г., на которых много говорилось о необходимости корректировки законодательства. И дополнительный год предполагалось потратить именно на то, чтобы устранить пробелы и противоречия законодательства, привести в соответствие друг другу ФЗ-152 и другие законы, нормы которых не стыкуются между собой.

Собственно, на решение части этих проблем и нацелен законопроект В.М. Резника, о котором говорилось в начале статьи и который был принят 5 мая сего года в первом чтении. Но всех проблем и противоречий он не решает.

## Проблемы законодательные

Обо всех проблемах, порожденных законом, в одной статье рассказать невозможно. Остановимся только на некоторых из них, системных, наличие которых ставит практически перед каждым оператором неразрешимую дилемму – нарушить закон, но сохранить бизнес, или отказаться от бизнеса только потому, что выполнить законодательные требования невозможно.

**Согласие субъекта на обработку.** За исключением исчерпывающего перечня случаев, закон предусматривает выражение субъектом согласия на обработку его персональных данных, причем на оператора возлагается обязанность доказать наличие этого согласия. Такая постановка вопроса делает невозможным применение интернет-технологий в бизнес-процессах, предусматривающих обработку персональных данных. Интернет анонимен, и единых идентификаторов, удостоверяющих конкретную личность, для Интернета не существует. Это значит, что проверить авторство лица, заполнившего онлайн-анкету или веб-форму, невозможно. А, значит, невозможно доказать наличие согласия того субъекта, чьи данные указаны в этой самой веб-форме. Даже при оплате в Интернете покупок и услуг кредитной картой согласие недоказуемо, поскольку совершить онлайн-сделку может любое лицо, в чьи руки попала платежная карта.

Но проблема не только в Интернете. Любая продажа товаров или услуг через агентов ставит перед продавцом, в чьих интересах действовал агент, нелегкую задачу подтверждения согласия субъекта на обработку данных именно продавцом. А если персональные данные для предоставления услуги нужны, но договор, в котором можно было отразить согласие, отсутствует вообще? Например, при покупке авиа- или железнодорожных билетов? Как быть тогда? Ответа в нынешнем законе нет.

**Получение персональных данных от третьих лиц.** Закон определяет практически невыполнимую процедуру действий оператора в тех случаях, когда он получает персональные данные не от самого субъекта, а от третьих лиц. В этом случае оператор *до начала обработки* таких персональных данных обязан предоставить субъекту персональных данных информацию, содержащую наименование и адрес оператора, цель обработки персональных данных и ее правовое основание, сведения о предполагаемых пользователях персональных данных, и разъяснить субъекту, чьи данные были получены, его права, установленные Федеральным законом.

Начнем с того, что в терминах закона сбор персональных данных – уже их обработка. И как можно сообщить субъекту о чем-то, еще не получив его данных, сказать сложно. Но это казус. Проблема в другом. Представьте себе покупку билетов или бронирование гостиницы одним человеком на большую компанию друзей или родственников. Передают необходимые для этого персональные данные не сами субъекты, а лица, представляющие их интересы, причем выполнение описанных действий нотариального подтверждения прав не требует. Таким образом, действуя строго по закону, оператор должен каким-то образом разыскать граждан, на чье имя куплены билеты или забронирован номер, и сообщить им информацию, указанную выше. Причем убедиться и иметь доказательство того, что она сообщена тем, кому нужно, и они подтвердили согласие на обработку.

Никак не вписываются в эту схему действий современные системы денежных переводов, предполагающие передачу сведений об отправителе и получателе не конкретному банку, а широкой сети партнеров, расположенных иногда даже в других странах. Каждый из участников системы, строго говоря, до начала обработки должен найти отправителя и получателя и довести до них необходимые сведения. Делать это не только очень сложно, но просто бессмысленно.

Головоломку предлагает закон и для страхового бизнеса, где очень часто страхователь при заключении договора сообщает страховщику персональные данные застрахованных лиц, выгодоприобретателей, водителей, включаемых в полис ОСАГО и т.п. Все эти данные в целях реализации договора и его перестрахования

страховщик должен сообщить третьим лицам – лечебным учреждениям, включенным в программу добровольного медицинского страхования, автосервисам, выполняющим ремонт по договорам КАСКО и т.д. И при каждом действии – проблема уведомления субъектов о начале обработки их данных все новыми и новыми операторами и получения на это согласия.

**Трансграничная передача персональных данных.** Требования о трансграничной передаче данных только в страны, принимающие адекватные меры защиты, или включении согласия на такую передачу в договор с субъектом дают основания усомниться, что люди, писавшие закон, знакомы с реалиями современного мира. Покупая авиабилет Москва–Чита, пассажир бронирует его не в АС перевозчика, а в международной системе Amadeus или Sabre, о чем пассажир чаще всего даже не имеет представления. А сам перевозчик, как правило, не знает, где конкретно владельцы систем хостят свои сервера и в какую конкретно страну осуществляется трансграничная передача. Примерно аналогичная ситуация с бронированием номеров в сетевых гостиницах, всяких там «Иннах» и «Хилтонах», с открытием банковских счетов в российских банках и заключением договоров страхования с компаниями, владельцы которых находятся за рубежом. Где находятся их автоматизированные банковские системы и база страховых договоров – тайна великая, во всяком случае для российского персонала.

**Прекращение обработки и уничтожение персональных данных.** Еще одна замечательная норма закона: «В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных».

Опустимся с небес законотворчества на нашу грешную землю и посмотрим, что это означает на практике. Закон ставит крест на ведении истории взаимоотношений с клиентом, которая во многих видах бизнеса фактически является его обязательной частью. Закрыл клиент депозитный счет в банке или закончилось действие договора кредитования – все данные надо немедленно уничтожить. Но принцип «Знай своего клиента» – один из основополагающих в банковском деле. Во всем мире от того, как ведет себя клиент в ходе своих взаимоотношений с банком, зависят условия его обслуживания и спектр предлагаемых ему услуг.

Крупные операторы связи имеют миллионы клиентов, значит, ежедневно заканчивается срок действия тысяч, десятков тысяч договоров на предоставление услуг связи. В биллинговой системе ежедневно надо найти соответствующих клиентов и уничтожить сведения о них – договор закончился, цель обработки достигнута. А что делать со сроком исковой давности взаимных претензий оператора и клиента? А как выполнить требования Постановления Правительства от 27.08.2005 № 538, требующего от операторов связи все сведения об абонентах и оказанных им услугах связи хранить в базах данных в течение трех лет? Причем требование это установлено не Федеральным законом «Об оперативно-розыскной деятельности», а постановлением Правительства и явно противоречит п. 4 ст. 21 ФЗ-152.

Я не говорю уже о технической стороне выполнения требования об уничтожении данных в биллинговой системе в трехдневный срок.

**Общедоступные персональные данные.** Закон устанавливает, что общедоступные персональные данные – это персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. При этом включение персональных данных в общедоступные источники допускается только с письменного согласия субъекта, и в любой момент по его требованию данные из таких источников должны быть исключены. Это теория закона.

А вот практика. Работодатель в целях выполнения работниками своих обязанностей предоставил им электронную почту. Корреспонденты работников предприятия по собственной воле сообщают в письмах свои персональные данные, абсолютно любые, по их усмотрению. Они могут содержать и специальные категории данных – сведения о здоровье, членстве в партии, религиозных убеждениях и т.п. Владелец почтовой системы эти данные не запрашивал, цели их обработки не определял, получены они по незащищенным каналам связи. И что, владелец почтового сервера становится помимо своей воли оператором, потенциальным правонарушителем и должен такую систему классифицировать и защитить по полной программе? А ему это надо?

Все мы в рамках деловых отношений обмениваемся визитными карточками, на которых указаны персональные данные. Рассчитывать на соблюдение конфиденциальности в отношении этих сведений лицом, получившим визитку, не приходится. А если данные из визиток переносятся на компьютер и обрабатываются не в личных, а в служебных целях? На вопросы, кто в этом случае оператор, какие меры защиты надо принимать и можно ли считать сведения из визитных карточек общедоступными, ответы в существующем законе найти невозможно.

Описание подобных коллизий можно продолжать достаточно долго. Беда в том, что в этих условиях почти каждый оператор, даже если он себя таковым и не считает, является потенциальным нарушителем закона. Правда, о серьезных санкциях пока не слышно. Это создает вторую проблему. В подобной ситуации велик соблазн избирательного применения санкций к операторам, выбираемым органами контроля, надзора, правоохранения, прокуратуры и судами по известным только им критериям. А это прямой путь к коррупции.

*О технических и государственных проблемах, связанных с законодательством о персональных данных, читайте в следующем номере «ИКС».*

# Эффективность системы хранения данных: требуется анализ

**Объемы данных, которые современным компаниям приходится обрабатывать и хранить, растут со скоростью 50–70% в год. Современные СХД активно увеличивают свою емкость и функциональные возможности, стоимость хранения 1 Мбайт информации с каждым годом снижается, но затраты на хранение информации все равно повышаются. В чем причина?**

**Игорь КАСЬЯНОВ,**
главный специалист отдела вычислительных систем Корпорации ЮНИ

На рынок постоянно выводятся новые аппаратные и программные средства записи и сжатия данных, резервного копирования и т.д. Однако корпоративные данные обычно очень разнородны, требуют различных методов обработки, условий хранения, защиты, скорости доступа и т.д. Поэтому типовых схем построения корпоративных систем хранения данных (СХД) по большому счету не существует, и создание любой СХД – это индивидуальный проект, учитывающий самые разные технические и экономические требования заказчика, объективные и субъективные факторы, присутствующие в организации.

Многие согласятся, что основным критерием эффективности СХД должна быть минимизация стоимости хранения данных, определяемая TCO (total cost of ownership). Но есть и некоторые нюансы: как показывает практика, современные российские заказчики крайне неохотно соглашаются потратить значительные средства (скажем, миллион и более долларов) даже на самую современную систему хранения, обещающую грандиозную экономию в будущем. Чаще всего они предпочитают уменьшить совокупную стоимость владения СХД хотя бы на 30% в ближайшей перспективе при минимальных капитальных затратах сегодня.

Далеко не всегда ключевым фактором при выборе аппаратных средств, ПО и методов построения корпоративных систем хранения является емкость СХД, так как зачастую на первый план выходят высокая надежность хранения, сверхскоростной доступ к данным, поддержка одновременной работы большого количества пользователей и т.п. Простое же увеличение объема СХД путем добавления быстродействующих и емких дисков может привести лишь к неоправданному увеличению затрат на хранение данных.

## Сколько компаний, столько и СХД

Изучение структуры спроса на СХД показывает, что их пользователей следует классифицировать не столько по размерам организаций и, следовательно, по объему хранимых данных, сколько по специфике их деятельности. Так, небольшая организация с двумя десятками пользователей может обладать объемным хранилищем фото- или видеоматериалов, не требующих скоростного доступа в режиме реального времени. А на другом предприятии тысячам пользователей необходимо обеспечить одновременный высокоскоростной доступ к небольшой по объему базе данных, состоящей из множества коротких записей.

Еще одно требование – унификация хранения данных. Например, банк желает хранить в своем централизованном и унифицированном хранилище данных финансовые данные операционного дня, видеопотоки с камер видеонаблюдения и пр. То есть большой объем видеоданных, к которым обращаются крайне редко, должен сочетаться с относительно небольшим объемом данных, пользующихся постоянным спросом и требующих высокоскоростного доступа. Таким образом, в одной СХД нужно реализовать очень разные требования.

Очевидно, что как при создании новой СХД, так и при модернизации или наращивании старой необходимы три вещи: анализ, анализ и еще раз анализ тех самых объективных и субъективных факторов и требований заказчика. Нужно детально изучить состояние системы хранения, характер ее использования, требования к новой СХД, экономические последствия их выполнения и т.д. и на основе результатов этого анализа правильно организовать хранение данных. Также нельзя упускать из виду, что основная цель всех преобразований состоит в оптимизации хранения данных.

Кроме того, со временем практически у всех компаний требования к системам хранения меняются. Кроме банального увеличения объема хранения, растет или уменьшается количество пользователей, появляется необходимость в хранении данных других типов, в ускорении доступа к данным и т.п. В ответ на это ведущие производители оборудования уже давно предлагают различные решения, например возможность замены контроллера и ПО для СХД или проведение модернизации операционной системы и микрокода в СХД высшего корпоративного класса, что позволяет подключать к старой системе новые модули расширения с поддержкой других протоколов и смешивать диски разного типа (SAS, SATA, Fibre Channel). Таким способом можно развивать систему хранения в течение многих лет, конечно, при условии, что пользователь четко знает, каким должно быть направление этого развития. Но для подобной оптимизации СХД опять же необходимо тщательно проанализировать ситуацию и поставленные задачи, чтобы определиться, какой в ре-

зультате должна стать СХД. Поэтому создание или модернизацию СХД разумно осуществлять с привлечением квалифицированных специалистов.

## Вездесущая виртуализация

Технологии виртуализации систем хранения данных многогранны. Их применение не всегда однозначно и не всегда может быть правильно определено. Однако существуют рекомендуемые области использования виртуализации СХД.

Например, технология виртуализации хорошо работает в деле объединения двух несовместимых СХД. Сегодня практически все производители СХД выпускают так называемые контроллеры виртуализации. В виртуализованной СХД пользователь «видит» принадлежащие ему однотипные тома и диски с указанием их функциональных характеристик (скорость доступа, объем и т.д.) без привязки к их физическому расположению на реальных дисках и томах СХД. В таких системах реализована поддержка даже очень старых устройств хранения с SCSI-интерфейсом. Эти системы при необходимости позволяют прозрачно для пользователя переносить данные из архивов на дешевых носителях на быстродействующие накопители для оперативной работы с ними, а потом отправлять их обратно без прерывания в обслуживании.

Виртуализация позволяет провести консолидацию всего многообразия корпоративных данных без деления их по принадлежности к тому или иному производственному подразделению. Благодаря виртуализации все данные имеют понятное централизованное представление, позволяющее легко управлять ими, несмотря на то что физически они могут находиться в разных отделах, зданиях, городах и даже странах. При этом централизованное хранение данных далеко не всегда оправданно: данные должны находиться как можно ближе к их потребителю, чтобы не загружать сеть передачей больших объемов информации, что связано с дополнительными расходами. Когда идет речь о консолидации данных, TCO старых СХД с контроллерами виртуализации часто оказывается ниже, чем у новых. Тем более что новые системы хранения всегда можно добавить к существующим без ущерба для прозрачности корпоративных данных.

## Иерархическое управление носителями

Еще одним важным способом снижения совокупной стоимости владения СХД, капитальных и операционных затрат является использование давно известной технологии многоуровневого хранения. В подавляющем большинстве ситуаций одноуровневая СХД, т.е. использующая один тип носителей (только диски, только ленты и т.п.), как бы ее ни оптимизировали, будет обходиться пользователю дороже многоуровневой.

Оптимизация многоуровневой системы представляет собой гораздо более благодарное занятие, тем более если речь идет об СХД крупной компании или большого инфраструктурного ЦОДа. Данные, постоянно нужные для работы, могут храниться даже на очень дорогих SSD-дисках, а прочие данные, потребность в которых возникает раз в два-три месяца, должны отправляться в ленточный архив; для промежуточной ситуации подойдут традиционные жесткие диски (в последнее время, как правило, дешевой архитектуры SATA), и это будет вполне оправданно с экономической точки зрения. Во времена старых больших компьютеров такой принцип называли иерархическим управлением носителями (Hierarchical Storage Management).

## Как же спроектировать корпоративную систему хранения данных?

Едва ли не самой важной стадией создания корпоративной системы хранения является ее проектирование и разработка. При проектировании корпоративных систем хранения данных требуется тщательный анализ имеющейся системы хранения и параметров будущей СХД:

- какие базы данных используются;
- какие данные в них хранятся;
- какие архивы нужны;
- для каких данных нужны резервные копии и сколько их должно быть;
- как часто надо обновлять данные;
- сколько у них пользователей;
- сколько пользователей будут работать с данными одновременно;
- как часто пользователи обращаются к тем или иным данным;
- какая скорость доступа им нужна и т.д.

Только проанализировав всю эту информацию, можно определить организационную структуру хранилища, необходимую дисковую емкость (в том числе SSD-дисков), объем ленточной библиотеки, размер промежуточного дискового кэша (если есть ограничения на время перекачки данных на ленту) и т.п. Некоторые производители оборудования предлагают специальные средства для помощи в проектировании СХД, которые автоматически обрабатывают данные, собранные посредством стандартных опросных листов, и на выходе дают рекомендации по организации хранения, а также экономические показатели эффекта от внедрения корпоративного хранилища. Однако работа с ними требует определенного опыта и подготовки.

■ ■ ■

Проблемы, стоящие на пути к эффективной СХД, могут оказаться очень сложными. Скажем, имеющиеся данные нужно перенести на новые носители или перераспределить между старыми и новыми носителями. Хорошо, если эти данные уже не меняются и не используются или используются очень редко. А если это данные, к которым пользователи обращаются 24 часа в сутки, 7 дней в неделю? А если старая и новая СХД выпущены разными производителями и в них используются разные внутренние протоколы обработки данных? Например, функции дупликации и репликации лент не работают между системами разных производителей и не всегда поддерживаются даже между системами разных поколений одного и того же производителя...

Решение всех этих проблем в каждом конкретном случае существует, но для его поиска требуется анализ, анализ и еще раз анализ, и лучше доверить его профессионалам. ИКС

# «Интернет ждет пришествия глянца»

**Суммарный объем российского рынка рекламы в I кв. 2010 г. АКАР оценила в 46 млрд руб. – на 5% выше, чем год назад. И если на эфирном ТВ прирост рекламы составил те же 5%, то в Рунете объем медийной рекламы увеличился на 16%, а контекстной – на 42%. С вопроса: «В чем причины такого опережающего роста?» – мы и начали беседу с Алексеем КАТКОВЫМ, коммерческим директором Mail.Ru.**

Алексей КАТКОВ

– Во время кризиса компании начинают более точечно расходовать маркетинговые бюджеты, поэтому за 2009 г. многие рекламодатели приучились тратить деньги на покупку рекламы на площадках, эффективность размещения на которых можно измерить. А Интернет, как известно, дает бренду возможность не только в интерактивном режиме контактировать с потенциальными клиентами, – которых мы можем отобрать для него по полу, возрасту, местонахождению, – но и получать в режиме онлайн всю статистику.

К тому же, по нашим оценкам, размещение охватной рекламы на крупнейших порталах Рунета по цене сравнимо сегодня с рекламой на телевидении, если говорить не о прайм-тайм, а о среднем GRP (Gross Rating Point).

**– Кризис способствовал снижению цены контакта бренда с пользователем?**

– В последнее время цена контакта у ведущих игроков рынка Интернет-рекламы уменьшалась за счет расширения предложения и роста аудитории. Было бы странно при большом количестве трафика повышать цены, ведь наши главные конкурентные преимущества – интерактивность, точечное донесение рекламы и цена. Так что в среднем по рынку цены снижались.

**– Какие виды таргетинга (социально-демографический, поведенческий), по опыту Mail.Ru, наиболее эффективны?**

– Наш опыт показывает, что большая часть баннерной рекламы покупается сегодня в лучшем случае с геонастройками – на Россию, на Москву, на какой-то другой регион. Использование социально-демографических настроек зависит от предпочтений рекламодателей. Одни готовы купить всю аудиторию: так дешевле. Другие просят «нарезать» ее сегментами, «потоньше». Оба подхода оправданны, но поскольку второй мы активно продвигаем, то рекламодатели часто покупают у нас женскую или мужскую аудиторию нужного им возраста.

Многие говорят о том, что поведенческая реклама хорошо работает. Однако мы считаем это скорее исключением, чем правилом, поскольку знаем, что ее несвоевременный показ может раздражать пользователя. И до тех пор пока нет четкого понимания, как такая реклама в определенных интервалах времени соотносится с поведением человека, ее размещение – это эксперимент.

Наиболее эффективна та реклама, которая размещается на соответствующих ей по тематике нишевых проектах – автомобильных, женских, туристических. Максимальный охват аудитории дают главные страницы, почтовые сервера, новостные ресурсы. Если этого недостаточно, возможно, стоит подумать о создании спецпроекта.

**– Как изменилось соотношение медийной, контекстной рекламы и спецпроектов в доходах компании Mail.Ru?**

– Поскольку до сих пор никто так и не знает, на что имеет смысл делать основную ставку, мы стараемся активно работать во всех направлениях. В прошлом году мы росли быстрее рынка в сегменте и медийной, и контекстной рекламы, но соотношение их долей в доходах, думаю, осталось таким же, как в 2008 г. (55% – медийная реклама, 20% – контекстная, 25% – платные сервисы. – *Прим. авт.*).

При этом в 2009 г. у нас существенно выросла доля спецпроектов – до 12–13% в объеме доходов от медийной рекламы. И мы считаем, что интерес к нестандартным способам коммуникаций будет только расти, поскольку они позволяют компаниям сделать потенциальным клиентам какое-то уникальное предложение, выделиться из общего ряда среди десятка других рекламодателей.

**– Удалось ли Mail.Ru увеличить долю платных сервисов в своих доходах?**

– В прошлом году действительно весь Интернет-мир перефокусировался на получение доходов от конечных пользователей, поняв, что по объемам эти доходы сравнимы с теми, которые можно получить от рекламодателей. И анализ наших результатов за 2009 г. подтвердил, что это действительно так.

Мы делали все для того, чтобы деньги пользователей заработать: открыли API на «Моем Мире», подключили много игровых приложений от внешних партнеров, приобрели компанию Astrum Online Entertainment, что позволило нам стать крупнейшим игроком на рынке платных сервисов в Рунете – сегодня это признают все.

**– Для того чтобы воспользоваться API, внешние разработчики делятся с вами доходами?**

– Наша философия такова: по-настоящему большой рост рынка получается тогда, когда его раскачивают много игроков. Вот почему сегодня мы оставляем 100% доходов разработчикам, а сами зарабатываем на собственных приложениях. И, судя по количеству под-

ключений к «Моему Миру», партнеры с удовольствием пользуются возможностью заработать тут деньги, а затем с таким же удовольствием реинвестируют их в свое дальнейшее развитие.

Со своей стороны, если мы понимаем, что открытое кем-то направление интересно, мы тоже стараемся туда идти, выступать в нем самостоятельно, поскольку нам важно минимально зависеть от партнеров. Это правильная модель, к которой рано или поздно должны прийти все.

**– В России активно строятся сети 3G, действуют сети мобильного WiMAX. Как компания Mail.Ru использует это для своего развития?**

– Сегодня все игроки стараются развить активность в мобильном направлении, и мы не исключение. Тон задали производители мобильных устройств, начав рекламировать их как средства, с помощью которых человек может получить доступ к любимым интернет-сервисам. И это был прорыв, заставивший ускориться производителей контента.

Мы выпустили усовершенствованный мобильный клиент «3 в 1» (Mail.Ru.Агент, Mail.Ru.Почта, Mail.ru.Карты): скачав его на мобильный телефон, пользователь получает сразу три самых востребованных с мобильных устройств сервиса. В 2008 г. каждое 12-е сообщение из Mail.Ru.Агента отправлялось с мобильного телефона, а в 2009 г. – уже каждое шестое. За это время количество пользователей мобильного Агента выросло на 100%, в этом году, судя по динамике первых пяти месяцев (с января по май прирост составил почти 54%), показатели увеличатся еще больше.

Единственно, мы пока не стали активно продавать в наших мобильных версиях рекламу, поскольку не очень понимаем, как коррелируют раздражение пользователей и количество денег, которые можно заработать. Пусть лучше, пока рынок маленький, люди приучаются пользоваться мобильными приложениями, а потом мы поймем, что с ними делать.

**– Какие ожидания вы связываете с нынешним годом?**

– Темпы роста рынка Интернет-рекламы в 2010 г. уже в несколько раз выше, чем в 2009-м. Так что прирост его объема на 20–40% вполне реалистичен. Появятся ли какие-то новые предложения, которые «взорвут» рынок? Я не думаю. Популярные сервисы (социальные сети, мобильные приложения, сервисы, связанные с видео) будут становиться еще популярнее, а те, которые отмирают, уйдут в прошлое.

В 2010 г. может состояться пришествие в Интернет «глянца». Многие дорогие издания, посвященные моде и стилю, по словам их же издателей, готовятся к приходу в Россию iPad. Уже сегодня очевидно, что он станет желанным подарком для активных и обеспеченных женщин и мужчин. А за «глянцевыми» изданиями в Рунет последуют бренды из сегмента luxury, поскольку там появится контент, на фоне которого они готовы размещаться. И поскольку делать это они будут за дополнительные деньги, у Интернета как у медиаканала снова будет возможность увеличить свою долю в «общем пироге» российского рекламного рынка.

Беседовала **Александра КРЫЛОВА**

# Корпоративная вычислительная сеть
## Как сделать ее неуязвимой?

**В последние несколько лет атаки извне на корпоративные вычислительные ресурсы происходят все чаще и наносят существенный ущерб. «Дыры» в защите информационных систем обычно возникают из-за стандартных ошибок в их проектировании и эксплуатации, и для проникновения в них нарушители пользуются не менее стандартными методами.**

**Артем СЫЧЕВ,** к.т.н., доцент, начальник управления информационной безопасности ОАО «Россельхозбанк»

**Дмитрий КУЗНЕЦОВ,** руководитель отдела консалтинга, компания Positive Technologies

Перечисляя наиболее актуальные угрозы информационной безопасности, специалисты обязательно называют три класса угроз:

- вирусные эпидемии;
- DoS-атаки на доступные извне информационные ресурсы компаний;
- использование сотрудниками компании внутренней информации, включая передачу инсайдерской информации третьим лицам.

Угрозы, связанные с проникновением нарушителей в информационные системы компаний извне, в качестве актуальных сегодня не рассматриваются. Подобная позиция основывается на двух утверждениях: во-первых, периметр вычислительной сети компаний обычно достаточно хорошо защищен; во-вторых, доступ к корпоративным информационным ресурсам не принесет нарушителю материальной выгоды.

Насколько эти утверждения соответствуют действительности? Несколько лет назад были выявлены случаи массовых атак на торговые сети (инциденты расследовались секретными службами США), которые вызвали широкий общественный резонанс. Эти примеры дают представление о масштабе деятельности хакеров (в ходе атак были украдены данные десятков миллионов платежных карт) и показывают, что факты взлома обнаруживаются далеко не сразу, а порой и вообще не обнаруживаются защищающейся стороной.

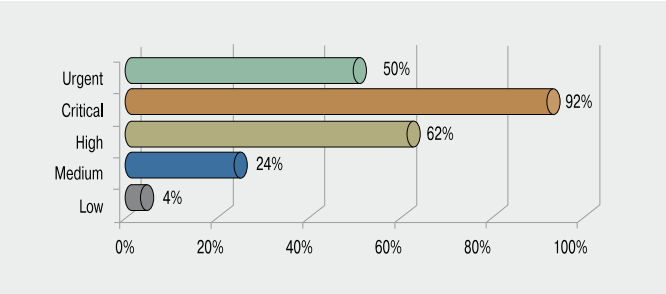
В России информация о подобных инцидентах не столь доступна, но это не означает, что такие атаки отсутствуют. Как правило, целью нарушителей становятся рабочие места, с которых проводятся платежи с помощью систем «клиент-банк». Причем если раньше нарушителям было достаточно только скопировать закрытые криптографические ключи, которыми подписываются платежные поручения, то в последнее время, с переходом на аппаратные ключевые носители, нарушителям приходится получать полный контроль над этими рабочими местами, отправляя поддельные платежные поручения непосредственно с них.

Как правило, причиной подобных инцидентов становятся стандартные ошибки в проектировании и эксплуатации информационных систем, и нарушитель пользуется для проникновения не менее стандартными методами, эксплуатирующими подобные ошибки. Эти ошибки и основанные на них методы взлома мы и рассмотрим.

### Уязвимости веб-приложений

Уязвимости веб-приложений – наиболее распространенный сегодня способ проникновения в информационные системы компаний и реализации атак на клиентов этих компаний. По результатам исследования[1], проведенного экспертами компании Positive Technologies, в 2008 г. практически каждый корпоративный веб-портал содержал уязвимости уровней Urgent или Critical (рис. 1),

***Рис. 1.*** Распространенность уязвимостей различных категорий




[1] Отчет «Статистика уязвимости Web-приложений за 2008 год», Д. Евтеев, 2009.

позволяющие нарушителю получить контроль над порталом и/или использовать его для атак на внутренние информационные ресурсы компании либо рабочие места посетителей портала.

Один из распространенных методов атаки – внедрение операторов SQL. Эта техника позволяет нарушителю передавать веб-приложению на исполнение произвольные (пусть и с некоторыми ограничениями) конструкции языка SQL. При этом используется распространенная ошибка разработки веб-приложений, при которой SQL-запросы к СУБД формируются на основании передаваемых пользователем параметров без дополнительной семантической проверки получившегося запроса. Это позволяет нарушителю, передавая не предусмотренные разработчиком приложения параметры, изменять семантику формируемых SQL-запросов, например, дополняя запросы собственными операторами или изменяя логические выражения в параметрах выборки. Самостоятельно формируя значение параметра id, нарушитель может передавать веб-приложению собственные SQL-запросы. Подобная техника позволяет нарушителю решать широкий круг задач: от изменения контента веб-приложения до получения контроля над ним.

Аналогичная ошибка, допускаемая разработчиками Web-приложений, состоит в том, что принимаемый от пользователя параметр передается в качестве аргумента при вызове из кода веб-приложения команд операционной системы. Такая ошибка классифицируется как «выполнение команд операционной системы» и позволяет нарушителю навязывать серверу исполнение собственных команд.

Еще одна часто встречающаяся ошибка – предсказуемый идентификатор сессии. Идентификация сессии – стандартный механизм авторизации пользователей в веб-приложениях. После успешной аутентификации приложение присваивает сессии пользователя уникальный идентификатор, который передается серверу в каждом последующем запросе этого пользователя и используется для подтверждения его аутентичности. Надежность такого механизма основана на двух предпосылках: что нарушитель не может перехватить идентификатор сессии и что длина идентификатора не позволяет в приемлемые сроки выполнить перебор возможных вариантов.

Данный механизм наиболее эффективен тогда, когда каждый следующий генерируемый приложением идентификатор является элементом равномерно распределенной случайной последовательности. Однако в реализации механизмов генерации идентификаторов сессии встречаются ошибки, сильно сужающие область перебора. При этом у нарушителя, имеющего в своем распоряжении один идентификатор, появляется возможность поиска идентификаторов сессий остальных пользователей, активно использующих приложение в момент атаки.

Ошибки в веб-приложениях не всегда используются для атак именно на это приложение. Зачастую цель взлома – рабочие места пользователей этого приложения, и чаще всего для этого используются уязвимости, приводящие к возможности межсайтового исполнения сценариев (XSS). Предпосылкой для их появления становится все та же ошибка программирования, при которой отображаемый контент формируется на основании параметров, передаваемых в HTTP-запросе, без семантической проверки этих параметров. Межсайтовое выполнение сценариев возможно тогда, когда значение передаваемого параметра непосредственно включается в тело формируемой веб-сервером HTML-страницы.

Уязвимости XSS разделяют на постоянные (persistent) и отраженные (reflected). Постоянная XSS позволяет нарушителю внедрять свой код в долговременный контент веб-приложения (например, в сообщения на форумах или в комментарии к новостям). Внедренный с ее помощью код будет исполнен в браузере каждого из посетителей измененной страницы. Отраженная XSS встречается значительно чаще и характерна для приложений, однократно отображающих значение переданного параметра в сгенерированной на основании пользовательского запроса странице (например, для поисковых систем, когда в результатах поиска отображается введенный пользователем запрос).

Уязвимости XSS широко и разнообразно используются при атаках на рабочие места пользователей с использованием методов социальной инженерии.

## Уязвимости инфраструктуры

### Проблемы парольной защиты

Разработчики бизнес-приложений часто допускают одновременно две ошибки:

- не предусматривают ограничения на минимальную сложность задаваемого пользователем пароля;
- не предусматривают механизмов противодействия автоматическому перебору паролей (ввод CAPTCHA, блокировка учетной записи после определенного числа неуспешных попыток аутентификации и т.п.).

Как показывают результаты исследования[2], проведенного компанией Positive Technologies, если применять средства, ограничивающие минимальную длину пароля, российские пользователи склонны выбирать пароли, являющиеся сочетанием клавиш, расположенных рядом на клавиатуре. При этом почти 9% пользователей используют один из 10 наиболее распространенных паролей (см. таблицу). Кстати, подобные пароли, хотя и в меньшей степени, характерны и для механизмов аутентификации операционных систем и приложений, в которых предусмотрены средства контроля сложности задаваемых паролей.

При такой частоте встречаемости паролей успех нарушителя при подборе учетных записей определяется двумя факторами: количеством пользователей в информационной системе и наличием перечня актуальных имен пользователей (или возможности подбора имен).

Как правило, на поздних этапах проникновения нарушитель уже имеет список актуальных имен пользователей, полученных в результате доступа к каталогу Active

[2] «Анализ проблем парольной защиты в российских компаниях», Д. Евтеев, 2009.

Топ-10 наиболее часто встречающихся паролей

| Пароль | Частота встречаемости, % |
|---|---|
| 1234567 | 3,36 |
| 12345678 | 1,65 |
| 123456 | 1,02 |
| <пустая строка> | 0,72 |
| 12345 | 0,47 |
| 7654321 | 0,31 |
| Qweasd | 0,27 |
| 123 | 0,25 |
| Qwerty | 0,25 |
| 123456789 | 0,23 |
| Итого | 8,53 |

Directory, таблицам баз данных, документам на рабочих местах пользователей или корпоративной электронной почте. Но и на начальных этапах у нарушителя зачастую есть возможность эффективного перебора имен.

Еще одной серьезной проблемой является использование стандартных паролей, устанавливаемых по умолчанию. При установке программного обеспечения создаются так называемые технологические учетные записи, которые служат для первого входа пользователя в систему или для взаимодействия программных компонентов между собой. Такие учетные записи стандартны для определенной версии программного обеспечения, их состав может меняться от версии к версии, а их количество для отдельного семейства программ может достигать десятков и сотен (к примеру, для СУБД Oracle различных версий известно до 1000 стандартных сочетаний имени и паролей «технологических» пользователей). Как правило, после установки системы администраторы забывают изменить заданные по умолчанию пароли или заблокировать ненужные учетные записи.

Кроме онлайновых методов подбора пароля, нарушителю доступны и другие методы. Например, из соображений безопасности в информационных системах хранятся не пароли пользователей, а результаты вычисления хэш-функции этих паролей. Необратимость хэш-функции обеспечивает невозможность восстановления пароля, однако это верно только для паролей достаточной сложности.

Согласно результатам того же исследования, большая часть пользователей использует пароли длиной до восьми символов включительно. В настоящее время в рамках нескольких открытых проектов (например, http://www.freerainbowtables.com) проводится расчет значений хэш-функции для паролей различной длины в различных алфавитах. Готовые таблицы значений хэш-функции, находящиеся в открытом доступе, обеспечивают высокий процент восстановления паролей такой длины, причем восстановление одного пароля занимает несколько минут.

Благодаря этому источниками паролей пользователей для нарушителя могут служить:

- конфигурационные файлы сетевого оборудования;
- файлы /etc/shadow операционных систем Unix;
- резервные копии операционных систем;
- сетевой трафик;
- системные таблицы СУБД, в том числе доступные с помощью уязвимостей веб-приложений, и т.п.

### Недостатки сетевой инфраструктуры

Ошибки в сетевой архитектуре упрощают нарушителю выполнение ряда атак. К наиболее распространенным можно отнести:

- проблемы сегментирования локальной вычислительной сети и межсетевого экранирования;
- использование сетевых протоколов, позволяющих нарушителю собирать информацию о сетевых устройствах или навязывать сетевым устройствам собственные настройки сетевого взаимодействия;
- использование незащищенных или недостаточно защищенных протоколов прикладного уровня.

При правильной организации локальной вычислительной сети рекомендуется разделять ее на сегменты разного функционального назначения и обеспечивать фильтрацию трафика на границах сегментов. Эти рекомендации зачастую не выполняются.

Распространенной ошибкой является предоставление доступа из Интернета к узлам, размещенным в пользовательском или серверном сегментах ЛВС. Это позволяет нарушителю, получив контроль над одним из приложений, серверов или рабочих станций, беспрепятственно атаковать остальные узлы ЛВС. Кроме того, нередко предоставляется доступ из Интернета к управляющим интерфейсам приложений, серверов и сетевого оборудования.

При подключении серверов и рабочих мест к коммутаторам ЛВС зачастую не принимаются меры противодействия сетевым атакам со стороны внутренних узлов ЛВС (от атаки типа «отравление кэша ARP» до эксплуатации уязвимостей в сетевых сервисах), а также не выполняются настройки протоколов управления, направленные на скрытие топологии сети от рядового пользователя. Это позволяет нарушителю, получив контроль над одним из внутренних узлов, исследовать сеть, выявлять соседние устройства и организовывать атаки на них.

При развертывании сетевых сервисов вместо защищенных вариантов протоколов прикладного уровня для передачи чувствительной информации используются их аналоги без криптографии или со слабой криптографической защитой – NTLM вместо Kerberos, POP3 вместо IMAP, SNMP v.2 вместо v.2c или V.3, а также SMTP, FTP и HTTP без поддержки SSL/TLS. Это позволяет нарушителю перехватывать чувствительную информацию, в том числе новые учетные записи.

### Уязвимости беспроводных сетей

В беспроводных сетях допускается несколько типичных ошибок, среди которых отметим две. Это защита беспроводного трафика с использованием протокола WEP и возможность подключения ноутбуков пользователей к произвольным точкам беспроводного доступа.

Протокол WEP использует слабые методы криптографической защиты, что позволяет нарушителю сравнительно легко восстановить криптографические ключи, применяемые при взаимодействии устройств. Это дает ему возможность подключаться к беспроводной сети и организовывать атаки, находясь внутри периметра защиты. Последствия такой атаки очевидны.

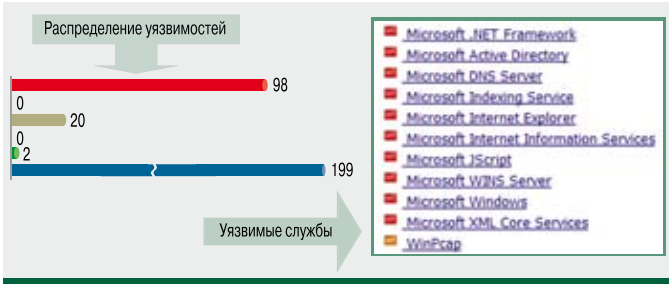
Использование сотрудниками компании ноутбуков создает для нарушителя дополнительный вектор проникновения. Соединяясь с посторонней точкой доступа, пользователь попадает в среду, созданную владельцем этой точки доступа. При этом совершенно не исключено, что точка доступа контролируется злоумышленником. Кроме того, владелец точки доступа, если он не является оператором связи, не имеет перед пользователем никаких обязательств по обеспечению тайны связи.

Как правило, в отношении мобильных устройств применяются те же меры защиты, что и для стационарных рабочих мест (особенно в части управления уязвимостями и установки патчей). Выбор этих мер ориентирован в первую очередь на работу внутри внешнего периметра защиты, который является первым рубежом защиты, отводя ряд угроз. При подключении к сторонней точке доступа этот рубеж отсутствует, о чем администраторы, настраивающие функции безопасности операционной системы и индивидуальные средства защиты, часто забывают.

## Уязвимости и ошибки конфигурации программного обеспечения

Одна из самых серьезных проблем в обеспечении информационной безопасности российских компаний – несвоевременная установка обновлений безопасности или отказ от их установки. Причины тому называют разные. Например, в случае установки обновлений на серверы, находящиеся в промышленной эксплуатации, обслуживающий персонал нередко опасается того, что программное обеспечение в результате будет работать нестабильно. Установка обновлений на рабочие места пользователей затрудняется большим количеством используемых программ и невозможностью своевременно отслеживать выпуск обновлений.

***Рис. 2.*** Пример результатов сканирования контроллера домена




Сканирование внутренних узлов ЛВС большинства российских компаний показывает примерно одинаковую картину (рис. 2).

Аналогичную картину можно наблюдать при анализе конфигурации программного обеспечения. Для безопасной работы Windows XP необходимо настроить свыше 200 параметров; из них около 60% настраиваются автоматически при инсталляции операционной системы, а остальные параметры требуют дополнительной настройки. Как правило, анализ конфигурации показывает, что подобная настройка не выполняется, что приводит к появлению на рабочих станциях типичных ошибок конфигурации:

- использование протокола NTLM;
- сохранение паролей (точнее, значений хэш-функции) LanManager;
- автозапуск с отчуждаемых носителей и т.п.

Подобные ошибки активно используются для проникновения в информационные системы. Возможность атаки на уязвимые сетевые сервисы появляется после преодоления внешнего периметра с использованием одного из перечисленных в предыдущих разделах недостатков. Однако в последние несколько лет нарушители предпочитают атаковать рабочие места пользователей, используя уязвимости клиентского программного обеспечения и недостаточную осведомленность пользователей в вопросах информационной безопасности.

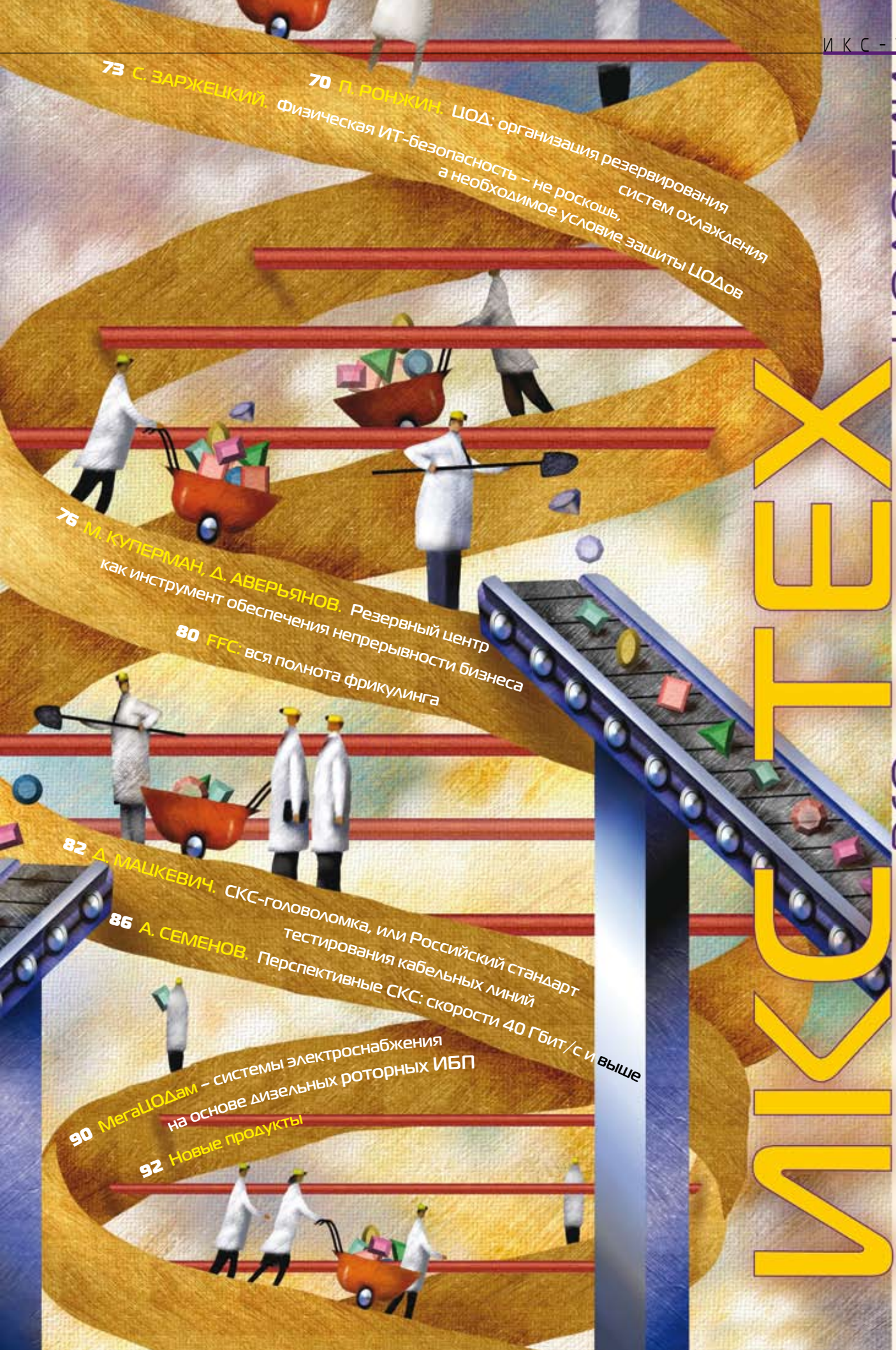
Итак, успешное проникновение в корпоративную вычислительную сеть – это, как правило, результат допущенных защищающейся стороной ошибок.

Наиболее эффективны с точки зрения приближения к цели методы атаки, позволяющие нарушителю получить учетные записи пользователей. Успех подобной атаки дает ему самый широкий спектр дополнительных возможностей, начиная с доступа к информационным системам от имени этого пользователя, с предоставленными ему правами и с использованием штатных средств доступа. Появляется и возможность ознакомления с документами и почтовыми сообщениями пользователя, откуда нарушитель может почерпнуть полезную информацию об информационных ресурсах, организации работы с ними, а также дополнительную информацию о сотрудниках компании, которую можно использовать для организации атак с применением методов социальной инженерии.

В представлении ИТ-специалистов наиболее опасны уязвимости сетевых сервисов – однако это не так. Как правило, нарушителю удается добиться поставленной цели еще до того, как у него появится техническая возможность поиска и эксплуатации уязвимостей программного обеспечения целевого сервера. Значительно быстрее приводит к цели использование ошибок в архитектуре информационных систем и настройках программного обеспечения.

Серьезную опасность представляют атаки на рабочие места пользователей с использованием методов социальной инженерии. В то же время первопричина успешной атаки – это, как правило, не низкая осведомленность пользователей, а наличие на рабочем месте уязвимостей и ошибок конфигурации, возможность использовать которые нарушитель получает в результате действий пользователя. ИКС

# ИКС pro технологии



# ЦОД: организация резервирования систем охлаждения

**Ни для кого не секрет, что системы охлаждения центров обработки данных должны оснащаться резервными кондиционерами и чиллерами. Но достаточно ли при проектировании ЦОДа просто увеличить количество охлаждающего оборудования или потребуется что-то еще?**

**Петр РОНЖИН,**
директор,
ООО «ВЕНТСПЕЦСТРОЙ»

К сожалению, обращение к российским стандартам не дает ответов на поставленные вопросы. Впрочем, и самих российских стандартов, посвященных теме резервирования систем охлаждения, нет. Есть безнадежно устаревшая, не соответствующая реалиям сегодняшнего дня, но от безысходности используемая Инструкция по проектированию зданий и помещений для электронно-вычислительных машин СН 512. В ней к обсуждаемой в данной статье теме относятся лишь несколько строк: «Для повышения надежности систем кондиционирования воздуха необходимо предусматривать блокировку кондиционеров попарно по приточным и рециркуляционным воздуховодам, дублирование наиболее важных элементов системы (вентиляционные агрегаты, компрессоры, насосы) или целиком кондиционеров. Указанные требования должны быть предусмотрены технологическим заданием». Еще инструкция содержит «полезное» требование, состоящее в том, что электроснабжение двигателей системы кондиционирования воздуха – холодильных машин, насосов, вентиляторов – должно соответствовать 2 категории надежности, а электроснабжение ЭВМ вычислительных центров – 1 категории. И это все.

Те, кто занимался ЦОДами или крупными серверными помещениями, понимают, что этой информации совершенно недостаточно для проектирования и строительства дата-центра, который мог бы соответствовать сертификационным требованиям западных стандартов. Здесь в первую очередь имеются в виду уже ставшие широко известными в России документы ANSI/TIA-942-2005 Telecommunication Infrastructure Standard for Data Centers и стандарт, разработанный Uptime Institute, Data Center Site Infrastructure Tier Standard: Topology.

Принятая в этих стандартах классификация дата-центров описывает уровни инфраструктуры инженерных площадок, требуемые для обеспечения работы ЦОДа. В классификации не указываются характеристики отдельных систем или подсистем, зато устанавливаются принципы их проектирования и строительства, а также взаимосвязи между различными инженерными системами.

Классификационные уровневые требования по инфраструктуре ЦОДов применительно к системам охлаждения следующие.

## Дата-центр уровня Tier I

Все инженерные компоненты такого ЦОДа могут использоваться без резервирования. Для систем охлаждения это означает, что допускается применение кондиционеров любого типа при условии, что их количество достаточно для снятия тепловой нагрузки. При выходе из строя какого-либо кондиционера или при проведении технического обслуживания кондиционерного оборудования или систем его электропитания придется частично или полностью остановить оборудование дата-центра.

Единственное серьезное требование заключается в том, что при наличии питания серверного и компьютерного оборудования от аварийных генераторов все системы кондиционирования также должны быть подключены к ним в режиме ожидания.

## Дата-центр уровня Tier II

Инженерная инфраструктура дата-центра Tier II должна строиться по принципу резервирования компонентов.

Охлаждающее оборудование резервируется по схеме N + 1, где N – необходимое количество оборудования для снятия 100% тепловой нагрузки. При этом должен быть предусмотрен один резервный кондиционер на каждые три-четыре работающих.

Трубопроводы контура холодоносителя не резервируются, но циркуляционные насосы и фильтры также устанавливаются в количестве N + 1.

Кондиционерные системы должны быть подключены к генераторам в режиме ожидания. Электропитание систем кондиционирования распределяется таким образом, чтобы свести к минимуму воздействие на климатические

# Виртуализация –
## это только половина битвы за эффективность


InfraStruXure™
DATA CENTERS ON DEMAND

### Принципы архитектуры InfraStruXure® для сред с высокой плотностью монтажа

1. Стойки для оборудования с высокой плотностью монтажа
2. Блоки распределения электропитания с контролем параметров на уровне стоек
3. Контроль температуры на уровне стоек
4. Программное обеспечение централизованного контроля (не показано)
5. Эксплуатационное программное обеспечение с возможностями прогнозирования и управления мощностью (не показано)
6. Эффективные системы охлаждения InRow®
7. Гибкие и масштабируемые системы электропитания с ИБП

### Вы можете развернуть стойки с высокой плотностью выделяемой тепловой мощности прямо сейчас

InfraStruXure можно развернуть как основу всей архитектуры центра обработки данных или серверного зала либо встроить в крупный существующий центр обработки данных.

## Виртуализация останется надолго

И это неудивительно — она позволяет экономить место и энергию, в то же время максимально использовать ИТ-ресурсы. Однако за компактность иногда приходится платить. Виртуализированные серверы — даже при загрузке на 50% мощности — требуют особого внимания к охлаждению независимо от их размера или расположения.

**1. Повышение тепловыделения.** Объединение серверов увеличивает плотность интеграции и тепловыделения в стойке, что создает риск простоев и сбоев.

**2. Снижение эффективности.** Периферийное охлаждение не позволяет справиться с перегревом в глубине стоек, а чрезмерная мощность охлаждения ведет к увеличению затрат и снижению эффективности.

**3. Сбой электропитания.** Виртуальные нагрузки постоянно меняются, что затрудняет прогнозирование доступной мощности электропитания и охлаждения, создавая риск повреждения сети.

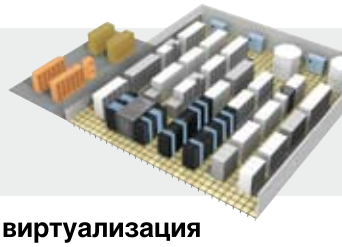
### Правильный подход к виртуализации

Новая архитектура InfraStruXure для сред с высокой плотностью монтажа помогает справиться с ростом тепловыделения благодаря охлаждению рядов стоек с виртуализированными серверами, управлению электропитанием на уровне стоек и мощному программному обеспечению для управления и моделирования систем. Виртуализация позволяет экономить энергию, однако реальная эффективность среды зависит также от относительной эффективности систем электропитания, охлаждения и серверов. Только оптимально подобранная мощность всей системы позволяет получить экономию за счет повышения эффективности. Чтобы построить оптимальную конфигурацию, положитесь на эффективную модульную архитектуру InfraStruXure для сред с высокой плотностью выделяемой тепловой мощности и нейтрализуйте тепло у его источника. Ваше оборудование будет работать более безопасно и эффективно, приближаясь к использованию мощности на 100%.

### Виртуализация — и нет проблем

Что вы ожидаете? Архитектура InfraStruXure для сред с высокой плотностью выделяемой тепловой мощности открывает возможности виртуализации для всех, в любое время и в любом месте. Просто разверните ее и приступайте к работе.

**Обозначения:**
- Блоки кондиционеров
- Стойки обычной плотности
- Централизованные ИБП
- Зоны Infrastruxure для сред высокой плотности



### Эффективность и виртуализация

Ваши серверы используются эффективно, но можно ли сказать то же о системах электропитания и охлаждения?

Использование мощности охлаждения | Серверы | Использование мощности электропитания

**ДО ВИРТУАЛИЗАЦИИ СЕРВЕРОВ**

Возможна большая экономия на серверах и системах электропитания и охлаждения.

- ☐ Оптимальное использование серверов
- ☐ Оптимальная мощность электропитания
- ☐ Оптимальная мощность охлаждения

Эффективность 29%

**ПОСЛЕ ВИРТУАЛИЗАЦИИ СЕРВЕРОВ**

Чрезмерно завышенная мощность электропитания и охлаждения гасит потенциальный выигрыш от виртуализации.

- ☑ Оптимальное использование серверов
- ☐ Оптимальная мощность электропитания
- ☐ Оптимальная мощность охлаждения

Эффективность 16%

**ВИРТУАЛИЗАЦИИ СЕРВЕРОВ С СИСТЕМАМИ ЭЛЕКТРОПИТАНИЯ И ОХЛАЖДЕНИЯ**

Оптимальная мощность электропитания и охлаждения смещает баланс в вашу пользу.

- ☑ Оптимальное использование серверов
- ☑ Оптимальная мощность электропитания
- ☑ Оптимальная мощность охлаждения

Эффективность 63%

t.a.c by Schneider Electric | PELCO by Schneider Electric | SQUARE D by Schneider Electric | CISCO PARTNER Technology Developer | Microsoft | IBM ALLIANCE PARTNER | DELL | EMC² SELECT

Загрузите **БЕСПЛАТНО** информационную статью APC №117 «Адаптивная инженерная инфраструктура центра обработки данных: оптимизация ценности бизнеса» и **станьте участником розыгрыша* — выиграйте компактную цифровую видеокамеру Canon Camcorder HV30.**

Зайдите на сайт **www.apc.com/promo** и введите код **78977t**

APC by Schneider Electric

**APC by Schneider Electric в Москве: 119334, Москва, 5-й Донской проезд, д. 21-Б, стр. 10. Тел.: + 7 495 916-7166, Факс: + 7 495 620-9180, Центр поддержки клиентов: +8 800 200 2722, E-mail: apcrustech@apc.com**

системы, которое может оказать выход из строя одной из систем электропитания. Все системы температурного контроля должны быть запитаны через ИБП.

Такой дата-центр должен работать 24 часа 365 дней в году, однако обслуживание критически важных узлов системы охлаждения, например полная замена холодоносителя в трубопроводах, потребует остановки всей системы охлаждения и, соответственно, всего ЦОДа.

## Дата-центр уровня Tier III

Инженерные системы такого ЦОДа, в том числе системы охлаждения, должны проектироваться таким образом, чтобы обеспечить возможность обслуживания систем одновременно (параллельно) с работой дата-центра. Это достигается путем использования нескольких распределительных силовых цепей и охлаждающих контуров, позволяющих отключать часть трубопроводов холодоносителя для проведения плановых работ и ремонта без воздействия на работу дата-центра.

При наличии водоохлаждающего оборудования каждая система охлаждения должна быть разделена на независимые друг от друга подконтуры (подсистемы). Резервирование чиллеров, кондиционеров, насосов, фильтров и т.д. на каждой подсистеме производится аналогично резервированию этих компонентов для систем охлаждения дата-центров уровня Tier II.

Запланированные воздействия на системы охлаждения – обслуживание, ремонт, замена компонентов, добавление или удаление кондиционеров, чиллеров, насосов, испытания компонентов и систем – не приводят к нарушениям в работе компьютерного оборудования дата-центра.

Питание компьютерного и телекоммуникационного оборудования должно осуществляться от нескольких вводов, и для обеспечения его бесперебойного функционирования при пропадании питания требуются две одновременно работающие активные распределительные линии. Эти линии должны быть подключены к двум раздельным ИБП, в которых каждая система имеет резервирование N + 1.

Системы охлаждения должны иметь такое же резервирование по питанию, как и компьютерное оборудование.

Ярким примером взаимосвязи отказоустойчивости инженерных систем является то обстоятельство, что ИБП и аккумуляторные помещения должны охлаждаться прецизионными кондиционерами, которые, в свою очередь, должны быть обеспечены бесперебойным питанием.

Непланируемые активности, такие как ошибки управления или спонтанные сбои инфраструктурных компонентов, могут привести к нарушению работы дата-центра.

## Дата-центр уровня Tier IV

Уровень технических решений, реализуемых в инженерной инфраструктуре дата-центра Tier IV, должен обеспечивать устойчивость к отказам, в том числе и к незапланированным действиям. Применительно к системе охлаждения это означает использование тех же принципов, что и для систем охлаждения дата-центров уровня Tier III, вкупе с резервными системами управления (контроллерами) на основе конфигурации «система + система». Для систем охлаждения, базирующихся на фреоновых кондиционерах с непосредственным расширением, должны предусматриваться альтернативные ресурсы холода на базе водяных аккумуляторов.

■ ■ ■

Столь подробное описание уровневых требований к системам охлаждения не случайно. Для нашей российской практики такой подход еще непривычен и поэтому не всеми принимается. Гораздо чаще в технических заданиях с большей или меньшей степенью детализации описывается оборудование, его технические характеристики и приводятся расплывчатые требования к работоспособности системы. В этом случае уровень доступности ЦОДа зависит от того, насколько компетентными оказались специалисты, готовившие ТЗ и делавшие по нему проект. Применение в России уже отработанных западных стандартов позволит значительно повысить качество проектов и гарантировать заявленный уровень отказоустойчивости ЦОДов. ИКС

# Физическая ИТ-безопасность – не роскошь, а необходимое условие защиты ЦОДов

**В Европе давно стало нормой при строительстве ЦОДа выделять из общего бюджета 15% на обеспечение его физической безопасности на основе промышленных решений. В России о существовании таковых до недавнего времени «цодостроители» даже не подозревали. Однако новый сегмент рынка ИТ-безопасности формируется буквально на глазах – и при непосредственном участии нашего собеседника, Станислава ЗАРЖЕЦКОГО, генерального директора ООО «Эксол».**

**– Станислав, в своей статье* в журнале «ИКС» Вы отмечали, что при строительстве ЦОДов в России выделяют немалые средства на обеспечение двух составляющих безопасности ИТ-инфраструктуры – технической (вычислительные мощности) и логической (ПО). Третий сегмент – физическая ИТ-безопасность – часто рассматривается как избыточный и неоправданно затратный. Почему это, на Ваш взгляд, происходит? И почему происходить не должно?**

– Не должно – потому что обычные строительные методы не защищают ИТ-оборудование от воздействия огня снаружи. Скажем, при пожаре с внешней стороны уже через 15–20 минут влажность в комнате достигнет 100%, поскольку любой кирпич или бетон начинает испарять влагу, из которой он состоит как минимум на 42%. Причем это будет горячий пар. ЦОД просто погибнет, никакое компьютерное оборудование работать в таких условиях не в состоянии. Только специальные решения позволяют при внешней температуре до 1100°C сохранять внутри температуру не выше 70°C и влажность не больше 85% в течение 120–180 минут. В Европе такой подход (как и другие требования по целому ряду параметров) предусмотрен нормой EN 1047-2. Это комплексные решения, которые защищают ЦОД от всего, что может его повредить или уничтожить. Они делятся на две большие категории. Первая – комнаты безопасности (или помещения безопасности), обеспечивающие защиту периметров большой площади (здание, помещение). Они предназначены для больших ЦОДов, аутсорсинговых или принадлежащих крупным компаниям. Вторая категория – модульные сейфы безопасности. Это решения для отдельных 19-дюймовых стоек с ИТ-оборудованием, они интересны компаниям среднего размера и выше.

Замечу, что мы приложили большие усилия, чтобы в России был принят ГОСТ, соответствующий EN 1047-2. До того ведь единственным нормативно-правовым актом в области требований к построению вычислительных центров у нас был стандарт, утвержденный в 1968 г. Десятки лет ГОСТ не менялся – при том что в последние два десятка лет быстрее всего меняющейся оказалась именно среда ИТ! Наконец, с 1 января 2009 г. вступил в действие ГОСТ Р 52919-2008 «Информационная технология. Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость. Комнаты и контейнеры данных» – стандарт, представляющий собой, по сути, русифицированный вариант EN 1047-2. Мы, конечно, этому рады. Но у нас же ГОСТы носят рекомендательный характер, а не исполнительный. То есть люди внимательно читают рекомендации, но не исполняют...

А что касается собственно вопроса «почему так происходит», то не будем забывать, что рынок промышленных решений физической ИТ-безопасности в России зародился всего лишь лет пять назад (к слову, во многом благодаря усилиям нашей компании с партнерами – системными интеграторами). До этого компании и организации в лучшем случае решали вопрос подручными средствами, в худшем полагались на «авось» (не сгорим, не утонем) либо вообще не задумывались на этот счет. Два года упорной просветительской работы принесли свои плоды: заказчики начали понимать, что надежная физическая защита ИТ-инфраструктуры – не роскошь, а необходимость. И начиная с 2005 г. рынок пошел. Сегодня в крупных ЦОДах российских госорганизаций и коммерческих компаний установлено 20 помещений безопасности Lampertz.

**– На всю Россию 20 помещений за пятилетку – не маловато?**

– Согласен. Ежегодно мы выполняем 30–40 проектов комнат безопасности. На выходе должно бы быть 20 комнат в год, однако получается две-три. Основная причина – на последнем этапе все упирается в деньги, конкретные люди принимают отрицательные решения. При этом мне совершенно непонятно, почему те же люди в своей личной жизни не скупятся на физическую безопасность, а в деловой на ней экономят.

**– Но силовые структуры – уж точно ваши заказчики?**

– Могу сказать, что у нас есть три открытых проекта со всеми нашими силовыми

* См. «Огонь, вода и коррозионный газ. Угрозы физической безопасности ЦОДа», «ИКС» №3'2010, с. 85.

структурами. Все проектные работы выполнены, а реализации пока нет, проекты переносятся из года в год. Вероятно, кому-то не удается доказать на заседаниях правительства необходимость физической ИТ-безопасности, но надеемся, что все же удастся. Более печально закончилась наша история с Росстатом: выполненный проект комнаты безопасности отклонили «вышестоящие инстанции» с резолюцией, что данный уровень защиты избыточен. Для меня загадка – почему это произошло. Но вот противоположный случай: такую комнату решила приобрести Российская академия спорта. Зачем? Нам объяснили: в их электронном хранилище данных собрана информация о результатах допинг-контроля всех наших спортсменов за последние пять лет, и если эта информация пропадет, то спортсмены не попадут ни на одно международное соревнование. Для них это реальная необходимость. Как и для Банка Москвы: по их словам, если ЦОД банка остановится, то 40% своих онлайн-сервисов они не смогут обеспечить и за время восстановления потеряют денег в несколько раз больше, чем стоит вся комната безопасности. Или Нижнетагильский металлургический комбинат, где в случае остановки ЦОДа законсервируется вся информация о погрузке-разгрузке – и уже через пять минут придется платить РЖД за простой вагонов. Они посчитали: если ЦОД не работает 3–4 дня, то потери комбината будут равны его годовой прибыли. Действительно, уж лучше потратиться на безопасность ЦОДа.

**– Какова же «цена вопроса», почем комнаты?**

– Это зависит от площади периметра, от комплектации... Невозможно определить стоимость конкретного решения без детального проекта. Но можно с уверенностью сказать, что эта сумма ниже тех 15%, которые выделяют из бюджета ЦОДов европейские компании.

**– А что представляет собой процесс строительства комнаты безопасности «под ключ»?**

– Когда заказчик принимает решение, наши проектировщики начинают работу над проектом. В течение 20–25 дней разрабатывается документация, создается рабочий проект. Потом этот рабочий проект переправляется в Германию, и по нему на заводе делают комнату. На это уходит еще около восьми недель. Затем модули помещения доставляются в Россию – и наши монтажники собирают ее в среднем за 20 рабочих дней. Итого весь процесс занимает три-четыре месяца. При этом, если ЦОД строится в новом здании, работы ведутся параллельно. Именно так в этом году мы реализовали крупный проект создания помещения безопасности для ЦОДа в новом здании «Роснано».

**Помещение безопасности Lampertz**

**– Пока что Вы упомянули только одного вендора – Lampertz. В России другие производители не представлены или их круг в принципе крайне узок? И, кстати, существуют ли отечественные промышленные решения?**

– На последний вопрос сразу отвечаю – нет. Что касается мирового рынка физической ИТ-безопасности, то именно Lampertz стояла у его истоков – первая в мире комната безопасности была создана этой компанией и проинсталлирована в Германии в 1982 г. – и в последующие почти полтора десятка лет оставалась единственным в Европе производителем помещений безопасности. В середине 90-х на европейском рынке начали появляться компании-последователи (в начале 90-х гг. подобное же решение было создано в США, однако за пределы страны оно не вышло). Сегодня пул европейских вендоров модульных комнат безопасности составляют пять компаний: Lampertz, ProRZ, PriorIT, SME, Remtech. В России представлены первые две: Lampertz – компанией «Эксол» (мы имеем статус квалифицированного центра компетенции по решениям Lampertz в России), SME – ЛАНИТ. Кроме того, мы ожидаем в скором времени выхода на российский рынок продукции компании ProRZ, которая сейчас активно в этом направлении работает.

**– То есть придет реальный конкурент Lampertz?**

– В категории «комнаты безопасности» выделяются два сегмента, в зависимости от степени защиты и цены. Если сравнивать с автомобилями, это как «Бентли» и «Мерседес». И то и другое хорошо, хотя и не идентично. Здесь уровню «Бентли» соответствует помещение безопасности LSR 18.6E от Lampertz – наивысшая степень защиты, превышающая даже требования EN 1047-2. По своим защитным свойствам и по цене в ту же категорию входит решение компании PriorIT, но оно проигрывает при установке: если LSR 18.6E собирают трое монтажников в безупречно чистой одежде, без пыли или грязи, то процесс инсталляции комнаты PriorIT очень похож на стройку. Соответственно помещение Lampertz можно монтировать в уже работающем ЦОДе без отключения оборудования, а

специалисты PriorIT сами советуют отключить аппаратуру либо защитить ее от пыли и мусора в период инсталляции. Такое вот серьезное различие между двумя решениями в самой верхней категории защиты. И я готов утверждать, что «бентлее» LSR 18.6E просто не бывает.

Безусловно, не всем заказчикам доступно решение такого уровня. Всем хочется «Бентли», но ведь и «Мерседес» – не «Лада-Приора». К «Мерседесам» мы относим помещения безопасности так называемого среднего уровня защиты: это решения компаний Remtech, SME, ProRZ. Есть такая комната и у Lampertz – LER Extend. На наш взгляд, по своим характеристикам, по защитным свойствам, по качеству исполнения, да и по цене сегодня лучшее решение в этом сегменте у компании ProRZ – помещение безопасности F 90+. Кстати, эта компания была создана в 2005 г. выходцами из Lampertz и за пять лет получила широкую известность на европейском рынке. В 2009 г. ProRZ обогнала Lampertz по продажам комнат средней степени безопасности, и теперь мы работаем над тем, чтобы и российский рынок получил их «Мерседесы». Кстати, к концу этого года ProRZ обещает представить рынку и свой «Бентли», решение комнаты наивысшей степени защиты. Вот тогда у Lampertz появится серьезный конкурент в обоих сегментах.

**– Мы пока обсуждали «Бентли» и «Мерседесы». А как с «Ниссанами» – второй из обозначенных Вами категорий решений физической ИТ-безопасности?**

**Модульный сейф Lampertz**

– Да, модульные сейфы безопасности можно сравнить с хорошими автомобилями эконом-класса. Это комплексы с системами кондиционирования, пожаротушения и т.п., которые рассчитаны на две-три стандартные 19-дюймовые стойки; они быстро доставляются по месту назначения и монтируются.

В России рынок этих решений начал развиваться несколько раньше рынка помещений безопасности. Так, когда в 2005–2006 гг. реализовывалась программа «Электронный паспорт», Федеральная миграционная служба закупила у нас 172 модульных сейфа, установив их в разных городах страны. Сейчас еженедельно мы получаем два-три заказа на такие решения, причем не только от компаний среднего размера, которые не могут потратить деньги на строительство ЦОДа, но и от крупных заказчиков, строящих ЦОДы стандартными строительными методами и устанавливающих в них два-три сейфа для физической защиты ИТ-сердцевины.

**– На рынке производителей сейфов, наверное, потеснее, чем в категории комнат безопасности?**

– В России такие решения представляют несколько производителей сварных и модульных конструкций. Но самые удобные сейфы, модульные, делают только те же Lampertz и ProRZ. Однако есть еще сейфы для хранения медианосителей, и в этом сегменте конкурирует множество производителей. Лидируют финские компании, их поджимают итальянские и испанские вендоры, а также Lampertz. Но я бы не сказал, что они массово покупаются. К сожалению, далеко не все компании понимают огромную разницу между сейфами для хранения бумаги и сейфами для хранения электронных носителей. Между тем «бумажные сейфы» при нагревании сохраняют температуру не выше 98–99°C, а «электронные» – не выше 50°C в течение 120 минут. Например, два года назад при пожаре в редакции известной молодежной газеты сгорел весь ее медиаархив. Потери они оценили в $3 млн. Мы посчитали: если бы этот архив хранился в специальных сейфах, они бы потратили 250 тыс. евро, но не потеряли бы эти миллионы.

Очевидно, что электронные носители информации следует хранить в специализированных сейфах для медианосителей. А «бумажный сейф» в современной компании должен остаться только в бухгалтерии.

**Сейф Lampertz DIS-DATA**

**– Итак, сегодня наиболее востребованы в России модульные сейфы безопасности. Это хорошо или не очень?**

– Наверное, это все-таки шаг вперед. Когда люди поймут, что у них есть решение эконом-класса, они со временем перейдут на следующий этап развития – к помещениям безопасности. Так, один из наших крупнейших банков сначала поставил у себя два модульных сейфа, а буквально через два года – комнату безопасности. При этом два сейфа он вынес на другую площадку и сделал там «зеркальное отображение» сердца своей информационной инфраструктуры. Я думаю, что модульные сейфы безопасности обеспечивают некий переходный этап к тем большим ЦОДам, которые рано или поздно все равно в России возникнут. А с ними – и большие помещения ИТ-безопасности. Знаете ли, стыдно признать, что у нас средняя площадь такой комнаты составляет 60–70 кв. м, а площадь самого большого помещения безопасности – 150 кв. м. Для, сравнения: в Бельгии построена комната безопасности на 2 тыс. кв. м, там стоит оборудование всех телекоммуникационных операторов Северной Европы... Для нас это пока только мечта.

# Резервный центр как инструмент обеспечения непрерывности бизнеса

**Марк КУПЕРМАН,**
ЗАО «Информсвязь Холдинг»

**Дмитрий АВЕРЬЯНОВ,**
ЗАО «Информсвязь Холдинг»

**Практически все крупные ведомства и корпорации имеют информационно-телекоммуникационные системы, обеспечивающие доступ к коллективным информационным ресурсам и коммуникационным сервисам. Для ряда таких систем вопросы надежности носят принципиальный характер. Однако резервирования важнейших узлов путем установки резервного комплекта рядом с основным не всегда достаточно для обеспечения непрерывности их работы.**

## Непрерывность бизнеса

Воздействие внешних факторов на ИТ-инфраструктуру компании, возникновение различных нештатных ситуаций несут в себе постоянную угрозу остановки бизнес-процессов компании. Поэтому тема управления непрерывностью бизнеса (Business Continuity Management, BCM) имеет давнюю историю. Управление доступностью, непрерывностью и мощностями, оценка рисков остановки бизнес-процессов, планы обеспечения непрерывности деятельности компании и восстановления после аварии – эти и другие подобные мероприятия описываются международными, национальными стандартами и рекомендациями, включены в фирменные методики ведущих ИТ-компаний и даже в банковские нормативные акты. Однако ISO/IEC 20000, ITIL, COBIT, BS 25999 и аналогичные документы не отвечают на вопрос: как построить ИТ-инфраструктуру, гарантирующую необходимый уровень непрерывности бизнеса?

Обеспечение непрерывности бизнеса, как правило, тесно связано с резервированием. Но пока нет полной ясности, в каких случаях необходимы резервные компоненты, каковы требования к ним, как их классифицировать по степени отказоустойчивости. Как известно, «нельзя управлять тем, что нельзя измерить» – следовательно, при отсутствии методик количественной оценки непрерывности бизнеса как-то странно говорить о BCM. Даже обоснование коэффициента готовности отказоустойчивых систем сегодня остается скорее философским вопросом, нежели математической задачей (см. «Правда «пяти девяток», «ИКС» №6, с. 84). Ясно одно: если от простоя информационных (платежных, телекоммуникационных и т.д.) систем компания несет убытки, для защиты ее критически важных бизнес-процессов необходим резервный центр.

## Катастрофоустойчивые ЦОДы

В обеспечении бизнес-процессов корпораций и государственных организаций фактор надежности корпоративной сети и информационных систем вносит основную долю рисков, связанных с потерей данных или недоступностью информационных сервисов. Чтобы обеспечить стабильность управления госструктурами или непрерывность бизнеса коммерческих организаций, помимо основных информационных систем предусматриваются резервные. Основу их составляют резервные центры обработки данных (ЦОДы), или дата-центры.

На резервный ЦОД возлагается основная задача обеспечения непрерывности вычислительного процесса при выходе из строя основных систем. Чтобы обеспечить толерантность базовых сервисов ИТ- и коммуникационных систем к различным аварийным ситуациям, на резервной площадке размещают дублирующий комплект серверов и телекоммуникационного оборудования; необходимы также механизмы переключения информационных нагрузок и механизмы репликаций для поддержания актуальной копии данных.

Централизация, повышение эффективности вычислений, рост объемов информации наряду с ужесточением требований к уровню ее сохранности и непрерывности процесса обработки – всё это обусловило сочетание двух подходов: консолидации информационных ресурсов в составе ЦОДа и структурного резервирования их аппаратно-программных комплексов. Повышенный интерес к резервным центрам объясняется, прежде всего, необходимостью обеспечить катастрофоустойчивость ядра ИТ-инфраструктуры организации. Типовое решение этой задачи – территориальное разнесение узлов обработки и хранения данных. Поэтому в целом наиболее эффективным будет резервирование совместно с территориальным разнесением ЦОДов. Это обеспечивает максимальный уровень живучести системы под воздействием как локальных деструктивных факторов (отказы аппаратуры, сбои программного обеспечения, случайные ошибки или злонамеренные действия пользователей), так и внешних угроз (террористический акт, пожар, затопление, авария в сетях энергоснабжения или сетях передачи данных провайдера, другие техногенные катастрофы и стихийные бедствия).

Таким образом, резервный центр, удаленный от основной площадки, обеспечивает не только отказо-, но и катастрофоустойчивость, определяющую максимальный уровень живучести ядра информационно-телекоммуникационной системы (ИТКС) и, следовательно, минимальный риск остановки бизнес-процессов организации.

DEPO computers

# МЫ ИХ СДЕЛАЛИ! ДЛЯ УСПЕХА ВАШЕГО БИЗНЕСА!

Реклама. Товар сертифицирован.

## DEPO Storm 3300P1 – сервер для центров обработки данных

Классический одноюнитовый **сервер DEPO Storm 3300P1** с гибкими возможностями масштабирования – это высокотехнологичное решение для центров обработки данных, сбалансированное по параметрам производительности, энергопотребления и тепловыделения.

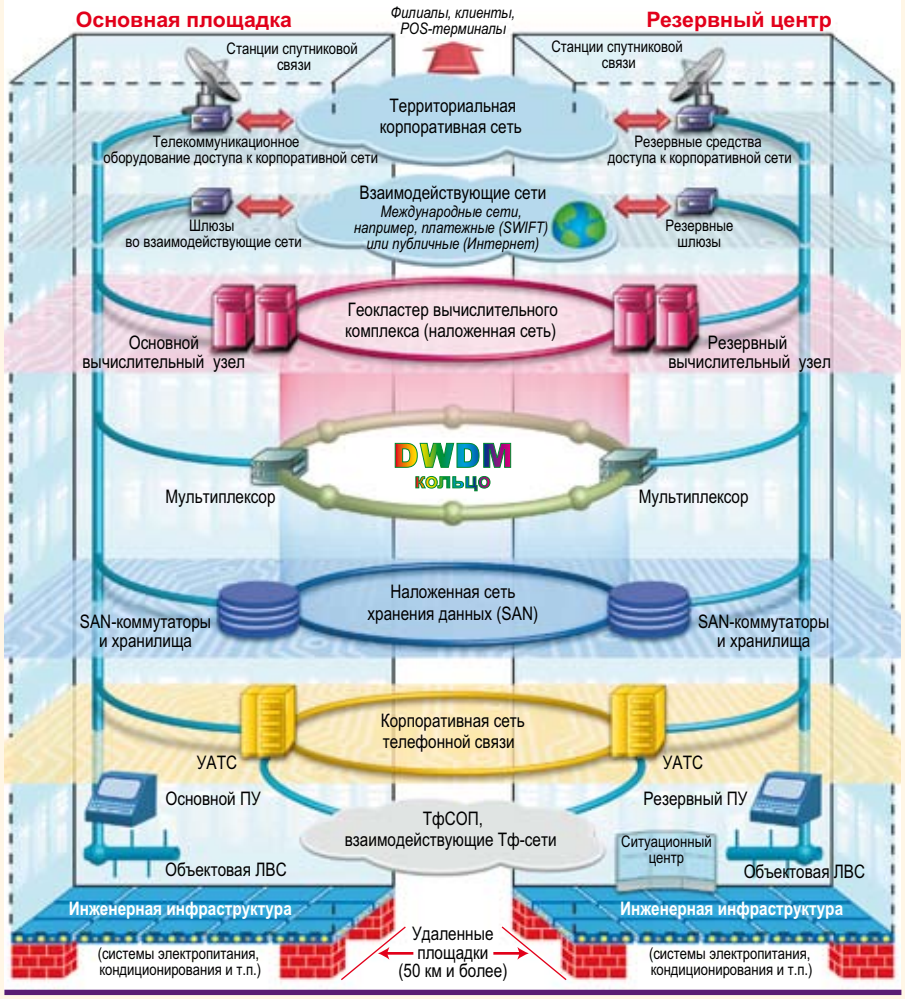
**DEPO Storm 3300P1** используется в комплексных IT-решениях DEPO для создания ферм виртуализации серверов с высокой производительностью и отказоустойчивостью и при этом занимающих минимальный объем в стойке.

**от 78 000 руб.**

- 1 или 2 процессора Intel® Xeon® 5500/5600 серии
- До 96 Гб оперативной памяти DDR3 1333/1066/800MHz ECC
- До 4 жестких дисков SAS емкостью до 600ГБ или SATA емкостью до 2ТБ с «горячей» заменой
- Слоты расширения 2xPCI-E x8
- Модуль удаленного управления IPMI 2.0 с поддержкой KVM o LAN
- Блок питания 650 Вт с «горячей» заменой
- Форм-фактор 1U, набор для монтажа в стойку в комплекте
- Гарантийные планы от 3 до 5 лет с возможностью обслуживания на месте эксплуатации

**Компания DEPO Computers**
**комплексные IT-решения • системная интеграция • компьютерные системы**
**тел. (495) 969-22-22, www.depocomputers.ru**

Типовая структура основного и резервного дата-центров




Обеспечение катастрофоустойчивой конфигурации ИТКС организации (ведомства) – весьма непростая и затратная задача, поэтому такие конфигурации имеют смысл лишь для ответственных применений. Широкое распространение резервные центры получили в банковском секторе, где бизнес, включая вопросы репутации, находится в прямой зависимости от доступности информационной системы. В данном случае высокая цена простоя платежных систем способна оправдать строительство резервного центра.

Обычно серьезные проблемы в банковских ИТ-системах тщательно скрывают, поскольку они могут отразиться на лояльности клиентов и престиже банка в целом. Поэтому примеры зависимости эффективной работы финансовых учреждений от качества функционирования ИТ-систем приходится брать из практики крупнейших зарубежных бирж, где факты простоев в результате остановки информационных систем широко известны. В апреле 2000 г. в течение восьми часов (почти всю торговую сессию) были парализованы торги на Лондонской фондовой бирже (LSE) из-за ошибок в работе программного обеспечения. Заметим, что на бирже эксплуатировались наиболее надежные FT-системы того времени с коэффициентом готовности свыше 99,999%. Убытки составили несколько миллионов фунтов. В сентябре 2008 г. снова на LSE был зафиксирован сбой, повлекший за собой остановку ее работы на четыре часа. Кроме прямых потерь – а около 40% дохода биржи приходится на продажу информации о курсах акций в режиме реального времени, – сбои на LSE сыграли на руку ее конкурентам. Известны случаи крупных аварий, в результате которых были остановлены критически важные сервисы, на других торговых площадках, включая Токийскую фондовую биржу и NASDAQ.

В нашей стране резервные центры имеют Банк России, Альфа-Банк, Банк ВЕФК, Московский кредитный банк, подразделения Сбербанка и другие банки. Резервные центры широко распространены в Министерстве обороны и других силовых ведомствах; например, крупный резервный ЦОД внедряется в интересах пограничной службы для обработки данных биометрических загранпаспортов граждан России.

## Структура основного и резервного центров

Чтобы создать системы, толерантные к серьезным авариям и катастрофам, используют территориальное разнесение вычислительных платформ и информационных хранилищ, организуя кампусные, метро- и континентальные кластеры. Для катастрофоустойчивых геокластеров разнесение узлов, как правило, составляет не менее 50 км. На рисунке представлена типовая структура основного и резервного центров, основанная на геокластерах. В ней выделены три основных элемента обеспечения катастрофоустойчивости:

- протяженная скоростная магистраль, соединяющая обе площадки (в данном случае в виде DWDM-кольца);
- вычислительный геокластер (с узлами кластера на основной и резервной площадках);
- геокластер систем хранения (Storage Area Network, SAN).

Чтобы обеспечить непрерывность вычислений, резервный центр обычно работает в режиме горячего резервирования. При этом подразумевается, что резервный узел всегда имеет актуальную информацию (путем репликации информации с основного узла) и готов незамедлительно переключиться на обслуживание задач.

Структура и элементы дата-центра на рисунке даны обобщенно, для каждого вертикального рынка можно подставить свои конкретные элементы. Например, для банковского сектора «шлюз в другие сети» может означать шлюз в международную сеть SWIFT.

Кроме ядра резервного центра – резервного ЦОДа, который обеспечивает основные операции автоматического обнаружения отказов, переконфигурирования системы для снятия нагрузки с неисправных комплексов и переключения ее на резервные, – важную роль играют и другие подсистемы. Даже в штатном режиме требуется постоянный детальный мониторинг всех систем (который обычно ведут системы управления телекоммуникационным оборудованием и вычислительными комплексами), например, в целях анализа сетей или вычислительных процессов для их оптимизации и прогнозирования нештатных ситуаций. Кроме того, при эскалации проблем необходим переход на автоматизированное или ручное управление; при этом требуется знание предаварийной обстановки и возможных сценариев устранения проблем. Заранее должны быть решены организационные задачи, предусматривающие ряд оперативных мероприятий для обнаружения и нейтрализации нештатных ситуаций, включая разработку аварийного плана действий (disaster recovery plan), в том числе для переключения информационных сервисов и восстановления работоспособности основного узла. Следует иметь в виду, что даже самая надежная вычислительная платформа, например, класса Permanent Availability, не сможет функционировать при отказе инженерной инфраструктуры, включая системы энергоснабжения и кондиционирования, а также системы их мониторинга и управления ими.

В задачи системы эксплуатации резервного центра входит контроль и поддержка работоспособности аппаратно-программных средств центра в зависимости от наличия нештатной ситуации или степени ее опасности. Для системы эксплуатации можно предусмотреть переменный количественный состав, который легко оперативно нарастить из штатного состава служб эксплуатации основной площадки.

При возникновении чрезвычайных ситуаций или длительного восстановления основной площадки может оказаться недостаточно переключения на аппаратно-программные резервные элементы. Для обеспечения непрерывного управления ИТ-системой организации, поддержания ее штатной функциональности силами резервного центра предусматривают заблаговременно подготовленные рабочие места для руководства и технического персонала, а также других структурных подразделений. Степень развертывания этих элементов увеличивается по мере эскалации проблем и деградации элементов основной площадки. Учитывая особенность работы резервного центра, целесообразно включать в его состав элементы, способствующие более эффективному решению управленческих задач в сложной обстановке и в условиях дефицита времени. Одним из таких элементов является ситуационный центр. Он позволяет повысить качество принимаемых решений путем визуализации информационного потока, а также результатов анализа, моделирования и прогнозирования развития нештатных ситуаций.

Развертывание перечисленных выше подсистем, на первый взгляд, может показаться излишним даже для крупного банка. Однако энергетический коллапс в Москве в мае 2005 г. показал уровень толерантности эксплуатируемых систем. Торги на биржах были остановлены, многие банки вынуждены были прекратить работу части офисов и филиалов. Некоторые даже выступили с официальным обращением к гражданам о «возможных временных затруднениях в обслуживании клиентов банка».

Учитывая, что сегодня банковские системы, как правило, ведут централизованную обработку платежной и другой информации, даже наличие автономных источников электроэнергии на основной площадке не гарантирует им связь с внешними объектами (филиалами, клиентами, другими платежными сетями). Нет гарантий работоспособности всей цепочки операторов связи в проблемном регионе. Кроме того, работа руководства и структурных подразделений организации на основной площадке в таких условиях будет затруднена дефицитом энергии из-за повышенного энергопотребления резервных источников. От способности безболезненно переносить подобные коллапсы и любые другие катаклизмы зависит, например, финансовая устойчивость и престиж банка. Поэтому все более широкое применение находят резервные центры, позволяющие нивелировать последствия не только технических аварий и ошибок обслуживающего персонала, но и крупных пожаров, обрушения зданий, заражения опасными программными вирусами, террористических актов (и ложных сообщений о них) и прочих чрезвычайных ситуаций. ИКС

# FFC: вся полнота фрикулинга

**Доля российских ЦОДов в общем энергопотреблении страны пока составляет менее одного процента, но и это дается владельцам дата-центров весьма недешево, причем в обозримом будущем ситуация не улучшится. Единственный выход – повысить КПД использования тех мощностей, которые есть, а значит, взяться за снижение PUE**

В общем энергопотреблении инженерного оборудования ЦОДа на долю системы охлаждения приходится более 70%, поэтому повышение ее энергоэффективности может сильно повлиять на PUE дата-центра. Но максимум энергоэффективности достигается тогда, когда серверы охлаждаются внешним природным источником холода, например, уличным воздухом. Стандартный диапазон рабочих температур для типовых далеко не новых серверов составляет +20–25°C, а температура воздуха в Москве по статистике превышает +23°C не более 400 часов в году. Иными словами, более 95% времени в наших дата-центрах можно использовать свободное охлаждение, или фрикулинг (freecooling).

## К полному фрикулингу

Производители систем кондиционирования уже несколько лет предлагают чиллеры с поддержкой функции свободного охлаждения, но они существенно дороже обычных. Гораздо более перспективными с экономической точки зрения представляются системы на базе роторных регенераторов. В компании Ayaks Engineering разработана система полного фрикулинга FullFreeCooling (FFC), работающая на этом принципе. Она уже прошла испытания и сейчас подключена к реальной нагрузке одного из наших заказчиков, обслуживая три серверные стойки общей мощностью 35 кВт. Правда, фрикулинг в ней не совсем полный, поскольку в установке все-таки присутствует чиллер, но включается он лишь тогда, когда уличная температура воздуха превышает 23°C. Следующий этап тестирования предполагает подачу на вход серверов воздуха с температурой 27°C, как разрешает последний стандарт ASHRAE и производители серверов, т.е. чиллер будет включаться, только если температура воздуха на улице поднимется выше 25°C.

Система состоит из двух разомкнутых контуров, наружного и внутреннего. Наружный имеет выход в атмосферу, а внутренний замкнут на серверное помещение дата-центра. Теплообмен между контурами происходит в роторном регенераторе -- основном компоненте системы FFC. Регенератор понижает температуру воздуха в серверном помещении ЦОДа с +37 до +24°C при температуре воздуха на улице от –40 до +23°C, т.е. 95% времени в году. При температурах выше +23°C подключается чиллер, установленный во внутреннем контуре системы. Причем на 100%-ную загрузку он выводится лишь при температуре +35°C.

Данные, позволяющие сравнить энергетическую эффективность (коэффициент COP*) системы FFC, обычных DX-систем охлаждения и чиллеров с динамическим фрикулингом, представлены в табл. 1. Видно, что система FFC по своему КПД уверенно обходит конкурентов при температурах до +25°C, т.е. 98% времени в году. Но и в оставшиеся 2% времени (одну неделю в году) отставание невелико; результирующий коэффициент COP составляет 7,3, а среднегодовой PUE равен 1,14 (правда, эти цифры отражают только энергопотребление системы холодоснабжения и ИТ-оборудования без учета потребления ИБП и других инженерных систем).

**Таблица 1. Энергоэффективность систем охлаждения разных типов**

| Параметр | Температурный диапазон (времени в году) | | | |
|---|---|---|---|---|
| | -30….0°C (40%) | 0…+15°C (42%) | +15…+25°C (16%) | +25…+35°C (2%) |
| **Прямое расширение DX. EC вентиляторы** | | | | |
| Номинальное потребление системы (+35°C), кВт | 489 | | | |
| Среднее потребление системы в период, кВт | 403 | 403 | 416 | 456 |
| COP, средний за период, кВт/кВт | 2,48 | 2,48 | 2,40 | 2,19 |
| COP, средний за год, кВт/кВт | **2,5** | | | |
| **Чиллерная система. Dynamic freecooling** | | | | |
| Номинальное потребление системы (+35°C), кВт | 581 | | | |
| Среднее потребление системы в период, кВт | 153 | 308 | 415 | 468 |
| COP, средний за период, кВт/кВт | 6,5 | 3,2 | 2,4 | 2,1 |
| COP, средний за год, кВт/кВт | **4,4** | | | |
| **Система FFC. Роторный регенератор** | | | | |
| Номинальное потребление системы (+35°C), кВт | 604 | | | |
| Среднее потребление системы в период, кВт | 122 | 127 | 233 | 415 |
| COP, средний за период, кВт/кВт | 8,2 | 7,9 | 4,3 | 2,4 |
| COP, средний за год, кВт/кВт | **7,3** | | | |

## Зарезервировано всё

Особо отметим, что устанавливать в дата-центре вторую резервную систему FCC нет никакой необходимости, поскольку все ее элементы, способные выйти из строя, и так зарезервированы: по два вентилятора в наружном и внутреннем контурах, два двигателя мощностью 2 кВт для вращения ротора. Такие вентиляторы и двигатели имеются на складах всех российских компаний, специализирующихся на климатическом оборудовании, и для их замены не требуется квалифицированный инженер. В алгоритме работы системы предусмотрены все варианты аварийных ситуаций. При выходе из строя вентилятора наружного или внутреннего контура задействуется резервный вентилятор. Если из строя выйдут оба вентилятора наружного контура или ротор, то включается чиллерное охлаждение. Если ломаются оба вентилятора внутреннего контура, внешний воздух направляется в обход ротора непосредственно в серверное помещение. Конечно, это будет аварийный ре-

* COP – коэффициент холодопроизводительности, показывающий соотношение производимого явного холода (в кВт) к потребленной системой охлаждения электроэнергии (в кВт).

жим работы, но система может функционировать в таком режиме достаточно времени, чтобы провести практически любой ремонт.

Систему FFC можно разместить внутри здания ЦОДа или в специальных конструкциях, пристроенных к зданию. Предусмотрен и вариант ее реализации в виде моноблока уличного исполнения. Охлажденный воздух подается в серверное помещение по воздуховодам, поэтому система FFC и серверное помещение должны располагаться в непосредственной близости друг от друга. Горячие и холодные зоны в серверном зале изолируются с помощью фальшпотолка, а находящийся в горячих зонах нагретый воздух удаляется через вытяжные воздуховоды.

Например, наша тестовая установка в виде моноблока смонтирована на крыше дата-центра непосредственно над серверным залом. Размеры моноблока для охлаждения нагрузки мощностью 35 кВт составляют 7,0x1,8x2,5 м, при этом используется ротор диаметром 1,5 м. Для нагрузки мощностью 500 кВт (это максимальная холодопроизводительность единичного модуля FFC) понадобится ротор диаметром 6 м, а общие размеры моноблока составят 12,0x7,7x7,5 м. Для ЦОДа с подводимой мощностью 1 МВт (28 стоек по 35 кВт каждая) нужно будет установить два ротора диаметром 6 м, и при внутреннем размещении системы FFC общая площадь дата-центра вместе с помещениями для коммутационного оборудования, электрощитовой, ИБП и газового пожаротушения составит около 600 м$^2$.



## Счёт деньгам

На примере того же самого ЦОДа с подводимой мощностью 1 МВт можно сравнить экономическую эффективность работы систем FFC, DX и чиллерной системы с фрикулингом (табл. 2).

**Таблица 2. Экономическая эффективность работы систем охлаждения разных типов (ЦОД мощностью 1 МВт, 2 года эксплуатации, цена электроэнергии – 3 руб./кВт·ч)**

| Параметр | Система DX | Чиллерная система с фрикулингом | Система FFC |
|---|---|---|---|
| Установленная мощность системы холодоснабжения, кВт | 479 | 546 | 396 |
| Мощность системы холодоснабжения, нуждающейся в бесперебойном электропитании (ИБП), кВт | 479 | 154 | 102 |
| Среднегодовой коэффициент холодопроизводительности (COP) | 2,46 | 4,36 | 7,3 |
| Среднегодовой коэффициент энергоэффективности (PUE) | 1,47 | 1,34 | 1,14 |
| Стоимость системы, руб. | 24 118 692 | 34 040 994 | 34 528 533 |
| Стоимость электроэнергии, потребленной системой холодоснабжения за год, руб. | 10 '671 923 | 7 414 333 | 3 850 846 |
| Общая стоимость владения за 2 года эксплуатации, руб. | 45 462 538 | 48 869 660 | 42 230 225 |

По потреблению электроэнергии система FFC оказывается самой экономной: на 30% по сравнению с чиллерной системой с фрикулингом и на 64% по сравнению с DX-системой. Экономия достигается за счет того, что чиллер работает всего 4% времени в году. Причем чиллер годится самый дешевый, без функции фрикулинга, и тогда цена всей системы FFC будет всего на 10% дороже чиллерной системы с поддержкой фрикулинга. Разница в цене с DX-системой составляет 30%, но за счет более низкого энергопотребления по общей стоимости владения система FFC выходит в лидеры уже через два года эксплуатации.

Эффективность системы можно увеличить еще больше. Во-первых, можно установить в дата-центре серверы, соответствующие новым нормам ASHRAE (температура воздуха на входе от +18 до +27°C). Это означает, что система FFC будет работать в режиме фрикулинга при уличной температуре до 25°C, а чиллер нужно будет включать лишь на 190 ч в год. Во-вторых, в наружном контуре можно установить камеру адиабатного охлаждения, которая охлаждает воздух, поступающий на ротор, от 2 до 5°C. В результате можно будет работать без чиллеров до температуры на улице +29°C, а более высокая температура в средней полосе по статистике наблюдается лишь 40 ч в году.

Одним из главных достоинств системы FFC является то, что подаваемый ею воздух заполняет все пространство ЦОДа, создавая избыточное давление. Благодаря этому температура в любой точке дата-центра практически любой конфигурации составляет +24°C. Таким образом, стойки разной мощности (от 1 до 40 кВт) можно ставить рядом друг с другом, установленное в них оборудование будет без индивидуальной разводки получать столько воздуха, сколько необходимо для поддержания заданной температуры на входе серверов. А высокий уровень отказоустойчивости и резервирования системы FFC позволяет создавать решения, удовлетворяющие требованиям к надежности, близким к уровню Tier 4. Мы провели консультации со специалистами Uptime Institute и получили заверения в том, что данная организация готова сертифицировать дата-центры, оснащенные нашей системой.

Да, система FFC имеет достаточно большие габариты, но благодаря ей можно увеличить плотность установки нагруженных стоек и решать те же самые вычислительные задачи меньшим количеством стоек. Кроме того, в дата-центре с системой FFC не нужно ставить шкафные кондиционеры, и за счет этого площадь серверного помещения тоже уменьшается. Еще одно направление экономии – сокращение потребления мощности городских электросетей, поскольку питание чиллеров, используемых максимум 5% времени в году, можно обеспечить от дизель-генератора.

Таким образом, в дата-центре, оборудованном системой FFC, можно добиться низких значений показателя PUE, не используя дорогого энергосберегающего оборудования.

# СКС-головоломка, или Российский стандарт тестирования кабельных линий

**С 1 января 2010 г. вступил в действие так необходимый российским специалистам по СКС документ – ГОСТ Р 53245-2008, в котором определены методы тестирования и сертификации кабельных линий. Однако из-за неточностей в стандарте и методических ошибок, допущенных разработчиками, пользоваться им затруднительно как заказчику СКС, так и исполнителю монтажных работ.**

**Дмитрий МАЦКЕВИЧ,**
эксперт в области СКС и ЦОД,
руководитель Интернет-проектов http://ockc.ru, http://dcnt.ru

По оценке экспертов, большая часть проблем в информационных системах вызвана неполадками в кабельных системах. Проблем, которые возникают из-за нарушения правил монтажа или выбора некачественных пассивных элементов для телекоммуникационной инфраструктуры, можно избежать, если на этапе сдачи-приемки работ провести тестирование смонтированных кабельных линий и сертифицировать структурированную кабельную систему (СКС).

Существует несколько методик проверки качества смонтированных медных кабельных линий. Можно проводить тестовые испытания по модели «канал» (channel) или по модели «постоянная линия» (permanent link); можно проверить параметры кабельной линии на соответствие требованиям конкретного приложения (например, 1000Base-T) либо требованиям категории (к примеру, категории 5e) или определенного класса (например, класса D). В случае тестирования волоконно-оптического кабельного сегмента разные методы тестирования кабельных линий могут дать разные результаты, а следовательно, будут сделаны разные выводы о соответствии либо несоответствии тестируемой кабельной линии требованиям стандарта. Существует также несколько стандартов, где описаны технические параметры кабельных линий и методики тестирования, которые могут отличаться друг от друга.

Перед исполнителем работ встает непростой вопрос: на что опираться при проведении испытаний кабельных линий на объекте, чтобы четко определить качество кабельной линии? Перед заказчиком, в свою очередь, встает вопрос о том, можно ли принять результаты работы. Поэтому как заказчику СКС, так и исполнителю монтажных работ необходима единая «точка отсчета», которую можно взять за основу при проведении тестовых испытаний на объекте и последующей сертификации кабельной системы. Иными словами, нужен базовый документ, описывающий методы испытаний и параметры тестирования кабельных линий, опираясь на который можно точно сказать, что протестированная кабельная линия отвечает требованиям данного документа.

## Точка отсчета – стандарт ГОСТ Р 53245-2008?

Существует много базовых документов для тестирования кабельных линий с описанием моделей и конфигурации тестирования, технических параметров и методики проведения испытаний на объекте. Есть международные стандарты серии ISO/IEC и американские стандарты TIA/EIA. Но эти стандарты написаны на английском языке и не всем доступны, поэтому и не получили широкого распространения в России. До 2010 г. в нашей стране не было национального стандарта, описывающего модели тестирования кабельных линий, технические параметры, которые необходимо измерять, методику тестирования и сертификацию кабельных линий в СКС.

Теперь базовый документ для тестирования и сертификации кабельных линий, входящих в состав СКС, появился и у нас. С 1 января 2010 г. введен в действие новый российский стандарт ГОСТ Р 53245-2008 «Информационные технологии. Структурированные кабельные системы. Монтаж основных узлов системы. Методы испытания». Этот стандарт вышел вместе с еще одним новым российским стандартом на СКС – ГОСТ Р 53246-2008 «Информационные технологии. Структурированные кабельные системы. Проектирование основных узлов системы. Общие требования». Про ГОСТ Р 53246-2008 в прессе и в Интернете сказано уже немало, а вот по ГОСТ Р 53245-2008 дискуссий нет. Объясняется это тем, что обсуждение вопросов тестирования и сертификации кабельных линий требует определенного уровня компетенции.

Мы рассмотрим некоторые положения стандарта, которые вызывают неоднозначные трактовки и требуют доработки. В статье сохранены термины, которыми пользовались разработчики стандартов ГОСТ Р 53245-2008 и ГОСТ Р 53246-2008.

## Область действия и цель

Область действия стандарта ГОСТ Р 53245-2008 ограничена структурированной кабельной системой. Иными словами, приведена методика испытаний для кабельных линий, входящих в состав СКС.

Заявленная цель стандарта – дать нормативную базу для безопасного и эффективного ввода и эксплуата-

ции СКС в помещениях пользователя. Цель заявлена достойная, но достичь ее разработчикам стандарта, к сожалению, не удалось.

## Нарушение принципов разработки

Стандарт ГОСТ Р 53245-2008 был разработан ООО «Стандартпроект». При его подготовке были нарушены основные принципы разработки российских стандартов, соблюдение которых обязательно. ГОСТ Р 1.2004 «Стандартизация в РФ. Основные положения» устанавливает следующее: национальные стандарты должны быть разработаны на основе международных стандартов, а также при достижении консенсуса всех заинтересованных сторон и установлении требований с учетом достижений в области техники и технологий.

При разработке данного стандарта обошлись без обсуждений и привлечения отраслевых специалистов и экспертов; тексты стандартов не были даже разосланы производителям СКС, которые присутствуют на российском рынке. Отраслевые специалисты и эксперты о выпуске стандарта узнали после его публикации, т. е. были поставлены перед фактом. Поэтому не имеет смысла говорить о каком-либо консенсусе заинтересованных сторон.

Еще в начале 2008 г. стало известно о новых достижениях в отрасли СКС. В феврале 2008 г. американские специалисты приняли 10-е дополнение TIA/EIA-568-B.1-10, в котором была введена новая категория 6A. В международный стандарт ISO/IEC 11801-2002 в апреле 2008 г. была включена поправка 1 с описанием требований к новым классам Class EA и Class FA. В международном стандарте для градации кабельных линий вместо понятия «категория» используется «класс». Стандарт ГОСТ Р 53245-2008 был утвержден и введен в действие только в конце 2008 г., а значит, было как минимум полгода, чтобы отразить в ГОСТ Р 53245-2008 требования к новой категории 6A. Однако разработчики российского стандарта проигнорировали отраслевые достижения.

За основу разработки национального стандарта был взят не международный стандарт и даже не американский TIA/EIA-568-B.1, а руководство некоей американской компании. Был сделан аутентичный перевод этого руководства, о чем прямо сообщается в тексте российского стандарта. Очень сильный ход «разработчиков», не правда ли?

Кстати, вполне может быть, что это хорошее руководство для инсталляторов СКС, поскольку в подобных внутренних документах вполне допустимы разночтения, использование своей уникальной терминологии. Но все это категорически недопустимо в таком документе, как национальный стандарт.

Мы не будем здесь останавливаться на терминологии, которую достаточно вольно используют переводчики американского руководства, а сразу перейдем к рассмотрению некоторых пунктов стандарта.

## Испытание кабельной системы на основе витой пары

В СКС устанавливаются и монтируются в основном кабельные линии на основе витой пары, и естественно, что в стандарте испытаниям витой пары уделено большое внимание. В ГОСТ Р 53245-2008 (раздел 3.1) приводится методика испытаний, *«...касающаяся измерительного оборудования, конфигураций тестирования, методов тестирования и предельных допустимых значений рабочих характеристик передачи структурированных кабельных систем».*

### Конфигурация тестирования – модели «канал» и «постоянная линия»

Стандартом ГОСТ Р 53245-2008 (пункт 3.1.2.1) разрешены следующие модели тестирования кабельных линий на основе витой пары – «канал» и «постоянная линия». В текстовом описании состава «канала» горизонтальной подсистемы в стандарт не включены аппаратные и коммутационные шнуры. При описании состава «канала» магистральной подсистемы в стандарт не включены коммутационные шнуры. Для тех читателей, которые не слишком близко знакомы с моделями тестирования, заметим, что в модель «канал» шнуры должны входить обязательно.

В начале пункта 3.1.2.1 стандарт сообщает, что при проведении полевых испытаний можно использовать одну из двух моделей тестирования («канал» или «постоянную линию»). Как будто все в порядке. Однако затем в этом же пункте идет следующее требование: «...все модели канала горизонтальной и магистральной подсистем на основе витой пары проводников с суммарной длиной кабелей, не превышающей 100 м, включая коммутационные и аппаратные шнуры, должны пройти полевое тестирование». К чему приводит такая формулировка? На основании данного положения стандарта, после того как исполнитель работ выполнит тесты по модели «постоянной линии», заказчик может потребовать от него еще и измерений по модели «канал», сообщив исполнителю, что в его СКС есть «каналы», не превышающие 100 м. А это будут все кабельные линии от розетки до кроссовых и коммутационных панелей. О ужас, подумает инсталлятор, придется снова выполнять тестирования всех витопарных кабельных линий! Не спешите огорчаться: исполнитель работ может отказаться это делать, сообщив заказчику, что он не в состоянии выполнить тестирование по модели «канал», так как согласно ГОСТ Р 53245-2008 (пункт 3.1.2.1) аппаратные шнуры в горизонтальном кроссе не входят в модель тестирования «канал».

С моделью «постоянная линия» для кабельных линий на основе витой пары в стандарте почти все в порядке, кроме, пожалуй, одного момента. Российский стандарт требует тестирования только горизонтальных и магистральных кабельных линий СКС, длина которых не превышает 90 м. С требованием к кабельным линиям в горизонтальной подсистеме можно согласиться. Действительно, длина горизонтальной кабельной линии от розетки до коммутационного устройства не может превышать 90 м. Но в магистрали длина кабельных линий может быть и большей. А если длина магистральной кабельной линии будет больше 90 м, то получается, что согласно ГОСТ Р 53245-2008 такую кабельную линию вообще не надо тестировать, и даже не потребуется про-

верка схемы соединения витых пар и проверка непрерывности экрана для экранированных систем.

Необходимо включить в положение стандарта проверку схем соединения и непрерывности экрана для экранированных кабельных линий в магистрали при превышении длины кабельной линии 90 м.

### Параметры тестирования

Стандартом ГОСТ Р 53245-2008 (пункт 3.1.3) определены параметры тестирования витой пары. Это практически стандартный набор, который описан в американском стандарте TIA/EIA-568-B.1 (пункт 11.2.4). Но в нашем национальном стандарте есть и нюансы.

**Измерение длины кабельной линии на основе витой пары.** Разработчики ГОСТ Р 53245-2008 (пункт 3.1.3.3) решили помочь инсталляторам повысить эффективность ввода СКС в эксплуатацию. Помните одну из целей стандарта? Читайте внимательно уникальное положение ГОСТ Р 53245-2008: *«При проведении сертификации СКС длина каналов и постоянных линий должна определяться только на основании физической длины оболочек кабелей, в них входящих. Тестирование длины кабельных сегментов с помощью полевого тестера служит исключительно для выявления ошибок монтажа и гарантии того, что время прохождения сигнала укладывается в допустимые временные пределы. Тестирование электрической длины кабеля не может заменить собой измерение его физической длины».*

Подобных положений нет ни в американском, ни в международном стандарте. Чего же требует формулировка разработчиков? Ответ: измерять физическую длину кабельных линий без использования приборов. Игорь Панов, региональный менеджер компании Fluke Networks, прочитав это положение стандарта, предложил ко всем поставляемым в Россию кабельным тестерам добавлять еще и линейки для измерения физической длины.

Требовать от инсталляторов при сертификации СКС измерения физической длины – это явно перебор... На такую работу потребуется дополнительное время, а значит, говорить об эффективности уже не придется.

Чем же руководствовались разработчики стандарта, вводя такое требование? Для оценки и расчета электрической длины кабеля используется параметр NVP (номинальная скорость распространения) – отношение скорости распространения сигнала в среде к скорости света в вакууме. Этот параметр может сильно варьировать от одной партии кабеля к другой и даже в пределах одной партии. Именно поэтому в американском стандарте допускается погрешность до 10% при оценке длины кабельной линии при помощи полевого тестера. Но американский стандарт TIA/EIA-568.B.1 не запрещает использовать кабельный тестер для измерения и оценки длины кабельной линии. А в международном стандарте параметр длины вообще носит информативный характер.

Пункт стандарта об измерении физической длины кабеля необходимо изменить.

**Вносимые потери, переходные затухания, возвратные потери.** В ГОСТ Р 53245-2008 (пункт 3.1.3.4) приведены формулы для определения вносимых потерь (insertion loss) по моделям «канал» и «постоянная линия» с предельными значениями по количеству коннекторов (соединителей).

По приведенным в стандарте формулам невозможно рассчитать, каким должно быть предельное значение вносимых потерь на какой частоте, поскольку в документе нет никаких дополнительных формул для расчета вносимых потерь в кабеле и в коннекторах (соединителях) в зависимости от частоты. Дана только таблица с предельными вносимыми потерями на нескольких дискретных частотах. Правильно оценить параметры кабельной линии по вносимым потерям согласно приведенной общей формуле, которая «повисла в воздухе», или по табличным данным во всем диапазоне частот просто невозможно. Следовательно, нет возможности оценить качество кабельной линии по вносимым потерям.

Как могло такое произойти? Российский стандарт – это аутентичный перевод руководства, разработанного американской компанией, а вовсе не американского стандарта, который на самом деле состоит из нескольких документов. В российский стандарт попала общая формула и табличные данные по вносимым потерям только из стандарта TIA/EIA-568-B.1, а сами значения вносимых потерь на кабель и соединители в зависимости от частоты приведены в другом документе – TIA/EIA-568-B.2. Понятно, что переводившие американское руководство «разработчики» российского стандарта такие нюансы знать не могут, поэтому в ГОСТ Р и приведена формула, по которой невозможно рассчитать характеристики кабельной линии для заданной категории. А при проведении тестовых испытаний на категорию или класс кабельная линия должна пройти тестирование во всем спектре частот от 1 МГц с заданным частотным шагом до верхней границы категории или класса (см. таблицу). Кстати, в ГОСТ Р 53245-2008 (пункт 3.1.5.3) требуется составление отчета от полевого тестера по всем измеренным параметрам во всем диапазоне частот.

| | Частота и шаг тестирования |
|---|---|
| Частота тестирования, МГц | Шаг частоты, кГц |
| от 1 до 31,25 | 150 |
| от 31,25 до 100 | 250 |
| от 100 до 250 | 500 |
| от 250 до 500 | 500 |

То же самое произошло и с другими параметрами, зависящими от частоты, в частности, с переходным затуханием на ближнем конце (NEXT) или возвратными потерями (RL).

**Приборы для сертификации высокого класса.** ГОСТ Р 53245-2008 (пункт 3.1.4.6) разрешает для сертификации СКС использовать полевые тестеры только двух классов: IIe и III. Так что если вы вдруг приобрели полевые приборы классом выше, более качественные и точные, то протестировать кабельные линии вы, конечно, можете, но для сертификации кабельных линий они не годятся – слишком уж высока точность.

**Параметры для категорий 3 и 5.** В российском стандарте на СКС ГОСТ Р 53246-2008 (пункт 6.8.1) раз-

решается в магистрали применять многопарные кабели витая пара категории 3 и категории 5. Однако никаких технических параметров для данных категорий в стандарте ГОСТ Р 53245-2008 не определено. Очевидно, по мнению разработчиков российского стандарта, магистральные кабельные линии не надо тестировать Заказчику придется поверить на слово, что они будут удовлетворять заданной категории.

## Испытание волоконно-оптической кабельной системы

В связи с уменьшением максимально допустимых вносимых потерь в канале для высокоскоростных приложений (от 1 Гбит/с) становится очень актуальным вопрос выбора правильной методики тестирования волоконно-оптической кабельной линии. Существует несколько методик, наиболее полно описанных в международном стандарте ISO/IEC 14763-3 (утвержден еще в 2006 г.). В российском стандарте описана единственная методика – метод одной перемычки, который приведен в TIA/EIA-568-B.1 (пункт 11.3) и используется только для тестирования кабельной линии по модели «постоянная линия».

### Конфигурация тестирования

В российском стандарте приведена только одна модель тестирования волоконно-оптической кабельной линии – «постоянная линия», модель «канал» в него не включена. В международном же стандарте описана модель тестирования «канал», причем эта модель может потребоваться заказчику на реальном объекте, чтобы удостовериться в том, что «канал» будет отвечать требованиям высокоскоростных приложений к качеству волоконно-оптической кабельной линии.

### Метод одной эталонной перемычки

Не может не вызвать улыбку фраза из ГОСТ Р 53245-2008 (пункт 3.2.3) о популярности использования метода тестирования волоконно-оптической кабельной линии: «Наиболее популярный из них метод одной (двух, трех и т.д.) эталонной перемычки». Так какой из них наиболее популярен – одной, двух или трех перемычек? А может быть, есть методы четырех, пяти перемычек и они тоже популярны?

### Параметры тестирования

Согласно требованиям российского стандарта, необходимо протестировать в полевых условиях два основных параметра оптической кабельной линии: вносимые потери и длину. В международном стандарте ISO 11801 фигурирует еще один очень важный параметр – полярность в парах оптических волокон.

Все стандарты, описывающие правила и требования к проектированию СКС, – и российский ГОСТ Р 53246-2008 не исключение – требуют обязательного соблюдения полярности в парах волокон между двумя коннекторами (соединителями) в кабельной линии. Почему необходимо соблюдать полярность? Предполагается, что для приложения внутри сети будет задействовано не одно волокно, а два: по одному будет происходить передача, а по другому – прием оптического сигнала. Необходимо, чтобы два источника света были соединены с двумя приемниками в каждой паре волокон. Для этого должна соблюдаться полярность.

Поэтому в международном стандарте ISO 11801-2002 среди обязательных параметров есть и такой, как проверка полярности волокон. В российском стандарте этому нюансу, к сожалению, не уделено внимания.

### Направление тестирования и соблюдение полярности в оптике

В стандарте ГОСТ Р 53245-2008 при тестировании горизонтальной и магистральной кабельных линий упоминается о тестировании оптической линии только в одном направлении, т.е. используется тот же подход, что и в стандарте TIA/EIA-568-B.1.

При тестировании волоконно-оптической кабельной линии в магистрали большое значение имеет выбор направления тестирования. Дело в том, что в двух разных направлениях значения вносимых потерь могут оказаться разными, а следовательно, будут сделаны разные заключения о соответствии кабельной линии требованиям стандартов.

В российских методиках, которые применяются при тестировании магистральных оптоволоконных линий, за результат тестирования принимается среднее значение, получаемое при измерениях в одном волокне в двух направлениях. Можно, конечно, возразить, что в СКС нет длинных кабельных линий и вполне достаточно измерить параметр в одном направлении. Однако с этим утверждением нельзя согласиться, и дело здесь не в вычислении среднего значения. Приведем пример построения магистральной линии в СКС с использованием многомодового волокна. При тестировании только в одном направлении кабельная линия будет отвечать требованиям высокоскоростного приложения. А потом в ходе эксплуатации свет будет распространяться в другом направлении – не в том, в котором он распространялся в ходе тестирования, – и вполне возможно, что высокоскоростное приложение не будет работать. В случае высокоскоростных приложений для устойчивой передачи данных может не хватить даже 0,25 дБ. Поэтому в оптической магистрали необходимо проводить измерения в паре волокон в двух направлениях.

### Использование мандрели (модового фильтра)

Пункт 3.2.4.1 ГОСТ Р 53245-2008 описывает использование мандрели (именно этот термин взяли на вооружение разработчики стандарта) в том случае, если вносимые потери на коротких отрезках больше ожидаемого значения. Наш стандарт не сообщает, какую эталонную перемычку – первую или вторую – следует наматывать на поверхность мандрели. Видимо, подразумевается, что читатели стандарта смогут сами догадаться, что первую.

### Тестирование в сети с централизованной оптической архитектурой

Всеми кабельными стандартами, включая и российский стандарт ГОСТ Р 53246-2008, разрешается построение волоконно-оптической кабельной сети с

централизованной архитектурой (в стандарте используется сокращение СОА). Это означает, что разрешается прокладывать оптические кабели от телекоммуникационных розеток до главного кросса (МС) без установки промежуточного кросса (IC) и горизонтального кросса (HC) на расстоянии больше 90 м.

Стандарт ГОСТ Р 53245-2008 (пункт 3.2.4.4) требует, чтобы вносимые потери не превысили 3,3 дБ в кабельной линии без консолидационной точки. Но разработчики не учли того, что в ГОСТ Р 53246-2008 (пункт 5.1.9.2) они разрешили использовать волоконно-оптический кабель с многомодовыми волокнами 50/125 мкм при реализации СОА на расстоянии до 500 м. А значение 3,3 дБ получено исходя из того, что в СОА длина волоконно-оптической кабельной линии не превысит 300 м. Коль скоро разработчики сами же в ГОСТ Р 53246-2008 увеличили максимально допустимую длину в СОА до 500 м, необходимо увеличить и вносимые потери на 0,7 дБ.

### Безопасность

Напомним про одну из заявленных целей российского стандарта – повышение безопасности ввода СКС. Это действительно важный вопрос. Персоналу, выполняющему тестирование, необходимо соблюдать правила техники безопасности, чтобы не нанести ущерб своему здоровью, особенно при тестировании волоконно-оптических кабельных линий. К сожалению, кроме заявления о цели, этому вопросу в национальном стандарте не уделено никакого внимания.

■ ■ ■

Очевидно, что текст стандарта не должен быть кроссвордом для инсталлятора и заказчика. Положения стандарта должны быть четко и ясно изложены, без опечаток и ошибок, текст не должен допускать двусмысленных трактовок.

Стандарт ГОСТ Р 53245-2008 в его сегодняшнем состоянии не рекомендуется использовать при разработке технического задания на установку СКС или технических требований к ней.

Остается только надеяться, что наш национальный стандарт будет переработан с учетом международных стандартов и к его разработке будут привлечены отраслевые специалисты. ИКС

# Перспективные СКС: скорости 40 Гбит/с и выше

**С середины текущего десятилетия начали широко использоваться сетевые интерфейсы, обеспечивающие скорость передачи 10 Гбит/с. Однако за пять лет их возможности были практически исчерпаны. Различные усовершенствования, например технологии Port trunking, дела не меняют. На повестку дня встал вопрос о переходе к следующему поколению сетевой аппаратуры с более высокой номинальной скоростью передачи.**

**Андрей СЕМЕНОВ,**
директор по развитию «АйТи-СКС»

СКС, реализованные на современной элементной базе категории 6а, имеют теоретическую пропускную способность по меньшей мере 18 Гбит/с. Поэтому они прекрасно передают 10-гигабитные потоки, однако не имеют резервов наращивания скорости. Переход на решения категории 7 качественных изменений не дает. Теоретическая пропускная способность этой техники – 55 Гбит/с, что недостаточно для обеспечения нормального функционирования даже 40-гигабитных систем.

Таким образом, наряду с новыми типами активного сетевого оборудования требуется разработать качественно новые СКС. С учетом большого срока службы кабельных систем внедрение техники следующего поколения должно осуществляться опережающими темпами. Активное сетевое оборудование и используемые им кабельные тракты образуют единый комплекс. Поэтому достижимые параметры СКС во многом определяют направления разработки сетевых устройств. В свою очередь, применяемые при создании сетевых устройств конструктивные решения оказывают сильное влияние на технику кабельных систем.

### Круг потребителей СКС следующего поколения

Так же, как и для 10-гигабитных систем (см. «ИКС» № 10'2009, с. 84), для кабельной техники нового поколения фокусной областью применения являются в первую очередь центры обработки данных. Определенные перспективы имеются в магистральных подсистемах крупных СКС офисного назначения; не следует сбрасывать со счетов и крупные промышленные СКС.

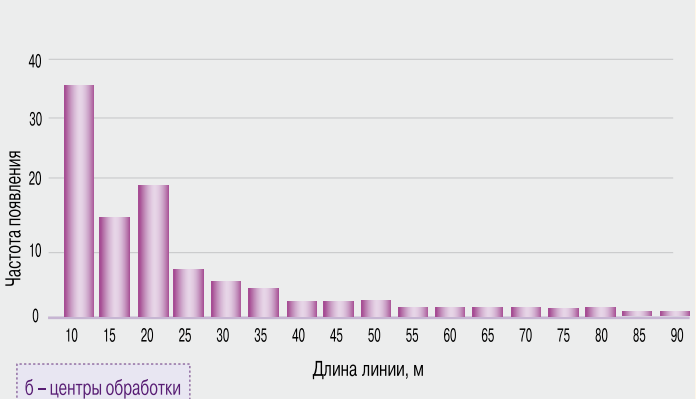
Наиболее реальные кандидаты на роль оборудования следующего поколения – системы Ethernet со скоростью передачи 40 и 100 Гбит/с. Причем эти технологии отнюдь не антагонисты. Предполагается, что 40-гигабитные системы будут применяться для связи между серверами, а 100-гигабитные – для организации магистральных каналов.

Отдельного упоминания как потенциального потребителя ресурсов СКС в ЦОДе заслуживает оборудование Fibre Channel и Infiniband. Эти разновидности сетевых устройств используют другой формат кадра, однако скорости передачи линейного сигнала близки к тем,

*Рис. 1.* Частотное распределение длин стационарных линий


а – подсистемы внутренних магистралей офисных СКС

**Источник:** «АйТи»




б – центры обработки данных

**Источник:** LAN Technologies

которые свойственны Ethernet, хотя традиционно несколько им уступают.

## Ориентация оптической подсистемы на схемы параллельной передачи

Выбор схемы сетевого интерфейса нового поколения во многом определяется тем, что передача 40- и 100-гигабитного информационного потока в одном канале сопряжена с большими техническими сложностями, вызванными слишком высокими частотами модуляции даже при использовании наиболее экономичных по ширине спектра сигналов в формате NRZ в сочетании с многоуровневой схемой кодирования.

Статистика реализованных проектов (рис. 1) свидетельствует о том, что независимо от области применения протяженность примерно 90% линий СКС не превышает 100 м. Поэтому для обеспечения 40- и 100-гигабитной пропускной способности канала связи целесообразно организовывать передачу в нескольких параллельных субканалах. Такой подход дает возможность в разы уменьшить тактовую частоту линейного сигнала.

Параллельная передача – это один из вариантов многоканальной передачи: передатчик каждого из субканалов работает по физически отдельной цепи (пространственное мультиплексирование). В сетях связи общего пользования параллельная передача не имеет перспектив, поскольку при протяженности линии даже в единицы километров ее использование не экономично. В ЛВС, где длина тракта в подавляющем большинстве случаев не превышает нескольких десятков метров, параллельная передача намного популярнее. В частности, она уже более десяти лет массово применяется на уровне межблочного соединения и организации стека коммутаторов.

Значительно лучшие стоимостные характеристики схем параллельной передачи для линий небольшой протяженности обусловлены рядом причин:

- ее использование устраняет необходимость установки на концах линии модулей оптических мультиплексора и демультиплексора, цены на которые остаются высокими даже после радикального снижения последних лет;

- можно не применять сложные линейные коды и во многом обеспечить унификацию 10-гигабитных систем и их более скоростных наследников;
- при построении линии связи можно отказаться от дорогостоящих оптических передатчиков с контролируемой длиной волны и узкой спектральной линией излучения.

Существенным аргументом в пользу выбора схемы параллельной передачи служит возможность применения многомодовых волоконных световодов категории OM3, оптимизированных для работы с лазерными излучателями и имеющих коэффициент широкополосности не хуже 2000 МГц • км на длине волны 850 нм. Несколько лучшие характеристики линии достигаются при использовании новейших волокон категории OM4 (A1a3 по стандарту IEC 60793-2-10) с лазерным коэффициентом широкополосности не хуже 4700 МГц • км. В частности, предельная протяженность тракта увеличивается как минимум до 125 м.

*Рис. 2.* Вилка разъема типа MPO

Параллельная передача производится в четырех или десяти (для 40- и 100-гигабитной системы соответственно) отдельных субканалах со скоростью в 10 Гбит/с в каждом. Приемопередатчики этих субканалов с минимальными схемными изменениями заимствуются из хорошо отработанных в производстве сетевых интерфейсов 10G BaseSR. Для улучшения экономических параметров решения в целом допустимая ширина спектра излучения VCSEL-лазера увеличивается в полтора раза до 0,65 нм.

Создание 40- и 100-гигабитной оптической техники заметно облегчается хорошим техническим заделом. Промышленность еще в конце 90-х гг. прошлого столетия освоила серийное производство ленточных сборок волокон, механических сплайсов и сварочных аппаратов, изначально ориентированных на работу с ленточным волокном, а также групповых разъемных соединителей, позволяющих одновременно коммутировать до нескольких десятков волокон.

Функции групповых разъемных оптических соединителей вполне могут выполнять изделия типа MPO (рис. 2). В последние несколько лет они хорошо зарекомендовали себя как один из обязательных компонентов оптических модульно-кассетных решений. Количество световодов, которые дают возможность одновременно коммутировать серийные варианты этих соединителей, достигает 72. Таким образом, разъем данного типа с заметным запасом удовлетворяет потребности практики.

## Необходимость новых типов оптических кабелей

Освоение нового диапазона скоростей требует создания новых разновидностей кабелей. Существующие распределительные кабели внутренней прокладки для этого мало пригодны, поскольку из-за большого разброса длин отдельных световодов нельзя добиться, чтобы разброс времени задержки (skew) не превышал 0,75 нс/100 м.

Один из путей достижения требуемой величины skew состоит в применении кабелей, конструкция которых обеспечивает жесткий контроль механической длины отдельных волокон. Таковы, например, ленточные световоды. Поскольку реализация 100-гигабитных систем с помощью передачи в 10 отдельных субканалах окончательно утвердилась, возникла необходимость освоить серийное производство 10-волоконных лент (ранее использовались 4-, 6-, 8- и 12-волоконные ленты).

Для 40-гигабитных систем можно использовать так называемые волоконные модули. От модулей кабелей внешней прокладки они отличаются тем, что не позволяют волокнам свободно перемещаться внутри трубки. Внешний диаметр модуля не превышает 0,9 мм, т.е. по параметру компактности (порядка 1 мм$^2$ на волокно) этот элемент практически не уступает ленточному решению. А при прокладке круглый кабель модульного типа оказывается заметно удобнее, чем плоский ленточный.

Ленточные сборки и волоконные модули, изначально предназначенные для параллельной передачи, обеспечивают величину skew не хуже 0,1 нс/100 м, что открывает перспективы увеличения предельной протяженности тракта по крайней мере до 150 м.

## 40 Гбит/с по медножильным трактам

Возможность использования симметричных кабельных трактов протяженностью 100 м на скоростях выше 10 Гбит/с практически подтверждена осенью 2008 г. специалистами Пенсильванского университета (США). В ходе проведенного ими эксперимента была достигнута скорость в 50 Гбит/с при требуемом для коммерческого использования качестве передачи.

Ключевые достоинства медножильного варианта 40-гигабитного сетевого интерфейса следующие:

- меньшая по сравнению с оптическим аналогом стоимость решения при организации широко распространенных именно в ЦОДах (см. рис. 1, б) линий длиной до 30 м;
- удобство формирования линейного сигнала на уровне модуля доступа к физической среде из четырех отдельных 10-гигабитных потоков;
- возможность прямого заимствования многих схем из интерфейса 10 GBaseSR;
- относительная техническая простота создания «медного» варианта сетевого интерфейса, рассчитанного на работу по кабельным трактам категории 7a (класса 7a).

Теоретическая пропускная способность кабельного тракта класса F составляет примерно 55 Гбит/с. В реальных условиях с привлечением простых технических средств она может быть использована примерно на 60%, т.е. фактическое значение очень близко к требуемым 40 Гбит/с.

Приведенные выше оценки пропускной способности делались в предположении, что для формирования тракта применяются компоненты категории 7, которые были

разработаны еще в середине 90-х гг. прошлого столетия. Переход на элементную базу категории 7а с увеличенной до 1000–1200 МГц верхней граничной частотой полосы пропускания и улучшенным параметром NEXT позволяет повысить пропускную способность в несколько раз (по крайней мере, потенциально).

Поскольку в ЦОДах нет необходимости применять линии, реализующие четырехконнекторную модель тракта передачи сигнала, обеспечение требуемого качества передачи несколько упрощается.

Значительная часть спектра субканального линейного сигнала 40-гигабитного интерфейса лежит выше 500 МГц. На столь высоких частотах при длинах линии, близких к предельным, существенно увеличивается затухание, что сопровождается усилением влияния тепловых шумов приемника на качество передачи данных. Поэтому уровень выходной мощности передатчика увеличивается с обычных 0 дБм до примерно +10 дБм. Такой прием позволяет, не меняя защищенность от переходной помехи, свести отрицательный эффект воздействия тепловых шумов до пренебрежимо малых величин.

Отдельно отметим, что техника категории 7 и выше может быть реализована только в полностью экранированном варианте (кабели S/FTP, а также разъемные соединители Tera, GG45 и его вариант ARJ45). При наличии качественного телекоммуникационного заземления такое исполнение эффективно решает проблему межкабельных переходных помех.

## Изменения в стандартах

Освоение диапазона скоростей 40 и 100 Гбит/с требует коррекции стандартов СКС в части, относящейся к оптической подсистеме. Для работы на таких скоростях были созданы и в настоящее время полностью нормированы многомодовые волоконные световоды категории OM4, характеристики которых позволяют заметно повысить эффективность оптических линий. В частности, максимальная протяженность 100-гигабитного многомодового тракта может быть увеличена минимум до 125 м против 100 м при его реализации на световодах категории OM3.

Применение техники параллельной передачи обусловливает необходимость разработки нормативной базы и методик измерения skew. Отдельную задачу представляет собой создание и налаживание серийного производства тестирующего оборудования для контроля этого параметра. Ее эффективное решение осложняется необходимостью фиксации малых различий во времени прохождения тестовых сигналов по отдельным волокнам.

Обеспечение дальности связи порядка нескольких сотен метров при использовании схемы параллельной передачи на экономически выгодной длине волны 850 нм нецелесообразно из-за неудовлетворительных дисперсионных характеристик существующих многомодовых волокон. В этой ситуации естественным выходом видится введение в СКС оптических линий нового класса OF-100, фокусной областью применения которых станут ЦОДы и офисные здания. Ранее такие линии нормировались только для кабельных систем промышленного назначения.

## Подведем итоги

Серийная и особенно вновь внедряемая техника СКС вполне пригодна для полномасштабной поддержки функционирования сетевых интерфейсов со скоростями передачи 40 и 100 Гбит/с. Данное утверждение полностью справедливо для оптических систем, а с определенными оговорками – и для медножильных трактов протяженностью до 100 м. В частности, медножильный 100-гигабитный вариант сетевых интерфейсов в обозримой перспективе может быть реализован при использовании элементной базы категории 7а.

Сетевые интерфейсы следующего уровня пропускной способности создаются в настоящее время на основе схем параллельной передачи, что должно соответствующим образом отразиться в стандартах СКС.

Внедрение промежуточного 40-гигабитного варианта сетевых интерфейсов позволяет задействовать для передачи их сигналов горизонтальные кабельные тракты СКС с предельной протяженностью 100 м не ниже категории 7а (в том числе ранее проложенные при условии соответствующей ресертификации).

Отметим, что для СКС, обеспечивающих скорости передачи 40 и 100 Гбит/с, не требуется разрабатывать и внедрять принципиально новые типы линейных кабелей и разъемных соединителей.

Переход в симметричных трактах на скорости 40 Гбит/с сопровождается увеличением объема использования экранированной техники. ИКС

# МегаЦОДам – системы электроснабжения на основе дизельных роторных ИБП

**Благодаря своей простоте, надежности и энергоэффективности системы на основе дизельных роторных ИБП являются идеальным решением для организации бесперебойного электроснабжения ЦОДов большой мощности.**

В 1956 г. Hitec Power Protection запатентовала идею роторных ИБП и ввела в эксплуатацию первую роторную систему ИБП. Эта система имела мощность 20 кВ•А и предназначалась для защиты электропитания оператора связи Royal Dutch Telecom Company (ныне KPN). С тех пор развитие роторных ИБП Hitec Power Protection тесно связано с развитием электропитания телекоммуникационного оборудования и ИТ-инфраструктуры. KPN до сих пор использует роторные ИБП Hitec Power Protection, но они, конечно, усовершенствованы с учетом современных технологических и технических стандартов и их номинальная мощность выросла в среднем в 100 раз. Так, в последние годы в новых мегаЦОДах KPN внедряются системы ИБП номинальной мощностью 2000 кВ•А. Например, в одном из них работает ИБП-система мощностью 24 МВ•А, и это только первая очередь системы, общая мощность которой должна составить 128 МВ•А.

В настоящее время Hitec Power Protection производит одномодульные системы с номинальной мощностью 500–3000 кВ•А и параллельные системы мощностью до 50 МВ•А. Сегодня по всему миру установлено более 1600 единиц оборудования Hitec Power Protection с общей мощностью бесперебойного питания свыше 1,7 млн кВ•А. Большая часть этого оборудования используется в ЦОДах. С появлением в многих странах мира, прежде всего в США и Европе, мегаЦОДов растет спрос и на дизельные роторные ИБП (ДР ИБП) компании Hitec Power Protection. Это вызвано как тем, что ДР ИБП идеально подходят для построения систем ИБП большой мощностью, так и тем, что Hitec Power Protection, являясь лидером на рынке ДР ИБП, обладает огромным опытом в области строительства ИБП-систем крупных ЦОДов. Тенденция к наращиванию мощностей ЦОДов прослеживается и в России, и поэтому в нынешнем году первые ДР ИБП от Hitec Power Protection появились и в российских ЦОДах.

В чем заключается преимущество использования технологии ДР ИБП для ЦОДов большой мощности по сравнению, скажем, с классической технологией, основанной на комбинации статических ИБП, батарей и ДГУ, с помощью которой тоже можно организовать электроснабжение крупных ЦОДов? Если попытаться сформулировать одним словом, то основным преимуществом технологии ДР ИБП является простота. Дело в том, что по мере изменения масштабов и конфигурации вычислительных мощностей и с учетом необходимости повышенной надежности инженерная инфраструктура систем энергоснабжения также должна соответствующим образом изменяться. На основе ДР ИБП эта задача решается легко, поскольку повышение мощности ИБП-системы достигается за счет увеличения номинальной мощности машин ДР ИБП при сохранении простой структуры электроснабжения. Например, для поставки критической мощности 10 МВ•А нужно всего пять машин ДР ИБП плюс одна резервная. Одна машина 2000 кВ•А сочетает в себе функции ИБП, аккумуляторных батарей и дизель-генераторной установки для бесперебойного электроснабжения мощностью 2000 кВ•А.

Схема работы одной машины ДР ИБП поразительно проста. Все основные энергетические элементы ДР ИБП – синхронный генератор, ротор накопителя энергии и дизель (рис. 1) – собраны на одной раме и соединены простой соосной механической связью. Следовательно, не нужны никакие внутренние силовые электрические соединения, коммутационная аппаратура и автоматика для связи модулей ИБП, аккумуляторных батарей и дизель-генераторной установки, причем речь идет о значительных токах. Для получения 10 МВА нужно всего 5 + 1 машин ДР ИБП. Простота решения здесь связана с уменьшением числа нужных компонентов большой мощности, что по известному принципу означает повышение надежности и доступности электроснабжения.

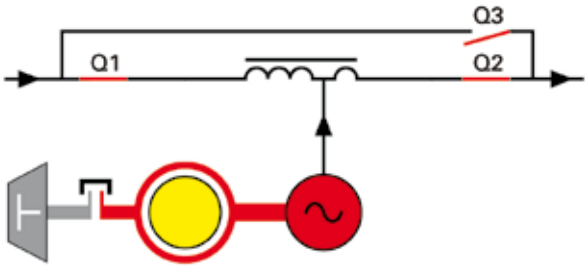



**Рис. 1. Схема одной машины ДР ИБП: нормальный режим при наличии сетевого питания. Нагрузка питается от сети, дроссель совместно с синхронным генератором работает как активный фильтр**

При использовании ДР ИБП не только упрощается структура электроснабже-

**Рис. 2. ЦОД, зал ДР ИБП: На площадке 30 х 20 м построена система бесперебойного гарантированного электроснабжения мощностью 18,4 МВ·А на основе параллельной конфигурации N + 1. В этом ЦОДе два таких зала ДР ИБП.**



ния ЦОДов большой мощности, но и снижаются капитальные затраты из-за того, что отпадает необходимость в аккумуляторных батареях, а значит, и в помещении, где они должны находиться, в организации кондиционирования, вспомогательной аппаратуре, противопожарной защите... То же самое можно сказать и о помещении для модулей статических ИБП с аппаратурой, требуемой для их работы. ДР ИБП устанавливаются в помещении или контейнере, соответствующем помещению, в котором находятся традиционные дизель-генераторные установки (рис. 2). При этом за счет отсутствия аккумуляторных и помещений для статических ИБП экономия занимаемых площадей составляет, как правило, 40–60%.

Для охлаждения ДР ИБП не требуется кондиционирования, для всех режимов работы достаточно простой вентиляции, что приводит к дополнительной экономии электроэнергии. Именно дополнительной, потому что ДР ИБП обладают высоким КПД за счет того, что отсутствует преобразование энергии. В нормальном режиме работы при наличии сетевого питания энергия поставляется из сети в нагрузку через дроссель. В этом основном режиме система функционирует как источник стабилизированного питания, компенсатор реактивной мощности ($\cos \varphi = 0{,}98$) и активный фильтр, который устраняет короткие перебои, пики, провалы напряжения и гармонические колебания. Очевидно, что потери энергии при такой схеме минимальные. Это же относится ко всей системе электроснабжения на основе ДР ИБП, которая способна экономить как минимум на 5% электроэнергии больше по сравнению с классической схемой, так как КПД ДР ИБП высокий, число компонентов системы электроснабжения меньше и кондиционирование не используется.

Так высокая энергоэффективность системы питания на основе ДР ИБП помогает решать задачу повышения энергоэффективности ЦОДов большой мощности. Системы ДР ИБП компании Hitec Power Protection работают в мегаЦОДах, показатель PUE которых достигает 1,31–1,27. Поскольку при использовании ДР ИБП нет необходимости периодически заменять и выбрасывать огромное количество аккумуляторных батарей, а срок службы самих ДР ИБП превышает 25 лет, то можно сказать, что ДР ИБП – экологически чистое решение.

Таким образом, благодаря простоте системы энергоснабжения на основе технологии ДР ИБП получается самая надежная, самая экономичная, самая экологичная и самая компактная система ИБП для ЦОДов большой мощности. И это еще без учета технических преимуществ и того факта, что Hitec Power Protection предлагает своим заказчикам не разрозненное оборудование, а полное решение от ввода сети до места присоединения критической нагрузки. В действительности в этом нет ничего сложного, поскольку систему ИБП заказчику не нужно собирать из разных электрических аппаратов от разных производителей, все задачи решает одна машина ДР ИБП. Необходимо также подчеркнуть, что решение на базе ДР ИБП отвечает требованиям Uptime Institute, причем некоторые ЦОДы, в которых используются ДР ИБП Hitec Power Protection, получили сертификат Tier III или Tier IV.

# Шкаф для оптических сетей доступа FTTH

Шкаф ШКО 32-портовый двухсекционный предназначен для подключения к одному волокну магистрального кабеля до 32 квартир в подъезде. Он служит для распределения оптических каналов посредством сплиттера, а также для транзита потоков в другие шкафы. Шкаф устанавливается на этажных площадках и в распределительных шкафах ШРП.

Дно шкафа делится на три части двумя уголками. Благодаря этому входящие на первую и вторую кассеты запасы модулей располагаются под кассетами соответственно. Среднюю часть отсека можно использовать для размещения модуля на дне бокса.

**ООО «Алюдеко»: (4942) 31-1733**

## Система защиты информации в веб-приложениях

Peter-Service Security Manager – программный комплекс для защиты персональных данных, обеспечивающий контроль целостности, управление доступом, регистрацию и учет доступа к информации. Предназначен для защиты информации в веб-системах массового обслуживания. Реализует централизованное хранение авторизационных данных и управление процессом предоставления доступа ко всем веб-системам и мобильным платформам инфраструктуры пользователя. Способен работать под управлением ОС HP-UX, Linux, Sun Solaris, Windows совместно с широким спектром веб-систем.

В состав Security Manager входят:

- средство защиты информации от несанкционированного доступа HAS Access Manager, сертифицированное ФСТЭК в соответствии с требованиями информационной безопасности;
- веб-сервер Apache с модулем XSLT-трансформации;
- высокопроизводительный сервер приложений (HAS-сервер);
- веб-интерфейс для управления атрибутами доступа в HAS-сервер;
- СУБД Oracle Database 10g Express Edition;
- инсталлятор под все поддерживаемые операционные системы.

**ЗАО «Петер-Сервис»: (812) 326-1299**

# Телекоммуникационный климатический шкаф

ШТК-100С ВН-С – стальной одностенный шкаф с приточно-вытяжной системой поддержания микроклимата. Шкаф используется для построения сетей связи типа WiMAX, 3G и др. и позволяет разместить систему электропитания, аккумуляторные батареи и оборудование связи вне отапливаемых помещений, на крышах, чердаках, столбах, опорах и т.д. Он обеспечивает поддержание внутренней температуры в пределах +5...+35°С при колебании внешней температуры

в диапазоне -40...+30°С. Система управления микроклиматом имеет опцию предварительного разогрева пространства внутри шкафа до положительной температуры перед подключением телекоммуникационного оборудования.

Шкаф предназначен для крепления на вертикальную поверхность (мачта, столб, стена и т.д.) либо для горизонтального размещения (устанавливается на цоколь заданной высоты). Шкаф имеет петли скрытого крепления, ригельный замок трехточечной фиксации. Он изготавливается из стали толщиной 2 мм, что обеспечивает защиту оборудования, установленного в шкафу, от несанкционированного доступа и взлома. Внешние габариты шкафа (В х Ш х Г) – 940 х 630 х 595 мм, масса – 60 кг (существует алюминиевый вариант весом 35 кг).

Система дистанционного оповещения о внештатных ситуациях позволяет диспетчеру оперативно получать информацию о состоянии шкафа и размещаемого в нем оборудования. Контроллер «Штиль» в комплекте с датчиками вскрытия двери, температуры, дыма, влажности и т.п. обеспечивает сбор и передачу информации по предоставленным каналам на пульт удаленного оператора.

**Группа компаний «Штиль»: (4872) 24-13-62**

# Набор средств разработки ПО
## для программирования сенсорных сетей

SDK Mote Runner представляет собой открытую платформу для программирования и облегчения использования сенсорных и приемопередающих узлов («мотов», motes) беспроводной сенсорной сети.

Mote Runner включает в себя среду имитационного моделирования, веб-ориентированную панель управления и интегрированную среду разработки на базе Eclipse для тестирования, отладки и обслуживания программных приложений для сенсоров. Эта платформа позволяет моделировать сети датчиков перед развертыванием «мотов» непосредственно на объекте. Она спроектирована для работы с ограниченными вычислительными ресурсами: 8-разрядный процессор, 8 Кбайт оперативной памяти и 64 Кбайт флэш-памяти. Поддерживает удаленное обновление по беспроводному каналу с минимальным прерыванием функционирования развернутой сенсорной сети. Mote Runner может использовать альтернативные источники энергии, например, солнечные батареи.

**IBM: (495) 775-8800**

# IP-камера
## «день/ночь»

Видеокамера Smartec STC-IPM3096A оснащена 1,3-мегапиксельной CCD-матрицей Sony ExViewHAD и передает цветные/монохромные видеопотоки при освещенностях до 0,4/0,06 лк. Она использует кодеки M-JPEG и MPEG-4 и способна транслировать один поток в M-JPEG с разрешением до SXVGA (1280 x 960 пикс) или одновременно два индивидуально настроенных видеопотока в разных форматах. Кроме того, камера STC-IPM3096A имеет детектор движения, «тревожный» вход/выход, аудиовход/выход, поддерживает PoE и комплектуется картой памяти SD емкостью 2 Гбайт для временного хранения данных. Записывать видеоданные на карту можно либо постоянно, циклически обновляя архив по мере его заполнения, либо только при возникновении тревожных ситуаций. Настройку камеры можно выполнять с веб-браузера, а управлять работой – с помощью полнофункционального русифицированного ПО NetStation или XProtect компании Milestone.

Оптимизация видеопотока в M-JPEG под пропускную способность канала осуществляется с помощью выбора степени сжатия видео: low, middle или high, а в формате MPEG-4 камера может транслировать видео VGA-стандарта в полнокадровом режиме. Исключить переход STC-IPM3096A между режимами «ночь»/«день» при кратковременных изменениях уровня освещенности можно путем задания времени задержки ее переключения на 5, 10, 15 или 30 с.

**«АРМО-Системы»: (495) 787-3342**

# Система инвентаризации на основе RFID

Система АйТи-АИ предназначена для автоматизации учета и инвентаризации имущества с применением технологии радиочастотной идентификации (RFID) и двумерного штрихового кодирования. Она обеспечивает:

- первичный учет имущества (в том числе заведение новых объектов), подготовку меток для объектов учета;
- инвентаризацию с помощью мобильного считывателя (контроль наличия, перемещения и состояния объектов учета, выявление излишков и недостач);
- обработку результатов инвентаризации (генерацию инвентаризационных отчетов об излишках, недостачах, проинвентаризованных объектах, автоматическое обновление данных по результатам инвентаризации);
- ведение информации по объектам учета (справочников, истории изменения атрибутов объектов учета), отслеживание жизненного цикла объектов (ввод в эксплуатацию, использование, вывод из эксплуатации, списание);
- синхронизацию с учетной системой заказчика;
- формирование сводной отчетности (аналитических отчетов, лицевых карточек ответственного, отчетов с использованием визуализированных поэтажных планов);
- контроль вноса/выноса объектов из здания с помощью противокражных ворот;
- планирование технического обслуживания и ремонта эксплуатируемых объектов благодаря ведению информации о выполнении гарантийных, плановых, внеплановых ремонтных работ, замене узлов, запчастей, расходных материалов (с помощью модуля АйТи-ТОРО).

Принцип работы системы


Система АйТи-АИ может быть реализована либо на базе SAP R/3, либо на базе «1С: Предприятие», либо в качестве оригинальной разработки на платформе SQL Server. При этом интеграция с любой учетной системой заказчика реализуется посредством настраиваемого обмена данными определенного формата.

**«АйТи»: (495) 974-7979**

# Блог, еще раз блог!



**Владимир ЛИТВИНОВ**

## Магические даты «Ростелекома»

>>>> Двадцать лет назад, 26 июня 1990 г. было создано АО «Совтелеком», взявшее на себя функции развития и эксплуатации сети междугородной и международной связи на территории СССР. Удивительно, но ровно через два десятилетия, 26 июня 2010 г. состоится судьбоносное собрание «Ростелекома» по присоединению МРК и созданию объединенной компании. Напомню, что после распада Союза «Совтелеком» преобразовали в международное акционерное общество «Интертелеком», на основе которого в сентябре 1993 г. и было создано ОАО «Ростелеком».

Вспоминаю первое собрание акционеров на московской «междугородке» ММТ – будущем филиале «Ростелекома». Зал, рассчитанный на тысячу мест, не мог принять всех желающих, к микрофонам, установленным в зале, выстраивались длинные очереди, а члены совета директоров сидели в президиуме в постоянном ожидании каверзных вопросов. Трудовой коллектив и ветераны (около 7 тыс. чел.) получили акции предприятия и стали его собственниками. Другое дело, что в эти акции после провальной ваучеризации верили немногие. Поэтому и продавали иногда свои пакеты за две бутылки водки. А ведь через три-четыре года на них уже можно было приобрести отечественный автомобиль.

Другая картина будет 26 июня 2010 г. Мелкая группа крупных акционеров и аффилированных лиц, разместившись в уютном зале на 100 человек учебного центра Бекасово, примет решение по присоединению МРК к «Ростелекому». Как уже ровно 10 лет назад, в 2000 г. было проведено присоединение ММТ к «Ростелекому». Не правда ли, удивительна кратность магических цифр и практически филигранное совпадение судьбоносных решений по «Ростелекому» (1990–2000–2010)?

Мелким миноритариям сегодня на этих собраниях делать нечего, они не могут влиять практически ни на что. <...> А результаты деятельности общества действительно «впечатляющие»: капитализация упала в 2 раза, чистая прибыль снизилась на 71%. Таких результатов за 20 лет существования компании не было, как, впрочем, и бонусов. Настоящим строителям «Ростелекома», в том числе московским ветеранам-связистам (по филиалам информацией не владею), ко дню Победы и празднику Связиста, вопреки 20-летней традиции, денежных средств не нашлось (раньше выделяли по 1 тыс. руб. каждому из 1 тыс. чел., итого 1 млн руб.). А ведь эти люди отработали в компании 20–30–40 и даже 50 лет (фактически линиям связи и сооружениям «Ростелекома» более 110 лет). Впрочем, будем точны: если ветерану исполнилось 80 и более лет, ему выделялся бонус в размере 3 тыс. руб. и продуктовый набор.

Такие нынче времена, берегите себя, здоровья вам до 80 и более лет.

комментировать

**Дмитрий КУТЯВИН**

## Тестовые зоны LTE помогут бюджету

>>>> Развитие новых технологий – это развитие бизнеса телекоммуникационных компаний. А также это дополнительные налоги для государства.

Согласно отчетности компаний, например, в I квартале 2010 г. размер налогов, уплаченных «МегаФоном», составил 2,5 млрд руб. В 2010 г. «ВымпелКом» заплатил налоги на сумму $593 млн (с учетом того, что 85% доходов собираются в РФ, налоговые выплаты могли быть близки к 15 млрд руб.).

Для сравнения – все расходы бюджета Екатеринбурга в 2010 г. составят по плану 21,5 млрд руб. А расходы бюджета Приморского края в 2010 г. превысят доходы на 8,2 млрд руб.

В Свердловской области и в Приморском крае могут быть развернуты тестовые зоны LTE.

Чем дольше будут «буксовать» тестовые зоны, тем дольше не будут работать коммерческие базовые станции, тем дольше абоненты не получат скоростного мобильного Интернета, и тем дольше не будут уплачены первые налоги.

комментировать

**Петр ДИДЕНКО**

## Nexus по Маяковскому

>>>> Nexus One – не телефон, а case study, желание Google показать телефонной индустрии, как может выглядеть хороший телефон на ОС Android. То есть задать таким методом стандарт качества для Android-телефонов.

Сейчас тот же Microsoft пытается сделать что-то похожее, но другим путем. А именно, заставляет производителей устройств соблюдать определенные минимальные требования к железу и минимальный же набор функций, которые телефон должен выполнять. При этом Microsoft загоняет всех в эти рамки насильно, а Google просто задрал планку довольно высоко.

Помните, у Маяковского, кроха-сын пришел к отцу с вопросом «что такое хорошо, что такое плохо». Папа на пальцах объяснил, и все стало понятно. Тут происходит нечто похожее.

В результате теперь не имеет смысла делать телефон хуже Nexus One – он просто будет плохо продаваться.

комментировать


Подпишись на журнал «ИКС»

## Подписчики журнала гарантированно получают*:

- Доступ к электронной версии журнала «ИКС» в день его выхода

## Оформляйте подписку:

- В редакции — по телефону: +7 (495) 785 1490 или e-mail: podpiska@iksmedia.ru
- Каталог Роспечать — индекс 73172, 71512
- Каталог Пресса России — индекс 12417
- Объединенный каталог — индекс 43247
- Список альтернативных агентств: http://iksmedia.ru в разделе подписка.

Специальные условия при оформлении подписки для корпоративных клиентов! Подробности по телефону отдела распространения: +7 (495) 785 1490

Тел.: +7 (495) 785 1490 • E-mail: podpiska@iksmedia.ru • ICQ: 491 320 884

* оформившие подписку через редакцию или альтернативное агентство

**Телеком • ИТ • Медиа** **www.iksmedia.ru**

# Реклама в номере

**3М РОССИЯ**
Тел.: (495) 784-7474
Факс: (495) 784-7475
**www.3mrussia.ru . . . . с. 34-35**

**ВЕНТСПЕЦСТРОЙ**
Тел.: (495) 775-3791
Факс: (495) 775-3790
E-mail: info@ventss.ru
**www.ventss.ru . . . . . с. 79**

**ГЛОБАЛ-ТЕЛЕПОРТ**
Тел.: (495) 647-7777
Факс: (495) 647-7733
E-mail: info_gt-port@synterra.ru
**www.globalteleport.ru . . . . с. 11**

**КОМКОР (АКАДО ТЕЛЕКОМ)**
Тел.: (495) 411-7171
Факс: (495) 411-7151
E-mail: info@akado-telecom.ru
**www.akado-telecom.ru . .1-я обл., . . . . . 2, 4, 27-32, 36-49**

**КОМПАНИЯ КОМПЛИТ**
Тел.: (812) 740-3010
Факс: (812) 740-30-11
E-mail: info@complete.ru
**www.complete.ru . . . . . с. 31**

**ЛОГИЧЕСКИЙ ЭЛЕМЕНТ**
Тел./факс: (495) 229-3632
E-mail: info@logic-cell.ru
**www.logic-cell.ru . . . . . с. 37**

**ПЕТЕР-СЕРВИС**
Тел.: (812) 326-1299
Факс: (812) 326-1298
E-mail: sales@billing.ru
**www.billing.ru . . . . . 4-я обл.**

**ЦЕНТРТЕЛЕКОМ**
Тел.: (495) 793-2424
Факс: (495) 650-3007
E-mail: vip@centertelecom.ru
**www.centertelecom.ru . с. 2, 4, 23**

**ШТИЛЬ ГК**
Тел./факс: (495) 788-8291
E-mail: mosoffice@shtyl.ru
**www.inels.ru. . . . . с. 33**

**APC BY SCHNEIDER ELECTRIC**
Тел.: (495) 916-7166
Факс: (495) 620-9180
E-mail: apcrus@apc.com
**www.apc.ru . . . . . с. 71**

**AYAKS ENGINEERING**
Тел.: (495) 229-9922
Факс: (495) 188-9374
E-mail: mail@ayaks.ru
**www.ayaks.ru . . . . . с. 80-81**

**CITRIX SYSTEMS RUSSIA**
Тел.: (495) 937-8249
Факс: (495) 937-8305
**www.citrix.ru . . . . . с. 15**

**DATADOME**
Тел.: (495) 580-7348
Факс: (495) 665-6200
E-mail: info@datadome.ru
**www.datadome.ru . . с. 28, 29, 70**

**DEPO COMPUTERS**
Тел.: (495) 969-2222
Факс: (495) 969-2229
E-mail: sales@depo.ru
**www.depocomputers.ru . . . с. 77**

**EATON**
Тел.: (495) 981-3770
Факс: (495) 981-3771
E-mail: UPSRussia@eaton.com
**www.eaton.ru . . . . . с. 13**

**EXSOL**
Тел.: (495) 228-9832
E-mail: info@exsol.ru
**www.exsol.ru . . . . . с. 73-75**

**HITEC**
Тел.: (+31) 546-589589
Факс: (+31) 546-589489
E-mail: info@hitec-ups.com
**www.hitec-ups.com . . . с. 90-91**

**HUBER+SUHNER**
Тел.: (495) 775-6653
Факс: (495) 775-7794
E-mail: info.ru@hubersuhner.com
**www.hubersuhner.ru . . . . с. 87**

**IBM**
Тел.: (495) 258-6348
Факс: (495) 258-6363
**www.ibm.com/ru . . . . 2-я обл.**

**LENOVO**
Тел.: (495) 663-8260
Факс: (495) 663-8261
**www.lenovo.com/ru . . . . . с. 3**

**MERCURY**
Тел.: (495) 225-5626
Факс: (495) 225-5670
E-mail: info@mercuryeng.com
**www.mercuryeng.com . . . с. 32, . . . . . 40, 42 , 50-51**

**RIT**
Тел./факс: (495) 684-0319
E-mail: marketing@rit.ru
**www.rit.ru . . . . . с. 89**

**STACK GROUP**
Тел.: (495) 980-6000
Факс: (495) 980-6001
E-mail:info@stack.net
**www.stack.net. . . . . с. 72**

**TRIPP LITE**
Тел.: (495) 799-5607
Факс: (495) 787-2767
**www.tripplite.com . . . . . с. 45**

# 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.