

Высокий старт

Новый торговый год российский рынок акций начал с очередного покорения вершин.



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

Традиционное предновогоднее ралли вывело отечественные фондовые индексы на максимальные годовые значения: индекс РТС достиг их 28 декабря (1776,17 пункта), индекс ММВБ – 7 декабря (1702,64 пункта). В первые торговые дни нового года российские площадки демонстрировали рост, отыгрывая позитив международных рынков, накопившийся за время долгих выходных. С середины недели рост на рынке сменился небольшой технической коррекцией – инвесторы поспешили зафиксировать прибыль.

В целом за рассматриваемый период, с 16 ноября 2010-го по 15 января 2011 г., индекс ММВБ прибавил 12,12% (до уровня 1744,74 пункта), а индекс РТС вырос на 16,19% (1870,09 пункта). Отраслевые индексы также зафиксировали рост: индекс «ММВБ телекоммуникации» увеличился на 10,59% (2523,88 пункта), индекс «РТС Телекоммуникации» прибавил 19,24% (279,71 пункта).

Под знаком «Связьинвеста»

Акции телекоммуникационного сектора с осени 2010 г. активно росли: как и прежде, внимание инвесторов к этому рынку привлекала реформа «Связьинвеста». Стартовав в первом квартале 2010 г., реорганизация телекоммуникационных активов уже прошла ряд ключевых этапов (среди которых расчет коэффициентов конвертации бумаг МРК и «Дагсвязьинформа» в обыкновенные акции «Ростелекома», одобрение реформы на общих собраниях акционеров, выкуп акций у несогласных с ней миноритариев). Кроме того, недавно в рамках создания единой телекоммуникационной компании на базе «Ростелекома» все генеральные директора МРК были назначены по со-

Итоги-2010

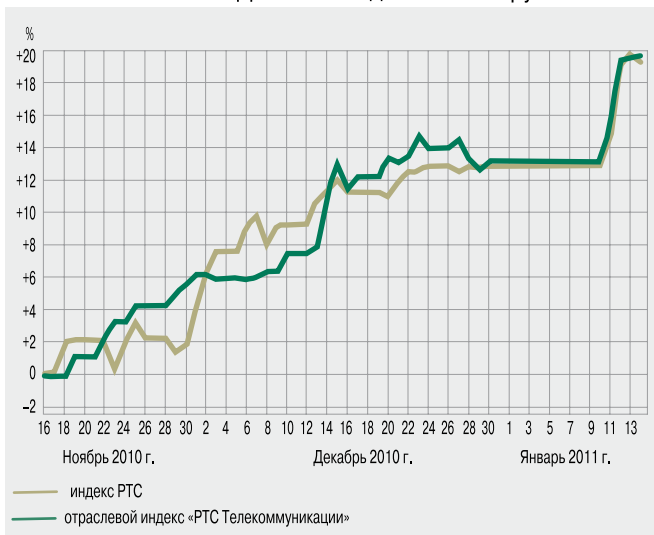


Российские фондовые индексы по итогам 2010 г. прибавили около 23% (РТС – 22,79%, ММВБ – 23,21%), опередив как биржевые индексы крупнейших развитых рынков, так и фондовые индикаторы группы БРИК. Незначительно уступил показателям российского рынка биржевой индикатор Индии, а худшую динамику в группе продемонстрировал фондовый рынок Китая, потерявший более 10% на опасениях замедления «локомотива» мировой экономики.

вместительству вице-президентами «Ростелекома»; в будущем они будут отвечать за развитие бизнеса на территории отдельных федеральных округов.

Инвесторы позитивно отыграли последние новости о реорганизации – акции «Ростелекома» выросли за рассматриваемый период на 26,53%, до отметки 176,88 руб. Остальные МРК

Динамика индексов и инструментов РТС



также показали впечатляющий рост: акции «Сибирь-телекома» выросли на 20,42% до 2,842 руб., капитализация «Северо-Западного Телекома» увеличилась на 20,51%, до отметки 32,05 руб. за акцию. Бумаги «Дальсвязи» вошли в растущий тренд еще в начале ноября, а наибольшие темпы роста показали в декабре, за последние два месяца года прибавив в цене 19,5% – до уровня 139,22 руб.

МРК: нас не догонят

Еще одним поводом для роста акций МРК, уже в текущем году, послужила новость о том, что «Сургутнефтегаз» и Raybrook Ltd. (структура основного владельца «Северстали» Алексея Мордашова), которым принадлежит по 10% акций ОАО «Национальные телекоммуникации» (НТК), предложили обменять свои доли в компании на пакет объединенного «Ростелекома» (речь идет о примерно 2% акций). Вышедшая новость 12 января привела к взлету обыкновенных и привилегированных акций «Ростелекома» на 10 и 4% соответственно, а спрос на бумаги остальных МРК приобрел ураганный характер.

Ряд активов российского телекоммуникационного сектора активно наращивал капитализацию на фоне корпоративных новостей. Так, впечатляющий рост зафиксировали акции «Центртелекома», прибавив за рассматриваемый период 21,20% (их цена составила 34,578 руб. за акцию). Позитивным моментом для бумаг компании стала новость о том, что агентство Standard & Poor's повысило долгосрочный кредитный рейтинг ОАО «ЦентрТелеком» с «BB-» до «BB», прогноз по рейтингу – «Стабильный». В то же время рейтинг «ЦентрТелекома» по национальной шкале был повышен с «ruAA-» до «ruAA».

Сопоставимые результаты за рассматриваемый период показали бумаги «Уралсвязьинформа» и

«Волгателекома», прибавив чуть больше 17% – до цены 1,513 руб. и 147,01 руб. за акцию соответственно. Обе компании представили позитивную отчетность за 9 месяцев 2010 г. по МСФО, значительно увеличив чистую прибыль по сравнению с аналогичным периодом прошлого года.

Mobile не догоняет fix

Сотовый сегмент рынка, на фоне взрывной динамики межрегиональных компаний электросвязи, выглядел довольно скромно: цена акций МТС подросла на 0,66%, составив 257,27 руб. Такой динамике сопутствовал целый ряд факторов. Так, 23 декабря акционеры «Комстар-ОТС» приняли ожидае-

→ Предложение «Сургутнефтегаза» и Raybrook, структуры А. Мордашова, обменять свои доли в компании НТК на пакет «Ростелекома» вызвало взлет акций объединенной компании и бумаг МРК

мое рынком решение реорганизовать компанию в форме присоединения к ОАО «Мобильные Теле-Системы». Негатива добавила новость о том, что правительство Туркменистана полностью остановило работу дочерней компании МТС, Varash Communications Technologies, и аннулировало выданную ей лицензию на оказание услуг сотовой связи с 1 января 2011 г. Данную новость инвесторы отыгрывали несколько дней, в результате чего акции МТС потеряли около 2%.

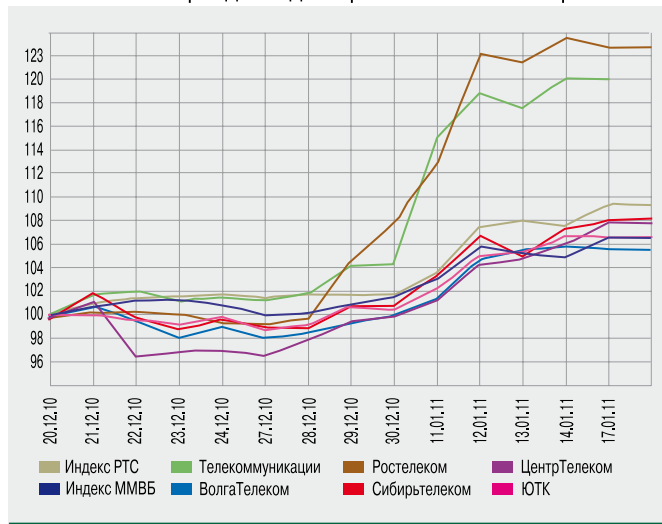
Технологичные компании повысили ликвидность

Стабильно высокие показатели в последние два месяца демонстрировал сегмент технологичных компаний. Если бумаги АФК «Система» выросли на 4,8% – до уровня 27,832 руб., то акции «Ситроникса» за рассматриваемый период подорожали на 44%. Хороший рост показали акции «РБК-ИС», прибавив 39%; они росли на ожиданиях скорой конвертации в бумаги «РБК-ТВ Москва». Согласно последним данным, с 19 января 2011 г. в ЗАО «ФБ ММВБ» начнутся торги акциями ОАО «РБК-ТВ Москва» в процессе обращения.

Переход GDR IBS Group в сегмент регулируемого рынка Франкфуртской фондовой биржи незамедлительно сказался на повышении их ликвидности. За рассматриваемый период бумаги компании выросли на 28%. Ранее GDR IBS Group торговались на Франкфуртской фондовой бирже в нерегулируемом сегменте, что весьма смущало потенциальных инвесторов.

Бумаги эмитента Mail.ru Group, торгующегося на Лондонской фондовой бирже, подорожали на 25%. Цены на акции росли в основном за счет стремительного роста зарубежных активов, таких как социальная сеть Facebook и сервис Groupon. ИКС

Динамика индексов РТС и телекоммуникационных компаний в период с 20 декабря 2010 г. по 15 января 2011 г.



Январь - февраль 2011. ИКС

Все вращается вокруг конвергенции, даже биллинг

Дискуссии о необходимости миграции к конвергентному биллингу закончились. Новые рыночные условия предъявляют новые требования к системам OSS/BSS, и операторы сегодня уже ведут речь о выборе конкретных решений и стратегии перехода.



**Татьяна
ТОЛМАЧЕВА,**
директор
по развитию
бизнеса
в России
и СНГ
Frost & Sullivan

Кардинально меняющаяся среда телекоммуникационного рынка – ужесточение конкуренции, бурное развитие конвергентных и мультисервисных сетей, появление коммуникационных сервисов, создающих иной стиль жизни, – заставляет операторов связи смещать основной фокус своих бизнес-процессов. В центре внимания оказывается Его Величество Потребитель. А чтобы поддерживать удовлетворенность потребителя на высоком уровне, в первую очередь необходимо «приспосабливать» все системы поддержки операционной и бизнес-деятельности к новым условиям современной динамичной среды. В итоге процесс объединения ИТ-ресурсов – от организации доступа абонентов до приложений всех уровней – становится для операторов все более важным. К системам OSS/BSS уже сейчас предъявляются новые требования, ключевыми из которых являются приближение взаиморасчетов к режиму реального времени, гибкость и масштабируемость. Биллинг в реальном времени позволяет более плотно вовлечь абонентов в процесс предоставления услуги, а гибкость необходима для целей тарификации, интеграции с другими системами и быстрого создания новых продуктов.

Биллинг в водовороте изменений

Новые системы поддержки операционной и бизнес-деятельности должны учитывать целый ряд вызовов времени.

Необходимость монетизации сервисов – рост потребления услуг мобильной и фиксированной связи (как следствие роста индивидуального потребления и увеличения абонентской базы) и распространение бытовой электроники с выходом в Интернет создают новые возможности извлечения доходов от услуг мобильного и проводного Интернет-доступа. Расширяется спектр услуг, а значит, требуется реали-

зовать разные принципы расчета и обрабатывать большее количество форматов учетной информации.

Гибкость систем и новый функционал – в современных системах OSS и BSS операторы получили гибкость в поддержке сложных продуктовых пакетов в режиме реального времени, в том числе и возможность контроля за пользованием услугами (на основе определенных клиентом финансовых ограничений и операционных параметров). Все это становится важным фактором реализации политики управления удовлетворенностью клиента.

Новые бизнес-модели – необходимо быть готовыми к новой модели предоставления услуг через «облака». Рынок пока только нацеливается на то, чтобы дать клиенту возможность получать самые современные услуги в любом месте в любое время от широкого круга партнеров. Такая модель в значительной степени зависит от партнеров и от наличия системы BSS, работающей в режиме реального времени, способной обрабатывать все форматы информации и обеспечивать функционал разделения доходов между операторами, поставщиками контента и независимыми сервис-провайдерами.

Оптимизация операционных затрат – необходимо повышать эффективность управления операционными затратами в условиях роста объемов данных, модернизации инфраструктуры, совершенствования бизнес-процессов и внедрения новых моделей.

Поддержка коммуникационных услуг, ориентированных на различные отрасли – существует потребность предоставлять новые сервисы, возникающие благодаря развитию коммуникаций и появлению новых типов устройств с выходом в Интернет. Эти сервисы предназначены для различных отраслей экономики, среди которых здравоохране-

ние, транспорт, государственный сектор, медиа и развлечения (в том числе книгоиздание), производство (в частности, автопром) и розничная торговля.

Все эти факторы дали толчок к появлению нового типа биллинга – конвергентного. Идея перехода к конвергентному биллингу появилась уже лет десять назад. И первым шагом в ее эволюции стало появление систем, обеспечивающих одновременное обслуживание авансовых и кредитных абонентов (prepaid and postpaid convergence). До того существовали две отдельные системы биллинга, каждая со своей собственной логикой развития. Postpaid-биллинг обычно использовался для выставления ежемесячных счетов абонентам фиксированной связи, Интернет-доступа, ТВ и в какой-то степени абонентам мобильной связи. Модель prepaid-биллинга появилась в результате эволюции технологии мобильной связи и потребности сократить время на предоставление услуг, когда верификация кредита затруднительна или вообще отсутствует. В настоящее время обе эти модели активно используются во всех сегментах среди всех потребительских групп.

Доходы операторов связи от авансовых и кредитных абонентов сильно варьируются от региона к региону, что не позволяет выявить и спрогнозировать взаимосвязь между покупательной способностью и моделями покупки. При этом стоит заметить, что в связи с расши-

рением границ телеком-рынка в результате его интеграции с рынком ИТ (хранение данных, услуги сетей безопасности), с рынком развлечений (интерактивные услуги), медиа и рекламы вопрос консолидации всей информации о клиентах, апгрейда систем и переосмысления бизнес-процессов становится критически важным. А традиционный подход к структурированию по методам оплаты (pre/postpaid) будет размываться в связи с тем, что абонент одновременно может использовать разные методы оплаты в зависимости от типа сервиса.

Биллинг в стратегиях конвергенции

Новые операторы, осознавая изменения рынка, с самого начала внедряют конвергентный биллинг (например, компания «Сумма Телеком» объявила, что на ее сети будет внедрен конвергентный биллинг до конца 2010 г.).

Существующим операторам на конвергентный биллинг приходится мигрировать. При этом, по отзывам поставщиков конвергентных биллинговых решений, самой большой проблемой при переходе становится задача объединения технологий нескольких производителей. Чем больше решений от разных поставщиков, тем дороже и сложнее переход на конвергентный биллинг. Именно поэтому стратегия миграции во многом зависит от того, как и какая система(системы) была

Что такое «конвергентный биллинг» и как его представляют себе игроки рынка

«ВымпелКом» Конвергентный биллинг – это возможность выставить клиенту счет независимо от того, какой системой оплаты (pre-, postpaid) он пользуется, включен ли он как неотъемлемая часть в корпоративное соглашение или выступает как частное лицо (может быть, как глава семьи), были ему предоставлены голосовые услуги или услуги передачи данных и т.д., и т.п.

«МегаФон» Единая концептуальная и технологическая платформа для мобильных и фиксированных сегментов сети, услуг и абонентов.

«Скай Линк» Конвергентный биллинг – это мультисервисный биллинг, позволяющий работать с неограниченным количеством платформ/приложений/услуг. Применительно к практике компании это биллинг, который обеспечивает поддержку конвергентных услуг и всех необходимых бизнес-процессов и приложений (как для внутренних, так и для внешних пользователей).

«Уралсвязьинформ» Конвергенция в сфере расчетов за услуги связи

происходит по нескольким направлениям. Оператору связи необходима конвергенция по методам расчетов, когда биллинговая система используется для одновременного обслуживания кредитных (postpaid) и предоплаченных (prepaid) схем. Возможна конвергенция по технологиям доступа, когда на единой технологической платформе обслуживаются абоненты сети связи общего пользования, сети подвижной радиотелефонной связи и сети передачи данных. В таком случае конвергентное биллинговое решение должно быть настроено на обработку данных от всего спектра телекоммуникационного оборудования. Наконец, существует конвергенция в направлении услуг. При этом появляется возможность создания единого портала самообслуживания по всем используемым услугам и выставления общего счета. Такая конвергенция сократит время, затрачиваемое на продвижение комплексных продуктов и услуг, позволит вывести на рынок

пакетные предложения для различных сегментов. Например, абоненту, пользующемуся двумя и более услугами, для повышения лояльности можно предоставить сервисные и тарифные бонусы в зависимости от объема потребленных услуг или накопленных платежей (по любой из услуг или их комбинации).

Amdocs Конвергентный биллинг – это универсальная биллинговая система, способная на одной платформе:

- обслуживать все виды бизнеса оператора (мобильная/проводная телефония, Интернет, ТВ и т.д.);
- обслуживать все виды абонентов (prepaid, postpaid, гибриды);
- работать со всеми форматами информации (CDR, события);
- работать со всеми сетями и протоколами (SS7, SIP и т.д.).

TELE2 Конвергентный биллинг – это полностью конвергентная система, осуществляющая расчеты с абонентами по всем видам услуг, предоставляемым компанией.

реализована. Большинство мобильных операторов в настоящий момент пользуются биллинговыми решениями от разных вендоров: например, в сети «Билайн» установлены системы нескольких поставщиков, включая Amdocs и Comverse. И такая ситуация достаточно типична.

Существуют несколько уровней реализации принципа конвергентности в биллинговых системах:

- 1) уровень продаж и маркетинга – для одновременного продвижения продуктов и услуг среди всех категорий клиентов;
- 2) уровень продукта – для единых подходов к «упаковке» продуктов и услуг для всей клиентской базы;
- 3) уровень потребителя – общий уровень обслуживания для всех абонентов, вне зависимости от их типа;
- 4) уровень сервиса – платформа управления услугами;
- 5) уровень ресурсов сети – объединение системы-медиатора с подсистемой управления профилем услуг.

Все российские операторы связи примерно одинаково определяют понятие «конвергентный биллинг» (см. врезку); тем не менее, как говорится, черт в деталях, поэтому самое интересное – как технически реализуется операторами принцип конвергентности в биллинге.

В настоящее время существует несколько подходов к стратегии перехода на конвергентный биллинг. Первый – это интеграция параллельно действующих биллинговых систем типа prepaid и postpaid через синхронизацию данных, например с помощью единого CRM-или SelfService-решения. Второй подход – модульный, он предполагает приобретение биллинговой системы с модульной архитектурой и поэтапную интеграцию дополнительных модулей до полной конвергенции. И наконец, третий подход – приобретение нового конвергентного биллинга и полная замена старой системы. Каждый из них имеет свои достоинства и недостатки.

Интеграция параллельно действующих систем – наименее затратный подход и наименее рискованный, так как она требует замены/добавления лишь каких-то отдельных функциональных модулей. Но эксплуатация одновременно нескольких схем расчетов существенно ограничивает гибкость и возможности адекватного ответа на предложения конкурентов, мешает быстро запускать новые услуги, маркетинговые инициативы, тарифные планы. «Лоскутное» развитие системы позволяет оператору решать отдельные краткосрочные неотложные задачи, но этот подход неэффективен и затратен с точки зрения эксплуатационных расходов (необходимо содержать штат специалистов с соответствующей экспертизой по каждой системе), а также общей стоимости владения (ТСО). При такой стратегии оператор рискует рано или поздно

«Если у вас не работает биллинг, у вас не будет связи»

– убежден Константин ЮНОВ, директор по инновационным технологиям ОАО «МегаФон», считая конвергентный биллинг разумной потребностью вертикального холдинга.



Константин ЮНОВ

– Было бы странно затратить \$745 млн на покупку фиксированного оператора и не приобрести универсальный инструмент для работы с клиентами. Когда принимаются бизнес-решения такого масштаба, смешно экономить на биллинге, с новыми активами надо работать.

– Константин Владленович, какие пути ведут оператора к конвергентному биллингу?

– Давно осталось в прошлом представление о конвергентном биллинге как о способе «обсчета» различных схем тарификации (скажем, prepaid или postpaid) и выставления единого счета. Речь идет о единой концептуальной и технологической платформе для мобильных и фиксированных сегментов сети, услуг и абонентов.

Я бы выделил три модели перехода на конвергентный биллинг. Первая – самая распространенная, но не самая верная, – заключается в попытке объединить уже действу-

ющие отдельные решения. Этот путь чреват большими отложенными эксплуатационными затратами, недостаточной функциональностью, невысокой гибкостью. В результате появляются две базы клиентов, что усложняет аналитику, целевые маркетинговые акции, сокращает возможности готовить общие предложения для разных групп клиентов и т.д. Не имея общей базы абонентов, не зная их предпочтений, невозможно делать правильные предложения на конкретном рынке. Знание клиента – конкурентное преимущество будущего. Слать бабушке, у которой в телефоне не подключен SMS-профиль, SMS-предложение посидеть в чате – как-то неправильно.

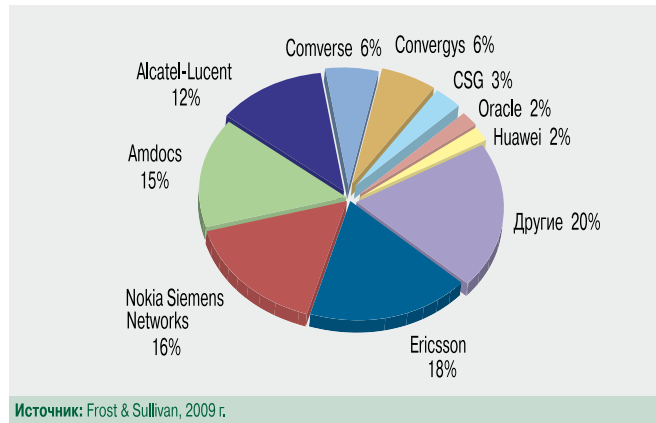
Модель номер два, если коротко, заключается в полной замене старой системы биллинга на конвергентную. Ее опасность – снижение качества обслуживания клиентов в процессе перехода на новую платформу. Иными словами, можно потерять абонентов: если у вас не работает биллинг, у вас не будет связи, базовые станции завязаны на биллинговую систему, это единый комплекс. Для биллинга даже переход на зимнее время – очень сложное техническое мероприятие, в котором занято много специалистов: мы не можем потерять секунды, потому что это большие деньги, например, скидки «привязаны» к суткам, и т.д. и т.п.

оказаться в ситуации, когда инфраструктура перестанет справляться с ростом.

Модульный подход предполагает наличие у оператора биллинговой системы с модульной архитектурой. Интегрируя дополнительные модули, операторы могут доводить свои системы до полной конвергенции. Такой подход позволяет, с одной стороны, распределять затраты во времени, приобретая и внедряя модули, необходимые для конкретных нужд сейчас, а с другой – быть конкурентоспособным, быстро запуская на рынок новые услуги путем самостоятельного подключения соответствующих модулей, без остановки всей системы. Такой стратегии миграции придерживается, например, «МегаФон».

Полностью конвергентный биллинг (конвергентный на всех уровнях) стирает для абонентов границы между различными услугами, он более прозрачен, а также позволяет формировать пакеты услуг, программы скидок, комбинировать и гибко менять формы оплаты и т.п. Большое значение имеет и заметное снижение затрат на приобретение и эксплуатацию единой системы биллинга. Необходимым условием для перехода на конвергентный биллинг является соответствующая реорганизация бизнес-процессов компании. Процессы должны быть ориентированы на клиента. Внедрение единого портала самообслуживания клиентов и единой системы CRM – обязательное условие перехода на конвергентную систему расчетов. Во всех случаях это наи-

Структура мирового рынка решений конвергентного биллинга



более дорогостоящий вариант миграции, и он же считается наиболее рискованным с точки зрения потенциального ухудшения отношений с клиентами в случае технических сбоев при переходе к новой системе.

Тем не менее, ориентируясь на стратегические цели, многие глобальные операторы уже успешно перешли на полностью конвергентный биллинг, и число их продолжает расти. Среди них североамериканская AT&T Mobility, ведущий оператор мобильной связи в Индонезии XL Axiata (23 млн абонентов), BT, Comcast, Sprint, Telefonica O2 Slovakia (и это только операторы, перешедшие на конвергентный биллинг Amdocs).

Модель номер три успешно испытал на себе «МегаФон». Еще в 2005 г. с компанией «Петер-Сервис» мы заложили основу системы биллинга из нескольких сегментов (в том числе фиксированного), которую вместе с коллегами из «Синтерры» доработаем до полнофункциональной схемы, полностью закрывающей весь цикл предоставления услуг любым клиентам (включая, естественно, технический учет). Мы получим полный биллинг с различными схемами тарификации для «МегаФона» в любом понимании термина конвергентности к концу 2011 г. Перед «Петер-Сервис» задача уже поставлена.

– Как эта модель реализуется на практике?

– На практике редко бывает такая счастливая история, чтобы биллинговую систему можно было доработать до полной конвергенции. Мы изначально приняли решение, которое спустя годы позволило нам идти по пути универсализации биллинга. К слову, у нас у единственной из компаний «большой тройки» биллинг построен на российском решении и российскими специалистами, и, по моему убеждению, он лучший с точки зрения функционала. Я уверен: мы никогда не получим высокоэффективную экономику без того, чтобы развивать этот интеллектуальный сектор программного обеспечения и этот высокомаржинальный бизнес.

У нас восемь полноценных унифицированных региональных комплектов биллинга, естественно, применяется релизная схема. Наша цель сейчас – перейти к оптимальному количеству комплектов (на сегодняшний день пять),

не потеряв региональные компетенции. Здесь очень тонкая грань. По заданию «из центра» с учетом местных инициатив работают Кавказ, Поволжье, Урал, Северо-Запад и другие филиалы, представляют свои наработки, которые потом тестируются, испытываются в столичном центре компетенции.

– Каковы затраты на эту работу?

– Затраты несопоставимы с тем экономическим эффектом, который получит компания в случае универсальности предоставления услуг – решение окупится за минуты!

– Какие факторы, обстоятельства сдерживают переход операторов на конвергентный биллинг?

– Скорее всего, отсутствие компетенций и риски, с которыми сопряжены любые «переделки». Однако позиция «от добра добра не ищут» – откровенно проигрышная. Я люблю известные слова из «Алисы в стране чудес»: «Чтобы остаться на месте, приходится бежать со всех ног. А чтобы попасть в другое место, надо бежать по крайней мере в два раза быстрее». У нас просто нет вариантов!

Технологии – обслуживающая функция бизнеса. Цель ИТ – дать бизнесу инструмент, причем инструмент универсальный. Конечно, можно сказать бизнесу: мол, вот здесь возьмешь молоток, а там – отвертку, но тогда обе руки будут заняты. А мы должны предоставить бизнесу такой инструмент, чтобы у него хотя бы одна рука была свободна, а значит, было больше шансов победить в конкурентной борьбе.

Подготовили Татьяна ТОЛМАЧЕВА, Наталия КИЙ

Компания	Стратегия
«ВымпелКом»	Компания считает свой биллинг конвергентным, так как система объединяет абонентов всех типов (физические и юридические лица), пользующихся разными услугами связи (мобильная связь, ШПД) с разными методами оплаты (авансовая и кредитная)
«МегаФон»	Модульный подход (см. интервью К. Юнова на с. 52), поставщик «Петер-Сервис»
МТС	Первые шаги миграции на конвергентный биллинг реализуются с момента интеграции «Башсел», у которого имелся фиксированный бизнес. На его базе и был протестирован конвергентный биллинг (запуск конвергентного решения 3-в-1 в Уфе в июле 2009 г.). Это был пробный опыт создания конвергентных предложений с мобильной голосовой связью и ШПД. Промышленный запуск конвергентных решений и связанного с ними биллинга в РФ планируется на вторую половину 2011 г., сначала для корпоративного сегмента, а затем и для физлиц. Основной сценарий перехода на конвергентный биллинг предполагает наличие и ведение единого контракта с клиентом на все услуги, наличие единого лицевого счета, предоставление единого счета на оплату услуг, а также возможность управления своим балансом. Задача выбора биллингового решения не стоит, планируется использовать уже существующее решение ФОРИС от «Ситроникс»
«Скай Линк»	В рамках консолидации регионов ведется переход на единую биллинговую систему. Проект стартовал в 2009 г., сейчас система работает в Московском регионе и Тверской области. Планируется в рамках программы консолидации регионов и унификации бизнес-процессов компании перевести на единое конвергентное решение все региональные компании группы
«Уралсвязьинформ»	«Уралсвязьинформ» и «Петер-Сервис» провели первый этап перевода абонентов ШПД на коммерческое обслуживание в биллинговую систему Peter-Service BIS. В октябре 2010 г. состоялся перевод абонентов безлимитных тарифов Курганского филиала «Уралсвязьинформ». Решение «Петер-Сервис» для обслуживания абонентов ШПД позволяет работать с кредитными и авансовыми абонентами. Поддерживается авторизация по различным атрибутам абонента, выдача квот на трафик и контроль его потребления в режиме онлайн. В биллинговой системе реализовано динамическое управление состоянием сессии абонента, реализован учет разных видов трафика. На первом этапе была реализована поддержка тарифных планов-конструкторов: абонентам доступен набор опций, каждая из которых влияет на условия доступа в сеть. Теперь в биллинговой системе Peter-Service BIS обслуживаются абоненты четырех стандартов: фиксированной связи, мобильной связи, ШПД и IPTV. Таким образом, «Уралсвязьинформ» находится на завершающем этапе конвергенции биллингового решения
TELE2	Конвергентный биллинг внедрен с момента развертывания GSM-сетей (поставщик – «Беркут»)

Источник: данные компаний

Каждый оператор самостоятельно выбирает подходящий именно его бизнесу способ миграции на конвергентную систему (см. таблицу).

Биллинг в калейдоскопе рынка

Рынок конвергентных биллинговых систем высококонкурентен (см. рисунок). В настоящее время свои конвергентные биллинговые решения предлагают более 90 поставщиков.

Традиционные производители телекоммуникационного оборудования всегда имели сильные позиции на рынке платформ интеллектуальных сетей, обеспечивающих контроль в реальном времени за голосовыми вызовами (их часто называют ррераид-биллингом). На сегодняшний день телекоммуникационные вендоры продолжают поддерживать значительную часть абонентской базы мобильной связи. Однако эти компании уже осознали необходимость единой биллинговой платформы, способной обслуживать все типы ррераид- и роstrpaid-услуг. Двое из числа традиционных телекоммуникационных вендоров, Huawei и ZTE, пошли по пути создания собственных конвергентных биллинговых систем; Alcatel-Lucent и NSN – по пути стратегии партнерства с ИТ-вендорами. Ericsson выбрала путь приобретения компании LHS – разработчика решений роstrpaid-биллинга и CRM. Сделка прошла в два этапа: в 2007 г. Ericsson приобрела 84% LHS, а в 2010 г. довела свою долю до 100%.

В свою очередь, ИТ-вендоры идут по пути расширения возможностей в сфере систем обслуживания клиентов посредством приобретений. Ярким примером такого подхода служит Amdocs, которая на протяжении последних 10 лет приобрела более 10 софтверных компаний, специализирующихся на решениях OSS/BSS. Благодаря этой стратегии Amdocs способна сегодня предложить полный спектр подсистем, необходимых для конвергентного биллинга.

Такой подход и процессы консолидации рынка усиливают и без того жесткую конкуренцию на рынке конвергентных систем автоматизированных расчетов. Но операторы от этого только выигрывают.



Текущее развитие рынка показало операторам связи, что конвергентный биллинг становится ключевым условием эффективного управления увеличивающимися объемами трафика и монетизации новых дополнительных сервисов.

Трансформация биллинговой системы ориентирована на совершенствование операций и повышение эффективности. Но для тех компаний, которые понимают силу персонализации абонента, это и возможность контроля за абонентами, и способ влияния на формирование, доставку и использование новых услуг. Операторы, имеющие гибкий инструмент монетизации и управления сетевыми активами, войдут в мир новых возможностей. ИКС

Регулирование 2.0

С точки зрения революционной целесообразности

«NGN – это технологическое решение, появившееся в тот момент, когда трафик данных оказался важнее голосового трафика, а компьютер – важнее телефона».

Н.С. Мардер

(Из выступления на конференции NGN'2009)

Инновационный прорыв означает введение нового регулирования для IP-коммуникаций. Но не толкнем ли мы тем самым отрасль в пропасть?



Александр ГОЛЫШКО,
канд. техн. наук

Караул устал

В прошлый раз мы остановились на реализуемых в развитых странах национальных проектах по предоставлению населению услуг ШПД и на том, что пора перестать защищать инвестиции, сделанные когда-то в TDM. Возьмем для примера хотя бы наш автопром, где мы десятилетиями защищаем инвестиции, а тут и там буквально в «чистом поле» строятся автозаводы, продукция которых откровенно лучше, потому что находится на принципиально ином технологическом уровне. И подавляющее большинство водителей скажут вам, что если сядешь за руль даже старой иномарки, выходить оттуда почему-то не хочется.

Пожалуй, надо совсем не знать нынешних инфокоммуникационных реалий, чтобы не чувствовать: существующее регулирование, исторически «танцующее» от услуг телефонии, не соответствует никаким сегодняшним трендам ИКТ-отрасли. Законодательство не работает и не исполняется, что, собственно, и позволяет отрасли как-то двигаться вперед на инициативе «снизу». Но это говорит лишь о том, что регулятор в таком виде и с такими нормативными документами неэффективен. Ну, разве что запретить может что-нибудь высококонкурентное типа VoIP. А Интернет, как известно, любую цензуру воспринимает как повреждение на линии и ищет обходные маршруты. Поэтому раз уж нельзя или трудно (а, в общем-то, и незачем) перебороть, то путь один – возглавить.

Но как же быть с иерархической структурой TDM, на которой до сих пор базируется наше регулирование, но которую уже давно не строят и не планируют строить ни один сколько-нибудь серьезный оператор? Очевидно, стронуть регулирова-

ние с места быстро не получится – вот уж не первый год представители отраслевого рынка, чиновники и депутаты в сварах с лоббистами пытаются подкорректировать законодательство, дабы хоть немного упростить жизнь операторам в новой реальности, но увы... Мало что доходит до принятых документов. А ждать дальше уже нельзя – весь мир стремительно переходит на новую инфраструктуру, новые социальные взаимодействия и пр. и пр.

Инновационный прорыв можно совершить только одним революционным способом – параллельным введением нового регулирования для IP-коммуникаций, IP-сервисов, доступа к информационным ресурсам на базе сетей передачи данных. Это регулирование может быть очень простым – скажем, представьте себе, что наступила «оттепель», и теперь все можно...

И отныне сеть передачи данных – базовая сеть Российской Федерации, поверх которой существуют все другие наложенные сети и с помощью которой предоставляются все сервисы и подключаются все информационные ресурсы. К примеру, если связь между абонентами осуществляется по IP – пусть это будет без какого-либо зонового принципа или обязательного канала к «разрешенному» магистральному оператору. Пусть можно будет создавать телефонную сеть хоть на всю страну с помощью одного программного коммутатора или с помощью одной платформы IMS. Впрочем, причем тут телефонная сеть? – это уже мультисервисная сеть с услугами FMC. А устаревшие TDM-сети (включая сети с фрагментами TDM), не работающие поверх сетей передачи данных, пусть продолжают регулироваться по-старому.

Пусть их операторы почувствуют упущенную выгоду. Через каких-нибудь пару лет мы удивимся, как быстро они сориентировались. И вот уже услуги Skype через МТС лучше, чем через Verizon или AT&T, а в «Ростелеком» приезжают консультироваться крупнейшие азиатские операторы связи. И устаревшее регулирование отомрет вместе с устаревшими технологиями. А модернизированные сети останутся. Вот так, одним росчерком пера, можно стимулировать модернизацию национальной инфраструктуры. Причем операторы сами во все инвестируют и сами все построят исходя из понятия «инвестиционная привлекательность». И еще договорятся, как сделать это вместе и лучше в рамках саморегулирования «снизу». Не страшно ли это? Не толкаем ли мы регулирование отрасли в пропасть?

Однако в отчете МСЭ «Тенденции в реформировании электросвязи» (март 2010 г.), отразившем опыт более 600 регулирующих органов со всего мира, утверждается, что свободное регулирование ИКТ может эффективно играть роль стимула, привлекая инвестиции в сети и ускоряя экономическое развитие. Финансовый кризис послужил толчком для осознания важности эффективного регулирования. Правительства и представители промышленности сейчас вынуждены пересмотреть свои роли и необходимость государственного вмешательства для обеспечения, среди прочего, развития новой широкополосной экономики. В отчете подчеркивается, что, независимо от изменений в инвестиционной политике, неблагоприятных условий для рыночного капитала и финансовых кризисов, размер инвестиций и разнообразие целей инвесторов гарантируют, что инвестирование в сектор ИКТ по-прежнему будет стабильным и многопрофильным. Создание независимых регуляторов ИКТ является одним из основных вопросов реформы регулирования.

В отчете МСЭ также утверждается, что конвергентные технологии усиливают конкуренцию. Услуги VoIP позволяют кабельным операторам, операторам широкополосной связи и поставщикам беспроводных услуг конкурировать непосредственно друг с другом, а также содействуют развитию конкуренции тем, что разрешают новым провайдерам услуг конкурировать с остальными, не имея собственной сетевой инфраструктуры. Однако изменение технологий и рыночных условий поднимает новые вопросы защиты прав потребителей. Вот тут и нужен будет регулятор, дабы заставить поставщиков услуг повышать качество в виде QoE (Quality of Experience, т.е. восприятия пользователем), которым сегодня, кстати, озабочен каждый серьезный поставщик оборудования связи. И пора озаботить этим операторов.

Но от регулятора сегодня ждут не только борьбы за качество услуг. Прежде всего от него ждут стимулирования развития отрасли, стимулирования инноваций. Стимулирования развития IP-инфраструктуры с доведением ее до каждого гражданина, инкапсуляции в нее функций электронного государства (электронное правительство с получением справок и до-

кументов – лишь первый шаг). Стимулирования появления сервисных инноваций и соответствующего развития бизнеса. Стимулирования формирования конкурентоспособного отечественного производителя. Стимулирования более широкого использования существующей инфраструктуры различными субъектами рынка и пр. и пр. Следует осознать, что в последнее время наиболее новаторские сервисы, приложения и инструментарий не были навязаны «сверху», а пришли «снизу», т.е. оттуда, где есть для этого соответствующие компетенции. И задача регулятора – создать условия, при которых таких инноваций будет больше. Первое требование – хотя бы не мешать. Второе – наносить вред гражданам, работоспособности других сетей и государственным секретам нельзя, а вот мешать чужим доходам, внедряя конкурентные решения, можно. Третье требование выполнить сложнее всего – установление любых барьеров, помимо вытекающих из второго требования, должно быть наказуемо. И еще остается проследить, чтобы в условия обеспечения работоспособности сетей не вписали лишнего.

Инфраструктура как Родина

Предоставление любых инфокоммуникационных услуг подразумевает выделение некоторого (пусть даже самого несущественного) сетевого ресурса, которым, однако, могут одновременно пользоваться сотни миллионов потребителей. И важно, чтобы они смогли им воспользоваться, не «положив» сеть. Осознание того факта, что национальная инфраструктура связи – это основа основ, должно подвигнуть регулятора:

- признать сети передачи данных базовым элементом национальной инфраструктуры, а ШПД – единственным способом доступа в современных инфокоммуникациях;
- реформировать систему лицензирования, выделив в отдельную область лицензирование деятельности по созданию, поддержке и развитию инфраструктуры;
- обсудить вопросы «сетевого нейтралитета» (мы сделаем это позже);
- установить преференции для «держателей инфраструктуры» и разработать систему соответствующих показателей ее состояния, потребностей и динамики (в частности, налоговые льготы для создателей высокоскоростных сетей);
- разработать схему финансирования развития национальной инфокоммуникационной инфраструктуры всеми работающими поверх нее рыночными субъектами (например, за счет оплаты лицензий на предоставление услуг или из фонда универсальной услуги или за счет взносов всех, кто подключается со своим контентом к сетям связи);
- сформировать единые «правила игры» для операторов фиксированной и мобильной связи – т.е. перестать делить сети на фиксированные и мобильные и отменить понятие доминирующего оператора и регулирование его тарифов;

- повысить эффективность использования инфокоммуникационных ресурсов сети связи общего пользования за счет централизованного управления;
- вывести все сооружения и линии связи в отдельную категорию, максимально упростить их развертывание, стимулировать их совместное использование (network sharing) и аутсорсинг;
- понять роль, место и существующие ограничения Интернета для инновационного развития инфокоммуникаций – как минимум необходимо «нарисовать» для Интернета и NGN «дорожную карту» по взаимопроникновению и дополнению;
- стимулировать развитие инфраструктуры cloud computing и grid-сетей с одновременным ростом их информационной безопасности и оптимизацией использования линий связи.

В общем, инфраструктуру надо не только развивать, но и защищать и финансировать. В конце концов, она обязательно будет позиционироваться каждым государством как национальное достояние. И оплачиваться всеми рыночными субъектами с помощью механизма, разработанного регулятором. Ведь за удовольствие нужно платить.

Универсальная услуга

В современных условиях необходима скорейшая реформа универсального обслуживания. Как отмечают ныне не только в Европе, США и Японии, субсидирование традиционной телефонии устарело – нужно стремиться обеспечить население доступным ШПД, поверх которого, как отмечалось ранее, могут быть доставлены любые услуги. Вот, к примеру, Евросоюз вполне может гордиться своими достижениями в области связи, поскольку даже в самых удаленных его уголках большинство людей имеет возможность получить базовые услуги телефонии и доступа к глобальной Сети. Однако представители исполнительной власти ЕС считают, что правила универсального обслуживания, утвержденные в 2002 г., требуют обновления за счет включения в базовый набор, гарантируемый каждому европейцу, широкополосного доступа в Интернет. Про аналогичные процессы, которые идут в США, мы уже говорили.

Чтобы предоставлять ШПД как универсальную услугу, усилий одних только операторов, возможно, будет недостаточно. Тут понадобятся и усилия регулятора, чтобы направить соответствующие инвестиции. Ведь, несмотря на все усилия операторов фиксированной связи и на активное развитие сетей 3G, а в перспективе 4G, «цифровое неравенство» в регионах России сохранится. Операторы приходят преимущественно в места концентрации платежеспособного населения – крупные и средние города, в то время как жители небольших городов и поселков часто остаются неохваченными. Это не только российская проблема, и надеяться лишь на операторов тут нельзя. Для сглаживания «цифрового неравенства» необходима соответствующая государственная инициатива.

Что касается реформы сервисного лицензирования, то она должна быть очень простой – надо объявить, что все лицензии отныне мультисервисные. И наличие или отсутствие каких-либо услуг у оператора – это не регуляторная проблема, а его дополнительная прибыль или упущенная выгода.

Нужно осознать неразрывную связь современного инфокоммуникационного сервиса и информационной безопасности. Или рассматривать информационную безопасность как неотъемлемую составную часть IP-коммуникаций и IP-сервисов. К примеру, какой может быть cloud computing без обеспечения информационной безопасности? В противном случае, как и с инфраструктурой, у одних игроков появится желание собирать деньги и ни за что не отвечать, а другим придется все обеспечивать и довольствоваться оставшимся. Очевидно, необходим концептуальный переход от понятия «сети связи общего пользования» к «сервисной инфраструктуре общего пользования». Следует постепенно стирать различия между так называемыми услугами связи и информационными услугами – ведь для всех них нужны сетевые ресурсы.

И еще об одной грани универсальной услуги. Создатель концепции современного Интернета (в виде WWW) Тим Бернерс-Ли считает, что доступ в Интернет должен быть у каждого жителя планеты, причем бесплатно. Правда, речь идет не о высокоскоростном безлимитном ШПД, а о самом базовом низкоскоростном Интернете, который должен быть доступен абсолютно каждому жителю Земли «по умолчанию». Подобная политика, по мнению изобретателя WWW, – вовсе не популизм, так как современный Интернет многим малоимущим открывает возможности получить образование, услуги врача и просто узнать о ситуации в стране и мире. На сегодня доступ к Интернету имеет лишь пятая часть человечества. А как насчет остальных 80%? По его словам, помочь в этом могут стремительно растущие мобильные сети. Конечно, есть множество людей, которых необходимо сначала обеспечить чистой водой и нормальным питанием, а уже потом говорить об Интернете. Но как бы то ни было, до тех пор пока эти люди не будут включены в состав интернет-сообщества, они не станут членами современного глобального информационного общества. Правда, признал Бернерс-Ли, пока это невозможно, так как даже самые дешевые варианты мобильного Интернета слишком дороги для малоимущих. Впрочем, он видит потенциал для снижения цен, с одной стороны, в развитии инфраструктуры провайдеров, а с другой – в снижении налоговой нагрузки на компании, предоставляющие «Интернет для бедных». В общем, тренд понятен, и, как говорит Бернерс-Ли, те, кто занят развитием информационного общества, должны ориентироваться не только на уже подключенных к Сети (что весьма комфортно для чиновников), а стремиться охватить Интернетом всех граждан. И это действительно важная государственная задача, решаемая не только операторами связи.

Об этих и других задачах – в следующий раз. ИКС

Сеть на аутсорсинге: cui prodest?

Игорь КИРИЛЛОВ

Сотни операторов мобильной связи во всем мире пользуются услугами аутсорсинга в сфере обслуживания и развития своих сетей и получают от этого выгоду. Однако передача сложных систем на обслуживание сторонней компании всегда связана с множеством потенциальных рисков и организационно-технических вопросов.

Обслуживание собственных сетей для крупных операторов связи со временем становится весьма объемным и дорогостоящим процессом. Затраты и сложность выполняемых работ постоянно растут. В ряде случаев гораздо удобнее и выгоднее переложить обслуживание и сопровождение работы сетей на плечи специализированной компании. Тем более что в роли таковых часто выступают известные мировые поставщики телекоммуникационного оборудования – Ericsson, Nokia Siemens Networks, Alcatel-Lucent, Huawei и др. Да и вендоры, судя по всему, готовятся в ближайшие несколько лет изменить структуру своих продаж. Основной доход им будет приносить не реализация отдельных позиций оборудования (базовых станций, коммутаторов и т.д.), а продажа комплексных телекоммуникационных решений, включая предоставление различных профессиональных услуг. При этом обслуживание сетей операторов мобильной связи – один из самых быстрорастущих сегментов телекоммуникационного бизнеса.

Лидерами по аутсорсинговому обслуживанию операторских сетей, занимающими в сумме более 60% мирового рынка, сегодня являются компании Ericsson (около 300 контрактов), Nokia Siemens Networks (более 220 контрактов) и Alcatel-Lucent (90 контрактов). Всего же, по подсчетам аналитиков, в мире заключено свыше тысячи аутсорсинговых контрактов на обслуживание крупных телеком-сетей. В числе компаний, которые уже пользуются такими услугами, – известные мировые и национальные бренды: British Telecom, Deutsche Telekom, VIVACOM (Болгария), Vodafone, China Mobile, Sprint (США), Telefonica, AT&T, Bharti Airtel, BT Global Services и др.

Аналитики прогнозируют, что общемировые расходы только операторов мобильной связи на аутсорсинг обслуживания сетей через пять лет приблизятся к \$30 млрд. И это не удивительно: ведь, как оценивают специалисты исследовательской компании Informa Telecoms & Media, средняя экономия оператора мобильной связи по одному такому контракту доходит до 20–25% его расходов на обслуживание и эксплуатацию сетей. В России рынок аутсорсинговых услуг находится пока в зачаточном состоянии, но первые проекты уже есть и, похоже, они не станут исключением.

Зоны ответственности

В процессе сотрудничества оператора и аутсорсинговой компании крайне важна четкая регламентация

действий и разделение зон ответственности – чем занимается оператор, а за что отвечает сторонняя компания. В части обслуживания операторских сетей мировые поставщики услуг могут выполнять широкий спектр функций. Как показывает практика международных проектов, чем больше работ возьмет на себя аутсорсер, тем больший экономический эффект может быть достигнут.

Аутсорсинг сегодня используется в самых разных сегментах – сетях доступа, транспортных, опорных, сервисных сетях или, что встречается реже, в системе поддержки бизнеса. Функции, обычно передаваемые на аутсорсинг, – дизайн, планирование, развертывание и эксплуатация операторской сети или отдельных ее элементов.

А вот такие ключевые задачи, как стратегическое планирование сети, выбор технологического стандарта для дальнейшего развития, выработку стратегии регионального продвижения, оператор, как правило, оставляет за собой. Также он занимается маркетингом, продажами, рекламой, развитием бренда и т.п.

Зачастую при использовании аутсорсинговой модели самым критичным этапом для всех участников процесса является перевод тех или иных подсистем оператора на внешнее обслуживание. Ведь его нужно произвести не только в сжатые сроки, но и с обязательным сохранением непрерывности бизнес-процессов и текущего уровня обслуживания. В ряде случаев оператор переводит в штат аутсорсинговой компании часть своего персонала (так, например, поступила МТС). При этом предполагается, что производители не будут менять условия трудовых соглашений (но на деле это соблюдается далеко не всегда). Подобная практика, получившая название «аутстаффинг», распространена у западных компаний: в штате Alcatel-Lucent трудятся свыше 16 тыс. специалистов из компаний, взятых на аутсорсинг.

На этапе перехода к аутсорсинговой модели эксплуатации сети приходится решать множество технических и организационных вопросов. В частности, в этот период улаживается всё, что сопряжено с переводом сотрудников (кадровые вопросы, размещение, компенсации, информирование, программы интеграции, дальнейшее повышение квалификации, удержание ключевых специалистов и т.п.), вырабатываются совместные бизнес-процессы, алгоритмы взаимодействия и определяются зоны ответственности. Далее создается модель управления на опера-

ционном уровне, на уровне среднего и высшего менеджмента, план миграции, необходимый инструментарий, средства коммуникации, оборудование. В итоге все решения, связанные с аутсорсингом, должны отвечать не только ожиданиям оператора и поставщика услуг, но и соответствовать требованиям регуляторных структур и органов безопасности.

Кроме того, аутсорсинговая компания, в роли которой, как правило, выступает производитель оборудования с мировым именем, может заниматься дальнейшим развитием и модернизацией сети. Оператор планирует и заказывает необходимый уровень развития, исходя из текущего состояния сети, маркетинговых планов, собственной стратегии, аутсорсер же выступает в роли исполнителя. Например, если оператор ставит задачу расширить покрытие сети, то производитель определяет, сколько базовых станций надо установить, и согласовывает это с оператором. Потом заказчик проверяет соответствие выполненных работ нормам и в случае несоблюдения оговоренных в контракте показателей применяет к аутсорсеру штрафные санкции.

Представители крупных компаний-производителей отмечают, что аутсорсинг в России все более востребован. Например, Валентин Рыжиков, директор департамента управляемых сервисов регионального отделения Huawei по России, Украине и Белоруссии, напоминает, что операторы рассматривают аутсорсинг в качестве одного из путей сокращения затрат, повышения эффективности, а также возможности сосредоточиться на ключевых направлениях бизнеса и инновациях. Сегодня большинство российских операторов отдают на аутсорсинг региональным субподрядчикам лишь небольшую часть эксплуатационной практики. Как правило, это регламентные, ремонтные и аварийно-восстановительные работы для части инфраструктуры транспортной и радиосети, не требующие углубленных профессиональных знаний. Однако состав услуг постепенно расширяется, что делает рынок все более привлекательным для крупных международных компаний, в первую очередь производителей оборудования, которые смогли бы поддержать процесс консолидации и привести в эксплуа-

тационные процессы свои инвестиции и компетенцию.

Азбука партнерства

Для того чтобы сотрудничество оператора и аутсорсера было продуктивным и взаимовыгодным, все действия, круг обязанностей и зоны ответственности должны быть четко задокументированы и одобрены обеими сторонами. Обычно ответственность регламентируется соглашением об уровне сервиса (Service Level Agreement, SLA), детальным описанием состава услуги и матрицей ответственности по всем функциям, связанным с эксплуатацией сети. Кроме того, в специальном разделе договора содержатся подробные описания работ. На этапе оформления сотрудничества определяют несколько десятков ключевых показателей эффективности (Key Performance Indicators, KPI), методики и необходимую инфраструктуру для их измерения. Немаловажным аспектом является разработка штрафных санкций за несоблюдение SLA для обслуживающей компании.

В контракте также указывается периодичность, с которой поставщик услуг отчитывается по показателям KPI. Рассмотрев эти показатели, специальный управляющий комитет оператора принимает в отношении аутсорсинговой компании решение о поощрении либо штрафах.

Отметим, что выбор ключевых показателей эффективности для обслуживания сетей операторов мобильной связи описан в рекомендациях ITU-T серии E.800. Этот документ позволяет оценивать как эффективность работы персонала, так и доступность, стабильность и надежность работы сети.

Для контроля эффективности работы аутсорсера применяются самые разные показатели – как поверхностные (например, сколько минут связи прошло через оператора, сколько было обрывов), так и более детальные – процент успешных вызовов в сети, процент сбоя вызовов, качество хендвера, безаварийность работы сети, скорость устранения аварий и т.д. Однако, как показывает практика, если аутсорсинговая компания своевременно решает все технические проблемы, то поверхностного анализа вполне достаточно.

Общий контроль над работой сети осуществляется круглосуточно из

Контракт

на управление

сетью имеет

смысл заключать

не менее чем

на 5–7 лет

специального центра управления сетью (Network Operation Centre, NOC). Возникающие неполадки устраняются удаленно или путем выезда на место специальной дежурной бригады. Для достижения наивысшей эффективности NOC зачастую разделяют на несколько логических групп – Help Desk, First Level Operations, Second Level Operations и т.д. В каждой группе работают профильные специалисты, действия и зоны ответственности которых, как правило, четко регламентированы.

Выгоды и нюансы

Один из основных факторов, обуславливающих целесообразность аутсорсинга, – повышение рентабельности инвестированного капитала. С точки зрения бизнеса также важна предсказуемость операционных расходов (точно известно, сколько стоит обслуживание сети) и гарантии качества работы. Кроме того, клиент зачастую получает возможность снизить операционные расходы, уменьшить количество необходимых точек контроля, использовать наработанную и постоянно совершенствуемую инфраструктуру производителя для повышения эффективности обслуживания сети. Как показывает мировая практика, нередко удается сэкономить на стандартных процедурах. А в ряде случаев стоимость обслуживания сети фиксируется на несколько лет. Производителям принятие компаний на аутсорсинг также весьма выгодно, поскольку это обеспечивает долгосрочное сотрудничество, финансово привлекательные контракты и гарантированный доход. С точки зрения эффективности для бизнеса, по мнению Павла Мосина, руководителя проектной группы по управляемым сервисам компании Ericsson, контракт на управление сетью имеет смысл заключать не менее чем на 5–7 лет. Поэтому при выборе аутсорсера ключевой вопрос для оператора – не столько «интересная» цена, сколько опыт и надежность партнера. Без этого будет трудно добиться серьезного снижения расходов на обслуживание сети, а значит, и повышения эффективности ее функционирования.

Несмотря на очевидные преимущества, с аутсорсингом связаны и определенные риски. Юрий Рубцов, начальник департамента по управлению качеством функционирования сети и эксплуатационными затратами «МегаФона», полагает, что в России полноценный рынок аутсорсинга пока не создан, мировые производители оборудования только начинают выходить на него и становление рынка будет поэтапным. Один из потенциальных рисков заключается в том, что поскольку в договоре все тонкости предусмотреть невозможно, аутсорсер с помощью юридических уловок может попытаться поднять фактическую стоимость обслуживания.

Кроме того, встречается навязывание ненужных услуг. Например, иногда производители заявляют, что некоторое оборудование не справляется со своими функциями и надо переводить его на новую платформу и запускать новые сервисы. При этом оператор может отчетливо осознавать, что эти сервисы не

Опытная зона покажет...



Андрей Ушацкий,
вице-президент МТС
по технике

– Во время работы опытной зоны мы планируем оценить, как повысится эффективность обслуживания сети МТС на данном участке. Будут учитываться не только показатели, связанные с прямой экономией средств, но и опосредованные выгоды –

применение эффективных технологий вендора, повышение качества работы специалистов и оперативности устранения неполадок, что в конечном итоге ведет к улучшению качества предоставляемых услуг, увеличению генерируемого трафика и росту выручки компании. В России до прошлого года не было практики передачи комплексной эксплуатации и обслуживания сети на аутсорсинг, для нашей страны это инновационное направление. Через год, после завершения опытного проекта, мы проанализируем результаты и примем решение о возможности его тиражирования в других регионах. В процессе подготовки проекта мы консультировались с нашим стратегическим партнером – крупнейшим мировым оператором Vodafone, который уже имеет положительный опыт реализации проектов по аутсорсингу сетей в Индии и Австралии.

окупятся. Но основной риск – это потеря рынка. Если аутсорсинговая компания будет развивать сеть недостаточно высокими темпами, то оператора, которого она обслуживает, обгонят конкуренты. Поэтому необходим жесткий контроль над соблюдением условий контракта. Ведь если не будет возможности оперативно влиять на качество работы сети, можно быстро потерять абонентскую базу. Однако, как правило, все проблемы и возможные риски обсуждаются сообща оператором и аутсорсером. В конечном счете они оба заинтересованы в плодотворном и долгосрочном сотрудничестве.

Первый в России

Аутсорсинг обслуживания операторских сетей приобретает в России вполне конкретные формы. Первые крупные проекты уже запущены. Как известно, весной 2010 г. МТС стала первым отечественным оператором, заключившим контракт о передаче на аутсорсинг функций эксплуатации и обслуживания своей сети. На данном этапе в 16 регионах ЦФО (за исключением Москвы) развернута опытная зона. В рамках проекта МТС и Nokia Siemens Networks распределили между собой зоны ответственности таким образом, что функция управления сетью остается за оператором, а производитель осуществляет регулярное и аварийное обслуживание инфраструктуры, элементов сети и сайтов базовых станций. Обслуживание биллинга и функционирования сервисных платформ на аутсорсинг не передавалось.

В ведении NSN находятся модернизация и развитие подсистем операторской сети в рамках проведения профилактики и ремонта отдельных элементов. Общее управление сетью и ее развитие, определение архитектуры, модернизацию и внедрение новых элементов осуществляет оператор.

При этом производитель является единой точкой ответственности и работает в соответствии с показателями KPI, установленными в соглашении об уровне обслуживания. В контракте МТС и Nokia Siemens Networks детально прописаны все измеримые параметры работы сети, соблюдение которых оператор строго контролирует. Для аутсорсера также действует система бонусов и штрафов в зависимости от текущего качества работы сети.

В ходе проекта 250 сотрудников МТС, непосредственно отвечающих за обслуживание сети, переведены в штат NSN. Оператор сохраняет небольшой внутренний офис для общего управления сетью, взаимодействия с аутсорсером, контроля его работы, а также для выполнения функций, которые невозможно передать сторонней компании (взаимоотношения с регулирующими органами, спецслужбами и т.п.).

Для обеспечения «бесшовного» перехода на аутсорсинговую модель обслуживания сети в МТС по контракту был предусмотрен четырехмесячный переходный период, в течение которого осуществлялась передача функций обслуживания сети и решались организационные задачи (в том числе перевод

персонала). Это позволило оператору обеспечить непрерывность бизнес-процессов и сохранить показатели качества работы сети.



Как отмечают некоторые специалисты, основная проблема российского рынка аутсорсинга состоит в необходимости постоянного контроля над деятельностью аутсорсеров, в отличие от практики стран Запада, где оператор может безбоязненно передать сторонней компании практически все функции по обслуживанию и развитию своей сети связи. С организационной точки зрения для российских операторов наиболее актуально разграничение полномочий и зон ответственности между подрядчиком и оператором. Важны также вопросы выполнения норм госрегулирования, требований по безопасности сети, взаимодействия со спецслужбами.

Тем не менее крупнейшие российские операторы вплотную подошли к порогу, за которым целесообразность передачи на аутсорсинг всех «технических» вопросов, связанных с эксплуатацией и развитием сетей мобильной связи, очевидна. МТС уже пользуется подобными услугами, серьезно рассматривают такую модель работы «Мегафон» и «ВымпелКом», а за лидерами, как правило, тянутся и другие участники рынка – перенимая опыт и исправляя ошибки. **ИКС**

10-я международная конференция

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ

24-25 марта 2011 г.
Москва, Марриотт Аврора

Конференция проводится общественно-государственным объединением «Ассоциация документальной электросвязи» при поддержке Министерства связи и массовых коммуникаций Российской Федерации.

Отличительной особенностью конференций АДЭ является высокий уровень представительства органов государственной власти и бизнеса, а также методологическая стройность, профессионализм, актуальность и практическая направленность программ, в реализации которых участвуют ведущие российские и зарубежные специалисты.

ОСНОВНЫЕ ТЕМЫ КОНФЕРЕНЦИИ:

- Обеспечение информационной безопасности социально значимых услуг
- Стандартизация безопасности телекоммуникаций
- Услуги информационной безопасности операторами связи
- Безопасность и доверие при работе в сети Интернет
- Стандартизация безопасности телекоммуникаций
- Обеспечение повышения уровня безопасности при предоставлении услуг потребителям
- Защита персональных данных (ПДн) в информационных системах операторов связи
- Реализация СОПМ в IP-сетях
- Безопасность облачных вычислений
- Подготовка и аттестация специалистов в области информационной безопасности
- Использование шифровальных (криптографических) средств на ССОП
- Управление идентификацией и конфиденциальностью
- Взаимодействие организаций по стандартизации
- Централизованное управление сетью связи общего пользования (ССОП) в повседневных условиях и в условиях чрезвычайных ситуаций

**ПРИГЛАШАЕМ ВАС НА МЕЖДУНАРОДНЫЙ ФОРУМ 2011 ГОДА ПО
ОБЕСПЕЧЕНИЮ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ!**

Оргкомитет:

тел.: (495) 673-34-28, 673-32-46, 673-48-83, 956-26-12, 995-20-11
факс (495) 673-30-29 • e-mail: info@rans.ru • http://www.rans.ru

Как защитить удаленный банкинг?



Атаки злоумышленников на системы удаленного банковского обслуживания не только не прекращаются, но делаются все более изощренными и дерзкими. Для того чтобы противостоять им, использовавшихся ранее программных комплексов обеспечения безопасности уже явно недостаточно. Выходом может стать применение аппаратных средств защиты ПО.



Олег ГЛЕБОВ,
ведущий
технический
специалист
Rainbow Security

Многие банки сегодня переходят от работы с клиентами «лицом к лицу» к дистанционному обслуживанию. Это позволяет им, сохраняя прежний уровень обслуживания клиентов, сократить разросшиеся штаты, повысить эффективность бизнеса и даже – благодаря упрощению доступа к банковским услугам – заложить фундамент роста клиентской базы.

Однако из-за широкого спектра внешних угроз удаленные банковские сервисы могут дать обратный эффект. Активное применение онлайн-систем и клиентоориентированных программных продуктов предоставило больше возможностей для различного рода мошеннической деятельности. Причем специфика интернет-банкинга зачастую позволяет злоумышленникам использовать сеть для сокрытия следов своих незаконных действий, «растворяясь» вместе с похищенными деньгами.

Мобильный банкинг

Хакеров особенно привлекает возможность онлайн-доступа к банковским сервисам с мобильных устройств (смартфонов, КПК, нетбуков). Помимо традиционных способов мошенничества в сотовых сетях (с помощью SMS-ловушек) и в Интернете, сегодня широко распространены атаки на определенные модели устройств, версии операционных систем и программного обеспечения, направленные на манипуляцию данными на стороне клиента. Невозможность использования в мобильных устройствах аппаратных средств, предлагаемых ранее (USB), обусловила большую уязвимость онлайн-услуг. Предоставляя конечным клиентам программные средства защиты (ЭЦП, сертификаты и ключи под управлением middleware), банкам приходится полагаться на добросовестность пользователей, так как у них нет уверенности в том, что ОС устройств не заражены. Это обстоятельство ведет к тому, что злоумыш-

ленник может заранее подготовить вирусную или иную атаку и дожидаться лишь момента, когда владелец устройства воспользуется услугами банка.

В результате, по данным Центробанка и Ассоциации российских банков, в 2010 г. среди хакерских атак на первое место вышел взлом мобильных систем. Такое положение дел требует внедрения в банковской сфере новых методов защиты мобильных систем и услуг. Недостаточная надежность программных средств защиты ставит вопрос о применении аппаратных комплексов, которые уже активно используются в промышленном секторе.

К таким решениям относятся средства аппаратной защиты мобильных форм-факторов: Compact Flash, Secure Digital и micro Secure Digital. Эти устройства, отличающиеся безотказностью, высоким быстродействием и длительным сроком службы, могут служить одновременно токеном, мобильным хранилищем данных и средством защиты программных продуктов. Тесная интеграция решений на основе карт SD и microSD с мобильными платформами Windows (а в будущем также Android и Apple iOS) может стать стимулом к применению методов защиты, в которых отдельное ПО хранится на карте памяти. А интеграция в PKI-решения, поддержка сертификатов и цифровых подписей позволит предоставить конечным пользователям значительно более высокий уровень безопасности при работе с веб-клиентом банка.

«Банк-клиент»

Отсутствие контроля над системой «банк-клиент» на стороне пользователя и в удаленных пунктах средних банков (крупные банки, имеющие квалифицированную службу безопасности, в большинстве случаев застрахованы от подобных угроз) явилось причиной увеличения числа мошеннических действий в сфере денежных переводов в первой половине 2010 г. Как любой программ-

ный продукт, приложение «банк-клиент» подвержено незаконной модификации вирусным ПО (троянами и др.), подмене сертификатов и ключей. Проводя атаку, встраиваемые хакерские модули инициируют ложные переводы, которые подписываются подлинными сертификатами и ключами конкретного отделения. Установление личности злоумышленника для такого рода действий почти невозможно, поскольку ложные транзакции все чаще путем взлома локальной базы данных привязываются к реальным пользователям системы переводов. В ряде случаев не обеспечивает надежной защиты и использование безопасных хранилищ ключей и сертификатов USB-токенов и OTP-генераторов, так как на зараженной системе пользователь вводит подлинный пароль с OTP-генератора, не зная о факте подмены. Незащищенность приложений класса «банк-клиент» позволяет злоумышленникам сначала создать узконаправленные вирусы для определенных банков, а впоследствии – разработать универсальные методы взлома банковского обеспечения на стороне клиента.

Аппаратные средства на рынке контроля цифровых прав совмещают в себе классический функционал хранилища сертификатов и ключей (токен) с возможностью защиты программных продуктов на базе комплексного шифрования AES. Поставляя конечному пользователю аппаратный ключ (в формфакторах USB, PCMCIA, CF, SD или microSD) взамен

USB-токена, банковская служба безопасности получает на стороне конечного пользователя комплекс, который обеспечит стопроцентную надежность передачи данных и целостность компонентов, поскольку внешнее устройство полностью защищено от нелегального доступа, модификации или подмены данных.

Банкоматы

Использование банкоматов до недавнего времени по праву считалось не только самым распространенным, но и самым безопасным способом удаленного взаимодействия с банком. Согласно требованиям безопасности, установленным Центробанком, средства удаленного обслуживания клиентов должны быть снабжены аппаратным межсетевым экраном, а данные должны передаваться в зашифрованном виде. По своей сути банкомат – это рабочая станция, на которой установлены операционная система (Windows XP и др.), специализированное ПО для взаимодействия с пользователем и средства шифрования трафика (с программным хранением ключей и сертификатов). Атаки на банкоматы могут осуществляться как с помощью встроенных средств удаленного обновления прошивки банкомата с подменой подлинного ПО хакерским, так и путем удаленного заражения ОС банкомата с установкой руткита.

Применение карт промышленного стандарта Compact Flash позволяет защитить ПО банкомата одним устройством. Новые поколения ключей защиты надежно хранят сертификаты, ЭЦП и ключи шифрования, участвуя в процессе защиты передаваемых данных как безопасное внешнее устройство и исполняя роль токена. Установка ОС на дополнительную флэш-память ключа позволяет контролировать отдельные файлы системы и целостное выполнение самой операционной системы непосредственно крипточипом ключа. Расширенный диапазон рабочих температур, средства самодиагностики для увеличения срока службы, высокая скорость чтения и записи (23–24 Мбайт/с) для повышения производительности – эти характеристики решения на основе карт CF обеспечивают уверенность в его безотказности. Работающее в банкомате ПО может быть полностью защищено шифрованием, надежно храниться на флэш-памяти и контролироваться крипточипом (контрольные суммы хранятся локально в устройстве). ИКС

В 2010 г.

среди хакерских

атак на первое

место вышел

взлом мобильных

систем

Кстати...



Появился платежный инструмент на microSD-накопителе

Visa выпустила коммерческую версию мобильного бесконтактного платежного решения In2Pay, представляющего собой карту microSD со специальным ПО и системой защиты данных. Карта устанавливается в смартфон и превращает его в платежный терминал. Устройство протестировано на совместимость с аппаратами BlackBerry Bold 9650, iPhone 3G/3GS/4 и Samsung Vibrant (Galaxy S), работающим на базе Android. В дальнейшем список моделей смартфонов и поддерживаемых ОС будет расширен.

Продукт разработан совместно с компанией DeviceFidelity (США) и опробован в нескольких крупных банках: JP Morgan Chase, Wells Fargo Bank, US Bancorp и Bank of America.

Унифицированные коммуникации, незаметные и вездесущие

В Россию унифицированные коммуникации (УС) пришли с опозданием: их развитие во многом тормозилось недоверием российских корпоративных клиентов к IP-телефонии.

По мнению Михаила КИРИЛЛОВА, руководителя российской группы разработчиков Zyxel X8004, для подобных предубеждений почвы уже нет.



Михаил
КИРИЛЛОВ

– Объем мирового рынка унифицированных коммуникаций, интегрирующих на основе IP средства связи для корпоративных пользователей, аналитики оценивают примерно в \$10 млрд. А что можно сказать о российском сегменте этого рынка?

О значительных объемах рынка УС говорить пока рано, но растет он очень быстро: по нашим оценкам,

через год-два 90% рынка корпоративных АТС емкостью более 50 внутренних линий займут решения на базе IP, предоставляющие естественную основу для унифицированных коммуникаций. При этом у большинства покупателей новых устройств то или иное оборудование корпоративных систем связи уже функционирует. Подвести этот разномасштабный «зоопарк» под один знаменатель, объединить в общую систему унифицированных коммуникаций – чрезвычайно сложная задача, и решить ее могут лишь открытые интерфейсы, стандартизация и гибкий подход, уже сегодня предлагаемые некоторыми из новых решений.

– Как определить, какой класс систем корпоративной связи оптимален для конкретной компании? В каких случаях целесообразно внедрять решения УС?

– Уровень систем связи определяется требуемым уровнем мобильности, доступности и безопасности бизнеса. Если нужна простая «звонилка», то незаменима аналоговая офисная АТС со своими жесткими правилами.

Классические и гибридные IP-АТС подходят предприятиям с разветвленной филиальной сетью и позволяют организовать бесплатную телефонную связь между офисами и единые номерные планы, с трудом реализуемые в рамках традиционной телефонии.

Если же требуются мобильность, многосторонние конференции и селекторные совещания, интеграция разных по своему назначению средств связи и информационных систем в единое целое, автоматизация оповещений и рассылок, массовый обзвон и личный кабинет с доступом к записям разговоров подчиненных и их статистике, то целесообразно посмотреть в сторону УС.

Унифицированные системы коммуникаций применимы в компаниях любого масштаба и отрасли – от турагентств, производственных предприятий и сферы

услуг до учебных учреждений, сферы МЧС, ЖКХ и т.д. К слову, в ноябре 2010 г. наша компания вывела на рынок унифицированную коммуникационную систему X8004, объединившую IP-телефонию (SIP V2), e-mail, факс, SMS, IM, открытые интерфейсы работы с БД, COM-объект, API и HTTP-управление для интеграции с внешними CRM/ERP-приложениями, а также функциональность мощного контакт-центра. Бесплатный программный клиент Z_CTI с модулем телефона позволяет интерактивно работать в личном кабинете и расширяет функциональность обычных и IP-телефонов, добавляя видео, конференции, статистику и аналитику на любое рабочее место. Традиционная проблема как «гибридных», так и «чистых» IP-решений – длительный период обучения (пользователи поначалу часто не способны выполнять даже элементарные операции, к примеру, перевод или удержание звонка, не говоря уже о видео и селекторном совещании, получении статистики и записей своих разговоров) – в X8004 преодолена благодаря графическому интерфейсу Z_CTI и его использованию как отдельно, так и совместно с любым SIP, FXS или USB-телефоном.

– Как Вы оцениваете перспективные направления развития на российском рынке корпоративных систем связи в целом и УС в частности?

– Считаю, что корпоративная голосовая связь в ближайшем будущем продолжит переход к единому информационному пространству, будет становиться все более удобной, незаметной и интегрированной в бизнес-процессы. Сделать это поверх существующего парка оборудования с приемлемыми затратами во многих случаях позволяют открытые стандарты – SIP, SQL, HTTP, XML, COM, API (C#).

Следующая массовая функция – видеоконференции. Я убежден, это должна быть просто новая полезная функция, доступная, не требующая дополнительного лицензирования и дорогостоящего оборудования. Мы планируем реализовать видеоконференции в X8004 к концу лета текущего года в рамках бесплатного обновления.

В более отдаленной перспективе будущее связи – это передача эмоциональной, невербальной составляющей человеческого общения с помощью аудио и видео высокой четкости, 3D, запахов, тактильных и вкусовых ощущений.

На данный же момент основная задача – унифицировать имеющиеся способы корпоративных коммуникаций для эффективного управления бизнес-процессами и взаимодействия с бизнес-клиентами и информационными системами.

Беседовала **Лилия ПАВЛОВА**

МИКРОТЕХ

66 Е. ВОЛЫНКИНА. Прогресс без революций
84 Е. КУРГАШЕВА. Пожар в ЦОДе: чем и как тушить

70 А. СЕМЕНОВ. Перспективы полностью
оптических СКС
73 А. ЖАК. Состав инженерных систем современного ЦОДа

79 Е. ВИШНЕВСКИЙ, М. САЛИН, Т. ТОЛОКОННИКОВ.
Оптимизация гидравлической обвязки
систем холодоснабжения ЦОДов

88 Новые продукты

Прогресс без революций

Евгения ВОЛЫНКИНА

Во многих отраслях «народного хозяйства» задолго до Нового года началось подведение итогов и рисование радужных перспектив на будущее. Завершившийся 2010 г. все с гордостью сравнивают с кризисным 2009-м и с удовлетворением отмечают: «растем, братцы, растем». Не является исключением и рынок ИБП.

Очевидно, что этот рынок всегда разделяет судьбу того оборудования, функционирование которого должны обеспечивать системы бесперебойного питания. Пока в докризисные годы компании увлекались строительством ИТ-инфраструктуры, спрос на ИБП автоматически рос. Когда все резко стали сокращать капитальные затраты и операционные расходы, деликатно называя это «оптимизацией», не избежали секвестирования и системы защиты электропитания.

От оптимизации к росту

В кризисном 2009 г. игроки этого рынка во многом жили за счет проектов, начатых еще до кризиса, но и уже запущенные проекты корректировались в сторону сокращения затрат на оборудование, ПО и системы автоматизированного управления. А некоторые заказчики, как отмечает Денис Андреев, руководитель департамента систем бесперебойного питания компании Landata, не только переходили на самые простые конфигурации, но даже уменьшали в проектах требуемую мощность ИБП. В 2010 г. процесс радикальной «оптимизации» в общем и целом закончился, возобновилось финансирование приостановленных проектов, стали запускаться новые – а с ними вновь пошли заказы на оборудование, в том числе на ИБП, и рынок заметно оживился. Практически все его участники говорят об увеличении количества тендеров и средних объемов закупок по ним. Вполне предсказуемо активизировалась проектная деятельность в финансовых организациях и банках, которые в массе своей пережили кризис без особых потерь. К отраслям, увеличившим объемы закупок ИБП, можно отнести и отрасль телекоммуникаций. «Очень заметное оживление произошло в сегменте так называемых промышленных ИБП, ориентированных на применение в крупных инфраструктурных проектах в энергетике, в том числе атомной, в нефтегазовой отрасли и на транспорте», – добавляет Олег Становов, генеральный директор ООО «Клорайд Рус».



Но и расслабляться поставщикам ИБП не приходится, так как многие проекты, предусматривающие установку такого оборудования, готовятся довольно долго, и за это время «ветер перемен» может внести в них существенные коррективы, а как показывает опыт многих компаний, в случае сокращения ИТ-бюджетов нередко первыми под нож идут средства, выделенные на системы бесперебойного электропитания.

Понятно, что перенесенный стресс не мог не отразиться на запросах заказчиков. Однако представления о том, как изменились интересы клиентов, у участников рынка разнятся, что в принципе неудивительно. Каждый смотрит на происходящее со своей колокольни: производители отслеживают главным образом свое оборудование, да и системные интеграторы тоже имеют определенную вендорную специализацию. Поэтому картина получается довольно пестрой: участники рынка отмечают активный рост спроса на средние и тяжелые решения, на системы ИБП, дружественные к ДГУ (что связано с активным строительством дата-центров), на мало-мощные «коробочные» ИБП для замены выходящих из строя, на ИБП с длительным временем автономной работы, на более сложные решения на базе ИБП. А вот Андрей Маркин, руководитель корпоративных продаж Powercom, в качестве основных современных трендов называет перераспределение долей производителей ИБП среди крупных заказчиков, снижение интереса к ИБП сомнительного качества и ограниченного функционала, а также к необоснованно дорогим моделям.

За что заплатит клиент

Несмотря на официальные объявления об окончании кризиса, влияние его довольно заметно. Во всяком случае, в памяти у клиентов он засел крепко, и потому для многих из них по-прежнему первое место в списке приоритетов занимает цена – и лишь потом идут надежность, компактность, удобство эксплуатации, энергоэффективность и т.д. Благодаря подоб-

ным тенденциям подняли голову производители «второго эшелона». Изменение настроений заказчиков в полной мере почувствовала на себе, например, компания INELT. По словам Евгения Жирнова, руководителя отдела дистрибуции ИБП INELT, объем продаж у компании в 2010 г. увеличился примерно на 70% по сравнению с 2009 г. и на 60% по сравнению с 2008-м.

В целом ситуация на рынке ИБП, как показывают результаты опроса «ИКС», не лишена противоречий. «Цена вопроса», несомненно, остается актуальной, но все же, по мнению большинства специалистов, самыми важными характеристиками для заказчика сейчас становятся надежность, высокая готовность, стабильность параметров и энергоэффективность ИБП. И конечно, расстановка приоритетов сильно зависит от потребностей конкретного заказчика. У домашнего пользователя, которому нужно защитить от сюрпризов электросети свой ПК и прочую бытовую электронику, на первом месте стоит соотношение цена/качество, а потом уже удобство эксплуатации, дружелюбность интерфейса, надежность, качество обеспечения бесперебойной работы защищаемого устройства и дизайн ИБП. А для администратора ЦОДа или ситуационного центра, отмечает А. Маркин, наиболее значимы повышенная надежность, возможность мониторинга, в том числе и удаленного, скорость восстановления работоспособности

системы в случае сбоя или неисправности, дополнительные функциональные и сервисные возможности, уровень энергопотребления. «Российские пользователи, как и пользователи во всем мире, все больше предпочитают ИБП с максимальным классом



Рынок ИБП всегда разделяет судьбу того оборудования, функционирование которого должны обеспечивать системы бесперебойного питания

защиты. Важную роль играет также небольшой вес систем ИБП и компактность, так как часто есть ограничения по допустимому давлению на пол и занимаемой площади», – добавляет Д. Андреев. Растет и спрос на такую нематериальную характеристику, как быстрая поставка ИБП со склада, в том числе ИБП больших мощностей.

Что же касается технологических изменений, на этом фронте революций и революционных ситуаций пока не наблюдается, и производители в соответствии с пожеланиями пользователей и своими представлениями об их благе раскрашивают перья той «синице», которая в руках. Соответственно в ход идут технологии энергосбережения (например, технология IEMi в ИБП от General Electric, позволяющая при падении нагрузки в модульных ИБП

ИБП Eaton

Абсолютная защита Вашей техники



www.eaton.ru/ups

Инновации и технологии, воплощенные в ИБП Eaton серий Pulsar и Powerware, гарантируют нашим клиентам уверенность в надежной и экономичной защите любого оборудования от всех проблем, возникающих в сетях электропитания.



реклама

отключать избыточные модули) или анализа качества электричества в питающей сети, чтобы еще на несколько десятых долей процента повысить КПД, который и так уже почти упирается в потолок (пример – новый ИБП Chloride Trinergy, появившийся в России в марте 2010 г., с КПД до 99%). Совершенствуются системы управления ИБП, которые теперь могут устанавливать режим работы по расписанию, заданному пользователем (с помощью ПО Tripp Lite PowerAlert пользователь может самостоятельно задавать временные диапазоны работы ИБП в нормальном или экономичном режимах). Расши-

Многие айтишники, имея дело с дата-центром, продолжают мыслить категориями старых серверных комнат, где на корректное завершение работы сервера требовалось 15 мин

ряется ассортимент модульных устройств, позволяющих заказчикам собрать ИБП из нужного числа небольших по мощности блоков (система Powercom Vanguard Chain мощностью до 40 кВ·А, построенная из модулей мощностью 6 и 10 кВ·А). Повышается и удобство эксплуатации ИБП (теперь хорошим тоном считается организация всего обслуживания ИБП только с его передней панели), а значит, сокращается время ремонта.

От статики к динамике

В прошедшем году появилась «первая ласточка» в деле внедрения в России дизельных динамических роторных ИБП, давно известных на западных рынках (в Европе их доля составляет примерно 25–30%, в США – 15–20%). Экспериментировать на себе в собственном ЦОДе решила компания КРОК, поэтому неудивительно, что реализацию этого проекта она считает самым ярким событием на российском рынке дата-центров в 2010 г. Тем не менее многие специалисты относятся к динамическим ИБП довольно скептически. Первым пунктом в списке «недостатков» идет цена. Василий Лапшин, руководитель направления продаж GE DE ООО «Абитех», добавляет к нему отсутствие опыта применения таких машин и сложность их обслуживания. Специалисты также отмечают общую неготовность заказчиков и проектировщиков к подобным решениям, которая, по мнению Алексея Волкова,

технического консультанта Tripp Lite Россия, Украина и Беларусь, отчасти объясняется тем, что экономическая выгода и совокупная стоимость владения такой системой в течение 3–5 лет пока неясны.

Конечно, высокая цена и сложность конструкции динамических ИБП не очень способствуют их популяризации, но если идея овладевает массами, технические вопросы отходят на второй план. По мнению Е. Жирнова (INELT), для широкого внедрения этой не-

SMART. Для качества сделано всё

ИБП серии SMART от Powercom:

- Чистая синусоида: электропитание без помех и сбоев
- Добавление внешних батарейных блоков
- Управление через USB и RS-232, внутренний слот для SNMP

Новая модель SMART KING RT (Rack/Tower)

Особенностью модели SMART KING RT является возможность выбора типа установки, для любой задачи и конфигурации рабочего пространства, а также замена батарей в «горячем» режиме. Серия SMART – защита персональных компьютеров, рабочих станций, серверов и другого ответственного оборудования.



традиционной технологии необходим переворот в сознании потребителей и проектировщиков, а для этого на российском рынке должна появиться мощная компания, заинтересованная в продвижении динамических ИБП и готовая вкладывать деньги в их маркетинг и поддержку.

Вообще-то многие специалисты говорят если не о перевороте в сознании заказчиков, то хотя бы о просветительской работе с ними, потому что есть еще немало клиентов, до сих пор указывающих в техническом задании «время автономной работы ИБП – 30 мин». А это сразу отсекает от проекта динамические роторные ИБП (их время автономии составляет 10–20 с, но больше в принципе и не надо, так как за это время должен включиться дизель-генератор). При этом как-то забывают, что в 99% случаев через ИБП подключена только ИТ-нагрузка, а без охлаждения высоконагруженные стойки будут работать лишь пару минут. Многие айтишники, имея дело с дата-центром, продолжают мыслить категориями старых серверных комнат, где на корректное завершение работы сервера требовалось 15 мин. Только теперь в своих требованиях к автономности ИБП они закладываются на время перемещения техника к рубильнику дизеля, если последний не включится автоматически, или на время, необходимое нынешним интеллектуальным кондиционерам для автоматического перехода на питание от стандартной электросети к дизель-генератору или обратно. Но если рассматривать ЦОД как единую систему, обеспечивающую непрерывное предоставление ИТ-сервисов, то длительность времени работы от ИБП особого смысла не имеет, а требования нужно предъявлять к уровню доступности дата-центра, и тогда динамические ИБП получают реальный шанс на рассмотрение в качестве одного из возможных решений в гораздо большем числе проектов. Кроме того, выше уже упоминалось о том, что дружелюбность к ДГУ является большим плюсом для традиционных ИБП и на эту характеристику всегда обращают внимание заказчики, строящие дата-центры. Для динамического же ИБП проблемы синхронизации с ДГУ просто не существует.

В принципе даже энтузиасты динамических ИБП признают, что пока их применение экономически оправдано лишь в дата-центрах мощностью не менее 1 МВт, иначе высокие капитальные затраты все равно перевешивают экономические выгоды отказа от традиционных ИБП (и затрат на замену их аккумуляторных батарей) и от дорогостоящей силовой автоматики. Очевидно, что динамические роторные ИБП могут стать популярнее с появлением в России большего числа мощных ЦОДов.

Сторонники динамических ИБП, кстати, призывают аккуратнее проводить расчеты их экономической эффективности, учитывая CAPEX и OPEX всех компонентов системы бесперебойного питания дата-центра – и ИБП, и ДГУ, и системы управления. В принципе, если заказчик планирует строить мощный ЦОД с высоким уровнем доступности, у него есть прямой



Структурированное кабельное решение

- АйТи-СКС — это сочетание опыта производителя СКС и системного интегратора
- Уникальная программа сервисного обслуживания — АйТи-СКС-сервис
- Электронное документирование СКС
- Расширенные функциональные возможности для офисов

БОЛЬШЕ, ЧЕМ
ПРОСТО СКС



Нам доверяют —
мы гарантируем

- 13 лет с даты выдачи первого гарантийного сертификата
- Более 1 500 000 инсталлированных портов
- Свыше 3000 сертифицированных специалистов

АйТи

Тел.: [495] 974-7979 | 974-7980 | e-mail: info@it.ru | www.it.ru

20 региональных офисов в России

www.it-scs.ru

резон рассматривать такое решение, поскольку уровень готовности и отказоустойчивости у динамических роторных ИБП гораздо выше, чем у традиционных систем бесперебойного питания. Правда, пока существует проблема с обслуживанием этой новой для российского рынка техники, но и она должна вскоре разрешиться: технический директор департамента интеллектуальных зданий компании КРОК Александр Ласый уверен, что в течение 2011 г. в России появится как минимум одна такая сервисная компания. Может быть, тогда «лед тронется». А там, глядишь, в небе появится очередной «журавль» – суперконденсаторы, которые, по мнению ряда специалистов, через два-три года начнут вытеснять динамические ИБП благодаря существенно меньшим габаритам и весу при той же длительности автономной работы.

Что год грядущий нам готовит

В ближайшей же перспективе технологических революций на рынке ИБП не ожидается. Рынок консервативен, это специалисты признают единодушно. Но прогресс, конечно, будет идти, и по традиции особенно быстро в самом интересном для многих производителей сегменте ИБП большой мощности. Прогнозы участников рынка можно резюмировать следующим образом: в отсутствие перспектив технологических прорывов наступивший год будет годом дальнейшей модернизации ИБП и «тюнинга» их характеристик для самых разных потребителей.

Однако прогрессивное посткризисное стремление к эффективности всего и вся имеет и отрицательные последствия, которые могут проявиться уже в наступившем году. Как предупреждает руководитель направления ЦОДов APC by Schneider Electric Олег Зябрев, активная работа производителей над

В 2011 г. рынок ИБП ожидают:

1. Рост общей энергоэффективности ИБП и «зелёности» систем электробезопасности.
2. Нарастание мощности ИБП, построенных на технологии IGBT.
3. Повышение удельной мощности ИБП, т.е. увеличение мощности при сохранении или даже уменьшении габаритов.
4. Модернизация уже существующих ИБП и/или выход новых, специально оптимизированных для работы в составе ЦОДов, т.е. удобных в эксплуатации, обеспечивающих высокое качество электропитания, обладающих минимальной (насколько это возможно) ТСО и высокой отказоустойчивостью.



снижением себестоимости ИБП в некоторых случаях может привести к ухудшению качества и надежности изделий из-за применения более дешевых комплектующих.



Общий настрой участников рынка ИБП остается оптимистичным. Некоторые даже полагают, что рост этого сектора будет обгонять общий рост ИТ-рынка, объясняя это изменением общего отношения потребителей к ИБП. Все больше компаний при модернизации своей инфраструктуры задумываются о надежном и безотказном функционировании системы, ее защите от сбоев и перепадов напряжения. Даже небольшой по обывательским меркам простой оборудования может иметь серьезные последствия для бизнеса компании, поэтому разумно экономить не на современных многофункциональных системах бесперебойного питания – а вместе с ними. ИКС

Перспективы полностью оптических СКС

Проектирование, строительство и эксплуатация СКС становятся заметно проще, если использовать в системе единый тип кабеля. Первый кандидат на роль идеального для всех случаев изделия – оптический кабель. Каков же масштаб его реального применения в разных областях?

Компьютерные информационные системы (ИС), без которых не обходится деятельность современной организации, реализуются в соответствии с известной моделью открытых систем. Принципы же построения их нижнего физического уровня могут различаться. В подавляющем большинстве случаев для этого используются проводные каналы связи; на современном этапе их линейная часть формируется на основе структурированной кабельной системы (СКС).

СКС представляет собой сложный технический объект, на создание которого затрачиваются очень большие финансовые, материальные и людские ресурсы. Естественное стремление минимизировать эти затраты требует одновременного учета множества факторов еще на этапе формирова-



Андрей СЕМЕНОВ,
директор по развитию «АйТи-СКС»

ния основных проектных решений. Как следствие, появляется ряд задач, и одна из них – выбор типа среды передачи для горизонтальной подсистемы (эта задача осложняется тем, что существует много вариантов ее решения). Переход, казалось бы, частной инженерной задачи в новый статус серьезной проблемы обусловлен тем, что на построение горизонтальной подсистемы СКС приходится подавляющая часть (около 85%) всех ресурсов, требуемых для реализации информационной кабельной системы в целом. Кроме того, в кабельной системе горизонтальный кабель представляет собой основной компонент с точки зрения финансовых затрат и наиболее ресурсоемкий – на этапе инсталляции.

В настоящее время техника структурированного каблирования, известная своими хорошими потребительскими качествами, широко используется в самых разных, радикально отличающихся областях. Соответственно существует несколько разновидностей СКС, изначальная адаптация которых к конкретной сфере применения позволяет в полной мере учесть особенности этой сферы. Типы кабелей, разрешенные для применения в процессе построения СКС, приведены в таблице. При этом для любой области использования нормативные документы лишь фиксируют разрешенные типы кабелей. Столь необходимые проектировщику и инженеру однозначные рекомендации даже по предпочтительным областям их применения – за исключением, может быть, предельной протяженности трактов – в публикациях отсутствуют.

Выбор единого типа кабеля

По вполне понятным причинам проще и удобнее проектировать (а впоследствии реализовать и эксплуатировать) такую систему, в которой использован единственный тип кабеля, – проблемы выбора при этом просто не возникает. Однако, чтобы добиться подобного удобства, необходимо предварительно решить не менее важную задачу – обоснованно выделить тот самый единственный тип в довольно обширном списке потенциальных конкурентов.

Само собой разумеется, условия реальных проектов настолько разнообразны, что идеального типа кабеля «на все случаи жизни» просто не существует. В доказательство заметим, что на рынке доступно несколько

серийных типов изделий, конкурирующих между собой, – а это заметно усложняет выбор типа кабеля.

Фактически проблема сводится к ответу на два дополняющих друг друга вопроса: проявятся ли в данных конкретных условиях преимущества определенной конструкции? и насколько значимыми в данных условиях окажутся ее недостатки?

Существенное влияние на результаты выбора оказывает и весьма далекое от собственно техники, но не становящееся от этого менее важным краевое условие: насколько значима для направления передачи и распределения информационных сервисов пользователю та область, в которой конкретное решение оказывается наилучшим по обобщенному критерию технико-экономической эффективности? Иначе говоря, стоит ли вообще выделять его в отдельное направление и не лучше ли из соображений удобства воспользоваться доступными наработками из

Условия реальных проектов настолько разнообразны, что идеального типа кабеля «на все случаи жизни» просто не существует

смежных областей, которые к тому же хорошо знакомы широкому кругу специалистов?

Достоинства и недостатки оптической связи

Первый кандидат на роль идеального изделия для информационной проводки – оптический кабель. Едва ли целесообразно снова приводить на страницах «ИКС» впечатляющие показатели дальности связи и скорости передачи, достигнутые на линиях оптической связи в массовых проектах. На серийной оптической элементной базе вполне реализуемы и окончательные участки линии непосредственно до абонента в сетях доступа или до пользователя в офисе при построении кабельных систем класса «волокно до рабочего места» – что подтверждается практикой проектов.

При рассмотрении оптического кабеля как среды передачи обычно подчеркивают его преимущества. Однако в контексте задачи поиска предпочтительного типа линейных изделий важно помнить и о довольно многочисленных недостатках этой техники (которые зачастую являются прямым продолжением ее достоинств).

Отметим, что оптическая техника сама по себе неоднородна. На коротких расстояниях, характерных для подсистемы внутренних магистралей СКС (и тем более для горизонтальной подсистемы), предпочтительны многомодовые решения. Не уступая своим одномодовым аналогам по скорости, они имеют заметное преимущество в стоимости в случае линий небольшой протяженности. На длинных линиях подсистемы внешних магистралей из-за существенно меньших дисперсионных искажений целесообразно использовать одномодовую технику. Одномодовые и

Типы кабелей, разрешенных для применения в СКС

Тип СКС	Симметричный	Оптический кварцевый	Оптический кварц-полимерный	Оптический полимерный	Коаксиальный
Офисная	Х	Х			
Для ЦОД	Х	Х			Х
Промышленная	Х	Х	Х	Х	
Бытовая	Х				Х

многомодовые кабели обязательно следует рассматривать отдельно, потому что при формировании составных трактов их нельзя соединять напрямую без промежуточного активного устройства (класса не ниже преобразователя среды). Конкретные расчеты показывают, что граница целесообразности при переходе от многомодовой техники к одномодовой находится в интервале от 600 до примерно 1200 м, причем по мере наращивания скорости передачи критическая длина имеет явную тенденцию к снижению. Последнее обусловлено как большей стоимостью высокоскоростной электроники, так и заметно растущими затратами на широкополосные многомодовые волоконные световоды категорий OM3 и OM4.

СКС и другие области применения оптических линий

Значимое влияние на выбор типа элементной базы оказывают и смежные области. В данном случае необходимо принимать во внимание технические направления, в которых используются те же или функционально близкие технологии. И первое из таких направлений – быстро развивающиеся в последнее время ЦОДы.

На масштаб применения оптической техники в ЦОДах существенно влияют следующие факторы. Во-первых, ЦОД как технический объект не обслуживает непосредственно пользователей, т.е. в нем отсутствуют

По вполне понятным причинам проще и удобнее проектировать – а впоследствии реализовать и эксплуатировать – систему, в которой использован единственный тип кабеля

известные ограничения системы «человек – машина», определяющие предельные скорости передачи информации. Далее, в ЦОДах поддержка телефонной сети предприятия не является первостепенной задачей и соответственно не востребована технология PoE. Задача обеспечения активного сетевого оборудования питающим напряжением в данном случае решается иными методами. Оптические кабели обладают заметно лучшими массогабаритными характеристиками по сравнению с симметричными, что упрощает создание системы охлаждения активного сетевого оборудования. И наконец, при работе на длинных линиях энергопотребление в случае оптических интерфейсов существенно меньше, т.е. легче строить «зеленые» ЦОДы.

Необходимо, однако, учитывать следующие обстоятельства. Во-первых, в предыдущих публикациях (см. «ИКС» №10'2010, с. 88) мы сделали вывод о том, что ожидаемый объем рынка СКС категории ба не превысит одной трети от рынка офисных СКС. Во-вторых, ранее («ИКС» № 7-8'2010, с. 86) мы приводили статистические данные по реально реализованным проектам. Из них следует, что средняя протяженность горизонтальной линии в ЦОДе не превышает 30 м, что обусловлено ком-

Достоинства и недостатки линий оптической связи

 	 
Прекрасные массогабаритные показатели	Относительно малая стойкость к механическим воздействиям, чувствительность к загрязнениям
Гальваническая развязка	Нет возможности централизованного дистанционного питания телефонных аппаратов
Высокая информационная пропускная способность	Нет преимуществ по скорости передачи на линиях небольшой протяженности

пактностью этого объекта – из-за естественного стремления к экономии дорогой площади со сложной инженерной «начинкой» (система гарантированного электропитания, прецизионного кондиционирования и т.д.). На таких расстояниях сетевой интерфейс, работающий по симметричному кабелю, функционирует в режиме short reach. Иными словами, протяженность большей части линий такова, что оптическая техника не дает значимых преимуществ в энергопотреблении.

В-третьих, в ЦОДах востребована скорость 40 Гбит/с, основная область применения которой – линии связи между серверами. В настоящее время такая скорость передачи уверенно может быть реализована на современной медножильной технике, которая остается более дешевой по сравнению с оптической. Фактически основным фактором, сдерживающим ее широкое внедрение, является отсутствие официальных стандартов, принятие которых ожидается в ближайшем будущем.

Таким образом, несмотря на заметно большую потенциальную нишу использования оптических решений в ЦОДах, по масштабам применения их нельзя даже сравнивать с классическими СКС офисного назначения ни в настоящее время, ни в обозримой перспективе.

Сети доступа

Необходимость учитывать сети доступа в данном контексте обусловлена тем, что они бесшовным образом стыкуются с ИС предприятия за счет того, что в них уже сейчас доминирует технология Ethernet.

Сеть доступа может быть построена на разных принципах, например, с привлечением уже построенной ранее инфраструктуры. С точки зрения массовости и глубины охвата имеющегося жилого фонда вне конкуренции оказываются симметричные кабели и технология xDSL. Определенные перспективы имеют и решения, основанные на наложении такой сети на волоконно-коаксиальные телевизионные сети.

Сети доступа, создаваемые заново, в подавляющем большинстве случаев строятся на базе оптической техники. Среднюю протяженность соединительной линии в этой части сети электросвязи можно принять равной примерно 1 км. В этой ситуации начинают в

полной мере проявляться достоинства одномодовой оптической техники (в форме PON или обычного Ethernet). В обоих случаях используется одноволоконная схема линии, что несколько улучшает экономические параметры проекта в целом. Уже одна эта особенность по крайней мере затрудняет стыковку сети доступа с ИС предприятия, в которой традиционно применяются классические двухволоконные линии.

Количество пользователей сетей доступа может заметно превышать количество пользователей ИС (как правило, индивидуальный доступ к последней необходим только управляющему звену компаний или организаций). Среди экономически активного населения соотношение рабочих (включая производственный и непромышленный сектор) и служащих принимается равным 4:1. При оценке количества линий в полностью построенных сетях доступа в первом приближении его можно считать равным числу домовладений. Поэтому даже без учета того, что в условиях всеобщей занятости на одно домовладение приходится по два потенциальных пользователя ресурсов ИС, получаем, что количество линий сетей доступа может превышать число портов СКС в разы, но вряд ли на порядок.

При оценке влияния техники сетей доступа на СКС необходимо учитывать, что основной объем трафика, создаваемого и принимаемого пользователями ИС, не выходит за ее пределы. Это внутренние телефонные звонки, обращения к локальным серверам, электронный документооборот и некоторые иные сервисы. Для оптимизации подобной структуры целесообразно подключать к сети доступа не отдельного пользователя, а всю ИС, например, с помощью учрежденческой АТС в телефонной подсистеме.

Из представленных выше соображений прямо вытекает, что особенности построения сети доступа при всей их массовости не оказывают значимого влияния на технические решения, используемые при построении СКС общего применения.



В обозримой перспективе полностью оптические СКС офисного назначения не будут играть не только преобладающей, но даже заметно большей роли. Они будут применяться только в случае особых требований к устойчивости к внешним электромагнитным помехам и к защите от несанкционированного доступа к конфиденциальной информации, т.е. в тех нишевых ситуациях, когда техника оптической связи не имеет конкурентов.

Объемы применения средств оптической связи в проектах построения СКС будут расти. Локомотивом данной тенденции объективно являются ЦОДы, где данный показатель может даже несколько превысить 50%. Рост будет иметь эволюционный характер и по темпам в годовом исчислении даже в условиях ненасыщенного рынка ЦОДов не превысит нескольких процентов.

С учетом относительной малости рынка СКС для ЦОДов по сравнению с сегментом аналогичных систем офисного назначения относительная доля оптических решений в технике структурированного каблирования вряд ли даже в пределе превысит 30–40%.

Влияние сетей доступа на масштабы применения оптических решений при построении СКС офисного типа – наиболее значимых для отрасли – можно считать пренебрежимо малым. ИКС

Состав инженерных систем современного ЦОДа

Инфраструктура «идеального» дата-центра – это совокупность тесно взаимодействующих комплексов различных инженерных систем, состав которых задается, в частности, рейтингом ЦОДа по классификации Uptime Institute.

Название статьи у большинства читателей вызовет, вероятно, удивление. Действительно, что нового может сказать автор по этой теме? Однако, как показывает практика, в представлении большого количества заказчиков, ЦОД – это практически любое помещение, в котором устанавливается некоторое количество шкафов с активным оборудованием и организуется «малый джентльменский набор» – электропитание из ближайшего электрощита, источник (или несколько источников) бесперебойного питания мощностью 1,5–3 кВ·А, пара бытовых кондиционеров сплит-системы, новый замок на дверь и пожарная

сигнализация. «Большой джентльменский набор» может дополнительно включать фальшпол, газовое пожаротушение и контроль доступа. Безусловно, это несколько карикатурное описание типичных требований некоторых заказчиков, однако правильно говорится: в каждой шутке есть только доля шутки.



Александр ЖАК,
технический директор
компании «ДатаДом»



В статье рассматривается состав инженерных систем «идеального» ЦОДа, соответствующего сводному рейтингу Tier IV – Gold по классификации Uptime Institute*. Дополнительно для каждой системы ориентировочно указан минимальный рейтинг ЦОДа, начиная с которого данная система считается необходимой для инфраструктуры. Требования наличия той или иной системы относятся исключительно к ЦОДам и не вступают в противоречие с российскими общестроительными нормами.

Архитектурно-планировочное решение ЦОДа

Чтобы лучше представлять себе назначение инженерных систем и их взаимосвязи, приведем архитектурно-планировочное решение ЦОДа по стандарту ANSI/TIA-942-2005 Telecommunications Infrastructure Standard for Data Centers (рис. 1).

Область 0 – вся территория ЦОДа (кампус). Подразумевает ограждение по периметру, наличие охранной зоны и средств охраны периметра, проходных, ворот для проезда транспорта с контрольно-пропускными пунктами. В области 0 обычно также располагаются площадки-анклавы области 2, на которых размещается технологическое оборудование ЦОДа (чиллеры, машинные генераторы, контуры заземления и т.д.).

Область 1 – здание (строение) или группа зданий, специально спроектированных и построенных для размещения ЦОДа.

Область 2 – собственно дата-центр. Между его областями существуют связи (физические и логические), отраженные на рис. 1.

С некоторой долей погрешности можно сказать, что уровень Tier I определяет минимальные требования к области 11 (серверные, машинные залы) и не рассматривает другие области. Требования уровня Tier II относятся к области 2 со всеми ее составляющими (серверные + технологические системы). Требования уровня Tier III касаются области 1 (серверные + технологические системы + здание в целом). И наконец, требования уровня Tier IV относятся ко всей территории ЦОДа в целом (область 0).

С точки зрения инженерно-технологической инфраструктуры (ИТИС) современный ЦОД – это совокупность тесно взаимодействующих комплексов различных инженерных систем. В ИТИС «идеального» ЦОДа (рис. 2) входят следующие комплексы: систем безопасности (КСБ), систем противопожарной защиты (КСПЗ), систем сервиса (КСС), систем электрооборудования (КСЭ), инженерно-технических систем (КИТС), систем многофункциональных залов (КСМЗ), а также комплекс обеспечения, обслуживания и технической поддержки (КОТП).

Чрезвычайно важная для «идеального» ЦОДа задача – обеспечение физической безопасности, поэтому еще до начала рабочего проектирования дата-центра необходимо определить количество и назначение зон ответственности на территории ЦОДа и их взаимное расположение (общая площадь, анклавы), сформировать политики физической безопасности каждой зоны, включая анклавы.

Зарубежные нормативные документы, в частности, упомянутый в начале статьи стандарт Operational Sustainability, формулируют требования к охране и доступу как «контролируемый доступ» без подробной детализации. В российских нормативных документах эти требования сформулированы точнее и строже.

Согласно документу РД 78.36.003-2002/МВД России, территории с ограниченным доступом, области и помещения объектов группы А с контролируемым входом (к которым относится ЦОД), подразделяются на три группы зон ответственности (три зоны ограничения доступа).

Первая зона (группа зон ответственности 1: области 0, 1, 3, 4 на рис. 1, исключая всю область 2) – контролируемая, предполагает свободное передвижение и пребывание персонала, представителей клиентов, посетителей после соответствующего контроля на входе. Выполняет функции охранного периметра, охватывающего все области ЦОДа.

Вторая зона (группа зон ответственности 2: область 2, исключая область 11) – усиленно контролируемая и охраняемая, предусматривает передвижение и пребывание определенного круга сотрудников и представителей клиентов после соответствующего контроля. Вторая зона – это площадь, на которой располагаются оборудование инженерно-технологической инфраструктуры ЦОДа (СГЭ, СНЭ, САП, СПМ и др., см. рис. 2),

*Определение сводного рейтинга ЦОДа – см. стандарты Data Center Site Infrastructure Tier Standard: Topology, Uptime Institute, LLC, 2010 и Data Center Site Infrastructure. Tier Standard: Operational Sustainability, Uptime Institute, LLC, 2010.

пост управления и мониторинга ИТИС. К группе зон ответственности 2 относятся также внешние площадки (анклавы), на которых устанавливается оборудование ИТИС (контур технологического заземления, ДГУ, дополнительные топливные емкости, чиллеры, драйверы и т.д.).

Третья зона (группа зон ответственности 3: область 11) – усиленно контролируемая, охраняемая и защищаемая, предусматривает пребывание строго ограниченного круга лиц. Доступ других лиц в эти помещения возможен только в сопровождении специально допущенных работников. Третья зона – площадь, на которой располагается серверное и коммутационное оборудование ЦОДа, а также хранилища данных, в том числе сейфы с носителями резервных копий информации.

Группы зон ответственности 2 и 3 должны быть физически отделены друг от друга, располагаться в разных помещениях и иметь отдельные входы. Возможно расположение группы зон ответственности 3 на территории (внутри) группы зон ответственности 2 при обязательном физическом разделении этих зон пожаровзломостойкими стенами с входами (дверями), оснащенными СКУД.

Комплексы систем ЦОДа: функции и термины

Непрерывный рост требований к надежности и бесперебойности работы современного ЦОДа влечет за собой столь же непрерывное совершенствование существующих технологических инженерных систем и по-

явление новых, еще недавно совершенно нетипичных для ЦОДов. Досмотровая техника, парковки, защитные оболочки, система телефонизации кампуса, спутниковые каналы связи, специально оборудованные конференц-залы, отопление, водопровод и канализация – вот некоторые совершенно нехарактерные для ЦОДа пятилетней давности системы, которые потребуются при строительстве современного дата-центра.

Ниже системы, входящие в состав ЦОДа, кратко описаны по комплексам (см. также рис. 2). В скобках указаны уровни надежности ЦОД (Tier), для которых данные системы являются необходимыми.

Безопасность

Комплекс систем безопасности (КСБ) включает в себя следующие системы.

СОТС – система охранной и тревожной сигнализации, обеспечивает охрану территории ЦОДа, включая все зоны ответственности (Tier I–IV).

СКУД – система контроля и управления доступом, предназначена для контроля и санкционирования доступа людей в зоны ответственности 2 и 3 (Tier II–IV).

ДТ – досмотровая техника, служит для контроля наличия у людей несанкционированных предметов, досмотра транспорта (Tier IV).

СТН – система телевизионного наблюдения, предназначена для круглосуточного визуального контроля территории и помещений ЦОДа (всех зон ответственности) и технологических процессов (Tier III–IV).

Б и з н е с - п а р т н е р

Проектирование ЦОДов: правильно, хорошо и надежно



Максим ИВАНОВ,
генеральный директор
ADM Partnership

Большинство участников рынка дата-центров сегодня четко отличают серверную комнату от центра обработки данных. Три основных критерия качества современного ЦОДа – «правильно», «хорошо» и «надежно». Отсюда и требования к составляющим комплекса, его проектированию и строительству.

Рассмотрим каждый из этих критериев с точки зрения компонентов ЦОДа. «Правильно» – этот аспект предполагает буквально правильно спроектированное системное решение, включающее полный набор необходимых компонентов и подсистем, в том числе и технологических, которые напрямую не ассоциируются с ЦОДом, но относятся к системам здания. Системы здания влияют на работу ЦОДа самым непосредственным образом, и игнорировать их как неотъемлемый системный фактор будет ошибочно.

«Хорошо» означает высокий уровень реализации проектных решений. Важно отметить, что уровень надежности любого ЦОДа определяется наименее надежным компонентом или системой. И это касается не только уровня резервирования, но и качества реализации конкретного узла системы. Кроме того, в понятие «хорошо» входит и продуманность проектных решений с точки зрения эксплуатации и удобства обслуживания оборудования и систем (включая регламентные работы и устранение возможных аварий). Системный подход в данном контексте подразумевает также учет влияния одной подсистемы (компонента) на другую.

Критерий качества «надежно» многогранен. С одной стороны, весь набор компонентов ЦОДа в целом должен обеспечивать необходимый уровень функциональной устойчивости. С другой стороны, надежность – это и обратная сторона продуманности проектных решений в ключе возможного развития ЦОДа в направлении увеличения мощности, адаптации к новым задачам или повышения функциональной устойчивости. Независимо от типа (корпоративный или коммерческий), дата-центр – это объект серьезных капитальных вложений, и от того, насколько эти вложения продуманы (в том числе и с точки зрения состава компонентов подсистем и их увязки друг с другом) зависит эффективность работы ЦОДа.

Учитывая, что для современных ЦОДов характерна тенденция к усложнению и увеличению потребления электроэнергии, постановка задачи и выполнение проектирования с учетом правильного и полного состава системы становится ключом к успеху в любом проекте дата-центра.



СИБ – система информационной безопасности, обеспечивает максимально возможный уровень защиты конфиденциальной информации, хранящейся и перемещающейся в компьютерных сетях ЦОДа. Требования к ней формулируются согласно документам ФСТЭК России. Как правило, необходима с уровня Tier III.

Средства физической защиты (защитные оболочки, сейфы и хранилища) рассмотрены в «ИКС» №10'2010 (с. 84) и 11'2010 (с. 83).

СКП – система контроля за протечками, предназначена для обнаружения нештатного появления жидкости и автоматического управления клапанами подачи технологической воды (Tier II–IV).

СМШ – система мониторинга шкафов, отвечает за контроль температуры, влажности, скорости воздушного потока внутри шкафов с активным оборудованием (область 11), регистрацию нештатных ситуаций (пожар, открытие дверей и т.п.) (Tier II–IV).

СИС – интерком и селектор, обеспечивают проводную связь между постами и/или техническими помещениями, службами и диспетчерской на территории ЦОДа (Tier III–IV).

ЦДП – центральный диспетчерский пост. Программно-аппаратный комплекс, предназначенный для объединения в единое целое систем ИТИС ЦОДа с целью оптимизации управления всеми входящими системами (Tier II–IV).

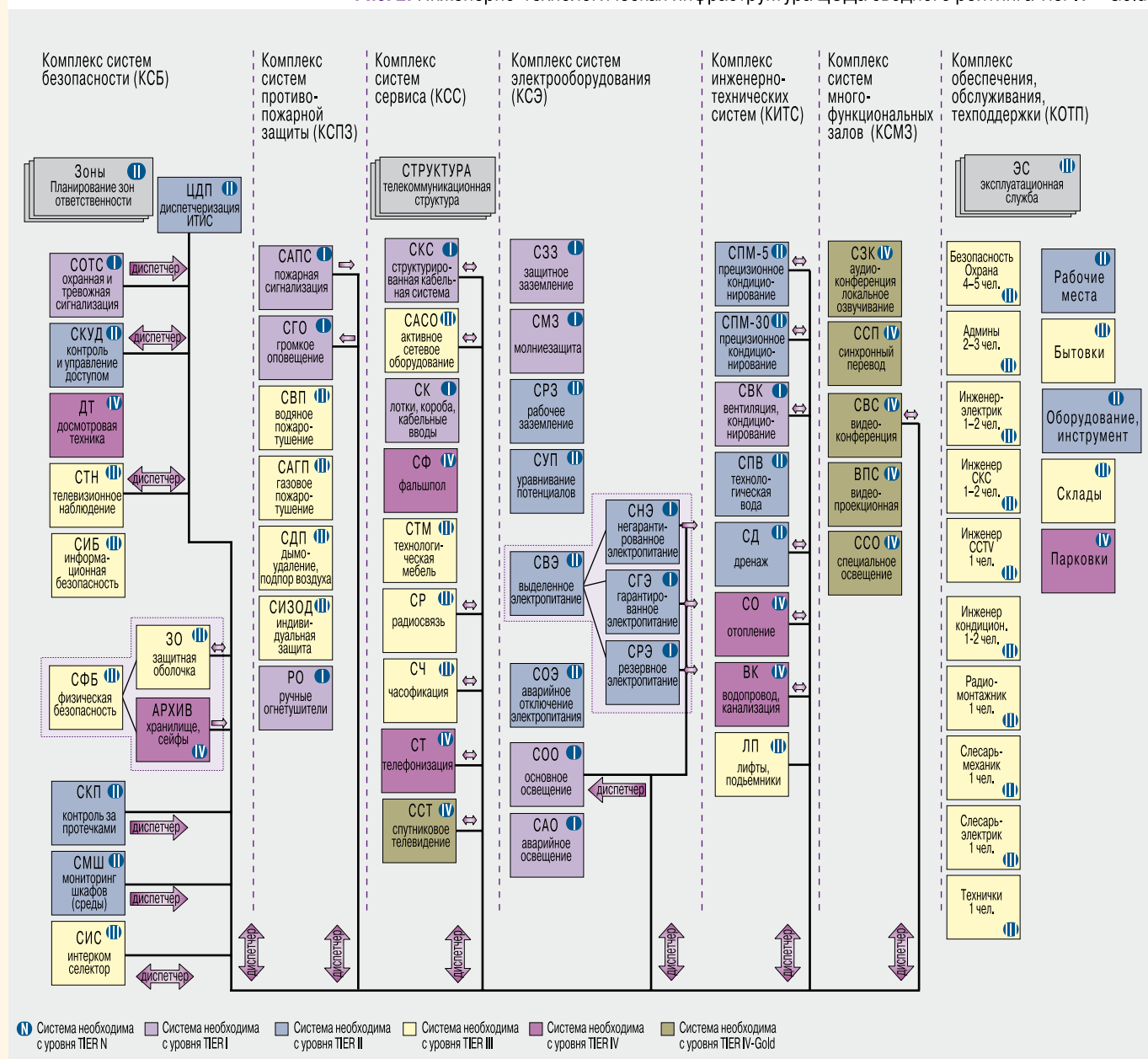
Противопожарная защита

В комплекс систем противопожарной защиты (КСПЗ) входят следующие компоненты.

САПС – система автоматической пожарной сигнализации, обеспечивает противопожарную охрану территории ЦОДа и материальных ценностей (Tier I–IV).

СГО – система громкого оповещения о пожаре и управления эвакуацией, отвечает за оповещение людей о пожаре, чрезвычайных происшествиях (Tier I–IV).

Рис. 2. Инженерно-технологическая инфраструктура ЦОДа сводного рейтинга Tier IV – Gold



СВП – система водяного пожаротушения, предназначена для локального тушения пожаров и охлаждения строительных конструкций в области 1, за исключением областей 4, 6–9, 11 (Tier III–IV).

САГП – система автоматического газового пожаротушения, обеспечивает противопожарную защиту помещений областей 4, 6–9, 11 (Tier III–IV).

СДП – система дымоудаления и подпора воздуха, предотвращает распространение огня, обеспечивает вентиляцию помещений и удаление продуктов горения после ликвидации пожара (Tier III–IV).

СИЗОД – средства индивидуальной защиты органов дыхания: самоспасатели, изолирующие противогазы (Tier III–IV).

РО – ручные огнетушители (Tier I–IV).

Сервис

Комплекс систем сервиса (КСС) состоит из следующих систем.

СКС – структурированная кабельная система. Обеспечивает передачу информации по стандартным протоколам систем связи, а также передачу телекоммуникационных и информационных сигналов (Tier I–IV).

САСО – система активного сетевого оборудования. Организует обмен информацией между различными абонентами системы СКС, включая преобразование, шифрование, пакетирование, маршрутизацию, передачу цифровой, речевой и видеоинформации (Tier III–IV).

СК – система кабелепроводов (лотки и короба). Ее назначение – размещение, упорядочение, защита и скрытие кабелей, проводов и коммуникаций всех инженерных систем (Tier I–IV).

СФ – система фальшпола. Предназначена для равномерного распределения веса оборудования по площади помещений ЦОДа, размещения коммуникаций, подачи кондиционируемого воздуха к стойкам с оборудованием (Tier II–IV).

СТМ – система мебели технологических рабочих мест, оптимизирует использование пространства над рабочим местом, помогает правильно организовать рабочее место (Tier III–IV).

СП – система оперативной радиосвязи. Обеспечивает личный состав службы безопасности беспроводной связью на территории объекта между собой и с ЦДП (Tier III–IV).

СЧ – система электрочасофикации, отображает единое и точное время и информацию в пределах ЦОДа. Синхронизируется от сигналов точного времени по радиоканалу DCF 77, по сигналу GPS со спутника (Tier III–IV).

СТ – система телефонной связи, обеспечивает территорию ЦОДа адресной голосовой (телефонной) связью (Tier IV).

ССТ – система спутникового телевидения. Нужна исключительно для достижения суммарного рейтинга ЦОДа Tier IV – Gold и не влияет на надежность функционирования ЦОДа.

Электрооборудование

В комплекс систем электрооборудования (КСЭ) входят следующие системы.

СЗЗ – система защитного заземления здания (контур заземления); сопротивление растеканию тока не более 4 Ом (Tier I–IV).

СМЗ – система молниезащиты. Здание ЦОДа должно быть оборудовано устройствами молниезащиты II категории с зоной защиты от поражения «Б» (СО 153-34.21.122-2003) (Tier I–IV).

СПЗ – система рабоче-защитного заземления. Отдельный второй контур телекоммуникационного заземления, с сопротивлением растеканию тока не более 1 Ом. Возможна организация третьего отдельного контура измерительного заземления (Tier II–IV).

СУП – система уравнивания потенциалов. Помещения ЦОДов (область 2 за исключением области 10) оборудуются устройством локального уравнивания потенциалов по Приложению В3 ГОСТ Р 50571.21-2000 (МЭК 60364-5-548-96) (Tier II–IV).

СВЭ – система выделенного электропитания. Служит для организации электропитания выделенных помещений и включает три составляющие: систему негарантированного электропитания (СНЭ), систему гарантированного электропитания (СГЭ) и систему резервного электропитания (СРЭ) (Tier II–IV).

СГЭ – система гарантированного электропитания (часть системы СВЭ). Обеспечивает электроэнергией потребителей, чувствительных к перебоям в электропитании (на базе ИБП и аккумуляторов). Время автономной работы – от нескольких минут до нескольких часов (Tier II–IV).

СРЭ – система резервного электропитания (часть системы СВЭ). Предназначена для автономного электропитания потребителей при продолжительных нарушениях в сетях общего назначения (на базе независимого машинного генератора электроэнергии). Время автономной работы ограничено только запасами топлива. Необходима с уровня Tier II; для уровней Tier III и IV является основной системой электропитания.

СОЭ – система аварийного отключения электропитания. Экстренно прекращает функционирование ЦОДа путем принудительного отключения электропитания (Tier II–IV).

СОО – система основного электрического освещения. Ее назначение – искусственное круглосуточное освещение помещений ЦОДа (Tier I–IV).

САО – система аварийного электрического освещения. Поддерживает искусственное освещение помещений ЦОДа в течение заданного времени при отказе всех систем электропитания – основного и резервного, в том числе ИБП (Tier I–IV).

Инженерно-технические системы

В состав комплекса инженерно-технических систем (КИТС) входят следующие компоненты.

СПМ-5 – система прецизионного кондиционирования (микроклимата) в ЦОДе, предназначенная для создания и автоматического регулирования параметров воздуха в закрытых технологических помещениях при подаче кондиционированного воздуха под фальшпол (Tier II–IV).

СПМ-30 – система прецизионного кондиционирования (микроклимата), предназначенная для снятия теплопритоков 10–30 кВт от одного шкафа с активным оборудованием. Строится на базе герметичных водоохлаждаемых шкафов и холодильной машины (чиллера) (Tier II–IV).

СВК – система вентиляции и кондиционирования в помещениях ЦОДа с постоянными рабочими местами. Организу-

ет воздухообмен для заданного состояния воздушной среды в помещениях и на рабочих местах (Tier I–IV).

СПВ – система подготовки технологической воды, отвечает за подготовку обессоленной воды для парогенераторов, входящих в состав систем контроля климата и кондиционирования (Tier II–IV).

СД – система дренажа для отвода конденсата систем прецизионного кондиционирования, ликвидации последствий протечек (Tier II–IV).

СО – система отопления, обеспечивает заданную температуру воздуха в помещениях и на рабочих местах (Tier IV).

ВК – водопровод и канализация. Обеспечивают снабжение ЦОДа водой для технологических и собственных хозяйственно-бытовых нужд (Tier IV).

ЛП – технологические лифты и подъемники. Предназначены для подъема технологического оборудования ЦОДа и других грузов (Tier III–IV).

Системы многофункциональных залов

КСМЗ – комплекс систем многофункциональных залов, предназначен исключительно для того, чтобы достичь суммарного рейтинга ЦОДа Tier IV – Gold. На надежность функционирования ЦОДа он не влияет.

Обслуживание и техническая поддержка

КОТП – комплекс обеспечения, обслуживания и технической поддержки. Включает персонал, обеспечивающий текущую эксплуатацию ЦОДа, охрану, рабочие места, оборудование и инструмент, склады, парковки (Tier III–IV).

В заключение отметим, что состав и практическое воплощение систем ЦОДа – это всегда некий компромисс между рамками нормативов, реальными условиями на объекте и возможностями инвестора. Взяв за основу приведенную на рис. 2 структуру и вычеркнув системы, которые не планируется устанавливать, инвестор может без посторонней помощи примерно оценить соответствие своих возможностей желаемому уровню надежности функционирования ЦОДа.

Представим себе, что спорный для России вопрос о целесообразности строительства ЦОДа, соответствующего сводному рейтингу Tier IV – Gold по классификации Uptime Institute, решен инвестором в пользу строительства. По мнению автора, такой проект в условиях России практически нереализуем. И дело не только в больших объемах инвестиций в инфраструктуру ЦОДа, что останавливает 99% инвесторов еще на этапе бюджетной оценки строительства. Непредсказуемыми остаются затраты, связанные с поиском и выделением подходящего участка под строительство, подведением к участку необходимых коммуникаций (электроэнергия, газ), получением необходимых разрешений и согласований. В нынешних российских реалиях такое строительство под силу только крупному государственному инвестору. ИКС



- Энергоэффективные решения для ЦОДов в области вентиляции и кондиционирования воздуха;
- Комплексные поставки оборудования для систем обеспечения микроклимата ЦОДов;
- Полный спектр услуг в области инженерных систем, включая проектирование, монтаж и пусконаладку оборудования.

Офис в Москве:
107589, Краснопресненская наб. 12, ЦМТ
т./ф. (495) 790-77-07
center@uelements.com

Офис в Санкт-Петербурге:
197110, ул. Б. Разночинная, д. 32
т. (812) 718-55-11, ф. (812) 718-55-14
market@uelements.com

реклама



Чиллеры **McQuay**

- Широкий выбор типов и моделей на спиральных, винтовых и центробежных компрессорах;
- Возможность применения встроенной функции «фрикулинга» (винтовые чиллеры);
- Точное поддержание температуры воды на выходе ($\pm 0,1^\circ\text{C}$).



Балансировочные клапаны **FlowCon**

- Автоматическая балансировка гидравлической системы;
- Две функции в 1-м клапане: балансировка и регулирование;
- Точное регулирование расхода хладагента (5%).



Прецизионные кондиционеры **TECNAIR LV**

- Совершенная аэро- и гидродинамика;
- Минимальная площадь основания и обслуживание со стороны передней панели;
- Вентиляторы с низким энергопотреблением, в т. ч. с использованием ЕС двигателей.



Оптимизация гидравлической обвязки систем холодоснабжения ЦОДов

Евгений ВИШНЕВСКИЙ, технический директор United Elements, канд. техн. наук

Михаил САЛИН, ведущий инженер отдела исследований и развития United Elements

Тимур ТОЛОКОННИКОВ, ведущий инженер отдела исследований и развития United Elements

Оптимизируя энергопотребление ЦОДов, следует иметь в виду и системы холодоснабжения. Как показывает сравнение различных схем водяного охлаждения, традиционные системы и энергетически, и экономически недостаточно эффективны.

Современные ЦОДы – высокоэнергоёмкие объекты, а потому повышение их энергетической эффективности становится одной из важнейших задач при проектировании. При этом разработчики стараются увеличить эффективность не только основного телекоммуникационного оборудования, но и вспомогательных систем, в том числе систем холодоснабжения.

Системы охлаждения ЦОДов выполняются на базе как фреоновых прецизионных кондиционеров с выносными конденсаторами, так и водяных прецизионных кондиционеров и чиллеров. Однако для фреоновых систем существуют ограничения на длину фреоновых трубопроводов (максимальная рекомендуемая длина – не более 50 м) и перепад высот между внутренними и наружными блоками (не более 30 м). Поэтому в ЦОДах средней и большой мощности (с тепловыделением более 500 кВт)

применяются системы с водяным контуром на базе чиллеров и водяных прецизионных кондиционеров.

Оптимизация гидравлической обвязки с целью улучшения энергетической эффективности работы ЦОДов сводится к правильному выбору схемы холодоснабжения.

Схемы холодоснабжения ЦОДов

В ЦОДах широко распространены двухконтурные системы холодоснабжения – с внутренним и внешним контурами хладоносителя. Во внешнем контуре, связывающем чиллер с промежуточным теплообменником, циркулирует водный раствор этиленгликоля, не замерзающий в холодное время; во внутреннем контуре, между промежуточным теплообменником и кондиционерами, – чистая вода. Кроме того, такая система позволяет применить фрикулинг без значительной переработки схемы.

б и з н е с - п а р т н е р

Альтернативные способы холодоснабжения ЦОДов



Андрей БОДРОВ,
заместитель
генерального директора
ЗАО «ТМК-Телехаус»

Тема холодоснабжения для ЦОДов всегда будет актуальна: ведь даже неспециалисты понимают, что тепло от стоек надо куда-то девать. Жаркое лето 2010-го показало, что принятые нормы проектирования для систем холодоснабжения не рассчитаны на такую высокую температуру наружного воздуха. В течение двух самых тяжелых для эксплуатации недель прошедшего июля, когда чиллеры и внешние блоки охлаждения не справлялись, вода в систему поступала с температурой на 5–10°C (а порой на 15–17°C) выше, чем при работе в штатном режиме. В этом случае не помогут даже резервные системы холодоснабжения.

Температура в ЦОДе поднимается очень быстро, и специалистам службы эксплуатации приходится принимать экстренные меры. Все эти меры давно известны и находятся у них под рукой. С помощью дополнительных вентиляторов можно принудительно увеличить циркуляцию воздуха от горячих коридоров к точке забора нагретого воздуха блоков системы охлаждения, тем самым повысив их КПД. Охладить оборудование можно и нагретым воздухом, вопрос только в его количестве и в том, как организовать этот поток.

В аварийных ситуациях службе эксплуатации приходится бороться за каждый градус в помещениях ЦОДа. Можно задействовать систему вентиляции здания, которая позволит дополнительно снизить температуру на 2–3°C, сняв часть нагрузки с кондиционеров. Не

надо забывать и о том, что в нашем регионе для охлаждения восемь месяцев в году можно использовать воздух с улицы. Простая система воздухопроводов и промежуточных вентиляторов позволит на время аварии или срочных ремонтных работ поддержать температурный режим в ЦОДе. Все эти вопросы необходимо предусмотреть на стадии проектирования, заложив в проект соответствующие технические решения, которые не требуют серьезных капитальных затрат, но дадут дополнительную гарантию, обеспечат надежность ЦОДа клиентам и спокойствие – службе эксплуатации.

И последнее, о чем хотелось бы сказать службам эксплуатации ЦОДов: нельзя забывать о человеческом факторе и о постоянных (периодических) тренировках для дежурной смены. Если каждый сотрудник службы эксплуатации четко знает, что делать в конкретном случае, вам удастся избежать до 80% нарушений работы ЦОДа в аварийных ситуациях.

Тел.: 790-7806, 790-7807

<http://tmk-telehouse.ru/>



Во внутреннем контуре применяются схемы как с постоянным расходом хладоносителя, так и с переменным. Первая схема, получившая широкое распространение, включает насосы с постоянным расходом и трехходовые регулирующие клапаны. Для управления производительностью кондиционеров применяется байпас части хладоносителя через трехходовой клапан в обход теплообменника. Для балансировки системы в этом случае, как правило, используются ручные балансировочные клапаны. Такая схема отличается простотой регулирования и легкостью подбора оборудования. Однако у нее есть и существенные недостатки: наладка ее весьма трудоемка из-за трудности гидравлической балансировки системы, а в процессе эксплуатации периодически требуется повторная балансировка из-за старения трубопроводов. К тому же схема с постоянным расходом хладоносителя малоэффективна в плане экономии энергии. Поскольку максимальная производительность требуется только в течение короткого отрезка времени, основная часть энергии насоса расходуется впустую.

Наиболее интересна с точки зрения энергоэффективности схема с переменным расходом хладоносителя. Она включает насосы с частотно регулируемым приводом и двухходовые регулирующие клапаны. Особенностью данной схемы является то, что при снижении нагрузки вместе с уменьшением расхода через кондиционер уменьшается скорость вращения привода насоса, благодаря чему сокращается потребление энергии.

Управление температурой при помощи регулирующего клапана

Работа регулирующих клапанов полностью зависит от давления. При закрывании клапана перепад давлений ΔP увеличивается, а поток Q на регулируемом участке уменьшается. В общем виде эту зависимость можно выразить следующей формулой:

$$Q = A\sqrt{\Delta P},$$

где A – коэффициент, зависящий от типа жидкости и геометрии местного сопротивления.

Если геометрия элемента гидравлического контура неизменна, то очевидна зависимость расхода жидкости от перепада давления в гидравлическом контуре (стрелки показывают, что при увеличении напора в системе расход жидкости увеличивается):

$$Q \uparrow = A\sqrt{\Delta P \uparrow}.$$

Например, при увеличении напора в одном из циркуляционных колец расход может превысить значение, необходимое для обеспечения заданной температуры. Чтобы вернуться к расчетному расходу, потребуется частично прикрыть регулирующий клапан, что приведет к изменению коэффициента пропорциональности A .

На практике регулирующий клапан должен постоянно реагировать на колебания давления в контуре. Если коэффициент клапана изменяется от $A1$ до $A2$, соответственно меняется и гидравлическая характеристика контура (рис. 1). Чем больше становится перепад давления в контуре,

Б И З Н Е С - П А Р Т Н Е Р

Схемы с переменным расходом: что на практике?



Виктор ГАВРИЛОВ,
технический
директор компании
«АМДтехнологии»

Вопрос об экономии электроэнергии в ЦОДе за счет применения систем холодоснабжения с переменным расходом хладоносителя весьма актуален. Безусловно, при переменной тепловой нагрузке, которая, как правило, и имеет место в машинных залах, вариант перераспределения хладоносителя между кондиционерами предпочтительнее, чем схема с постоянным расходом. Однако стоит отметить, что далеко не случайно схемы с постоянным расходом являются наиболее распространенными. Практически любой производитель прецизионных кондиционеров шкафного типа стандартно комплектует их трехходовыми клапанами, т.е. по умолчанию оборудование предназначено именно для схемы с постоянным расходом. В качестве опции производители предоставляют возможность укомплектовать кондиционеры двухходовыми клапанами, но это будут стандартные клапаны (не путать с комбинированными клапанами PICV, недавно появившимися на рынке, которые совмещают функции регулирующего и балансировочного клапана).

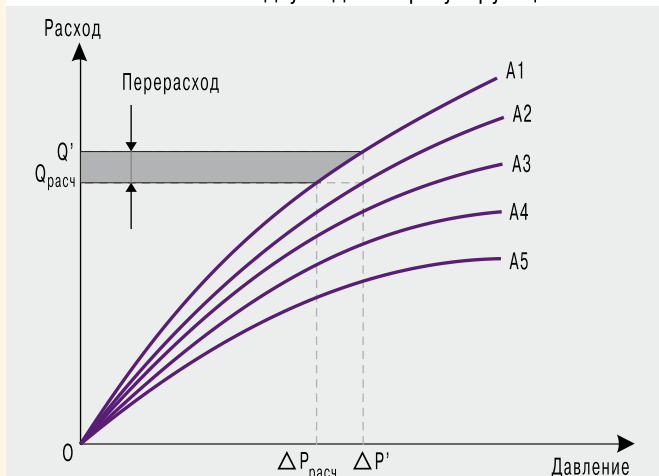
В последнее время, особенно в проектах зарубежных компаний, все чаще встречаются схемы с переменным расходом. Связано это с тем, что в рекомендациях ASHRAE появились требования по экономии энергии за счет использования систем с переменным расходом хладоносителя. Однако на практике, применяя подобные схемы, пользователи могут столкнуться

с проблемами, вызванными использованием двухходовых клапанов (переменное гидравлическое сопротивление участка сети, большие потери давления на клапане, точность регулирования и т.д.). В результате попытка сэкономить на электроэнергии может привести к нестабильной работе климатического оборудования, вплоть до образования зон перегрева серверных стоек.

В связи с этим кажется интересным и перспективным предложение использовать двухходовые комбинированные клапаны вместо стандартных. В этом случае гидравлическая схема действительно становится проще в балансировке и эксплуатации. Но, на наш взгляд, при этом заказчик может столкнуться с новой проблемой. Производители оборудования комплектуют кондиционеры стандартными клапанами, заказать кондиционер вообще без клапана тоже не получится, так как привод клапана связан с контроллером и участвует в процессе регулировки производительности кондиционера. Остается вариант отправить на завод запрос на изготовление оборудования в специальном исполнении – но это будет уже другая история.



Рис. 1. Расходно-напорная характеристика двухходового регулирующего клапана



A1-A5 – характеристика клапана в зависимости от максимального расхода;
 $Q_{расч}$, Q' – расчетное и фактическое значения расхода;
 $P_{расч}$, P' – расчетное и фактическое значения давления

тем больше требуется прикрывать регулирующий клапан. Если поддерживать постоянный поток в контуре, то зависимость «расход – напор» будет иметь следующий вид:

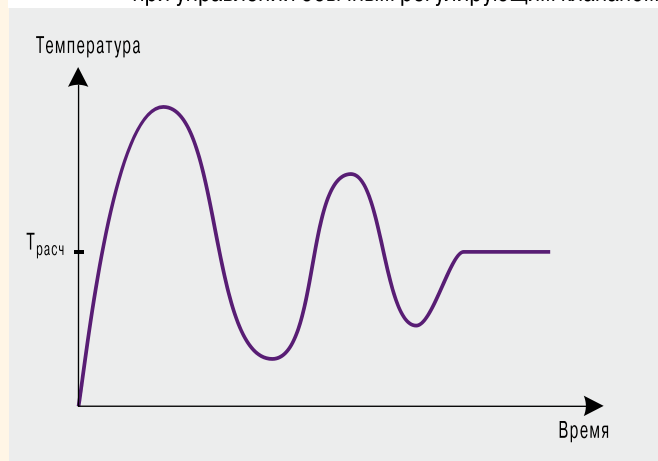
$$Q = A \sqrt{\Delta P}$$

Из сказанного выше понятно, что работа обычного регулирующего клапана очень сильно зависит от потерь давления в контуре вообще и от сопротивления отдельных его элементов (труб, балансировочных клапанов, теплообменников) в частности. Из-за неизбежных колебаний давления расход в теплообменнике не будет постоянным, что повлечет за собой колебания температуры в помещении (рис. 2).

Влияние потерь давления в контуре на регулирующий клапан определяется значением авторитета клапана. Величина авторитета клапана α характеризует его способность воздействия на поток, которая зависит в основном от правильного выбора проходного сечения (а точнее, пропускной способности клапана). Чем больше клапан соответствует требуемому авторитету, тем меньше потребуются воздействовать на поток. Авторитет двухходового регулирующего клапана определяется по формуле

$$\alpha = \frac{\Delta P_{РЕГ.КЛ.}}{\Delta P_{РЕГ.КЛ.} + \Delta P_{БАЛАНС.КЛ.} + \Delta P_{ТО}}$$

Рис. 2. Колебания температуры в помещении при управлении обычным регулирующим клапаном



где в числителе – только сопротивление регулирующего клапана, а сумма в знаменателе включает сопротивления всех элементов гидравлического контура: регулирующего клапана ($\Delta P_{РЕГ.КЛ.}$), балансировочного клапана ($\Delta P_{БАЛАНС.КЛ.}$) и теплообменника ($\Delta P_{ТО}$).

Сопротивление труб обычно меньше других составляющих потерь давления в контуре, поэтому его значением в расчетах часто пренебрегают. Однако справедливости ради нужно заметить, что учет сопротивления труб хоть и незначительно, но ухудшает авторитет клапана. Обычно считается, что значение авторитета должно быть равно примерно 50% (или 0,5). Это означает, что минимальное сопротивление двухходового клапана будет определяться равенством

$$\Delta P_{РЕГ.КЛ.} = \Delta P_{БАЛАНС.КЛ.} + \Delta P_{ТО}$$

В итоге значение потерь давления на клапане и в контуре может оказаться довольно большим. Получается, что увеличенные потери энергии вызываются не только плохим качеством регулирования, но и стремлением к достижению требуемого качества регулирования (авторитета регулирующего клапана). Значение авторитета меньше 0,5 показывает, что зависимость потока от проходного сечения клапана не является пропорциональной. Иными словами, после сигнала от датчика температуры регулирующий клапан будет открываться больше, чем требуется. И наоборот, при закрывании клапана влияние его на поток будет меньше, чем должно быть, что

Холодоснабжение и кондиционирование дата-центров от проекта до технического обслуживания на базе оборудования RC Group

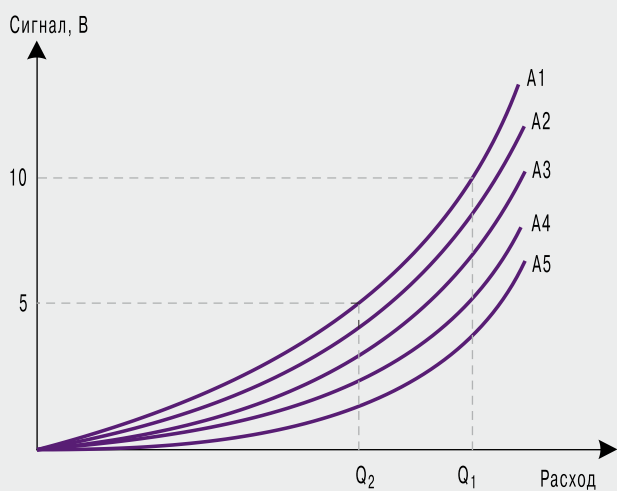
RC GROUP

ВЕНТСПЕЦСТРОЙ
VENTCONSTRUCTION

www.ventss.ru • info@ventss.ru • (495) 775-37-91

реклама

Рис. 3. Производительность двухходового регулирующего клапана в зависимости от входного сигнала



A1–A5 – характеристика клапана в зависимости от максимального расхода;
 Q₁ – расход при 100%-ной нагрузке (100%-ное открытие клапана);
 Q₂ – расход при 50%-ной нагрузке (80%-ное открытие клапана)

также приведет к сильным колебаниям температуры в помещении, увеличению потерь и снижению комфорта. Более того, из-за непропорционально большого расхода через теплообменник (80% от номинального расхода вместо 50%) перепад температур на входе и на выходе окажется меньше расчетного. Проблема недостаточного перепада ΔT – это следствие избыточного потока через теплообменник. Данная проблема является всеобщей и неизбежной при использовании двухходовых регулирующих клапанов в системах кондиционирования.

На рис. 3 приведена зависимость расхода от регулирования: для гидравлического контура с авторитетом клапана, равным 50%, показаны режимы работы теплообменника для клапана, открытого полностью или наполовину. Как было видно из рис. 2, расход сначала регулируется с большой амплитудой, что вызывает значительное отклонение температуры от уставки. Эти колебания обусловлены невозможностью обеспечить авторитет клапана, равный 100%, если на работу регулирующего клапана влияют другие элементы гидравлического контура.

Управление температурой при помощи комбинированного клапана

Комбинированный клапан выполняет функции регулирующего и балансировочного клапанов. Его также называют регулирующим клапаном, независимым от давления (Pressure Independent Control Valve, PICV). С учетом функции регулирования давления формула для определения расхода примет следующий вид:

$$Q = A(\sqrt{\Delta P})_{\text{CONST}}$$

В формуле остается лишь одна переменная A, поэтому при постоянном перепаде давления на регулирующем клапане можно обеспечить пропорциональное регулирование потока. Каждому положению штока в

зависимости от значения параметра A будет соответствовать точно заданный расход (рис. 4).

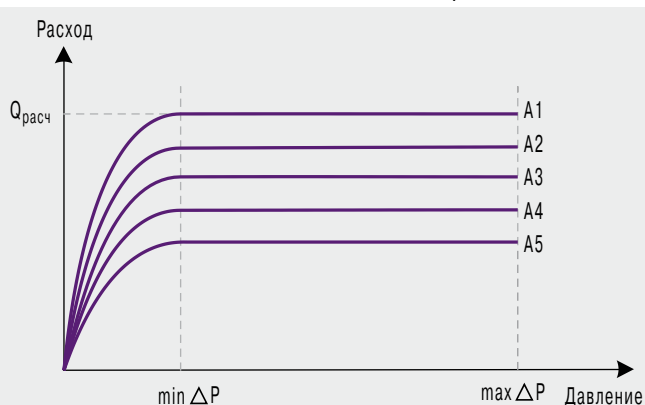
Сравнение характеристик традиционного регулирующего клапана и комбинированного клапана (см. рис. 1, 4) наглядно показывает преимущество автоматической балансировки. Автоматические клапаны обеспечивают пропорциональное регулирование даже при переменных давлениях и расходах в контурах. Колебания давления от $\min \Delta P$ до $\max \Delta P$ не будут влиять ни на расход воды в теплообменнике, ни на теплоотдачу. Еще одно достоинство автоматической балансировки – простота выбора клапанов, так как рассчитывать авторитет теперь не требуется. Расчет авторитета важен в контурах, где расход и потери давления связаны. В комбинированном клапане расчетный расход остается неизменным при любых значениях ΔP в широком диапазоне, который можно варьировать в зависимости от условий работы клапана. Расход через клапан зависит только от положения штока (A1, A2...). Это означает, что авторитет клапана будет равен 100%. В данном случае становится неважным влияние сопротивления теплообменника, трубопроводов, самого клапана на регулирование потока. Учитывая вышесказанное, можно охарактеризовать графическую зависимость расхода от управляющего сигнала как линейную. Так, при перемещении штока на половину хода поток изменится на 50%.

Пропорциональное регулирование потока можно обеспечить только за счет совместного использования автоматического балансировочного и регулирующего клапанов. Если поток изменяется точно в соответствии со степенью воздействия управляющего сигнала (напряжения), то температура обратного трубопровода тоже будет адекватно изменяться для поддержания ΔT . Таким образом, исчезает проблема недостаточного перепада температуры на теплообменнике. При любых колебаниях давления в гидравлической системе комбинированный клапан точно управляет потоком. Как следствие, стабильность расхода обеспечивает номинальные значения температуры и ΔT .

Сравнение гидравлических схем

Преимущества любой новой технологии становятся очевидными только при тщательной оценке экономиче-

Рис. 4. Расходно-напорная характеристика комбинированного клапана



A1–A5 – характеристика клапана в зависимости от максимального расхода

Затраты на арматуру для различных схем системы холодоснабжения мощностью 5 МВт

	Ручные балансировочные клапаны, V = const		Комбинированные клапаны, V = var	
	Количество, шт.	Стоимость, евро	Количество, шт.	Стоимость, евро
Трехходовые пропорциональные клапаны Danfoss	82	139 600	-	-
Ручные балансировочные клапаны Danfoss	186	98 530	-	-
Комбинированные пропорциональные клапаны FlowCon	-	-	82	210 760
Итого:	268	238 130	82	210 760

ского эффекта от внедрения. Попробуем разобраться с тем, что даст потребителю использование автоматической балансировочной арматуры. В качестве примера рассмотрим систему холодоснабжения ЦОДа с нагрузкой на холодильное оборудование 5 МВт. Система состоит из двух изолированных схем, одинаковых по мощности и конфигурации. Тип схемы – двухконтурная, с промежуточным теплообменником. В первичном контуре чиллера в качестве охлаждаемой жидкости используется водный раствор этиленгликоля, во вторичном контуре – вода. В каждой схеме вторичного контура имеются три насоса, один из которых резервный. Производительность каждого насоса составляет 216 м³/ч. Каждая схема вторичного контура состоит из 41 прецизионного кондиционера общей холодопроизводительностью 2990 кВт с учетом резервного оборудования: 27 кондиционеров имеют производительность 103 кВт, еще 14 кондиционеров – 15 кВт.

Оставляя неизменной компоновку первичного контура и чиллера, сравним два варианта обвязки прецизионных кондиционеров и балансировки гидравлических контуров.

В первом варианте для управления кондиционерами служат трехходовые пропорциональные клапаны. Насосы обеспечивают постоянный расход. Балансировку системы выполняют с помощью ручных балансировочных клапанов.

Во втором варианте управление расходом и балансировка осуществляются с помощью пропорциональных комбинированных клапанов (PICV). Насосы с частотно регулируемым приводом обеспечивают переменный расход.

В схеме с ручными балансировочными клапанами увязку гидравлической системы приходится выполнять поэтапно, в зависимости от количества циркуляционных колец. Сначала необходимо сбалансировать байпасную линию на каждом кондиционере, поскольку ее гидравлическое сопротивление меньше, чем сопротивление кондиционера. Далее уравниваются кондиционеры на каждой ветке, а затем – каждый стояк. Таким образом, для рассматриваемой схемы, включающей 41 кондиционер, требуется 134 ручных балансировочных клапана. Для данной системы пусконаладочные работы довольно сложны, поскольку при изменении сопротивления в одной ветке меняется и сопротивление на других участках.

В схеме с комбинированными клапанами клапаны совмещают функции автоматической балансировки и регулирования расхода хладоносителя. Поэтому вместо трехходовых регулирующих и отдельных ручных балансировочных клапанов в ней установлены двухходовые комбинированные клапаны. Они автоматически поддерживают

нужный расход через прецизионный кондиционер, изменяя его в зависимости от управляющего сигнала датчика температуры воздуха в охлаждаемом помещении.

В таблице описанные выше варианты сравниваются по первоначальным затратам на арматуру для обеих схем системы холодоснабжения мощностью 5 МВт. В качестве трехходовых клапанов на прецизионных кондиционерах применялись клапаны VF3 (Danfoss) с пропорциональным управлением. В первой схеме использовались ручные балансировочные клапаны ISV-I и MSV-F2; во второй – комбинированные клапаны FlowCon с пропорциональным регулированием.

Экономия на капитальных затратах от применения автоматических балансировочных клапанов зависит от конфигурации системы холодоснабжения: чем более разветвленной она будет, тем значительнее разница в стоимости комплекта регулирующей арматуры. Сравнение показало, что при рассматриваемой конфигурации гидравлической схемы замена ручных балансировочных клапанов на комбинированные снижает затраты на арматуру не менее чем на 10%.

Подведем итоги

С точки зрения современных требований к энергосбережению традиционные схемы на базе трехходовых регулирующих и ручных балансировочных клапанов в системах холодоснабжения ЦОДов недостаточно эффективны. Наиболее перспективное направление в этой области – системы с переменным расходом хладоносителя с использованием комбинированных клапанов и насосов с частотно регулируемым приводом. За счет работы насосов в режимах частичной нагрузки большую часть эксплуатационного периода потребление электроэнергии значительно сокращается.

Комбинированные клапаны позволяют с высокой точностью поддерживать требуемый расход хладоносителя через кондиционер и тем самым обеспечивают истинно прецизионный контроль микроклимата, что особенно важно для ЦОДов.

Помимо этого, крупные системы с переменным расходом хладоносителя на базе комбинированных клапанов могут оказаться выгоднее с точки зрения капитальных затрат (что и демонстрирует сравнительный анализ альтернативных гидравлических систем на конкретном примере).

Таким образом, схемные решения на базе комбинированных клапанов и насосов с переменным расходом хладоносителя обладают несомненными достоинствами в свете повышения энергетической эффективности систем холодоснабжения ЦОДов. ИКС

Пожар в ЦОДе: чем и как тушить



Елена КУРГАШЕВА,
ведущий эксперт компании
«АРМО-Системы»
по системам пожарной
сигнализации

Сегодня предприятия, относящиеся к любой отрасли экономики (производство, сфера услуг, финансовые структуры и др.), все больше и больше зависят от работы вычислительного и коммуникационного оборудования. Выход его из строя неизбежно приводит к прерыванию производственных и бизнес-процессов, т. е. влечет за собой высокие косвенные затраты. В связи с этим эффективная пожарная защита имеет особое значение для ЦОДов, где сконцентрировано серверное оборудование многих компаний.

Развитие пожаров в ЦОДах и их обнаружение

Как известно, существуют определенные сценарии развития пожаров в помещениях различного типа, в том числе и в ЦОДах. Для каждого этапа формирования пожара существуют строго определенные средства обнаружения, эффективные именно в этот период.

1 этап: тление (например, проводов или микросхем). Выделяющийся дым присутствует в воздухе в минимальной концентрации. Для обнаружения пожара в этой фазе используют аспирационные системы раннего обнаружения возгорания. Следует отметить и тот факт, что при пожаре в ЦОДе ущерб электронному оборудованию часто наносит вовсе не пламя, а выделяющийся при тлении и горении газ, который окисляет электронные контакты. Поэтому в помещениях данного типа рекомендуется устанавливать газоанализаторы, встроенные в систему раннего обнаружения пожара.

2 этап: сильное задымление стоечного пространства. Чтобы его обнаружить, используют неадресные датчики дыма, установленные внутри стоек. Как правило, сигналы от этих извещателей обрабатываются программой мониторинга серверного оборудования, установленного в дата-центре, и используются в качестве дополнительной информации для контроля всех систем данного объекта. Иногда данный способ обнаружения пожара используют для активации системы пожаротушения отдельной стойки.

Ущерб от простоя крупных дата- и call-центров, по данным американской Федеральной комиссии по коммуникациям (FCC), обходится в среднем в \$2 млн в час. Одна из причин простоев – пожары, в которых оборудование не только выходит из строя, но и бывает безвозвратно утеряно. Именно поэтому в современных ЦОДах, помимо систем раннего обнаружения возгорания, необходимы и средства тушения пожаров, не разрушающие дорогое оборудование.

Сегодня предприятия, относящиеся к любой отрасли экономики (производство, сфера услуг, финансовые структуры и др.), все

3 этап: сильное задымление помещения ЦОДа. Такой тип задымления детектируется с помощью адресных или неадресных датчиков общей системы пожарной сигнализации, установленных внутри помещения дата-центра. В качестве центрального приемно-контрольного оборудования здесь выступают пожарные панели иностранных и отечественных производителей. Все эти пожарные приборы должны быть сертифицированы для управления системами газового пожаротушения (ГПТ). Пожарные панели автоматически запускают системы активного пожаротушения при обнаружении возгорания. На 3-м этапе процесс тушения охватывает уже все пространство ЦОДа.

Как правило, в помещениях ЦОДов не устанавливают ни спринклерные, ни дренчерные системы тушения пожаров, потому что в случае их срабатывания дорогостоящее оборудование будет залито водой и непоправимо испорчено. Таким образом, для защиты ЦОДов системы газового пожаротушения оказываются незаменимыми.

Способы тушения пожаров

Обычно системы автоматического пожаротушения активируются только в тех случаях, когда развитие пожара уже невозможно остановить другими способами, например, отключив задымившийся сервер или системы кондиционирования. Существует два принципа организации пожаротушения при оборудовании ЦОДов системами ГПТ: это стоечное тушение пожара, когда воздействию подвергается отдельная стойка, и общее пожаротушение, когда соответствующие системы задействуются на всей площади ЦОДа. Рассмотрим подробнее оба эти подхода.

Стойное пожаротушение. Применяется для отсеков с оборудованием специального назначения, особенно если потеря хранящихся там данных обойдется дороже уста-



Система стоечного пожаротушения

новки и эксплуатации газовой системы пожаротушения. Срабатывание такого рода систем позволяет не прерывать работу оборудования, установленного в других стойках. Особенно это удобно, когда стойки, расположенные в дата-центре, арендуют разные компании: пожар в одной из стоек не приводит к отключению остальных серверов. Такой подход существенно

уменьшает число претензий арендаторов из-за простоев, а также в значительной мере помогает избежать косвенного ущерба.

Общее газовое пожаротушение. Выполняет функцию обнаружения и тушения очага возгорания на всей площади защищаемого дата-центра. Такая система состоит из магистрального и распределительного трубопровода, насадок для выпуска газа, датчиков для обнаружения пожара, контроллеров управления, а также из батарей баллонов с огнетушащим составом. Систему можно собрать из отдельных компонентов от разных производителей.

При тушении пожара с помощью газа используются следующие механизмы ликвидации возгорания:

- охлаждение;
- изоляция;
- разбавление (подавление очага пожара за счет уменьшения концентрации кислорода в помещении, заполненном тушащим газом);
- ингибирование (связывание активных центров, что приводит к обрыву цепной реакции горения).

Как правило, при тушении пожара с помощью ГОТВ используется сразу несколько механизмов в различных комбинациях.

Выбор огнетушащего вещества

В большинстве случаев (90% и более) в современных установках для тушения пожаров используются перечисленные ниже газы (табл. 1).

Хладон 125ХП. Действие этого вещества основано на эффекте ингибирования с незначительным использованием принципа разбавления. В ходе тушения выделяется большое количество вредных соединений в результате химического разложения газа.

Хладон 227еа. Как и предыдущий, газ действует на основе эффекта ингибирования, останавливая процесс горения на химическом уровне и поглощая тепло. В ходе тушения также выделяется множество вредных веществ.

Инерген. Пожаротушение с помощью этого вещества основано на механизме разбавления, т.е. происходит за счет снижения концентрации кислорода в помещении (вытеснение воздуха). Для инергена характерно значительное расширение вещества в газовой фазе при выпуске, что обеспечивает сильное понижение температуры в помещении.

Novac 1230. Этот газ создает эффект охлаждения за счет отбора тепловой энергии у цепной реакции горения. При этом температура в защищаемом помещении также незначительно (не более чем на 2–3 градуса) понижается.

Вопрос о выборе «правильного» тушащего вещества волнует и заказчиков и проектировщиков, поэтому в каждом конкретном случае рекомендуется проводить соответствующий анализ с учетом нужд защищаемого объекта. При этом можно выделить ряд параметров, по которым легко провести сравнение ГОТВ как по техническим, так и по экономическим показателям. Вот эти параметры:

- механизмы тушения;
- безопасность для людей;
- безопасность для окружающей среды;
- экономическая эффективность;
- количество ГОТВ, необходимое для создания огнетушащей концентрации;
- количество модулей ГПТ;
- площадь, занимаемая установкой ГПТ;
- наличие проблем при эксплуатации;
- сложность трубных разводок;
- срок службы установок и газового огнетушащего состава;

- электрическое сопротивление в газовой фазе;
- необходимость постановки модулей ГПТ на учет в Ростехнадзоре.

При выборе огнетушащего вещества необходимо также учитывать специфику помещения, где оно будет использоваться. В нашем случае это помещение дата-центра с размещенным в нем высокотехнологичным оборудованием, имеющим электронную начинку, а для защиты помещений с электронным и электротехническим оборудованием крайне важен такой параметр, как диэлектрическая проницаемость ГОТВ. Для оценки диэлектрических свойств различных огнетушащих веществ их принято сравнивать с изолирующими свойствами осушенного азота (см. табл. 1).

К числу важнейших параметров, влияющих на выбор ГОТВ для защиты помещений дата-центров, относят огнетушащую концентрацию и безопасность для человека и окружающей среды. Для сравнения этих показателей можно опираться на данные табл. 2. Отметим, что все приведенные в ней вещества имеют нулевой озоноразрушающий потенциал.

Табл. 1. Диэлектрическая проницаемость средств пожаротушения

Торговое наименование в России	Производитель, официальное наименование	Относительная диэлектрическая проницаемость (для N ₂ принята за 1)
Novac 1230	3M, FK-5-1-12	2,3
Хладон 125ХП	Dupont, FE-25	0,95
Хладон 227еа	Great Lakes/Dupont, FE-227	2,0
Инерген	TSS/Ansul, IG-541	1,03

Источник: документация производителей



Компоненты системы газового пожаротушения

Табл. 2. Основные показатели средств пожаротушения

ГОТВ	Химическая формула	Огнетушащая концентрация, % об.	NOAEL*, % об.	LOAEL**, % об.	Коефф. безопасности***	Время жизни в атмосфере, лет	Потенциал глобального потепления
Novac 1230	$CF_3CF_2C(O)CF(CF_3)_2$	4,2	10,0	>10,0	2,38	0,014	1
Хладон 125ХП	C_2HF_5	9,8	7,5	10,0	0,76	32,6	2800
Хладон 227еа	C_3HF_7	7,2	9	10,5	1,25	36,5	3500
Инерген	52% N ₂ , 40% Ar, 8% CO ₂	36,5	43,0	52,0	1,42	Нет	0

*NOAEL (No Observable Adverse Effect Level) – максимальная концентрация ГОТВ, при которой не наблюдается вредных последствий для человека; **LOAEL (Lowest Observed Adverse Effect Level) – наименьшая концентрация химического вещества, вызывающая вредные последствия для человека; ***коэффициент безопасности (отношение NOAEL к огнетушащей концентрации газа) показывает, во сколько раз максимально допустимая концентрация ГОТВ превышает необходимую для тушения пожара.

Источник: документация производителей и материалы World Meteorological Organization (WMO) 1998, Model-Derived Method; Intergovernmental Panel on Climate Change (IPCC) 2001 Method, 100 Year GPP

Самым важным параметром с точки зрения ликвидации пожара является огнетушащая концентрация: чем она меньше, тем эффективнее применение газового состава. Из табл. 2 следует, что огнетушащая концентрация увеличивается в ряду от Novac 1230 к хладону 227еа и хладону 125ХП. Сравнение по данному параметру с инергеном проводить несколько сложнее, поскольку он поставляется в виде модулей со стандартной заправкой (фиксированное количество ГОТВ в баллоне), следовательно, при его использовании огнетушащая концентрация может быть значительно превышена.

Поскольку для хладонов огнетушащая концентрация выше, чем для Novac 1230, то для защиты аналогичного помещения их потребуется больше, а следовательно, и установка газового пожаротушения займет большую площадь. В случае инергена модули с газовым составом занимают площадь в 5–6 раз большую, чем для Novac 1230. Заметим также, что инерген в баллоне находится под очень высоким давлением – 300 атм (для сравнения: у остальных ГОТВ давление не превышает 65 атм).

Исходя из параметров гидравлического расчета, можно утверждать, что для хладонов 125ХП и 227еа и инергена необходимо большее количество выпускающих насадок, чем для Novac 1230. Практика подтвердила эти расчеты, показав, что для подачи хладонов по сравнению с Novac 1230 действительно требуется в 3–4 раза больше насадок. Как следствие, при использовании Novac 1230 значительно упрощается трубная разводка и уменьшаются затраты на монтажные работы.

Чтобы оценить безопасность ГОТВ для окружающей среды, мы выделили два основных параметра: «потенциал глобального потепления» и «время жизни в атмосфере». Эти показатели у Novac 1230 значительно лучше, чем у хладонов. Для инергена эти параметры не рассматриваются, поскольку он состоит из газов, обычно присутствующих в атмосфере.

Одним из важных требований к установкам ГПТ является необходимость сохранения тушащих свойств в течение длительного времени; таким образом, мы имеем еще один важный параметр для сравнения ГОТВ – гарантийный срок хранения. Для хладона 125ХП этот срок составляет не более пяти лет, через 10 лет требуется его регенерация. По данным корпорации 3М (см. 3M Performance Materials Laboratory, December 2003), ГОТВ Novac 1230 не разлагается при хранении и не требует регенерации на протяжении всего срока службы, кото-

рый составляет 30 лет. Кроме того, химический состав Novac 1230 позволяет провести перезаправку модулей газовой установки непосредственно на объекте.

Сколько стоит противопожарная система

При расчете стоимости системы пожарной безопасности необходимо учитывать объем и площадь защищаемого помещения, а также наличие отдельно защищаемых компонентов систем. Допустим, что стоимость системы газового пожаротушения в расчете на средний ЦОД объемом 700 куб. м составляет около 50 тыс. евро (цена зависит от ГОТВ и производителя модулей, мы приводим усредненное значение). Несколько удорожает систему использование средства стоечного пожаротушения PanelSafe, цена которого составляет 5 тыс. евро на стойку. Тем не менее можно сказать, что затраты на систему газового пожаротушения не превысят нескольких процентов от стоимости всего ИТ-оборудования, установленного в ЦОДе. При этом установка аспирационной системы раннего обнаружения пожара обойдется не более чем в 1% от стоимости ИТ-оборудования, примерно в 1,5–3,5 тыс. евро. Расходы же на обычную пожарную сигнализацию и того меньше: например, датчики Esser, Simplex и Bosch стоят 70, 71 и 67 евро соответственно.



За время существования ЦОДов как самостоятельных объектов в них уже не раз были зафиксированы случаи возникновения пожаров, имевших весьма разрушительные последствия. Как правило, в ходе их тушения страдает дорогостоящее оборудование, причем не только от огня, но и от воды. В результате пожаров в дата-центрах крупных провайдеров было выведено из строя множество серверов, тысячи клиентов этих компаний понесли убытки из-за потери данных.

Все вышесказанное ведет к однозначному выводу: в дата-центрах необходимы системы пожаротушения надежных производителей – как для обнаружения пожара, так и для предотвращения его дальнейшего распространения. Установка таких систем не только сводит к минимуму прямой ущерб от гибели оборудования, но и существенно снижает косвенные затраты, связанные с прерыванием технологических и бизнес-процессов. ИКС

Полка расширения дисковой памяти

IBM System Storage EXP2500 предназначена в первую очередь для малого бизнеса и предприятий с ИТ-инфраструктурой, состоящей из одного или нескольких серверов, где хранение данных осуществляется на внутреннем дисковом пространстве. EXP2500 создана для решения проблем, связанных с нехваткой свободного места на серверах стандартной архитектуры.

Полка расширения работает по прямому подключению к серверу через RAID-контроллер IBM M5025 для серверов System X и позволяет расширить дисковое пространство до 408 Тбайт. EXP2500 использует новый интерфейс SAS 6 Гбит/с и представлена двумя моделями – EXP2512



и EXP2524 – на 12 дисков формфактора 3,5” и 24 диска формфактора 2,5” соответственно. Полки имеют одинаковые габариты (2U) и оптимизированы для установки в стоечный шкаф. Допускается одновременное подключение полок с разными типами жестких дисков. Отказоустойчивость системы обеспечивается продублированными блоками питания «горячей» замены и вентиляторами.

EXP2500 поддерживает различные уровни RAID (0, 1, 5, 10, 50, 6 и 60), а также динамическое расширение емкости (OCE), изменение уровня RAID (RAID Level migration) и тома большого объема.

Контроллер M5025 обладает выделенной кэш-памятью на 512 Мбайт, которая защищена от сбоев питания батареей.

IBM: (495) 775-8800

ПО для защиты доступа к смартфонам

Junos Pulse Mobile Security Suite – комплексное программное обеспечение для защиты мобильных устройств и хранящихся на них данных от вирусов, вредоносного ПО, утери, кражи, неподобающего использования и других угроз. Junos Pulse Mobile Security Suite включает в себя антивирус, персональный защитный экран (брандмауэр), анти-спам и средства контроля и мониторинга, созданные специально для смартфонов и подобных устройств. ПО способно удаленно делать резервные копии, восстанавливать данные и уведомлять о факте замены или выброса sim-карты или изменении ее состояния.

Пользователи могут отследить потерянное или украденное устройство через GPS и при необходимости активировать удаленное уничтожение данных для защиты секретной информации, а также осуществлять родительский контроль и предотвращать доставку детям «взрослого» контента.

Junos Pulse Mobile Security Suite позволяет предприятиям предоставлять безопасный доступ к корпоративной сети и приложениям с мобильных устройств.

Juniper Networks: (495) 680-6753

СКЗИ для защиты данных в СУБД Oracle

Средство криптографической защиты информации (СКЗИ) «Крипто БД» состоит из сервера баз данных, клиентского ПО eToken SecurLogon, консоли управления ключами и паролями и рабочей станции коллектора аудита, предлагаемой опционально. Решение совместимо с Oracle Database в редакциях Standard/Enterprise Edition версий 9i/10g/11g, на клиентских машинах работает под управлением ОС Windows XP/ Vista (32/64 бит). В СКЗИ реализованы российские криптографические алгоритмы, соответствующие ГОСТ 28147-89.

Использование «Крипто БД» обеспечивает:

- дополнительную аутентификацию пользователей для доступа к защищенным данным с помощью электронных ключей eToken;
- аудит и мониторинг доступа к зашифрованным данным;
- гибкое управление электронными ключами шифрования, исключающее возможные несанкционированные действия администраторов БД.



С помощью «Крипто БД» можно выборочно шифровать произвольное число колонок таблиц в СУБД Oracle, что существенно снижает нагрузку на аппаратные ресурсы по сравнению с шифрованием всего массива информации базы данных. Выполняя функции «надстройки» над штатными функциями СУБД, СКЗИ «Крипто БД» позволяет анализировать и фиксировать все операции с защищенными данными, независимо от уровня привилегий пользователей.

СКЗИ сертифицировано по требованиям ФСБ России. Лицензируется «Крипто БД» по модели «клиент-сервер»: с использованием серверных лицензий и лицензий клиентского доступа.

«Аладдин Р.Д.»: (495) 223-0001

Высокомощные бестрансформаторные ИБП

Chloride 80-NET – ИБП мощностью от 300 до 500 кВт, предназначенные для использования в ЦОДах. Замена трансформаторов быстродействующими цифровыми контроллерами напряжения и тока обеспечивает увеличение активной мощности ИБП практически на 20%.

Основные характеристики Chloride 80-NET:

- технология IGBT с двойным преобразованием на инверторе и выпрямителе;
- высокий КПД преобразования (подтвержденный сертифицированный показатель – до 98%) при полном соответствии нормам Tier 4 по энергозащищенности;
- способность обеспечивать питание без снижения характеристик и независимо от коэффициента мощности (как для емкостных, так и для индуктивных нагрузок);
- полная коррекция коэффициента мощности на входе (PFC) при следующих входных характеристиках: коэффициент мощности (PF) > 0,99; максимальное гармоническое искажение по току (THDi) < 3%;



- автоматическое наращивание выходной мощности до 10%;
- персональная карта идентификации ИБП, содержащая все рабочие параметры и позволяющая сократить время отключения для техобслуживания;
- оперативная «горячая» масштабируемость: функция параллельного подключения, дающая системе возможность автоматически обнаруживать добавление новых ИБП без остановки работы;
- интегрированная служба круглосуточного удаленного мониторинга и диагностики Chloride LIFE.net;
- полная гальваническая развязка в качестве стандартной опции.

Кроме того, Chloride 80-NET снабжаются 10” сенсорным экраном с поддержкой 15 языков, обеспечивающим полное интерактивное управление ИБП. Он позволяет просматривать всю необходимую информацию и значения параметров, связанных с входной электросетью и подключенной нагрузкой, а также текущим состоянием устройства.

Chloride: (495) 781-2883

ИБП для ЦОДов

Модульные ИБП с коэффициентом мощности 0,9 серий Delphys MX и Modulys Green Power (GP) ориентированы в первую очередь на дата-центры.

В серии Delphys MX добавились две старшие модели мощностью 800 и 900 кВА, допускающие установку параллельно до шести устройств, что позволяет обеспечить бесперебойным электропитанием ЦОД мощностью до 5,4 МВА. Максимальный КПД ИБП

Delphys MX в режиме двойного преобразования напряжения составляет 93,5%, и он остается таковым при изменении нагрузки от 50 до 100% номинала. Для удобства эксплуатации доступ ко всем компонентам ИБП осуществляется с передней панели.

ИБП Modulys GP с КПД, равным 96%, предназначены для виртуализированных дата-центров, в которых нагрузка может сильно изменяться во времени.

Модульная конструкция ИБП Modulys GP позволяет наращивать его мощность с шагом 20 кВА вплоть до 120 кВА, а при объединении двух ИБП можно довести общую мощность системы до 240 кВА. Для автоматизации работы ИБП разработана адаптивная система зарядки батарей EBS и функция проверки состояния аккумуляторов ВНС, предотвращающая их выход из строя.

Socomec UPS: (495) 775-1985

Внешний радиомодуль (ODU)

Семейства оборудования SkyMAN производства InfiNet Wireless предназначен для территориально распределенных систем видеонаблюдения, подключения базовых станций сотовой связи Picocell, точек доступа Wi-Fi, инфраструктуры DECT IP и т.п. Его отличительной особенностью является наличие дополнительного интерфейса Fast Ethernet с поддержкой PoE согласно стандарту 802.3af.

Платформа SkyMAN представляет собой универсальную многофункциональную программно-аппаратную платформу широкополосного беспроводного доступа, обеспечивающую объединение в единую виртуальную сеть территориально разнесенных подразделений (поддержку VPN), фиксированный доступ в Интернет, VoIP, передачу видео и телеметрии, создание каналов связи для подключения базовых станций 2G/3G/4G/LTE, быстрое развертывание временных сетей топологии



MESH, подключение точек доступа Wi-Fi, создание высокоскоростных магистральных беспроводных каналов с возможностью ретрансляции сигналов.

ODU оборудован встроенной грозозащитой и механизмом компенсации разности давлений внутри и снаружи корпуса для предотвращения разгерметизации и попадания влаги и пыли. Допускается «холодный старт» при температуре до –55°C.

«МувиКом»: (495) 665-6479

Перечень публикаций журнала «ИКС» за 2010 г.

■ НОВОСТИ

КОЛОНКА РЕДАКТОРА № 1–12

АКТУАЛЬНЫЙ КОММЕНТАРИЙ

- А. ЗАЙЦЕВА. Фондовый рынок под напором структурных изменений № 1-2
 О. УСКОВА. Инвестиции в инновации: сделаны, но недоступны . . . № 3
 Д. АНДРИКОВ. Защита персональных данных: исполнять нельзя ждать. № 5
 Н. КИЙ. Без прогнозов № 6
 А. КРЫЛОВА. До «Информационного общества» осталось... пять месяцев № 7-8
 В. ДРОЖЖИНОВ. Е – упало, М – пропало, U – осталось, или Вперед к вездесущности! № 9
 Е. ВОЛЫНКИНА. Добро пожаловать, или Своим вход воспрещен № 10
 А. ЛИПОВ. «Мы на пороге электронного межведомственного взаимодействия». № 11
 С. БАУКИН. Наша@Почта.РФ писем не принимает № 12

ЛИЦА № 1–12

ПЕРСОНА НОМЕРА

- А. МИКОЯН. Переводчик особого значения № 1-2
 А. МАЛИНИН. Дежурный по эфиру № 3
 Н. БРОДСКИЙ. «Энергию экономить вредно, если эта энергия – твоя собственная» № 4
 Ш. КОЛЛАР. «Я связист и никем другим никогда не был» № 5
 Н. МАКАРОЧКИНА. Надо ли преодолевать комплекс отличницы? . . № 6
 А. ТИТОВ. «Я не верю в чудеса, а верю в поступательность» . . . № 7-8
 С. МИШЕНКОВ. По радиоволнам памяти № 9
 А. ТАРАСОВ. Джентльмен инновационного бизнеса № 10
 О. СВИРСКИЙ. Везучий человек везущий № 11
 С. ПОРТНОЙ. Просвещенный фанатик № 12

КОМПАНИИ

Новости от компаний № 1–12

СОБЫТИЯ

- Н. КИЙ. Футурология мобильного Интернета № 1-2
 Е. ВОЛЫНКИНА. Эффективность для внутреннего употребления № 1-2
 А. КРЫЛОВА. Игры против рынка № 1-2
 Л. ПАВЛОВА. Мультимедийная цифра. № 1-2
 Л. ПАВЛОВА. ФилOSSофия оптимизации № 1-2
 Л. ПАВЛОВА. АСТРАномия российского ИТ-аутсорсинга № 1-2
 Е. ВОЛЫНКИНА. Беспокойное хозяйство MSK-IX № 1-2
 Н. КИЙ, Е. ВОЛЫНКИНА, А. КРЫЛОВА, Л. ПАВЛОВА. Стереозффект перехода на цифру № 3
 Н. КИЙ. Требуется сценарий! № 3

- Е. ВОЛЫНКИНА. Год безопасного Интернета. Бета-версия № 3
 Е. ВОЛЫНКИНА. ЦОД с сертификатом на доверии № 3
 Е. ВОЛЫНКИНА. И опыт, сын ошибок трудных № 4
 Л. ПАВЛОВА. IPTV в полосе препятствий № 4
 Л. ПАВЛОВА. Тонкости тарификации, или На что опереться оператору № 4
 А. КРЫЛОВА. iFin мечтает о финансах 2.0 № 4
 Л. ПАВЛОВА. ТВ-каннибализация неизбежна? № 5
 Н. КИЙ. БезОБЛАЧНОЕ будущее ОБЛАЧНЫХ вычислений. № 5
 А. КРЫЛОВА. Context-центр как предчувствие? № 5
 А. КРЫЛОВА. Мультимедийные услуги: танго втроем № 5
 Л. ПАВЛОВА. Опорный узел экономики региона № 5
 А. КРЫЛОВА. Рунет-2010: есть новый драйвер роста! № 6
 Л. ПАВЛОВА. Кто о чем, а операторы – о контенте № 6
 А. КРЫЛОВА. Электронное правительство без граждан? № 6
 Л. ПАВЛОВА. ГЛОНАСС нацелился на массовый рынок № 7-8
 Е. ВОЛЫНКИНА. Чемпионы монтируют VSAT за 8 мин 42 с № 7-8
 А. КРЫЛОВА. «Облака» для госсектора № 7-8
 А. КРЫЛОВА. ШПД: экспансия продолжается № 7-8
 А. КРЫЛОВА. Симметричный ответ № 7-8
 Е. ВОЛЫНКИНА. Страсти по LTE, или Очередной передел № 9
 Е. ВОЛЫНКИНА. ЦОДы 2010 догоняют мировой уровень № 10
 А. КРЫЛОВА. IP-сервисы: драйверы и точки монетизации № 10
 Н. КИЙ. Аутсорсинг грозит стать глобальным № 10
 Л. ПАВЛОВА. Инфобез в триединстве и борьбе № 11
 Н. КИЙ. Кто разбудит сонное царство TETRA? № 11
 Е. ВОЛЫНКИНА. Интернет и руководящий дилетантизм № 11
 Е. ВОЛЫНКИНА. Облачность будет при любой погоде № 11
 Е. ВОЛЫНКИНА. Поход в облака становится массовым № 11
 Л. ПАВЛОВА. Экспресс с остановкой № 11
 Е. ВОЛЫНКИНА. Менталитет для аутсорсинга № 12
 Н. КИЙ. Свято место для свободного ПО № 12
 Л. ПАВЛОВА. Под угрозой Ф3-152 № 12
 А. КРЫЛОВА. Предвосхищая желания № 12
 Е. ВОЛЫНКИНА. Виртуализация: сделай сам № 12
 Н. КИЙ. Качество требует административной реформы. № 12

СУБЪЕКТ ФЕДЕРАЦИИ

- М. САВВАТИН. Конкурентная Рязань. № 1-2
 М. БОДЯГИН. Алтайское широкополосье обещает конкуренцию. . № 3
 К. АНКИЛОВ. Козельск, Жиздра, Таруса ждут своих провайдеров. . № 4
 Е. КРЫЛОВА. Традиционные ценности Костромы. № 5
 М. САВВАТИН. Курган: плодородная почва для бурного роста . . № 6
 Ю. ФЕДОРОВА. Брянщина: интернет-разрыв между городом и деревней № 7-8
 М. БОДЯГИН. На дорогах Смоленщины конкуренция буксует . . № 9
 К. АНКИЛОВ. Lupus tambovicus amicus te est № 10
 М. САВВАТИН. Город Ярослава силен конкуренцией. № 11
 И. ЯКИМЕНКО. Связь на «островах сокровищ» № 12
КАЛЕНДАРЬ СОБЫТИЙ № 1–12

■ ТЕМА НОМЕРА

УСЛУГА В ПАКЕТЕ. ЧТО ПОЛОЖИЛИ?! № 1-2



Фокус

Больше пакетов – хороших и разных

Гуру

С. БЕРШЕВ. В динамическое пакетирование инвестировать стоит!

Игроки

М. ГЕРЧУК. Чем больше пакет,

тем довольнее абонент

Н. БРОДСКИЙ. Обоюдovýгодный пакет

П. БАСОВ. Фокусироваться надо на востребованных предложениях
 Т. ПОЖАРНАЯ. Через два года услуги без пакета будут неактуальны

Сценарий

ТВ в пакете

С. ТЕРПУГОВ. Как продавать IPTV?

О. ЛИСЕНКОВА. Мультисервис = пакет?

Аналитик

А. ГОЛЫШКО. Пакет от конвергентного оператора

Модель

Пакет для компаний: больших или маленьких?

Ю. КОРОЛЕВА. Пакет со срочным контрактом

Ракурс

А. ШУНИН. Основой пакетирования станут конвергентные платформы
 Д. КУТЯВИН. Конвергентные пакеты будут строиться на IMS
 Л. БЕЛЬСКИЙ, А. ЧУРИН. Трансформация для пакетизации
 М. САМСОНОВ. Биллинг для пакета

Концептуальный поворот

С. БЕЛОВА, Я. СЛОКА. Доход с двух сторон

ТВ ПОД ГИПНОЗОМ ЦИФРЫ. № 3

Фокус

Долгий быстрый переход
 А. МАЛИНИН. Не ФЦП единой

Позиция

Э. САГАЛАЕВ. Вслед за «большой восьмеркой»
 В. ЛИВШИЦ. Парадигма меняется

Модель

К. КУКК. Региональное цифровое вещание: как построить эффективную платформу

Игроки

Е. ГЕРАСИМОВ. IPTV оптом и в розницу
 Т. ПОЖАРНАЯ. IPTV как опция
 Д. БАГДАСАРЯН. «Кабельная цифра» идет в регионы

Ракурс

С. СКВОРЦОВА. Большой мировой переход

Дискуссионный клуб «ИКС»

Среда вещания: конкуренция обостряется



Н. ДЬЯКОНОВА. Структура спроса на фоне кризиса

А. КОРОТАЕВ. Вендоры укрупняются, заказчики мельчают

Ракурс

В. СОЛОНИН. Корпоративная IP-телефония в России: выгоды прямые и косвенные
 П. БЕГУН. От UC к Collaboration UC: от концептуальности к реальности

Комментарий юриста

Н. ДМИТРИК. Тюбик Пандоры на правовом поле

Концептуальный поворот

А. СВИРИДЕНКО. Золотая середина ВКС
 Д. ИВАНОВ. Мотивация на рынке ВКС. Имиджевый взгляд
 Д. АВЕРЬЯНОВ. Что поможет изменить корпоративный рынок ВКС?

Позиция

А. ЛУЧКИВ. Никакой политики – только бизнес
 И. ФЕДОРУШКИН. Круговорот кадров и просвещение
 М. РУДЕНКО. Корпоративные коммуникации. Russian Edition

Дискуссионный клуб «ИКС»

В поисках разумной достаточности

Бизнес-партнер

Видеоконференцсвязь высокого разрешения: эмоционально и рационально



ДЕЛО – ТРУБА. ИЛИ?.. № 4

Фокус

Не так страшна труба, как ее...

Гуру

Г. ДЖОНСТОН. К оператору брендов!

Позиция

Р. ТАНАШЕВ. Межрегиональный оператор против предубеждений

Модель

Р. ВОЛОДИН. Увеличивать сечение трубы бессмысленно
 А. МИНАЕВ. Надо вступать в партнерские отношения



С. СКВОРЦОВА. Рецепты прибыльных сервисов мобильного ШПД

Особое мнение

Э. РАЗРОЕВ. Могу ходить с плакатом: «Оператор – труба»
 И. ТОРГОВ. Давления со стороны сервис-провайдеров нет

Игроки

С. ЖУРАВЛЕВ. Сколько путей ведет к сервисам?
 С. АЛЫМОВ. Мы не заходим на территорию своих партнеров
 В. КРАМАРЬ. И «труба», и «сервис поверх трубы»
 В. СЛИЗЕНЬ. На выручку приходит вертикальный холдинг
 А. МАРЬИН. Для смены бизнес-модели одной платформы недостаточно

Проекты

В. ВАХРУШИН. Домашним сетям нужен контент-агрегатор
 В. КРЫЛОВ. Кекс без изюма – невкусный

Ракурс

С. МОЛЧАНОВ. Контент умеет кусаться!
 А. ЛАРЬЯНОВСКИЙ. Противоречий между нами нет

Комментарий юриста

А. МИШУШИН. Инь и Ян телекоммуникаций

СВЯЗЬ НА РАБОТЕ: ОТ ТЕЛЕФОНА К TELEPRESENCE № 5

Фокус

Корпоративные коммуникации – между «на вырост» и «на выброс»

ИНФОКОМ: ТОТАЛЬНАЯ ЭКРАНИЗАЦИЯ № 6

Фокус

Айда в видео!
 Связисты, овладейте экранами!
 Интересное кино

Ракурс

3-е поколение Рунета
 е-правительство требуются стандарты
 Д. БЫСТРУЕВ. е-правительство начинается с детского сада

Подробности

Трансформация бизнеса



Фабрика трансформации

Бренд «Комстар» уходит в историю
 Ребрендинг выставки
 В ожидании LTE, не забывая о WiMAX
 «Скай Линк» открывает фабрику MVNO
 Выставка в квадрате
 Кто такой российский производитель?
 Д. ДЕРИНГ. От 3G к LTE

Оптика остановилась на ближних подступах к абоненту
 Операторам – FTTH, пользователям мобильный – WiMAX

Технологическая платформа

Сценарий

Футурум-инфоком

ЦОД: ЦЕНА ВЛАДЕНИЯ № 7-8

Фокус

За эффективность и uptime-защиту
 А. ПАВЛОВ. Нам придется подтянуться до мирового уровня
 Цена вопроса

А. ШАПИРО. Кошелек или... дата-центр?
 А. ПЛАТОНОВ. Цена вопроса? Уже не главное!

В. ВАНЬКОВ. За что заплатит крупный клиент

Аналитик

В. ДЕМЧИШИН, А. СВИРИН. Московский дата-центр на «рынке покупателя»



Позиция

А. МАРТЫНЮК. Минимизация TCO по-русски

Модель

С. ЛЕБЕДЕВ. От резервирования персонала к аутсорсингу
Б. ГУСЕВ. Контейнер или стационар?

Концептуальный поворот

С. АНДРОНОВ. ЦОД; типичные заблуждения

Дискуссионный клуб

Между дефицитом, перепроизводством и техническим прогрессом

Бизнес-партнер

В. ЯКОВЕНКО. Энергоэффективность без дополнительных вложений

Климатические шкафы: минимизируем габариты и затраты
Безопасность данных и персонала

М. КУЛИГИН. Мониторинг АКБ оптимизирует расходы на обслуживание в ЦОДе

Д. О'САЛЛИВАН. Наш принцип – точное соблюдение правил в строительстве дата-центров

ЗАЩИТА ПО-КОРПОРАТИВНОМУ № 9



Фокус

Д. ЗАХАРЕНКО. На корпоративных рубежах обороны

Ракурс

М. КОНДРАШИН. Виртуализация – страшный сон отдела безопасности!
М. РОМАНОВ. Пять тактик защиты в виртуальной среде

Модель

Д. КОСТРОВ. Центр безопасности

операторов в ожидании стандартизации

С. КОТЬКАЛО. Базовый уровень – основа стандартизации операторов

Концептуальный поворот

С. ГОРДЕЙЧИК. Compliance как угроза

Бизнес-партнер

Е. ЯБЛОКОВА. Как помочь оператору превратить защиту информации в качественную и полноценную услугу

Подробности

А. МЕДВЕДЕВ. Защищаем базы данных

Д. БЫРДИН. Услуги по защите информации пора пакетировать

П. ПЕТРОВ. Самая большая брешь в системе безопасности – это персонал

М. ЕЛИН. Архитектура беспроводной сети должна обеспечивать выполнение политики безопасности

Д. БУРЛАКОВ. Защита VPN-каналов – главная забота крупных компаний

Комментарий юриста

И. СЛАБЫХ. Сколько стоит нарушение авторских прав

ИТ-АУТСОРСИНГ.

ПРОФЕССИОНАЛЬНОЕ

СОПРОВОЖДЕНИЕ № 10

Фокус

ИТ-локомотив – пока на запасном пути?

Ракурс

Телекомы идут в аутсорсинг

А. БАЧИКАЛОВ. «Казактелеком» обустраивается в «облаках»



К. ЮНОВ. «МегаФон» сервирует «трубу»

Аналитик

Т. ФАРУКШИН. Аутсорсинг за «облаками»

В. ШАБАТ. SaaS как коммунальный аутсорсинг

Модель

Приоткроем бизнес-кейсы?

Р. СУХОВ. Нужен ли большому российскому бизнесу ИТ-аутсорсинг?

Р. ВОЛКОВ. Готов ли рынок покупать «ИТ как сервис»?

Р. СУЛИЦКИЙ. ЦОД как место встречи спроса и предложения

А. ИЛЬИН. Сеть на аутсорсинге

Дискуссионный клуб «ИКС»

Школа повзрослевшего аутсорсера

ЭЛЕКТРОННАЯ БЮРОКРАТИЯ. № 11



Фокус

Так что же все-таки мы строим

Подробности

А. НАЩЕКИН. «Мы создаем новый рынок для всех ИТ-компаний»

С. САПЕЛЬНИКОВ. Органам власти не нужен «велосипед»

Ракурс

В. БАЛАСАНЯН. Таких реформ не было со времен Петра I

В. ИПАТОВ. Две стороны электронной услуги

А. САБАНОВ. Что сдерживает появление в России межведомственного электронного документооборота?

О. УСКОВА. Стандарты разумного

Дискуссионный клуб «ИКС»

Что нам стоит СЭД построить?

Особое мнение

Е. ЗИНДЕР. Инструментарий для строителей e-Gov

Модель

В. СЕРЕБРЯКОВ. У каждого региона своя специфика

Б. ВОЛЬПЕ. Дорастить решение до универсального

М. ИВАНКОВ. Шлюз между госорганами, гражданами и бизнесом

Бизнес-партнер

Умные инструменты для e-бюрократии

Концептуальный поворот

В. ДРОЖЖИНОВ. Электронизация госуслуг: пазлы инноваций

БОЛЬШОЙ РАЗБЕГ КАМЕРНОГО РЫНКА № 12

Фокус

Око бизнеса

Проекты

А. ГЕРМАН. Гражданин – пройдемте! Вот вам камера... ВКС

В. ВЛАСОВ. Экономические споры по монитору

В. ГРЕВЦЕВ. Телепортации нет, но есть ВКС

Позиция

Д. ОДИНЦОВ. С точки зрения софтверной

Дискуссионный клуб «ИКС»

Эффект присутствия

Бизнес-партнер

Wireless broadband для видеонаблюдения

Ракурс

О. САЕНКО. Всепроницающее бизнес-видео

О. УКОЛОВА. IP-видеонаблюдение становится частью ИТ-инфраструктуры



■ ДЕЛО

Экономика и финансы



- А. ЗАЙЦЕВА. Защитные бумаги телекомов торговались лучше рынка **№ 3**
 А. ЗАЙЦЕВА. Обгоняя позитив. **№ 4**
 А. ЗАЙЦЕВА. Информационный фон формирует «Связьинвест» **№ 5**
 А. ЗАЙЦЕВА. Телеком выглядит лучше падающего рынка. **№ 6**
 А. ЗАЙЦЕВА. Телеком снижается, но держится **№ 7-8**
 А. ЗАЙЦЕВА. У телекома рейтинг позитивный **№ 9**
 А. ЗАЙЦЕВА. Начало делового сезона: настроение позитивное **№ 10**
 А. ЗАЙЦЕВА. По пути реорганизации **№ 11**
 А. ЗАЙЦЕВА. Телекомы отстали от «широкого» рынка **№ 12**

Доля рынка



- Т. ТОЛМАЧЕВА. ОК, или «Модные штучки» для бизнеса **№ 3**
 С. АЛЫМОВ. Спутниковые антенны: миграция в сторону мобильности **№ 3**
 П. ТЕПЛОВ. Эконом-класс для IP-сетей **№ 3**
 Г. ШЕРРИ. Эффективность дата-центра = соответствие стандартам **№ 4**
 Д. АВЕРЬЯНОВ, И. УСПЕНСКИЙ. 3D, 4D, 5D... Видеоконференцсвязь следующего поколения **№ 4**
 М. ШНЕПС-ШНЕППЕ. Умный дом по стандартам ITU G.hn **№ 4**
 Е. СОЛОМАТИН. Московский ЦОД. Прогноз спроса до 2014 г. **№ 5**
 Д. НЕЛЮБОВ. Коммунальная башня **№ 6**
 Ю. ХАСЕГАВА. PMR сквозь призму двух брендов **№ 6**
 А. КАТКОВ. «Интернет ждет пришествия глянца» **№ 7-8**
 А. ХЕРЦОГ. Сеть – в чужие руки? **№ 11**
 А. ШИРОКИХ. Требуется централизация **№ 11**
 А. КРЫЛОВА. Как тестировать терминалы LTE **№ 11**

Управление



- А. ГОЛЫШКО. Регулирование 2.0. С точки зрения будущего **№ 5**
 А. ГОЛЫШКО. Регулирование 2.0. С точки зрения прошлого **№ 6**
 А. ГОЛЫШКО. Регулирование 2.0. С точки зрения мира **№ 9**
 А. РОКОТЯН. Как ускорить развитие российских телекоммуникаций в русле мировых тенденций **№ 10**
 А. ГОЛЫШКО. Регулирование 2.0. С точки зрения национальных интересов **№ 11**

High-Tech-маркетинг



- Н. БУШЕВА. Кроссмедиа в молодежном маркетинге **№ 3**

Рубежи обороны



- Кто в ответе за детей в Интернете? Круглый стол **№ 3**
 М. КОНДРАШИН. Убережем детей от угроз Сети **№ 5**
 М. ЕМЕЛЬЯНИКОВ. Камо грядеши, закон? **№ 7-8**
 А. СЫЧЕВ, Д. КУЗНЕЦОВ. Корпоративная вычислительная сеть. Как сделать ее неуязвимой? **№ 7-8**
 М. ЕМЕЛЬЯНИКОВ. Камо грядеши, закон? Часть 2. **№ 9**
 М. ЕМЕЛЬЯНИКОВ. Почему «не устанавливается» режим коммерческой тайны **№ 9**

- С. РЯБКО. Защищенность IP-телефонии в историческом и практическом контексте **№ 10**
 А. САБАНОВ. Защитим электронный документооборот **№ 12**
 А. СОВА. Контроль доступа к конфиденциальным документам. **№ 12**
 Симметричный ответ на новые угрозы безопасности **№ 12**

Бизнес-модель



- А. МАРЬИН. Деволюция коммуникаций **№ 5**
 И. КАСЬЯНОВ. Эффективность системы хранения данных: требуется анализ **№ 7-8**
 А. ТАРАСОВ. Инновационный бизнес = гениальные разработчики + профессиональные продавцы. **№ 9**

Решение



- К. ДЗАХОЕВ. Гибридный доступ: скорость, качество, сохранение инвестиций **№ 3**
 А. МАСЛЕННИКОВ. От продажи каналов – к продаже услуг Ethernet **№ 4**
 Многоуважаемый шкаф. **№ 5**
 А. ВАСИЛЕНКО. OpenScare преодолевает коммуникационные «заторы». **№ 5**
 А. ГИТИН. Verimatrix и потоковая передача с адаптивным битрейтом: платное телевидение на распутии **№ 6, 9**
 И. ЗАНЕГИН. Управляемый климат **№ 9**
 Возможности управления жизненным циклом услуг Carrier Ethernet **№ 10**
 М. СУКОННИК. Виртуализация on demand. **№ 11**
 А. БОГАЧЕВ. Оптимальная горизонталь, или В ЦОДах все по-другому **№ 11**
 Л. ПАВЛОВА. «Всегда рядом» – говорит банк, уводя клиентов из «сберкасс» в удаленные каналы обслуживания **№ 12**

Услуги



- А. ФИЛИППОВ. Верификация абонентского оборудования. Как повысить качество услуг triple play. **№ 1-2**
 В. МАКСИМЕНКО. Как оценить качество услуг контакт-центра **№ 6**
 Д. СЕМЕНОВ, Л. ДАДАЯН. Цифровое мобильное телевидение готовится выйти в массы **№ 9**
 Н. БАТАЛОВА. Информационная безопасность на новом уровне – тема года для российского телекома **№ 9**
 А. АНОШИН. О чем не знают пользователи корпоративной IP-телефонии **№ 10**
 К. СИЛИВЕРСТОВ. Услуги triple play на сетях доступа FTTx **№ 10**
 М. ИВАНКОВ. За госуслугой в МФЦ. **№ 10**

Проблема



- Ю. ЧЕРНОВ. Цифровое радио. Плюсы и минусы **№ 1-2**
 Ю. ЧЕРНОВ. Где DRM'у жить хорошо **№ 3**
 К. КОРНИЛЬЕВ. Инновации на конвейере, или Куда катится мир!? **№ 5**
 А. СЕРОВ. Система мониторинга как домкрат для Tier дата-центра **№ 5**
 А. КИРИЛЛОВ. IMS у времени в плену **№ 5**
 О. САУШКИН. Контакт-центр: бизнес-задача превалирует. **№ 5**
 К. КОРНИЛЬЕВ. Инновации на конвейере, или Свечной заводик нам не нужен! **№ 6**
 В. ДРОЖЖИНОВ, А. ШТРИК. Кризис ИТ-рынка в оценках и прогнозах **№ 6**
 А. КРЫЛОВА. Мне с башни видно всё, или Бизнес – людям **№ 9**

И. ЕХРИЕЛЬ, И. РОЗЕНЦВАЙГ. Найти и больше не терять.	№ 12
Д. МАРТЫНОВ. Системы ERP: заменять, модернизировать или?	№ 12
И. УСПЕНСКИЙ. Повышаем эффективность корпоративной мультисервисной сети	№ 12

Опыт



В. ДРОЖЖИНОВ. Непрерывность бизнеса: рынок формируется.	№ 1-2
Л. ПАВЛОВА. Кредиты, вклады и их технологическая основа	№ 4
Е. ВОЛЫНКИНА. На весах инноваций и традиций	№ 12

Горизонты



Коммунальная сеть – будущее телекома!?	
Круглый стол	№ 7-8
Бизнес-партнер	
Оборудование ШПД под надежной защитой	№ 11

НА ПОРТАЛЕ IKSMEDIA

Блог, еще раз блог!	№ 1-12
-------------------------------	---------------

«ИКС» proTEХнологии

Е. ВОЛЫНКИНА. Дата-центр в проекте. Требуется бесперебойное питание	№ 1-2
Д. МОРГУНОВ. Интерфейсы МТР/МРО в кабельной инфраструктуре ЦОДов	№ 1-2
А. МАРТЫНЮК. ИТ-система переезжает.	№ 1-2
О. СУХОВ. Классика или IP? Что предпочтительнее в системе безопасности	№ 1-2
Р. БЕКЕР. Тестирование LTE-приемника: ключевые факторы ухудшения распространения сигнала	№ 1-2
Д. МОРГУНОВ. Проектирование оптических кабельных систем высокой плотности	№ 3
Магазины Adidas, IP-объединяйтесь!	№ 3
П. РОНЖИН. Системы охлаждения для ЦОДов. Как снизить потребление энергии	№ 3
С. ЗАРЖЕЦКИЙ. Огонь, вода и коррозионный газ. Угрозы физической безопасности ЦОДа	№ 3
А. НОВИЧКОВ. Как Metro Ethernet живет в России?	№ 3
Е. ВОЛЫНКИНА. Тратим или экономим? Мониторинг и автоматизация управления систем электропитания ЦОДов	№ 4
Д. САХАРОВ. Виртуализация наступает!	№ 4
А. МАРТЫНЮК. Корпоративные и отраслевые стандарты для дата-центров	№ 4
М. МАМАЕВ. Особенности национальных совещаний и корпоративного биллинга	№ 4
И. КИРИЛЛОВ. Новые грани IP-телефонии	№ 4
Синергия технологий во благо коммуникаций	№ 4
Д. МОРГУНОВ. Оценка бюджета потерь в оптических кабельных системах	№ 4
П. РОНЖИН. Системы охлаждения ЦОДов. Какую выбрать?	№ 5
Сетевые решения НЗС для дата-центров: производительность выше, управление проще	№ 5
И. КИРИЛЛОВ. MSAN: платформы «переходного периода».	№ 5
А. СЕЛИН. С атомных станций – в российские ЦОДы	№ 5
А. МАРТЫНЮК. Первые шаги к виртуальной архитектуре	№ 5
Д. МОРГУНОВ. FTTH – оптический тракт в беспроводных сетях	№ 5
О. СУХОВ. Четыре подхода к построению систем IP-видеонаблюдения	№ 5
Е. ВОЛЫНКИНА. Орудия электропитания среднего и большого калибра.	№ 6
ЛВС: продукт сетевого семейства, или Король играет свита	№ 6
А. ПАВЛОВ, С. ЛЕБЕДЕВ. Сколько стоит эксплуатация ЦОДа?	№ 6
М. КУПЕРМАН, Д. АВЕРЬЯНОВ. Правда «пяти девяток»	№ 6
А. СЕМЕНОВ. Что нового в СКС?	№ 6
П. РОНЖИН. ЦОД: организация резервирования систем охлаждения	№ 7-8
С. ЗАРЖЕЦКИЙ. Физическая ИТ-безопасность – не роскошь, а необходимое условие защиты ЦОДов	№ 7-8
М. КУПЕРМАН, Д. АВЕРЬЯНОВ. Резервный центр как инструмент обеспечения непрерывности бизнеса	№ 7-8
FFC: вся полнота фрикулинга	№ 7-8

Д. МАЦКЕВИЧ. СКС-головоломка, или Российский стандарт тестирования кабельных линий	№ 7-8
А. СЕМЕНОВ. Перспективные СКС: скорости 40 Гбит/с и выше	№ 7-8
МегаЦОДам – системы электроснабжения на основе дизельных роторных ИБП	№ 7-8
А. МАРТЫНЮК. Какой спрос с консультанта?	№ 9
Е. ВИШНЕВСКИЙ, М. САЛИН, В. ГУМИНСКИЙ, Н. КОРСАК. Топливные элементы в системе резервного электроснабжения базовых станций	№ 9
Д. МОРГУНОВ. Обслуживание оптических разъемов в корпоративных сетях	№ 9
Е. КУРГАШЕВА. Аспирационные системы для раннего обнаружения возгораний в ЦОДах	№ 9
Е. ВОЛЫНКИНА. Инженерная инфраструктура ЦОДа: мода на зеленое	№ 10
Е. ВОЛЫНКИНА. СХД в эпоху борьбы за эффективность хранения	№ 10
Е. ШУМИЛОВА. Переход на IPv6: сегодня – рано, завтра – поздно?	№ 10
А. ЖАК. Защитные оболочки ЦОДов. Необходимый элемент инфраструктуры.	№ 10
А. СЕМЕНОВ. СКС категории 6а. Технические особенности и рыночные перспективы	№ 10
А. КРЫЛОВА. ЦОД на вырост. От проектирования до эксплуатации	№ 11
Д. САХАРОВ. Что 2009-й отложил, то 2010-й наверстал	№ 11
А. ЖАК. Защитные оболочки ЦОДов. Проектирование и строительство	№ 11
Д. МОРГУНОВ. Системы кабельных коробов в инфраструктуре ЦОДов	№ 11
Д. САХАРОВ. ИТ-инфраструктура ЦОДа устремляется в «облака»	№ 12
А. ГОРНАК. Миграция к сетям стандарта 802.11n	№ 12
А. МАРТЫНЮК. Эффективное командообразование в проекте ЦОДа	№ 12
Е. ВИШНЕВСКИЙ, Т. ТОЛОКОННИКОВ. Резервирование и оптимизация систем холодоснабжения ЦОДов	№ 12

НОВЫЕ ПРОДУКТЫ № 1-12



Михаил ЕМЕЛЬЯННИКОВ

**Школьники-двоечники
в параллельных мирах**

>>>> С полным ощущением deja vu под новый год специалисты следили за стремительным принятием, одобрением, подписанием и опубликованием нового закона об очередном переносе сроков приведения ИСПДн в соответствие с требованиями Федерального закона 152.

С высочайшей организованностью и поражающим единодушием наши законодатели еще на полгода, до 1 июля теперь вот 2011 г. сдвинули сроки. Почему? Цитирую пояснительную записку к законопроекту: «Выполнение органами государственной власти, органами местного самоуправления, бюджетными организациями требований к информационным системам персональных данных потребует резкого увеличения расходов из бюджетов всех уровней, что неосуществимо в условиях кризиса. Кроме того, сами расходы для приведения информационных систем в соответствие с требованиями закона не предусмотрены Федеральным законом «О федеральном бюджете на 2010 г. и на плановый период 2011 и 2012 гг.»».

Следуя логике законодателей, с той же организованностью и единодушием они немедленно начнут править федеральный бюджет и изыскивать средства, чтобы все ИСПДн срочно привести в соответствие с законом. Но почему-то таких предложений в законопроекте не было. Перенести срок – и точка.

Такая ситуация больше всего напоминает поведение школьника, получившего двойку в дневник. Можно выучить предмет, вызваться к доске и попытаться исправить ситуацию. Но это трудоемко, рискованно и просто лень. Есть путь проще – спрятать от родителей дневник и перенести неотвратимое наказание на неопределенный срок – скорее всего, до родительского собрания. А на него родители могут и не пойти.

Ничего за эти полгода измениться радикально не может в принципе.

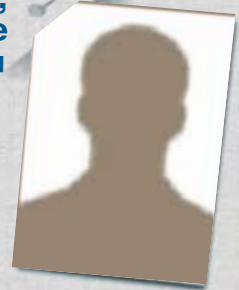
А тем временем мы продолжаем жить одновременно как минимум в двух мирах. В одном из них действует ФЗ-152. Там оператор обязан подтвердить наличие согласия субъекта на обработку персональных данных, и регулятор разъясняет, что в электронном мире таким подтверждением является ЭЦП, а при ее отсутствии оператор обязан проверить достоверность полученных данных или получить письменное согласие. В другом мире стремительно развивается электронная торговля, где можно совершить сделку анонимно или от имени любого лица, приобрести товары и услуги для других, указав необходимые для этого чужие персональные данные. И никто ничего не проверяет, проверять не собирается и третьих лиц ни о чем не уведомляет.

В одном мире трансграничная передача персональных данных значительно ограничивается законом, а в другом – российские авиакомпании практически полностью переносят процесс бронирования и продажи билетов (на перелеты внутри России в том числе) в облако глобальных операторов Sabre и Gabriel, где о национальных границах говорить как-то даже неприлично, но при этом пассажиру о трансграничной передаче никто не сообщает и согласия от него не получает.

И так до бесконечности...

Существуют эти миры параллельно, нигде, кроме нашего сознания, видимо, не пересекаясь.

Видимо, такова наша судьба – жить одновременно в нескольких мирах под надзором двоечников, прячущих дневник от несуществующих строгих родителей.

[КОММЕНТИРОВАТЬ](#)**VSATman
Эксперты,
держите
меня
четверо!**

>>>> Недавнюю аварию «Протонов» не обошли вниманием не только профильные отраслевые, общеполитические, экономические, но и развлекательно-сенсационные издания. Жанр обязывает, чтобы журналист знакомил любопытного читателя с мнением авторитетного ЭКСПЕРТА о прошедшем событии, каковой и обнажает неизвестные публике детали происшедшего. Правда, толкового эксперта еще надо поискать, а дедлайн неумолимо приближается... Итак, извлеченные журналистом из неизвестных секретных космических организаций «ЭКСПЕРТЫ» поведали ему, что:

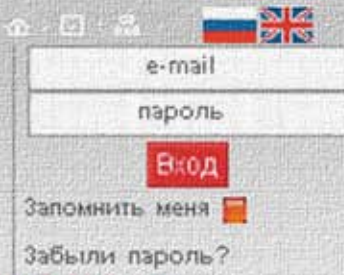
1) «Спутники могли быть оснащены дополнительным оборудованием, которое из-за секретности могли не учесть при расчетах массы выводимого груза», – заявил Life News источник, знакомый с ходом расследования.

2) Опрошенные Life News эксперты также не исключают, что «перевес» возник из-за того, что на «Протоне» было не три, а четыре спутника.

Сдается мне, что, высказав сокровенное знание, «эксперты» зажали в потной руке полученный гонорар в виде 100-рублевой купюры и направились в ближайший ларек, дабы пополнить запас знаний.

[КОММЕНТИРОВАТЬ](#)

Перелом десятилетий – не шутка. Случаются фантазмагории, мигом отражающиеся в блогосфере IKS MEDIA.RU. Объекты фантазмагорий? А вы не догадываетесь? Закон о персональных данных, авария «Прото-на», громкие сделки, «Сколково»...



Вячеслав БОРИЛИН Игры инвесторов

>>>> Сделка по приобретению Skype сервиса Qik, скорее всего, осуществлена американским венчурным фондом Andreessen Horowitz, основатели которого Марк Андреессен и Бен Хоровиц не так давно вложили деньги в Qik, и они же владеют долей в Skype.

Обычно те инвесторы, которые входят в неприбыльный бизнес (вроде Qik) последними, первыми получают деньги от его продажи. Сама сделка

похожа на внутренние игры инвесторов.

...Технологически в области видеокommunikаций Qik значительно отстает от Skype. Получается, основное приобретение Skype – это R&D-команда. Вероятно, Skype, желая добавить себе функциональность видеошаринга на мобильных платформах, купил команду, которая может это делать, и Qik как самостоятельный продукт может перестать существовать.

Резюмируя – Qik продали не русские программисты, и даже не индусы-основатели, а вошедшие последними американские опытные инвесторы из Andreessen Horowitz, и именно они, а не основатели, на этом, наверное, и заработают.

[комментировать](#)



Кристофер ТОМПСОН Канада – Россия 3:5

>>>> Вечером 6 января я ехал с работы, предвкушая удовольствие от предстоявшего финала чемпионата мира по хоккею с участием молодежных сборных Канады и России, где мои соотечественники имели все шансы на победу и золотые медали.

...Моим американским коллегам не понять специфику канадо-российских взаимоотношений в том, что касается хоккея. Эти связи сложились еще до моего рождения и претерпели немало перемен на протяжении моей жизни. Это отношения равноправных партнеров, испытывающих взаимное уважение и не боящихся бросить вызов друг другу. Вот о чем я думал, берясь за проект под названием «Премия инноваций Сколково».

...Пока же я продолжаю переживать проигрыш канадских хоккеистов в чемпионате мира – и радуюсь первым достижениям «Премии инноваций Сколково». До окончания срока приема заявок на участие в этом конкурсе остался практически месяц. К 11 января участие в проекте приняли более 2 тыс. человек, на конкурс поданы почти 600 великолепных идей и мы получили около 4800 комментариев к этим идеям. Точные данные вы найдете на сайте www.cisco.ru/go/skolково, я же предлагаю проанализировать полученные к настоящему времени данные.

...Есть повод и для некоторых разочарований: среди участников очень мало женщин. Кроме того, мы получили гораздо меньше заявок, чем хотелось бы, от студентов и исследователей. Большинство участников – предприниматели мужского пола.

И все же не может не поражать, сколь динамично наш конкурс развивается. Лидеры и ведущие идеи все время меняются. И так же, как в финальном матче за звание чемпиона мира по хоккею среди молодежных команд, я ожидаю коренного перелома в «третьем тайме» нашего соревнования, тем более что за последние пару-тройку недель заметно выросло количество участников и число новых заявок, несмотря на новогодние каникулы в России.

[комментировать](#)

Петр ДИДЕНКО Зачем ставить большие цели

>>>> Большие цели – это большие мечты. Планы помогают понимать, как претворять мечты в жизнь. Какие преимущества дают, например, планы на год?

Цели на год сложнее «провалить». Если в феврале произойдет непредвиденное событие и вы вынуждены будете заниматься преодолением его последствий две недели, то будет еще много времени до конца года, чтобы выполнить первоначальные планы. Если планы на месяц, то вы наверняка их «завалите».

Большие цели позволяют не дергаться. Если вы знаете, что у вас есть Цель, которой надо достичь когда-то нескоро, но обязательно, то вы правильно спланируете ресурсы и время для того, чтобы выполнить то, что нужно, в ненапрягающей манере. Если же у вас планы краткосрочные, может просто не найтись никакого удобного времени, а только «сейчас, здесь, аврал».

Известно также, что сознание того, что впереди еще «о-го-го как много времени», разлагает и внушает иллюзию, что пока можно не дергаться, и сейчас можно не дергаться, и сейчас тоже, а потом вдруг – ой, завтра дедлайн, а у нас ничего!! Поэтому обязательно большую Цель надо порезать на несколько целей поменьше.

План – хорошая возможность посмотреть со стороны на то, что планируется сделать, и определить конкретные проблемные места, в которых всему плану грозит провал. Надо подумать, улучшить план и знать, как мы решаем предсказуемые проблемы.

Итого. Важно помнить, что для того, чтобы реализовать Мечту, нужен хороший большой план. А чтобы реализовать большой план, нужно уметь делить его на много мелких планов. Будет здорово, если вы учтете все возможные риски и покажете план другим людям, чтобы они дали feedback и присоединились к претворению мечты в жизнь.

[комментировать](#)

Реклама в номере

АЙТИ Тел.: (495) 974-7979 Факс: (495) 974-7980 E-mail: info@it.ru www.it-scs.ru c. 69	Факс: (495) 775-3790 E-mail: info@ventss.ru www.ventss.ru c. 81	E-mail: nst@nstel.ru www.nstel.ru c. 37	ADM PARTNERSHIP Тел.: (495) 958-5665 Факс: (495) 958-5675 E-mail: business@admpartnership.ru www.admpartnership.ru c. 75	Факс: (495) 663-8261 www.lenovo.com/ru c. 3
АМДТЕХНОЛОГИИ Тел.: (495) 963-9211 Факс: (495) 225-7431 E-mail: info@amd-tech.ru www.amd-tech.ru c. 80	ИНТЕРСПУТНИК Тел.: (499) 252-8333 Факс: (499) 271-0784 E-mail: dir@intersputnik.com www.intersputnik.ru . . 4-я обл.	СОКК Тел./факс: (846) 955-0963 E-mail: sales@soccom.ru www.soccom.ru . . . 2-я обл.	EATON Тел.: (495) 981-3770 Факс: (495) 981-3771 E-mail: UPSRussia@eaton.com www.eaton.ru c. 67	POWERCOM Тел.: (495) 651-6281 Факс: (495) 651-6282 www.pcm.ru c. 68
ВЕНТСПЕЦСТРОЙ Тел.: (495) 775-3791	НОВЫЕ СИСТЕМЫ ТЕЛЕКОМ Тел.: (495) 641-4045 Факс: (495) 641-4048	ТМК-ТЕЛЕХАУС Тел.: (495) 790-7807 Факс: (495) 790-7574 E-mail: info@tmk-telehouse.ru www.tmk-telehouse.ru. c. 79	LENOVO Тел.: (495) 663-8260	QNAР Тел.: (495) 772-9909 www.qnap.ru c. 7
			UNITED ELEMENTS Тел./факс: (495) 790-7434 E-mail: center@uelements.com www.uel.ru c. 78	

Указатель фирм

3M 85	HR-VISION 6, 22	Standard & Poor's 49	«Интеллект Телеком» 8	«Радист» 23
A&CM Consulting 29	Holding Group 6, 22	TELE2 23, 51, 54	«ИнтелТелеком» 12	«РБК-ИС» 49
ABBYU 16	Huawei Technologies . . . 8, 13,	Telefonica 58	МОКС «Интерспутник» . . . 14	«РБК-ТВ Москва» 49
ADM Partnership 75	45, 53, 54, 58	Telefonica O2 Slovakia . . . 53	«Инфосистемы	«Ростелеком» 11, 12,
Akorri Networks 12	IBM 15, 20, 87	T-Mobile Germany 17	Джет» 15, 18, 45	«РусАТ» 38
Alcatel-Lucent 13, 19, 53,	IBS Group 49	Tripp Lite 68	«Казахтелеком» 33	«РyCАТ» 38
54, 58	IDC 21	TSS 85	«Караван» 36	«Рэйс-Коммуникайшн» . . . 14
Altor Networks 12	i-Free Innovations 16	TTI Telecom 20	«Киевстар» 8, 41	«Связной Банк» 15
Amazon.com 16	INELT 67, 68	Uniflair S.p.A. 12	ООО «Клорайд Рус» 66	«Связьинвест» 48
Amdocs 20, 20, 51, 52, 53, 54	InfNet Wireless 88	United Elements 79	«Комкор» 36	«Северо-Западный
Ansul 85	Informa Telecoms & Media . 58	Uptime Institute 74, 78	«Комстар» 8	Телеком» 15, 49
Apple 39	INFRATEL 12	US Bancorp 63	«Комстар-ОТС» 8, 12, 23,	«Северсталь» 49
ASHRAE 80	Iskratel 15	Utel 8	28, 34, 38, 49	«Сибирьтелеком» 49
AT&T 56, 58	JP Morgan Chase 63	VansonBourne 21	«Комстар-Регионы» 12	«Синтра» 31, 53
AT&T Mobility 53	Juniper Networks 12, 46, 87	Verizon 56	«Корбина» 29	ООО «Сиско Системс» . . . 45
Attachmate Corp 12	Landata 14, 66	«Vervysell Проекты» 15, 45	ФГУП «Космическая	«Система Телеком» 8, 12
Avaya 12, 30	Lenovo 14	Visa 63	связь» 11, 14	АФК «Система» 8, 12, 49
Bank of America 63	LHS 54	VIVACOM 58	КРОК 70	«Ситроникс» 19, 54
«Beeline-Украина» 41	LineSider Technologies 12	VMware 21	ЗАО «КТС» 12	«Ситроникс-Татарстан» . . . 19
Bercut 12	Mail.ru Group 49	Vodafone 58	«Кубинтерсвязь» 23	«Скай 1800» 13
British Telecom 53, 58	Microsoft 10, 11	Wells Fargo Bank 63	«Кубтелеком» 23	«Скай Линк» 13, 23, 29,
BT Global Services 58	OOO «Microsoft Рус» 11	XL Axiata 53	«ЛАНК Телеком» 12	30, 35, 51, 54
CA Technologies 21	MITSUI & Co. 12	Zelax 47	«Лощман Плюс» 14	«Скандинавский Дом» 11
China Mobile 58	MONT 11	Zenoss 21	«М.Видео» 18	«Сочителеком» 23
Chloride 68, 88	MOTOROLA 19	ZTE 54	МГТС 8, 34	«Стрим-ТВ» 23
Cisco 12	Naumen 12, 20	ZyXEL Россия 64	«МегаФон» 8, 11, 12,	«Сумма Телеком» 11, 51
Citrix Systems 11	NEC 13	«Абитех» 68	13, 14, 23, 28, 31, 32,	«Сургутнефтегаз» 49
C-Media 12	«NEC Нева Коммуникационные	«АЙТи-СКС» 70	51, 52, 53, 54, 60	ИА «Татинформ» 19
CNews 21	Системы» 11, 13	«АКАДО-Столица» 29, 37	ММВБ 49	«Таттелеком» 19, 40, 41
CNews Analytics 21	NetApp 12	«Аладдин Р. Д.» 9, 10,	МСС 13	«Телесет» 41
Comcast 53	NICE 12	15, 87	МТС 11, 12, 13,	«Технический центр
Compellent Technologies 12	Nokia Siemens Networks . . 17,	«АМДтехнологии» 80	15, 23, 29, 34,	ПТУС ТАССР» 8
Comverse 52, 53	45, 53, 54, 58, 60, 61	«АРМО-Системы» 84	49, 54, 56, 58, 61	«Технический центр связи
Convergis 53	Novell 12	«Атлант-Информ» 10	«МТС Россия» 29, 34	Министерства связи
CSG 53	Okstel 12	ИФК «Банкорп» 19	МТТ 11, 20	Татарской АССР» 8
Dell 12	Optenet 15	«Башсел» 54	«МТУ-Интел» 8	«Техносерв» 20
Deutsche Telekom 58	Oracle 18, 53, 87	«Белгородские цифровые	«МТУ-Информ» 8	«ТМК-Телехаус»
DeviceFidelity 63	Paragon Software 16	магистрала» 12, 28	«МувиКом» 88	ТНПКО 41
Dupont 85	PEOPLEnet 8	«Беркут» 54	«Мультирегион» 23	«Торус-Телеком» 19
Eaton 14	Powercom 66	«Билайн Бизнес» 30	«Национальные	«Узбектелеком» 33
eBay 16	PwC 11	«Веллинк» 46	телекоммуникации» 49	«Украинская
Ericsson 26, 45, 53, 54, 58	Qiwi 12	«Волгателеком» 14, 49	«Новосибирская мультисервисная	мобильная связь» 8
ESET 11	QTech 39	«ВымпелКом» 8, 11, 12,	компания» 12, 28	«Укртелеком» 41
Facebook 29	R&D NetCracker 20	13, 14, 28,	«Новые Системы	«Уралсвязьинформ» 49,
Frost & Sullivan 50, 53	Rainbow Security 62	29, 32, 41, 42,	Телеком» 37	51, 54
General Electric 67	Raybrook Ltd 49	51, 52, 53, 54, 60	НТЦ АРГУС 20	УК «Финам Менеджмент» . . 48
Genesys 12	SAP 18	«Гарс Телеком» 11	НЭК	ОАО «ФСК ЕЭС» 18
Gigaset Communications 15	Schneider Electric 12, 70,	«Голден Телеком» 8, 29	Инфокоммуникации» 13	«ЦентрТелеком» 14, 49
Google 34, 39	85	«Дагсвязьинформ» 48, 49	«Открытые Технологии» . . . 15	ЦТС 23
Great Lakes 85	Siebel 18	«Дальсвязь» 49	«Петер-Сервис» 15, 53, 54	«Энергодата» 18
Groupon 49	Siemens IT Solutions	«ДатаДом» 73	«Петерстар» 31	«Энфорта» 12, 14
GSMA 11	and Services 20	НИИ «Дельта» 8	«Плюс Один» 11, 13	«ЭР-Телеком Холдинг» 40
Hitachi Global Storage	Socomec UPS 88	«Дельта-Телеком» 13	АНО «Радиочастотный	«ЭР-Телеком» 15, 41
Technologies 11	Sprint 53, 58	«Евросеть» 11	центр МО» 42	ЮТК 23

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.