

Фигуранты фондового рынка-2012: ПОСТНОВОГОДНЕЕ РЕВЮ



Выход на IPO «МегаФона» – последним из большой тройки, тянувшаяся реорганизация «Ростелекома», споры владельцев VimpelCom, проблемы с рентабельностью РБК, движение в активах Mail.ru, покупка Сбербанком «Яндекс.Денег» – эти и другие события формировали картину рынка акций отечественных компаний в ушедшем году.



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

Прошедший год оказался для мировых фондовых рынков довольно удачным, но динамика российского рынка акций выглядела несколько более скромной. При этом фондовый рынок РФ из-за высокого бета-коэффициента демонстрировал сильную волатильность: отечественные индексы показывали опережающую динамику во время глобальных ралли, но при коррекции падали сильнее аналогов. Несмотря на большое количество внутренних новостей, определяющее влияние на динамику котировок российских эмитентов оказывали внешние тренды и восприятие рисков инвесторами.

тывать интересы всех акционеров компании, оказало поддержку акциям оператора в конце года.

...и насыщенный для сотовиков

Более успешно сложился прошедший год для российских операторов мобильной связи. Так, акции МТС, обращающиеся на Московской бирже, в 2012 г. подорожали на 33,7%, достигнув отметки в 246 руб. На протяжении всего прошлого года бумаги компании демонстрировали восходящий тренд, скорректировавшись вниз только в мае (с 240 до 206 руб. за акцию) – вместе с отечественными индексами. Однако коррекция была отыграна инвесторами уже в середине июля, а в сентябре бумаги оператора зафиксировали максимальное значение года – 254,7 руб. за акцию.

В целом прошлый год выдался для МТС весьма насыщенным на корпоративные события. Так, росту капитализации оператора способствовали новости о расширении географического покрытия связи стандарта 3G. Позитивное влияние на капитализацию оказала информация о возобновлении работы МТС в Туркменистане после полуторагодового перерыва, а также отмена через суд национализации узбекской «дочки» МТС (правда, после уплаты весомого штрафа в размере \$600 млн). Динамика роста финансовых показателей оператора в течение года выглядела благоприятно: так, консолидированная чистая прибыль за III квартал по US GAAP составила \$630 млн против убытка в \$681,8 млн во II квартале 2012 г. Сильные рыночные позиции и стабильную деятельность МТС отметило в конце года и агентство Fitch, присвоив компании рейтинг «BB+» со «стабильным» прогнозом.

Капитализация VimpelCom Ltd. на Нью-Йоркской бирже (NYSE) возросла за прошедший год на 11% – до уровня \$10,49. Год для бумаг телекоммуникационного холдинга оказался очень сложным и волатильным – в июне акции опустились к минимальной исторической отметке в \$7,23. Восстановить потери они смогли только в сентябре, зато в октябре достигли уровня в \$12,26.

Не лучший год для «Ростелекома»...

Для национального телекоммуникационного холдинга «Ростелеком» прошедший год оказался весьма неудачным. Начав его с отметки 153 руб. за бумагу, акции оператора скатились в мае к годовому минимуму в 105 руб. Всего по итогам 2012 г. бумаги компании потеряли 21%, остановившись на отметке 120,4 руб.

На динамику акций оказал влияние ряд значимых сделок. Так, в прошлом году «Ростелеком» консолидировал 100% акций НТК, стал владельцем оператора мобильной связи «Скай Линк» и британского оператора RETN, приобрел 100% голосующих акций ЗАО «Норильск-Телеком». Однако, несмотря на приобретения и весьма неплохую отчетность в течение всего года, бумаги «Ростелекома» продолжали двигаться вниз. Причиной снижения капитализации, вероятно, стало отставание процесса реорганизации компании от намеченного графика – по заявлению главы Минкомсвязи Николая Никифорова, завершение реформы возможно в октябре 2013 г. В то же время сделанное на декабрьском совете директоров «Ростелекома» заявление вице-премьера РФ Аркадия Дворковича о том, что в ходе предстоящей реорганизации необходимо учи-

Справка ИКС



Индекс РТС по итогам 2012 г. прибавил 11% – до 1528,47 пункта. Капитализация индекса ММВБ увеличилась за год лишь на 5%, составив 1474,72 пункта. Отраслевой индекс ММВБ «телекоммуникации» завершил год с ростом капитализации на 4% – до 2157,23 пункта.

На динамику акций по-прежнему оказывал влияние конфликт между Telenor и Altimo, которые продолжили споры о долях владения в VimpelCom.

Однако важнейшим, пожалуй, событием на рынке мобильной связи стало публичное первичное предложение (IPO) компании «МегаФон» – последнего непубличного оператора большой тройки. IPO состоялось на Лондонской фондовой бирже (LSE) и Московской бирже в конце ноября 2012 г.: инвесторам было предложено 14,8% уставного капитала (с учетом greenshoe) по цене \$20 за бумагу. Объем привлеченных средств составил \$1,83 млрд; таким образом, оценка «МегаФона» в рамках IPO равнялась \$12,4 млрд. Следует отметить, что после публичного размещения акции оператора демонстрировали восходящую динамику – их стоимость на Московской бирже выросла к концу года более чем на 11%. Примечательно также, что большую часть заработанных на размещении «МегаФона» денежных средств Altimo израсходовала на покупку акций VimpelCom Ltd., в итоге ее пакет достиг 47,85%.

Под сенью Facebook

Лидером роста капитализации среди интернет-компаний стали бумаги Mail.ru Group, которые за год прибавили 31% (до \$34 за шт.). Начало прошлого года для них выдалось вполне удачным – с январской отметки в \$26 акции Mail.ru Group подобрались к цене \$43,7, что и стало максимумом года, однако затем стали резко терять в стоимости. Снижение проходило на фоне значительной коррекции бумаг Facebook (после IPO соцсети в мае), что оказало влияние на котировки всех ведущих интернет-компаний. Второе полугодие акции Mail.ru Group провели в «боковике» \$30–35. В конце лета хорошим поводом для роста послужило сообщение о выплате специальных дивидендов в размере \$3,80 на акцию. Дополнительную поддержку акциям компании оказала новость о продаже инвесторам 12 млн глобальных депозитарных расписок (GDR) Mail.ru Group стоимостью \$34 за шт., на общую сумму \$408 млн. Волну распродаж Mail.ru Group спровоцировало заявление Алишера Усманова о планах отойти от активного управления подконтрольными ему компаниями, консолидировав перед этим все свои активы в один холдинг. Далее Mail.Ru Group сообщила об уменьшении своей доли сразу в нескольких активах. Например, компания продала свой пакет в социальной сети Facebook, и теперь ее доля составляет 0,52%. Чуть позже стало известно, что Mail.ru Group полностью вышла из состава акционеров Groupon и Zynga.

Yandex N.V., материнская компания ведущего российского поисковика «Яндекс», по итогам года прибавила более 9% капитализации – акции достигли отметки \$21,54. Среди основных событий, повлиявших на динамику стоимости бумаг, стоит отметить сделку между Facebook и Face.com, на которой Yandex смог прилично заработать. Напомним, что российский поисковик инвестировал в Face.com \$5,3 млн в 2010 г. совместно с инвестфондом Rhodium («Яндексу» принадлежало 18,4% акций компании). Нельзя не отметить, что значи-

тельный вклад в динамику акций Yandex внесло ожидание IPO Facebook. Одним из ключевых для рынка событий стало в преддверии Нового года вхождение Сбербанка в капитал платежной системы «Яндекс.Деньги». За 75%-ный пакет акций этого актива госбанк заплатил \$60 млн, после завершения сделки пользователи системы получают доступ к инфраструктуре Сбербанка, который, в свою очередь, сможет продвигать свои финансовые услуги клиентам «Яндекса».

Общепромышленный позитив

Бумаги АФК «Система» завершили год, прибавив 9,4% – до уровня 25,49 руб. Весь год бумаги холдинга торговались в рамках широкого коридора 22–28 руб. Динамика их рыночной конъюнктуры формировалась под влиянием ряда корпоративных новостей. С одной стороны, давление на акции холдинга оказывали проблемы основного актива, оператора МТС, связанные преимущественно с ведением бизнеса в некоторых странах Центральной Азии. С другой стороны, агрессивная политика менеджмента холдинга по отношению к ряду публичных активов поддерживала акции АФК «Система». Тем не менее, несмотря на проводимую диверсификацию бизнеса, акции «Системы» по-прежнему остаются недооцененными.

Бумаги РБК по итогам года потеряли 7,33%, остановившись на отметке 12,699 руб. Начало года для акций компании сложилось весьма успешно – в I квартале стоимость их практически удвоилась (с 13,75 до 24,38 руб.). Определенную поддержку РБК оказала информация о планах Комитета по вопросам собственности внести изменения в закон об иностранных инвестициях в предприятия, имеющие стратегическое значение для обороны страны и безопасности государства, – законопроект предлагал дополнить список стратегических предприятий компаниями, оказывающими «социально значимые услуги в сети Интернет», к числу которых относится основная масса ведущих российских интернет- и медиакомпаний. По итогам 9 месяцев 2012 г. РБК опубликовала хорошую отчетность по МСФО: выручка достигла 3,754 млрд руб. (+25% год к году), при этом наибольшими темпами росли сегменты «Телевидение» и «Интернет». Однако инвесторы не могли проигнорировать информацию о слабом контроле над затратами – рентабельность бизнеса РБК остается основной проблемой компании (несмотря на выход показателя в положительную зону).

Для акций IBS Group 2012 г. также оказался весьма благополучным – капитализация компании увеличилась на 5,13%, до \$15,98 за бумагу. Помимо общепромышленного позитива спросу на акции компании способствовала публикация в целом благоприятной отчетности по US GAAP за 6 месяцев 2012 г. Так, консолидированная выручка ГК IBS увеличилась на 6% по сравнению с аналогичным периодом прошлого года и составила \$378 млн. Выручка в сегменте ИТ-услуг выросла на 1,8% в долларовом и на 12,4% в рублевом выражении, а в сегменте разработки программного обеспечения – на 13,5% в долларовом выражении. ИКС

Один спутник вместо трех

Если сегодня для охвата ТВ-вещанием всей территории России требуются три спутника, то планируемый к запуску в 2013 г. ABS-2 справится с этой задачей в одиночку, уверен Тимофей АБРАМОВ, коммерческий директор «ИНТЕРСПУТНИКА».



Тимофей АБРАМОВ

– В 2009 г. «ИНТЕРСПУТНИК» подписал контракт с оператором Asia Broadcast Satellite (ABS) на долгосрочную аренду части транспондеров ABS-2. Потребовалось ли за эти три года провести совместно с оператором какую-либо работу?

– Мы принимали активное участие в конфигурировании российского луча спутника ABS-2, потому что мы, конечно, лучше, чем Asia Broadcast Satellite, знаем российский рынок; знаем, где и какие виды услуг востребованы. Например,

необходимо, чтобы в зону обслуживания с высокой энергетикой попали все города-миллионники, все территории с наибольшей плотностью населения. Оператор пошел нам навстречу: от Калининграда до Владивостока в Ku-диапазоне мы получаем ЭИИМ до 51 дБВт. Нам также нужно, чтобы страны СНГ были включены в зону обслуживания на требуемом уровне энергетикой. Например, Таджикистан: сейчас с ABS-1 при помощи «ИНТЕРСПУТНИКА» вещается все национальное телевидение Таджикистана, и нам важно, чтобы на спутнике ABS-2 такая возможность сохранялась. Владелец аппарата учел и это наше пожелание.

– Сколько транспондеров в каких диапазонах арендует «ИНТЕРСПУТНИК» на ABS-2 и какие планы связывает с этой емкостью?

– В общей сложности 12 транспондеров Ku-диапазона, которые могут быть использованы как для спутникового непосредственного ТВ-вещания, так и для организации сетей передачи данных. С учетом того, что спутник обеспечивает хорошее покрытие с уверенной энергетикой, для приема ТВ-сигнала можно использовать антенны малого диаметра (60 см). Одно из важных преимуществ этого спутника с точки зрения географического покрытия – возможность распространения ТВ-сигнала на всю территорию России. Сейчас для этого требуются три аппарата, а ABS-2 справится с такой задачей в одиночку, что означает реальную экономию для операторов, которые планируют заниматься бизнесом на его базе.

Транспондеры C-диапазона традиционно применяются для организации выделенных каналов связи. В настоящее время мы с коллегами из ABS определяем их окончательные технические характеристики. В зависимости от них будет определена и емкость C-диапазона, используемая в интересах наших клиентов.

– ABS-2 заменит действующий спутник ABS-1. Все клиенты «ИНТЕРСПУТНИКА» перейдут на новый спутник, потому что старый закончит службу?

– ABS-1 функционирует с 1999 г., но у него достаточно ресурса, чтобы активно работать еще лет пять. Владелец аппарата принял решение перевести его в другую орбитальную позицию, поскольку ABS-2 полностью перекрывает его возможности.

На ABS-1 большая часть арендуемой нами емкости относится к C-диапазону, а на ABS-2 мы расширяем свое присутствие и в Ku-диапазоне. Поэтому на ABS-2 не только перейдут все клиенты ABS-1, но появятся и новые. Практически весь арендованный ресурс ABS-2 – 12 транспондеров Ku-диапазона – уже продан. Сейчас сделки в процессе завершения, надеемся закрыть их до конца года. Возможно, какая-то часть емкости еще будет доступна в следующем году, так что рынок должен знать об этом спутнике, о его возможностях. Мы помогаем в этом случае даже не себе, а нашим пользователям, нынешним и будущим.

– Есть ли у «ИНТЕРСПУТНИКА» планы по аренде емкости следующего спутника ABS-2A, который должен быть запущен в ту же позицию в 2014 г.?

– Мы рассматриваем эту возможность. Но для того чтобы уверенно ответить на вопрос, необходимо все же дождаться запуска ABS-2 и посмотреть, насколько он дефицитен. Хотя, возможно, начнем переговоры и до запуска. Второй аппарат ABS-2A в этой точке обеспечивает нашим клиентам, во-первых, гарантированное наращивание емкости и возможность строить долгосрочные планы, а во-вторых, резервирование. Невозможность резервирования – ахиллесова пята аппаратов, которые стоят в орбитальных позициях по одному. Вот почему мы поддерживаем планы по запуску в эту точку второго аппарата и готовы начинать переговоры как с пользователями, так и с оператором.

Характеристики спутника ABS-2:

- ▶ орбитальная позиция – 75° в.д.;
- ▶ полезная нагрузка – 88 транспондеров C-, Ku- и Ka-диапазонов, подключенных к 8 антеннам;
- ▶ мощность полезной нагрузки – более 12 кВт;
- ▶ масса спутника – 2800 кг, с топливом – 6000 кг;
- ▶ зона покрытия – Ближний Восток, Африка, Азиатско-Тихоокеанский регион, Россия и страны СНГ;
- ▶ SAC – 15 лет;
- ▶ изготовитель – Space Systems/Loral;
- ▶ ракета-носитель – Ariane 5;
- ▶ запуск запланирован на 2013 г.

Надо сказать, точка 75° в.д. уникальна. Ее физическое расположение позволяет охватить всю территорию РФ с максимальными энергетическими характеристиками. Поэтому совместно с ABS мы будем повышать ее коммерческую привлекательность, использовать ее потенциал для России и других стран.

Беседовала Лилия ПАВЛОВА



121099, Москва, Россия, 2-й Смоленский пер., д. 1/4
Тел.: +7 (499) 252-8333
Факс: +7 (499) 241-0784
dir@intersputnik.com

«Ростелеком». 20 лет спустя

В 2013 г., в сентябре, исполнится 20 лет со дня официальной регистрации ОАО «Ростелеком» – самой крупной телеком-компания в стране, пережившей, пожалуй, самые большие пертурбации.



Владимир
ЛИТВИНОВ,
миноритарный
акционер
ОАО «Ростелеком»

По итогам прошедшего года

«Ростелеком» сохранил почти монопольные позиции на рынке фиксированной телефонии и лидирует на рынке ШПД. Число абонентов ШПД возросло до 8,9 млн, число подписчиков платного ТВ достигло 6,4 млн. Следует отметить, что после консолидации «Скай Линка» структура объединенного бизнеса оператора стала более сопоставимой с бизнесом большой тройки. Однако по тем-

пам роста выручки «Ростелеком» уступает этим грандам, в основном из-за стагнации фиксированной телефонии (местной и МГ/МН-связи). Впрочем, и объем выручки у МТС (\$12 млрд) превысил показатели «Ростелекома» (\$10,2 млрд), а в спину уже дышат «МегаФон» и «ВымпелКом». Хотя на рынке мобильной связи «Ростелеком» – нишевой игрок, тем не менее перспективы объединения с Tele2 и возможная реализация MNP могут быть для оператора весьма благоприятны. Конечно, рынок мобильных услуг в настоящее время насыщен, темпы роста не превышают 2% в год, но мобильная передача данных включает в себе существенный резерв (до 40%) роста выручки.

В настоящее время в «Ростелекоме» работают 165 тыс. человек, при том что штат операторов большой тройки почти в шесть раз меньше. Разработка и реализация долгосрочной программы перевода местных сетей на «оптику» позволит вдвое сократить штат «Ростелекома». Впрочем, на мой взгляд, для государственного оператора не менее важный показатель – число вновь соз-

даваемых рабочих мест при внедрении современных инфокоммуникаций.

Сегодня рынок связи России поделен между четырьмя телеком-монстрами: госоператором «Ростелеком», старейшей и одновременно самой публичной компанией, и тремя частными операторами МТС, «ВымпелКом» и «МегаФон». Именно различием в принадлежности, думается, объясняется разница в трендах капитализации компаний. Так, у МТС положительная годовая динамика роста акций – 35% (180/245 руб. за акцию), а у «Ростелекома» тренд, наоборот, отрицательный – 20% (145/120 руб. за акцию). И это при наличии у «Ростелекома» общероссийской сети фиксированной телефонии (70% общего числа линий) и значительного ресурса объектов недвижимости.

Практически весь год «Ростелеком» подвергался информационным и прочим атакам конкурентной среды. Оклады, бонусы, «парашюты» и опционы его руководства становятся, в отличие от частных структур, достоянием общественности и вызывают негативное к нему отношение. Все-таки госоператор – это своего рода национальное достояние. Действительно, «народ хочет знать» (при штате, напомним, 165 тыс. чел.) и требует объяснений, за что топ-менеджмент и совет директоров получают такие опционы, «парашюты» и т.д. Любопытно, что серьезный разрыв в оплате между чиновничьей верхушкой и рядовыми служащими образовался почти 100 лет назад. «В 1914 г. оклад начальника Главного управления почт и телеграфов в 50 раз превышал оклад рассыльного и в 30 раз – оклад надсмотрщика», – писал министр связи Н.Д. Псурцев в книге «Развитие средств связи в СССР». Сегодня оклады президента «Ростелекома» и низового эксплуатационного звена различаются примерно в 100 раз, а «парашют» президента составляет 200 млн руб. – комментарии, как говорится, излишни.

Конечно, на функционировании «Ростелекома» скандальности и

Что было

Принятый в 1987 г. закон о госпредприятии подорвал стабильность административно-командной системы управления экономикой, по существу лишив Минсвязи СССР функций распределения материальных и финансовых ресурсов, и предприятия магистральной связи, не имея прямых доходов и клиентов, оказались в затруднительном положении. В результате в 1990 г. было образовано акционерное общество «Совтелеком», взявшее на себя задачи эксплуатации и развития магистральной

сети связи. А в 1991 г., уже после распада Союза, «Совтелеком» был преобразован в международное акционерное общество «Интертелеком», правопреемником которого и стал в 1993 г. российский национальный оператор «Ростелеком».

На первом этапе «Ростелеком» объединил 22 филиала, в том числе территориальные центры управления междугородными связями (ТЦУМС), расположенные по всей России, Главный центр управления междугородными связями (ГЦУМС), а несколько позднее и

международную станцию МнСРТ. Первым гендиректором «Ростелекома» стал Олег Белов (он дольше других занимал этот пост – в 1993–1999). Сохраним для истории имена и остальных гендиректоров: Николай Королев (1999–2001), Сергей Кузнецов (2001–2003), Дмитрий Ерохин (2003–2007), Константин Солодухин (2007–2009), Антон Колпаков (2009–2010), Александр Провоторов (с 2010-го по настоящее время). В 2000 г. с целью наращивания клиентской базы и устойчивого роста доходов к «Ростелекому» было

Действия госорганов

Шесть гендиректоров сменилось в «Ростелекоме» за последние 12 лет, в среднем по два года на человека. Для столь крупной компании это недопустимо. Сухая статистика выявляет жесткую взаимосвязь между отставками министров связи и гендиректоров «Ростелекома» (после ухода министра связи Булгака ушел гендиректор «Ростелекома» Белов, после отставки Реймана – Солодухин). Вместе с тем завершение реформы «Связьинвеста» продолжает откладываться. Срывается выполнение президентского указа о завершении в марте 2013 г. второго этапа реформы «Связьинвеста».

Я задаю себе вопрос, а где в Москве на позициях топ-менеджеров крупных телеком-операторов сохранились профессиональные связисты – выпускники институтов связи. В минувшем году последние московские аксакалы от телекоммуникаций – Мартиросян, Заболотный, Кравченко – ушли в отставку, и лишь академик Минсвязи Наум Семеныч Мардер, как феникс, возродился в «Ростелекоме». Почему «эффективными менеджерами» «Ростелекома» могут быть юристы, переводчики и даже строители, а профессионалы-связисты признаются негодными для руководства национальным оператором? Почему в его совете директоров интересы собственника-государства представляют в основном финансисты, инвестбанкиры, юристы, хотя «Ростелеком» – это «народное достояние», активы компании фактически стали создаваться более 100 лет назад со строительством первых линий связи. К примеру, во времена министра связи Булгака председателями советов директоров крупнейших компаний связи были назначены бывшие министр и заместители министра связи СССР.

Я вспоминаю работу в совете директоров ММТ под руководством бывшего министра связи СССР Василия Александровича Шамшина, который – не получая, кстати, как и все члены СД, бонусов и опционов – с успехом справлялся со сложными процессами функционирования предприятий связи после приватизации.

Проблема «Ростелекома»

во многом состоит сегодня в том, что очередные «эффективные менеджеры» не работали непосредственно

в телекоммуникациях. Они просто не чувствительны к традициям, не знают историю связи и историю появления компаний, в которые их занесло стечением обстоятельств. Поэтому не приходится удивляться принимаемым управленческим решениям. До сих пор плохо понимаю, как может происходить консолидация активов «Ростелекома» в московском регионе, почему во главе этого процесса стоит компания НТК – кабельный и интернет-провайдер, который должен консолидировать технологические комплексы фиксированных сетей «дочек», в том числе старейших предприятий российской связи.

В следующем году исполняется 80 лет с момента, когда 1 января 1934 г. нарком связи Рыков подписал приказ о выделении Московской междугородной станции из Центрального телеграфа и подчинении ее Наркомсвязи. Не настала ли пора обратной консолидации активов ЦТ и бывшей «междугородки», а также московских «дочек» «Ростелекома»? На мой взгляд, сегодня для госоператора наступает время, когда для реализации стратегической концепции развития должны появиться профессиональные топ-менеджеры новой формации со своей командой, не обремененные шлейфом землячества, совместной учебы и т.п.



В последнее время вновь актуализировались вопросы дальнейшей приватизации «Ростелекома» (хотя создается впечатление, что государство нащупало систему контроля электронных СМИ посредством Роскомнадзора и «Ростелекома» и ослаблять эту функцию не собирается). В целом собственная инфраструктура национального оператора – сеть магистральных каналов и местные сети, центры обработки данных, – облачные сервисы, развитие услуг ШПД и высокомаржинального мобильного бизнеса, а также выполнение крупных национальных проектов («электронное правительство», «Сочи-2014» и др.) создают серьезную основу для успешной реализации стратегии компании. Все это дает основания прогнозировать в долгосрочной перспективе существенный (в три-четыре раза) рост капитализации «Ростелекома». ИКС

Что было

присоединено ОАО «Московский междугородный и международный телефон», ставшее его Столичным филиалом. В последующие годы «Ростелеком» приобрел оператора IP-телефонии «Зебра Телеком» и интернет-провайдера «РТКомм».

В 2010 г. было принято решение о присоединении к «Ростелекому» семи межрегиональных компаний связи («Центртелеком», «Сибирьтелеком», «Дальсвязь», «Уралсвязьинформ», «Волгателеком», СЗТ и ЮТК) и «Дагсвязьинформа». С учетом приобретенных операторов «Скай

Линк» и «Национальные телекоммуникации» объединенная компания сегодня предоставляет весь комплекс телекоммуникационных услуг: фиксированную и мобильную связь, широкополосный доступ в Интернет, платное ТВ.

Вместе с тем окончательная ликвидация холдинга «Связьинвест» сдерживается не присоединением последних дочерних компаний: «Центральный телеграф», ММТС9, «Башинформсвязь», «Ингушэлектросвязь» и «Чукоткасвязьинформ». В этих, прежде всего московских «дочках», видимо,

имеются влиятельные миноритарии, не согласные с ценой поглощения компаний.

Таким образом, в результате первого этапа реформы «Связьинвеста», поглощений и приобретений активов в России создан ведущий национальный оператор по всему спектру телеком-услуг: ШПД (1-е место в России по числу абонентов), цифровое ТВ (2-е место), услуги фиксированной связи (1-е место) и мобильной связи. Магистральная сеть «Ростелекома» насчитывает 500 тыс. км, а его абонентами являются 100 млн человек.

Организатор



Партнеры



Цена защиты бизнеса

На фоне множасьихся угроз и растущих объемов утечек данных бюджеты на информационную безопасность отнюдь не увеличиваются. Как в этой ситуации «инфобезопасникам» получать средства на развитие и поддержание своих систем и обосновывать свою позицию, обсудили участники круглого стола «Затраты на информационную безопасность. Много? Мало? Сколько надо?», организованного журналом «ИКС».

Как найти общий язык

В России бизнес и информационная безопасность исторически развивались в разных «системах координат». Поэтому обосновать затраты на ИБ бывает сложно. «Хорошая безопасность – это когда ничего не случается, – прокомментировал модератор круглого стола Михаил Емельяников (консалтинговое агентство «Емельяников, Попова и партнеры»). – А когда ничего не случается, трудно показать свою работу». Как же перевести на язык бизнеса ИБ-терминологию, и нужно ли это делать?



И. ТРИФАЛЕНКОВ, «Ростелеком»

Есть два пути преодоления этого «языкового барьера», считает Илья Трифаленков («Ростелеком»). Либо бизнес в лице директоров компании освоит терминологию безопасности (есть примеры, когда руководители высокого уровня способны оперировать такими понятиями, как «криптография», «межсетевые экраны», «резервное копирование», «защита от DDoS-атак» и пр., правда, в основном в силу личного интереса), либо «безопасники» выучат язык бизнеса и смогут объяснить, каким рискам подвергнется бизнес, если не будут приниматься меры информационной безопасности. Второй путь – наиболее реальный и становится мейнстримом, полагает И. Трифаленков.

Однако обучение должно быть взаимным. Подобно тому, как «безопасники» учат язык бизнеса, нуж-

но обучать информационной безопасности и ее терминологии весь персонал компании, от руководства до рядовых сотрудников. Александр Шубин (банк «Возрождение») уточнил, что обучение должно вестись дифференцированно для разных категорий сотрудников – топ-менеджеров, основного персонала, айтишников и сотрудников, к ИТ формально отношения не имеющих. Для каждой категории необходим свой процесс обучения. Скажем, первому лицу надо на уровне презентации быстро и сжато дать понимание того или иного вопроса, актуального в данное время. Для топ-менеджеров информация может быть более развернутой, но тоже строго дозированной. Чем ниже уровень, тем более широкие могут даваться знания. При этом оптимальным будет использование дистанционного обучения. «Тогда и смета, и состояние ИБ в компании будут хорошие», – резюмировал А. Шубин.

Еще один путь – привлечение внешних консультантов. Александр Сикорский (МТС) подчеркнул, что в части оценки рисков для руководства компании бывает более важно получить информацию не от своих сотрудников, а от консалтинговой компании, которая провела соответствующее независимое исследование. Причем компания должна иметь вес и известность в этой области. «Как правило, на основе таких убедительных результатов руководство склоняется в правильную сторону», – заключил А. Сикорский.

Как обосновать бюджет

В обосновании затрат на ИБ существуют два основных подхода – методический и практический. В первом случае используются методики и показатели эффективности (TCO, BCP, ROI и др.), во втором оцен-

ка делается без детальных расчетов на основе best practice (исходя из того, что стоимость системы ИБ должна составлять примерно 10–20% стоимости КИС). Говоря о преимуществах и недостатках каждого подхода, М. Емельяников заметил, что с точки зрения безопасности первый подход реализовать сложно: «Какой возврат инвестиций может быть от замка, повешенного на дверь гаража? Здесь только затраты, и они никогда не вернуться». Поддерживая эту позицию, Михаил Суконник (Radware) указал, что следует сначала делать отбор, опираясь на best practice, а потом сравнить выбранные решения с помощью тех или иных методик. «Но говорить об окупаемости этих решений нельзя, – уверен М. Суконник. – Надо помнить, что это – безопасность. Единственное, на что можно опираться, – недопущенный ущерб от атак, а это зачастую миллионы долларов».

Для руководства государственных организаций, по словам Владимира Поихало (Федеральный фонд обязательного медицинского страхования), наиболее веский аргумент при обосновании бюджета на ИБ – нормативные требования регуляторов и деятельность проверяющих органов. Однако бизнесу скорее понятны другие доводы, считает Александр Хрусталеv (МГТС). «Любая информация имеет определенную стоимость, любой простой выльется в потери, – убеждал он. – Соответственно, представляя решение по информационной безопасности руководству, нужно объяснять риски в денежном выражении: сколько потеряет компания при DDoS-атаке и т.д. Если риски ИБ перевести в деньги, разговор станет более конструктивным».



А. СИКОРСКИЙ, МТС

Методический и практический подходы, по мнению А. Сикорского, следует разумно сочетать. Наличие рисков и вероятность их реализации с помощью определенных методик можно трансформировать в вероятность потерь тех или иных финансовых средств. Другое дело, если подразделение обосновывает свою деятельность тем, что показывает, какие риски уже предотвращены и ущерба на какую сумму удалось избежать. В этом случае используются другие методики, опираясь на которые можно обосновывать затраты на дополнительные средства защиты.

В числе методик, понятных бизнесу, можно назвать матрицы рисков. Так, Александр Кириллов («Северсталь») рассказал, что предприятие, которое он представляет, с прошлого года ведет масштабное внедрение комплексной системы снижения издержек бизнеса. Составной частью системы является информационная безопасность, а общий подход предусматривает составление матрицы рисков, включающей характеристики рисков, вероятности их реализации и стоимостную оценку последствий этой реализации. Такие матрицы созданы на нескольких уровнях иерархии системы – и бизнес получил понятную картину и по бизнес-процессам, и по функциональным блокам, и по необходимым затратам.

Для обоснования бюджета на ИБ необходимы стратегия или хотя бы тактический план развития и поддержания уровня информационной безопасности в компании, учитывающие направления развития бизнеса. «Например, бизнес осваивает новые территории, где требуется внедрить определенные средства защиты, или создаются новые бизнес-единицы, новые сервисы. В этих случаях нужно провести анализ рисков и показать, что при запуске такого-то сервиса нужны такие-то вложения, – пояснил Дмитрий Устюжанин («ВымпелКом»). – Это позволит сформулировать бизнес-обоснование внедрения тех или иных средств или процессов ИБ. С другой стороны, развитие бизнеса обуславливает развитие ИТ – и план развития информационной безопасности должен учитывать ИТ-стратегию компании. И третье направление – обоснование затрат на поддержку уже существующих систем».

Говоря о рискованной методологии, о конкретных технических средствах обеспечения ИБ, о категориях подлежащих защите активов, следует учитывать динамическую природу этих объектов, считает Павел Волков (ARinteg). «Мир рисков можно разделить на две части. Есть часть аналитическая – мнение эксперта о том, что является объектом защиты, каковы требования к нему, что является рискованным сценарием и как ему противодействовать, – прокомментировал П. Волков. – И есть часть событийная – фактическая, говорящая о том, что на самом деле происходит в защищаемой системе. Поэтому если мы говорим об эффективной системе обеспечения ИБ, об обоснованном бюджете, нужно не только учитывать регуляторные требования, не только грамотно считать риски и правильно согласовывать с бизнесом стоимость активов, но и соотносить события, которые происходят с защищаемыми активами, с нашим прогнозом. Современное развитие SRM/SPM- и SIEM-систем уже позволяет достичь хорошего уровня объективизации оценки рисков и, соответственно, существенно приблизиться к обоснованному уровню затрат на ИБ, стоит только захотеть».

Как оценить риски

Этот подход сложно оспорить, однако в жизни, как водится, реализовать его не так-то просто. «Я работаю в страховой компании, и мне всегда казалось, что страхование умеет оценивать риски, – поделился своими проблемами Артем Кроликов («АльфаСтрахование»). – Когда мы начали оценивать риски, мы изучили 20 мето-



П. ВОЛКОВ, ARinteg

дик и выбрали, по нашему мнению, наиболее понятную. Сформулировали риски, представили их руководству. И столкнулись с тем, что среднестатистический бизнес-пользователь проведенную оценку рисков (а она была выполнена качественно!) оказался не способен воспринять. Бизнес либо игнорирует риски, либо принимает их. Теперь я вынужден составлять некий документ о том, как бизнес должен обрабатывать риски, что он может и чего не должен делать в том или ином случае».

Еще одна проблема – собственно «событийная часть». «К сожалению, по России у нас нет статистических данных – например, сколько за определенное время произошло попыток взлома внешнего периметра банка, – констатировал Андрей Калашников



А. КИРИЛЛОВ, «Северсталь»

(Сберкред Банк). – А в отсутствие статданных, которые можно предъявить руководству и обосновать затраты на безопасность, мы вынуждены пугать бизнес регулятором, как это делает, например, федеральный фонд обязательного медицинского страхования». С ним согласен А. Кириллов, подчеркнувший, что на профессиональном информационном поле у «безопасников» крайне мало фактов.

Информационный вакуум отчасти объясняется сообщениями той же безопасности, однако именно сообщая «безопасники» могут получить неплохие результаты. Например, модель угроз для ДБО была разработана группой экспертов из разных банков. «Первое, к чему мы с коллегами пришли, – пора отказываться от расчета рисков до конкретного объекта, надо говорить о рисках процесса в целом и рассматривать угрозы с точки зрения нарушения той или иной характеристики этого процесса, – отметил Павел Головлев (СМП Банк). – Второе: мы решили не привлекать внешних консультантов». В итоге представители банков мозговым штурмом составили перечень рисков, актуальных для ДБО, создали перечень защитных мер, которые требуются для компенсации этих рисков, и получили приемлемую и понятную схему модели угроз.

Информационный вакуум отчасти объясняется сообщениями той же безопасности, однако именно сообщая «безопасники» могут получить неплохие результаты. Например, модель угроз для ДБО была разработана группой экспертов из разных банков. «Первое, к чему мы с коллегами пришли, – пора отказываться от расчета рисков до конкретного объекта, надо говорить о рисках процесса в целом и рассматривать угрозы с точки зрения нарушения той или иной характеристики этого процесса, – отметил Павел Головлев (СМП Банк). – Второе: мы решили не привлекать внешних консультантов». В итоге представители банков мозговым штурмом составили перечень рисков, актуальных для ДБО, создали перечень защитных мер, которые требуются для компенсации этих рисков, и получили приемлемую и понятную схему модели угроз.

Почему не хватает денег

Нередко даже в случае утверждения бюджета на ИБ-проект «неожиданно» возникает необходимость в существенных дополнительных затратах, которые изначально не планировались и на которые нет ресурсов. И. Трифаленков назвал две основные причины таких ситуаций: «Первая связана с действиями регулятора. К примеру, мы выполняли ра-

боты по созданию систем защиты персональных данных по классам К1, К2, К3 и К4, и в один прекрасный день все критерии этих классов государство изменило. Возникла нестыковка тех затрат, которые планировались, и тех, которые пришлось планировать. Второй причиной может стать переход проекта из стадии реализации в стадию поддержки и эксплуатации. Как правило, при переходе от CAPEX к OPEX что-то теряется, потому что занимаются этими двумя стадиями разные подразделения и мостик между ними проследить не всегда получается».

Еще одна причина потребности в дополнительных затратах кроется в недоговоренностях на стадии составления технического задания. «Система внедряется в соответствии с техзаданием, но на стадии "пилота" бизнес-подразделение решает расширить функционал системы сверх оговоренного в ТЗ. Вопрос рассматривается на самом верхнем уровне. В результате заказчик обращается к исполнителю, который отвечает: любой каприз за ваши деньги, и зачастую подписывается дополнительное соглашение к договору», – проиллюстрировал ситуацию А. Шубин.



А. ШУБИН, банк «Возрождение»

Подводные камни могут обнаружиться и в системе планирования проектов самой компании, считает П. Головлев. «Наверняка всем знакома ситуация, когда вдруг "из ниоткуда" возникает еще один проект от другого бизнес-заказчика, который развивался параллельно. На выходе они сталкиваются и оказываются перпендикулярны – тут приходится быстро "на коленке" что-то собирать, и это приводит к дополнительным затратам на оба проекта», – отметил он.

Кто принимает вызов BYOD

По данным аналитиков, в 2011 г. число мобильных уязвимостей выросло на 93% и мобильные вирусы



сы впервые представили реальную угрозу для бизнеса. Можно ли в этих условиях создать действительно эффективную систему информационной безопасности? Как сообщил М. Емельяников, есть компании, в которых не то что в сеть не войдешь со своего телефона, но сами телефоны, планшеты, флешки сдаются на проходной и хранятся в специальных ячейках.

Но, очевидно, прогресс не остановить, и службам ИБ надо искать компромиссы с консьюмеризацией. В банковской сфере такого компромисса частично можно достичь, по словам А. Шубина, выдачей сотрудникам корпоративных мобильных устройств «после того, как с ними службами ИТ и ИБ произведены определенные действия». Тем не менее феномен BYOD проникает уже и сюда. Но одно дело защищать унифицированную инфраструктуру, где есть определенные стандарты, стоят известные серверы, рабочие станции с заданными операционными системами и приложениями, и совсем другое – впустить в корпоративную сеть пользователей неподконтрольных устройств со всем многообразием версий всех существующих ОС и их приложений.



Д. УСТЮЖАНИН, «ВымпелКом»

«Сами операторы мобильной связи, по большому счету приветствуя покупку смартфонов и планшетов, признают, что и для них BYOD стал головной болью. «Как корпорация мы тоже страдаем, – подтвердил Д. Устюжанин. – Если раньше руководитель службы информационной безопасности был человеком, который говорил нет, то сейчас ставить запреты практически невозможно даже в серьезных вопросах, даже в банках. С этим надо жить. Что делать в этой ситуации службе информационной безопасности? Мы сейчас рассматриваем решения класса MDM (Mobile Device Management), которые появляются на рынке. Как только решим этот вопрос для себя, будем такой сервис предоставлять и другим компаниям. Вообще мы внимательно рассматриваем сегмент предоставления сервисов безопасности. "Последняя миля" – это все чаще мобильный доступ, и я уверен, что операторы мобильной связи должны играть решающую роль в обеспечении безопасности этого доступа».

Так что же мы защищаем

Несколько лет назад, по словам Д. Устюжанина, служба информационной безопасности оператора получила от внешнего аудитора замечание, что «заточена» на защиту инфраструктуры, сетевых подключений и пр., в то время как защищать надо собственно информацию, данные. «Мы развернулись в этом направлении, не оставляя, разумеется, и прежнего, – сказал Д. Устюжанин. – А сейчас уже все понимают, что надо защищать сам бизнес и бизнес-процессы компании, обе-

спечивать мониторинг обстановки в киберпространстве вокруг ключевых информационных активов и реагировать на аномальные активности».

Любопытными данными поделился в этой связи М. Суконник: в прошлом году компания Radware проанализировала отчеты более 100 крупных корпораций по всему миру и обнаружила, что примерно в 36% случаев атака успешно проводится именно на системы, призванные защищать бизнес от атак снаружи (IPS, firewall, IDS). Таргетированные атаки, как указал М. Емельяников, свидетельствуют о том, что бизнес не так уж и защищен, если есть большое желание нанести ему ущерб в информационной сфере.



Е. АРТАСОВ, «Телеинком»
М. СУКОННИК, Radware

Одной из основных задач службы информационной безопасности, подчеркнул Виктор Минин (АРСИБ), должно быть выявление чувствительных компонентов бизнеса и их защиты. Это может быть и инфраструктура, и информация, и даже носители информации – люди. А. Шубин уточнил, что бизнес не существует без бизнес-процессов, как бизнес-процессы не существуют без информации. «Поэтому в основу надо положить классический принцип, которым в силу его рутинности не хотят заниматься ни айтишники, ни "безопасники", но который, как показывает практика, необходим. Это инвентаризация информационных ресурсов и технологических бизнес-процессов, – убеждал А. Шубин. – После того как инвентаризация проведена, необходима классификация информации, обрабатываемой в бизнес-процессах. И тогда становится ясно, что конкретно и где надо защищать в первую очередь, что во вторую и т.д.»

Главным критерием построения системы информационной безопасности являются бизнес и бизнес-процессы, в этом участники дискуссии были единодушны. Действительно, они защищают не хосты, не каналы связи, а бизнес-процессы, и главным инструментом защиты становится риск-менеджмент, на основании которого принимается то или иное решение. При этом ни в коем случае нельзя замыкаться внутри своего подразделения – надо работать с другими, в первую очередь бизнес-подразделениями, чтобы понимать, куда движется компания и что актуально сегодня. А чтобы с ними работать, придется учить бизнес-язык. «Если не сможете обосновать свои потребности – информационная безопасность будет финансироваться по остаточному принципу. Все это сильно меняет и задачи, и состав работ подразделений ИБ. Значит, надо менять понимание своего места в строю», – резюмировал М. Емельяников.

Подготовила **Лилия ПАВЛОВА**

Под знаком ОТТ

Новые абонентские устройства, мотивирующие пользователей получать видеоконтент на любой экран в любое время в любом месте, изменяют рынок платного ТВ. «Что еще определяло в 2012 г. направление ветра перемен в телеиндустрии?» – спросили мы у Александра ГИТИНА, регионального директора компании Verimatrix.



Александр ГИТИН

В точке пересечения нового и зрелого рынков

– Минувший год прошел на мировом рынке платного ТВ под знаком сервисов Over-the-Top (ОТТ), или, как их еще называют, интернет-телевидения. Развитие в этом относительно новом сегменте было настолько бурным, что поставщики ОТТ-сервисов начали всерьез конкурировать не только с операторами IPTV, но и с операторами ка-

бельных, спутниковых и эфирных сетей платного телевидения. Впрочем, как оказалось, последние сами не прочь расширить за счет ОТТ-предложения свою базу подписчиков. Таков первый фактор, в течение всего 2012 г. задававший вектор движения вперед как всего рынка платного ТВ, так и нашей компании.

Второй фактор, который мы видим, – всплеск интереса операторов DVB к технологиям так называемого гибридного телевидения, совмещающего в себе классическое однонаправленное телевидение по кабельному или спутниковому каналу с передачей видео по запросу по обратному IP-каналу. За год развитие этого сегмента существенно ускорилось.

– Видеоконтенту в сетях гибридного (DVB + IPTV) телевидения требуются какие-то особые технологии и средства защиты?

– Рынок DVB очень зрелый, он поделен между несколькими крупными поставщиками систем условного доступа, основанных на традиционной технологии смарт-карт. Однако, по нашему мнению, будущее сетей гибридного телевидения не за карточными, а за программными решениями для защиты контента. И сегодня мы видим, что этот наш подход к обеспечению безопасности находит отклик у операторов цифрового ТВ. В числе игроков, которые его поддерживают, новые операторы, решающие задачу перехода с аналогового телевидения на «цифру», например в Индии. Разделяют его и действующие операторы DVB-сетей, воплощающие в жизнь концепцию «множества экранов» и сетевых услуг. Им он дает возможность перевести свои старые системы CAS/DRM (разграничения доступа) на современные программные решения, обеспечивающие «сквозное» управление безопасностью доставки видеоконтента по сетям всех типов.

– А как на рост бизнеса ОТТ-провайдеров отреагировали правообладатели?

– Студии и мейджоры, владеющие правами на премиальный контент, повысили свои требования к обеспечению его безопасности при распространении Over-the-Top. Их цель – добиться такого же прозрачного управления «цифровыми правами» в сетях ОТТ, как и в сетях DVB и IPTV. Для ее достижения они заключили специальные контракты со всеми поставщиками технологий CAS/DRM, в которых четко сформулированы требования к защите «цифровых прав» в интернет-телевидении.

И в этом смысле у компании Verimatrix, признанной аналитиками MRG лидером в области IPTV в Европе, Латинской Америке, на Ближнем Востоке и в Африке, очень прочные позиции. Наша система защиты контента VCAS (Video Content Authority System), обеспечивающая управление доступом к контенту в сетях платного ТВ всех типов и стандартов, позволяет ОТТ-операторам получать от правообладателей и предлагать подписчикам контент премиум-класса, что очень важно для их бизнеса.

Неоценимый рост

– Какова на сегодня доля ОТТ-проектов в структуре продаж Verimatrix?

– Я не возьмусь оценить ее в процентном выражении, поскольку этот рынок развивается не только сам по себе, но и в сочетании с IPTV, операторы которого смогут с помощью интернет-телевидения привлекать новых подписчиков. Эти технологии активно внедряют и операторы однонаправленного цифрового телевидения, поскольку ОТТ придает их услугам недостающую с точки зрения потребителей ценность – интерактивность и позволяет предлагать разнообразные дополнительные сервисы. Словом, вариаций масса, и выделить долю решений защиты видеоконтента для ОТТ-сервисов (чистые ОТТ-проекты у нас есть, безусловно) из большого количества проектов, где они комбинируются с DVB и IPTV, мне сложно. В одном я убежден: рынок интернет-телевидения будет расти на протяжении как минимум ближайших десяти лет, и на этом убеждении базируется наша ОТТ-стратегия.

– А в целом, каким оказался прошедший год для бизнеса Verimatrix в глобальном масштабе?

– Это был очередной год очень активного роста. Нам удалось не только выполнить все, что мы запланировали, но и сделать даже больше. Мы закончили его с рекордным количеством заказов, с рекордным объемом продаж, добились повышения удовлетворенности клиентов.

Число наших ключевых заказчиков выросло, в том числе за счет более 40 ОТТ-операторов. Это голланд-

ская компания Ziggo, шведский оператор Com Hem, сербский провайдер Serbia Broadband, российский TVzavr, латвийский «Латтелеком», австралийский QuickFlix, оператор из Гонконга PCCW/NOW TV. Все эти операторы выбрали Verimatrix VCAS3 для защиты своего контента и доходов.

На сегодняшний день у компании Verimatrix более 620 заказчиков в более чем 90 странах мира. Наши системы VCAS3 защищают контент на примерно 25 миллионах различных экранов – телевизоров, персональных компьютеров, смартфонов и планшетов на OS Android, устройств Apple. Таким образом, сегодня мы управляем доступом к контенту практически со всех существующих абонентских устройств, включая Smart TV со встроенной поддержкой адаптивных потоковых протоколов, таких как HTTP Live Streaming (HLS).

Кроме того, весь год мы активно развивали нашу компанию: набирали новых сотрудников во всех странах.

– Защиту контента в Smart TV компания Verimatrix в отдельное направление не выделяет?

– Smart TV сегодня уже составляет конкуренцию широко распространенным классическим видеоприставкам – STB. Это реальность, но тем не менее мы рассматриваем защиту контента для «умных» телевизоров в рамках своей OTT-стратегии. Единая платформа Verimatrix VCAS3 обеспечивает защиту контента в Smart TV точно так же, как в OTT-сервисах для множества других разнообразных абонентских устройств.

На российских просторах

– Как в 2012 г. складывались отношения компании Verimatrix с ее основными клиентами – операторами IPTV?

– В России мы видели очень динамичное развитие всех сегментов видеослужб: и IPTV, и OTT, и цифрового ТВ в стандарте DVB. На протяжении всего 2012 г. мы активно участвовали в наращивании абонентской базы таких известных в России поставщиков услуг IPTV, как «Ростелеком», «Таттелеком», «Башсвязьинформ». О результатах этой работы говорят цифры: у «Ростелекома», например, на сегодняшний день насчитывается более полутора миллионов пользователей систем условного доступа компании Verimatrix. Очень показательным я считаю и пример компании «Башсвязьинформ», которая с нашей системой защиты контента смогла привлечь в ряды подписчиков услуги интерактивного телевидения около 40% всех интернет-пользователей в республике.

– А удалось ли компании Verimatrix заинтересовать своими решениями наших провайдеров OTT-сервисов?

– Я считаю, что в 2012 г. на российском рынке произошел прорыв в области OTT. Сразу несколько операторов поняли, что для получения прав на премиальный контент им необходимы серьезные эффективные средства для его защиты. А поскольку компания Verimatrix сегодня является практически единственным поставщиком решений, способных доставить контент в защищенном виде на все типы абонентских устройств, с нами заключили контракты такие замет-

ные на российском рынке поставщики услуг OTT, как TVzavr.ru, Ivi.ru. В настоящее время мы ведем переговоры о заключении контрактов с другими видимыми участниками этого нового рынка.

Безусловно, радует нас и факт подписания договора с компанией «МегаФон», которая будет использовать наши решения для защиты контента как в IPTV, так и в своих OTT-сервисах. Добавлю, что в стадии переговоров мы находимся сейчас с целым рядом заметных игроков российского рынка цифрового ТВ.

Заглянем в будущее?

– Начало года – время строить планы на будущее, определять приоритетные направления развития бизнеса. С какими новыми разработками компания Verimatrix планирует познакомиться посетителей выставки CSTB'2013?

– В рамках нашей стратегии мы будем развивать платформу Verimatrix VCAS3, которая обеспечивает защиту видеоконтента для всех видов сетей и устройств в рамках концепции «множества экранов» (multiscreen). Рассчитываем реализовать в ней поддержку OTT-сервисов для новых, недавно появившихся на рынке платформ – Windows 8 и Blackberry10, и абонентских устройств, работающих под их управлением. Наша задача – расширить границы сферы защиты видео- и медиаконтента. Уже в 2013 г. мы продолжим сотрудничество с европейскими партнерами – производителями «умных» телевизоров, приставок, разнообразных игровых устройств. Безусловно, мы будем участвовать в разработке новых международных отраслевых стандартов, таких как протокол адаптивного потокового видео MPEG-DASH, и устройств, которые его поддерживают.

Поскольку сегодня большое значение придается формированию положительного опыта у конечных потребителей, для более удобного получения всего интересующего их контента на всех видах устройств мы предложим операторам платного телевидения оценить наш MultiRights – подход multu-DRM, реализованный в одноименном модуле нашей платформы. Он позволяет втянуть под наш «зонтик» DRM-технологии других вендоров, в частности Microsoft PlayReady, которую мы уже сегодня поддерживаем, чтобы операторы, применяющие сегодня не нашу систему защиты контента, могли бы обогатить ее возможности функционалом системы условного доступа компании Verimatrix.

Очень важно для нас и развитие Operation Management Interface – модуля, который позволяет организовать единую для всей сети оператора точку интеграции системы Verimatrix с биллингом, middleware, другими сторонними программами.

И конечно, весь год мы будем открыты для всех пожеланий наших ключевых клиентов, чтобы внести эти пожелания в план развития наших продуктов и реализовать в ближайшее время.

Нужно ли российскому бизнесу свободное ПО?



Большое будущее свободному программному обеспечению в корпоративном и государственном секторах российской экономики аналитики и эксперты пророчат уже несколько лет. Насколько оправдались оптимистичные прогнозы? Кто из российских компаний и почему внедряет свободный софт?



Полина
КОНДРАТЮК,
менеджер
проектов,
Etersoft

СПО шагает по стране

На сегодняшний день можно говорить о том, что доля СПО, используемого в российских организациях, хоть и не семимильными шагами, но растет. В первую очередь это касается применения Linux на серверах. По оценкам IDC, доля этой свободной ОС в данной сфере выросла в России с 20,8% в 2010 г. до 22,8% в первом полугодии 2012 г., а доля Windows Server за тот же период сократилась на 1,7%. Отмечается и рост использования Linux на десктопах, но здесь доля ее пока крайне мала (примерно 1%). Заметно лучше ситуация со свободными клиентскими приложениями: многие компании в среде Windows охотно используют Mozilla Firefox как основной браузер и OpenOffice.org в качестве офисного пакета.

Надежды на более активное использование клиентского софта в последние несколько лет во многом были связаны с инициативами правительства РФ по внедрению СПО в государственных организациях. Так, в 2010 г. были выпущены распоряжения 2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011–2015 годы» и 1815-р «О государственной программе “Информационное общество”». Был проведен конкурс на разработку прототипов Национальной программной платформы на основе свободного софта. Однако последующие запланированные конкурсы не были объявлены, и других действий по переходу госорганов на СПО фактически не предпринималось. Минкомсвязи пока не дает четких ответов о судьбе проекта, и после смены администрации связи его перспективы выглядят неопределенными.

Так или иначе эта ситуация вызвала резонанс лишь в узком кругу разработчиков, имеющих отношение к конкурсу, и в части СПО-сообщества. Большинство российских компаний отнеслись к идее

тотального перевода госорганов на СПО более чем спокойно: «Поживем – увидим, что получится».

Действительно, отечественный бизнес в последние годы выработал прагматичный подход к использованию свободного софта: не внедрять СПО ради СПО, но исходить из задач и бизнес-процессов организации, трезво оценивать преимущества и недостатки тех или иных решений. Подход, надо сказать, весьма здравый, и здесь правительству стоило бы поучиться у бизнеса.

Потепление отношений

В последние годы планы перехода на свободный софт для российского бизнеса были окутаны множеством предубеждений и вполне обоснованных опасений и сомнений (рис. 1). Руководители больше не склонны доверять сисадминам «линуксоидам» с горящими глазами, мечтающими перевести все на СПО во имя идеи. Хотя стоит отметить, что такие внедрения далеко не всегда обречены на крах, они могут стать весьма успешными. Но чтобы успех не был случайным, именно холодный расчет стоит ставить во главу угла, принимая решение о переходе на СПО: нужно понять, как изменятся затраты на ИТ, какие задачи удастся решить и какие риски стоит предусмотреть.

Как бы то ни было, интерес к свободным решениям в российском корпоративном секторе есть, и он возрастал на протяжении последних лет. По нашим наблюдениям, растет число успешных Linux-внедрений в компаниях самого разного уровня в различных отраслях; увеличивается и число организаций, осведомленных о возможностях СПО, но пока находящихся в стадии оценки возможных рисков и выгод.

Об интересе к СПО свидетельствует и внимание к Linux со стороны крупных российских разработчиков проприетарных продуктов. Фирма «1С», пять лет назад не рассматривавшая Linux-

Рис. 1. Что препятствует внедрению СПО (по данным опроса разработчиков СПО и корпоративных пользователей)



Источник: North Bridge, 2012

рынок всерьез, объявила о полной поддержке этой ОС в «1С:Предприятие 8.3». Совместимостью со свободной ОС достаточно давно озаботилась компания «Гарант», последние несколько лет регулярно проводящая тестирование своей системы в среде Linux на основе Wine.

Отметим, что для некоторых компаний польза от перехода на СПО не ограничивается экономией на лицензиях и обеспечением нужной функциональности. Внедрение СПО может стать интересным инфоповодом, конкурентным преимуществом, признаком технической продвинутости. На это сделали акцент, к примеру, «Компьютер-центр Кей», московский туроператор «Лабиринт», томский завод по производству манометров «Манотомь» и ряд других более или менее известных российских компаний. Ведь переход на СПО – это весомый ИТ-проект в копилке компании, повод для гордости и неплохая возможность для пиара.

Мирное сосуществование

В каких отраслях можно говорить о стабильном интересе к свободным решениям? В первую очередь это розничная торговля и производственные предприятия. Значительная часть сотрудников компаний данной сферы использует приложения для решения стандартного круга задач (работа с документами, Интернетом, почтой и т.п.) Именно для них на сегодняшний день существуют вполне зрелые свободные продукты, функциональность которых с лихвой покрывает потребности рядового работника. И наоборот, если работа компании завязана на специфический софт (графические программы, САПР, специализированные корпоративные системы), которому среди СПО не найти аналогов нужного уровня, перспективы использования СПО резко осложняются.

Но даже в таких случаях стоит задуматься о том, где есть смысл оптимизировать ИТ-инфраструктуру и сократить затраты на лицензирование программного обеспечения за счет использования свободных решений. Здесь можно порекомендовать следующее:

- Смело переводите на СПО те отделы и те функции, которые не требуют специализированного ПО и для решения задач которых хватает свободных продуктов: это бухгалтерия, продажи, закупки и т.п.
- Для запуска многих Windows-программ, пока не имеющих Linux-версий, выходом может стать использование свободного софта (например, Wine) как ПО уровня совместимости. Тестирование программы в среде Wine позволит определить, насколько такой вариант возможен для каждого конкретного приложения.
- Как уже было сказано, серверные решения – та область, где СПО (не только Linux, но и Web-сервер Apache, свободные СУБД MySQL и PostgreSQL и др.) хорошо себя зарекомендовало. Помимо возможности сэкономить на лицензиях привлекательны надежность и гибкость решений.

В целом мы рекомендуем избегать подхода «все или ничего» – ведь свободные и проприетарные решения могут отлично сосуществовать в инфраструктуре одной компании.

Open source в тренде

За последние пару лет СПО как таковое не так уж часто оказывалось в поле внимания журналистов ИТ-изданий и представителей бизнес-сообщества. Наиболее обсуждаемые ныне темы – это облака, виртуализация, мобильные технологии и всевозможные корпоративные системы. И хотя, как и в случае с СПО, российские компании относятся к подобным «модным» технологиям без эйфории, с высокой долей осторожности, с уверенностью можно говорить, что именно эти тренды будут определять развитие ИТ в ближайшие несколько лет.

Между тем часто забывают, что в основе многих проектов, «выстреливших» в последние годы, лежит открытый код, и влияние open source на развитие «трендовых» технологий весьма велико. Разработчики СПО, в свою очередь, одними из первых улавливают тенденции и предлагают миру весьма интересные проекты в сферах SaaS, облачных вычислений, мобильных технологий и т.п. (рис. 2).

Облака на свободе. Гибкость, масштабируемость, высокая скорость работы – эти требования часто предъявляются к облачным решениям. И эти же черты исконно присущи разработкам с открытым кодом. Поэтому неудивительно, что СПО становится хорошей основой для облачных проектов.

По данным ежегодного исследования Future of Open Source, проводимого инвестиционной компанией North Bridge Venture Partners, на данный момент в мире развивается более 470 свободных проектов в сфере облачных вычислений. Пожалуй, наиболее известный из них – OpenStack, открытое ПО для создания публичных и частных вычислительных облаков. На сегодняшний день OpenStack используют более 180 организаций, как государственных, так и частных, по всему миру.

Родословная Android. Как было сказано выше, доля Linux на десктопах остается весьма скромной. В то же время именно Linux лежит в основе одной из самых

Рис. 2. Развитию каких технологий способствовали проекты СПО (по данным опроса разработчиков СПО и корпоративных пользователей)



Источник: North Bridge, 2012

популярных систем для мобильных устройств – речь, разумеется, об Android. По данным IDC, во II квартале 2012 г. доля смартфонов на этой платформе составила 68%, Android значительно опережает ближайшего конкурента – Apple iOS с 16,9% рынка. В России Android установлена на каждый второй смартфон. Помимо самой ОС с открытым кодом, большое распространение получают свободные приложения из Google Play.

Это лишь наиболее яркие примеры того, как СПО оказывает влияние на развитие технологий. Немало достаточно зрелых и привлекательных для бизнеса решений существует в сферах виртуализации (VirtualBox, OpenVZ, Xen), корпоративных приложений (OpenERP, SugarCRM, Alfresco) и технологий удаленной работы.

Интерес для бизнеса в этом контексте представляет не само по себе свободное ПО, а решения на его основе. Главное, чтобы функциональность таких решений удовлетворяла потребностям бизнеса, а сокращение затрат на лицензии, упрощение масштабирования, гибкость становятся приятными дополнениями.

Предложение в ответ на спрос

Давайте посмотрим, что готов предложить российский рынок СПО в ответ на интерес к свободным решениям, понимают ли разработчики и интеграторы потребности бизнеса. Для начала определим, из чего этот рынок складывается (мы приводим лишь характерные примеры компаний, список далеко не исчерпывающий).

Разработчики. В первую очередь это «дистрибутистроители», среди которых в качестве наиболее бизнес-ориентированных стоит выделить компанию ALT Linux – одного из старейших представителей рынка, амбициозную РОСА и, пожалуй, LinuxWizard. В дополнение к линейке Linux-дистрибутивов для решения различных задач эти компании готовы предложить

клиентам сервис, включающий не только официальную техподдержку, но и возможность внедрять свои продукты, дорабатывать их и организовывать обучение.

Кроме того, в России разрабатывается ряд прикладных и инфраструктурных решений на основе СПО (среди наиболее популярных – интернет-шлюз «Интернет Контроль Сервер» на базе FreeBSD). Ряд компаний – как правило, из числа интеграторов – занимается заказной разработкой решений на основе СПО. Несколько особняком в этом ряду разработчиков стоит Etersoft, создающая решения для обеспечения совместимости свободного и проприетарного софта.

Интеграторы. Для ряда крупнейших интеграторов (это, в частности, «КОРУС Консалтинг», Softline, сюда же можно отнести PingWin SoftWare в составе ГК «АйТи») СПО является одним из направлений деятельности, которое координирует соответствующий департамент. Такие интеграторы ориентированы на крупные заказы, в первую очередь от государства.

ПО open source является основным направлением деятельности для таких компаний, как «ГНУ/Линуксцентр» и «Флант». Они во многом покрывают потребности московских и петербургских организаций различного уровня в качественных услугах по внедрению и сопровождению СПО. Интеграторы, так или иначе занимающиеся установкой и настройкой Linux и свободных программ, есть во многих крупных городах России. Но в регионах они не специализируются на СПО-внедрениях, сочетая их, например, с деятельностью «1С:Франчайзи», продажей всевозможного софта, поставкой и монтажом оборудования. В такой ситуации компании, решившей внедрять у себя свободный софт или отдать свою Linux-инфраструктуру на аутсорсинг, не так-то просто найти квалифицированного внедренца.



В целом можно говорить о том, что российский рынок СПО за последние годы заметно подрос, но у него еще есть большие перспективы для развития. На данный момент рынок во многом ориентирован на крупный госзаказ. В то же время наблюдается дефицит квалифицированных интеграторов в регионах, которые готовы предоставлять услуги по внедрению СПО малым и средним компаниям, понимают их задачи и потребности. И до тех пор, пока такой рынок не сформируется, об успехе свободного ПО в России говорить сложно.

«Многогранность» компаний, предлагающих услуги и продукты в сфере СПО, порой оказывается весьма на руку клиенту. Ведь тогда ему предложат не конкретную технологию, а решение, которое может складываться из различных продуктов – свободных и проприетарных, – но неизменно заточено под потребности его бизнеса.

И как бы ни мечтались приверженцам идей Р. Столлмана, сегодня для бизнеса свободное ПО – это не самоцель, но неплохое средство решения многих ИТ-задач. Именно в таком контексте open source может принести российским компаниям ощутимую пользу, завоевать долгожданную популярность и весомую долю рынка. ИКС

На чем **МОЖНО** и **НЕЛЬЗЯ** ЭКОНОМИТЬ при строительстве ЦОДа

Любой дата-центр – объект весьма недешевый, и стремление уменьшить затраты при его создании вполне понятно. Однако экономия должна быть грамотной, тем более что простор для действий здесь действительно есть.



**Константин
ЗИНОВЬЕВ,**
технический
директор
центра инженерных
систем,
IBS

Говорят, что правила техники безопасности написаны кровью тех, кто их не соблюдал. Нарушение правил экономии при строительстве дата-центра не столь опасно для физического здоровья заказчика, но может иметь негативные и даже катастрофические последствия для его финансового благополучия.

Практически все поставщики оборудования для ЦОДов делают акцент на характеристиках своих продуктов, которые имеют отношение к повышению энергоэффективности и, соответственно, к сокращению затрат на их эксплуатацию. Но заказчик должен понимать, что дата-центр – это сложная система, компоненты которой друг от друга сильно зависят, поэтому нужно тщательно взвешивать влияние тех или иных технических решений на результирующую стоимость создания объекта и владения им.

Все приведенные ниже данные были получены при анализе семи проектов строительства ЦОДов (выполнявшихся исходя из требований Tier III), в которых автор принимал участие. Выборка вроде бы небольшая, тем более что проекты были разной степени сложности и комплексности. Однако, несмотря на разнородность проектов, вклады различных компонентов инженерной инфраструктуры дата-центра в общий бюджет проекта получились примерно одинаковыми (табл. 1). Поэтому даже такие ограни-

ченные статистические данные, на мой взгляд, позволяют делать выводы о направлениях разумной экономии и о том, на чем экономить не стоит.

Как мы видим, на архитектурную часть, системы электроснабжения и кондиционирования приходится почти 80% затрат на проект, т.е. именно за счет них можно получить наиболее заметную экономию, а поиск способов снижения затрат в системах пожаротушения, диспетчерского управления и безопасности – занятие куда менее благодарное, которое по его эффективности можно отнести к экономии на спичках.

Рассмотрим ситуацию с каждым компонентом инженерной инфраструктуры ЦОДа в отдельности.

Экономия электрическая...

Именно система бесперебойного и гарантированного энергоснабжения должна обеспечивать электричеством все системы дата-центра. Для определения ее мощности и, следовательно, цены нужно корректно подсчитать энергопотребление всех компонентов. А вот с этим, как показывает практика, бывают проблемы, потому что каждый специалист, ответственный за составление задания на проектирование того или иного компонента ЦОДа, обычно запрашивает электрическую мощность с запасом (далеко не всегда обоснованным). Так что в ито-

Табл. 1. Структура расходов на создание инженерной инфраструктуры ЦОДа

Компоненты	Доля в бюджете проекта, %
Система бесперебойного и гарантированного энергоснабжения	34,4
Архитектура (строительство здания, защищенных и подсобных помещений, устройство фальшполов)	23,2
Система кондиционирования (охлаждение, вентиляция, газоудаление, отопление)	21,3
Структурированная кабельная система	6,6
Шкафная инфраструктура	6,5
Система пожаротушения	3,6
Автоматизированная система диспетчерского управления	2,3
Системы безопасности	1,3

ге закладываемая в проект мощность системы энерго-снабжения может вдвое превысить реальные потребности – с очевидными последствиями для стоимости.

Свой вклад в удорожание системы энергоснабжения вносит взаимное расположение систем в ЦОДе. Очевидно, что чем ближе ДГУ и ИБП находятся к полезной нагрузке, тем короче трассы для силовых кабелей и, соответственно, меньше затраты на их прокладку. Однако не все знают, насколько сильно цена таких систем зависит от протяженности кабельных трасс (если бы знали, то ставили бы дизели в непосредственной близости от серверов). Например, в одном из проектов мы рассчитали стоимость построения трассы длиной 120 м от восьми трансформаторов мощностью 2,5 МВт каждый. Она оказалась равной почти \$1,5 млн! Практически тот же эффект можно получить при размещении ИБП в одном помещении с главным распределительным щитом (ГРЩ), что не только дает экономию на длине питающих линий, но и позволяет обойтись без промежуточных щитов и соответствующих затрат на них.

Большое влияние на стоимость системы энергоснабжения оказывают схемы резервирования систем ИБП. Сравним два решения, которые соответствуют одному и тому же уровню надежности ЦОДа – Tier III–IV (см. рисунок). В первом решении используется схема резервирования N + 1 (три ИБП мощностью 100 кВА каждый), во втором – 2N (два ИБП по 200 кВА). Конечно, стоимость ИБП в первой схеме будет меньше, чем во второй. Но если рассмотреть всю систему в комплексе с учетом затрат на щиты гарантированного и бесперебойного питания, а также на систему распределения электропитания, то окажется, что стоять они будут практически одинаково. Дополнительным доводом в пользу «более дорогой» схемы резервирования 2N является простота системы распределения, очевидная даже неспециалисту.

Еще один параметр, влияющий на стоимость законченного решения, – запрашиваемое заказчиком время автономной работы ИБП. До сих пор можно встретить

требование обеспечить работу ИБП от батарей в течение 45 мин, и лишь самые смелые соглашаются ограничиться 10 мин. Что заставляет вписывать такие требования в ТЗ? Судя по всему, только генетическая память энергетика, запускавшего судовой дизельный генератор. Три (!) запуска ДГУ в соответствии со всеми регламентными правилами занимают не более 2 мин, а в реальных условиях при отключении питания дизель стартует в течение максимум 5 с. И даже если произойдет осечка, то по схеме резервирования включится второй дизель. Так что затраты на лишние батареи не имеют никакого смысла. Аналогичная ситуация с обходными схемами электропитания (байпасами), которые проектировщики, похоже, составляют уже просто по привычке. При резервировании по схеме 2N они тоже не нужны. Отказ от этих избыточных резервов позволит заметно уменьшить капитальные затраты.

Ну а операционные расходы на систему электропитания сильно зависят от ее энергопотребления. Производители ИБП неустанно твердят заказчикам о высоком КПД своих изделий, которому до заветных 100% осталась самая малость. Однако следует помнить, что речь при этом обычно идет о КПД при полной или близкой к таковой нагрузке. А, скажем, при схеме резервирования 2N даже при полной загрузке дата-центра нагрузка на ИБП, как правило, не превышает 40%, и лишь в пике она может достигать 50%. Например, для нас в свое время неприятным сюрпризом стал тот факт, что при нагрузке меньше 10% КПД трансформаторных ИБП не превышал 50%. При нынешних мощностях дата-центров это означает, что при оплате электроэнергии немалые суммы выбрасываются на ветер. Так что более полезным параметром ИБП является его КПД при неполной нагрузке и именно на него надо обращать внимание в первую очередь, коль стоит задача экономии.

...КОНДИЦИОНЕРНАЯ И...

Если при создании систем энергоснабжения заказчики и проектировщики, как правило, завышают потребности ЦОДа в электричестве, то при проектировании системы кондиционирования типичен некорректный подбор технологий охлаждения и оборудования, следствием чего являются локальные перегревы оборудования, нехватка мощностей охлаждения при полной загрузке и т.п. В этом случае заказчикам можно посоветовать только одно – выбрать правильного подрядчика, и лучше всего такого, который будет отвечать не за отдельную систему кондиционирования, а за функционирование ЦОДа в целом. ASHRAE рекомендует для увеличения энергоэффективности поднять температуру воздуха на входе серверов, и это действительно позволяет сэконо-

Выбор уровня резервирования системы бесперебойного питания

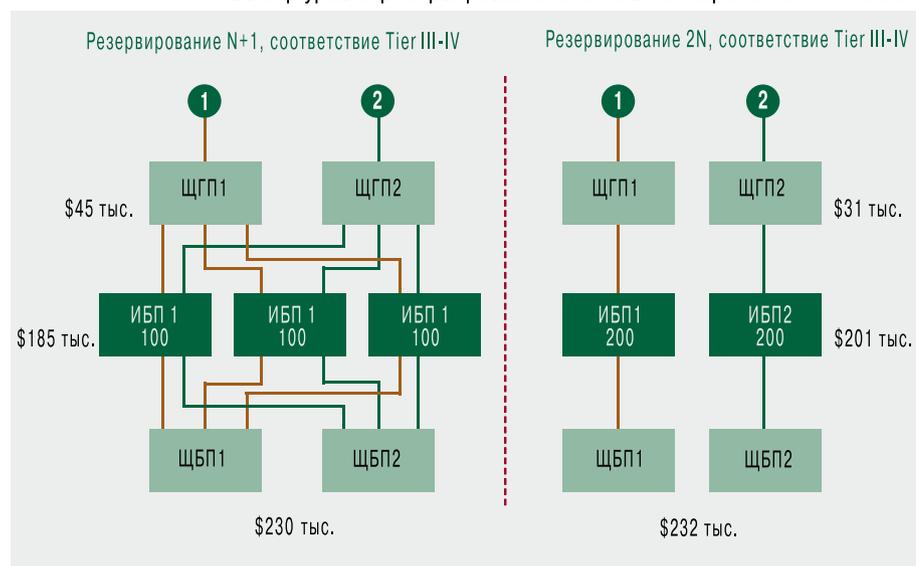


Табл. 2. Сравнение разных систем кондиционирования ЦОДа

Параметры	Чиллерное охлаждение (TurboCoc + мокрые градирни)	Воздушное охлаждение (колесо рекуперации KyotoCooling)	Адиабатическое охлаждение (EcoBreeze)
Среднегодовой холодильный коэффициент (COP)	~7	~10	~10
Возможность наращивания	Есть (кратно одному кондиционеру)	Под вопросом (большой размер машин)	Под вопросом (большой размер машин)
Продолжительность реализации, месяцев	6	4	4
Годовая стоимость электроэнергии, тыс. долл.	142	100	100
Требуемая мощность подключения, МВт	1,3	1,5	1,5
Стоимость подключения, млн долл.	2,6	3	3

мить на системе охлаждения. Но вот на чем не стоит экономить – так это на изоляции холодных и горячих коридоров. Кроме сокращения эксплуатационных расходов, она позволит получить прогнозируемую картину распределения воздушных потоков внутри дата-центра.

Делая принципиальный выбор технологий охлаждения, нужно учитывать влияние разных систем ЦОДа друг на друга, в частности, системы кондиционирования на систему энергоснабжения. Например, в одном из наших проектов мы провели расчет затрат на организацию разных вариантов системы кондиционирования: с использованием чиллерных систем с компрессорами TurboCoc и мокрыми градирнями, воздушного и адиабатического охлаждения (табл. 2).

КПД чиллерной системы был заметно ниже, чем у систем воздушного охлаждения на базе роторных теплообменников KyotoCooling и адиабатического охлаждения на базе системы EcoBreeze: среднегодовой холодильный коэффициент у чиллеров в данном случае составил около 7, и это хороший показатель для данного вида оборудования, а у альтернативных вариантов он достигал 10. Но общие затраты на реализацию чиллерной системы оказались меньше. Дело в том, что чиллерная система на базе компрессоров TurboCoc требует меньшей подводимой электрической мощности, чем системы KyotoCooling и EcoBreeze (1,3 МВт против 1,5 МВт), и объясняется это более высокой эффективностью компрессоров TurboCoc при работе под нагрузкой, чем компрессоров, применяющихся в обоих экологических решениях. Подключение же дополнительных

200 кВт по расценкам энергосбытовых компаний обойдется в \$400 тыс. (\$2 тыс. за 1 кВт подключаемой мощности). Конечно, энергоэффективные решения на основе KyotoCooling или EcoBreeze имеют хороший PUE, который можно с гордостью анонсировать на публике, но получение финансового выигрыша от их внедрения вместо традиционной чиллерной системы в российских условиях растянется на 10 лет, а это устроит далеко не каждого заказчика.

Гораздо продуктивнее выглядит утилизация тепла, выделяемого ЦОДом. Нельзя сказать, что технологии в этой области сильно развиты (ЦОД выделяет много тепла, но оно низкопотенциальное). Тем не менее использование тепловых насосов для отопления здания дает ощутимую экономию на эксплуатации.

...архитектурная и пожарная

Архитектурная часть проекта создания ЦОДа, в которую входит строительство здания, защищенных и подсобных помещений, а также устройство фальшполов, занимает в структуре затрат второе место (см. табл. 1). Безусловно, ее финансовая стоимость будет зависеть от того, какой проект выбирает заказчик, планирует ли он строить для дата-центра специальное здание или будет вписывать ЦОД в имеющееся и какой реконструкции оно для этого потребует. Конечно же, на цену здания повлияет его конструктив – бетонные панели обойдутся дороже, чем быстровозводимые конструкции. Но в любом случае при выборе и выполнении строительного проекта надо помнить, что грамотная компоновка систем энергоснабжения и кондиционирования су-

На архитектурную часть, системы электроснабжения и кондиционирования приходится почти 80% затрат проекта ЦОДа, т.е. именно за счет них можно получить наиболее заметную экономию

щественно уменьшает требуемые для их размещения площади. А это позволяет сократить затраты не только при строительстве, но и при дальнейшей эксплуатации дата-центра. В частности, для снижения капитальных затрат весьма полезны уже упомянутое объединение в одном помещении ГРЩ и ИБП, максимальное приближение холодильного центра и электропитания к нагрузке (это полезно и с точки зрения эксплуатационных расходов), а также многоуровневая компоновка систем инженерной инфраструктуры ЦОДа. Эксплуатационные расходы также можно снизить за счет грамотной организации и уменьшения длины подъездных путей к дата-центру и путей транспортировки оборудования и материалов внутри него. Кроме того, серьезно сокращает эксплуатационные расходы отсутствие пересечений кабелепроводов, трубопроводов, вентиляционных коробов и прочих труб, что требует соответствующего проектирования.

Завершить обзор наиболее «влиятельных» систем ЦОДа правильнее всего системой пожаротушения, несмотря на то что ее среднестатистический вклад в бюджет проекта совсем невелик (3,6%). Объясняется это тем, что от ее конфигурации, определяемой квалификацией проектировщика, зависит общая компоновка дата-центра. Например, как-то пришлось встретиться с оригинальной командой, которая запроектировала в каждом помещении ЦОДа отдельную систему пожаротушения, и для реализации такой схемы нужно было установить 180 баллонов с газом. А для централизованной системы пожаротушения их потребовалось бы порядка 70–80. Так что для минимизации затрат на систему пожаротушения можно посоветовать обращаться к грамотным проектировщикам.

Резервы СКС

Список менее финансово весомых систем дата-центра возглавляет структурированная кабельная система. На ее долю в среднем приходится 6,6% затрат на проект. Но это в среднем. Как показывает практика, в некоторых проектах она может достигать 13%. Цена СКС сильно зависит от выбора категории оптических или медных компонентов. Заказчикам следует обратить особое внимание на их характеристики (табл. 3) и соотнести их с текущими и перспективными требованиями активного оборудования к пропускной способности каналов.

Пропускная способность 10 Гбит/с может быть достигнута как с использованием медного кабеля категории 6 (при длине последнего не более 37 м), так и с по-

мощью оптического кабеля категории OM3 (длина до 300 м). Но при этом надо помнить, что средняя длина канала в ЦОДе – порядка 20 м, а на таких расстояниях при скоростях до 10 Гбит/с включительно нормально работает и более дешевая медь. Поэтому если на данном участке не планируется проводить в дальнейшем модернизацию с увеличением пропускной способности, то разумнее применять оптические и медные кабели более низкой категории. Еще одна возможность сэкономить – отказаться от использования более дорогих претерминированных кабельных решений и дать возможность заработать отечественным монтажникам (если, конечно, сроки не сильно поджимают).

Экономия, которая выйдет боком

На шкафной инфраструктуре, на долю которой приходится в среднем 6,5% затрат, экономить я не рекомендовал бы вообще. Шкафы – это фактически лицо ЦОДа. Именно их в первую очередь видят посетители и потенциальные заказчики. Крупные операторы дата-центров на них никогда не экономят. Кроме того, это граница между серверным оборудованием и инженерной инфраструктурой. Поэтому лучше выбрать качественные шкафы известного производителя, который гарантирует совместимость своих изделий с серверами и другим ИТ-оборудованием, с системами электропитания, охлаждения и мониторинга, с конструкцией системы изоляции горячих и холодных коридоров, а также обеспечивает удобство монтажа и последующей эксплуатации всего устанавливаемого в них оборудования.

Точно так же бессмысленно экономить на автоматизированной системе диспетчерского управления. Она с лихвой отработывает свои 2,3% бюджета. Это ваши глаза и уши в ЦОДе, которые контролируют работу всего инженерного оборудования, выполняют мониторинг параметров энергопотребления и климатических условий функционирования ИТ-оборудования в каждой стойке и выводят всю информацию через общий интерфейс системы диспетчеризации. Но при этом можно вполне обойтись без огромных видеостен, которые с практической точки зрения представляют собой явное излишество.

И уж совсем неразумно пытаться сэкономить на системе безопасности – на нее приходится всего 1,3% затрат. По статистике, причина 60% сбоев в дата-центре – человеческий фактор, а правильно организованная система безопасности может существенно сократить количество этих ошибок. Так что ее можно считать выгодным вложением средств.

Табл. 3. Параметры СКС

Тип канала	Максимально допустимая длина канала, м		
	1 Гбит/с	10 Гбит/с	40–100 Гбит/с
Медь, категория 6	100	37 (55)	-
Медь, категория 6а	100	100	-
Оптика OM3	550	300	100
Оптика OM4	550	550	150

При строительстве дата-центра любого размера, конфигурации и уровня надежности можно и нужно экономить. Но стремление к экономии не должно превращаться в самоцель. Она должна быть разумной и эффективной, т.е. построенной на грамотных расчетах и учитывающей зависимость всех систем ЦОДа друг от друга и реальный финансовый вес каждой из них. ИКС

ИКС ТЕХ

66 Я. ГОРОДЕЦКИЙ. Видеосервисы в сети оператора связи
68 М. БАЛКАРОВ. АКБ как основа бесперебойного питания в ЦОДе

73 В. ШЕПЕЛЕВ. Liebert PCW: точное охлаждение для облачных сред, обеспечивающее максимальную экономию энергии
74 А. МАРКИН, В. БЕЛУГИН. Правильное питание для... томографа

75 Э. АЛЕХИН. Операционная устойчивость ЦОДа: новое увлечение или реальная потребность?
80 П. РОДЖИН, В. КАЗАКОВ. О влиянии климата на параметры механических систем ЦОДа

86 А. СЕМЕНОВ. Горизонтальные кабели малого диаметра в ЦОДе
89 Новые продукты

Видеосервисы в сети оператора связи



↑
Ярослав ГОРОДЕЦКИЙ,
генеральный директор,
CDNvideo

История вопроса

У передачи видеоконтента по IP-сетям история достаточно короткая – первые подобные опыты были проведены менее 20 лет назад, в 1994 г., когда через Интернет с помощью системы IP-видеоконференцсвязи была показана одна из программ американского телеканала ABC. Годом позже, в 1995 г., появился термин IPTV. Так назывался первый коммерческий сервер для показа видеоконтента в IP-сетях. Спустя несколько лет компания – производитель этого сервера, Precept Software, была куплена Cisco Systems.

Однако в 90-е годы широкополосные сети доступа были развиты плохо, интернет-каналы были по сегодняшним меркам очень дороги, потому роскошь передавать видео по IP-сетям могли позволить себе только немногие корпоративные клиенты. Качество передачи видео оставляло желать лучшего: видеокodeки обеспечивали довольно посредственный уровень компрессии и при этом были чувствительны к потерям пакетов. К тому же на IP-сетях того времени не было механизмов поддержки качества – видео невозможно было приоритизировать относительно других типов IP-трафика. Поэтому в 90-е годы возможность передачи видео по IP-сетям вызывала скепсис у представителей телекоммуникационного бизнеса.

Первые коммерческие IPTV-сервисы в сетях операторов связи

Получать прибыль от показа видео в своих сетях – мечта любого оператора связи. Однако удается это далеко не всем: для многих операторов контентные проекты, наоборот, становятся источником дополнительных расходов и головной боли. Почему это происходит, и как оператору сделать видеосервис прибыльным?

появились на рубеже 1990-х – 2000-х годов в Великобритании, США и Канаде. Внедрялись эти сервисы, как правило, параллельно с услугами широкополосного доступа по технологии DSL. Кстати, сегодня большинства операторов – пионеров IPTV не существует: многие из них были куплены в ходе падения рынка акций высокотехнологичных компаний, случившегося в 2001 г.

В России первой внедрила IPTV компания «Стрим» (ныне входит в состав МТС) в сентябре 2005 г. Остальные российские операторы с интересом ждали этого проекта, но никто не спешил его повторять – все понимали, что проект дорогостоящий и сложный в продвижении. Поэтому операторы хотели сначала посмотреть, будет ли чужой проект успешным, а потом уже реализовывать свой. И только примерно через год, когда стало ясно, что услуга востребована, начали появляться проекты IPTV у других российских операторов.

Типы видеосервисов

Как вы, наверное, заметили, до сих пор мы говорили лишь об IPTV-сервисах, хотя статья посвящена видеосервисам в целом. Под термином IPTV обычно понимается услуга предоставления видеоконтента по модели Walled Garden («сад забором») – т.е. оператор показывает видеоконтент только абонентам своей сети, создавая для этого отдельную подсеть на принадлежащей ему сетевой инфраструктуре. До сегодняшнего времени именно модель IPTV имела у операторов наибольший успех. Однако услуги IPTV – не единственный тип видеосервиса.

Другим типом являются сервисы, обычно называемые в телеком-сообществе Over the Top (OTT). Это сервисы, для предоставления которых используется публичный Интернет. Сейчас многие операторы связи задумываются о внедрении видеосервисов этого типа.

Также видеосервисы можно разделить по типу вещания контента: live (вещание прямых эфиров, как правило, телеканалов) и VoD (видео по запросу, когда производится передача предварительно записанного контента – видеороликов, фильмов и пр. – из хранилища).

Качество и транспорт

Еще сравнительно недавно упоминание публичного Интернета в качестве транспорта для передачи видео вызывало у операторов усмешку, ведь «публичный Интернет» был синонимом неконтролируемого или даже гарантированно плохого качества. Операторы IPTV передавали видео по частным IP-сетям, используя при этом технологии, позволяющие управлять трафиком на сети и приоритизировать видеотрафик относительно других типов трафика. Для разделения видеотрафика на магистральной сети обычно применялась технология MPLS, на уровне доступа трафик разносился по разным VLAN. Таким образом, IPTV-операторы гарантировали, что видео всегда будет доставлено до пользователей, но для этого им приходилось идти на существенное увеличение стоимости разрывания сети и ее содержания.

Однако в последние годы оказалось, что пользователи вполне успешно смотрят видео через пуб-

личный Интернет. Это стало неожиданностью для многих IPTV-операторов и поставило под сомнение необходимость вложений в транспортную инфраструктуру, используемую для вещания видео в IPTV-сетях. Дело в том, что к настоящему времени интернет-технологии полностью адаптировались для целей передачи видео. Во-первых, появились новые кодеки, гораздо лучше прежних сжимающие видео и не столь чувствительные к потерям пакетов, которые случаются в IP-сетях (например, H.264 AVC, также известный как MPEG-4 Part 10). Во-вторых, появилась технология адаптивного потокового вещания (adaptive streaming), которая позволяет подстраивать скорость доставки видео под состояние сети. Если доступна широкая полоса пропускания, видео будет показано в максимально высоком качестве, а если пропускная способность сети падает, то пользователю придется смотреть менее качественный видеопоток. В-третьих, свое развитие получили сети доставки контента (Content Delivery Network, CDN), которые приближают видеоконтент к конечным пользователям за счет его кэширования на серверах, установленных внутри городских операторских сетей. Это позволяет не передавать контент через «бутылочные горлышки» на магистральных каналах и межоператорских стыках.

Конечно, видеосервисы, работающие по модели IPTV (Walled Garden), гарантируют качество доставки контента до каждого пользователя сети оператора, а OTT-сервисы – нет. Однако с учетом перечисленных выше моментов для большинства пользователей, особенно проживающих в крупных городах, качество вещания видеосервисов, работающих по модели OTT, будет столь же высоким, как и тех, которые используют модель IPTV. Правильность этого тезиса подтверждается широким распространением таких OTT-сервисов, как Ivi и Zoomby в России или Netflix и Hulu на Западе. Они не стали бы так популярны, если бы их качество не устраивало пользователей.

Оборудование и ПО для построения видеосервисов

Принципы работы видеосервисов по моделям IPTV и OTT во многом схожи. В обоих случаях требуется принимать контент от контент-провайдеров, хранить, перекодировать и категоризировать его, а затем транслировать пользователям. Однако реализация сервисов IPTV и OTT различна.

Видеосервисы, работающие по модели IPTV, обычно строятся «под ключ» интеграторами или вендорами на основе имеющихся на рынке коммерческих продуктов. В состав типовой IPTV-платформы входят источники контента (головные станции, принимающие видеопотоки), системы управления контентом middleware, системы условного доступа и клиентские устройства. Каждый из этих компонентов теоретически можно заменить компонентом от другого производителя, но практически это маловероятно: продукты разных производителей не всегда совместимы между собой и чтобы такую замену произвести, требуется искусство системной интеграции. Если «привязанность» к вендорам не представляет особой проблемы для оборудования внутри сети оператора (лишь бы оно работало), то обязательное использование конкретных моделей пользовательских устройств – это очевидный недостаток. Пользователям может быть неудобно или неприятно устанавливать у себя в доме дополнительное навязываемое им устройство – оно может не вписываться в интерьер гостиной по размеру или дизайну, быть неудобным в эксплуатации или просто не нравиться.

При построении OTT-сервисов обычно применяют другие подходы. По сути, их два: можно нанять программистов и реализовать весь сервер собственными силами (на российском рынке сейчас достаточно программистских команд с необходимым опытом и квалификацией), а можно воспользоваться стандартными видеоплатформами. Видеоплатформы позволяют создавать видеосервисы из облака: вести интернет-вещание телеканалов, выкладывать архив передач,

кодировать контент для различных пользовательских устройств (планшетов, мобильных телефонов, Smart TV), генерировать собственные интернет- или интранет-телеканалы. Они фактически содержат в себе функциональность всех компонентов решений IPTV. Но, в отличие от собратьев из мира IPTV, видеоплатформу можно не только купить, но и арендовать по модели SaaS. Таким образом, видеоплатформа – это ключевой элемент для построения OTT-сервисов: они обеспечивают возможность загружать, хранить, перекодировать и распространять в Интернете видеоконтент, причем могут делать все это из облака, без установки аппаратного и программного обеспечения на площадке оператора связи.

В отличие от IPTV-сервисов, требующих наличия у пользователей определенных телевизионных приставок, OTT-сервисы, как правило, можно смотреть на стандартных устройствах всех типов: на персональных компьютерах через сайт OTT-сервиса, в приложениях для популярных планшетов и смартфонов (под управлением операционных систем iOS, Android, Windows), а также на Smart TV (Samsung, LG, Sony и пр.) и стационарных медиаплеерах (BBK, iconBIT и т.д.). Естественно, создатели OTT-сервисов должны позаботиться о доступности приложений для всех перечисленных платформ – их можно разработать самостоятельно либо воспользоваться стандартными решениями, предоставляемыми провайдерами платформ.

Content is King

Теперь, когда в общих чертах ясно, как строить видеосервисы, остается последний шаг – найти для этих сервисов контент. И тут оператору нужно принять важное решение: заниматься ли поиском контента самому или отдать его на откуп посредникам – агрегаторам контента.

Второй путь, конечно, гораздо проще – разговоры с контентодержателями всегда нелегки для оператора. Но будет ли видеосервис, включающий только контент, пре-

доставляемый агрегаторами, отличаться от сервисов конкурентов? Вряд ли. Поэтому я настоятельно рекомендовал бы любому видеосервису иметь некую долю эксклюзивного контента, которого не найдешь у других.

В частности, операторам из российских регионов стоит обратить внимание на местные телеканалы: сейчас многие из них лишаются доступа к эфиру в связи с цифровизацией ТВ и недостатком места в мультиплексах, так что они будут рады попасть к пользователям через OTT-или IPTV-сервисы. А их постоянные телезрители, в свою очередь, будут рады стать вашими абонентами (если вы включите эти местные телеканалы). Кстати, по информации ведущих российских OTT-сервисов, у пользователей наиболее популярен контент российского производства, причем в каждом регионе – свой профиль потребления и свои пользовательские предпочтения. Поэтому доставка локального контента своим абонентам – это перспективная область для региональных операторов связи.

Что делать?

Какие же именно сервисы стоит реализовывать оператору? Рассмотрим комбинации типов вещания контента – live (прямой эфир) и VoD (видео по запросу) – и моделей видеосервисов IPTV и OTT.

Начнем с первой пары – IPTV-сервисы с трансляциями телеканалов (live IPTV). Здесь у операторов есть определенные перспективы: пользователи привыкли смотреть телевизор, и во многих регионах готовы вносить ежемесячную плату за доступ к телевизионному контенту. Такие услуги, хоть и находятся на грани рентабельности, позволят операторам увеличить ARPU (средний ежемесячный доход от абонента) и уменьшить отток пользователей. Но, конечно, это произойдет только при правильно подобранном контенте (см. таблицу).

Следующая пара – IPTV-сервисы с видео по запросу (VoD IPTV). Если оператор реализует подобный сервис, он автоматически начинает конкурировать со всеми существующими в Интернете OTT-сервисами, где видео доступно бесплатно: торрентами, «ВКонтакте», Ivi и пр. Поэтому строить подобные сервисы я бы не рекомендовал.

Теперь об OTT-сервисах прямых трансляций (live OTT). Как ни странно, в России этот рынок все еще не развит, хотя, например, в Европе и США такие сервисы крайне востребованы. По-видимому, свою роль тут играет доступность эфирного телевидения. Ведь в нашей стране можно принимать бесплатно гораздо больше эфирных телеканалов, чем на Западе, и контент на российских эфирных каналах по-

казывается зачастую более качественный – например, на Западе вы не увидите киноблокбастеров ни на одном общедоступном телеканале. Поэтому сегодня я не рекомендовал бы операторам запускать свои live OTT-сервисы, если речь не идет об эксклюзивном контенте – например, о телеканалах на языках национальных диаспор. Но я не исключаю, что в будущем ситуация эфирного телевидения его проникновение может упасть, проникновение Smart TV к этому времени вырастет, и тогда востребованность live OTT-сервисов повысится.

Стоит ли внедрять видеосервис?		
Тип сервиса	live	VoD
IPTV	Да	Нет
OTT	Только эксклюзивный контент	Да

А вот OTT с видео по запросу (VoD OTT) – крайне интересный сегмент рынка уже сегодня. С одной стороны, интернет-пользователи привыкли смотреть видеоролики, а не трансляции, с другой – в российском Интернете достаточно хорошо развиты схемы монетизации такого контента. Так что если региональный оператор сделает сайт с интересным для региона своего присутствия контентом, он будет не только на нем зарабатывать, но и продвигать свои услуги целевой аудитории. ИКС

АКБ как основа бесперебойного питания в ЦОДе



Михаил БАЛКАРОВ,
технический эксперт,
Emerson Network Power,
ATD, CDCDP

Большинство ЦОДов и серверных требуют бесперебойной работы. Поэтому в составе системы электроснабжения обязательно присутствует ИБП, обладающий в свою очередь источником энергии, позволяющим несколько минут или часов не зависеть от внешнего мира. Как подобрать такой источник и как правильно его обслуживать?

Суперконденсаторы, маховики, натриевые и литиевые батареи – список используемых на практике типов источников энергии для ИБП продолжает расти. Но пока наиболее распространенным вариантом являются батареи

AGM VRLA. Остальное либо слишком дорого, либо неспособно обеспечить достаточно длительное время работы, либо неудобно в обслуживании. Рассмотрим этот самый распространенный вариант попристальнее.

AGM VRLA крупным планом

Длинная аббревиатура расшифровывается как Absorbed Glass Mat Valve Regulated Lead Acid, т.е. свинцово-кислотные батареи с клапанным регулированием и абсорбирующими стекломатами. Несмотря на тот же материал электродов и состав электролита, что и у классических наливных аккумуляторов, батареи AGM VRLA достаточно сильно от них отличаются.

Пластины в батареях AGM VRLA разделены стекловолоконной набивкой, которая удерживает в себе весь имеющийся электролит. С ней связан принципиальный момент – рекомбинация выделяющихся газов. Поскольку набивка волокнистая, она не полностью смочена, и в структуре имеются каналы с воздухом. За счет этого выделяющиеся при заряде кислород и водород попадают на противоположные электроды и снова превращаются в воду (рекомбинируют). Разумеется, набивка плотно прилегает к пластинам, что предохраняет их от осыпания активного вещества.

Поскольку электролита берется относительно мало, используется повышенная концентрация серной кислоты. Сами пластины изготавливаются из специальных сплавов свинца, уменьшающих газы выделение при работе. Для еще большего уменьшения газы выделение допускается применение специальных присадок, катализирующих рекомбинацию.

Корпус у батарей AGM VRLA более прочный, чем у классических, способный выдерживать повышенное давление. При нормальных условиях он герметичен. Для сброса избыточного давления имеется предохранительный клапан.

На сегодня технология AGM VRLA уже вполне отработана, и присущие ей достоинства и недостатки хорошо известны. Многие эксперты достаточно жестко отзываются о маркетинговых мифах, связанных с этими батареями. Сравнивая их с классическими наливными свинцовыми батареями, нужно отметить следующие негативные факты:

- AGM VRLA-батареи тоже выделяют водород. При недооценке этого явления бывали случаи взрывов (кстати, это пример недобросовестного маркетинга – на самом деле водорода выделяется мало, и чтобы не возникало подобных проблем, достаточно избегать герметичной установки и сочетания перегрева с постоянным зарядом);
- они более чувствительны к температуре среды (кондиционирование помещения с батареями строго обязательно);
- чаще склонны к внезапным отказам;
- чаще склонны к катастрофическим отказам, в частности, к возгоранию и взрывам;
- чаще склонны к отказам вообще (при правильной эксплуатации уровень отказов порядка 1% в год на элемент);
- не могут прослужить 10 лет даже в идеальных условиях (учитывая, что в типичной батарее ИБП несколько сотен элементов, и при отказе одного отказывает вся батарея, это неудивительно);

- для гарантии работоспособности AGM VRLA-батареи требуют гораздо более продвинутого мониторинга (чем у нас в стране, как правило, пренебрегают);
- за счет необходимости регулярного мониторинга стоимость их обслуживания получается в итоге не меньшей, чем у наливных (вот поэтому мониторинг зачастую и не ведется);
- при этом AGM VRLA-батареи дороже аналогичных по параметрам наливных.

К реальным достоинствам AGM VRLA-батарей, по сравнению с теми же наливными, относятся:

- большая компактность. Кроме того, основную массу конструкций можно смело располагать в положении на боку;
- меньшие требования к вентиляции. Главное, чтобы она в принципе была;
- отсутствие необходимости работать с электролитом (следовательно, меньшие требования к квалификации сотрудников и помещениям и меньшая вероятность несчастных случаев);
- практически отсутствующая возможность разлива абсорбированного электролита, даже при разрушении корпуса. Соответственно, нет требований к отделке помещения. Кстати, и с разрушенным корпусом батареи AGM VRLA способны какое-то время работать. Такие эксперименты проводились, в частности, во ВНИИ ПО;
- по причине герметичности намного меньшая вероятность развития коррозии контактов и прочих конструкций вокруг;
- могут выдержать даже заливание водой, если это не приведет к сильному разряду или короткому замыканию;
- ну и, разумеется, наибольшая на сегодня распространенность и известность.

Что стоит за номинальными значениями

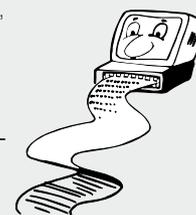
Номинальное напряжение – понятие абстрактное. Если аккумулятор не нагружен, то напряжение на нем

Наведем порядок в терминологии

Элемент, банка или ячейка – это емкость, в которой, собственно, и размещаются электродные пластины и сепараторы с электролитом. В одном корпусе может находиться как один элемент, так и несколько, которые соединены последовательно, формируя аккумулятор или батарею. Типичный аккумулятор – это один, три или шесть элементов с номинальным напряжением 2, 6 или 12 В соответственно.

Линейка – это штатное количество аккумуляторов, соединенных последовательно внешними проводами или перемычками для получения требуемого для работы ИБП напряжения. В некоторых моделях используется двухплечевая схема с нейтральной точкой посередине, состоящая из двух линеек. Замечу также, что у мощных ИБП напряжение постоянного тока высокое, поэтому собранные линейки требуют крайне внимательного отношения.

Аккумуляторной батареей называется весь набор аккумуляторов ИБП.



заметно выше. Это напряжение разомкнутой цепи (плавающее напряжение). По мере разряда под нагрузкой напряжение постепенно падает ниже номинального, до величины конечного напряжения разряда, при котором производитель рекомендует разряд прекращать.

Номинальная емкость аккумуляторов, указываемая традиционно в ампер-часах, как и номинальное напряжение, к реальности практического использования отношение имеет отдаленное. Она скорее характеризует конструкцию самого элемента. По определению, это ток, который аккумулятор способен непрерывно выдавать до достижения напряжения разряда, помноженный на время разряда. В маркировке производителем обычно приводится значение для 10 или 20 ч разряда и напряжения окончания разряда 1,8 В. Обозначается номинальная емкость как C_n , где n – число часов разряда.

Рассмотрим, к примеру, абстрактный аккумулятор номинальной емкостью 7 Ач, способный в течение 10 ч выдавать ток 0,7 А, т.е. с $C_{10} = 7$ Ач. Объединим несколько таких аккумуляторов последовательно. Очевидно, что чем их больше, тем больше мощность (произведение тока и напряжения) полученной конструкции. А вот номинальная емкость у нее ровно та же – 7 Ач. Поэтому, не зная общего количества элементов в плече ИБП (а в некоторых ИБП это количество может заметно варьироваться), оценить фактическую емкость линейки невозможно.

Также нужно учитывать существенное снижение фактически отдаваемой мощности по мере продолжения разряда. Это связано с тем, что электрохимические процессы, которые, собственно, и обеспечивают выделение электроэнергии, не успевают пройти полностью. В результате рассматриваемый аккумулятор при попытке получить от него 7 А в течение одного часа сможет выдавать такой ток минут 20, не больше.

В современной практике ИБП обычно рассчитываются на небольшое время работы, поэтому может показаться, что номинал их батарей значительно завышен. К тому же батареи для ИБП конструктивно отличаются от тех, которые используются в качестве стартерных (к примеру, в автомобилях): они просто не предназначены для разряда в течение нескольких минут. Так что если формально подобрать батареи на 1 мин, на деле можно получить их отсутствие. Время работы батареи для ИБП не должно быть меньше 4–5 мин.

Еще одна проблемная точка – выбор напряжения окончания разряда. Если расчетное время работы батареи составляет несколько часов, то разряд должен прекращаться по достижении 1,8 В на элемент. Иначе возможно разрушение элементов. К сожалению, для свинцово-кислотных батарей любой конструкции переразряд критичен и должен обязательно отслеживаться. Самым правильным будет физически разрывать батарейную цепь при помощи выключателя, срабатывающего по достижении заданного напряжения. Это предотвратит любые дальнейшие утечки тока. Кроме того, если полный разряд выполнен относительно малым током, то в обязательном порядке следует сразу же начинать процедуру заряда. Невыполнение этого

правила может не просто сократить время жизни батареи, а сократить его именно до текущего момента.

При малом времени разряда существенная доля заранее запасенной энергии так и остается в аккумуляторе. В этом случае разряд можно продолжать до более низких значений напряжения – 1,7 или 1,6 В. Соответственно, фактическая емкость батареи может довольно заметно зависеть от наличия и правильности установки этой настройки в ИБП.

Вывод из всего сказанного достаточно очевиден. При подборе батарей следует пользоваться либо специализированной расчетной программой для ИБП, либо программами, таблицами и графиками производителя батарей. Номинальные значения пригодны лишь для качественной проверки результата.

Мои года – мое богатство. А как у АКБ?

Фактическая емкость батарей также меняется в зависимости от температуры в помещении и продолжительности эксплуатации. В начале использования батарей AGM VRLA их фактическая емкость может быть немного ниже номинальной, далее в течение некоторого периода, до года или двух, она увеличивается, после чего начинается ее монотонное снижение, характеризующее старение батарей.

Связано это с тем, что герметичные батареи поставляются с небольшим избытком воды. В начальный период эксплуатации их способность к рекомбинации мала, и часть газов теряется через клапан. В дальнейшем, по мере потери воды, в сепараторе, разделяющем пластины, появляется больше пор и эффективность рекомбинации растет. Этот период занимает от нескольких недель до нескольких месяцев. Батареи входят в рабочий режим, ток плавающего заряда растет. Так продолжается обычно год или два.

Поскольку рекомбинация в любом случае не идеальна, газ в небольших количествах продолжает теряться, количество воды уменьшается, растет концентрация кислоты. Процессы коррозии решеток также потребляют воду и увеличивают концентрацию электролита. За счет этого уменьшается электрохимический потенциал, и постепенно этот эффект становится доминирующим. Поэтому далее, по мере старения, ток плавающего заряда начинает падать и монотонно падает до конца срока жизни батареи.

Однако важно понимать, что способность к рекомбинации продолжает с течением времени увеличиваться. А тепло выделяется в основном именно при этой реакции. В первом приближении происходит вот что: при подаче на батарею постоянного напряжения она разогревается за счет рекомбинации. Ток через горячую батарею увеличивается, выделяется больше газов, они рекомбинируют и еще сильнее разогревают батарею. Процесс продолжается до выхода батареи из строя по причине «теплового разгона».

Проблема возникает в переходном режиме. Ток еще высок, а батареи почти заряжены, и начинается выделение кислорода в больших количествах. Для новых батарей это приводит к интенсивному удалению из-

лишков воды, а вот у старых, с интенсивной рекомбинацией, наступает сильный разогрев.

Еще больше усугубляет ситуацию то, что батареи заряжаются не одновременно. И наибольшее количество тепла выделяется на тех банках, которые зарядились первыми. Именно поэтому при зарядке батарей AGM VRLA обычно рекомендованный производителем предел зарядного тока – 10–20% емкости батареи.

Впрочем, на практике все обстоит не так мрачно, как описано выше. Если корпус ячейки успевает отдавать тепло, то тепловыделение от рекомбинации особого ущерба не наносит. А зарядные устройства современных ИБП поддерживают необходимые ограничения автоматически. Поэтому, хотя явление «теплого разгона» у герметизированных батарей в принципе неустранимо, предпосылки для него в современных системах отсутствуют. В частности, в зарядных устройствах применяется так называемая термокомпенсация: с ростом температуры в помещении зарядное устройство автоматически уменьшает максимально допустимый ток. Но несмотря на это, длительное пребывание в условиях высокой или низкой температуры значительно сокращает срок службы батареи.

Доверять или проверять? Проверять! Но как?

Для герметизированных батарей, как и для старинных наливных, фактическая емкость является показателем здоровья. И стандарты, и практика утверждают, что после деградации емкости до 80% номинальной вероятность внезапного отказа становится слишком высокой.

Традиционно измерения напряжений свинцово-кислотных батарей придаетается большое значение как достаточно простому методу мониторинга. К сожалению, для батарей AGM VRLA, особенно для новых, это не так информативно. Вмешиваются следующие факторы.

При саморазряде, к которому AGM VRLA очень склонны, напряжение на разных банках меняется по-разному. В итоге после подзарядки еще достаточно долгое время сохраняется неравенство напряжений, поскольку окончательно заряд выравняется слабым током подзаряда. Из этого очевидно, что подзаряжать сильно разряженные при хранении аккумуляторы лучше по отдельности.

Аналогичный, но противоположный эффект наблюдается в переходном периоде, когда у части банок уже идет интенсивная рекомбинация, а часть еще имеет избыток воды. В итоге самые «хорошие» банки имеют пониженное напряжение. А для выравнивания напряжений, наоборот, требуется дополнительно длительно заря-

жать банки, у которых напряжение и так повышенное. Такой вот парадокс. Традиционное выдерживание под повышенным (выравнивающим) напряжением при этом, разумеется, не помогает.

В обоих этих случаях самая правильная рекомендация – не волноваться. За несколько месяцев все батареи постепенно придут в норму. Ну и в обязательном порядке нужно регулярно подзаряжать батареи, если они хранятся на складе или ИБП на долгое время отключен от сети.

Качественной мерой оценки состояния здоровья VRLA-батарей остается побаночное измерение импеданса, сопротивления или проводимости, а точным средством измерения – нагрузочное тестирование.

Почему, несмотря на развитие систем постоянного мониторинга, нагрузочное тестирование по-прежнему рекомендуется? Тому есть несколько причин:

- это единственный известный способ достоверно оценить емкость VRLA-батарей;
- это один из самых эффективных способов найти неисправные элементы;
- оно позволяет проверить систему в целом;
- оно позволяет анализировать изменения в батареях.

Да, известны поучительные истории о том, как цикл тестирования оказался последним успешным циклом в жизни батарей. Тем не менее пожертвовать несколькими циклами для понимания текущего положения дел вполне разумно.

Почему речь идет о жертве? Срок жизни батарей определяется не только временем, но и фактическими произошедшими циклами «разряд-заряд». В случае полного разряда их типичное число – порядка нескольких сотен. При частичном разряде количество выдерживаемых циклов увеличивается примерно пропорционально этой «частичности». То есть при разряде на 50% емкости – удваивается. Поэтому завышение емкости батарей в общем случае может увеличивать срок их службы.

Вернемся к нагрузочному тестированию. В процессе его проведения необходим побатарейный монито-

ИКС - ТЕХ

ИБП для ЦОДов
www.ikgulliver.ru

ИСПОЛЬЗУЮТСЯ ДЛЯ ЗАЩИТЫ КРУПНЕЙШИХ ДАТА-ЦЕНТРОВ РОССИИ

- ✓ Стоечные 19": 0,5 - 20 kVA
- ✓ Напольные: 10 - 800 kVA
- ✓ Модульные: до 600 kVA

СКЛАД В МОСКВЕ, ПРИГЛАШАЕМ РЕГИОНАЛЬНЫХ ПРЕДСТАВИТЕЛЕЙ

Компания "ИК Гулливер", г. Москва, Огородный пр-д, д.5
Офис: +7 (495) 663-21-72, info@ikgulliver.ru
Ваш персональный менеджер: +7 (916) 200-96-61, georg@ikgulliver.ru

Инжиниринговая компания **ГУЛЛИВЕР**

ринг. Без него тестирование не только не очень полезно, но и может быть опасным. Плохая ячейка может расплавиться или даже взорваться. При снижении напряжения на любой из батарей ниже заданного тестирование следует немедленно прервать. К тому же без мониторинга тестирование сразу лишается основного смысла – выявления плохих элементов. В итоге, если в линейке из сотни ячеек имеется одна проблемная, вы получаете падение емкости на 1%. Прекрасный показатель. А завтра эта ячейка полностью разрушается, теряя проводимость или, наоборот, замыкает, и зарядное устройство начинает работать только на эту линейку, эффективно разрушая остальные ячейки.

Так что при отсутствии мониторинга отдельных батарей режим автоматического тестирования, имеющийся во многих ИБП, – на самом деле профанация. Оно действует по принципу проверки спичек из анекдота – хорошая, хорошая, хорошая, плохая... Его как раз имеет смысл отключить, чтобы не расходовать зря циклы.

Как подобрать батареи для конкретной инсталляции

В первую очередь, чтобы не создавать единую точку отказа и иметь возможность менять и тестировать батареи по отдельности, желательно использовать несколько линеек в параллель и при этом подключать их не через один автоматический выключатель, а через несколько. К примеру, удобно для расчетов подобрать четыре линейки батарей, обеспечивающие номинальное время работы, и просто добавить пятую, которая позволит выдержать заданное время работы вплоть до старения батарей на 20%. Кстати, достаточно часто производители готовых батарейных шкафов указывают время работы без учета снижения емкости со старением. Обязательно уточняйте этот момент.

Сразу же появляется традиционный вопрос: производители батарей AGM VRLA допускают объединение в параллель от четырех до восьми батарей. Не возникнут ли проблемы? Длительная практика эксплуатации ИБП с модульными батареями доказывает, что несколько десятков линеек в параллель работают совершенно нормально. Дело в том, что рекомендации производителей относятся к объединению единичных батарей. Их действительно стоит в этом случае соблюдать, поскольку разброс характеристик может приводить к значительному перераспределению зарядных и разрядных токов.

В соединенной последовательно батарее ИБП элементов несколько сотен. Разброс их характеристик взаимно компенсируется, и линейки в целом достаточно идентичны. Кроме того, все современные ИБП имеют зарядное устройство с ограничением тока в начальный момент заряда и поддержанием постоянного на-

пряжения в конце (см. рисунок). Это также сужает возможность возникновения проблем.

Батареи меньшей емкости относительно дороже, но зато при выходе их из строя замена и проще, и дешевле. К сожалению, если батареи проработали какое-то время, то из-за описанных выше эффектов приработки заменить в линейке только неисправную может не получиться.

Из тех же соображений я рекомендую использовать батареи с меньшим штатным сроком службы. На практике при правильной эксплуатации пятилетние батареи сохраняют работоспособность до трех лет. Десятилетние – до шести лет. Стоимость отличается примерно в два раза. А вот вероятность случайного отказа одинакова. И замена пятилетних обойдется гораздо

дешевле, к тому же будет не так обидно за напрасно потраченные деньги.

Если срок службы действительно важен, используйте никель-кадмиевые аккумуляторы. Они гарантированно отработают весь срок службы, более того, падение со временем емкости до 80% означает лишь падение емкости, а не рост вероятности отказа. В мониторинге они практически не нуждаются (за исключением удаления остатков испарившихся при падении на клеммы инструментов). Увы, цена вопроса – практически вдвое более высокая по сравнению с AGM VRLA.

Для того чтобы исключить неожиданные случайные отказы, батареи AGM VRLA требуют постоянного мониторинга, причем, как уже упоминалось, не напряжения, а внутреннего сопротивления. Отслеживая изменения, можно достаточно точно предсказать потенциально проблемные ячейки. Увы, такие системы по стоимости сопоставимы с самим батарейным массивом ИБП, поэтому не получили достаточного распространения у нас в стране. С другой стороны, использование нескольких параллельных линеек с независимой зашитой позволяет смягчить эту проблему.



В некоторых местах я сознательно не приводил точные цифры, поскольку у разных моделей разных производителей они слегка различаются. Общее правило: обязательно читайте оригинальные материалы производителя батарей, даже если они поставлены вместе с ИБП.

Статья основана на собственном более чем десятилетнем опыте (точнее, на опыте, нарабатанном на проблемах заказчиков), инструкциях производителей батарей и материалах замечательной конференции Battcon. Настоятельно рекомендую материалы на ее сайте (www.battcon.com) – это настоящая энциклопедия идей, знаний и информации о текущем состоянии данной области. ИКС



Liebert PCW: точное охлаждение для облачных сред, обеспечивающее максимальную экономию энергии

Компания Emerson Network Power кардинально расширила функциональные возможности своей системы охлаждения Liebert PCW.

Фальшпольная система прецизионного охлаждения Liebert PCW, работающая на захоленной воде, предназначена для средних и крупных центров обработки данных, а также небольших ЦОДов и компьютерных залов. Liebert PCW идеально подходит для дата-центров, ориентированных на облачные вычисления. Система прекрасно адаптируется к динамической среде ЦОДа и изменениям тепловой нагрузки, характерным для облачных вычислений.

МАКСИМАЛЬНАЯ ЭФФЕКТИВНОСТЬ ПРИ МИНИМАЛЬНОМ ЭНЕРГОПОТРЕБЛЕНИИ

Ключевое отличие Liebert PCW – оптимизированная внутренняя аэродинамика. Инженеры Emerson Network Power изучили характеристики воздушного потока внутри устройства и полностью переработали внутренние компоненты Liebert PCW. Благодаря новой аэродинамической конструкции Liebert PCW сопротивление воздуха внутри установки минимально. Это обеспечивает максимальную эффективность охлаждения, снижает энергопотребление вентилятора и, как следствие, сокращает расходы на эксплуатацию системы охлаждения и дата-центра в целом.

Liebert PCW объединяет в себе специально разработанные ЕС-вентиляторы нового поколения (Liebert EC Fan 2.0), высокоэффективные фильтры тонкой очистки, способствующие сни-

жению уровня шума, ультразвуковой увлажнитель и систему управления Liebert iCOM, которая реализует интеллектуальный алгоритм управления, разработанный для решений SmartAisle (холодные коридоры). Она позволяет осуществлять точное управление температурой и наиболее эффективно подводить охлаждающий воздушный поток к серверам, не допуская при этом потери ни одного ватта.

Система Liebert PCW проста в установке и отличается гибкими настройками. Она динамически реагирует на потребности дата-центра в любой момент времени, поддерживает максимальную доступность и оптимальную энергоэффективность.

КОНТРОЛЬ ЗА PUE

Оптимизировать энергоэффективность ЦОДа помогает и новое бесплатное приложение под названием Liebert PCW, доступное для скачивания на iPad в онлайн-магазине AppStore. Приложение предоставляет управляющему персоналу ЦОДа возможность отслеживать его PUE, что будет способствовать принятию более точных решений о том, как и где можно экономить энергию. Приложение включает в себя два отдельных калькулятора: калькулятор PUE для расчета энергоэффективности ЦОДа и калькулятор общих эксплуатационных расходов, позволяющий рассчитать, сколько именно средств можно сэкономить, установив более эффективное оборудование, например такое, как Liebert PCW.

Приложение также предоставляет обзор компонентов Liebert PCW, давая возможность изучить технические особенности данного решения и понять, как та или иная технология может помочь экономить энергию в ЦОДе.

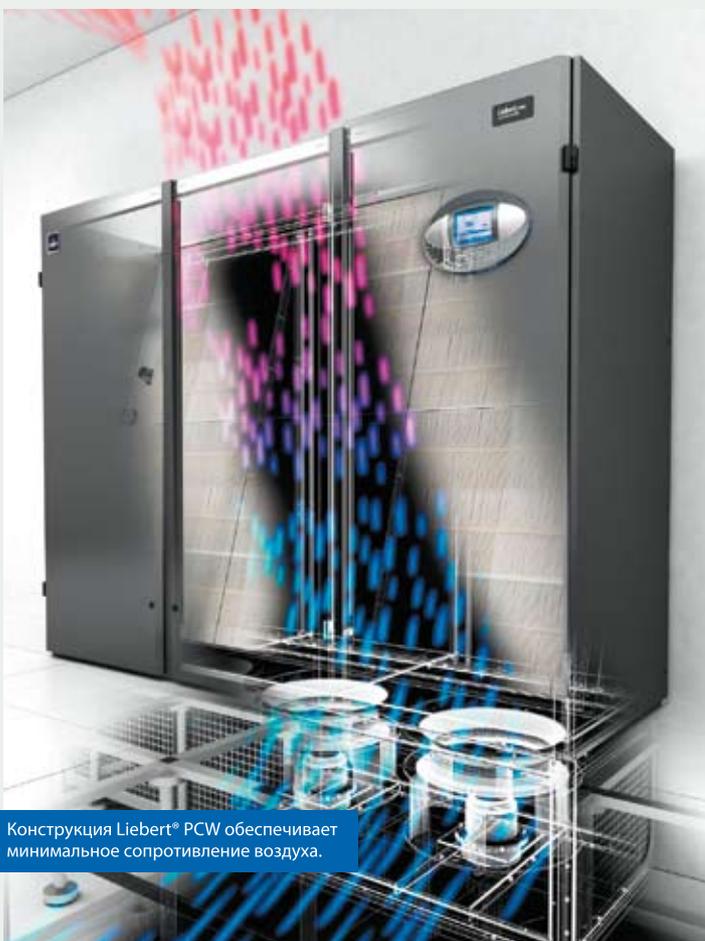
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ДЛЯ ЕМЕА

В странах региона ЕМЕА доступен дополнительный набор опций для Liebert PCW, нацеленный на повышение энергоэффективности и защиту окружающей среды. В их числе:

- Новая модель Liebert PCW с двойным контуром. Эта конфигурация обеспечивает избыточное охлаждение для заказчиков, которые не имеют возможности установить два блока без ущерба для энергоэффективности. На сегодняшний день Liebert PCW обеспечивает самую высокую в отрасли энергоэффективность (до 65%), и при установке ее в качестве дополнительной системы к Liebert HPC Freecooling Chiller PUE может достигать значения 1,11.
- Новый размер – теперь система поставляется в корпусе 3350 мм, позволяя увеличить мощность охлаждения до 240 кВт. Это дает возможность довести установленную мощность ИТ-оборудования до 7,5 МВт без изменения контура управления.
- Возможен заказ на выбор – инфракрасный увлажнитель, ультразвуковой увлажнитель и измеритель уровня. Это способствует улучшению рабочих характеристик Liebert PCW в установках, где предусмотрен мониторинг температуры и влажности.



Владимир ШЕПЕЛЕВ,
бренд-менеджер
Emerson Network
Power Cooling



Конструкция Liebert® PCW обеспечивает минимальное сопротивление воздуха.

Правильное питание для... томографа



Андрей МАРКИН,
руководитель
отдела по работе
с партнерами,
представительство
Powercom



Виктор БЕЛУГИН,
руководитель
департамента
инженерных систем,
группа компаний
МАУКОР

В рамках городской программы по модернизации здравоохранения на 2011–2012 гг. больницы и поликлиники Москвы получили более 28 тыс. единиц новой медтехники. Насколько эффективно она будет использоваться, в немалой степени зависит от соблюдения при ее установке отраслевых стандартов по электропитанию.

Особенно строго нужно им следовать при развертывании сложного диагностического оборудования высокой точности – магнитно-резонансных и компьютерных томографов. Ведь стоимость одного такого аппарата может составлять сотни миллионов рублей, а любое отклонение напряжения от заданных значений, тем более перебои в питающей электросети, может вывести его из строя.

Каковы основные требования к защите электропитания высокотехнологичного медицинского оборудования? Во-первых, применяющиеся для этой цели источники бесперебойного питания должны отличаться высоким качеством исполнения, подтвержденным протоколами испытаний на заводе-изготовителе, которые предоставляются заказчику. Во-вторых, для удобства транспортировки и размещения в отведенном для них помещении они должны быть компактными. В-третьих, требуется наличие встроенных в системы средств мониторинга для передачи информации обо всех нештатных ситуациях в их работе на пульт диспетчера. В-четвертых, важно, чтобы в конструкции ИБП для медучреждений был предусмотрен изолирующий трансформатор, обеспечивающий гальваническую развязку между ИБП и нагрузкой. В-пятых, таким системам необходимо иметь фильтры защиты от помех, которые могут возникать при работе питаемого ими медицинского оборудования. Кроме того, встроенный в источник бесперебойного питания байпас должен иметь высокую перегрузочную способность – до 150% в течение 1 мин.

Исходя из этих требований, компания Powercom, став участником программы модернизации здравоохранения Москвы на 2011–2012 гг., в рамках которой ей пред-

стояло поставить 70 источников бесперебойного питания для магнитно-резонансных и компьютерных томографов в целом ряде медицинских учреждений столицы, предложила использовать для защиты электропитания этого дорогостоящего оборудования свои мощные и надежные трансформаторные системы серии

ONL Second Generation

Несмотря на то что ONL-33-II – новая линейка онлайнновых ИБП Powercom высокой мощности, входящие в нее системы уже хорошо зарекомендовали себя в ГКБ № 36 в Измайлово, в Перинатальном центре в Хабаровске и некоторых других российских стационарных и амбулаторных лечебных учреждениях.

В этих трехфазных источниках бесперебойного питания под управлением высокопроизводительного цифрового сигнального процессора (Digital Signal Processor, DSP) конструкторы Powercom сумели добиться редкого для подобных устройств сочетания высокой надежности и стабильности характеристик с простотой и удобством эксплуатации, компактностью и энергоэффективностью.

В ИБП серии ONL-33-II используется высокочастотный инвертор с широтно-модулированным управлением, с высокой стабильностью поддерживающий выходное напряжение идеальной синусоидальной формы, точность которой – $\pm 1\%$ – не имеет пока аналогов в отрасли. Наличие в конструкции устройства изолирующего трансформатора обеспечивает гальваническую развязку – полную изоляцию выходной цепи от входной, что служит залогом высокой помехозащищенности и надежности, особенно востребованных в медицинском диагностическом оборудовании,

чувствительном к любым видам помех и шумов. А трехфазный выпрямитель позволяет свести к минимуму помехи ИБП во входной сети.

Для надежного и бесперебойного питания магнитно-резонансных томографов, которым требуется 380 В, весьма полезное свойство систем Powercom серии ONL-33-II – сохранение работоспособности без перехода на аккумуляторные батареи в диапазоне входных напряжений от 340 до 460 В. Это помогает увеличить срок службы батарей, а также время автономной работы диагностического оборудования.

Наличие мощного зарядного блока дает возможность всем ИБП серии ONL-33-II работать с большим количеством внешних



ИБП Powercom ONL-33-II (120 кВА)

аккумуляторных блоков различной емкости. Продлению срока службы аккумуляторов способствует интеллектуальный алгоритм зарядного устройства, позволяющий управлять режимом плавающего заряда.

Максимальную энергоэффективность этих ИБП обеспечивает интеллектуальная система охлаждения, построенная на основе управляемых вентиляторов и контрольного механизма. Благодаря такому подходу к вентиляции конструкторам удалось добиться максимально эффективного охлаждения при минимальных затратах электроэнергии, увеличения срока службы и повышения надежности при одновременном понижении уровня шума.



Компьютерный томограф в ГКБ № 1 им. Н.И. Пирогова

Отдельно следует сказать о том, какие в этих устройствах предусмотрены

Средства удаленного мониторинга

Для этой цели в ИБП ONL-33-II служит переносной сенсорный 7-дюймовый дисплей, обменивающийся данными с самим источником посредством Wi-Fi. Его интуитивно понятный русскоязычный интерфейс с всплывающими подсказками позволяет в считанные секунды настроить систему бесперебойного энергоснабжения или устранить неполадки.

Программное обеспечение UPSMON Plus, поставляющееся в комплекте с системой бесперебойного питания и работающее со всеми распространенными операционными системами, предоставляет возможность задавать разные параметры работы ИБП (расписание включения/выключения, время отключения при работе от батарей, запуск тех или иных процедур при возникновении определенных событий и т.п.). А система голосового оповещения сообщает обо всех изменениях в состоянии устройства. При этом специалисты по эксплуатации могут самостоятельно запрограммировать голосовые команды.

Эти интеллектуальные возможности системы управления и мониторинга Powercom сочетаются в ИБП серии ONL-33-II с такими привычными интерфейсами, как RS-232/485, слотом для подключения SNMP-карт, с помощью которых можно не только отслеживать состояние устройства, но и подключать к нему различные датчики. Кроме того, в этих системах предусмотрен и расширенный набор «сухих» контактов – до 18 сигнальных контактов и четырех контактов, программируемых пользователем.

Пусконаладка

Как показывает опыт компании Powercom, установка источников бесперебойного питания для защиты диагностического оборудования в медицинских учреждениях – часть комплексного проекта, предусматривающего расчет нагрузки на электрическую сеть, оценку готовности помещений к размещению оборудования, прокладку и монтаж электрических подводок, установку автоматов защиты. Главная задача такого проекта – обеспечение «бесшовного» сопряжения ИБП с защищаемой ими нагрузкой, а также с другим ранее установленным оборудованием.

Пусконаладкой всех 70 ИБП ONL-33-II, поставленных компанией Powercom в медицинские учреждения Москвы для защиты электропитания томографов Toshiba, занимались специалисты сервисного партнера – группы компаний МАУКОР, работающей в этом статусе в 20 субъектах РФ.

Прежде чем установить источник бесперебойного питания и аккумуляторный шкаф и провести подключение электропроводки, специалисты МАУКОР проверяют отведенное под прибор помещение на пригодность – на соответствие требованиям к температурному режиму и вентиляции, на наличие фильтров, препятствующих попаданию в оборудование грязи и пыли. И составляют акт обследования помещения, к которому прикладываются фотографии объекта. Поскольку часть медицинских учреждений располагается в старых зданиях с деревянными перекрытиями, обязательно проводятся расчеты, выдержат ли они такую нагрузку, как ИБП и шкафы с аккумуляторами.

Установка всего необходимого оборудования и подключение его к электросети в среднем занимает у инженеров МАУКОР два-три дня. Но это в том случае, если выделенное для него помещение находится в состоянии строительной готовности. Если же таковой нет, придется подождать, поскольку МАУКОР обязан четко выполнять все технологические требования вендора, отчитываться перед ним о ходе работ и при необходимости обращаться к его техническим специалистам для принятия совместного решения по возникшим нестандартным ситуациям.

Приемка

Вендор и его сервисный партнер прикладывают максимум усилий к тому, чтобы защита электропитания дорогостоящего высокотехнологичного диагностического оборудования была надежной и бесперебойной. Для защиты и резервного питания томографов и ангиографического комплекса в новом кардионеврологическом корпусе ГКБ № 1 им. Н.И. Пирогова (Первая градская больница) были установлены ИБП Powercom ONL-33-II мощностью 120 кВА. Находящемуся в режиме сканирования магнитно-резонансному томографу они обеспечивают минимальный требуемый запас по мощности (не менее 7%), а при более низком энергопотреблении диагностического оборудования – 12-кратный запас. Более того, при перегрузке ИБП выдерживают превышение номинальной мощности в полтора раза в течение 1 мин. А в целом, благодаря дополнительному батарейному блоку большой емкости в случае отключения внешнего напряжения системы ONL-33-II (120 кВА) обеспечивают электропитание томографа в течение 15 мин.

В конце августа прошлого года новый корпус ГКБ № 1 им. Н.И. Пирогова, построенный за год и два месяца и оснащенный по последнему слову медицинской техники, бесперебойное электропитание которой обеспечивают ИБП Powercom ONL-33-II, был открыт в присутствии мэра столицы С.С. Собянина.



Представительство Powercom
в России, Казахстане
и Республике Беларусь:
+7(495) 651-6281;
www.pcm.ru

Операционная устойчивость ЦОДа

новое увлечение
или реальная
потребность?



Заурбек АЛЕХИН,
независимый консультант

структуру дата-центров, ее функционирование и образующие ее системы. Работоспособность ИТ-оборудования ЦОДа предметом нашего рассмотрения не является и остается вне рамок данной статьи.

Что такое эксплуатация дата-центра

Любое изделие в своем жизненном цикле проходит через стадию эксплуатации, т.е. период его использования по назначению и связанные с этим дополнительные активности, в том числе техническое обслуживание и ремонт. Это относится и к дата-центру. К сожалению, хотя сегодня много говорят и пишут об обслуживании отдельных систем ЦОДа, комплексный взгляд на его организацию и особенности эксплуатации встречается редко.

С точки зрения эксплуатации дата-центр можно охарактеризовать как сложный объект, объединяющий ряд инженерных систем с различными требованиями и нормативами обслуживания. Некоторые системы особо критичны для работоспособности ЦОДа и реализации его целевого назначения. Не являясь изолированными и независимыми, системы могут существенно влиять на качество работы друг друга. Основное назначение ЦОДа диктует высокие требования к функционированию всех его инженерных систем, включая, как правило, постоянную их доступность.

Отметим, что наиболее важными для работы дата-центра справедливо считают системы электроснабжения, а также системы кондиционирования, вентиляции и холодоснабжения. Именно нормальное функционирование этих систем обеспечивает возможность полноценной работы установленного в дата-центре ИТ-оборудования. Тем не менее не следует упускать из виду и остальные инженерные системы: пожаротушения, сигнализации, контроля доступа и др.

Все оборудование, входящее в состав инженерной инфраструктуры дата-центра, в процессе эксплуатации обязательно должно проходить техническое обслуживание, а при необходимости и ремонт. Ввиду большого

Обеспечение стабильности функционирования дата-центров на основе операционной устойчивости – подход относительно новый. По мнению Uptime Institute, он помогает существенно повысить качество работы ЦОДа.

Сразу сделаем важное замечание: здесь и далее, говоря о дата-центрах, их функционировании, составляющих их системах и т.п., мы будем иметь в виду инженерную инфра-

структуру дата-центров, ее функционирование и образующие ее системы. Работоспособность ИТ-оборудования ЦОДа предметом нашего рассмотрения не является и остается вне рамок данной статьи.

Операционная модель

Под операционной моделью понимается некое абстрактное описание того, каким образом организация осуществляет свою деятельность, включая реализуемые процессы, с учетом используемых ресурсов и технологий. Нас, в частности, будет интересовать операционная модель деятельности по эксплуатации дата-центра.

Как уже отмечалось, техническая эксплуатация инженерных систем дата-центра – деятельность сложная, имеющая различные аспекты и взаимосвязи. Ее наиболее крупной и значимой областью является собственно техническое обслуживание оборудования и систем, в широком смысле включающее и плановый ремонт.

Необходимость регулярного технического обслуживания дата-центра обусловлена практически теми же причинами, которые побуждают нас заниматься регулярным техобслуживанием автомобиля. Благодаря тех-

По ГОСТу

Эксплуатация – стадия жизненного цикла изделия, на которой реализуется, поддерживается и восстанавливается его качество. Примечание. Эксплуатация изделия включает в себя в общем случае использование по назначению, транспортирование, хранение, техническое обслуживание и ремонт.

ГОСТ 25866-83. Эксплуатация техники. Термины и определения
Техническое обслуживание – комплекс операций или операция по поддержанию работоспособности или исправности изделия при использовании по назначению, ожидании, хранении и транспортировании.

Ремонт – комплекс операций по восстановлению исправности или работоспособности изделий и восстановлению ресурсов изделий или их составных частей.

ГОСТ 18322-78. Система технического обслуживания и ремонта техники. Термины и определения

обслуживанию мы получаем возможность поддерживать ЦОД в состоянии постоянной готовности, выявляя и устраняя дефекты еще до того, как они приведут к поломке, а также сохранять гарантию производителя. В целом, текущее обслуживание систем дата-центра (включая их плановый ремонт) – это основная, наиболее трудоемкая и ответственная задача эксплуатации. При ее качественном выполнении почти не остается причин для другой, гораздо чаще упоминаемой и более критичной задачи – устранения аварий (сбоев, существенного снижения производительности и т.п.).

К сожалению, полностью избежать аварий невозможно. Поэтому надо быть к ним готовыми. То есть в случае возникновения аварии персонал эксплуатирующей организации должен не пребывать в растерянности, а без промедления приступить к мероприятиям, позволяющим восстановить работоспособность пострадавшей системы в кратчайшие сроки, уменьшая тем самым отрицательное влияние и последствия аварии. Причем вне зависимости от масштаба аварии и других ее характеристик персонал в любых обстоятельствах должен знать, что ему следует делать. В противном случае ситуация станет неуправляемой.

Таким образом, две важнейшие области деятельности службы эксплуатации – это текущее обслуживание и устранение аварий. Операционная модель эксплуатации дата-центра должна описывать действия в рамках решения этих задач по всем системам дата-центра, а также необходимые для их решения ресурсы. Это тот минимум, без которого говорить об эксплуатации бессмысленно. Но, конечно, не следует забывать и про остальные задачи. Например, про необходимость управления мощностями дата-центра. Или про взаимодействие с внешними поставщиками, которых можно привлекать для исполнения отдельных работ, особенно если своих ресурсов недостаточно. А еще – о плановой замене оборудования, о капитальных ремонтах, о финансовом обеспечении...

Возникает закономерный вопрос: неужели нет единой модели, которая учитывала бы все необходимые для правильной эксплуатации дата-центра элементы? Если бы ответ был отрицательным, мы не стали бы его задавать. Итак, встречайте:

Стандарт операционной устойчивости от Uptime Institute

Сегодня наиболее известным и популярным документом из разработанных Uptime Institute является Data Center Site Infrastructure Tier Standard: Topology (Стандарт на топологию) – методологическая основа для сравнения функциональных и мощностных характеристик, а также ожидаемых уровней доступности и производительности ЦОДа исходя из топологии их инженерной инфраструктуры. На основании этого стандарта Uptime Institute осуществляет сертификацию инженерных решений и построенных ЦОДов, присваивая им определенный уровень – Tier – от I до IV в зависимости от полноты соответствия описанным в стандарте критериям.

К сожалению, в последнее время соответствие дата-центра требованиям Стандарта на топологию возведе-

но в абсолют. При этом упускаются из виду ключевые замечания, сделанные как в самом стандарте, так и в комментариях к нему и сопутствующих документах: соответствие объекта изложенным в стандарте требованиям является лишь указанием на принципиальную возможность обеспечить некоторый уровень надежности функционирования инфраструктуры дата-центра. И не более! Никаких гарантий того, что ЦОД, построенный и сертифицированный в соответствии со Стандартом на топологию, например, на уровень Tier IV, в принципе окажется работоспособным и тем более обеспечит доступность не ниже 99,99%, никто не дает! Причина этому простая, и любой специалист ее хорошо знает: как бы ни была надежна техника, она может давать сбой. А уж если в цепочке появляется человек, о котором, кстати, нигде в Стандарте на топологию ничего не говорится, то гарантировать что-либо в принципе невозможно. А поскольку без службы эксплуатации дата-центр работать не может, то...

Для того чтобы разрешить эту коллизию, специалисты Uptime Institute подготовили новый стандарт – Data Center Site Infrastructure Tier Standard: Operational Sustainability (Стандарт операционной устойчивости). Актуальная версия документа доступна для скачивания на сайте этой уважаемой организации.

Предполагается, что стандарт разработан для идентификации основных элементов модели эксплуатации и требований к их реализации с целью обеспечить качественное функционирование дата-центров с учетом зало-



АБИТЕХ
АБСОЛЮТНАЯ ТЕХНИКА



GE Digital Energy™ SG Series UPS
лучшие в своем классе
по характеристикам и
энергоэффективности ИБП

Технология eBoost™:
e = энергоэффективность до 99 %;
Boost = быстрое переключение на инвертор < 2ms

- Диапазон 60–600 кВА в одиночном исполнении, до 3,6 МВА при установке в параллель
- КПД в режиме двойного преобразования >94 %, КПД в режиме eBoost™ до 99 % для одиночных ИБП и параллельных систем
- Работа на любую нагрузку с коэффициентом мощности до 0,9 без снижения выходной мощности
- Трансформатор инвертора, обеспечивающий гальваническую изоляцию нагрузки и более высокие токи короткого замыкания
- Соответствует требованиям по напряжению ITI (СВЕМА)



ООО «АБИТЕХ» – официальный дистрибьютор GE Digital Energy™ в России
Тел./факс: +7 (495) 234-01-08
E-mail: info@abitech.ru
Web: www.abitech.ru

Реклама

женных в инженерных решениях возможностей. Как заявляют в Uptime Institute, он предоставляет владельцам, операторам и менеджменту дата-центров приоритизированный набор активностей и рисков, характерных для обеспечения текущего функционирования объекта.

Документ в целом носит концептуальный характер, задает принципы и ограничения верхнего уровня. В нем рассмотрены три составляющие, способные оказать существенное влияние на качество эксплуатации дата-центра:

- операционная модель;
- характеристики зданий;
- расположение площадки.

В приложениях к стандарту перечисляются элементы модели и ожидаемая их реализация (ожидаемое поведение эксплуатирующей структуры, если речь идет об операциях) и указывается, для какого уровня (Tier) дата-центра они необходимы, а для какого – нет. Проводится также оценка рисков местоположения ЦОДа и изучается влияние характеристик здания на возможность и качество исполнения операций. К слову, приложения таким образом оказались наиболее интересным и информативным разделом документа. Отметим также непривычную логику отнесения тех или иных требований в конкретный раздел. Здесь, скорее всего, сказываются новизна и пока не слишком большой опыт применения документа (короткий список сертифицированных по стандарту ЦОДов – тому подтверждение).

Кроме того, стандарт описывает три уровня сертификатов операционной устойчивости – золотой, серебряный и бронзовый. Бронзовый – это минимально

допустимый уровень качества, при котором эксплуатируемый дата-центр будет работать все же предсказуемо; серебряный – уровень эксплуатации в принципе нормальный, но есть что улучшать; золотой – это идеал, к которому всем следует стремиться. Причем в отличие от сертификатов на соответствие Стандарту на топологию сертификат операционной устойчивости действует ограниченное время. Бронзовый – один год, серебряный – три, золотой – пять. Это вполне логично, поскольку основной вклад в оценку соответствия вносит операционная модель, а она подвержена риску деградации в существенно большей степени, чем техника. Так что проверять надо регулярно...

Ключевое требование стандарта: правильная операционная модель

Наибольший интерес для нас представляет именно операционная модель, рекомендуемая Uptime Institute для эффективной эксплуатации инженерных систем дата-центра (на рис. 1 – один из возможных вариантов ее графического изображения).

Основной набор элементов модели – это все, что относится к собственно обслуживанию: профилактическое обслуживание, управление обслуживанием и действия, непосредственно с ними связанные, включая мониторинг критичных параметров, общую организацию работ на объекте, взаимодействие с внешними исполнителями. В этой части никаких откровений нет, об этом говорилось многократно в разных источниках.

Во вторую группу входит все, связанное с планированием, координацией и управлением эксплуатацией.

Рис. 1. Основные требования стандарта

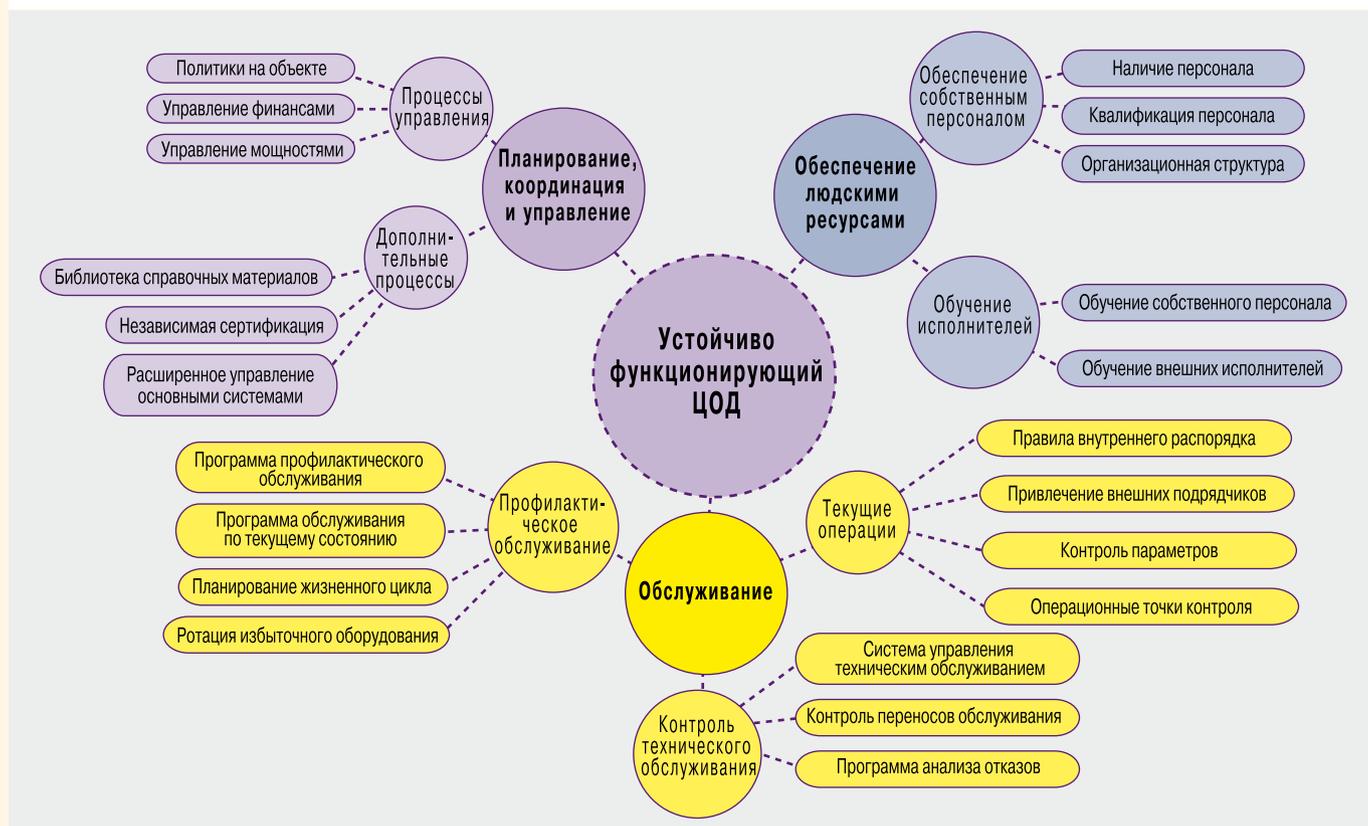


Рис. 2. Требования стандарта в отношении особенностей здания и внешних рисков



Это неудивительно, если учесть распространенное за рубежом увлечение менеджментом и различными вариантами процессного подхода к деятельности организации. Однако следует отметить, что выбранные в качестве значимых элементов процессы управления мощностями, финансами и общие политики на площадке могут на первый взгляд таковыми не показаться. Поэтому тем, кто заинтересуется стандартом, придется приложить дополнительные усилия для того, чтобы понять суть предъявляемых требований и причину, по которой они столь важны.

А вот третья группа довольно неожиданна. То, что кадры решают все, мы давно уяснили, но еще не привыкли рассматривать вопросы обучения персонала с точки зрения обеспечения надежности функционирования инженерного оборудования. Особо обращают на себя внимание требования наличия программы повышения квалификации собственного персонала и регулярного обучения привлекаемых внешних (!) исполнителей. По мнению Uptime Institute, недостаточно подписать с подрядчиком хороший контракт и своевременно платить по нему. Надо еще и персоналом подрядчика заниматься почти как своим собственным – иначе риски некачественного обслуживания вырастут и надежность дата-центра упадет. Да, тут действительно есть над чем задуматься...

Остальные требования стандарта: особенности здания и внешние риски

Описание стандарта не будет полным, если мы не рассмотрим требования, не имеющие прямого отношения к операционной модели. Таковые можно объединить в четыре группы (рис. 2).

Группа инфраструктурных требований (в основном рассматриваются характеристики помещений) направлена на обеспечение возможности обслуживания. Речь идет о вспомогательных инструментах (включая, например, устройства для подъема и перемещения гру-

зов), а также о достаточности площадей для исполнения работ. Отдельно отмечаются наличие возможностей и гибкость в наращивании мощностей.

Продолжением темы является раздел, посвященный особенностям зданий ЦОДов. Помимо общих вопросов в него входят организация контроля доступа, а также возможность безопасного для персонала прибытия и покидания объекта в экстренных ситуациях.

Особняком стоит группа требований по подготовке ЦОДа к эксплуатации (кстати, не совсем понятно, почему эти требования попали в раздел «характеристики зданий», поскольку они отражают переходные процессы и мероприятия, в большей степени характерные для инициирования операционных процессов). По сути, речь в них идет о необходимости полноценной приемки и тестирования построенного объекта.

Местоположение объекта в основном рассматривается с точки зрения внешних рисков и влияний, включая природные (паводки, наводнения, землетрясения и т.п.) и техногенные (близость потенциально опасных объектов – химических предприятий, аэропортов и др.). Здесь возможности управления ситуацией, как правило, отсутствуют, и требования направлены скорее на формирование адекватной оценки ситуации и при необходимости на корректировку ожиданий владельцев и клиентов дата-центра.

А вот вопросы управления персоналом, его безопасности, защиты окружающей среды в стандарте сознательно не обсуждаются. Эти направления, безусловно, тоже оказывают значительное влияние на качество функционирования дата-центра, но, по мнению авторов стандарта, они должны быть под контролем иных общекорпоративных процессов, требований регулирующих органов и т.п.

О порядке применения Стандарта операционной устойчивости и о сертификации ЦОДов на соответствие этому стандарту – в следующем номере «ИКС».

О влиянии климата

на параметры механических систем ЦОДа



Петр РОНЖИН,
главный инженер отдела
климатических систем,
NVision Group



Василий КАЗАКОВ,
ведущий инженер,
NVision Group

Те, кому приходилось сталкиваться со строительством инженерных систем для ЦОДов или серверных не только в своем регионе, на опыте узнали, что их работа очень сильно зависит от климатических условий местности. А тем, кто не решал такие задачи, будет полезно задуматься над вопросом: «Какие особенности должна иметь моя инженерная система на данной площадке, в данном регионе, в данном климате?»

На примере механических систем, к которым относятся системы отопления, вентиляции, кондиционирования и холодоснабжения, мы расскажем о влиянии наружных климатических условий на основные параметры таких систем и о том, на что обратить внимание при их проектировании и строительстве.

Климатические параметры

Чтобы обсуждать влияние климатических условий, первоначаль-

но определимся с тем, какие параметры характеризуют собственно климат. В данной статье мы разделим их на основные и второстепенные, но подчеркнем, что такое деление весьма условно: как будет показано ниже, какой-либо второстепенный параметр может оказать решающую роль на выбор механической системы и ее работоспособность.

развитием и разрушением медленно движущихся областей высокого давления – антициклонов – и относительно быстро перемещающихся огромных вихрей – циклонов, в которых господствует пониженное давление. За всю историю метеонаблюдений отмечены колебания атмосферного давления на уровне моря в пределах 641–816 мм рт. ст. (внутри смерча давление может достигать значения 560 мм рт. ст.). Но тем не менее основными факторами, определяющими атмосферное давление, являются значение ускорения свободного падения в данном месте и высота над уровнем моря, поскольку давление создается вышележащим слоем атмосферы. Поэтому атмосферное давление в конкретной местности характеризуется некоей постоянной среднестатистической величиной, определяемой на основе длительных метеонаблюдений.

Атмосферное давление, как и температура, существенно влияет на плотность воздуха. Следствием неправильно принятого значения давления для выбранной территории могут стать ошибки в дальнейших расчетах механических систем. Чем выше над уровнем моря располагается объект строительства, тем меньше плотность воздуха – и соответственно меньше теплоперенос – при тех же самых объемных расходах. При подборе оборудования следует указывать величину атмосферного давления или высоту над уровнем моря, так как по умолчанию все программы подбора рассчитывают характеристики при работе систем на уровне моря.

Температура воздуха

Этот параметр чаще всего фигурирует при обсуждении механических систем. При проектировании систем вентиляции, кондиционирования и холодоснабжения, обслуживающих машинные залы ЦОДов, прежде всего важны экстремальные (как отрицательные, так и положительные) значения температур наружного воздуха. В этом заключается коренное отличие механических систем для дата-центров от систем гражданского назначения, которые проектируются в соответствии с расчетными температурами наружного воздуха в теплый и холодный периоды года. В разработанном Uptime Institute стандарте Data Center Site Infrastructure Tier Standard: Topology указывается, что

но определимся с тем, какие параметры характеризуют собственно климат. В данной статье мы разделим их на основные и второстепенные, но подчеркнем, что такое деление весьма условно: как будет показано ниже, какой-либо второстепенный параметр может оказать решающую роль на выбор механической системы и ее работоспособность.

К основным параметрам климата относятся атмосферное давление, температура воздуха, относительная влажность. С ними жестко связаны другие параметры, характеризующие состояние окружающей среды: абсолютное влагосодержание воздуха, энтальпия, температуры сухого и влажного термометров и т. п. Основные параметры воздуха можно вычислить друг из друга по формулам, но удобнее пользоваться так называемыми психрометрическими диаграммами влажного воздуха различного вида.

Атмосферное давление

На земной поверхности давление атмосферы меняется от места к месту и во времени. Особенно важны определяющие погоду непериодические изменения атмосферного давления, связанные с возникновением,

эффективная мощность инженерного оборудования должна определяться при пиковых значениях для данного климатического региона, которые публикуются каждые четыре года Американским обществом по отоплению, охлаждению и кондиционированию (ASHRAE). В соответствии с документом под названием ASHRAE Handbook проектная температура влажного термометра должна быть выбрана по максимальному среднегодовому значению, а проектная температура сухого термометра – по максимальному значению за 20 лет наблюдений.

Следует сказать несколько слов о том, как определяются температуры по сухому и влажному термометру. Если два одинаковых термометра закрепить на штативе и на один из них надеть специальный колпачок из тонкой материи, опустив ее конец в резервуар с водой, то этот термометр будет показывать более низкую температуру, чем сухой (поскольку некоторое количество тепла затрачивается на испарение воды с влажного термометра). Следует учитывать, что чем меньше в окружающем воздухе водяных паров, тем интенсивнее испаряется вода с влажного термометра и тем больше в результате будет разница температур между показаниями двух термометров.

Для вычисления показателя эффективности использования электроэнергии в ЦОДе (PUE) выполняются расчеты энергопотребления механическими системами при различных наружных условиях. Для получения

корректного значения среднегодового коэффициента PUE необходима достоверная статистика, показывающая, в течение какого времени в году наблюдается определенный температурный интервал. Наиболее точный расчет будет соответствовать случаю, когда весь возможный для данной местности температурный диапазон, от абсолютного минимума до абсолютного максимума, разбит на узкие интервалы, например с шагом в 1 градус.

Влажность

Значения температур сухого и влажного термометров очень важны для определения относительной влажности воздуха, которая, в свою очередь, играет определяющую роль при проектировании механических систем, использующих, например, адиабатическое охлаждение. Изучив статистические данные по температурам сухого и влажного термометра, характерные для данной местности, можно сделать вывод о целесообразности использования на проектируемом объекте оборудования с адиабатическими процессами.

Другие параметры

Не стоит забывать и о второстепенных, но важных параметрах: запыленности, задымленности, загазованности – и о наличии в составе атмосферы вредных примесей (кислот, солей и т. п.) В нашей практике был случай, когда наружный блок прецизионного конди-

б и з н е с - п а р т н е р

Прямое свободное охлаждение в российском климате оптимально по энергоэффективности



Сергей ЗЕЛЕНКОВ,
руководитель
отдела технического
сопровождения продаж,
HTS

Многообразие систем охлаждения ЦОДов ставит перед проектировщиками непростую задачу выбора наиболее энергоэффективного решения. Сейчас для получения хороших показателей энергоэффективности оптимально применение систем свободного охлаждения.

На выбор решения в числе прочего влияют характеристики окружающей среды. Как показывает климатическая карта России, на всей территории нашей страны возможно использование свободного охлаждения. Если же расширить диапазон допустимых значений параметров воздуха в помещении ЦОДа, то свободное охлаждение можно будет применять в течение большего количества дней в году.

Компания HTS совместно с партнерами уже реализовала несколько объектов с непрямым свободным охлаждением (технология DFC для кондиционеров Stulz). Данные системы подходят для любого климата, обеспечивая надежную и эффективную работу. А различные вариации исполнения делают решение поистине универсальным.

Если принять некоторые ограничения, то можно также использовать новую систему прямого свободного охлаждения от Stulz – DFC2. Наиболее эффективны решения с водяными системами охлаждения. Такое решение способно обеспечивать работу в режиме свободного охлаждения почти круглый год, подключать чиллеры в этом случае понадобится только на несколько недель в году.

Однако таким решениям сопутствует очень острая проблема – поддержание влажности в помещении ЦОДа. При этом очень важно сохранить полученные значения энергоэффективности, а значит, приходится отказываться от использования стандартных систем изотермического увлажнения.

Зато применение адиабатического увлажнения позволяет получить дополнительный холодильный эффект.

Конечно, каждый объект имеет свою индивидуальную концепцию, и если строительство ЦОДа ведется «с нуля», то проектировщикам доступно большее количество технических решений.

В прошлом году команда специалистов HTS прорабатывала концепции решений на оборудовании с прямым свободным охлаждением для нескольких климатических зон. Были использованы данные о распределении температуры и влажности по часам за весь год, учитывались направления ветров и количество осадков в году, характерные для выбранных регионов, были проведены расчеты необходимого расхода воды за год. Для одного из проектов ЦОДов, согласно расчетам, количество дней работы чиллера равнялось десяти! Результатом этой работы станет реализация в текущем году первого в России объекта с прямым свободным охлаждением.



Рис. 1. Распределение температур по году для Москвы



ционерера каждое лето полностью выходил из строя по причине загрязнения теплообменников пылью, приносимой преобладающими ветрами с расположенного рядом цементного завода: под действием влажного воздуха цементная пыль превращалась в камень.

Задымленность атмосферы (вспомним летние торфяные пожары под Москвой) может сыграть злую шутку в случае использования систем с прямым свободным охлаждением (fresh air cooling). Задымленный воздух, попавший в ЦОД, может вызвать ложное срабатывание системы пожаротушения со всеми вытекающими отсюда последствиями.

В случае строительства дата-центра на морском побережье с особой тщательностью необходимо проработать вопросы коррозионной стойкости оборудования (ряд фирм выпускают так называемые исполнения для морского климата), а также учесть повышенную влажность воздуха.

Данные о климате различных районов России, о которых речь шла выше, можно найти в стандартах ГОСТ 16350-80 «Климат СССР. Районирование и статистические параметры климатических факторов для технических целей» и СНиП 23-01-99 «Строительная климатология».

В жару и в мороз

При выборе типа механических систем и их расчете рассматривают работу систем в холодный, переходный и теплый периоды года.

Холодный период определяет мероприятия по обеспечению работоспособности оборудования и системы в целом при низких температурах, вплоть до абсолютного мини-

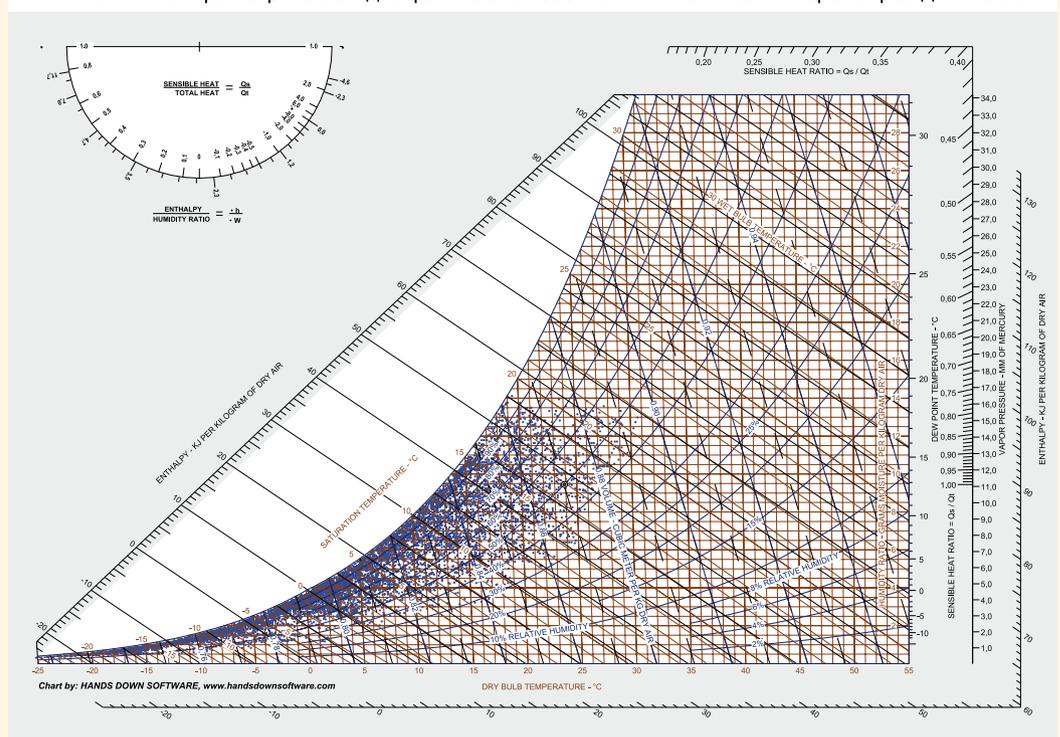
муму для данной местности. Мы должны убедиться, что все составляющие оборудования (вентиляторы, контроллеры и т.п.) работоспособны при этих температурах, а мощность caloriferов в приточных установках достаточна для нагрева воздуха до нормы.

К примеру, если рассматривать фреоновые кондиционеры с выносными воздушными конденсаторами, оборудованные низкотемпературными комплектами, то их применение возможно только в районах с абсолютным минимумом температур не ниже -40°C . Скажем, в Ярославле мы бы не советовали применять такую систему кондиционирования, так как абсолютная минимальная температура для этого прекрасного города составляет -46°C ! Конечно, такие морозы случаются нечасто, но ЦОД, если вы строите настоящий ЦОД, должен быть готов работать и в лютые холода. В этих случаях используют другие решения, например закрытые градирни, подбирая тип холодоносителя и его концентрацию так, чтобы он не замерзал при оставке системы.

Сейчас часто используются холодильные машины наружного исполнения со свободным охлаждением. При низких температурах компрессоры отключаются. Следует проверить: допускается ли производителем оборудования хранение компрессора при этих температурах? Как будут вести себя на морозе материалы панелей чиллера? В ряде случаев приходится предусматривать подогрев даже для неработающих частей оборудования.

Теплый период – диаметрально противоположность холодному, он определяет работоспособность оборудования при экстремально высоких температурах наружного воздуха. По аналогии с холодным периодом рассмотрим работу фреоновых кондиционеров.

Рис. 2. Психрометрическая диаграмма с нанесением климатических параметров для Москвы



Размеры воздушных конденсаторов рассчитывают, исходя именно из максимальной температуры наружного воздуха. При возрастании наружной температуры растет температура конденсации фреона в теплообменниках и, соответственно, давление конденсации. Рост давления конденсации не может продолжаться бесконечно, при малых размерах теплообменников давление превышает допустимые значения и происходит остановка кондиционеров. Если невозможно дальше увеличивать площадь теплообмена, можно использовать адиабатическое охлаждение наружного воздуха перед конденсатором. Опять-таки, прежде чем применять адиабатическое охлаждение, необходимо поинтересоваться данными о влажности воздуха в данном регионе. Если влажность в периоды жаркой погоды значительно уменьшается, такую систему применять можно. В регионах же, где в жаркую погоду влажность остается высокой, например в приморских или тропических, эта система будет бесполезной. Аналогичная ситуация и в случае систем с градирнями или с моноблочными чиллерами.

Переходный период не накладывает блокирующих ограничений на системы кондиционирования и холодоснабжения. Но он не менее важен при расчете годового потребления электроэнергии механическими системами. Ключевую роль в данном случае играет распределение температур по году (рис. 1): по оси абсцисс таких графиков откладываются свойственные

данной местности температуры, а по оси ординат – суммарное количество часов за год, в течение которого наблюдаются эти температуры. Чем больше выпуклая часть графика смещена влево, к минимальным температурам наружного воздуха, тем меньше будет годовое потребление электроэнергии, и наоборот. Помимо этого график распределения температур наилучшим образом подходит для выбора типа систем, так как на нем сразу видны и экстремальные значения для системы охлаждения, и ее загрузка в течение года.

В случае механических систем с адиабатическим охлаждением задача еще больше усложняется – необходимо рассматривать распределение сочетания параметров на психрометрической диаграмме и распределение температур мокрого термометра. Это обусловлено тем, что именно температура мокрого термометра является определяющей для подбора как адиабатических конденсаторов и мокрых градирен, так и экономайзеров с адиабатическим предварительным охлаждением. В связи с этим чаще всего мы используем психрометрические диаграммы с указанием распределения температур сухого и мокрого термометров, на которых видны экстремальные точки лета и зимы, а также основная зона работы системы (рис. 2). Облако из синих точек на рис. 2 характеризует распределение климатических параметров для определенной местности. Таким образом, в диаграмме учтена влажность воздуха, что позволяет оценить самую воз-

Б И З Н Е С - П А Р Т Н Е Р

Климат России: вызов и зимой, и летом



Сергей ШАГАЛОВ,
специалист по продажам,
STL-R

Работоспособность системы кондиционирования ЦОДа оказывается под особой угрозой при достижении летних и зимних температурных экстремумов. Часто причина отказов кроется в том, что оборудование неправильно подобрано и не предназначено для работы в температурном диапазоне, характерном для данного района. К сожалению, очевидная простота этого вопроса часто провоцирует небрежное к нему отношение.

Можно снизить риски, опираясь на данные многолетних наблюдений, при этом следует учитывать актуальные абсолютные значения температуры в данной местности. Летом 2010 г. температура воздуха в Москве в июле-августе побила ряд рекордов, дойдя до отметки 38,2°C, что вызвало массовые остановки оборудования. Этот переломный момент разделил специалистов на два лагеря: оптимистов, упрямо опирающихся в расчетах на принятое значение 37°C, и пессимистов, рассчитывающих системы для Московского региона исходя из +42 и даже +45°C.

Глобальные климатические тенденции не оставляют шансов оптимистам. С другой стороны, для пессимистов прогноз метеорологов тоже неутешителен: температура в 42°C летом в Москве не будет актуальна, по крайней мере, в ближайшие два десятилетия.

А вот выбор оборудования для эксплуатации в условиях русской зимы требует особого внимания, поскольку не все производители систем кондиционирования готовят их к работе в резко

континентальном или субарктическом климате, ограничиваясь нижним пределом температуры, характерным для мягкой европейской зимы. Оборудование, предлагаемое компанией STULZ на российском рынке, готово к работе при температурах до -45°C. В ряде случаев рабочий диапазон может быть расширен в сторону отрицательных температур.

В зимний период надежная работа холодильных машин STULZ обеспечивается с помощью электрического подогрева критически важных узлов, включая электрический щит и испарители. Точная работа компонентов холодильного контура достигается за счет использования низкотемпературных комплектов, включающих сертифицированную для работы в экстремальных условиях регулируемую арматуру. Гарантией запуска кондиционеров прямого испарения даже в самый суровый мороз служит применение специальных низкотемпературных смазочных материалов в двигателях конденсаторов и обязательный подогрев картера компрессора.

Надежность работы оборудования STULZ подтверждена опытом эксплуатации в самых суровых климатических условиях нашей страны, включая объекты в сердце Якутии, где годовая амплитуда температур, одна из самых широких на планете, достигает 100°C.



www.stl-r.ru

возможность адиабатического предварительного охлаждения и его характеристики.

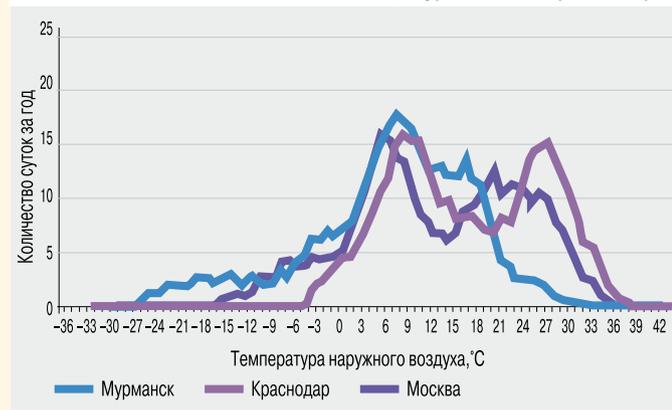
Расчет и оптимизация

Теперь, определив ключевые параметры механической системы, рассмотрим их влияние на основные показатели системы холодоснабжения и кондиционирования на примере ЦОДа с мощностью ИТ-оборудования 1 МВт. Из всего многообразия регионов нашей необъятной Родины мы выбрали три: Мурманск, Москва, Краснодар. Для всех городов мы применили универсальное техническое решение, позволяющее работать в климатических условиях выбранных регионов. Для начала рассчитаем основные показатели механической системы, а потом выясним, как мы могли бы ее оптимизировать.

Итак, при ИТ-нагрузке в 1 МВт мощность системы холодоснабжения и кондиционирования с учетом теплопоступлений от ИБП, насосов, вентиляторов, системы вентиляции, солнечной радиации и т. п. должна составлять 1,3 МВт. Для расчета мы остановили свой выбор на системе с чиллерами внутренней установки с центробежными компрессорами и с двумя контурами (контур испаритель – потребитель и контур конденсатор – сухая градирня). Испаритель чиллера охлаждает воду с 15 до 10°C, а конденсатор охлаждается 40%-ной этиленгликолевой смесью с температурами 30/35°C. Для уменьшения температуры конденсации в градирнях мы предусмотрели адиабатическое предварительное охлаждение наружного воздуха. В качестве устройств охлаждения ИТ-оборудования выбраны межрядные кондиционеры с горизонтальным движением воздуха. Ряды стоек монтируются таким образом, чтобы соблюдался принцип изоляции холодных и горячих коридоров, это позволяет нам поддерживать большую разницу температур, чем без разделения коридоров. Температура воздуха в холодном коридоре составляет 24°C, в горячем – 39°C.

Мы рассчитали среднегодовой коэффициент использования энергии PUE для каждого региона, в котором, как предполагается, будут работать системы охлаждения. Для расчетов мы воспользовались климатическими данными за 2011 г. для трех выбранных городов (рис. 3).

Рис. 3. Распределение температур по году для Москвы, Мурманска и Краснодара



Расчетные значения потребления энергии всеми инженерными системами дата-центра

	Мурманск	Москва	Краснодар
Общее энергопотребление ЦОДа за год, кВт·ч	2 918 573	3 115 217	3 295 326
Разница в энергопотреблении по сравнению с Краснодаром, кВт·ч	376 753	180 109	0

Несмотря на существенные отличия температурных графиков в этих регионах, для абсолютно одинаковых систем охлаждения были получены почти одинаковые расчетные значения PUE: Мурманск – 1,32, Москва – 1,34 и Краснодар – 1,36. Из таблицы видно, как сказывается эта небольшая разница в значениях PUE на энергопотреблении ЦОДов.

Каким же образом можно оптимизировать показатели механических систем для этих регионов?

В Мурманске можно снизить температуры теплоносителя в контуре конденсатора и уменьшить давление конденсации в чиллере, тем самым снизив энергопотребление компрессоров чиллера. Учитывая невысокие летние температуры, следует отказаться от системы адиабатического предварительного охлаждения на градирнях и проверить, можно ли уменьшить их размеры, что позволит сократить капитальные затраты на систему охлаждения.

В Краснодаре вполне возможно уменьшение концентрации этиленгликоля и повышение за счет этого эффективности работы чиллеров при одновременном сокращении мощности циркуляционных насосов.

Для Москвы исходная конфигурация системы является оптимальной.



Из приведенного примера становится ясно, что построив одинаковые по схеме системы для разных регионов, мы не получим существенных различий в значениях коэффициента PUE. Тем не менее энергопотребление, а значит, операционные затраты будут различаться. Помимо увеличения затрат на энергопотребление система охлаждения для краснодарского ЦОДа потребует еще и больших капитальных вложений по сравнению с мурманским.

Для того, чтобы добиться лучших показателей по капитальным и операционным затратам, следует для каждого региона разрабатывать индивидуальное техническое решение, оптимизирующее все факторы. К сожалению, проектировщики не всегда ищут оптимальное решение для системы охлаждения, им гораздо проще использовать какой-либо уже известный вариант. Поэтому мы считаем нужным перед принятием решения о применении той или иной схемы охлаждения провести для заказчика предварительные расчеты совокупной стоимости владения в случае разных механических систем – речь об этом шла в нашей предыдущей статье (см. «Технологии охлаждения в ЦОДах: как снизить коэффициент PUE», «ИКС» №10'2012, с. 88). ИКС

Развертывание ИТ-сред еще никогда не было настолько простым и оперативным!



Руководства по типовым решениям

Простота

Мы делаем все возможное, чтобы наши решения становились еще проще в установке, конфигурировании и интеграции с существующими и новыми ИТ-системами и ЦОДами. Системы APC by Schneider Electric поставляются, насколько это возможно, «готовыми к монтажу» (например, шкафы подготовлены к установке блоков распределения питания без применения инструментов, со стандартными средствами организации кабелей и т.п.). Благодаря простоте конфигурирования инфраструктуры заказчик получает возможность сосредоточиться на более насущных вопросах, таких как угрозы сетевой безопасности.

Адаптивность

Наши решения могут быть сконфигурированы в соответствии с особенностями ИТ-среды — будь то небольшое ИТ-помещение или крупный ЦОД — на любом этапе ее эксплуатации. Шкафы одинаково хорошо подходят для размещения оборудования всех производителей, разнообразие моделей позволяет развернуть ИТ-систему в любом имеющемся пространстве — от небольшого, зачастую нескоро приспособленного помещения до крупного ЦОДа.



Конфигурации, рассчитанные на любые ИТ-среды!

Управляемость

Локальное и дистанционное управление упрощается благодаря контролю выходных розеток ИБП, встроенным средствам мониторинга характеристик среды и отчетности об энергопотреблении. Возможность управления по сети и мощные средства подготовки отчетов помогают предотвращать неисправности ИТ-систем и максимально оперативно устранять те, что все же возникли, — находясь в любой точке мира! А наши услуги на всех этапах жизненного цикла решения помогают оптимизировать его функционирование.

Мониторинг и управление ИТ-средой из любой точки!



Простая в развертывании инженерная инфраструктура для любых ИТ-сред

Руководства по типовым решениям охватывают весь круг современных задач. Основа нашей системы: шкафы для оборудования и стоечные блоки распределения питания, совместимые с продукцией любых производителей — сконструированы в расчете на максимально простое развертывание. Легко адаптируемые компоненты, встроенные крепления для сцепливания шкафов между собой, предварительно установленные выравнивающие опоры, а также средства организации кабелей, которые могут дополнительно устанавливаться без применения инструментов, минимизируют затраты времени и сил на установку.

Business-wise, Future-driven.™

Infra²truxure

Комплексные решения на базе архитектуры Infra²truxure включают все необходимое для развертывания инженерной инфраструктуры ИТ-сред: средства защиты и распределения электропитания, системы охлаждения, шкафы и стойки, а также ПО управления. Модульные решения могут масштабироваться в зависимости от уровня ИТ-объекта: от небольшого коммутационного узла и серверной до крупного ЦОДа.



Узнайте больше о продукции компании APC by Schneider Electric.

Зайдите на сайт www.apc.com/promo, введите код 79219v

и скачайте наши информационные статьи.

APC
by Schneider Electric

Горизонтальные кабели

малого диаметра в ЦОДе



↑
Андрей СЕМЕНОВ,
доктор техн. наук

Использование в СКС для дата-центров кабелей с уменьшенным внешним диаметром – результат оптимизации, нацеленной на учет влияния других инженерных систем и экономическую эффективность.

Информационная кабельная проводка в ЦОДе в соответствии с требованиями профильных стандартов (TIA-942A, EN 50173-5) должна быть реализована на основе структурированной кабельной системы с использованием электропроводных и волоконно-оптических кабелей. Нормативные документы не конкретизируют тип элементной базы для создания линий и трактов, оставляя ее выбор на усмотрение автора проекта ЦОДа. Тем не менее результаты расчетов и практика проектов показывают, что при наличии технической возможности (скорости не свыше 10 Гбит/с, а в ближайшей перспективе – до 40 Гбит/с) линии длиной не более 35–40 м целесообразно реализовывать на симметричных кабелях. На линиях большей протяженности из-за отсутствия альтернативы предпочтительна многомодовая волоконно-оптическая техника. В основе такого разделения лежит в первую очередь энергетическая выгодность электропроводных изделий при построении линий небольшой протяженности.

Взаимное влияние оборудования в ЦОДе

Системы и подсистемы, входящие в состав дата-центров, четко делятся на две основные группы. Объекты, объединяемые в группу вычислительных систем, отвечают за выполнение ЦОДом своих основных функций – обработки данных. Комплекс же систем инженерного обеспечения создает компьютерным и телекоммуникационным устройствам условия для нормального функционирования, а обслуживающему персоналу – комфортные условия работы.

Уникальной особенностью ЦОДа как инженерного сооружения является очень тесное взаимодействие оборудования различного назначения, в том числе относящегося к разным группам. Один из примеров – взаимосвязь таких ключевых компонентов, как система воздушного охлаждения и СКС. Это обусловлено тем, что фальшпол, обязательный в аппаратных залах ЦОДа, несмотря на внешнюю простоту, представляет собой многофункциональное устройство. С точки зрения системы промышленного кондиционирования образуемое им пространство выполняет функции камеры статического давления для охлаждающего воздуха; с другой стороны, это пространство также используется для прокладки информационных кабелей.

Одним из ключевых количественных параметров, свидетельствующих о степени тщательности проработки и о качестве исполнения проекта ЦОДа, является известный коэффициент PUE. Система воздушного охлаждения с ее высоким энергопотреблением оказывает на него самое непосредственное влияние. Довольно эффективным средством приближения PUE к теоретическому минимуму является уменьшение аэродинамического сопротивления на всех участках тракта прохождения воздушного потока – от выхода прецизионного кондиционера до охлаждаемого оборудования на прямом участке и от горячего коридора до входа кондиционера на обратном. Отсюда немедленно вытекает необходимость всемерного уменьшения объемов различного оборудования, которое находится в пространстве фальшпола, в том числе кабелей СКС.

Минимизация внешнего диаметра кабелей

Задачу уменьшения объемов кабельных изделий, находящихся под фальшполом аппаратного зала, можно решить разными способами. Первый из них – вынос кабельных трасс в пространство над шкафами. Главным недостатком этого решения считается сложность текущей эксплуатации кабелей и опасность ухудшения качества связи из-за повышенной температуры, а также не слишком эстетичный вид зала.

Известная концепция установки коммутаторов локальной сети непосредственно рядом с серверами (top of the rack) позволяет существенно уменьшить количество линейных кабелей за счет мультиплексирования сигналов. Но ее практическое внедрение заметно сдерживается сложностью получения неблокируемой архитектуры и плохими экономическими характеристиками решения в целом из-за того, что трудно достичь высокого коэффициента использования портов активного сетевого оборудования.

В этих условиях наилучшие в комплексе характеристики обеспечивают кабели с уменьшенным внешним диаметром. Улучшение массогабаритных характеристик достигается за счет снижения диаметра токопроводящей жилы витой пары вплоть до обращения к проводам калибром 26AWG. Отметим, что именно этот путь дополнительно стимулируется экономическими условиями, сложившимися в последние несколько лет. В первых, существует естественное стремление к минимизации капитальных затрат на физический уровень информационной системы за счет уменьшения материалоёмкости кабельных изделий, особенно если учесть рост цен – в несколько раз за последнее десятилетие –

на сырье (нефть и медь) для изготовления ее основных компонентов. Во-вторых, использование линий на основе симметричных кабелей экономически выгодно из-за их заметно большей энергоэффективности по сравнению с оптическими решениями при передаче информации на те небольшие расстояния, которые характерны для ЦОДов. В-третьих, нет объективной необходимости в массовой поддержке серийного оборудования дистанционного питания в вариантах PoE и PoE+ (в ближайшей перспективе к ним, скорее всего, добавится PoE++) в фокусной области применения. Наконец, потенциальная емкость рынка кабельных систем для ЦОДов довольно высока, что создает все условия для быстрого возврата инвестиций в НИОКР, нацеленные на создание нового класса кабельных изделий.

Технические подробности

Основные стандарты, регламентирующие различные аспекты построения СКС в офисных зданиях и ЦОДах в части обеспечиваемых параметров линий, полностью гармонизированы между собой. Однако заложенная в действующие нормативно-технические документы предельная протяженность тракта в 100 м для ЦОДов на практике явно избыточна. В таких условиях потенциальный выигрыш, который будет получен в результате отказа от этой нормы, вполне мог бы быть направлен на улучшение массогабаритных характеристик линейных кабелей.

Кабель, на основе которого невозможно создавать 100-метровые тракты для поддержки интерфейсов

10G Ethernet, имеет заметно более высокое погонное затухание. Однако более жесткое ограничение по предельной длине позволяет сохранить отношение сигнал/шум (параметр ACR в различных вариантах) на входе приемника, необходимое для получения заданного качества связи.

Впервые на уровне серийного продукта похожий прием был частично (без отказа от соблюдения норм стандартов затухания) использован еще в 2004 г. компанией Krone в кабелях серии CopperTen категории 6a. Он был основан на снижении затухания за счет целенаправленного структурирования изоляции отдельных проводов. Но из-за высокой технической сложности это направление не было поддержано другими производителями.

Особо отметим, что потери в качестве принимаемого сигнала из-за увеличения затухания частично компенсируются некоторым выигрышем по значениям переходного затухания различных видов, характерного для рассматриваемых кабелей. Это явление имеет объективный характер и заключается в том, что уменьшенный диаметр токопроводящей жилы дает возможность уменьшить площадь витка за счет как более плотного прилегания проводов друг к другу, так и некоторого уменьшения шага скрутки. Это сопровождается уменьшением излучения в окружающее пространство. Из-за обратимости процесса также падает восприимчивость витой пары к внешнему электромагнитному излучению.

Кабели с уменьшенным внешним диаметром тестируют по тому же перечню параметров, что и их аналоги, применяемые для построения офисных СКС. При

iKS-Consulting
предлагает Вашему вниманию
Аналитический отчет:



«Российский рынок коммерческих дата-центров 2012-2016»

- Российский и мировой рынки коммерческих дата-центров
- Региональное развитие рынка дата-центров
- Перспективы развития «облачных» услуг в дата-центрах
- Новые проекты на российском рынке
- Бизнес-модели российских дата-центров
- Структура рынка по игрокам, услугам, регионам
- Перспективы и прогнозы
- Профили основных игроков

Параметры отчета:

■ Количество страниц: **120** ■ Количество таблиц: **32** ■ Количество графиков: **42** ■ Цена: **95 тыс. руб.** без НДС

Подробная информация:
E-mail: ef@iks-consulting.ru; тел.: +7 (495) 505-10-50

www.iks-consulting.ru



этом в технических данных, указываемых производителем, фигурируют преимущественно те же самые величины, которые указываются в стандартах. Исключение составляет затухание, которое имеет заметно большее значение, что, собственно, определяет предельную дальность связи.

Для конструкций с уменьшенным внешним диаметром широко применяется экранирование. Пленочные экраны, накладываемые на витые пары, минимально увеличивают их габариты, одновременно обеспечивая рост переходного затухания примерно на 20 дБ во всем частотном диапазоне.

В результате одновременного применения экранирования и снижения диаметра проволоки внешний диаметр кабеля категории 6а, относящегося к группе малогабаритных изделий, оказывается устойчиво ниже 6 мм независимо от материала внешней оболочки. Таким образом, получается, что кабель на десятки процентов тоньше своих полномасштабных аналогов.

Предполагается, что одной из наиболее емких областей применения кабелей малого диаметра станет зона проводки в ЦОДе. Несмотря на это, производители в своих фирменных материалах и руководствах пока не приводят аналитических соотношений, позволяющих простыми средствами определить предельную протяженность стационарной части составного тракта в зависимости от длины коммутационных шнуров. Эта особенность требует от проектировщиков и инженерно-технического персонала ЦОДа более высокого уровня профессиональных знаний.

Категории элементной базы

Само собой разумеется, что категория рассматриваемой элементной базы – понятие условное, так как обсуждаемые кабели принципиально не могут соответствовать всем тем условиям, которые зафиксированы в стандартах. Из аналогичных соображений не удастся воспользоваться понятием класса линии, так как их максимальная протяженность не достигает нормативных 90 м. Тем не менее мы употребляем именно термин «категория», привычный широкому кругу русскоязычных специалистов.

Фокусной областью применения изделий новой разновидности являются ЦОДы, в которых в настоящее время и в ближайшей перспективе наиболее востребованы 10-гигабитные сетевые интерфейсы. Естественным образом стоит ожидать наибольшего предложения кабелей категории 6а, которая в свое время была создана для работы именно с таким активным сетевым оборудованием. При этом в изделиях категории 6а наиболее последовательно доведена до своего логического конца основная идея новой разработки: предельная минимизация внешнего диаметра. Максимальная протяженность тракта не превышает 55 м, т.е. она гармонизирована с категорией 6.

Намного более скупо представлены кабели категории 7 и ее новейшей модификации 7а. В этом случае калибр токопроводящей жилы уменьшен до 23 AWG, что, вообще говоря, характерно для продукции катего-

рии 6. Особенность этих изделий в том, что проигрыш по затуханию оказывается намного меньше, а максимальная протяженность стационарной линии при передаче 10-гигабитного информационного потока может достигать 80 м. Таким образом, их можно рассматривать как средство построения длинных линий при возникновении такой необходимости по местным условиям конкретного проекта.

Рыночные перспективы

Благодаря очевидным выгодам, которые в фокусной области применения дает обращение к симметричным кабелям категории 6а и выше с уменьшенным внешним диаметром, они в настоящее время широко представлены на рынке и выпускаются множеством производителей, в том числе такими известными компаниями, как Brand Rex, Panduit, Draka, Datwyler и Nexans. То, что в данном перечне присутствуют в основном европейские компании, объясняется наличием у них опыта разработки и производства экранированных конструкций, что безусловно необходимо для рассматриваемой продукции.

Справедливости ради следует отметить, что ряд других известных производителей (например, Siemon) проявляют в отношении этой техники достаточно большой скепсис. В основе такой позиции лежит соображение о том, что кабели малого диаметра не имеют никаких резервов в части поддержки перспективных 40-гигабитных сетевых интерфейсов. В этой ситуации более предпочтительной стратегией видится дожидаться завершения работ по созданию элементной базы категории 8 с увеличенной до 1,5–2 ГГц шириной полосы нормирования параметров (проект 100Ohm Next Generation Cabling). Выигрыш с точки зрения улучшения условий работы системы воздушного охлаждения, несмотря на заметно больший внешний диаметр кабелей, достигается за счет уменьшения их количества.

Отметим, что максимальная протяженность тракта, реализованного на элементной базе категории 8, также будет составлять 50–55 м, уже привычные для ЦОДов.



Симметричные кабели СКС с уменьшенным внешним диаметром имеют достаточно большие перспективы при построении физического уровня информационной инфраструктуры аппаратного зала ЦОДа. Появление таких кабелей – естественный результат целенаправленной оптимизации СКС под коммерчески емкую область использования, выполненной с привлечением дополнительных данных с более высокого системного уровня. На рынке достаточно много изделий этой разновидности, предлагаемых рядом ведущих производителей СКС.

С учетом потенциально высокой практической востребованности кабелей с уменьшенным внешним диаметром в перспективе вполне возможно их выделение в отдельный самостоятельный подкласс кабельных изделий СКС. ИКС

Сервер для сред «БОЛЬШИХ ДАННЫХ»

HP ProLiant SL4500 Gen8 – это сверхплотный сервер, созданный на основе концепции конвергентной инфраструктуры HP, с показателями надежности, производительности и экономичности, отвечающими требованиям сред «больших данных».

Сервер имеет модульную архитектуру, что позволяет подобрать такую конфигурацию вычислительных ресурсов и ресурсов хранения, которая будет соответствовать требованиям конкретной среды. Он отличается большой плотностью размещения дисков – до 240 Тбайт в шасси высотой 4,3U (2,16 Пбайт в стандартной стойке 42U).

Сервер ProLiant SL4500 создан на основе архитектуры HP ProActive Insight, включающей встроенные средства аналитики и автоматизации:

- HP Predictive Spare Activation перемещает данные на другое устройство в случае угрозы сбоя, обеспечивая бесперебойную работу и защиту данных;
- HP Active Health поддерживает максимальную доступность сервера;
- HP Smart Update автоматизирует обновление микрокода сервера;
- HP Insight Online предоставляет доступ к широкому ассортименту услуг и программ гарантийной поддержки;
- HP Intelligent Infrastructure помогает снизить расходы на питание в ЦОДе и повысить коэффициент «производительности-на-ватт» до 70% по сравнению с серверами предыдущих поколений.



ProLiant SL4500 с технологией HP Smart Array обеспечивает в семь раз более высокую производительность ввода-вывода по сравнению с серверами предыдущего поколения. Интеллектуальные средства аналитики HP SmartCache оптимизируют управление трафиком подсистемы хранения, что уменьшает время отклика.

Архитектура, заложенная в серверы HP ProLiant SL4500, поддерживает различные реализации Apache Hadoop, в том числе решения компаний Cloudera и Hortonworks, а также дополнительное ПО, включая OpenStack Cloud и MongoDB.

HP: +7 (495) 797-3500

Система управления инфраструктурой дата-центра

DCIM-система StruxureWare for Data Center построена на базе программной платформы StruxureWare Data Center Expert, предназначенной для базового мониторинга в реальном времени состояния оборудования инженерной инфраструктуры разных производителей и окружающей среды помещений ЦОДа. Эта платформа имеет средства автоматического обнаружения новых устройств и их массовой настройки, а также инструменты для составления пользовательских отчетов и уведомления о любых сбоях с поддержкой возможности рассылки этой информации по протоколам Web, SNMP и Modbus, в том числе на мобильные устройства Apple и Android.

В единое решение для дата-центра входит также платформа StruxureWare Data Center Operation, позволяющая построить математическую модель дата-

центра, получить данные об ИТ-нагрузке ЦОДа и выполнить аудит ИТ-оборудования. Функции этой платформы можно расширить с помощью дополнительных модулей Capacity (планирование и оптимизация параметров работы систем электропитания и охлаждения, моделирование отказов оборудования и последствий изменений в его размещении), Change (автоматизация рабочих процессов в дата-центре, организация работ, контроль добавления, удаления и перемещения ИТ-оборудования ЦОДа), Vizor (считывание штрихкодов для инвентаризации ИТ-оборудования, доступ к данным по оборудованию инженерной инфраструктуры), Energy Cost (контроль энергопотребления) и IT Optimizer (мониторинг и оптимизация использования ресурсов ИТ-оборудования).

Schneider Electric: +7 (495) 777-9990

Модульный колл-центр

Колл-центр Panasonic – полнофункциональный продукт архитектуры клиент-сервер, состоящий из модулей, которые могут быть выбраны в зависимости от потребностей заказчика. В него входят следующие программные пакеты: CCAccounting (Учет), CCView (Контроль) (или CCView Lite, CCView 2012, CCView Lite 2012) и CCPro (Профессиональный).

CCAccounting обеспечивает учет и протоколирование поступающих вызовов, составление статистических отчетов по каналам связи и внутренним линиям.

CCView позволяет проводить мониторинг всех компонентов системы в режиме реального времени, оповещение абонента о расчетном времени удержания вызова до постановки в очередь. В версии CCView Enterprise сбор информации осуществляется с нескольких АТС на одном сервере. Собираемая информация включает в себя состояние каждого канала и внутренней линии, тип вызова, номер телефона и имя абонента каждой стороны, участвующей в вызове, а также нагрузку на линию связи. Поддерживается расширенное управление более чем 200 видами счетчиков и таймеров (активные, суммирующие, пиковых параметров).

CCPro обладает всеми перечисленными выше возможностями других модулей, а также возможностью контроля и обработки вызовов, поступающих к оператору (переадресация, консультации, конференции). Модуль обеспечивает работу с всплывающими окнами на рабочих столах операторов для быстрой идентификации абонентов и оповещение абонентов о расчетном времени ожидания в очереди. CCPro содержит комплексные инструменты накопления статистических данных и сбора информации в реальном времени. Поддерживает интеграцию с MS Outlook и другими CRM/ECM-приложениями.

Модули CCView и CCPro могут быть дополнены приложением CC Record Pro, инструментом для записи разговоров с гибкими настройками масштабируемости и мониторинга в режиме реального времени. Доступ к записываемым переговорам защищается несколькими уровнями системы безопасности. Продолжительность записи – 17 тыс. часов для хранилища емкостью 500 Гбайт. Функции Rapid Search (быстрый поиск) и Retrieve Easily (легкий доступ) позволяют находить запись по номеру внутренней линии, дате и времени, номеру линии, идентификации абонента, имени абонента и т.д.

Panasonic: +7 (495) 270-1635

Ультракомпактные волоконно-оптические ответвители

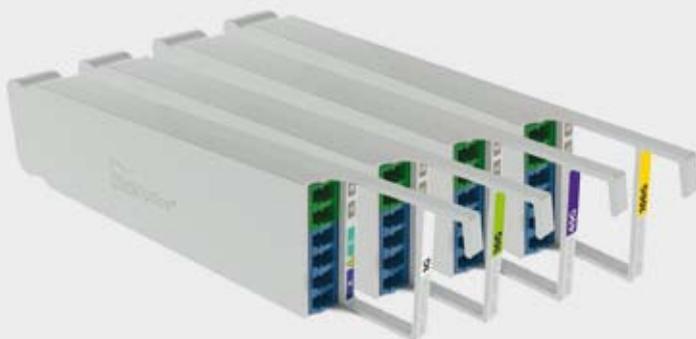
Будучи подключенными к волоконно-оптическим сетевым каналам, которые нужно контролировать, ответвители Flex Tap производства компании Net Optics обеспечивают полную видимость передаваемого по этим каналам дуплексного трафика (включая ошибочные пакеты) для устройств сетевого мониторинга и обеспечения информационной безопасности. В одно шасси высотой 1U, предназначенное для установки в аппаратную стойку, можно поместить до 24 ответвителей Flex Tap, что позволяет сэкономить зачастую дефицитное стоечное пространство.

Ответвители Flex Tap имеют полностью оптическую конструкцию и являются абсолютно пассивными устройствами, не нуждающимися в электропитании. Таким образом, они могут обеспечивать постоянный доступ к контролируемым сетевым каналам, не создавая угрозу отказа последних и не мешая передаче трафика по ним.

В семействе ответвителей Flex Tap есть многомодовые и одномодовые модели, имеющие разные коэффициенты деления мощности – от 50/50 до 90/10 – и предназначенные для передачи трафика с максимальной скоростью 1, 10, 40 или 100 Гбит/с.

Подключенное через ответвитель устройство мониторинга не нуждается в IP-адресе. Не имея его, это устройство является изолированным от сети, что значительно уменьшает его подверженность хакерским атакам. Ответвители Flex Tap совместимы с любыми протоколами и устройствами мониторинга, включая анализаторы протоколов, пробники и системы обнаружения вторжений.

Syrus Systems: +7 (495) 937-5959



Перечень публикаций журнала «ИКС» за 2012 г.

■ НОВОСТИ

КОЛОНКА РЕДАКТОРА № 1–12

АКТУАЛЬНЫЙ КОММЕНТАРИЙ

- С. АПОЛЛОНОВА. Статус отечественного. Примем на веру? . . . № 1-2
- М. ЕМЕЛЬЯННИКОВ. А что нам будет за то, что мы ничего по защите персональных данных делать не будем? № 3
- А. КАЛЛИС. Заново найти себя № 4
- Н. КИЙ. У вас продаются услуги связи? Услуги проданы. Остался СХ № 5
- Н. КИЙ. Бум проектов. 2008–2012-м посвящается № 6
- В. СЕРДЮК. Цифровому эфирному ТВ требуется HbbTV без условного доступа № 7-8
- Л. ПАВЛОВА. 20 лет, 20 зим № 9
- Л. ПАВЛОВА. Куда идешь, универсальная услуга? № 10
- Е. ВОЛЫНКИНА. Рейтинги не терпят суеты. № 11
- Е. ВОЛЫНКИНА. Три дороги российских ИТ № 12

ЛИЦА № 1–12

ПЕРСОНА НОМЕРА

- Сергей ЛЫСАКОВ. Mobilis in mobile, подвижный в подвижной среде. № 1-2
- С. АПОЛЛОНОВА. Дум высокое стремление и внутренняя вредность. № 3
- С. КАРПОВ: «Быть оптимистом и жить с улыбкой» № 4
- М. ТИМОФЕЕВ. Личное дело связиста-международника № 5
- Несколько жизней Бориса БОБРОВНИКОВА. № 6
- А. СВИРИДЕНКО: «Делай что должно – и будь что будет» № 7-8
- О. ВАТУЛИН: «Железо должно работать, и эмоции здесь ни при чем» № 9
- А. МАКАРОВ: «В жизни побеждают честные парни» № 10
- Д. НЕЛЮБОВ. Ощущая ритм времени № 11
- М. КАМЕННОВА. В согласии с собой. № 12

КОМПАНИИ

Новости от компаний № 1–12

- А. СЕМЕНОВ. Управлять сетевой инфраструктурой по-новому: опыт региональной телерадиокомпании № 5
- Д. ХЭМНЕР. В многомерном пространстве ЦОДа № 7-8
- Серверы, которые заботятся о себе сами № 7-8

КАДРОВЫЕ НАЗНАЧЕНИЯ

- С. РАСКАЗОВ. Глобальный игрок просчитывает сценарий роста. № 3

СОБЫТИЯ

- Н. КИЙ. Для тех, кто родился с выходом в Интернет № 1-2
- Л. ПАВЛОВА. Эфирная цифра на переправе № 1-2
- Е. ВОЛЫНКИНА. Большой IP-брат наступает. № 1-2
- Е. ВОЛЫНКИНА. Интернет на пороге доменного взрыва? № 1-2
- Л. ПАВЛОВА. НепрОSSтое уравнение № 1-2
- Н. КИЙ, А. КРЫЛОВА, Л. ПАВЛОВА. Неладно что-то в телевизионном королевстве. № 3
- Л. ПАВЛОВА. Киберзащите требуется консолидация № 3
- Л. ПАВЛОВА. Бизнес-болезни ВРМ № 3

- А. КРЫЛОВА. Электронный документооборот: две стороны одного рынка № 3
- Е. ВОЛЫНКИНА. Взаимность драйверов № 4
- Л. ПАВЛОВА. ТВ-товарищество держит удар № 4
- А. КРЫЛОВА. Что предложить клиенту вместо снижения цены? № 4
- Л. ПАВЛОВА. Что на календаре безопасности? № 5
- А. КРЫЛОВА. Контакт-центры в ожидании третьей волны. № 5
- Е. ВОЛЫНКИНА. От IQ – к AQ. № 5
- А. КРЫЛОВА. Мобилизация корпораций: рынок тронулся. № 6
- Л. ПАВЛОВА. ГЛОНАСС вразнобой № 6
- Е. ВОЛЫНКИНА. Гендерный вопрос в телекоме № 6
- А. КРЫЛОВА. На грани цифрового передела? № 6
- Л. ПАВЛОВА. Как примирить трубу и контент № 6
- А. КРЫЛОВА. На светлой стороне Рунета № 6
- Н. ШТАЛТОВНАЯ. Пощусь у облака № 6
- Н. КИЙ. Джаз-менеджмент. Зачем управлять контентом предприятия № 7-8
- Н. КИЙ. Человек со смартфоном – мечта мобильного бизнеса. № 7-8
- Л. ПАВЛОВА. Ностальгия по ясности № 7-8
- А. КРЫЛОВА. Камни преткновения на пути m-коммерции № 7-8
- Е. ВОЛЫНКИНА. 10% виртуализации с перспективами № 7-8
- Е. ВОЛЫНКИНА. Инфономика для оптимистов № 9
- Е. ВОЛЫНКИНА. Облака, Russian Edition № 9
- Л. ПАВЛОВА. Облака с условностями № 9
- Л. ПАВЛОВА. На «умной» мобильной волне № 9
- Е. ВОЛЫНКИНА. «Умный дом» пока без драйвера № 9
- Л. ПАВЛОВА. Как защитить мобильное рабочее место № 10
- А. КРЫЛОВА. Альянс для выпуска доверенных устройств № 10
- Е. ВОЛЫНКИНА. Российские ЦОДы в мировых трендах № 10
- Е. ВОЛЫНКИНА. Дотянуться до беспроводного гигабита № 10
- А. КРЫЛОВА. CRM как зеркало бизнес-процессов № 10
- Л. ПАВЛОВА. «ИнфоБЕЗсекьюрیتی»-2012 № 11
- А. КРЫЛОВА. Корпоративная мобильность: еще не массовое, но уже явление № 11
- А. КРЫЛОВА. PMP в России: парад стандартов № 11
- Л. ПАВЛОВА. Региональное ТВ готовит «кабельные подушки» № 12
- Е. ВОЛЫНКИНА. IPv6: хватит выжидать № 12
- Л. ПАВЛОВА. Услуги дефицитных емкостей № 12
- Р. МАЛКИН. Кто меняет правила игры? № 12
- А. КРЫЛОВА. Кому нужен голос клиента № 12
- А. КРЫЛОВА. Мобильные приложения для жизни в большом городе № 12

СУБЪЕКТ ФЕДЕРАЦИИ

- Ю. ФЕДОРОВА. Белгородчина: M&A не кончается № 1-2
- Ю. ФЕДОРОВА. Иркутские самородки по сходной цене. № 3
- Ю. ФЕДОРОВА. Кузбасс: кому достанутся золотые прииски № 4
- Ю. ФЕДОРОВА. Интернет для изобретателей № 5
- Ю. ФЕДОРОВА. Мультиинтернет в моногородах № 6
- Ю. ФЕДОРОВА. Вятские кружева оптики № 9
- Ю. ФЕДОРОВА. Пензяки, быстрее, выше, сильнее! № 10
- Ю. ФЕДОРОВА. Башкирия контрастов № 11
- Ю. ФЕДОРОВА. Вологодчина: местная связь не сдает позиции № 12

КАЛЕНДАРЬ СОБЫТИЙ № 1–12

■ ТЕМА НОМЕРА

ПРОФЕССИОНАЛЬНЫЙ АПГРЕЙД № 1-2



Фокус
Где, как и чему научат айтишника?
Анна КРЫЛОВА. Инвестиции в обучение по безопасности возвращаются
М. ЕМЕЛЬЯННИКОВ. Учитесь у лучших

Ракурс
Эффект (не)зависит от формы
М. ЗАЙЦЕВА. Когда регионы – впереди

Подробности
И. МОРОЗОВ. Расходы, которых избежать нельзя

Позиция
Д. ИЗМЕСТЬЕВ. Не бойтесь сертификации
А. ГРОМОВ. С сертификатом специалист дороже

Модель
В. ДУРЫГИН. ИТ-специалист – первая скрипка в оркестре технологий
Т. ЗОЛОТАРЕВА. Как прирастить нематериальный актив

Дискуссионный клуб «ИКС»
Предложение и спрос: встречным курсом?

Проекты

Вебинар федерального масштаба

Мэтры советуют

ОБЛАКА СОСРЕДОТАЧИВАЮТСЯ № 3



Фокус

В облака с открытыми глазами
А. НАЦЕКИН. Россия может задавать
мировые стандарты по облачным
вычислениям

Аналитик

М. БОДЯГИН. SaaS в России, или Почему
мы переезжаем в облака

Модель

В. МАЛАНИН. Интеллект облака для
мышц виртуализации

К. ФРИДРИХ. Кабельная инфраструктура для облака

Ракурс

Е. АКИМОВ. Защита в облаках – дело тонкое

А. РАЗУМОВ. Заметки реалиста

Сценарий

А. КУТУКОВ. В облако рука об руку с заказчиком

Р. ВОЛКОВ. Облака утоляют кадровый голод

К. АНИСИМОВ. Российским облакам не хватает конкуренции

Д. ИНШАКОВ. Облака – следующий виток развития ИТ?

В. ТКАЧЕВ. Российским облакам не хватает виртуализации

Дискуссионный клуб «ИКС»

Три проекции облака

Концептуальный поворот

В. КОРНИЕНКО. Требуется фигурная формовка кирпичей

Ю. ЗЕЛЕНКОВ. Куда могут завести SaaS-облака

Бизнес-партнер

Л. ШИШЛОВ. Как стать законодателем «облачной моды»

ГЛОНАСС: РЫНОК ПО ГОСЗАКАЗУ № 4



Фокус

Особенности национальной навигации

Ракурс

Ю. УРЛИЧИЧ, Г. СТУПАК.

ГЛОНАСС третьего поколения

Подробности

ГЛОНАСС повышает IQ на транспорте

Аналитик

Д. КУСКОВ. Персональная навигация

Модель

И. НЕЧАЕВ. Внимание: новый
операторский бизнес

Дискуссионный клуб «ИКС»

Бизнес под созвездием

Концептуальный поворот

Пока «пробел» не стал пробелом

ВСЕМ – БОНУС. В СЕТЯХ ПРОГРАММ ЛОЯЛЬНОСТИ. № 5

Фокус

Орудие неценовой конкуренции

Ракурс

О. СЕЙКО. Вишня на торт маркетолога,

или 5 аспектов программы лояльности

Ж. ЧАВАРРИЯ. Заправил машину – получи

мегабайты

А. МЕРЗЛЯКОВ. СНГ: типаж один,

дизайн – разный



С. ОЛЕХОВ. Благодарность оператора = приверженность абонентов

С. ШАМЗОН. Лояльность регионального рынка

Проекты

А. СОКОЛОВЕРОВ. Любимый клиент почты России

Сценарий

В. ЛУКАНИН. «Наша коалиция – весь мир»

М. ЖИГУНОВ. Лояльность в розницу

Аналитик

С. ХИТРОВ. Кобрендинг: выгоды и ограничения

Дискуссионный клуб «ИКС»

В инструментальной обработке

Концептуальный поворот

Ю. ГОДЫНА. Проповедь лояльности

ОПЕРАЦИЯ «КООПЕРАЦИЯ» № 6



Фокус

Е. ВОЛЫНКИНА. ВТО подкралась незаметно

Л. ПАВЛОВА. За всемирную кооперацию
в кибербезопасности

Ракурс

Н. КИЙ. Зона партнерства

Сценарий

Л. ПАВЛОВА. Платформенная
консолидация

Е. ВОЛЫНКИНА. Электронный регион:
от Москвы до самых до окраин

Проекты

Н. КИЙ. Технопарки вышли в ноль

А. КРЫЛОВА. Статус статуса

Модель

Л. ПАВЛОВА. ТВ третьего рынка

А. КРЫЛОВА. М2М: командная игра на зеленом поле

ЦОД В ШАГЕ ОТ ЗРЕЛОСТИ № 7-8

Фокус

От зрелости технологий – к зрелости
бизнеса и сервисов

М. БОДЯГИН. Зрелость впереди, пока рост

Ракурс

О. СИМАКОВ. Технологическая
зрелость ~ SLA

С. ШУРШАЛИН. Зрелость на троечку

Д. КАЛГАНОВ. У нас свои масштабы
зрелости

А. ПЛАТОНОВ. Среднюю прослойку –
на аутсорсинг

Подробности

А. АЛЯЕВ. Вся Москва – в коммерческом ЦОДе

А. СИНЯЧЕНКО. Все в гособлака?

Модель

С. АНДРОНОВ. Quality Assurance – «козырной туз» цодостроения

Бизнес-партнер

А. ГЕРАСИМОВ. Перспективы отечественной виртуализации

Г. БАЛДЕНКОВ. Питание для МегаЦОДа: без права
на ошибку

Дискуссионный клуб «ИКС»

Вырабатываем критерии зрелости

Концептуальный поворот

Д. МИЛОВ. Укрупнение – явный тренд

С. ХАЛЯПИН. Заказчики становятся прагматичнее

С. КИГИМ. Ожидаем дефицита и роста доходов



«ДОРОЖНАЯ КАРТА» ОБЛАЧНОЙ БЕЗОПАСНОСТИ № 9



Фокус
 Бетонный блок на облачном шоссе
 И. ТРИФАЛЕНКОВ. Практикум облачной безопасности

Гуру
 Д. КОСТРОВ. Движение на трех уровнях

Модель
 А. САНИН. Приглашение к ревизии

Ракурс
 В. УДАЛОВ. Разрушение мифа

Т. ФЛИНК. Проблема или возможность развития бизнеса?
 А. ГЕРАСИМОВ. Хранение данных: курс на централизацию
 12 правил защиты в виртуальной среде

Проекты

А. ПЛЕТНЕВ. Теперь нет классического подхода к информационной безопасности

Подробности

Чего не впишешь в документ
 А. ЛУКАЦКИЙ. Обратной дороги нет
 М. ГОТАЛЬСКИЙ. Лицо-голос вместо логина-пароля

Сценарий

Р. ЮСУПОВ. Цепочка доверия

Особое мнение

М. ЕМЕЛЬЯННИКОВ. Не по дороге с облаками

Дискуссионный клуб «ИКС»

Без периметра

Бизнес-партнер

В. ВОРОТНИКОВ. Производительность шлюзов безопасности: «кот в мешке» или разумный расчет

НА ГРЕБНЕ ИНФОРМАЦИОННОЙ ВОЛНЫ. № 10



Фокус
 ЕСМ – средство с омолаживающим эффектом

Аналитик
 Т. ФАРУКШИН. Рынок ЕСМ снаружи и изнутри

Полезные советы
 А. АКСЕЛЬРОД. Универсальных критериев выбора нет
 О. ПОДОЛИНА. Как оценить эффективность ЕСМ?

Проекты

А. ЕРМОЛАЕВ. Электронный документооборот в «Информационном городе»
 А. ГОДУНОВ. ЕСМ – последний штрих к автоматизации бизнес-процессов
 У медицины свой контент

П. СМЕРНОВ. СЭД – своими руками

Сценарий

В. СТЕПАНОВ. Ставка на сервисный подход
 А. ГАВРИН. Внедрять универсальную ЕСМ-систему не будем

Игроки

Р. ЩЕМЕЛЕВ. ЕСМ – угроза секретарям
 Л. АЛДОШИН. Рост ЕСМ опередит ИТ-рынок
 А. ЯКУНЧЕНКОВ. ЕСМ в банке

Дискуссионный клуб «ИКС»

ЕСМ в зеркале рынка

Бизнес-партнер

М. КАМЕННОВА. Бренд под тренд

ГОРОД С УМОМ. № 11



Фокус
 Город с высоким IQ

Ракурс
Город умнеет
 А. ЩЕРБАКОВ. Иркутская история
 А. ЖУЛИН, А. КОСТЫРКО, Л. СИНЯТУЛЛИНА. Умный город. Moscow edition
 А. ТИМОШИНА. Москва в рейтинге интеллекта мегаполисов

Бизнес-партнер
 С. КОНТОПЕР. К цифровому дому без проводов

Позиция

А. РТИЩЕВ. Умный дом – уже не дорогая игрушка
 В. ВОЛОБУЕВ. Интеллектуальное здание – пока имиджевый объект

Модель

Квартал транспорта
 И. ТЕМИРОВ. Универсальность транспортного интеллекта
 А. ЧИБИЗОВ. Концепция интеллектуальной транспортной системы только зарождается

Сценарий

Коммунальный квартал
 Умное расставание с деньгами за ЖКХ
 К. АНДРЕЕВА. Город как сервис

Полезные советы

С. МАСЛЕННИКОВ. Не надо есть слона целиком
 М. ЛУНЬКОВ. Умный выбор умных услуг

Подробности

И. ШУТОВ. Мониторинг должен быть интеллектуальным и прозрачным

Дискуссионный клуб «ИКС»

Мозги для дома и города

ГОСУДАРСТВО И БИЗНЕС. ЕДИНСТВО И БОРЬБА № 12

Фокус
 Ягодные места государства и бизнеса
 Д. КОСЕНКОВ. Кто поможет государству и бизнесу найти общий язык?

Проекты

К. БЫСТРУШКИН. ТВ-техника на господдержке
 Мультиплексное ГЧП
 Ю. ПРОХОРОВ. Формируется новый подход к ТВ

Ракурс

Зависшая платформа
 И. БУХШТАБ. Почему не выбирают свободное ПО
 В. РУБАНОВ. Открытые стандарты у закрытых дверей

Сценарий

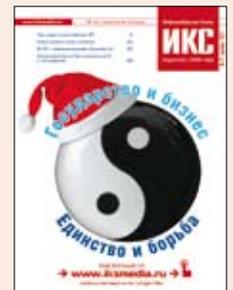
В. ВАЛЬКОВИЧ. Рынок спутниковой связи: арена интересов бизнеса и государства
 Партнерство в космической отрасли

Подробности

Д. ГОРДИЕНКО. Госзаказ из раза в раз

Модель

М. ТИМОФЕЕВ. Как государство лоббирует бизнес
 К. СОЛОДУХИН. Чего хотят низы и что могут верхи
 А. ЯКУНЧЕНКОВ. Синхронизация баз данных – основа успешного диалога государства и бизнеса



ДЕЛО

Экономика и финансы



- А. ЗАЙЦЕВА. Лучше широкого рынка. № 1-2
 А. ЗАЙЦЕВА. Выпавший из обоймы. № 3
 А. ЗАЙЦЕВА. Обгоняя растущий рынок. № 4
 А. ЗАЙЦЕВА. Вопреки широкому рынку. № 5
 А. ЗАЙЦЕВА. На волне распродаж. № 6
 А. ЗАЙЦЕВА. Без оглядки на конъюнктуру. № 7-8
 А. ЗАЙЦЕВА. Рост на фоне позитива. № 9
 А. ЗАЙЦЕВА. Опережая широкий рынок. № 10
 А. ЗАЙЦЕВА. Политические игры на фондовом рынке. № 11
 А. ЗАЙЦЕВА. Под давлением негатива. № 12

Доля рынка



- Е. ВОЛЫНКИНА. За ... лет до облачной эры. № 1-2
 Т. ТОЛМАЧЕВА. ИТ-помощь медицине. № 1-2
 И. СУНЧЕЛЕЙ. Медь и оптика: за мирное сосуществование. № 3
 А. КРЫЛОВА. ЦОДы упрочняются, вызовы множатся. № 5
 Rittal – традиции непрерывного развития. № 6
 И. ЯКИМЕНКО. Какое будущее у ЭЦП? № 6
 Е. ВОЛЫНКИНА. Виртуализация: низко висящие яблоки сорваны. Что дальше? № 6
 О. ХОЛОДНЫЙ. Серверы операторского класса: прошедшие сквозь огонь. № 6
 Н. ШКОЛЬНИКОВ. Этот умный, умный, умный мир. № 7-8
 Ю. ПРОХОРОВ. Дела земные и небесные. № 10
 А. ШИБАЕВ. В ИТ – незначительная облачность. № 12

Управление



- А. ГОЛЫШКО. Регулирование 2.0. С точки зрения сервисов. № 4
 А. ГОЛЫШКО. Регулирование 2.0. С неожиданной стороны. № 7-8
 А. КРЫЛОВА. Радиосвязь в начале нового цикла. № 7-8

High-Tech-маркетинг



- А. ЧУРИН. От вызовов – к возможностям. Повышаем лояльность абонентов. № 7-8

Рубежи обороны



- И. ЕХРИЕЛЬ, Э. БАЖЕНОВ, В. КОЛЕСНИК. Безопасность и фрод-контроль в сетях NGN/IMS. № 1-2
 И. ЕХРИЕЛЬ, Э. БАЖЕНОВ, В. КОЛЕСНИК. Безопасность и фрод-контроль в сетях NGN/IMS. *Окончание*. № 3
 Э. БЕЙБУТОВ. Мониторинг безопасности из облака. № 4
 И. МОМЧИЛОВИЧ. DLP: куда утекают данные. № 4
 Д. МИЛЛЕР. Защитить мобильные сети и их пользователей. № 5

Проблема



- Ю. ЧЕРНОВ. Всеу свое место. DRM'у тоже. № 3
 В. СЕРДЮК. Зачем общественному ТВ адресное управление. № 6
 В. СЕРДЮК. Цифровому эфирному ТВ требуется HbbTV без условного доступа. № 7-8
 П. ВАСИЛЬЕВ. Нам не страшен... WTO? № 9
 А. ВРОНЕЦ. Что может и чего хочет саморегулирование? № 11
 Дела и замыслы саморегулирования. № 11
 В. БОНДАРЬ. Между законодательными базами. № 11
 Р. КРЕЙНИН. Прикладное нормотворчество. № 11
 Эксплуатация снова на повестке дня! Круглый стол. № 11
 Эксплуатация снова на повестке дня! Круглый стол. *Окончание*. № 12
 Д. АВЕРЬЯНОВ. Мыльные пузыри, «мегафишки» и другие двигатели ИТ-рынка. № 12

Бизнес-модель



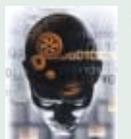
- А. КРЫЛОВА. FMC в эпоху универсализации. № 4
 Н. МАЗУР. Конвергенция начинается с бизнес-модели. № 4
 Е. ГРИГОРЬЕВА. Конвергенция растет, как мобильный Интернет. № 4
 Унифицированный биллинг как основа конвергенции. № 4

Право



- В. ЛЕВЧИК. Закон «О персональных данных»: поправки приняты, концепция не изменилась. № 3
 В. ЛЕВЧИК. Закон «О персональных данных»: поправки приняты, концепция не изменилась. *Окончание*. № 4
 А. МИШУШИН. Двое на одном стуле. № 4
 Е. КОВАЛЬ. Волоконно-оптические линии связи – возможна ли общая собственность? № 5
 А. МИШУШИН. Потребитель начинает и выигрывает? № 7-8

Опыт



- Л. КАН. Интегрируем оптимальную маршрутизацию трафика и взаиморасчеты. № 3
 Как организовать DNS в интересах блогосферы. № 4
 Edge-Core Networks Corporation: уроки завоевания рынка. № 5
 ЦОД для ЖКХ. № 5
 А. ШИБАЕВ. Из тумана – в облака. № 6
 Т. МОХОВА. Когда переезд # пожару. № 6
 А. ШИБАЕВ. Из тумана – в облака. Информационная безопасность в облаке. № 7-8
 В. БРЕТМАН. Опыт Microsoft требует движения вперед. № 9
 А. ПОЗДНЯКОВ. Мы за гибридную инфраструктуру. № 10
 Дж. КУДРИТЦКИ: «Молодые инженеры в России хотят строить ЦОДы правильно». № 11
 СК NG. Гигабит. 10, 40, 100... № 12
 Д. БХАНДАРКАР. Как сократить издержки на инфраструктуру. № 12

Человеческий фактор



- Т. БОНДАРЕВА, В. ОВЕРЧЕНКО. Как учить айтишника дистанционно? № 5
 И. КАНАРДОВ. Как мотивировать айтишника? № 6
 Д. БАШАКИН. Вы не любите виртуальные команды? Вы просто не умеете их готовить! № 9
 Д. БАШАКИН. Вы не любите виртуальные команды? Вы просто не умеете их готовить! *Окончание*. № 11

Горизонты



- А. ШАЛАГИНОВ. Временем не плененные. Феномен 20-летия. № 9
 А. ШАЛАГИНОВ. Феномен 20-летия. *Окончание*. № 10
 К. УИЛЛЕТТС. Эффект Кодака: как его избежать и преуспеть в цифровом мире. № 10
 К. УИЛЛЕТТС. Цифровой мир: жизненно необходим лидер! № 11

Решение



- Комплексные решения для ЦОДа в контексте CeBIT 2012. № 4
 Идеальная серверная стойка – Rittal TS IT. № 10

Услуги



- Д. ДЯКИВ, В. ЛЕВИН. Как не стать облаку грозой тучей. № 10

НА ПОРТАЛЕ IKSMEDIA

- Блог, еще раз блог! № 3–12

■ «ИКС» proTEХнологии

- И. КИРИЛЛОВ. ИБП для ЦОДов: выбор концепции № 1-2
- С. ЕРМАКОВ. Неочевидные решения для энергоснабжения ЦОДов № 1-2
- А. АННЕНКОВ. Противопожарная защита ЦОДов: нужен ли тест на герметичность № 1-2
- Дж. НИМАНН, Дж. БИН-мл., В. АВЕЛАР. Экономичные режимы работы систем охлаждения ЦОДов. Ч. 2 № 1-2
- И. МИХАЛЬЧУК. Интеллектуальный мониторинг – необходимый компонент ИТ-инфраструктуры ЦОДов № 1-2
- А. СЕМЕНОВ. Сетевые интерфейсы Ethernet 40 и 100 Гбит/с: что внутри? № 1-2
- Н. ПРИВЕЗЕНЦЕВА. Старая новая виртуализация в мире СХД . . . № 3
- Дж. НИМАНН, Дж. БИН-мл., В. АВЕЛАР. Экономичные режимы работы систем охлаждения ЦОДов. Ч. 3 № 3
- Е. ВИШНЕВСКИЙ, Т. ТОЛОКОННИКОВ. Климат региона и микроклимат ЦОДа. Учет климатических зон при анализе эффективности системы холодоснабжения № 3
- Е. КУРГАШЕВА. Бессменный часовой. Организация системы физической безопасности в здании ЦОДа № 3
- Д. МОРГУНОВ. Оптические разъемы LC при высокой плотности монтажа № 3
- В. ГАВРИЛОВ. Погода для ЦОДа. Нетрадиционные системы охлаждения № 4
- И. КИРИЛЛОВ. ДГУ в дата-центре: акцент на мощность и безотказность № 4
- А. ЛАСЫЙ, П. ВАШКЕВИЧ. Резервы повышения энергоэффективности ЦОДа № 4
- Р. НЭЙМЕК, Э. ФУРНЬЕ. Как снизить энергопотребление ЦОДа за счет выбора параметров работы чиллера № 4
- А. МАРТЫНЮК, И. АНИСИМОВ. Модернизация классики цодостроения: модульные дата-центры № 4
- В. МАКСИМОВ, П. ИВАНОВ. Новые подходы к пожаротушению в современных ЦОДах № 4
- Е. ВОЛЫНКИНА. Облака и мобильность на полпути друг к другу № 5
- Л. ПАВЛОВА. Технологии энергетического авангарда № 5
- Д. УИЛСОН. Гибридная энергетика в наружных установках . . . № 5
- П. РОНЖИН. Системы фрикулинга на базовых станциях сотовой связи № 5
- Телекоммуникационное оборудование «Энергомера» – качественно, надежно, перспективно № 5
- П. КОСТЮРИН. Что включить в SLA при обслуживании инженерной инфраструктуры ЦОДа № 5
- А. СЕМЕНОВ, Е. СОКОЛОВ. Медь и оптика в перспективных ЦОДах № 5
- И. КИРИЛЛОВ. Охлаждение ЦОДа – задача для практиков. Ч. 1. Моновендорные решения № 6
- Е. ВИШНЕВСКИЙ. Адиабатическое охлаждение воздуха в современном ЦОДе № 6
- А. ПАВЛОВ, Д. КУСАКИН, Д. БАСИСТЫЙ. ЦОД своими руками. Как не наступить на грабли чужих ошибок. 14 советов № 6
- М. МАЛОВ. Видеоконтроль в офисе. Критерии выбора IP-камер . . № 6
- И. КИРИЛЛОВ. Охлаждение ЦОДа – задача для практиков. Ч. 2. Мультивендорные решения № 7-8
- А. ВОТАНОВСКИЙ. Модульные ИБП Liebert АРМ – максимальная эффективность в минимальном пространстве № 7-8
- П. РОНЖИН. Климатические системы модульных ЦОДов. Новое или хорошо забытое старое? № 7-8
- А. ПАВЛОВ, Д. КУСАКИН, Д. БАСИСТЫЙ. Бизнес-план и финансовая оценка создания ЦОДа высокого уровня надежности № 7-8
- Д. ПАВЛОВ. ВКС меняет парадигму № 7-8
- А. АННЕНКОВ. Локомотив инноваций № 7-8
- Р. НЭЙМЕК. Внутривенное охлаждение для высоконагруженных стоек № 7-8
- А. МАРТЫНЮК. Создание ЦОДов: как разумно потратить деньги № 9
- М. БАЛКАРОВ. Легенды и мифы прецизионного кондиционирования № 9
- С. ЕРМАКОВ. Динамика против статики? Нет! И динамика и статика! Гибридная схема бесперебойного электропитания № 9
- П. КОСТЮРИН. Построение службы эксплуатации ЦОДа № 9
- А. СЕМЕНОВ. Оптические кроссы высокой плотности. Насколько они востребованы? № 9
- П. ИВАНОВ, В. МАКСИМОВ. Еще раз о газовом пожаротушении в ЦОДах. Выбираем тип установки № 9
- А. КРЫЛОВА. Инженерная инфраструктура ЦОДа: слагаемые эффективности № 10
- Ю. КОЛЕСОВ. Комплексное решение проблем ЦОДа № 10
- А. АБРАМОВ, О. АНТИПОВА. Дом по имени ЦОД: архитектурные идеи инженерных вершин № 10
- Д. САХАРОВ. Рынок серверов пока продолжает рост № 10
- Д. КУСАКИН, Д. БАСИСТЫЙ, А. ПАВЛОВ. Управление проектом создания ЦОДа. Из российской практики № 10
- А. ЛАСЫЙ, П. ВАШКЕВИЧ. Оптимизируем ЦОД под заказчика № 10
- П. РОНЖИН, В. КАЗАКОВ. Технологии охлаждения в ЦОДах: как снизить коэффициент PUE № 10
- Д. САХАРОВ. ЦОД, где живут облака № 11
- А. АБРАМОВ, О. АНТИПОВА. Цодостроение на аутсорсинге . . . № 11
- Р. ЗАЕДИНОВ. Аварийное восстановление из облака № 11
- А. СЕМЕНОВ, М. ШОЛУДЕНКО. Отечественный стандарт на симметричные кабели связи для СКС и ШПД № 11
- Е. ВИШНЕВСКИЙ. Как уменьшить счет за электроэнергию? . . . № 11
- Е. КУРГАШЕВА. Единая система пожарной сигнализации для офиса и ЦОДа № 11
- Е. ВОЛЫНКИНА. Проектирование и строительство ЦОДа: уникальность с типизацией № 12
- М. БАЛКАРОВ. Легенды и мифы прецизионного кондиционирования-2 № 12
- А. ПАВЛОВ, Д. КУСАКИН, Д. БАСИСТЫЙ. Типовые отказы ЦОДов и их профилактика № 12
- А. АННЕНКОВ. Автономное и универсальное новое устройство пожаротушения российского производства № 12
- С. КУЧУМАРОВ. Сети для систем безопасности: оптимальные топологии № 12
- А. СЕМЕНОВ. Системы интерактивного управления в малых и средних СКС № 12
- НОВЫЕ ПРОДУКТЫ № 1-12**



АБИТЕХ
Тел./факс: (495) 234-0108
www.abitech.ru **с. 77**

ИК ГУЛЛИВЕР
Тел./факс: (495) 663-2172
E-mail: info@ikgulliver.ru
www.ikgulliver.ru **с. 71**

ИНТЕРСПУТНИК
Тел.: (499) 252-8333
Факс: (499) 271-0784

E-mail: dir@intersputnik.com
www.intersputnik.ru **с. 49**

ЛАНИТ
Тел.: (495) 967-6650
Факс: (499) 261-5781
E-mail: lanit@lanit.ru
www.lanit.ru **с. 39**

СВЯЗЬСТРОЙДЕТАЛЬ
Тел.: (495) 786-3434
Факс: (495) 786-3432
E-mail: mail@ssd.ru
www.ssd.ru **с. 15**

DR.WEB
Тел.: (495) 789-4587
Факс: (495) 789-4597
www.drweb.com **4-я обл.**

EMERSON NETWORK POWER
Тел.: (495) 981-9811
Факс: (495) 981-9810
E-mail: sales@emerson.com
www.emersonnetworkpower.com **с. 73**

HOSSER TELECOM SOLUTIONS
Тел.: (812) 363-1193

Факс: (812) 363-1194
E-mail: spb@h-ts.ru
www.h-ts.ru **с. 81**

POWERCOM
Тел.: (495) 651-6281
Факс: (495) 651-6282
www.pcm.ru **с. 74-75**

APC BY SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.apc.com/ru **с. 85**

SONY ELECTRONICS
Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu **с. 13**

STL-R
Тел./факс: (495) 747-6000
E-mail: info@stl-r.ru
www.stulz.com **с. 83**

VERIMATRIX
Тел.: (926) 525-7624
www.verimatrix.com **с. 56-57**

Указатель фирм

«1С» 58	Ivi.ru 57, 67, 68	Verimatrix 56, 57	Координационный центр национального домена 12	РСК 15
3М 9	J'son&Partners 29	VimpelCom Ltd. 47, 48	сети Интернет 12	«РТКомм» 51
Accenture 16	Krone 87	Vodafone 28	«КОРУС Консалтинг» 60	РТС 47
Acer 29	KyotoCooling 63	Yandex N.V. 48	КРОК 31, 45	«Самсунг» 43
Allied Telesis 12	LETA 44	Yota Networks 17	«Лабиринт» 59	Электроникс Рус 6, 47, 48
ALT Linux 60	LG 67	Zenprise 13	«Лаборатория Касперского» 30, 44	Сбербанк России 53
Altimo 48	LinuxWizard 60	Ziggo 57	ЛАНИТ 12, 39	Сберкред Банк 53
App Central 33	Mail.ru Group 19, 47, 48	Zynga 48	«Латтелеком» 57	«Связьинвест» 22, 51
Apple 29, 30, 34, 37, 57	MasterCard 15	«Ай-Текно» 14	«Манго Телеком» 34	«Связьинформ» 21
ARInteg 8, 44, 53	ГК MAYKOR 30, 45, 74, 75	ГК «АйТи» 8	«Манотомь» 59	«Северсталь» 53, 54
Artezio 12	Meraki 13	ГК «АйТи» 29, 30, 36, 60	МГТС 53	СЗТ 51
ASHRAE 62, 81	Microsoft 8, 12, 19, 45, 57	Академия народного хозяйства 8	«МегаФон» 21, 35, 36, 47, 48, 50, 57	«Сибирьтелеком» 51
Asia Broadcast Satellite 49	«MOBI. Деньги» 12	«АльфаСтрахование» 53	Межрегиональный центр межотраслевой информатики 8	«Синезис» 20
ASUS 29, 45	Moscow Business School 8	«Аналитика Плюс» 17	Госатомнадзора России 8	«Синтерра» 21
AT&T 28	Net Optics 90	«Антивирусный Центр» 8	МИСИ им. Куйбышева 8	ООО «Сиско Системс» 12
BBK 67	Netgear 12	АРСИБ 55	ММБИ 8	АФК «Система» 48
Borland 8	Nexans 88	«Астерос Консалтинг» 30, 38	ММВБ 47	«Скай Линк» 21, 47
Brand Rex 88	North Bridge 58, 59, 60	«Башинформсвязь» 51, 57	ММТС9 51	СКН 20
CDNvideo 66	Venture Partners 80	«Белтел» 12	«Москва, которой нет» 12	СМП Банк 53
Check Point Software Technologies 41	Oracle 13	«ВестБалт Телеком» 21	Московская биржа 47, 48	СО ЕЭС 12
China Electronics Software 15	Orange Business Services 28	«ВКонтакте» 68	«Московские новости» 12	«Совтелеком» 50
Cisco 13, 15, 66	Panasonic 20, 90	ВНИИ ПО 69	Московский автомобильный институт 8	НП «Сообщество потребителей энергии» 18
Citrix 13	Panduit 88	Военный Краснознаменный институт МО 8	«Московский межгородный и международный телефон» 22, 51	«С-Терра СиЭспи» 40
Clearwire 13	PCCW/NOW TV 57	«Возрождение» 52, 54	МТС 8, 12, 15, 17, 21, 29, 33, 47, 50, 52, 53, 60, 66	Стокгольмская школа экономики 9
Cloudera 89	PingWin Software 60	«Волгателеком» 51	МФТИ 15	«Стрим» 66
Coca-Cola 9	PowerCom 74, 75	«ВымпелКом» 8, 12, 18, 21, 28, 31, 50, 53, 55	«Национальные телекоммуникации» 47, 51	«СЦС Совинтел» 8
Cocacola 9	Precept Software 66	«Газинтернет» 21	ГК «НКТ» 8	«Таттелеком» 57
Com Hem 57	QuickFix 57	«Гарант» 59	«Норильск-Телеком» 47	«Телеинком» 55
Credant Technologies 13	Radware 53, 55	ГКБ № 1 им. Н.И. Пирогова 75	Нью-Йоркская фондовая биржа 47	«Телесет Лтд.» 21
Datwyler 88	RETN 47	ГКБ № 36 74	Перинатальный центр (Хабаровск) 74	«ТехноСерв Евразия» 12
Dell 13	Rhodium 48	Главный центр управления межгородными связями 50	«ПетерСтар» 21	«Техносерв» 20
Draka 88	RIM 29, 32	«ГНУ/Линуксцентр» 60	РАЗК 12, 19, 23	«ТИС-Диалог» 21
Eaton 15	Samsung Electronics 12, 29, 41, 67	«Голден Телеком» 8	РБК 47, 48	ТК 15, 31
Eloqua 13	SAP 46	«Дагсвязьинформ» 51	РЖД 13, 32	«Универсальная электронная карта» 6
Emerson Network Power 73	SAS 16	«Дальсвязь» 51	РОСА 60	«Уралсвязьинформ» 51
Ericsson 9, 10	Scania 9	Европейская Ассоциация операторов связи 16	«Росгосстрах» 30, 31	УК «Финам Менеджмент» 47
Etersoft 58, 60	Serbia Broadband 57	«Евро-Телеком» 21	РОСНО 8	«Флант» 60
Face.com 48	Siemens Enterprise Communications 30, 42	«Емельяников, Попова и партнеры» 52	Российское агентство развития ИО 6	Фонд информационной демократии 6
Facebook 15, 48	Softline 44, 60	«Зебра Телеком» 51	«Ростелеком» 6, 7, 15, 17, 18, 21, 22, 28, 29, 47, 50, 51, 52, 57	Фонд содействия развитию технологий и инфраструктуры 6
Forrester Research 33	Sony 67	«Ингушэлектросвязь» 51	«Роснано» 46	сети Интернет 18
Google 42	Space Systems/Loral 47	Институт электронного государства 6	РОСНО 8	«Центральный телеграф» 12, 28, 51
Group 48	Sprint Nextel 13	«ИНТЕРСПУТНИК» 49	«ИнтерТраст» 29	«Центртелеком» 51
GSM 16	STL-R 83	«Интертелеком» 50	«Комбелла» 8	«Чукоткасвязьинформ» 51
Hortonworks 89	Stulz 81, 83	«ИнтерТраст» 29	«Коминком» 8	«Шнейдер Электрик» 89
HP 8, 13, 89	Sun Microsystems 8	«Комбелла» 8	«Компьютер-центр Кей» 59	ЭВОЛА 44
HTS 81	Syrus Systems 90	«Компьютер-центр Кей» 59	НТЦ «Комсет» 17, 28	ЮТК 51
IBM 14, 16	Tableau Software 17	НТЦ «Комсет» 17, 28		«Яндекс» 48
IBS 61	Tele2 21, 50			
IBS Group 48	Telenor 48			
IBS Platformix 44	TVzavr 57			
iconBIT 67	Uptime Institute 77, 79, 80			
iKS-Consulting 21				
IMS Research 20				
Intel 15				
ITV/AxonSoft 20				

Учредители журнала «ИнформКурьер-Связь»:

**ЗАО Информационное агентство
«ИнформКурьер-Связь»:**
127273, Москва, Сигнальный проезд, д. 39, подъезд 2,
офис 204; 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.