Рост вопреки традициям

В апреле российские площадки продолжили снижение, тогда как биржи Европы и США демонстрировали рост. Но затем, нарушив майскую традицию, отечественный рынок начал активно восстанавливать позиции. Телеком-сектор, следуя этому же тренду, в итоге оказался в плюсе.

Анна ЗАЙЦЕВА,
аналитик,
УК «Финам Менеджмент»

Нисходящий тренд апреля зашел так далеко, что во второй декаде месяца наши площадки достигли минимальных значений в текущем году. Причиной падения рынка РФ стал огромный отток капитала из фондов, инвестирующих в Россию. В мае же, несмотря на минимальные объемы торгов, российский рынок акций перешел к росту, чему способствовал позитивный внешний фон, а именно действия мировых ЦБ и завершающийся сезон корпоративной отчетности в США.

«Ростелеком» обновляет кадры и обещает дивиденды

Капитализация «Ростелекома» за рассматриваемый период выросла на 1,17%, до 116,34 руб. за акцию. Месяц оказался насыщенным на корпоративные события. В холдинге произошел ряд кадровых назначений: старшим вице-президентом «Ростелекома», ответственным за реализацию проектов в рамках ФЦП «Информационное общество», был назначен Андрей Чеглаков, а коммерческий блок оператора в ранге вице-президента возглавила Лариса Ткачук.

Среди других значимых событий следует выделить одобрение советом директоров «Связьинвеста» покупки более 12,64 млн акций «Ростелекома» у ООО «Мобител» по цене 136,05 руб. Таким образом, на приобретение акций будет направлено в общей сложности 1,72 млрд руб. В результате сделки количество принадлежащих «Связьинвесту» акций вырастет до 1,346 млрд штук (до 45,72% в акционерном капитале и 42,23% в УК). Следует отметить, что вопрос о реорганизации ОАО «Ростелеком» в форме присоединения к оператору ОАО «Связьинвест» и 20 принадлежащих им стопроцентных «дочек», будет рассмотрен на внеочередном общем собрании акционеров 26 июня 2013 г.

На 17 июня запланировано годовое общее собрание акционеров (ГОСА) ОАО «Ростелеком». Ранее совет директоров компании рекомендовал собранию направить на выплату дивидендов по итогам 2012 г. 8,17 млрд руб. (соответствует 25% чистой прибыли по РСБУ или 23,18% по МСФО). Таким образом, размер дивидендов составит 2,4369 руб. на одну обыкновенную акцию и 4,1022 руб. на «преф». Право на получение дивидендов получат лица, числящиеся акционерами «Ростелекома» по состоянию на 30 апреля 2013 г.

В прошлом месяце «Ростелеком» опубликовал негативную отчетность по РСБУ за I квартал 2013 г. Так, чистая прибыль компании снизилась на 42,6%, до 7,64 млрд руб. при снижении выручки на 11% (67,744 млрд руб.). Себестоимость сократилась на 5,5% (до 54,45 млрд руб.), а валовая прибыль – на 28,2% (до 13,291 млрд руб.). Спад основных показателей руководство холдинга объяснило значительными «единовременными» доходами и расходами в рамках проекта организации видеонаблюдения за выборами президента РФ.

В начале апреля была закрыта сделка по покупке банком ВТБ у шведского холдинга Tele2 компании Tele2 Russia, при этом покупатель заявлял о намерении снизить свою долю в приобретенном активе ниже контрольной. Многие участники рынка ожидают, что конечным бенефициаром данной сделки выступит именно «Ростелеком», который в результате консолидации Tele2 Russia мог бы стать четвертым по величине игроком российского рынка сотовой связи. Примечательно, что ФАС, как сообщил глава службы Игорь Артемьев, может одобрить покупку Tele2 Russia «Ростелекомом», если будет подана соответствующая заявка (пока ее в ведомство не поступало). О стремлении «Ростелекома» укрепить свои позиции в мобильном сегменте свидетельствует, в частности, информация о запуске в коммерческую эксплуатацию сети 3G+ в пяти регионах УрФО. Напомним, в настоящий момент оператор ведет строительство сетей мобильной связи третьего поколения в 27 регионах РФ.

Большая тройка отчиталась за квартал

Динамика акций мобильных операторов в прошлом месяце была разнонаправленной. Так, акции ОАО МТС подешевели на 1,72% – до 259,55 руб. Вероятно, основным поводом для негатива стала опубликованная оператором отчетность по РСБУ по итогам I квартала 2013 г. Чистая прибыль МТС снизилась в 3,1 раза по сравнению с аналогичным периодом прошлого года, откатившись до 7,38 млрд руб. При этом выручка увеличилась

Справка ИКС

За период с 15 апреля по 15 мая индекс ММВБ прибавил 0,46% – до отметки 1391,98 пункта, а индекс РТС так и не сумел отыграть потери (–0,7%), остановившись на отметке 1391,01 пункта. Капитализация отраслевого индекса «ММВБ телекоммуникации» за месяц выросла на 1,12%, составив 2092,59 пункта.

на 4,5% – до 66,24 млрд руб., а валовая прибыль достигла 31,6 млрд руб. (+8,7%).

Ряд опубликованных в апреле новостей оказал поддержку капитализации МТС. В частности, следует выделить утверждение советом директоров компании положения о дивидендной политике в новой редакции, предусматривающей рост дивидендных выплат в 2013–2015 гг. в среднем на 30%. Совокупный объем выплат дивидендов за этот период составит минимум 120 млрд руб. Следует отметить, что по итогам 2012 г. совет директоров оператора рекомендовал собранию акционеров (оно состоится 25 июня) выплату дивидендов в размере 14,6 руб. на одну обыкновенную акцию. Таким образом, общая сумма дивидендов может достичь 30,2 млрд руб. Реестр акционеров был закрыт 8 мая 2013 г.

Бумаги VimpelCom за месяц подешевели более чем на 10% (–10,83%, до $10,95 за шт.). Коррекция носит преимущественно технический характер в период отсечек, хотя инвесторов могло насторожить, что дивидендная доходность по бумагам компании ($1,14 на акцию, всего $2 млрд) составила практически 13% – рекордное значение для телекоммуникационной отрасли, и это на фоне высокой долговой нагрузки VimpelCom.

В апреле оператор опубликовал в целом неплохую отчетность по стандартам РСБУ и МСФО. Так, чистая прибыль «Вымпелкома» в I квартале 2013 г. по российским стандартам выросла на 29,8%, до 19,78 млрд руб. (по сравнению с аналогичным периодом прошлого года) при росте выручки на 5,7% (до 69,47 млрд руб.) и валовой прибыли – на 3% (до 43,053 млрд руб.). В свою очередь, чистая прибыль VimpelCom Ltd по МСФО увеличилась в I квартале на 28% (до $408 млн), тогда как выручка оператора практически не изменилась ($5,591 млрд против $5,619 млрд), что свидетельствует о росте эффективности бизнеса. Рентабельность по EBITDA повысилась с 41,1 до 42%.

Из важных событий, произошедших в отчетный период, следует выделить получение VimpelCom $1,4 млрд от Altimo в рамках конвертации 128,532 млн привилегированных акций в обыкновенные, конверсионная премия составила $10,835 за акцию. В результате экономическая доля Altimo в VimpelCom выросла с 52,7 до 56,2% при сохранении прежней голосующей доли. В кадровой сфере следует отметить переизбрание наблюдательного совета VimpelCom – он сохранился в прежнем составе. При этом о намерении покинуть компанию осенью текущего года заявил ее финансовый директор Хенк Ван Дален, объяснив это окончанием срока действия трудового контракта.

Акции «Мегафона», вопреки динамике бумаг остальных операторов большой тройки, прибавили за месяц 12,32% – до 1035 руб. за шт. Новостной фон вокруг компании нельзя назвать насыщенным, однако все публикуемые новости имели достаточно высокую значимость для инвесторов. В частности, «Мегафон» заявил об отказе от представления отчетности по US GAAP в пользу МСФО – и 15 мая опубликовал отчетность по МСФО за I квартал 2013 г. Чистая прибыль оператора по сравнению с аналогичным периодом прошлого года выросла на 36,5% (до 12,641 млрд руб.), консолидированная выручка – на 7,6% (до 67,72 млрд руб.), рост OIBDA составил 26,8% (до 32,38 млрд руб.). По прогнозу менеджмента «Мегафона», рентабельность OIBDA по итогам 2013 г. может достигнуть 42,5–44% вместо ожидаемых ранее 41,6–43%. При этом объем капитальных вложений на 2013 г. составит 55–60 млрд руб. На прошедшем совете директоров ОАО «Мегафон» общему собранию (состоится 28 июня) было рекомендовано утвердить дивиденды по итогам 2012 г. в размере 54,17 руб. на одну обыкновенную акцию. Кроме того, СД рекомендовал выплатить промежуточные дивиденды за I квартал 2013 г. в размере 10,34 руб. В результате совокупные выплаты акционерам «Мегафона» составят 33,585 млрд руб. за 2012 г. и 6,411 млрд руб. – за I квартал 2013 г.

ИТ-компании подорожали

Капитализация российских публичных ИТ-компаний за рассматриваемый период преимущественно выросла. Безусловным лидером роста стали бумаги компании Yandex N.V., подорожавшие на 20,82%, до $27,22 за бумагу. Повод для активных покупок акций очевиден – отличная финансовая отчетность «Яндекса» по итогам I квартала 2013 г. по US GAAP. Чистая прибыль поисковика выросла на 79% (г/г), до 2,2 млрд руб., выручка – на 36%, до 8 млрд руб., операционная прибыль – на 57% (до 2,5 млрд руб.), а скорректированный показатель EBITDA увеличился на 47% (до 3,5 млрд руб.). Помимо отчетности драйвером роста акций «Яндекса» могла стать информация о том, что Oppenheimer Funds увеличил долю в Yandex N.V. до 11,17% акций класса «А» (20987050 голосов).

Бумаги Mail.Ru Group подорожали за месяц на 5,96% – до $29,14 за шт. Выручка интернет-холдинга в I квартале 2013 г. по МСФО выросла на 29,4% по сравнению с январем-мартом 2012 г., составив 6,3 млрд руб. Как сообщила компания, ключевыми факторами роста стали контекстная реклама и ММО-игры, выручка от которых увеличилась на 47,9% (736 млн руб.) и 41,5% (1,54 млрд руб.) соответственно. Постепенное восстановление темпов роста демонстрировали и доходы от медийной рекламы. На 7 июня 2013 г. запланировано ГОСА, где будет рассмотрен вопрос о совете директоров компании: акционерам предстоит выбрать восьмерых из девяти кандидатов, среди которых два новых – Бретт Синклер Эрмитедж и Борис Добродеев. Не вошли в список кандидатов три действующих директора, в том числе соучредитель Mail.ru Григорий Фингер.

Акции АФК «Система» прибавили 4,62%, до $27 за шт. Согласно отчетности компании по US GAAP за IV квартал 2012 г., чистая прибыль корпорации возросла на 36,9% – до $357,9 млн, выручка увеличилась на 13%, до $9,5 млрд (г/г), а показатель OIBDA без учета корректировок снизился на 1,9% (до $2,1 млрд) по причине роста расходов по налогам в АНК «Башнефть». Как заявил президент АФК «Система» Михаил Шамолин, корпорация намерена увеличить размер дивидендов за 2012 г. Кроме того, менеджмент компании не исключает в перспективе возможности проведения SPO как одного из источников привлечения ресурсов для развития, но не при текущих ценах, которые недостаточно высоки. ИКС

Выиграть с партнерами *или* проиграть в одиночку

В соответствии с традиционной бизнес-моделью телекома оператор один владеет и управляет всеми ресурсами, необходимыми для оказания услуги. Но в цифровом мире это встречается все реже, поэтому важным конкурентным преимуществом становится умение создавать и поддерживать взаимовыгодные партнерские отношения.

Кит УИЛЛЕТТС,
председатель,
TM Forum

Модель автономного предоставления услуг сегодня быстро вытесняется подходами, в соответствии с которыми компоненты услуги создаются группой партнеров в рамках сотрудничества. Эти компонентные услуги предоставляются кругом поставщиков, широким, как никогда ранее, и могут включать в себя такие возможности, как подключение к сети связи, ресурсы процессорной обработки, хранилища данных, приложения, а также управление взаимодействием с пользователем – биллинг, клиентское обслуживание и т.д. Компоненты составной услуги оказываются во взаимной зависимости: они либо совместно обеспечивают ее работоспособность, либо вместе испытывают проблемы.

Таким образом, возникают все более сложные партнерства, в которых компании выступают одновременно и в роли поставщиков, и в роли потребителей внешних управляемых сервисов. Этот дуализм поставщика/потребителя свидетельствует о том, что на смену цепочке добавленной стоимости с фиксированными точками соединения приходит сеть добавленной стоимости. Например, при организации сервиса Whispernet компания Amazon является и поставщиком облачных управляемых услуг, и потребителем управляемых коммуникационных услуг.

Но эволюционируют не только бизнес-модели – сами услуги становятся все более сложными и изощренными. Хотя первоначально цифровые услуги были нацелены преимущественно на потребительский рынок, сейчас они все шире используются корпоративными пользователями, которым необходимо высокое качество услуг, базирующееся на соглашениях об уровне обслуживания. Предоставление услуг, для которых вы готовы обеспечить гарантии качества, действующие вдоль всей цепочки из многих партнеров, требует большого опыта управления взаимодействием этих партнеров.

Что такое управляемые услуги?

В отличие от аутсорсинга, который зачастую подразумевает лишь передачу людей и/или инфраструктуры вместе с ответственностью третьей стороне, управляемая услуга – это, как правило, «черный ящик». Вы не вникаете в детали ее реализации, а концентрируетесь на том, что именно поставляется. Пожалуй, наиболее наглядным примером может служить поставка электроэнергии: она к вам просто поступает, и все, что вас заботит, это чтобы напряжение, частота и цена соответствовали контракту. А как она вырабатывается или передается, вас не интересует. Другой подобный пример – услуги связи.

Облачные решения и виртуализация поднимают управляемые услуги на новый уровень, на котором практически всё, что ранее поставлялось в виде программного обеспечения или «железа», делается доступным в виде услуги. Вместе с тем управляемые услуги могут быть и вполне материальными, скажем, предоставление в аренду сотовых вышек или инфраструктуры дата-центра (см. рисунок). И, кроме того, услуги могут комбинироваться произвольным образом.

Становиться партнером или нет?

Существует много причин, по которым вы можете предпочесть управляемые услуги предоставлению конкретного компонента самостоятельно. Например, это может позволить вам сосредоточиться на своем основном бизнесе или дать доступ к новым знаниям, талантам или эксплуатационной экспертизе. Это также может подстегнуть изменения, направляя инновации, помогая реструктурировать статьи затрат, повысить качество, ускорить вывод услуг на рынок или обеспечить лучшее управление рисками.

Но использование управляемых услуг как способа быстро избавиться от проблем – идея в общем случае не очень хорошая. То, что вы передоверили ту или иную функцию кому-то другому, не означает, что вы больше не несете ответственности за ее предоставление. Если вы построили свою услугу поверх сервисов, обеспечиваемых партнерами, то при возникновении проблем пострадают ваша абонентская база и ваш бренд.

Другой неподходящий мотив для использования управляемых услуг – желание просто сократить затра-

Игроки рынка управляемых услуг

ты: если это возможно, то все в порядке, но обычно минимальные затраты означают и минимальное качество и минимальную гибкость. Вы должны рассматривать партнеров так же, как любую другую критичную часть своей модели доставки услуг, поскольку они таковой и являются. Вашими приоритетами должны быть получение конкурентных преимуществ, повышение уровня восприятия клиента, увеличение гибкости, непрерывности и операционной эффективности бизнеса.

Как определить правильное место партнеров в стратегии?

Использование управляемых услуг – серьезное стратегическое решение, почти столь же серьезное, как если бы речь шла о неотъемлемой части вашей собственной системы доставки услуг клиентам. Переход к управляемым услугам фундаментальным образом изменит вашу бизнес-модель, а также организацию и управление операционной деятельностью. К сожалению, слишком часто руководители допускают, чтобы такой переход произошел на тактическом уровне, тогда как управляемые услуги должны быть глубоко интегрированы в корпоративную стратегию. Причем при создании этой стратегии нужно руководствоваться ответами на следующие вопросы:

- **Почему** в компании рассматривается вопрос привлечения партнера по управляемым услугам? Обозначьте проблему.
- **Какой** бизнес-результат ожидается от управляемых услуг? Каковы цели?
- **Кто** будет обеспечивать предоставление услуг? Какие услуги останутся внутри компании, а какие будут делегированы и кому?
- **Кто** будет нести ответственность за сквозное предоставление услуги и как технически будет реализован контроль за обеспечением доступности услуги?
- **Как** управляемая услуга должна предоставляться, чтобы обеспечить ее максимальную ценность?
- **Где** будет исполняться управляемая услуга? Как предоставление услуги должно быть распределено и каковы будут последствия?

Если обслуживание клиентов будет частично зависеть от партнеров, то лучше предварительно проработать базовые вопросы бизнеса, связанные с такого рода обслуживанием, чем обнаружить, что подразделения, ответственные за разные части процесса предоставления услуги, уже согласовали множество контрактов с различными уровнями обслуживания, сроками действия и другими условиями. Такой подход порождает операционный и организационный хаос, что случается часто, когда структурные единицы действуют самостоятельно.

Все подразделения должны точно понимать, какое место они занимают в цепочке предоставления сквозной услуги, и добиваться того, чтобы обязательства перед конечным пользователем были выполнены. Важно, чтобы договоры об управляемых услугах были частью общего взгляда на предоставляемую сквозную услугу, а не ворохом нестыкующихся друг с другом соглашений, которые дорого менять и из которых трудно выйти.

Распределенная ответственность и доверие

Одним из важнейших условий успешного использования партнеров является доверие. При отсутствии полного доверия компании часто не решаются передать управление поставщику управляемых услуг и не предо-

ставляют ему необходимую информацию, которая позволила бы успешно справиться с задачей. В результате возникает порочный круг, в котором поставщик управляемых услуг не может функционировать достаточно хорошо, что еще больше подрывает доверие к нему. Это особенно часто встречается в ситуациях, когда поставщик управляемых услуг берет на себя функции, которые ранее выполнялись внутри компании и в отношении которых существует стойкое предубеждение, что «никто не сможет сделать эту работу лучше нас». Держа поставщика управляемых услуг на «голодном пайке», когда дело касается важной информации или совета, и относясь критически к любой возникающей проблеме, компания может запустить процесс разрушения партнерства на самых ранних этапах его формирования.

Построение делового сотрудничества немного напоминает женитьбу: чтобы создать устойчивое партнерство, основанное на доверии, нужно в первую очередь выбрать подходящего партнера. Для обеих сторон всегда полезно как можно больше знать друг о друге. Это предполагает глубокую, всестороннюю оценку предполагаемого партнера, включая анализ присутствующих рисков: каковы организационная структура, финансовое положение, профессиональный опыт, культура, бизнес-цели и т.д. В таком анализе не следует проявлять поспешность, старая пословица «женился на скорую руку, да на долгую муку» в той же мере справедлива в деловом сотрудничестве, как и в личной жизни.

Определение требований к услуге и показателей качества, которые поставщик должен обеспечить, представляет собой сложную, но важную задачу. Слишком многие договоры фокусируются на показателях, которые ранее использовались внутри компании, вместо того чтобы сделать акцент на целях, которые обеспечат полезный бизнес-эффект. Покупатель должен сосредоточить свое внимание на том, что он хочет получить, и предоставить возможность партнеру самому решить, как он этого достигнет.

■ ■ ■

Нравится это вам или нет, но цифровой мир быстро становится сложной сетью партнерских отношений, и настоящего успеха добьются те игроки, которые, помимо всего прочего, действительно знают, как извлечь максимум выгоды из партнерских связей. Старый подход «хозяин-слуга», подразумевающий готовность сделать из партнера отбивную ради получения наилучших условий и цены, в долгосрочной перспективе не будет работать на фоне конкурентов, которые строят надежные и длительные партнерские отношения, основанные на взаимной выгоде.

Чтобы овладеть такими навыками, крупным организациям понадобится время. Рано или поздно делать это придется, поэтому лучше всего начать учиться прямо сейчас! ИКС

Редакция благодарит сотрудников компании «Техносерв Консалтинг» за помощь в подготовке публикации.

Базовые правила успешного взаимодействия с партнерами

Надо

Сфокусироваться на том, ЧТО вы делаете, а не на том, КАК. Не нужно рассказывать партнеру, как следует предоставлять необходимую вам услугу, – в конечном счете, это его базовая компетенция. Лучше сосредоточиться на том, что вы хотите получить, включая доступность, надежность, генерацию доходов и удовлетворенность клиентов.

Использовать правильные мотивацию и управление, чтобы добиться нужного поведения всех вовлеченных лиц. Структура управления должна быть ориентирована не только на общие задачи, но и на суть происходящего. Она должна обеспечивать решение проблем в духе партнерства.

Удостовериться в том, что у вас есть гарантии и заинтересованность высшего руководства в организации партнерства.

Ожидать сопротивления. Всегда найдется кто-то, кто думает, что сможет выполнить функцию внутри компании лучше, чем партнер. В конце концов, это может быть его работой.

Регулярно перепроверять условия договора, чтобы быть уверенным, что ценности и ресурсы продолжают соответствовать вашим бизнес-задачам. Если что-то не работает, найдите способ это исправить вне зависимости от сложности проблемы.

Убедиться в том, что со стороны партнера задействованы ключевые сотрудники и обеспечить участие сотрудников с ключевыми компетенциями и со стороны вашей компании, чтобы правильно управлять партнерским взаимодействием и при необходимости иметь возможность вернуть функцию обратно в компанию.

Использовать стандартизованные бизнес-процессы и интерфейсы между вами и партнером. Это сэкономит вам время, деньги, усилия и ресурсы, необходимые для интеграции и последующего тестирования. Кроме того, если произойдет худшее и вам придется сменить партнера, то сделать это будет значительно проще.

Убедиться в том, что условия партнерского договора достаточно гибкие для того, чтобы быстро следовать за изменениями рынка. Иначе при повторном согласовании условий договора ожидаемая выгода может исчезнуть.

Всегда помнить о восприятии клиентов – и не жертвовать им ни при каких обстоятельствах, так как в долгосрочной перспективе подобный подход дорого вам обойдется.

Не надо

Придерживаться подхода «копейку сэкономлю, рубль потеряю». Когда компания выбирает партнера исключительно по соображениям цены, это может привести к проигрышу в качестве и уровне обслуживания.

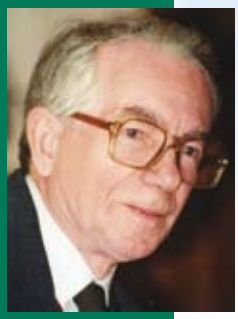
Использовать управляемые услуги в качестве «быстрой затычки» для решения своих проблем. Управляемые услуги должны обеспечивать ценности для клиентов и бизнеса, а не служить быстрым решением каких-либо бизнес-проблем.

Разменяться на мелочи. Сосредоточьтесь на нескольких по-настоящему важных бизнес-целях.

Играть в игру с ничейным результатом. Другими словами, не следует полагать, что все, что хорошо для партнера, автоматически плохо для покупающей стороны. Ищите пути, которые позволят обеим сторонам выиграть от любого улучшения.

Луч света в царстве DRM

Осуществление мечты о цифровом радиовещании на частотах ниже 30 МГц, скорее всего, реально. Но непонятно, почему при очевидных своих преимуществах DRM так медленно продвигается в жизнь.



Юрий ЧЕРНОВ,
докт. техн. наук

Помнится, как на заре DRM (везде далее имеется в виду DRM30, без расширения DRM+), еще в 2000-х, громко звучали лозунги: «Завтра все будем оцифрованы и заживем в новом мире – мире непрерывного сладкозвучия». Но прошло время, и всплыла в памяти народная мудрость-предупреждение: «Не говори гоп, пока не перепрыгнешь». Природа много сложнее наших простых представлений о ней, и всё важное узнать и учесть сразу не представляется возможным. Среди технических специалистов, имеющих дело с трудно продвигающимися разработками, давно родилось яркое выражение: «В принципе работает, а в натуре – нет». С DRM все происходит по классической схеме: есть и «гоп», есть и «в принципе работает». Уже больше 12 лет в разных странах проводятся испытания, многие специалисты не высказывают серьезных замечаний, хотя в ряде случаев отмечают недостаточный уровень напряженности поля. Однако пока ни одна страна не вводит у себя новую систему вещания в полном объеме.

Да и сам Консорциум DRM в опубликованном в апреле 2013 г. документе «Прогресс во внедрении системы DRM для перехода к цифровому звуковому радиовещанию» заявил: «С переходом к цифровому телевидению, в настоящее время хорошо продвинутому, уместно рассмотреть еще раз, почему низок стимул со стороны части администраций связи или запросов от слушателей осуществить полный переход к цифровому звуковому радиовещанию». К сожалению, дальше постановки вопроса дело не пошло. Повторение известных лозунгов о пользе DRM и отсутствие анализа причин «низкого стимула» к переходу на цифровой формат и заставило автора взяться за написание предлагаемой статьи.

Почему пробуксовывает DRM?

Причин видится несколько – технических, организационных, финансовых и психологических.

Организация радиовещания в СВ/ДВ-диапазонах – это прежде всего планирование. Для планирования важен целый ряд параметров, главные из которых – защитные отношения и минимальная (или достаточная) напряженность поля. В предыдущих публикациях* эти вопросы не раз обсуждались на базе экспериментальных данных, полученных за рубежом. Вместе с очевидными достоинствами цифровой системы отмечались и не до конца ясные моменты на пути ее внедрения в районах со сложными климатическими условиями. При вещании на коротких волнах не менее важна и возможность адаптации слушателей к прерывистой передаче в условиях недостаточного уровня сигнала или в сложной ионосферной обстановке. Есть в планировании и глобальные вопросы, ответы на которые еще не найдены.

Между тем пропущено уже два срока пересмотра созданного в 1975 г. Плана радиовещания на длинных и средних волнах для регионов 1 и 3 (GE75). Появление цифровой системы еще более осложнило положение. Как изменятся зоны обслуживания после введения новой системы при ее самостоятельной работе или вместе с аналоговой, никому не известно. Для первичной апробации МСЭ-Р разрешил работу цифровой системы с передатчиками, имеющими излучаемую мощность на 7 дБ (не менее 6,6 дБ**) ниже, чем у заменяемого аналогового передатчика. Реальное положе-

*Чернов Ю. Цифровое радио. Плюсы и минусы. «ИКС» № 1–2'2010, с. 55.
Чернов Ю. Где DRM'у жить хорошо. «ИКС» № 3'2010, с. 58.
Чернов Ю. Как внедрять DRM будем? «ИКС» № 3'2011, с. 67.
Чернов Ю. Ионосфера и DRM. Быть ли свадьбе? «ИКС» № 10'2011, с. 53; № 11'2011, с. 65.
Чернов Ю. Всему свое место. DRM'у тоже. «ИКС» № 3'2012, с. 56.
**Письмо МСЭ-Р CCRR/43(Rev.1)-R.

ние дел подробно изучалось в Частотной рабочей группе Комитета по электронной связи (ECC) в рамках Европейской конференции администраций почт и электросвязи (CEPT). Приведем несколько фрагментов из двух документов, выпущенных этой группой по поводу введения и планирования DRM-сетей. Рабочая группа перечисляет целый ряд моментов, вызывающих вопросы. Одни из них вселяют надежду, другие будят тревогу. Документы подготовлены в 2007 г., но принципиальных изменений с тех пор не произошло.

Будет ли новый план?

Сначала прислушаемся к мнению авторов документа «Управление переходом на цифровое звуковое радиовещание в ДВ/СВ-диапазонах»* (курсив мой. – *Прим. авт.*).

1. *«Основополагающей величиной для построения планов радиовещания в НЧ-, СЧ-, УВЧ- и ОВЧ-диапазонах является напряженность поля».*

2. «В первом приближении *для DRM-передачи требуется такая же мощность, как и для боковых полос АМ-сигнала.* Поэтому при отсутствии несущей возникает значительная экономия по мощности».

3. *«Прежде чем будет проведен какой-либо пересмотр плана для внедрения цифрового вещания, необходимо тщательно изучить условия распространения сигнала, различающиеся в светлое и темное время суток.* Это нужно для оценки неблагоприятных воздействий на качество приема цифрового сигнала в тех областях, где радиосигнал распространяется одновременно и земной, и пространственной волной. Для АМ-вещания этот эффект проявляется в виде замираний, которые образуются в зоне, где земная и пространственная волны накладываются друг на друга и уровень сигнала непрерывно изменяется от очень низкого до более высокого (квакающего звука), хотя содержание радиопрограммы остается понятным. Для DRM-вещания эффект проявляется в резком исчезновении слышимости, когда приходящий сигнал изменяется от хорошего до почти полностью исчезающего, что хуже, чем в АМ-вещании».

4. «Пространственная волна, имеющая место в темное время суток, в сочетании с высокой мощностью радиовещательных станций дает возможность охватывать вещанием огромные территории. Именно это обстоятельство превратило бы созыв любой конференции для пересмотра Плана GE75 в монументальную задачу, сопоставимую по масштабу с региональной радиоконференцией RRC06, но с по крайней мере вдесятеро большими диапазонами координации и числом стран, от которых *потребуется одобрение увеличения числа передатчиков большой мощности.* Это очень трудоемкое и дорогостоящее мероприятие…».

5. *«Перепланирование сетей в ДВ/СВ-диапазонах на предстоящей конференции потребовало бы дополнительного времени и дополнительных ресурсов.* Кроме того, у радиовещателей есть сомнения в благоприятном разрешении этого вопроса, и все вместе вызывает нежелание подвергаться такому риску. Проектирование и строительство ДВ/СВ-передающих станций требуют больших финансовых вложений и проведения более серьезных мероприятий в решении вопросов здравоохранения и безопасности для населения, чем для радиостанций ЧМ ОВЧ».

Теперь обратимся к документу «Возможные технические и регулирующие мероприятия для облегчения внедрения DRM-излучения в радиовещательных ДВ/СВ-диапазонах в Регионах 1 и 3»**.

6. «В документе МСЭ-Р Рек. BS.1615 "Параметры планирования" приводятся основные данные для определения всех параметров планирования для цифрового звукового (DRM) радиовещания, передающего на частотах ниже 30 МГц… Выбор значений параметров …*частично базируется на теории и нуждается в проверке на практике в рамках Плана GE75.*

…Поэтому в течение двух-пяти лет, к тому моменту, когда ожидается значительное увеличение количества DRM-передатчиков, необходимо провести практические измерения, чтобы подтвердить возможность совмещения…».

7. «…Пересмотр заключительных актов Региональной конференции по радиовещанию 1975 г. может быть согласован только через созыв очередной региональной конференции. Хотя требуемые изменения существенны, они не должны затронуть частотные присвоения в Плане GE75. Поэтому эти изменения, вероятно, можно согласовать на специальной региональной конференции, нацеленной только на пересмотр технических параметров и связанных с ними процедур. *Однако до проведения такой конференции необходимо в течение нескольких лет накапливать информацию для оценки качества DRM-передач на потребительских приемниках.* Эта информация требуется, чтобы подтвердить или улучшить параметры планирования, содержащиеся в рекомендациях МСЭ».

8. *«С учетом всего вышесказанного вывод об отсутствии необходимости замены частотного Плана GE75 на предполагаемой конференции в настоящее время или в обозримом будущем представляется разумным и прагматичным.* Этот вопрос, как уже отмечалось, должен быть повторно поднят позже и с большим пониманием такого требования».

Сделаем небольшие пояснения. В п. 1 подчеркивается ключевая роль напряженности поля, поскольку именно она определяет необходимую мощность передатчика и стоимость его работы. При этом отношение сигнал/помеха является лишь важным технологическим параметром. Использовать его в качестве основного фактора планирования затруднительно вследствие большой непредсказуемости суммарного уровня помех и шумов. Из п. 2 следует, что если использовать аналоговую систему без несущей с одной боковой полосой (ОБП), как предполагалось в МСЭ несколько ранее, то аналог и цифра становятся энергетически эквивалентными. В п. 7 специально отмечено, что говорить о параметрах планирования следует после апробации

*Doc. CEPT FM PT45(07)039.

**Doc. CEPT FM PT45(07)038.

системы на потребительских приемниках. Но тестирование работы DRM в большинстве случаев проводится на профессиональных приемниках и почти всегда в открытой местности, что не дает правильной картины приема вещания в бытовых условиях.

В целом же и без комментариев понятно, почему через процитированные документы красной нитью проходит нежелательность, преждевременность и нецелесообразность перепланирования сети для перехода на цифровую систему. Иными словами, учитывая все рассмотренное, CEPT не видит возможности в обозримом будущем составить в мировом масштабе работоспособный план работы цифровой сети. Здесь сказывается и то, что многие мощные передающие радиоцентры представляют собой достаточно крупные населенные пункты, которые невозможно, как телевизионные передатчики, при необходимости переместить на другое место.

Врастание DRM в социальную и информационную среду путем последовательных проб видится теперь достаточно долгим. Поскольку соответствующая конференция не планируется и обязательного глобального перехода, как в телевидении, не предписано, то внедрение DRM пущено на самотек. При этом администрация связи в каждой стране сама решает, что ей больше подходит.

Неясная перспектива развития мировой сети вещания как единого целого с привнесением в нее цифровой системы (все станции связаны взаимными помехами, особенно в темное время суток через ионосферу) является, на взгляд автора, **одной из причин пробуксовки DRM** и неготовности вещателей вкладывать средства в новую систему. В CEPT, как можно было убедиться, отчетливо понимают сложность внедрения DRM в существующую мировую сеть, и вряд ли можно лучше, чем они, сформулировать суть стоящих проблем. Рабочая группа, подготовившая рассмотренные документы, описала в них причины медленного развития событий и по существу предсказала пробуксовку.

Почему на цифровое ТВ и DRM+ смотрят, а на DRM30 – нет?

Одновременно с DRM началось развитие цифрового вещания в метровом и более высокочастотных диапазонах и цифрового телевидения. С точки зрения технических условий планирования названные системы имеют по сравнению с DRM целый ряд преимуществ:

- Передатчики в сетях УКВ-радиовещания и ЦТВ на порядок компактнее и легче, проще устанавливаются, не требуют специальных мощных подводов электроэнергии, устройств охлаждения и т.п. Это связано с ограниченным радиусом их полезных зон, практически не превышающим расстояния прямой видимости (при высоко поднятых антеннах – до 50–70 км).
- Введение цифровых систем в сетях УКВ РВ и ЦТВ кроме повышения стабильности звукового или телевизионного сигнала позволяет многократно увеличить число передаваемых программ, что не только обеспечивает значительную экономическую выгоду, но и существенно расширяет сферу информационных и развлекательных услуг.
- Передатчики этих сетей мобильны, не требуют высоких дорогих антенн, во многих случаях могут работать без постоянного присутствия персонала.
- На ультракоротких волнах сигналы на расстоянии прямой видимости практически не имеют замираний. Поэтому вопрос о запасе мощности на замирания во времени остро не стоит.
- Каждый УКВ-передатчик является самостоятельной единицей, ни от кого не зависящей (кроме приграничной полосы), не связанной с другими мировыми территориями. На больших расстояниях он никому не мешает.

Один из ключевых факторов, из-за которого в телевидении все безоговорочно перешли на цифру, – это практическая независимость зоны хорошей работы сети от природных условий. Главный параметр – дальность радиогоризонта. За этой границей, как для аналогового сигнала, так и для цифрового, во всех странах возможность приема падает почти одинаково круто. Проверив систему на одной территории и убедившись, что все работает, как ожидалось, можно переносить опыт и на другие страны.

Когда в процессе внедрения находятся две системы, в нашем случае DRM и цифровое ТВ, то мы невольно их сравниваем. Происходит неизбежная умственная работа, незаметно подводящая нас к внутреннему выбору. Это связано с психологическими законами оценивания. Сравнивая аргументы за цифровое ТВ и DRM+ с аргументами за DRM30, мы видим, что в ДВ- и СВ-диапазонах ситуация совершенно иная. Есть страны, где весь год сохраняется одинаковый зеленый покров, температура почти постоянная, уровень сигнала в дневное время стабилен*. В таких условиях, подобрав один раз параметры сети, можно быть уверенным, что сеть будет работать без сбоев. В других странах, преимущественно в средних и высоких широтах, положение намного сложнее. В изменяющихся природных условиях поведение аналогового и цифрового сигналов заметно различается. Без долговременного опыта работы с цифровой системой, охватывающего все природные колебания, как сезонные, так и спонтанные, администрациям связи с большим числом мощных передатчиков трудно решиться на крупномасштабную и дорогостоящую модернизацию сети, не имея уверенности, что она не окажется убыточной. Заметно увеличить число каналов в СВ-диапазоне с DRM не удастся. Еще менее ясен вопрос о работе цифровой сети в темное время суток при наличии взаимных помех по ионосферным каналам. Об

*Чернов. Ю. Где DRM'у жить хорошо. «ИКС» № 3'2010, с. 58.

этом же в проанализированных выше документах говорит и CEPT.

Таким образом, по сравнению с сетями УКВ- и ТВ-вещания сети с DRM на частотах ниже 30 МГц куда менее привлекательны. Более того, сегодня стандарт DRM требует модернизации для улучшения его защитных и энергетических характеристик, как было сделано, в частности, в телевидении. Все это наводит на мысль, что DRM-вещание будет значительно менее эффективно, чем цифровое ТВ или DRM+. И именно в этом, по-видимому, коренится **вторая причина пробуксовки.**

Непрезентабельная презентация

Можно с большой уверенностью утверждать, что главная, хотя и неосознанная, ошибка при внедрении DRM состоит в том, что для демонстрации преимуществ цифры перед аналогом были выбраны короткие волны. DRM вообще первоначально рассматривался как спасительное средство именно для коротких волн, и только в следующую очередь – для СВ- и ДВ-диапазонов. Кроме того, легче всего поддаются переоборудованию КВ-передатчики относительно небольшой мощности (до 100 кВт). Другой мотив выбора коротких волн заключается в том, что КВ-вещание охватывает практически весь мир, и это дает возможность познакомить с достоинствами новой системы в сотни раз больше слушателей и потенциальных вещателей, чем в диапазонах СВ и ДВ. Так или иначе, но мировое радиовещание начало пробовать цифру именно на коротких волнах, и по сию пору подавляющее большинство станций, работающих с DRM, коротковолновые.

Однако поведение сигналов в КВ-диапазоне намного более сложное и непредсказуемое, чем на длинных и средних волнах. В этом диапазоне очень трудно добиться высокой надежности работы канала. Но вещание – это прежде всего расписание. Если работа по расписанию обеспечена быть не может и перерывы в приеме попадают то на новости, то на спорт и т.п., это уже не вещание. Наиболее близка к такому неустойчивому состоянию работа ионосферных каналов, т.е. именно в КВ-диапазоне. Практика его использования почти за 100 лет показывает, что в КВ-диапазоне даже в наиболее спокойных средних широтах достичь надежности выше 80% в течение продолжительного периода времени (например, сезона) при типичных мощностях передатчиков чрезвычайно сложно. Такое возможно, только если во время работы канала не будет помех от других станций или затухание на трассе не превысит допустимых значений. Ни то ни другое гарантировать нельзя. А на широтах, близких к 60° или выше, положение гораздо сложнее. Здесь, и это подробно рассмотрено во многих публикациях, понятию работы по расписанию трудно придать практический смысл.

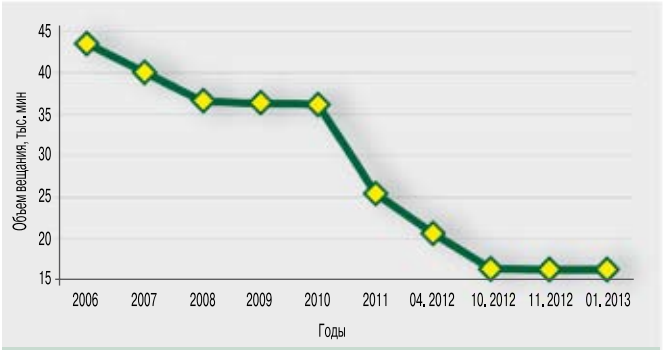
Можно предположить, что часть слушателей КВ-передач, столкнувшись с непостоянством приема на коротких волнах, не поверила во всемогущество DRM. О низком проценте приема DRM на КВ свидетельствуют многочисленные сообщения в интернете*, и это может быть **третьей причиной пробуксовки** внедрения DRM. Если бы авторы DRM предложили слушателям для знакомства с новым стандартом вещания передачи не на КВ, а, например, только на СВ, то активность вещателей и результат могли бы быть совсем другими.

У DRM ниже 30 МГц по сравнению с УКВ-системами есть одно неоспоримое преимущество. Это большая дальность действия: на КВ – практически весь мир, на ДВ и СВ – многие сотни километров. И возможность передавать информацию на большие расстояния из своего собственного центра без переприема и без опасности нарушения канала по чужой воле, что свойственно только вещанию на частотах ниже 30 МГц, всегда будет востребована.

Луч света может появиться уже завтра

Характерным показателем отношения радиовещательного сообщества к развитию цифрового направления в полосах ниже 30 МГц является объем работы мировой сети DRM-станций. На сайте Консорциума DRM (www.drm.org) регулярно публикуются списки радиостанций, заявленных для работы в режиме DRM. За последние пять-семь лет число таких станций, как и время вещания в эфире, вопреки прогнозам CEPT, не только не увеличилось, но существенно уменьшилось. С 2006 г. суммарное время DRM-вещания в мире снизилось в три раза (см. рисунок).

Объем DRM-вещания в мире в 2006–2013 гг.



Источник: по данным www.drm.org

Общее число станций также сократилось (см. таблицу). В частности, в активном 2008 г. работало 44 станции, из них 18 – в диапазонах ДВ и СВ, в КВ-диапазоне – 26 станций, т.е. доля ДВ- и СВ-станций составляла 41%. В 2012 г. число станций уменьшилось в 1,7 раза: всего работало 26 станций, две из них (7,7%) – в ДВ- и СВ-диапазонах, 24 станции – в КВ-диапазоне. Наибольшее число задействованных средств и выходов в эфир наблюдалось в 2008–2009 гг.

*См. www.drm.org/?page_id=151.

Характеристики DRM-вещания в 2006–2013 гг.

Всего заявлено вещания в эфире, мин	2006	2007	2008	2009	2010	2011	04.2012	10.2012	04.2013
	43 491	≈40 000*	36586	≈36 350*	36225	25493	20666	16380	16106
Число центров	38		44						26
Число центров, ДСВ	13		18						2
Число выходов в эфир в сутки, всего	108		122						78
Число выходов в эфир в сутки, КВ	95		102						74
Число выходов в эфир в сутки, ДСВ	21		20						4
Число выходов в эфир в сутки, РФ	12		12						14
Число центров, РФ	1		2						5

*Интерполяция
Источник: по данным www.drm.org

Сегодня в СВ-диапазоне работают два передатчика: один мощностью 0,1 кВт на частоте 909 кГц – в Германии, а второй, на частоте 1080 кГц мощностью 25 кВт – в Индии. В такой ситуации проведение «практических измерений, чтобы подтвердить возможность совмещения» в мировом масштабе, как это предполагалось в цитированном выше документе рабочей группы CEPT, становится проблематичным.

Вместе с тем число стран, работающих с DRM, с 2006 г. не уменьшилось. Всего их 16, хотя состав несколько изменился: одни страны прекратили работу, другие начали пробовать DRM. Наиболее активны в настоящее время администрации связи следующих стран: России – 14 выходов в эфир в сутки, Индии – 11 выходов, Новой Зеландии – восемь выходов, Австралии – семь выходов, Румынии и Испании – по шесть.

Пример самостоятельного решения проблемы «внедрять или не внедрять» подает администрация связи Индии. Страна расположена в регионе, отнесенном к тем, в которых «DRM'у жить хорошо»*. В январе 2013 г. на конференции-выставке Broadcast Engineering Society Expo в Нью-Дели было заявлено, что индийская администрация связи заказала для радиовещания 36 передатчиков с цифровой модуляцией, которые предположительно начнут работать в декабре 2013 г. Предполагается также, что цифровая система будет использоваться в диапазонах FM, СВ и КВ на программах Всеиндийского радио. Прием таких программ планируется осуществлять на мобильные телефоны. Председатель Консорциума DRM Руксандра Обрежа, принимавшая участие в конференции, отметила, что у Индии есть потенциал стать самым большим рынком цифрового радио.

Прием на мобильные телефоны как по качеству, так и по назначению, конечно, отличается от того, что называется радиовещанием, но тем не менее он будет служить дальнейшему накоплению опыта работы с цифровыми вещательными системами. Несколько ранее сообщалось, что для Всеиндийского радио был заказан цифровой СВ-передатчик мощностью 1000 кВт. Важно, что его предполагается использовать в режиме simulcast, т.е. одновременно в режиме АМ на частоте 1071 кГц и DRM на частоте 1080 кГц. Вещание на таких сдвоенных каналах с большой мощностью в рамках существующего плана возможно в исключительных случаях или с много меньшими мощностями, не создающими помех уже работающим станциям.

Если администрации связи Индии удастся осуществить намеченное и добиться хороших результатов, то это станет прорывным событием, которое завтра, возможно, увлечет за собой другие страны данного региона.

Основное блюдо или десерт?

Переходя к странам со сложными природными условиями, можно сказать, что в целом DRM интересен, и было бы желательно и полезно иметь его на подходящих территориях. Но только там, где случаи всегда возможного временного отсутствия приема по причинам ухудшения сигнала не могут привести к нежелательным последствиям. Все-таки пороговый сигнал где-то внезапно исчезает или превращается в отдельные вспышки или фрагменты. Такое уточнение будет необходимо до тех пор, пока деградация сигнала в DRM не приобретет деликатный характер.

Вполне можно допустить, что новый частотный план будет составлен настолько удачно, что граничные территории действия DRM со всеми неприятными сопутствующими пограничными явлениями будут закрыты другими локальными системами с хорошим качеством. Это снимет основную волну возможных претензий. Скорее всего, DRM-вещание будет развиваться наряду с существующим аналоговым (последнее – в экономичном варианте, т.е. с управляемой несущей или, что еще лучше, с ОБП), и это развитие будет напоминать отдельные островки как в масштабе земного шара, так и внутри какой-либо страны. В таком случае можно сказать, что DRM-вещание будет не основным блюдом, а своего рода экзотическим десертом. ИКС

*Чернов. Ю. Где DRM'у жить хорошо. «ИКС» № 3'2010, с. 58.

На смерть приватности

Может быть, приватность еще не совсем умерла, но при смерти точно.

Михаил ЕМЕЛЬЯННИКОВ,
«Емельянников, Попова и партнеры»

21-й век стремительно уничтожает выпестованный столетиями институт приватности сведений о гражданах. Мы наблюдаем фантастическую, разворачивающуюся в реальном времени картину изменения характера, фундаментальных взглядов и менталитета людей под влиянием информационных технологий. Я не социолог, но рискну предположить, что такой резкой смены отношения к собственной жизни в течение столь короткого срока человечество еще не видело. Атака на личную тайну идет одновременно со всех направлений.

Тайна частной жизни атакуется «снизу» – потому что приватность уничтожают сами люди. Стремительное проникновение во все стороны нашей жизни интернета и особенно социальных сетей привело к тому, что пользователи добровольно, без всякого принуждения, стали сообщать огромное количество сведений о себе, своих близких, своей жизни неограниченному кругу лиц. Познакомился, поругался, обручился, женился, заболел, поехал в отпуск – с указанием не только страны, но и конкретного отеля, с какого вокзала, с кем вместе, какую машину арендовал, что съел и выпил (обязательно с фото), и так без конца и ограничений.

Приватность атакуется «сверху». Трещит по всем швам выкованная тысячелетним опытом банковская тайна, причем трещина пошла не от тоталитарных стран, принуждающих граждан к полному повиновению, а от Швейцарии, бывшей эталоном в совсем недалеком прошлом. Капитулировал еще один недавний образец недоступности банковских счетов – Люксембург. К американскому закону о налогообложении иностранных счетов (FATCA) уже присоединились семь государств (три из них подписали, но не ратифицировали соглашение), еще семь – в стадии активных переговоров (из них два – офшорные острова Мэн и Джерси), предварительный диалог ведут 17, изучают варианты заключения 14.

Не отстают и наши законодатели. Вот-вот получат доступ к счетам физических лиц налоговики, а руководитель одного из банковских сообществ и депутат по совместительству внес в Думу законопроект о расширении круга субъектов, которым могут быть предоставлены сведения, составляющие банковскую тайну, чем ошарашил даже правительство.

И, что важно, мы не на финише. Мы в начале процесса.

Боковые атаки на приватность тоже множатся. Знамя запертого в эквадорском посольстве Ассанджа, заварившего эту кашу в мировом масштабе, но пока ограниченного в возможностях, подхватил консорциум журналистов ICIJ, создавший невиданных масштабов базу данных владельцев счетов и фирм в офшорах Offshoreleaks.

Никто не удивляется вываливаемым ежедневно в СМИ и интернет гигабайтам материалов прослушки и электронных писем кого угодно – от политиков до воров в законе (разница есть не всегда) или шоу-звезд и телеведущих. Никто не удивляется и никто, что для меня более странно, не возмущается. А все эти прослушанные-перехваченные продолжают говорить по обычным сотовым телефонам и слать электронные письма через публичные серверы.

Видя такую беспредельную толерантность граждан к нарушению приватности, радостно оживают государственные фискалы и спецслужбы, готовые не только воспользоваться данными, явно слитыми кем-то из их коллег, но и под шумок упростить доступ к переписке и разговорам частных лиц.

Не теряют времени и крупнейшие компании, построившие свой бизнес в мире, где главный источник информации, главное средство коммуникации и главное место покупок и развлечений – интернет. Они настойчиво и, похоже, успешно лоббируют смягчение требований к защите персональных данных в Европе, а пока новые нормы не приняты – строят мощнейшие системы сбора данных о каждом чихе своих клиентов в Сети, научившись по кукам и движению мышки определять возраст, пол и цвет кожи, фиксируя каждый посещенный сайт, каждую покупку и сливая полученные данные рекламным компаниям и продавцам.

Все это – факты, собранные в течение лишь одного месяца аналитиками нашего агентства для ежемесячного обзора.

Такой взгляд на приватность по сути поддерживает значительная часть населения, усилиями которой на повестку дня выдвинут безумный лозунг «Честным людям скрывать нечего». Я много раз его слышал от вполне адекватных, казалось бы, людей.

Мне кажется, эйфория открытости неизбежно пройдет. Человек – животное стадное, но не до такой же степени. И тогда придется думать, что делать в высокотехнологичном мире, просвечивающем людей получше любого рентгена. Многое можно сделать уже сегодня. Но об этом как-нибудь в следующий раз.

ЕЩЕ БОЛЬШЕ НА www iksmedia.ru/blogs

Безопасность в технологической радиосети обмена данными

Радиосети обмена данными УКВ-диапазона – идеальное средство для управления подвижными службами охраны общественного порядка. Одно из ключевых условий использования таких сетей – безопасность передаваемых в них данных.

Сергей МАРГАРЯН, заместитель генерального директора по ИТ и специальным проектам – главный конструктор, НПП «Родник»

Автоматизированные системы оперативно-диспетчерского управления (АСОДУ) предназначаются для планирования, мониторинга работы, управления действиями и информационного обеспечения мобильных подразделений служб безопасности в оперативной зоне. Внедрение и эксплуатация таких систем формируют определенные требования к радиосетям обмена данными, обеспечивающим решение основных функциональных задач АСОДУ, причем значительной их части – в близком к реальному масштабе времени.

Наиболее полно предъявляемым требованиям удовлетворяют технологические радиосети обмена данными УКВ-диапазона. Такая сеть не требует развертывания сложной технической инфраструктуры и способна функционировать с использованием имеющегося радиочастотного ресурса. Она может также использоваться в составе систем дистанционного управления техническими средствами, сбора данных, идентификации и контроля, обеспечивая их быстрый монтаж на объекте и оперативное перемещение в другой район в случае изменения задачи.

Возможности технологической радиосети обмена данными УКВ-диапазона расширяют оперативно-технические параметры информационной системы МВД РФ и существенно дополняют функциональность современных голосовых радиосетей, включая цифровые транковые радиосети стандартов APCO25 или TETRA, в части обмена данными с подвижными объектами.

Отметим, что сопряжение с современными автоматизированными системами управления других министерств и ведомств, использующими радиосети обмена данными с подвижными объектами, позволяет решать комплекс технически сложных задач, связанных с управлением и обеспечением безопасности дорожного движения в крупных населенных пунктах и на междугородных трассах. Актуальность этого возрастает в период проведения массовых мероприятий, таких как Универсиада-2013 в Казани и Олимпиада-2014 в Сочи.

Архитектура и свойства сети

Архитектурно технологическая радиосеть обмена данными представляет собой группу базовых станций, установленных таким образом, чтобы охватить всю оперативную зону в территориальном образовании с учетом плотности размещения пользователей в населенных пунктах и на междугородных магистралях. Каждая базовая станция обслуживает группу подвижных объектов в закрепленной зоне, обеспечивая двусторонний обмен данными. Все базовые станции сопряжены с центральным компьютером, который также выполняет функции коммутации сообщений, передаваемых в радиосети, обеспечивая их автоматическое доведение до адресатов.

Работа в составе радиосети происходит по IP-протоколу, оптимизированному для обслуживания подразделений служб общественной безопасности и предусматривающему автоматическую передачу данных о местоположении подвижных объектов при каждом сеансе связи. Радиосеть обеспечивает двусторонний обмен данными между стационарными пунктами управления и подвижными объектами (одним, группой или одновременно всеми), что позволяет организовать автоматизированное управление с гарантированным доведением команд диспетчера до подвижных средств и докладов с подвижных средств – до соответствующих должностных лиц. Каждое сообщение в системе отправ-

> Для управления органами внутренних дел Российской Федерации создается ведомственная система связи и передачи данных, в том числе и защищенная, являющаяся составной частью интегрированной государственной системы связи России и состоящая из стационарных и подвижных узлов связи территориальных органов внутренних дел – пунктов управления, каналов и линий связи между пунктами управления, линий привязки узлов связи пунктов управления к стационарным узлам связи общегосударственной сети связи.
>
> *Из инструктивного доклада заместителя начальника Главного штаба – начальника Управления связи и автоматизации МВД РФ на Всероссийском совещании-семинаре начальников штабов МВД, ГУВД, УВД, УВДТ, УВД УРО «Задачи штабов по организации ведомственной системы связи, сети передачи данных, автоматизации органов внутренних дел и пути их решения»*

ляется строго по заданному адресу и не может быть получено и использовано абонентом, не имеющим прав доступа к нему. Весь обмен данными автоматически контролируется центром коммутации сообщений.

Безопасность данных в стационарных и подвижных технологических радиосетях является одним из ключевых условий их применения, при строительстве таких радиосетей учитывается необходимость полностью исключить или максимально затруднить компрометацию передаваемой по ним информации. Степень защиты данных оказывает непосредственное влияние на надежность радиосети и ее живучесть.

Отметим, что вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления выходят за рамки данной статьи.

Что может технологическая радиосеть

В одном радиоканале УКВ-диапазона можно организовать прием через каждую базовую станцию сообщений от 300 и более подвижных объектов с периодичностью обновления навигационных данных о каждом объекте раз в минуту. Сообщение объемом в страницу машинописного текста в адрес группы из 300 подвижных объектов может быть доведено в течение доли секунды и подтверждено в течение минуты.

Устойчивость к перехвату данных

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако задача не так сложна для специалиста, имеющего соответствующую подготовку (подтверждение этому – многочисленные успешные атаки хакеров на информационные системы ведомств и организаций). Кабельная сеть прокладывается внутри здания или комплекса зданий; отдельные ее сегменты укладываются в подвалах зданий, коллекторах, потернах и т.п., которые службами безопасности не контролируются и представляют собой потенциальные точки несанкционированного подключения. Теоретически любой человек, знающий структуру кабельной системы, может получить доступ к ней в этих точках. После подключения к проводной системе связи доступ к информации – дело техники, поскольку во всех открытых проводных сетях используются стандартные протоколы связи и обмена данными, серийно выпускаемые и общедоступные программно-технические средства.

Средой передачи данных в стационарных и подвижных радиосетях служат радиоволны, которые принимает любой приемник на относительно большом расстоянии от передатчика. Однако радиосигналы, передаваемые в радиосетях обмена данными с использованием современного радиотехнического оборудования, не так доступны, как кажется на первый взгляд.

Во-первых, для организации перехвата необходимо точно знать номинал рабочей частоты обмена данными. При соблюдении пользователями минимальных правил безопасности получение этой информации крайне затруднено. Поскольку передаваемые данные не воспринимаются на слух, при определении номинала рабочей частоты с помощью доступных средств перехвата, например частотных сканеров, фиксируется только факт передачи сигналов на определенной частоте, а сами сигналы представляются как набор шумов. Установление принадлежности этих сигналов тому объекту, поиск которого ведется, без доступа к передаваемой информации практически невозможно.

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это приводит к тому, что невозможно получить доступ собственно к передаваемой информации в отсутствие соответствующего приемного оборудования или специальных приборов для анализа сигналов. Распространение радиотехнического оборудования, в отличие от проводных средств связи, имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального приобретения оборудования, которое можно использовать для доступа к передаваемой в технологических радиосетях информации, практически равна нулю.

В-третьих, в большинстве радиосетей, особенно имеющих топологию «звезда», в которых обмен данными происходит через базовую станцию, в отдельно взятой точке могут приниматься только данные, передаваемые в одном направлении (от базовой станции к удаленному объекту). Это связано с принципами построения сети, в которой базовая станция разворачивается на возвышенности и имеет высоко подвешенную приемо-передающую антенну, что обеспечивает ей связь со всеми удаленными станциями сети, в то время как удаленные объекты такой возможности не имеют. Для организации перехвата оборудование необходимо разместить на столь же выгодной позиции, что в большинстве случаев невозможно. При другом размещении удается получить только данные от базовой станции, которые в большинстве стационарных технологических радиосетей представляют наименьший интерес с точки зрения перехвата (это, например, запросы, которые дают минимальное представление о работе информационной системы).

Наконец, в отличие от проводных сетей обмена данными, где кабельная инфраструктура и аппаратура для ретрансляции сигналов распределены на больших территориях, радиооборудование передачи данных может быть полностью развернуто в охраняемых помещениях, со строго ограниченным физическим доступом.

Совокупность перечисленных качеств делает стационарные и подвижные технологические радиосети обмена данными более безопасными в части перехвата информации по сравнению с проводными сетями связи и обмена данными.

Устойчивость к несанкционированному подключению

При подключении к сети обмена данными цель обычно состоит в том, чтобы получить доступ для работы в составе информационной системы или просмотра передаваемых данных. Для этого требуется терминал, поддерживающий используемые в сети обме-

на данными протоколы. Такой терминал легко реализовать на базе современного компьютера, но решить вторую часть задачи не столь просто.

Трудности, возникающие при организации перехвата, имеют место и при попытке получить доступ к работе в составе сетей обмена данными, как радио-, так и проводных.

Часть технологических радиосетей (в первую очередь стационарных) использует протоколы опроса, в которых заложены определенные возможности обеспечения безопасности. Чтобы терминал пользователя распознавался информационной системой, он должен быть внесен в «опросную таблицу», которая ведется и поддерживается на центральном компьютере. Несмотря на то что система способна самостоятельно распознавать новые терминалы и автоматически вносить их в таблицу, содержание таблицы постоянно контролируется администратором сети, который может локализовать нового пользователя, получившего доступ к сети, и принять меры, исключающие возможность его работы в составе информационной системы. Если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Значительная часть технологических радиосетей используется для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых терминалов вообще не предусматривается.

Не исключено, что профессиональный крэкер* или хакер сможет перепрограммировать компьютер таким образом, чтобы получать данные без внесения дополнительного адреса в опросную таблицу, однако в этом случае он не сможет передавать свои данные в центральный компьютер (а это в большинстве случаев и является основной целью).

Попытки работы через технологическую радиосеть обмена данными под прикрытием другого терминала путем дублирования его идентификационного номера приводят к генерации некорректных данных и подтверждений, получаемых центральным компьютером. Этот факт незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа и принять соответствующие меры для установления контроля за работой или предотвращения доступа к информационной системе. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает дальнейшие действия взломщика бессмысленными.

На практике выявить и локализовать несанкционированную работу в технологической радиосети обмена данными намного проще, чем в проводной системе связи. Если крэкеру или хакеру предоставляется возможность продолжать контролируемую работу в сети, излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приема сообщений легко запеленговать (а поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и воздействию помех

Подавление или намеренная постановка помех работе радиосети – задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства технологических радиосетей это маловероятно.

Подверженность радиосигналов воздействию помех и возможность их подавления – непреложный факт. Однако для решения этой задачи необходимо знать номинал рабочей частоты радиосети обмена данными, установить который не так просто, поскольку передача ведется короткими сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, в том числе при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра.

Поэтому на практике гораздо проще незаметно перекусить кусачками пару проводов, чем поставить помеху радиосистеме, используя сложное и дорогостоящее специализированное оборудование и серьезно рискуя быть при этом пойманным. Работа кусачками займет не более 30 секунд, а установка специального оборудования радиопротиводействия потребует времени и крупных финансовых затрат, но при этом его воздействие не может быть продолжительным.

Что может технологическая радиосеть

Наличие радиоканала обмена данными с адекватной пропускной способностью позволяет применять АСОДУ на подвижных объектах: например, комплекс «Сова» может использоваться в движении на борту патрульного автомобиля, обеспечивая выборочную проверку транспортных средств непосредственно в потоке транспорта, без их остановки.

Безопасность работы подвижных технологических радиосетей

Подвижные технологические радиосети обмена данными подвержены всем описанным выше угрозам, однако опасность таких угроз существенно больше, поскольку удаленные объекты постоянно перемещаются, и их контроль оказывается более сложным по сравнению со стационарными радиосетями, а количество одновременно работающих в составе подвижной радиосети пользователей динамически изменяется. В подвижных радиосетях более высока угроза утраты радиотехнического оборудования и его использования для несанкционированного доступа в радиосеть.

* Крэкер (от англ. cracker) – взламывает системы защиты информационных систем или создает программные средства для такого взлома. В абсолютном большинстве случаев крэкер не располагает исходным кодом программы, поэтому изучает ее связкой дизассемблера и отладчика с применением специальных утилит.

Исходя из практического опыта эксплуатации подвижных радиосетей обмена данными служб общественной безопасности, рассмотрим угрозы на примере двух наиболее типичных ситуаций: целенаправленный перехват сообщений или угон служебного автомобиля, оснащенного бортовым радиотехническим оборудованием для работы в составе радиосети. Напомним здесь, что в современных подвижных технологических радиосетях используется схема централизованного управления, а все данные передаются через базовые станции. В них применяется асимметричная схема адресации, т. е. аппаратура базовой станции и подвижного объекта ведут себя по-разному, а сообщения, передаваемые в эфир одним подвижным объектом, не могут приниматься и использоваться другим без «разрешения» базовой станции. Таким образом, архитектура подвижной технологической радиосети обладает определенными свойствами, повышающими ее надежность и живучесть в условиях внешних воздействий.

Целенаправленный перехват

Организация перехвата сообщений в подвижной радиосети, использующей современные протоколы обмена, в которых возможна инициализация работы по инициативе подвижного объекта, связана с теми же трудностями, что и в радиосетях, применяющих более простые протоколы «опроса». Дополнительные трудности для перехвата создаются за счет наличия уникальных адресов, которые «прошиваются» в радиотехническую аппаратуру в заводских условиях и не могут быть изменены пользователем. Каждое устройство связи (радиомодем) для подвижного объекта имеет несколько адресов (индивидуальный, групповой и циркулярный). Все сообщения, за исключением циркулярных, направляются в адрес строго определенного пользователя и не могут приниматься другим радиомодемом, работающим в составе радиосети.

Таким образом, даже при наличии не зарегистрированного в радиосети комплекта бортового радиотехнического оборудования можно получить доступ только к циркулярным сообщениям, транслируемым базовой станцией. Комплект базового оборудования теоретически позволяет принимать адресованные базовой станции сообщения. Однако для этого необходимо изменить адрес базового радиомодема на адрес радиомодема, реально используемого в составе радиосети, и развернуть оборудование в точке, обеспечивающей прием сообщений от всех или значительной части подвижных объектов, работающих в достаточно большой зоне. Но даже в этом случае эффект от перехвата данных будет весьма мал, поскольку основную оперативную ценность в значительной части современных подвижных технологических радиосетей представляют исходящие данные (управляющие сигналы, команды, распоряжения, результаты обработки обращений к базам данных и т.д.), передаваемые базовой станцией в адрес мобильных пользователей.

Дополнительная безопасность данных обеспечивается применяемыми в аппаратуре для подвижных радиосетей обмена данными методами и средствами, включая парольную защиту. И хотя такое препятствие не может рассматриваться как серьезное для специалиста, оно достаточно надежно страхует от «случайного доступа» к данным. Обеспечение более высокого уровня безопасности информации достигается за счет применения штатной аппаратуры шифрования.

Угон служебного автомобиля с подключенным к радиосети радиотехническим оборудованием

В случае угона служебного автомобиля при включении установленного в нем оборудования невозможно получить полный доступ ко всей циркулирующей в сети обмена данными информации, как в голосовой радиосети. В отличие от конвенциональных голосовых радиосетей, где каждый подключившийся к сети пользователь может принимать циркулирующие в ней сообщения, в радиосетях обмена данными это полностью исключено.

Поскольку устанавливаемая на подвижных объектах радиотехническая аппаратура имеет свой уникальный адрес, она может принимать только общие циркулярные сообщения и сообщения, адресованные именно данному подвижному объекту в составе группы или индивидуально. Но если администратор информационной системы получает информацию об угоне служебного автомобиля, он может оперативно исключить адрес установленного на нем оборудования из общего списка адресов и предотвратить передачу данных на компьютер в угнанном автомобиле. Передача циркулярных сообщений на период локализации ситуации с угоном также может быть временно прекращена, а до остальных пользователей данные будут доводиться с использованием групповых и индивидуальных адресов.

Поскольку управление работой всей сети обмена данными строго централизовано и обеспечивается дистанционно с базовой станции, аппаратуру на угнанном автомобиле можно просто дистанционно отключить. Факт отключения радиомодема легко подтверждается, поскольку каждая переданная в его адрес команда, включая команду на отключение, автоматически контролируется и фиксируется. В этом случае передача циркулярных сообщений в радиосети будет беспрепятственно продолжаться.

В некоторых реально действующих АСОДУ реализована специальная функция, обеспечивающая трансляцию на компьютер в похищенном автомобиле ложных сообщений, имитирующих реальный радиообмен. Это вводит похитителя в заблуждение и в большинстве случаев способно подтолкнуть его к действиям, гарантирующим его задержание.

В современных системах, использующих навигационные средства, данные о местоположении подвижного объекта автоматически передаются диспетчеру. Таким образом, в случае угона служебного автомобиля администратор радиосети сможет дистанционно его контролировать. Поскольку управление работой бортовой аппаратуры и передачей навигационной информации с подвижного объекта также происходит дистанционно, через базовую станцию, можно изменить режим ее работы, увеличив интенсивность трансляции навигационных данных с борта угнанного автомобиля, что гарантирует задержание угонщика и возврат машины. ИКС

Защита, которая по карману

Безопасность виртуальных кошельков и электронных платежных транзакций не дается бесплатно. Соответственно, банки и платежные системы реализуют только те меры защиты, которые экономически оправданы. В такой ситуации пользователям не стоит проявлять излишнюю беспечность.

Темир ШАМИЛЬ,
вице-президент по развитию бизнеса в банковском секторе, MAYKOR

Использование интернет-ресурсов в качестве площадки для торговли – один из наиболее эффективных способов сокращения издержек. Именно поэтому практически каждая крупная розничная компания в дополнение к традиционной торговой сети имеет интернет-магазин, а значительное количество средних и мелких ритейлеров предпочитают вести свою деятельность исключительно в интернет-пространстве. В интернет-магазинах помимо традиционных видов оплаты – наложенным платежом, банковским переводом на счет продавца, наличными курьеру при доставке и т.д. – наиболее удобными и потому востребованными являются моментальные платежи с использованием систем интернет-банкинга или через электронные платежные системы. Виртуальные деньги, как и реальные, – постоянная мишень мошенников. Поэтому самый критичный фактор, влияющий на дальнейшее развитие моментальных платежей, – их безопасность.

Нельзя придумать абсолютную защиту. Любую преграду можно преодолеть. Вопрос только в целесообразности, вернее, в соотношении себестоимости подготовки и реализации мошеннической схемы и количества украденных денег. Если для того чтобы украсть 100 руб., необходимо потратить 110, то какой смысл красть? Даже если затраты составят 90 руб., все равно проще положить деньги на депозит в банк. Самый правильный подход к обеспечению безопасности – это одновременно увеличивать затраты на каждую мошенническую операцию и уменьшать величину «улова». В какой-то момент воровать станет невыгодно. Это в теории. Но на практике все новые технологии постепенно устаревают, становятся более доступными, а потому дешевеют. И метод мошенничества, еще вчера казавшийся дорогим, сегодня вполне удовлетворяет финансовым чаяниям нечистых на руку граждан.

Риски можно снизить и диверсифицировать

Основная цель мошенников – получить доступ к управлению счетом добропорядочного пользователя. Для этого мошеннику необходимо завладеть идентификационными данными, с помощью которых он, выдав себя за истинного владельца аккаунта, осуществит перемещение средств в собственных интересах. Чтобы получить доступ к нужным идентификационным данным, некоторые мошенники выбирают очень затратный и технологичный, но приносящий неплохие дивиденды способ – взлом самой системы. Это происходит нечасто, но приводит к серьезным потерям. Защитить себя от таких угроз владельцы виртуальных кошельков никак не могут. Единственное, что они могут сделать, – это принять некие превентивные меры для сокращения возможных потерь. Например, держать на своем аккаунте минимальные суммы денег и пополнять счет только перед совершением операции. Тем самым пользователь избегает и другой угрозы – целенаправленного взлома именно его кошелька. Ведь тратить много сил и времени, чтобы украсть несколько рублей, неэффективно. Если же пользователь является активным участником финансовых взаимоотношений в интернете и ему необходимо постоянно иметь значительные суммы на виртуальном счете, то можно завести много счетов с небольшими суммами и консолидировать средства на одном из них непосредственно перед оплатой. Таким образом риски диверсифицируются между всеми счетами. Можно придумать и другие методы снижения рисков, но все они, так или иначе, создают препятствия не только для мошенников, но и для самих пользователей. Так что каждый должен выбрать для себя некий средний вариант, который уменьшит риски до приемлемых размеров, но все же не сделает обращение к сервису настолько сложным и неудобным, что тот потеряет свою привлекательность.

Похожим путем идут и сами платежные системы – в их распоряжении всегда есть несколько методов усиления безопасности, но стоимость их внедрения превышает возможные потери от реализации угроз. Они осознанно идут на определенный риск, откладывая внедрение новых эшелонов защиты, и периодически проводят переоценку рисков. Если пользоваться наиболее известными платежными системами, то можно рассчитывать, что они применяют наиболее эффек-

тивные меры защиты из числа финансово оправданных на текущий момент.

Пользователь, не теряй бдительности

Другой способ получить доступ к деньгам – это выудить необходимые данные у самой жертвы. Предложить действенный способ защиты от подобных угроз невозможно, поскольку он должен лежать не в сфере технологических решений, а в сфере психологии. Можно только посоветовать никому и никогда не сообщать персональные данные своего счета. Однако в самой этой рекомендации кроется противоречие: ведь тогда невозможно будет совершать операции, поскольку без идентификационных данных пользователя не распознает система. Поэтому каждый раз, набирая на клавиатуре логин, пароль или временный код, пользователь должен хорошо понимать, что и кому он сейчас сообщает.

Должным образом защитив от посягательств данные в системе и приняв все необходимые меры предосторожности со стороны пользователя, все равно нельзя быть полностью уверенным в целостности средств. Ведь идентификационные данные можно получить еще из одного источника – платежной транзакции. При формировании транзакции используются не только данные о собственно платеже – его сумма, валюта, но и идентификационные данные пользователя. Конечно, при передаче данных они шифруются, проводятся защищенные сессии. Но любые шифры поддаются расшифровке, это лишь вопрос времени.

Для борьбы с такими хищениями сегодня применяется один из наиболее эффективных методов защиты – одноразовые коды, отправляемые по SMS или предоставляемые заранее. Их эффективность зиждется на том, что такой код нельзя использовать повторно и логически он никак не связан ни с предыдущим кодом, ни с последующим. В результате, перехватив и взломав какую-либо транзакцию, мошенники не смогут инициировать другую. Но в этом случае пользователь должен строго следить за сохранностью карты с одноразовыми кодами, если он таковой пользуется, или за своим телефоном, на которой ему присылают SMS с кодом. И при утере немедленно связаться с платежной системой или банком для аннулирования карты или прекращения SMS-отправки кодов.

■ ■ ■

Многие пользователи пребывают в эйфории, считая, что структура, которой они доверили свои деньги, должна самостоятельно бороться за целостность и безопасность их средств, и ведут себя более чем беспечно. При этом они не понимают, что система безопасности, на которую они могли бы безусловно положиться, стоит настолько дорого, что они скорее откажутся оплачивать расходы на ее создание (а кто же еще будет за нее платить?), нежели продолжат пользоваться такой надежной, но такой дорогой услугой. ИКС

Горькое лекарство аудита

Случается, спустя непродолжительное время после ввода дата-центра в эксплуатацию работа его инфраструктуры становится далека от оптимальной. Как выявить источник проблем и устранить их, рассказывает руководитель подразделения профессиональных сервисов IT Business Schneider Electric Александр МИРОНЕНКО.

Александр МИРОНЕНКО

– Какие проблемы чаще всего возникают в работе российских дата-центров?

– Большинство российских ЦОДов построено пять-десять лет назад и даже раньше, когда, в частности, тепловыделение ИТ-нагрузки было заметно ниже, и основные проблемы у них связаны с охлаждением. Причем самая печальная ситуация наблюдается в небольших корпоративных ЦОДах, где до сих пор нередко используется оборудование, для дата-центров не предназначенное (вплоть до бытовых кондиционеров). Кроме того, в дата-центрах зачастую отсутствует система мониторинга изменений (информация об установке нового оборудования, изменении схем и т.п. не вносится должным образом в документацию, а сама документация теряется), и из-за этого могут возникать серьезные угрозы работоспособности ЦОДа.

– Можно ли решить эти проблемы в работающем ЦОДе?

– Что бы ответить на этот вопрос, нужно прежде всего провести внешний аудит инфраструктуры дата-центра. В зарубежных дата-центрах эта процедура уже стала традиционной. Но и в России есть специалисты, способные вскрыть болевые точки и дать конкретные рекомендации владельцам ЦОДов по модернизации и оптимизации работы всех элементов инженерной инфраструктуры.

– В чем состоит процедура аудита дата-центра?

– Аудит, как правило, начинается с жалобы «больного»: например, у него происходят сбои электропитания, не получается охладить до нужной температуры те или иные стойки или оборудование отключается из-за перегрева. Чтобы оценить общий масштаб бедствия, аудитор предлагает цодовладельцу ответить на ряд общих вопросов о его дата-центре (площадь, количество стоек, средняя мощность на стойку и т.п.). Затем он отправляется на место для предварительного обследования, результатом которого становится список инженерных систем ЦОДа, которые нуждаются в обследовании. Сама процедура аудита состоит в том, что на объект выезжают инженеры по электропитанию, охлаждению и архитектуре, устанавливают разнообразное измерительное оборудование и в течение нескольких дней записывают информацию об энергопотреблении стоек, режимах работы кондиционеров и чиллеров, расходе воздуха, распределении температуры и влажности и т.д. Обработка полученных данных занимает около двух недель, и ее итогом является отчет с таблицами, графиками, объяснением источников проблем и, что самое важное, с конкретными рекомендациями по их устранению.

Рекомендации обычно делятся на три группы. В первой содержится список элементарных мер, реализация которых не требует отключения оборудования и может быть выполнена силами заказчика. Как показывает практика, эти простейшие меры позволяют снизить энергопотребление на величину до 10%. Для осуществления второй группы мер (передвинуть стойки, заменить один кондиционер, отрегулировать работу другого и т.п.) нужны частичная остановка работы ЦОДа и определенные инвестиции. Третья группа – это рекомендации по глобальной реконструкции дата-центра, если таковая необходима в данном случае.

– Наверняка аудит такого серьезного объекта, как дата-центр, не обходится без сложностей?

– Главная сложность в том, что в аудите дата-центра заинтересовано фактически только высшее руководство компании, причем в российских условиях этот интерес нередко проявляется лишь после аварии с остановкой ЦОДа. Очень часто службе эксплуатации, по большому счету, все равно, какое у ЦОДа энергопотребление, в оптимальном ли режиме работает инженерное оборудование. Главное, чтобы к службе не было претензий. ИТ-департамент тоже обычно не горит желанием проводить какие-либо модернизации, особенно если они грозят сверхурочными ночными работами. Бывает, что эти подразделения вообще не взаимодействуют друг с другом. И всегда они очень настороженно относятся к внешним аудиторам, от которых ждут всяких неприятностей, вплоть до обвинений в непрофессионализме.

Аудит – операция технологически сложная, небыстрая, но необходимая для понимания, что именно не в порядке в ЦОДе и как это исправить. Он нужен, как горькое лекарство, ведь только взгляд со стороны позволяет получить объективную картину происходящего. Нельзя не отметить, что сегодня все больше руководителей компаний начинают использовать аудит в качестве инструмента для повышения надежности своих ЦОДов.

Беседовала **Евгения ВОЛЫНКИНА**

Выбор стратегии в эпоху мобильности – дело тонкое

Какое влияние окажет прогнозируемое аналитиками глобальное снижение продаж десктопов на бизнесы, тесно связанные с этим сегментом ИТ-устройств, например производство ИБП? Об этом – Майк ЛЮ, генеральный менеджер по продуктам компании Powercom, мирового производителя систем защиты электропитания.

Майк ЛЮ

– С какими новыми вызовами сталкивается сегодня производитель ИБП?

– Мы видим, что в развитых странах, в том числе в России, продажи ИБП, предназначенных для домашних пользователей, SOHO и SMB, сокращаются под влиянием повального увлечения смартфонами и планшетами. Для сохранения позиций на этих рынках нам приходится не только развивать уже имеющиеся компетенции, но и смещать фокус в сегмент систем бесперебойного электропитания средней и высокой мощности, а также искать новые ниши, например в области портативных устройств, домашней техники. Поиск баланса между такими рынками и рынками развивающихся стран, где сегменты SOHO и SMB по-прежнему растут, это одновременно и вызов, и новая возможность, которую хотелось бы использовать.

В этих условиях приходится более внимательно относиться к OEM-проектам, доля которых в обороте компании в настоящее время составляет 50%. С одной стороны, они обеспечивают масштаб производства и позволяют поддерживать прибыльность бизнеса, а с другой – ограничивают узнаваемость нашего бренда.

– Как наблюдаемая сейчас мобилизация отражается на бизнесе Powercom в глобальном масштабе?

– В структуре наших продаж налицо перераспределение долей недорогих интерактивных ИБП и «тяжелых» корпоративных решений высокой мощности. Понимая, что первый сегмент немного «сожмется», мы оптимизируем свою линейку маломощных устройств, сосредоточиваясь на их качестве, надежности, универсальности для того, чтобы сделать их «умными» внутри и удобными снаружи.

– А как вы оцениваете конкурентную ситуацию, сложившуюся на рынке систем защиты электропитания?

– Если сравнить текущий уровень конкуренции с тем, который был в 1987-м, в год основания компании, то он стал гораздо выше. Большинство производителей смотрят в сторону систем защиты электропитания для ЦОДов, облачных технологий, мобильных устройств. И это неудивительно: именно в этих областях открываются новые возможности для бизнеса, которые каждый производитель ИБП хотел бы использовать.

Мы тоже изучаем возможность более активно играть в сегменте дата-центров. В мире много стран, где качество электроснабжения низкое и где для надежного функционирования ЦОДов требуется защищать электропитание не только внутри здания, но и на вводе, и в этой роли вполне могут выступать мощные трансформаторные системы, имеющиеся в нашем продуктовом портфеле. Кроме того, есть и другие отрасли со специфическими требованиями к ИБП – медицина, производство.

– Считаете ли вы, что мобильные рабочие места постепенно заменят собой персональные компьютеры, а вместе с ними и ИБП?

– Я не думаю, что все отели и банки, скажем, в Европе полностью откажутся от ПК в пользу планшетов, пожертвовав безопасностью и стабильностью работы ради удобства. Кроме того, мы видим рост спроса на персональные компьютеры и ИБП для защиты их электропитания в развивающихся странах и считаем, что в ближайшие несколько лет этот рост продолжится.

– А в каких странах пользуются спросом решения Powercom для солнечной энергетики?

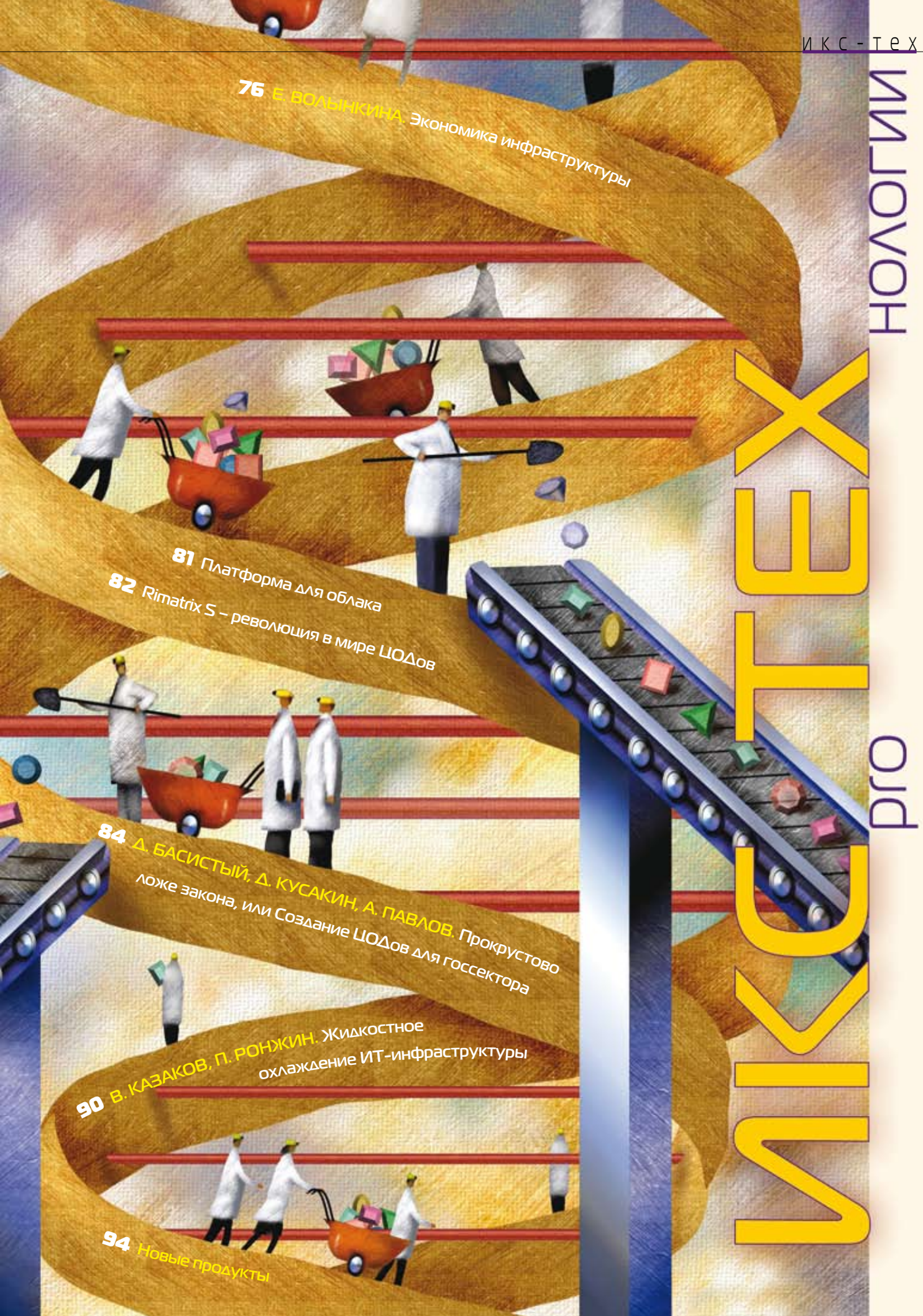
– К сожалению, в европейских странах, переживающих рецессию, государственная поддержка альтернативной энергетики оказалась заморожена. К тому же этот новый рынок фактически разрушили китайские производители, предлагавшие очень дешевые, но некачественные решения. Так что наш фокус смещается в страны Азии, где неплохие перспективы развития альтернативных источников электроэнергии, поскольку данная отрасль поддерживается государствами и, в отличие от Европы с ее плотной застройкой, есть свободные площади для строительства солнечных электростанций. В настоящее время мы реализуем крупный проект в Японии, которая после аварии на Фукусиме полностью отказалась от АЭС в пользу альтернативной энергетики. Также мы выступаем в роли поставщиков «солнечных» решений и консультантов в Таиланде и Китае.

– Как изменятся традиционные ИБП в пятилетней перспективе?

– Полагаю, развитие пойдет в сторону наращивания «интеллектуальных способностей» этих систем, уменьшения размеров и снижения их веса, в том числе за счет использования в них батарей, подобных тем, которые применяются в мобильных устройствах. Сегодня подобные решения достаточно дороги, а через пять лет можно ожидать их удешевления.

Беседовала **Александра КРЫЛОВА**

ИКС pro технологии



Экономика инфраструктуры

Евгения ВОЛЫНКИНА

Строить надежные дата-центры в России научились – что подтверждено уже шестью сертификатами Uptime Institute на проекты ЦОДов и тремя сертификатами на готовые площадки. Надежность не означает автоматически экономической эффективности объекта, но эти две категории вполне могут дополнять друг друга.

В том, как с умом потратить деньги на строительство, оснащение оборудованием, модернизацию и организацию эксплуатации дата-центра, пытались разобраться участники международной конференции Data Center Design & Engineering, организованной журналом «ИКС».

У истоков эффективности

Начинать проектирование ЦОДа надо с формулирования требований бизнеса, так как только они позволяют определить все технические характеристики будущего дата-центра, в том числе его доступность, масштабируемость, уровни безопасности и резервирования, энергоэффективность, операционную устойчивость. Вроде бы ЦОДы во всем мире строятся далеко не первый год, но до сих пор, как рассказал управляющий партнер подразделения инжиниринга и консалтинга ЦОД компании Edarat Group Адель Ризк, встречаются заказчики, которые просят построить дата-центр уровня Tier IV, но при этом на вопрос о допустимом для их бизнеса времени простоя ИТ-сервисов отвечают: два дня. Конечно, такой недалекий заказчик, если его финансовая состоятельность действительно соответствует заявленному уровню Tier IV, позволит исполнителю хорошо заработать, но вряд ли последнему стоит строить стратегию своего бизнеса на неинформированности клиентов.

Как раз с точки зрения стратегии лучше помочь заказчику понять его собственные цели и задачи и соотнести их с его возможностями. Заявление о том, что каждый проект ЦОДа уникален, – не просто красивые слова, потому что проект должен зависеть от очень многих параметров: от назначения дата-центра (корпоративный или коммерческий, и если коммерческий, то на каких клиентов рассчитан), услуг, которые он будет предоставлять, местоположения (и связанных с этим особенностей климата, природных и рукотворных рисков и угроз, доступности дорог, электричества, топлива, воды и т.п., наличия нужных специалистов, в конце концов), от местного законодательства и регуляторных ограничений, бюджета, срока возврата инвестиций, требований к непрерывности бизнеса, срокам восстановления работоспособности ИТ-систем после аварии и общей стоимости владения, от наличия или отсутствия унаследованного оборудования и приложений, планов дальнейшего развития и т.д. и т.п. Во всяком случае, зарубежные компании, которые стараются закрепиться на перспективном российском рынке дата-центров, уже вовсю предлагают (как, например, M+W Group и уже упомянутая Edarat Group) полный пакет работ по созданию ЦОДа «под ключ» – от помощи заказчику в разработке концепции будущего дата-центра до выбора площадки, проектирования, получения всех разрешений, строительства, запуска готового объекта в эксплуатацию и его сертификации в Uptime Institute.

Однако есть у нас уже заказчики, которых и заказчиками-то сложно назвать, это вполне самодостаточные компании, которые, подобно Google или Facebook, выстраивают свои дата-центры, их инженерную и ИТ-инфраструктуру в соответствии с особенностями своих вычислительных задач, требованиями бизнеса и стратегией его развития. Возможно, кому-то технологический уровень инженерной инфраструктуры их дата-центров покажется недостаточно высоким, а PUE – недостаточно низким, однако такие компании интересует прежде всего финансовая эффективность дата-центра. По мнению руководителя проектов строительства ЦОД «Яндекса» Николая Иванова, энергоэффективность и надежность систем дата-центров нельзя рассматривать в отрыве от капитальных и операционных затрат и только при тесном взаимодействии инженеров и финансистов компании можно получить действительно эффективное решение. Причем на его эффективность влияет не только грамотное проектирование и активная «работа» с поставщиками оборудования, но и качество электропитания. К сожалению, далеко не все владельцы дата-центров имеют возможность, как «Яндекс», построить собственную подстанцию и подключиться к сетям ФСК ЕЭС, обеспечивающей практически стопроцентную надежность электропитания при напряжении как минимум 110 кВ (да и цена электричества у ФСК ЕЭС ниже, чем у региональных и ведомственных поставщиков). Но знание реальных параметров качества потребляемой электроэнергии в любом случае позволит более грамотно и без лишних затрат построить систему резервирования электропитания ЦОДа.

Greenfield и модернизация

О создании ЦОДа с чистого листа российским цодостроителям приходится только мечтать, гораздо чаще стоит задача модернизации уже имеющегося дата-центра. Нарастить вычислительную мощность серверных стоек относительно легко, а вот модернизация инженерной инфраструктуры – куда более сложная задача, и, по большому счету, такая возможность должна закладываться еще на этапе проектирования дата-центра. Как отметил директор по развитию бизнеса консалтинговой группы «Борлас» Владимир Иванов, это предполагает прежде всего модульный принцип построения всех инженерных систем и повышение уровня их надежности за счет организации резервирования по схеме 2N (да, при схеме N+1 начальные затраты будут ниже, но такое резервирование сильно осложнит не только будущую модернизацию, но и текущее регламентное техническое обслуживание). Кроме того, необходимо обеспечить возможность прокладки дополнительных кабелей питания и установки дополнительных систем охлаждения без проведения каких-либо строительных работ. Как показывает практика, изначально грамотное проектирование инженерной инфраструктуры позволяет наращивать системы электропитания и кондиционирования даже в совсем небольших ЦОДах, где на счету каждый квадратный метр. Очень способствуют повышению эффективности использования имеющейся инфраструктуры развитые системы автоматизации, диспетчеризации и мониторинга всех систем дата-центра.

Масштабный проект модернизации и реконструкции действующих площадок идет сейчас в «Ростелекоме». В частности, ведутся работы в ММТС-9, где базируется самая крупная в России точка обмена интернет-трафиком MSK-IX и установлено оборудование более 300 операторов связи, которое нельзя отключить даже временно, и это очень сильно усложняет решение поставленной задачи – создания новых технологических помещений и кратного увеличения числа серверных стоек. В такой ситуации, по словам директора проекта ЕРЦОД «Ростелекома» Александра Мартынюка, главным правилом является принцип «не навреди». Подобный проект прежде всего требует тщательного обследования объекта, которое занимает 3–5 месяцев, а результатом его может оказаться решение о нецелесообразности модернизации и реконструкции данной площадки при имеющемся износе здания и инфраструктуры, требуемых конструктивных изменениях и бюджетных ограничениях. Но это тот

случай, когда отрицательный результат – тоже результат: даже дорогое обследование гораздо дешевле строительства сомнительного в техническом отношении объекта.

К эксплуатации готовься!

Но вот здание подготовлено, коммуникации подведены, стойки расставлены... Теперь все это хозяйство нужно вводить в эксплуатацию. Проблема в том, что проектировщики, строители и ИТ-отдел понимают этот процесс по-разному. Если делать все по правилам, рекомендуемым Uptime Institute, то это будет серьезная программа тестирования всего оборудования дата-центра на пределе возможностей его работы. Как выразился исполнительный директор Uptime Institute Джулиан Кудрицки, во время ввода в эксплуатацию нужно попытаться сломать ЦОД. Причем делать это можно совершенно свободно, потому что бояться нечего – официально дата-центр еще не работает, т.е. никаких финансовых последствий для бизнеса не будет (ну не считать же большими расходами оплату дизельного топлива, которое все равно нужно периодически менять), к тому же все оборудование еще находится на гарантии производителя. По данным Uptime Institute, большинство отказов в работе ЦОДов (70%) обусловлены человеческими ошибками, а процесс ввода в эксплуатацию – это важный этап обучения команды, которая будет управлять дата-центром. К запуску ЦОДа в эксплуатацию должно быть готово не только оборудование, но и команда «эксплуататоров» (даже Uptime считает, что профессиональная служба эксплуатации важнее резервирования), а также описание процессов, выполнение которых должно обеспечить нормальную эксплуатацию оборудования дата-центра. Проверить соответствие этих процессов стандартам можно с помощью операционного аудита. Как заявил руководитель подразделения профессиональных сервисов IT Business Schneider Electric Александр Мироненко, этот, уже довольно распространенный в мире сервис, скоро должен появиться и в России. Предполагается, что он заинтересует тех владельцев ЦОДов, которые не собираются сертифицировать свою службу эксплуатации в Uptime Institute, но хотели бы минимизировать риски отказа оборудования, которые так или иначе связаны с человеческим фактором.

Вопрос о том, как сделать эксплуатацию ЦОДа недорогой и эффективной, встает, наверное, перед владельцем любого дата-центра – и корпоративного, и коммерческого. Держать в штате высококвалифицированных специалистов по всем инженерным системам ЦОДа слишком накладно, привлекать для всех работ специализированные сервисные компании не всегда

разумно. Например, компания Mail.Ru, построив собственный крупный ЦОД, поначалу возложила функции наблюдения за работой инженерного оборудования на смену ИТ-инженеров, заключив договоры на обслуживание этого оборудования со сторонними сервисными организациями. Однако, вкусив реалий российского аутсорсинга, решила модернизировать систему мониторинга и диспетчеризации и завести более серьезную службу эксплуатации. Теперь в ЦОДе есть свой главный инженер-электрик с круглосуточной службой дежурных электриков и инженеры по системам кондиционирования и вентиляции, которые, по словам технического директора ЦОДа Mail.Ru Сергея Кубасова, настолько качественно выполняют все плановые регламентные работы, что представитель сервисной организации, приезжающий для аудита раз в полгода, зачастую не находит повода для замечаний. С одной стороны, затраты компании на персонал ЦОДа возросли, но с другой – снизились затраты на оплату работы сервисной организации, на закупки ЗИПа и расходных материалов. При этом время реакции на проблему сократилось с 2 и более часов до 5 мин, и это, наверное, главный плюс организации собственной службы эксплуатации для компании, у которой ЦОД является одним из основных элементов бизнеса.

База экономии

Свой вклад в экономику инфраструктуры дата-центров вносят, конечно, и производители оборудования. Не первый год в стане производителей ИБП идет борьба за дополнительные доли процентов КПД, которые, несмотря на их кажущуюся ничтожность, все же реально снижают счета за электроэнергию и затраты на обслуживание ИБП. Но общая эффективность работы системы бесперебойного питания ЦОДа зависит не только от КПД, но и от загрузки. Минимизировать излишки мощности при сохранении гибкости масштабирования позволяет модульная архитектура. В качестве примера можно привести ИБП серии Liebert APM 30–150 кВА компании Emerson Network Power: его мощность варьируется в диапазоне от 30 до 150 кВА с шагом 30 кВА, причем «шаг» представляет собой совершенно независимый ИБП со своей системой управления. Этот трехфазный ИБП с возможностью «горячей» замены и силовых, и батарейных модулей работает в режиме двойного преобразования с КПД 96%. Допускается установка в параллель до четырех таких ИБП, т. е. максимальная мощность системы достигает 600 кВА.

Уже не первый год Emerson продвигает на рынок мощную модульную систему Liebert Trinergy с возможностью интеллектуального выбора режима работы (режим двойного преобразования, онлайновый и офлайновый). Своя технология переключения режима работы под названием eBoost есть и у компании General Electric (GE). Она реализована, например, в новой модификации ИБП серии SG 160–500 кВА (их инсталляции уже есть в России). Технология eBoost позволяет быстро – время переключения не превышает 2 мс – изменять режим работы ИБП из энергоэффективного в режим двойного преобразования и обратно в зависимости от качества внешнего электропитания. Даже если пользователь отключает возможность такого переключения, система eBoost все равно будет вести мониторинг качества работы электросети и накапливать соответствующую статистику. Так что эксплуатационщики через некоторое время смогут уже со знанием дела принять решение об активизации этой технологии или отказе от нее. Не забыта в GE и традиционная борьба за КПД. Как рассказал начальник отдела технической экспертизы компании «Абитех» Константин Соколов, совсем недавно на российском рынке появился бестрансформаторный ИБП GE TLE series, имеющий в режиме двойного преобразования КПД 96,5%, что подтверждено независимыми испытаниями (в энергоэффективном режиме eBoost его КПД достигает 99%).

Динамика и статика

Свои преимущества – у динамических дизельно-роторных ИБП (ДР ИБП), которые их производители позиционируют как экономичное и энергоэффективное решение для бесперебойного и гарантированного электроснабжения ЦОДов мощностью выше 1 МВА. Кроме того, в соответствии с рекомендациями Uptime Institute (→ см. с. 20) ДР ИБП, объединяя в себе функции ДГУ и ИБП, упрощают систему электропитания ЦОДа, одновременно повысив ее надежность. По словам руководителя Hitec Power Protection по международным продажам Рене Лацины, ДР ИБП компании установлены сейчас на семи объектах в России, четыре из которых уже запущены в эксплуатацию. Причем

«процесс пошел» только три года назад, когда у нас начали строить крупные мегаваттные ЦОДы.

Однако создатели даже мультимегаваттных ЦОДов далеко не всегда выбирают динамические дизельные ИБП. Например, в дата-центре в Алабушево (Зеленоградская ОЭЗ) с заявленным энергопотреблением 21 МВт в системе электропитания будут использоваться традиционные статические ИБП AEG Protect Blue общим числом 108 штук по 250 кВА каждый. Коммерческий характер данного ЦОДа предполагает его поэтапный запуск (всего запланировано 27 залов) и довольно длительный период работы с неполной загрузкой. Поэтому, как объяснила директор по развитию бизнеса компании RadiusGroup Марина Карпунина, чтобы получить максимально эффективное с экономической точки зрения решение, важно было выбрать компактный, хорошо масштабируемый ИБП с высоким КПД при минимальных нагрузках. Новый ИБП AEG Protect Blue, появившийся на рынке осенью 2012 г., имеет КПД 96% даже при нагрузке, составляющей 25% от номинальной. Он допускает установку в параллель до 16 силовых блоков по 250 кВА, что в сумме дает 4 МВА. При таких мощностях даже десятые доли процента КПД дают немалую прямую экономию электроэнергии, но высокий КПД позволяет получить и косвенную экономию: чем он выше, тем меньше тепловыделение, а значит, можно снизить мощность системы кондиционирования.

Литий-ионные перспективы

Решения, о которых шла речь выше, при всей их технологической продвинутости, нельзя назвать прорывом. Тем не менее предпосылки некого подобия революции в сфере ИБП уже просматриваются: это может случиться, когда на рынок массово выйдут литий-ионные аккумуляторные батареи. Они втрое легче нынешних традиционных свинцово-кислотных батарей, занимают как минимум вдвое меньшую площадь, очень долго держат напряжение, а срок

их службы составляет 20–25 лет (и это доказано испытаниями). Как отметил технический директор компании Engross Сергей Ермаков, былые проблемы с пожароопасностью литий-ионных батарей уже решены; кроме того, их можно устанавливать в современные серийно выпускаемые ИБП без серьезной переделки последних. Они обладают высоким КПД (97–99%) и работают в диапазоне температур от 0 до 40°C без деградации емкости и срока службы, т.е. их можно установить вместе с ИБП в общем щитовом помещении и отказаться от специальной системы кондиционирования. Существенными достоинствами являются также высокая скорость заряда и возможность поэлементной замены, что еще больше снижает общую стоимость владения. Правда, такие батареи пока дороже, чем свинцово-кислотные, но прямое сравнение цен нельзя признать корректным, поскольку сроки их службы сильно различаются.

Эффективный холод

Революций в системах охлаждения тоже ждать пока не приходится, зато имеет место поступательное движение в сторону более энергоэффективных и экономичных решений, и спрос на российском рынке уже начинает смещаться от традиционных DX-систем в сторону фрикулинга. По мнению коммерческого директора HTS Михаила Андреева, на ситуацию явно повлиял пример «Яндекса», еще несколько лет назад начавшего эксперименты с внедрением новых технологий свободного охлаждения. Сама же компания HTS реализует сейчас в России первый проект с использованием системы прямого фрикулинга DFC 2 (Direct Free Cooling), у которой в зависимости от температуры забортного воздуха предусмотрено пять режимов работы – с разными сочетаниями технологий DX-охлаждения, фрикулинга и циркуляции воздуха. О том, сколько эта установка, рассчитанная на отвод 1 МВт тепла, позволит сэкономить в российских условиях, говорить пока рано: впереди монтаж и первая зимняя эксплуатация.

В направлении использования наружного воздуха в максимально широком диапазоне температур работает и компания NordVent, открывшая в этом году представительство в России. Как рассказал его генеральный директор Андрей Миляев, в системах NordVent Mirage с роторными и гибридными кондиционерами применяются технологии фрикулинга и адиабатического охлаждения наружного воздуха, которые по сравнению с системами механического охлаждения имеют существенно более низкое энергопотребление. Правда, рабочий диапазон температур для установленных в системе роторных и гибридных кондиционеров Mirage RT и rT+

простирается от –10 до +30°С, и за его пределами нужно будет использовать системы механического охлаждения. Но в нашем климате б́ольшую часть года этого делать не придется, так что суммарное энергопотребление системы, по заявлению А. Миляева, будет в несколько раз ниже, чем у традиционных DX-систем.

В российских условиях энергоэффективные решения зачастую применяют не из экологических соображений, а из необходимости вписаться в имеющиеся лимиты энергопотребления. А если сюда добавляется проблема нехватки площадей, то задача становится очень нетривиальной. Например, в проекте строительства четвертой очереди ЦОДа Stack M1 требовалось отвести 1875 кВт тепла, но места для установки внешнего оборудования системы охлаждения на крыше или снаружи здания не было. Поэтому специалисты инженерной компании «Гулливер» приняли решение использовать вместо чиллеров воздушные конденсаторы фирмы LU-VE, имеющие оптимальное для данной задачи соотношение габаритов и производительности, и разместить их на стене здания на специально оборудованной эстакаде. Выглядит все это не очень эстетично, но, наверное, безупречное с архитектурной точки зрения решение может получиться только при постройке ЦОДа с нуля, а это, как уже говорилось выше, в российских условиях пока очень большая редкость.

Защитить созданное

Все эти – энергоэффективные и не очень – решения для электропитания и охлаждения дата-центров, а также их ИТ-оборудование нуждаются в защите. Затраты на нее, конечно, влияют на экономику всего объекта, но это тот случай, когда экономия может выйти боком, поэтому задача построения физически безопасного ЦОДа представляется очень актуальной. При выборе площадки для дата-центра нужно учитывать и вероятность природных катаклизмов в данной местности, и возможность рукотворных инцидентов, но главными рисками являются огонь и вода, и они часто идут рядом. Конечно, любой ЦОД должен быть оснащен системами пожарообнаружения и пожаротушения, но, как напоминает менеджер по продукции для ИТ-инфраструктуры компании Rittal Александр Нилов, по статистике только 20% пожаров возникают внутри ЦОДа, а 80% – снаружи. При этом ущерб от внешнего пожара может быть катастрофическим: при нагреве вода, содержащаяся в бетонных стенах, начинает быстро испаряться с образованием горячего агрессивного пара, присутствие которого в серверных помещениях недопустимо. Поэтому Rittal предлагает строить внутри машинных залов модули безопасности. Такая конструкция, защищающая оборудование от огня, воды и несанкционированного доступа, имеет модульную структуру, и ее размеры при необходимости можно увеличить. В ней размещается и ИТ-оборудование, и обеспечивающая его работу инженерная инфраструктура. Согласно результатам тестов по европейскому стандарту такая конструкция выдерживает внешнюю температуру 1100°С в течение 60 мин, при этом внутри защищенного помещения температура не превысит 70°С, а влажность – 85%, т.е. ЦОД продолжит нормальную работу.

Но, конечно, до такого пожара дело лучше не доводить. А наиболее безопасным для персонала и оборудования дата-центра противопожарным решением являются системы, использующие газовое огнетушащее вещество Novec 1230. Эта бесцветная диэлектрическая жидкость совершенно нетоксична, а по своим тушащим свойствам намного превосходит системы с хладоном. Кстати, противопожарной системой с Novec 1230 оснащен дата-центр DataSpace 1, который первым в России получил сертификат Tier III Facility от Uptime Institute. Оснащенных подобными системами российских ЦОДов с каждым годом становится все больше, а недавно их поставщик компания «Пожтехника» выпустила мини-вариант такого противопожарного решения – устройство R-LINE, предназначенное для тушения отдельных стоек. Само оно размещается в той же 19-дюймовой стойке и занимает отсек высотой 2U. По заверениям производителя, несанкционированное срабатывание системы не пробьет брешь в бюджете заказчика, поскольку проблема решается заменой баллона, содержащего всего 1 кг Novec 1230.

■ ■ ■

В общем, оборудование, позволяющее строить не только надежные, но и экономически эффективные решения для дата-центров, в арсенале вендоров уже есть и постоянно появляется новое. Дело за информированными заказчиками и грамотными системными интеграторами. ИКС

Платформа для облака

Системный интегратор КОМПЛИТ развернул производительную, надежную, масштабируемую и экономически эффективную программно-аппаратную облачную платформу, позволяющую компании Inoventica предоставлять инновационные сервисы для клиентов.

Группа компаний Inoventica реализует проекты построения публичных, гибридных и частных облаков в национальном масштабе. Ее клиентами являются свыше 5 тыс. компаний, из которых более 30% составляют государственные структуры и учреждения, компании сегмента SMB, крупные корпорации, системные интеграторы, операторы связи, хостинг-провайдеры, разработчики ПО, операторы ЦОДов. В рамках реализации стратегии группы Inoventica в части увеличения ее доли на рынке облачных сервисов компания развернула кластерное решение на базе новейшего оборудования HP, представленного программно-аппаратной платформой и системами хранения данных. Кластерное решение Inoventica размещено в первом облачном ЦОДе группы компаний, расположенном во Владимирской области. Оно позволило втрое увеличить существующие вычислительные мощности Inoventica, а также повысить качество предоставляемых облачных сервисов, среди которых основную долю занимают IaaS, ИТ-инфраструктура в аренду и виртуальные серверы в облаке.

Расширение спектра услуг и повышение надежности их предоставления потребовало оптимизации используемых площадок ЦОДа и внедрения высокотехнологичной облачной ИТ-инфраструктуры, неотъемлемой частью которой является система хранения данных. Конкурс на проектирование и внедрение новой ИТ-платформы выиграла компания КОМПЛИТ, которая, имея солидный опыт в проектировании подобных решений, смогла оперативно предложить оптимальный вариант. В активе системного интегратора – центр компетенции по облачным технологиям, авторизованный по программе HP Cloud Center of Excellence, а также полнофункциональный сервисный центр, способный осуществлять техническую поддержку и сервисное обслуживание в режиме 24×7. Специалисты КОМПЛИТ помогли заказчику выбрать и в кратчайшие сроки внедрить оптимально соответствующее требованиям данного проекта инфраструктурное решение, основанное на продуктах и технологиях HP.

В качестве решения был выбран комплекс, состоящий из модульных серверов семейства HP BladeSystem, стоечных серверов Proliant DL380p Gen8, а также СХД HP Left Hand P4500 и массива HP 3PAR 7400. Вместе с основным пакетом ПО СХД HP 3PAR заказчиком были приобретены лицензии для таких функций, как создание локальных копий данных, динамическое изменение параметров логических томов без прерывания работы и расширенные возможности генерации отчетов.

Ключевые преимущества этого решения с низким уровнем энергопотребления – масштабируемость вычислительных ресурсов и емкости хранения, автоматическое распределение данных между уровнями СХД, автоматизированные процедуры управления системой, а также динамическое выделение емкости под приложения. Средства виртуализации позволяют создавать внутри одной системы HP 3PAR несколько изолированных виртуальных массивов для нужд определенных групп пользователей. Поддержка смешанной нагрузки способствует оптимизации производительности системы.

Внедрение оборудования происходило в несколько этапов. Первый состоял в выборе платформы. В сжатые сроки нужно было проанализировать требования и выбрать оптимальный вариант. Так как специалисты КОМПЛИТ уже имели опыт разработки и реализации подобных систем, варианты решения были предложены заказчику в течение одной рабочей недели.

Поставка оборудования заняла шесть рабочих недель, а внедрение и обучение специалистов заказчика работе с системой – в общей сложности две недели. На этапе внедрения специалисты КОМПЛИТ установили и настроили комплекс, который состоит из системы HP BladeSystem (включающей модульное шасси HP BL c7000 с 16 серверами BL460c Gen8, модулями сетевых соединений Virtual Connect Flex-10/10D и коммутаторами SAN HP BladeSystem B-Series 8/24c) и дискового массива HP 3PAR StoreServ 7400 в конфигурации с четырьмя контроллерами, восемью дисковыми полками и 176 дисками с интерфейсом SAS 6 Гбит/с и емкостью по 900 Гбайт. Также была установлена и настроена кластерная система хранения HP 4500 G2 Virtualization SAN, предоставляющая данные серверам по протоколу iSCSI, надежность, производительность и масштабируемость которой обеспечивается использованием технологии сетевого RAID, и более дюжины серверов HP Proliant DL380p восьмого поколения.

Сочетание виртуальных серверов с виртуальными дисковыми массивами позволило создать надежную и производительную ИТ-среду, обеспечивающую масштабирование ресурсов без прерывания функционирования, что очень важно для заказчика. В дальнейшем планируется расширение системы путем установки второго такого же комплекса модульных серверов и наращивания емкости массивов.

«Компания КОМПЛИТ известна как один из ведущих партнеров HP, уделяющий особое внимание сотрудничеству с перспективными инновационными компаниями, – говорит и.о. генерального директора, коммерческий директор Inoventica Павел Поздняков. – Уверен, что уникальность и масштабность проекта по внедрению облачной платформы HP позволит нам повысить качество оказываемых услуг и увеличить долю компаний группы на рынке IaaS, а также предложить рынку отраслевые решения».

Rimatrix S – революция в мире ЦОДов

Стандартизированный модульный центр обработки данных (ЦОД) Rimatrix S компании Rittal коренным образом меняет сложившиеся представления о проектировании и строительстве в мире ЦОДов.

Какие преимущества дает использование готовых модулей вместо индивидуальных систем, стандартных решений вместо изготовления на заказ? Самые разные, если учитывать динамично меняющиеся требования, предъявляемые современными прикладными задачами.

Традиционно центры обработки данных представляют собой индивидуальные решения. Однако сегодня, в эпоху Web 2.0, услуги ЦОДов перестали быть такими уникальными, какими они были несколько лет назад. Наряду со специализированными услугами, которые различаются от предприятия к предприятию, все большую и постоянно растущую долю составляет стандартизация. Многие ЦОДы давно практически неотличимы друг от друга по целому ряду параметров, и в обозримом будущем ситуация не изменится.

ИТ-решения демонстрируют тенденцию к централизации. Данные уже не хранятся на планшетах и смартфонах: для этого используются облачные хранилища данных, размещаемые в ЦОДах. Соответствовать таким тенденциям можно только при помощи современной инфраструктуры, для которой необходимы гибкие, масштабируемые решения. Оборудование и программное обеспечение, предлагаемое пользователям поставщиками облачных услуг, в значительной степени схоже. Однако при проектировании, внедрении и эксплуатации ЦОДа, в котором размещаются такие облачные структуры, все еще преобладают индивидуальный подход и индивидуальные решения, зачастую лишенные возможности роста в будущем. То же касается малых и средних предприятий: построение ЦОДа предполагает многие месяцы работ по проектированию, поставке и инсталляции. Это удорожает проект, поскольку практически не существует стандартизированных процессов и компонентов, которые можно определить один раз и в дальнейшем использовать многократно.

Стандартизированные модули

Именно на решение вышеназванных проблем нацелена мировая новинка компании Rittal – система Rimatrix S, дополняющая имеющуюся линейку продуктов Rimatrix. В ее основе лежит принцип построения ЦОДа из готовых стандартизированных модулей, в число которых входят стойки для серверов, системы контроля микроклимата, системы мониторинга и управления, источники бесперебойного питания. Самый малый вариант Rimatrix S – Single 6 – состоит из шести серверных стоек, стойки для СКС, ИБП, стойки распределения питания. Более крупный вариант Double 9 включает 18 серверных стоек. Модули охлаждения предназначены для установки оборудования с рассеиваемой мощностью от 60 до 180 кВт. Несколько модулей Rimatrix S можно объединить в несколько блоков, тем самым создавая масштабируемые центры обработки данных мощностью до 450 кВт.

Таким образом, единицей проектирования становятся модули ЦОДа, а не разрозненные решения. Это значительно ускоряет составление предложения: Rimatrix S – первый ЦОД в мире, имеющий единый артикульный номер. Монтаж такого оборудования также производится значительно быстрее, чем монтаж систем по индивидуальным проектам. Кроме того, стандартизированные компоненты позволяют сэкономить время и деньги на администрировании, техническом обслуживании и хранении запасных частей.

В комплект поставки Rimatrix S может входить ИБП, входят стойки распределения питания для вторичного распределения по рядам шкафов и блоки PDU для распределения питания в шкафах. Это значительно ускоряет ввод ЦОДа в эксплуатацию. Электрораспределение в шкафу распределения питания реализовано с резервированием при помощи двух контуров – фидеров A и B, причем ветвь B подключена к ИБП. ИБП – модульный, с резервированием по схеме N + 1. Концепция модулей достаточно гибкая: в системах Single 9 и Double 9 ИБП не поставляются и может использоваться централизованный ИБП.

Инновационный контроль микроклимата

Неотъемлемый компонент Rimatrix S – новая система контроля микроклимата, которая компактно размещается под фальшполом. Мощные электронно-коммутируемые вентиляторы, изоляция холодных и горячих коридоров, индивидуально разработанные воздухо-водяные теплообменники, расположенные прямо под серверными стойками, обеспечивают эффективное охлаждение. Перед каждой серверной стойкой через решетку подается холодный воздух, серверы забирают его с помощью своих встроенных вентиляторов, охлаждаются, и нагретый воздух выбрасывается в изолированный горячий коридор, где он засасывается вентиляторами и охлаждается с помощью воздухо-водяного теплообменника. Холодные и горячие зоны везде разделены перегородкой. Раз-

мещение под фальшполом позволило компании Rittal реализовать компактную систему охлаждения по принципу Zero-U-Space Cooling-System (ZUCS), которая не занимает монтажного пространства серверов.

Важная особенность системы контроля микроклимата – резервирование по схеме N + 1. Каждый холодильный агрегат под серверными стойками обеспечивает мощность охлаждения 12 кВт. Хотя на 60 кВт серверного модуля Single 6 достаточно пяти климатических установок, в модуле их используется шесть. Это гарантирует работу оборудования при выходе из строя одного из агрегатов и обеспечивает более эффективное использование электронно-коммутируемых вентиляторов, поскольку их нагрузка остается ниже максимальной. Если модуль Rimatrix S устанавливается вместе с системами обратного охлаждения (чиллерами) от компании Rittal, коэффициент PUE (Power Usage Effectiveness) может составить менее 1,15, т.е. на каждый киловатт мощности, потребляемый серверами, дополнительный расход энергии, например на контроль микроклимата и обеспечение бесперебойного питания, не превысит 15%.

Модули Rimatrix S предлагаются в трех вариантах установки: размещение в здании, в контейнерах или в помещении повышенной безопасности от компании Rittal, имеющем сертификат ECB-S. Таким образом, для любой задачи и условий установки можно подобрать оптимальное исполнение Rimatrix S.

Трехуровневый мониторинг

В серверных модулях Rittal реализован трехуровневый мониторинг. На нижнем уровне находятся датчики расхода электроэнергии и температуры, которые передают данные на контроллер Computer Multi Control (CMC III). Блок CMC III локально управляет в серверном модуле соответствующими исполнительными элементами и всеми системами, в том числе ИБП и теплообменниками, которые имеют собственные встроенные контроллеры. Кроме того, собранные данные может получать и обрабатывать и опционально поставляемая программа для управления инфраструктурой ЦОДа Data Center Infrastructure Management (DCIM) – RiZone. В результате для каждого модуля рассчитывается модель работы, которая в зависимости от разных параметров среды определяет наибольшую эффективность. Заказчик впервые получает возможность еще на этапе проектирования провести достоверный анализ затрат на эксплуатацию и окупаемость. Чтобы стандартизированный модульный датацентр мог оптимально работать в комплексной инфраструктуре ЦОДа, программа RiZone позволяет интегрировать в нее данные от оборудования сторонних производителей. Имеются также интерфейсы для подключения к системам управления зданием, инженерному оборудованию здания и ПО для управления ИТ-системами.

Программа RiZone обеспечивает не только оптимальный режим эксплуатации ЦОДа. К примеру, она может отправить администратору сигнал тревоги при возникновении нештатной ситуации с оборудованием. Чтобы изменения в систему могли вносить только уполномоченные специалисты, для всех активных компонентов предусмотрена система разграничения прав.

Комбинирование и расширение

Существенная особенность системы Rimatrix S – возможность комбинирования модулей для создания больших ЦОДов. Модули можно располагать последовательно, создавая длинные серверные ряды. Также возможно зеркальное расположение, при котором два модуля имеют общую холодную зону, а если к ним присоединяется третий, то создается общий горячий коридор. Таким образом можно без проблем расширять уже действующий ЦОД. По сравнению с обычной модернизацией ЦОДа расходы на подключение дополнительных модулей невелики.

Индивидуальность

Система Rimatrix S удовлетворяет многим современным требованиям к ИТ-инфраструктуре – от проектирования и монтажа до эксплуатации. Это энергоэффективное и гибкое решение, которое подходит для типичных условий применения и внедряется в очень короткое время. Несмотря на это, Rimatrix S остается для Rittal расширением основной линейки оборудования для ИТ-инфраструктуры. Возможность проектирования и строительства центра обработки данных по индивидуальному проекту клиента из отдельных компонентов Rimatrix будет по-прежнему доступна. Таким образом, каждый заказчик может получить ЦОД, который будет полностью соответствовать его потребностям.

Прокрустово ложе закона, *или* Создание ЦОДов для госсектора

Дмитрий БАСИСТЫЙ, независимый консультант
Дмитрий КУСАКИН, независимый консультант
Андрей ПАВЛОВ, эксперт и антрепренер

Строительство дата-центров для государственных заказчиков имеет столько особенностей, что эти ЦОДы вполне можно отнести к особой категории – «госЦОДов».

Что мы называем госЦОДом

По сложившейся в России и за рубежом традиции дата-центры по их основному назначению подразделяются на корпоративные и коммерческие.

Корпоративный ЦОД – это объект, используемый для собственных нужд владельца. В нем размещается главным образом оборудование вычислительных систем корпоративной сети либо аффилированных с компанией-владельцем организаций. При создании корпоративного ЦОДа учитываются специфические требования владельца к уровню надежности и безопасности, а также характеристики запланированного к установке серверного и телекоммуникационного оборудования. Подобные дата-центры не предназначены для предоставления услуг внешним организациям без дополнительных подготовительных и адаптационных мероприятий.

Коммерческий ЦОД – это объект, на площадке которого размещается оборудование сторонних организаций, услуги им предоставляются в рамках классической модели аутсорсинга – дата-центр как услуга. При его строительстве учитывают тенденции спроса на подобный тип услуг и динамику развития технологий вычислительных систем в среднесрочной перспективе. Владельцу коммерческого ЦОДа также приходится решать, в каком сегменте рынка он будет предоставлять свои услуги, и затем, опираясь на маркетинговую стратегию продаж, прогноз для выбранного сегмента рынка и общие тенденции развития серверного оборудования, определяться с требованиями к уровню надежности и безопасности будущей площадки, требованиями к комплексу инженерно-технических систем ЦОДа.

В последнее время все активнее развивается еще одно направление – строительство ЦОДов, где заказчиком выступают государственные организации, компании госсектора. Если следовать приведенным выше определениям, то очевидно, что дата-центры государственных организаций следует отнести к классу корпоративных в силу того, что основное их назначение – обеспечивать внутренние, корпоративные потребности в размещении и функционировании оборудования собственных вычислительных систем или систем подведомственных организаций.

Несмотря на то что ЦОДы госсектора несут на себе «родовые метки» класса корпоративных дата-центров, у них есть и определенная специфика, проявляющаяся в первую очередь на стадиях создания. Мы склонны рассматривать такие объекты как третий класс – государственные ЦОДы (госЦОДы). Здесь мы обсудим специфические отличия госЦОДов от классических коммерческих и корпоративных дата-центров с точки зрения процесса их создания; вопросы эксплуатации мы рассматривать не будем.

О специфике госЦОДов в целом

Для того, чтобы «поймать», почувствовать специфику госЦОДов, было бы правильно провести их сравнение с двумя названными выше типами дата-центров. Впрочем, сравнение с коммерческим дата-центром представляется нам бесперспективным в силу несоответствия задач, поэтому мы будем сравнивать ЦОД классического корпоративного типа с определенным нами типом «госЦОД».

Основные различия в создании государственных и корпоративных дата-центров сведены в таблицу, отдельные пункты которой мы затем рассмотрим более подробно.

Процессы подготовки

Цели и задачи

Существует масса причин, в силу которых компания вступает на путь создания собственного дата-центра, отказываясь от сторонних площадок. Это и повышенные требования к безопасности информации, специфические требования к надежности и безотказности работы, которые коммерческие ЦОДы зачастую не могут обеспечить, отсутствие на рынке требуемых объемов и мощностей дата-центров.

К государственным ЦОДам как объектам инфраструктуры могут предъявляться дополнительные требования, связанные с тем, что хранящаяся и обрабатываемая в них информация большей частью подпадает под действие закона №152-ФЗ «О персональных данных». Почти всегда возникают ограничения, вызванные фактом наличия в ИС госЦОДов информации, составляющей государственную тайну. В таких случаях государственные дата-центры в полной мере демонстрируют специфику как процедур отбора поставщиков и проведения работ по проектированию и строительству, так и решений, реализующих требования к техническим параметрам подобных объектов.

Когда развитие ведомственных ИТ-систем заходит в тупик либо, наоборот, под проект требуется установка нового технологического оборудования, тогда и всплывает уже не новая, но все еще модная в государственных структурах идея строительства собственного дата-центра. Сложно спорить с тем, что запуск проекта создания ЦОДа – заметное событие, привлекающее внимание и позволяющее госорганизации выделиться сре-

Чем различаются процессы создания корпоративных и государственных ЦОДов

	Корпоративный ЦОД	Государственный ЦОД
Цели и задачи	Собственная инфраструктура, удовлетворение потребностей компании	Собственная инфраструктура, удовлетворение потребностей организации – в рамках выделенных на развитие бюджетных средств
Финансирование	Собственные средства, средства владельцев	Средства госбюджета
Конкурсные процедуры	По внутренним корпоративным регламентам, с учетом действующего законодательства	По внутренним ведомственным регламентам, отвечающим требованиям Федерального закона №94-ФЗ и другим законодательным актам
Контрактование	Относительно быстрое (зависит от степени бюрократизации компании в целом), практикуется старт работ по гарантийному письму	Множественные согласования, затягивание сроков заключения госконтрактов, старт работ по гарантийному письму – в единичных случаях
Этапность создания	Традиционная, без специфики, использование международных практик	Традиционная с некоторой спецификой, связанной с раздельными контрактами на проектирование и строительство
Сроки создания	Не отличаются от традиционных, возможны изменения сроков в связи с финансовыми затруднениями или изменением приоритетов бизнеса	Не отличаются от традиционных, но есть специфика привязки к окончанию бюджетного года, изменение сроков обычно невозможно
Технические решения	Консервативные, основанные на достижении окупаемости, эффективности и надежности; возможно применение новых энергоэффективных решений для демонстрации своих преимуществ на рынке	Более широкий диапазон решений и простор для фантазии заказчика. Дополнительные условия – для соответствия требованиям регуляторов в части персональных данных и государственной тайны. Особые требования к объектам критически важной государственной инфраструктуры (редко)
Процесс строительства	Традиционный, без специфики	Традиционный, есть риски затягивания приемки выполненных работ
Управление подрядчиком	Классический набор способов управления; специфика характерна для отдельных представителей класса корпоративных заказчиков. Возможно использование международных практик	Дополнительные и административные меры воздействия на подрядчика (федеральный реестр недобросовестных поставщиков и т.п.)
Надзор и контроль	Всевозможные проверки государственных надзорных органов	Менее пристальное внимание со стороны государственных надзорных органов, но неизбежные проверки Счетной палаты
Организация проекта	Как правило, строгая организационная модель с выделенным управляющим комитетом, спонсорами и руководителем проекта	Менее четкая организационная структура, с возможным скрытым влиянием отдельных персон и их неявным управлением проектом

ди тех, у которых нет собственного полноценного дата-центра (порой в этом и кроется причина принятия решения о строительстве, без оглядки на экономическую целесообразность всей затеи).

Нередко при создании государственного дата-центра появляется еще одна задача – «освоение» дополнительного финансирования, выделенного государственной структуре в рамках строительства. Дополнительные задачи могут ставиться независимо от наличия утвержденного технического задания или содержания работ, что добавляет определенные риски при реализации таких проектов.

Финансирование

Вне зависимости от масштабов ЦОДа для государственных органов схема финансирования его строительства подразумевает ряд дополнительных активностей со стороны генерального проектировщика и генерального подрядчика во исполнение закона №94-ФЗ* и иных обязательных законодательных актов.

В число дополнительных действий входит обязательное проектирование любого объекта строительства согласно Постановлению правительства РФ «О составе разделов проектной документации и требованиях к их содержанию» №87. В частности, требуется составление сметной документации по нормам федеральных единичных расценок и территориальных единичных расценок в строительстве, а также строгое исполнение работ в соответствии с данными сметными нормами. Ограничения связаны с тем, что источником финансирования является государственный бюджет и все платежи проходят через Федеральное казначейство.

Стоит отметить, что к безусловной специфике любого рода проектов в государственных органах (не только строительства дата-центров) относятся неизбежные аудиторские проверки Счетной палаты РФ. Этот фактор заставляет государственного заказчика каждый свой шаг сверять с будущими проверками: и выбор решений, и его обоснование, и сметные расчеты, и все остальное, что связано с созданием госЦОДа.

Как правило, финансирование проекта или его этапа привязано к бюджету конкретного года и обязательно к исполнению в точности в том объеме, который был запланирован. Это приводит к формированию финансовой документации именно на указанный объем, но никак не на фактически выполненный, что может внести дополнительные риски перерасхода бюджета и невыполнения запланированного объема работ в указанные сроки.

Подготовка проектной документации к конкурсу

Еще один фактор может негативно повлиять на успешность проекта строительства ЦОДа. К сожале-

* Федеральный закон «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» от 21.07.2005 № 94-ФЗ (принят ГД ФС РФ 08.07.2005, действующая редакция от 01.01.2013). Документ утрачивает силу с 01.01.2014 в связи с принятием Федерального закона от 05.04.2013 № 44-ФЗ.

Специфика процедур – и успех проекта

Различные составляющие специфики проектов создания государственных ЦОДов можно оценить с точки зрения их влияния на успех проекта. Ниже для каждой группы элементов специфики приводятся экспертные оценки этого влияния по пятибалльной шкале (5 баллов соответствует максимальному влиянию).

	Оценка степени влияния:	
	в баллах	качественная
Цели и задачи	2	Незначительное
Финансирование	5	Максимальное
Конкурсные процедуры	3	Среднее
Контрактование	4	Значительное
Этапность создания	3	Среднее
Сроки создания	4	Значительное
Технические решения	5	Максимальное
Процесс строительства	5	Максимальное
Управление подрядчиком	4	Значительное
Надзор и контроль	3	Среднее
Организация проекта	4	Значительное

нию, этот фактор – прямое следствие №94-ФЗ, а конкретнее – невозможности указать конкретные марки и модели инженерно-технологического оборудования в проектно-сметной документации. Федеральный закон требует в обязательном порядке добавлять в выставляемую на конкурс проектную документацию (в составе конкурсной документации) фразу «или аналоги» по каждой позиции спецификаций, в которых указана марка или производитель оборудования.

С одной стороны, это улучшает конкурентную среду и позволяет допустить к конкурсу поставщиков услуг, независимо от «резервирования» цен на заложенное проектировщиком оборудование. Но, с другой стороны, эта фраза развязывает руки недобросовестным подрядчикам – участникам конкурса, готовым заменить запроектированное оборудование на менее качественные аналоги в ущерб качеству объекта в целом.

В такой ситуации возникают неизбежные коллизии между ответственностью проектировщика за свои решения, прошедшие согласования и госэкспертизу, и предложениями конкурсантов, ответственность которых за замену номенклатуры оборудования и ее влияние на параметры функционирования ЦОДа весьма сложно зафиксировать.

Единственный способ хоть как-то уменьшить влияние этой ситуации на конечный результат – ввести дополнительную ответственность как проектировщика, так и генерального подрядчика за проведение приемосдаточных испытаний и мероприятий по вводу в эксплуатацию по заранее разработанным и согласованным с заказчиком методике и программе.

Конкурсные процедуры

Внедрение инструмента электронных площадок для проведения аукционов на право заключения государственных контрактов, по мнению инициаторов данной идеи, должно было повысить прозрачность госзакупок и их эффективность при одновременной оптимизации цены. В реальной жизни данный механизм зачастую работает не совсем корректно. Например, заказчики с целью скрыть конкурс от «посторонних» глаз намеренно вносят ошибки в его наименование (скажем, заменяя русские буквы в ключевых поисковых словах «ЦОД», «инженерные», «кондиционирование», «серверное» на латинские символы, сходные по написанию) либо вовсе маскируют суть работ так, что сложно догадаться, о чем идет речь. Подобные махинации резко ограничивают круг претендентов на выполнение работ, так как компании, не знающие о конкурсе, не смогут его случайно обнаружить. Подобные уловки неоднократно становились предметом общественных обсуждений и внимания правоохранительных органов, и тем не менее нельзя утверждать, что эта порочная практика искоренена.

Есть и обратная сторона медали, закрывающая добросовестным подрядным организациям возможность участвовать в конкурсе и ставящая под угрозу срыва строительство в целом. На рынке присутствует масса поставщиков, стремящихся выиграть аукцион любыми средствами: они «ломают» аукционы, опуская цены ниже себестоимости, а потом стараются уменьшить свои затраты путем снижения качества поставляемого оборудования и материалов, выполняемых работ. Проблема рейдерства*, безусловно, присуща не только государственным, но и коммерческим конкурсам. Но в случае государственных торгов (в основном аукционов) рейдер может значительно затянуть сроки завершения конкурсных процедур и объявления победителя, что, в свою очередь, сказывается на темпах и сроках строительства.

Стоит отметить, что технологии электронных торгов и электронных торговых площадок, типичные для государственных конкурсов, практически не используются для конкурсов в коммерческом секторе. Размещение объявлений об аукционах и конкурсах на корпоративных веб-сайтах коммерческих организаций является скорее информационной составляющей процедуры. Как правило, в таких случаях предполагаемым участникам заранее сообщают о предстоящих конкурсах напрямую.

Подрядчики

Сравнивая перечни исполнителей, привлекаемых к проектированию и строительству дата-центров в корпоративном и государственном секторе, нельзя не заметить, что они различаются: в подавляющем большинстве государственных проектов привлекаются организации-подрядчики, неизвестные экспертному сообществу отрасли цодостроения. Как правило, это крупные государственные или окологосударственные образования, демонстрирующие участие в масштабных строительных

*Если следовать классическому определению рейдерства, то оно означает недружественное поглощение предприятия против воли владельцев. В последние годы это понятие значительно расширилось и, по нашему мнению, стало универсальным, в том числе для описанных действий.

контрактах в интересах госструктур – но, к большому сожалению, не имеющие достаточного опыта проектирования и строительства именно дата-центров. В лучшем случае за спиной этих образований работают компании, хоть как-то представляющие себе суть и специфику объекта. В худшем – мы получаем полуфабрикат, который приходится итерационно приводить к рабочему состоянию.

В этом кроется серьезная проблема для государственных заказчиков. Привлеченные к проектам строительства госЦОДов известные и не очень строительные компании, слабо знакомые со спецификой дата-центров, допускают грубые ошибки в проектировании, не справляются со сроками строительства, нарушают правила и условия (а также очередность) проведения работ и в итоге передают госзаказчику объекты более низкого качества за более высокую цену.

Проблема могла бы быть разрешена за счет привлечения к процессу создания госЦОДа компании – независимого консультанта, которая подготовила бы требования к проектированию, оказала поддержку конкурсным процедурам, взяла бы на себя экспертное сопровождение процессов проектирования и реализации проектных решений. Но такая агентская схема слабо реализуется в условиях действующего законодательства. Выбор агента – отдельный конкурс, а значит, дополнительное время и усилия, на что государственные структуры не идут.

Отдельного упоминания заслуживает тот факт, что в силу ряда требований по безопасности и гостайне, предъявляемых к отдельным госЦОДам, к проектированию и строительству таких объектов не могут быть допущены иностранные компании.

Контрактование и старт работ

Сроки строительства ЦОДа в госсекторе также несколько отличаются от типичных для корпоративных объектов. В частности, большой проблемой для исполнителя могут стать чрезвычайно сжатые сроки создания объекта, ограниченные временем действия государственного контракта. Финансирование не очень крупных объектов чаще всего планируется в пределах года, и завершение строительства, невзирая на дату начала действия контракта, обычно привязывают к концу календарного года, когда традиционно происходит закрытие госконтрактов и выделение окончательного финансирования.

Поскольку не всегда существует физическая возможность довести до конца строительные работы в указанный в госконтракте период и по итогам выполненных работ без существенных проблем получить оставшиеся платежи, подрядные организации по договоренности с заказчиком идут на любые ухищрения для закрытия контракта в установленные сроки. Например, подрядчики начинают закупку оборудования и строительно-монтажные работы до заключения госконтракта, порой и до подведения итогов конкурса, а документальное закрытие строительно-монтажных работ подчас проводится до их фактического окончания. Не все эти способы легальны, но порой структура государственных конкурсов и этапность их финансирования не оставляет сторонам контракта другого выбора.

Жесткие, порой нереальные сроки исполнения обязательств по государственному контракту создают проблемы обеим сторонам: заказчику и исполнителю. В первую очередь это касается освоения финансирования на отчетные периоды. Нередки случаи, когда госзаказчику для того, чтобы не потерять бюджетные ассигнования текущего года, приходится прибегать к практике выплаты авансов и упреждающего актирования закрытия работ, что нередко находится на грани закона.

Реальный срок подписания контракта может значительно превысить срок, указанный в конкурсной документации, но, как показывает практика, госзаказчик не стремится к тому, чтобы передвинуть соответственно и срок завершения контракта. Либо срок упирается в конец финансового года, либо заказчику это в принципе не интересно. В свою очередь, подрядная организация, не выполнившая контракт в срок, может заполучить проблемы с финансированием либо попасть в реестр недобросовестных поставщиков – государственный «черный список», который ведется Федеральной антимонопольной службой (ФАС). Оба варианта абсолютно неприемлемы для компаний, и опять-таки это провоцирует как заказчика, так и поставщика на совершение противозаконных действий.

Стоит отметить, что у корпоративных заказчиков широко распространена практика подготовки гарантийных писем, которые позволяют приступить к проектированию или строительству еще до подписания контракта или начала финансирования. В случае государственного заказчика такая форма гарантирования почти невозможна, и получается, что подрядчик вынужден начинать работы на свой страх и риск.

Проектирование и строительство

В целом перечень и последовательность этапов создания ЦОДа для государственного и корпоративного сектора существенно не различаются. В обоих секторах изначально формулируется идея создания объекта, определяются его основные технические параметры и функциональные требования, составляется техническое задание, разрабатывается проектная документация и выполняется процедура строительства ЦОДа.

Проектные работы

Нередки случаи, когда этап проектирования и этап реализации могут быть разнесены в различные государственные контракты, а значит, строительство может начаться лишь после закрытия контракта на проектирование и выделения финансирования. В таких ситуациях неизбежен ряд проблем.

Зачастую в рамках контракта на проектирование госЦОДа в конкурсной документации значится, что всю исходную информацию для проектирования, в том числе технические условия на подключения, подрядчику обязан предоставить заказчик. Но на практике это почти фантастическая, нереальная ситуация, и подрядчик, дабы не сорвать контракт и не испортить отношения с заказчиком, вынужден собирать эту информацию самостоятельно, теряя время и отвлекая собственные ресурсы, снижая свою прибыль.

Добавим еще, что в большинстве государственных организаций подобная информация, вполне вероятно, будет почти полностью отсутствовать. Может не быть ни проектной документации на существующие инженерные системы, ни разрешительных документов, ни достоверной информации о нагрузочной способности перекрытий, а в итоге сбор информации выливается для поставщика в полноценное обследование, которое не было учтено в цене государственного контракта. Естественно, подрядчику приходится все эти работы проводить самостоятельно и в качестве «жеста доброй воли», надеясь только, что эти послабления с его стороны сделают госзаказчика более лояльным к будущим «прегрешениям» и возможным формальным нарушениям условий контракта.

Возможны задержки сроков реальной подготовки проектной документации, что в конечном счете влияет на сроки начала и окончания строительных работ: второй, строительный контракт подписан и действует, а генпроектировщик еще не может сдать финальную версию проектной документации.

Не всегда проектная документация профессиональна и полна. Заказчик может не предоставить доступ к помещению, в котором должен быть построен дата-центр, поэтому претенденты вынуждены готовить свои предложения на конкурс, основываясь исключительно на проектных решениях (в том числе ошибочных, некачественных и т.д.). Существенные ошибки, допущенные при подготовке проектно-сметной документации, могут заметно изменить сметную стоимость. Отсутствие полноценной проектной документации на создаваемую систему или полноценного доступа к ней, при невозможности изменять цену госконтракта, влечет за собой рост затрат на реализацию, увеличение сроков, недовольство заказчика.

Технические решения

Казалось бы, технические решения для таких объектов инфраструктуры, как дата-центры, слабо зависят от организационно-правовой формы заказчика: коммерческой или государственной. Вместе с тем стоит отметить, что все-таки есть одна особенность, характерная для подготовки технических решений госЦОДов: более широкий диапазон применяемых технических решений как следствие меньшей зависимости от сроков их окупаемости.

Поскольку организации корпоративного сектора в большей степени ориентированы на окупаемость объекта, целесообразность и экономическую эффективность тех или иных технических решений, то и спектр применяемых решений относительно невелик. Государственные заказчики в большинстве своем мыслят и мечтают в рамках выделенных бюджетов. И если обоснование и «выбивание» финансирования удается в полной мере, то они могут позволить себе реализовать в ЦОДах любые фантазии, в том числе новейшие и не всегда апробированные технологии и системы или завышение уровня надежности (например, Tier IV, когда и Tier III хватает с избытком).

Экспертиза проектно-сметной документации

Исключением из традиционной схемы процесса создания дата-центров в случае госЦОДов является обязательный этап государственной экспертизы проектно-сметной документации на строительство. Если для объектов, создаваемых без участия средств госбюджета, отдельная экспертиза сметной документации необязательна, то в случае госЦОДов, не имея заключения госэкспертизы по сметной стоимости объекта, госструктуры даже не могут объявить конкурс на выбор генерального подрядчика.

Какие элементы специфики создания госЦОДов встречаются чаще всего

Каждую группу элементов специфики, свойственных созданию госЦОДов, можно оценить с точки зрения частоты их проявления в проектах (экспертные оценки даны на основании многолетнего опыта авторов).

Обратим внимание читателей на выделенные группы элементов специфики: частота их проявления равна 100% или близка к тому. Это означает, что они имеют абсолютный характер – встречаются во всех проектах.

Строительные работы

Поскольку заказчик имеет существенное влияние на поставщика и по своему усмотрению может менять объемы работ, особенно в рамках контракта на проектирование, то нередко складывается ситуация, когда заказчик требует выполнения дополнительных разделов проектной документации согласно Постановлению правительства РФ №87 «О составе разделов проектной документации и требованиях к их содержанию».

Эти разделы входят в общий перечень разделов проектной документации, но не во всех случаях они необходимы и обязательны. Например, если небольшой ЦОД создается в рамках существующего здания без изменения объемов и вмешательства в конструкцию здания, данные работы можно трактовать как проведение ремонта. Это не требует подготовки таких разделов документации, как ПОС (проект организации строительства), и некоторых других, но заказчик, шантажируя проектировщика непринятием работ, может заставить его подготовить данный раздел, хотя он не был прописан в задании на проектирование, а это повлечет за собой дополнительные временные и финансовые затраты. В частности, такая ситуация может вызываться неточностями в трактовке и терминологии строительного законодательства, когда можно по-разному трактовать понятия «модернизация», «ремонт», «капитальный ремонт» и «капитальное строительство».

Случается, что затягиваются сроки принятия решения по согласованию проектной документации и оперативных решений в ходе строительства. И снова заказчик крайне неохотно идет на подписание дополнительных соглашений об изменении сроков контракта, а задержки ложатся на плечи исполнителя. Особенно часто это происходит, когда держателем госконтракта и непосредственным заказчиком проектирования или строительства являются разные подразделения одного ведомства, а порой и разные организации. Острое нежелание российских чиновников брать на себя ответственность за принятие решений, особенно тех, которые могут поставить под угрозу их работу в государственной структуре, выливается для исполнителя в месяцы бездействия.

Стоит отметить, что в проектах строительства госЦОДов в какой-то степени снижена нагрузка на строительного подрядчика со стороны контролирующих и надзирающих государственных служб. Отчасти это продиктовано осознанием принадлежности к государственному сектору, отчасти тем, что объекты госЦОДов нередко размещены на закрытых территориях, недоступных для надзора.

Изменения в проекте и смете в ходе строительства

Нередко на стадии строительства возникает необходимость увеличить сметную стоимость работ. В подавляющем большинстве случаев это результат некачественного проектирования, когда отсутствие практики и профессионализма не позволяет учесть все нюансы ЦОДа как сложного объекта инженерно-технической инфраструктуры. В редких случаях причиной бывают внешние обстоятельства.

Согласование дополнительных работ в контрактах, выполняемых за счет средств госбюджета, также крайне затруднительно. Средства из бюджета выделяются под обоснованные сметами объемы, а отступление от согласованных государственной экспертизой смет попадает под статью нецелевого использования. И даже когда в результате детального обследования объекта выясняется, что не учтен, например, демонтаж скрытых в стенах коммуникаций или другие объективные, но неявные работы, задача получения дополнительного финансирования труднореализуема. Это потребует повторного прохождения государственной экспертизы, а следовательно, приведет к автоматическому сдвигу (срыву) сроков выполнения проекта.

Задача получения дополнительного финансирования в случае корпоративных дата-центров также непроста, но вполне решаема, если дополнительные работы вызваны объективными причинами и имеют обоснование.

Приемка работ и ввод в эксплуатацию

Ставшее традиционным отсутствие полноценной и единой службы эксплуатации ЦОДа на стороне госзаказчика приводит к затягиванию этапа приемки у подрядчика выполненных работ и передачи объекта в эксплуатацию. Если служба эксплуатации не готова, то нередко приемка тормозится до появления официально назначенных ответственных за эксплуатацию.

Часто разрозненные подразделения в службе главного инженера (или аналогичной службе), как правило, отвечающие каждое за свой фронт работ, предъявляют при сдаче свои специфические требования, не понимая всей специфики ЦОДа не только как строительного объекта, но и комплексного, сложного объекта ИТ-инфраструктуры.

Корпоративные заказчики, со своей стороны, отчетливо понимают, что дата-центр – это инструмент повышения их конкурентоспособности, а порой и основа жизнедеятельности, и стараются максимально в рамках своих компетенций организовать эффективную процедуру эксплуатации объекта до окончания работ по созданию ЦОДа. В этом различие в подходе между ними и государственными организациями.

Особая категория рисков при работе по госконтракту – высокая степень незащищенности прав поставщика услуг. Государственный заказчик может легко управлять подрядчиком, отказываясь подписывать акты выполнения работ и настаивая на получении дополнительных услуг, сверх оговоренных в проектно-сметной документации и в условиях контракта. Отказ подрядчика выполнять такого рода «просьбы» чреват проблемами в настоящем и будущем. Практически отсутствующая история судебных процессов, в которых ответчиком выступали бы государственные организации, тому подтверждение. Инициация такого процесса – «смерть» для подрядчика: скорее всего, он больше никогда не сможет выиграть конкурс и получить государственный заказ.

Заключение

Перечисленные в статье особенности создания дата-центров в государственном секторе основаны на опыте и практике авторов и не претендуют на абсолютную истину. Мы допускаем, что не «все кошки одинаково черны ночью» – есть и еще будут примеры беспроблемных проектов создания ЦОДа для государственных нужд, лишенные большей части (но, увы, не всех) описанных недостатков. Но пока что специфика общей картины строительства госЦОДов нам представляется именно такой.

Подводя итоги поиска общего и специфичного в проектах создания госЦОДов, еще раз отметим, что основные причины описанной выше специфики связаны с тремя главными факторами:

- несовершенной системой закупок для государственных нужд;
- процедурами финансирования проектов за счет бюджетных средств;
- общими принципами функционирования государственной бюрократической машины.

Организационные модели таких проектов – с их скрытыми, неявными влияниями на принятие и утверждение решений – добавляют в и без того стохастический процесс дополнительные финансовые риски, которые, очевидно, ложатся дополнительным бременем на бюджет. С другой стороны, прозрачные и четко детерминированные модели, к примеру, с включением независимых и заинтересованных в конечном результате экспертов, могут добавить таким проектам эффективности. ИКС

Жидкостное охлаждение ИТ-инфраструктуры

Василий КАЗАКОВ,
ведущий инженер,
NVision Group

Петр РОНЖИН,
главный инженер отдела климатических систем,
NVision Group

Жидкостное охлаждение серверов вызывает многочисленные споры в профессиональных кругах. Действительно ли это еще один шаг на пути совершенствования систем охлаждения или очередной пиар-ход?

Какие преимущества выделяют сторонники жидкостного (водяного) охлаждения? Это, во-первых, высокая теплоемкость воды, значительно большая, чем у воздуха, что позволяет переносить в 3463 раза больше тепла одним и тем же объемом теплоносителя. Во-вторых, это использование закрытого водяного контура – а значит, исключено попадание в него пыли и других загрязняющих веществ. Кроме того, возможно повысить допустимую температуру воды, чтобы использовать свободное охлаждение в более широком диапазоне температур.

Сторонники же воздушного охлаждения в первую очередь, как ни парадоксально, отмечают традиционность этого подхода. И возразить здесь нечего – действительно, воздушное охлаждение используется с момента создания первых ЭВМ и до сегодняшнего дня, накоплен огромный опыт реализации таких систем, имеется широкий ассортимент оборудования, как охлаждающего, так и охлаждаемого воздухом. Второй довод в пользу воздушного охлаждения – это различные технологические трудности, которые возникают при использовании охлаждения жидкостного.

Мы рассмотрим здесь некоторые варианты жидкостного охлаждения, чтобы читатели могли самостоятельно оценить будущее разных типов систем.

Особенности жидкостного охлаждения

Для начала немного теории. В чем коренное отличие жидкостных систем охлаждения от воздушных? Все довольно просто: в воздушных системах тепло процессоров, жестких дисков, видеокарт и прочей «начинки» сервера отводится исключительно потоком воздуха, но потом все равно передается какой-либо другой среде, например холодоносителю в теплообменниках прецизионных кондиционеров. При использовании

Рис. 1. Движение тепла от ИТ-оборудования к наружному воздуху (для условий Москвы)

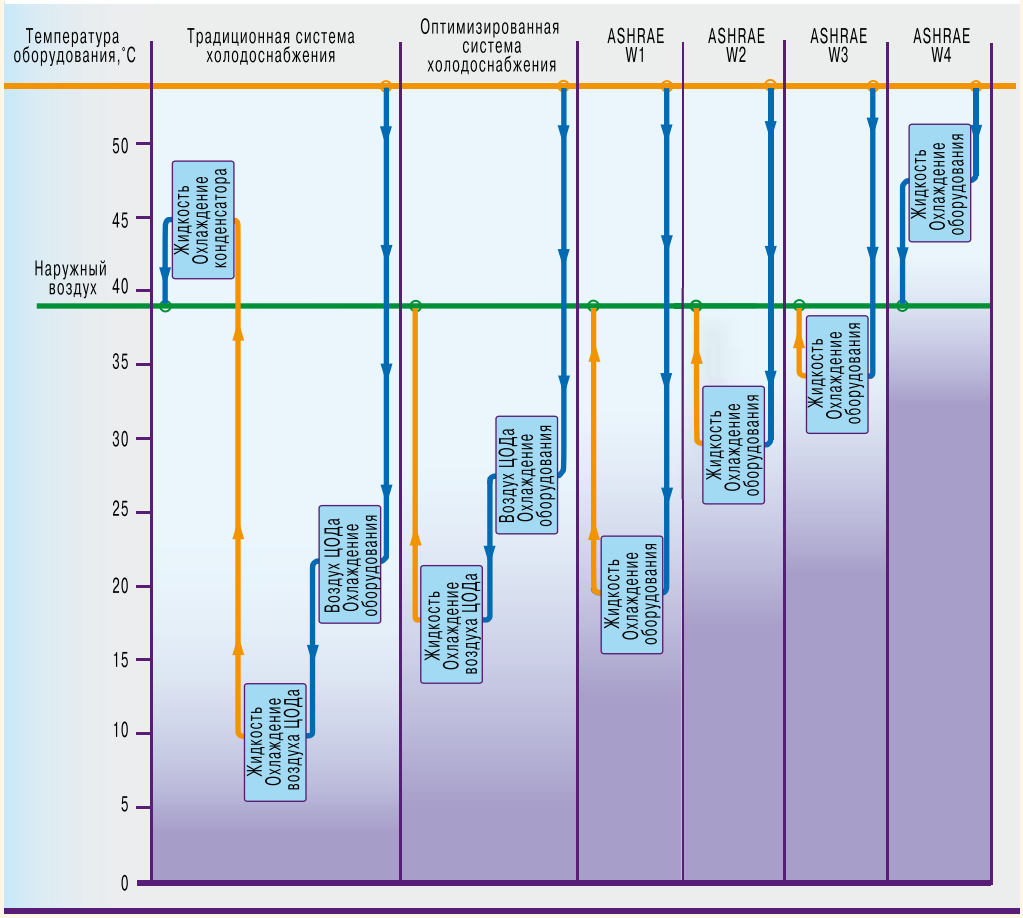
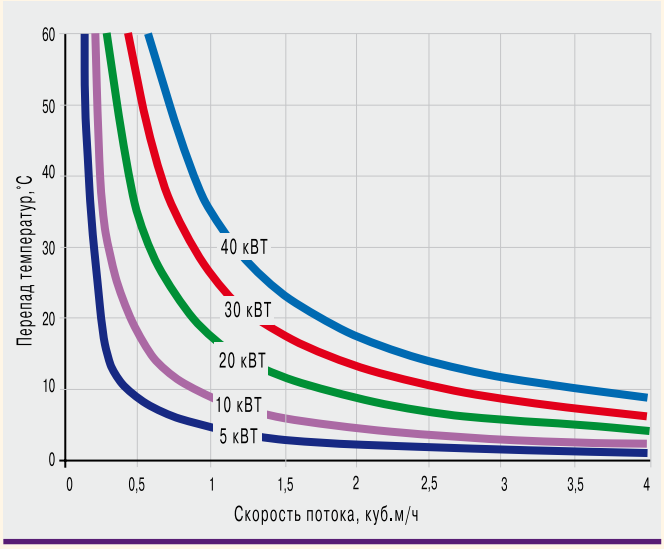


Рис. 2. Перепад температур охлаждающей жидкости (воды) в зависимости от ее расхода и мощности системы



Классификация оборудования для систем жидкостного охлаждения

Класс жидкостного охлаждения	Типовой дизайн инфраструктуры		Температура охлаждающей жидкости, °С
	Основное оборудование системы охлаждения	Дополнительное оборудование	
W1 (рис. 3а)	Холодильная машина/градирня	Водяной экономайзер (сухой охладитель или градирня)	2–17
W2 (рис. 3а)			2–27
W3 (рис. 3а)	Градирня	Холодильная машина	2–32
W4 (рис. 3б)	Водяной экономайзер (сухой охладитель или градирня)	–	2–45
W5 (рис. 3в)	Системы отопления здания	Градирня	> 45

жидкостной системы тепло отводится либо сразу жидкостью (непосредственно), либо через твердую стенку (косвенно). В обоих вариантах жидкостного охлаждения для снятия теплоизбытков с ИТ-оборудования воздух включается в процесс только в самом конце – при сбросе тепла в окружающую среду.

Чтобы выделить основное преимущество жидкостных систем, сравним традиционную и оптимизированную системы холодоснабжения и системы жидкостного охлаждения ИТ-оборудования при помощи диаграмм движения тепла (на рис. 1 они показаны применительно к условиям Москвы). В традиционной системе используются кондиционеры с температурой воздуха 18/25°С и жидкости 7/12°С и холодильные машины внутренней установки с температурами жидкости, охлаждающей конденсаторы, 42/47°С. В оптимизированной системе это кондиционеры с температурами воздуха 23/32°С, жидкости – 15/20°С и с холодильными машинами внешней установки со встроенным свободным охлаждением. Остальные четыре диаграммы отображают работу жидкостной системы охлаждения при различных разрешенных температурах охлаждающей воды. На всех четырех графиках для жидкостного охлаждения взят температурный перепад, равный 5°С, хотя в конкретном случае он может быть другим.

Как известно, тепло переходит от более нагретого материала к менее нагретому, на диаграммах такое движение отображено синими линиями. В остальных случаях требуется совершение работы (оранжевые линии) – и эта работа в нашем случае совершается холодильными машинами. Как видно из рис. 1, наибольшая величина работы – в традиционной системе. В системах же жидкостного охлаждения величину работы удается значительно снизить, а в ряде случаев мы вообще могли бы отказаться от использования холодильных машин.

Следующим положительным моментом в использовании жидкостных систем охлаждения является повышение температуры начала частичного свободного охлаждения и температуры перехода на полное свободное охлаждение. Повышая температуру охлаждающей воды, мы снижаем количество часов в году, при которых работает механическое охлаждение.

Еще одна особенность жидкостных систем – возможность создания значительного перепада температур охлаждающей жидкости. Это позволит существенно снизить расход жидкости, а значит, энергопотребление насосов, и уменьшить размеры коммуникаций (зависимость перепада температур от расхода жидкости и мощности системы показана на рис. 2).

Теперь поговорим о классах систем охлаждения, точнее, о том, какое оборудование соответствует классам систем жидкостного охлаждения. Классификацию ввело сообщество ASHRAE в стандарте для жидкостных систем охлаждения – 2011 Thermal Guidelines for Liquid Cooled Data Processing Environments (см. таблицу).

Рис. 3. Схемы систем жидкостного охлаждения по классификации ASHRAE

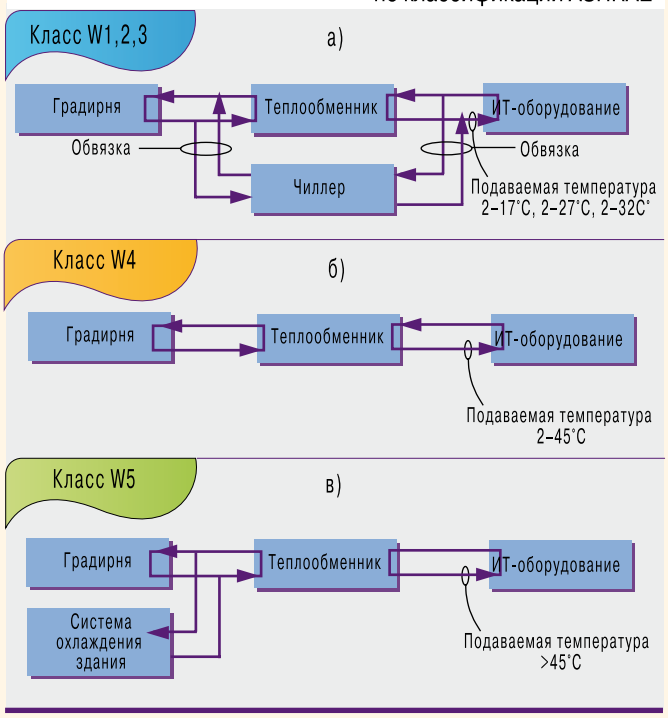


Рис. 4. В вычислительном узле серверное оборудование контактирует с теплоотводящими пластинами

Рис. 5. Охлаждающая пластина покрывает всю поверхность вычислительного узла

В дополнение к данной таблице ASHRAE рекомендует применять схемы систем охлаждения, показанные на рис. 3. Отметим, что при использовании 4-го класса систем жидкостного охлаждения можно отказаться от применения холодильных машин.

Технические решения

Жидкостное охлаждение горячих компонентов компьютера впервые было применено в американском суперкомпьютере Cray-2 еще в 1982 г.: платы этого суперкомпьютера были погружены в охлаждающую диэлектрическую жидкость. В дальнейшем технологии жидкостного охлаждения практически не развивали – можно сказать, создали работающий концепт и оставили «до поры». И вот пора пришла.

Небезызвестная компания IBM создала систему косвенного отвода тепла, суть которой в том, что наиболее «горячие» точки серверного оборудования контактируют с теплоотводящими пластинами. В результате объединения нескольких таких горячих точек и пластин получается вычислительный узел (рис. 4), который затем объединяется еще с несколькими серверами в полноценную серверную стойку. Данный подход обеспечивает съем тепла только с наиболее горячих компонентов, но многие другие остаются без внимания. Множество таких компонентов, включая проводники печатной платы, по которым течет ток, необходимо дополнительно охлаждать воздухом. Формирование каналов циркуляции воздуха внутри системы сказывается на ее общей плотности, хотя этот показатель у нее все же лучше, чем у систем с воздушным охлаждением. Но необходимость организации комбинированного охлаждения внутри сервера значительно усложняет и, скорее всего, увеличивает себестоимость этого подхода.

Решение, предложенное российской компанией «РСК Технологии», – тоже косвенная система охлаждения, но в ней используется всего одна охлаждающая пластина, которая полностью покрывает всю поверхность вычислительного узла (рис. 5). Этот подход обеспечивает полный теплосъем со всей площади компонентов узла, тем самым исключая лишние воздушные компоненты. Такая реализация отвода тепла позволила увеличить температурный перепад и за счет уменьшения расхода жидкости сделать систему более эффективной и максимально плотной.

Но в ассортименте систем жидкостного охлаждения есть решения не только с косвенным, но и с непосредственным охлаждением серверов. Производитель одной из таких систем – компания Iceotope. Ни для кого не секрет, что жидкости на основе воды нельзя использовать для непосредственного охлаждения процессоров и плат, для этого применяют жидкости-диэлектрики. В данном случае используется Novec 1230 от компании 3M. Тепло отводится через стенку емкости, в которую погружен сервер, к жидкости, далее отводящей тепло в атмосферу (рис. 6). Подход интересен тем, что диэлектрическая жидкость Novec 1230 за счет естественной конвекции внутри изолированного объема омывает все горячие компоненты. С другой стороны, пассивная конвекция в сочетании с необходимостью передачи тепла через стенку накладывает ограничения на мощность процессоров и энергетическую плотность такого решения.

Рис. 6. Жидкость-диэлектрик отводит тепло через стенку емкости, в которую погружен сервер

Другая разработка на основе погружения в жидкий диэлектрик принадлежит компании Green Revolution Cooling. Здесь оборудование погружается в жидкость GreenDEF, схожую по свойствам с трансформаторным маслом. Серверы помещаются в ванну с такими же габаритами, как у обыкновенной телекоммуникационной стойки, но расположенную горизонтально (рис. 7).

К очевидным недостаткам таких систем можно отнести охлаждение высоконагруженных компонентов с помощью потока вязкой жидкости. А взаимодействие гидрофильной жидкости с атмосферой подразумевает регулярные процедуры ее очистки и осушения. В то же время значительная масса и площадь горизонтально расположенного резервуара, заполненного теплоносителем, накладывает определенные ограничения на

Рис. 7. Серверы для охлаждения погружены в жидкий диэлектрик

выбор помещения. Но при всех перечисленных недостатках система имеет и ряд явных преимуществ, таких как возможность использования стандартных ИТ-компонентов в среде жидкого диэлектрика, низкая стоимость жидкости и простота конструкции, реализовать которую можно и не имея производственной базы.

■ ■ ■

Представленные в статье решения не единственные, но довольно показательные. К примеру, решения, аналогичные разработкам компаний IBM и «РСК Технологии», применяют и другие производители оборудования: Dell, Fujitsu, SGI и т.д. А к решениям, аналогичным системам Iceotope и Green Revolution Cooling, приходят другие группы разработчиков. У любого из них, будь то прямое жидкостное или косвенное охлаждение, есть свои достоинства и недостатки. Но выбор оптимального варианта, как и в случае с воздушным кондиционированием, должен быть индивидуальным. В каждом конкретном случае любой фактор может оказаться как преимуществом, так и недостатком.

Применение систем с жидкостным охлаждением в основном обусловливается потребностями заказчика. В 2012 г. о начале промышленной эксплуатации вычислительной системы с жидкостным охлаждением объявила европейская компания из нефтегазового сектора. В России наиболее яркий пример системы с жидкостным охлаждением в промышленной эксплуатации – Главный вычислительный центр Росгидромета.

Вероятно, в недалеком будущем в создаваемых коммерческих дата-центрах будет предусматриваться возможность установки систем как с воздушным, так и с жидкостным охлаждением. Тем более что технологическая база для реализации жидкостного охлаждения имеется, а преимущества таких систем уже не раз склоняли чашу весов в их сторону. ИКС

Опорные маршрутизирующие коммутаторы

MPLS-коммутаторы серии QSW-9800 – это высокопроизводительные скоростные 10G/40G-платформы, предназначенные для магистрального уровня сетей операторов, корпоративных сетей и End of Raw-уровня центров обработки данных. Коммутаторы поддерживают размещение до 384 портов 1G или 10G, имеют максимальную производительность коммутации до 2496 Гбит/с и пропускную способность до 1857 млн пакетов в секунду. Расширенная поддержка функций L2 и L3 обеспечивает высококачественное предоставление комплексных услуг нового поколения.

Модульная архитектура MPLS-коммутаторов, гибкость размещения портов на корпусе и их высокая плотность позволяют укомплектовать платформу для разнообразных условий. Качество услуг гарантируется широкой поддержкой QoS (восемь очередей на порт, функции SWRR/SP/WRR/WRED, классификации трафика на основе 802.1p CoS/ToS/DiffServ Traffic Shaping, PRI Mark/Remark).

Для обеспечения безопасности в серии QSW-9800 реализованы функции IEEE 802.1X (в том числе на основе MAC-адресов), RADIUS и TACACS + AAA, Anti-Sweep, защита от атак PING-DoS и DDoS, а также используются протоколы DHCP/ARP/PPPoE trustport, URPF и др. Балансировка нагрузки и отказоустойчивость достигаются поддержкой протоколов IEEE 802.1w RSTP, IEEE 802.1s MSTP, IEEE 802.3ad LACP, G8031/32 ERPS, что позволяет строить сети с избыточными линками и быстрой сходимостью, реализовать L2-распределение нагрузки на резервных линках и увеличивать полосу пропускания

за счет автоматического агрегирования нескольких физических линков.

Qtech: +7 (495) 797-3311

Трехфазные ИБП

ИБП серий SG и TLE производства GE Critical Power функционируют в режиме VFI и разработаны с учетом жестких требований к КПД. Благодаря резервируемой параллельной архитектуре мощность системы ИБП и уровень резервирования могут быть увеличены за счет параллельного подключения дополнительных устройств (до шести ИБП). ИБП SG и TLE поддерживают работу с АКБ различных технологий; для проверки состояния АКБ и контроля автономии используются функции SBM.

Режим экономичной работы eBoost обеспечивает снижение накладных расходов при соблюдении требований к качеству электропитания ответственных потребителей (например, в ЦОДе). Эта технология обеспечивает минимальное (менее 2 мс) время переключения на инвертор при выходе параметров напряжения за допустимые пределы. Отличие технологии eBoost в устройствах серий SG и TLE – возможность реализации этого режима работы как для одиночного ИБП, так и для параллельной системы.

Платы управления ИБП допускают установку дополнительного модуля «черного ящика» для регистрации быстропротекающих процессов внутри ИБП. Связь с внешними системами управления инженерным оборудованием объекта и диагностическим ПО обеспечивается с помощью интерфейсов RS232, контактов реле, протоколов SNMP и Modbus TCP/RTU.

ИБП серии SG мощностью 60–500 кВА выпускаются с выпрямителями, разработанными по технологии Purepulse. В них реализован алгоритм управления работой IGBT-выпрямителя, снижающий нелинейные искажения входного тока до уровня ниже 3%. Трансформаторная конструкция инвертора ИБП обеспечивает гальваническую развязку нагрузки и шины постоянного тока (АКБ), выравнивает токи в плечах инвертора даже при несимметричной нагрузке, гарантирует более высокий ток в режиме К.З. и незагруженную нейтраль.

Серия TLE имеет мощности 160–400 кВА/кВт. КПД этих ИБП в режиме двойного преобразования достигает 96,5% и 99% – в режиме eBoost. В базовой комплектации устройства имеют цветной сенсорный дисплей с поддержкой русского языка, встроенную защиту от обратного тока и сервисный байпас.

«Абитех»: +7 (495) 234-0108

Аккумулятор для гибридных телекоммуникационных систем

Аккумулятор PowerSafe SBS, предназначенный для эксплуатации в тяжелых нагрузочных и циклических режимах работы, расширяет номенклатуру продуктов, созданных на базе технологии EON. В PowerSafe SBS наряду с известными технологиями EnerSys применяются технология тонких пластин из чистого свинца (TPPL) и корпуса OPzV в соответствии со стандартом DIN. Также предусмотрено увеличение удельной емкости до 50% в сравнении со стандартными герметизированными необслуживаемыми свинцово-кислотными аккумуляторами VRLA. Аккумулятор разработан в соответствии с требованиями международного стандарта МЭК 60896-21/22.

Дополнительные характеристики:

- возможность ускоренного перезаряда;
- высокий показатель объемной и гравиметрической плотности энергии;
- высокая работоспособность в циклическом режиме;
- широкий диапазон рабочих температур;
- срок хранения благодаря низкой скорости саморазряда достигает 24 месяцев (при температуре 20°C) – по сравнению с 6 месяцами для элементов OPzV;
- устойчивость к тяжелым условиям эксплуатации (расчетный срок службы – 15 лет при температуре 20°C).

Официальный запуск продукта назначен на вторую половину 2013 г. Планируется введение серии одноэлементных аккумуляторов напряжением 2 В с диапазоном емкости от 320 до 900 Ач.

EnerSys: +7 (495) 925-5648

Сетевые накопители для бизнеса и 10GE-сетей

Накопители TS-870U-RP и TS-1270U-RP из бюджетной серии TS-x70 предназначены для решения таких ресурсоемких задач, как высокоскоростное резервирование больших объемов данных в виртуализированных средах и сетевая обработка HD-мультимедиа.

Обе модели выполнены в стоечных корпусах высотой 2U с восемью и 12 запираемыми hotswap-слотами для жестких дисков соответственно. Поддерживаются винчестеры формфактора 2,5" и 3,5" с интерфейсом SATA I/II/III объемом до 4 Тбайт. Аппаратное обеспечение базируется на двухъядерном процессоре Intel с тактовой частотой 2,4 ГГц и оперативной DDR3-памяти объемом 4 Гбайт с возможностью увеличения до 16 Гбайт. Набор интерфейсов включает два порта Gigabit Ethernet, два разъема USB 3.0, четыре разъема USB 2.0, два слота eSATA, а также два слота для дополнительных сетевых карт, в том числе с портами 10GbE. Каждое устройство укомплектовано двумя встроенными блоками питания для резервирования и двумя тихими вентиляторами (7 см, 12 В).

Вместе с полной поддержкой кроссплатформного доступа к файлам и интерфейса iSCSI, сетевые накопители могут использоваться в виртуализированных средах на основе программных платформ VMware vSphere, Citrix XenServer и Microsoft Hyper-V. Устройства официально сертифицированы по программе VMware Ready для работы с гипервизором ESXi 5, совместимым как с vSphere 4, так и с vSphere 5, а также поддерживают комплекс технологий VAAI.

QNAP: +7 (495) 587-7627

ИБП для виртуализированных сред

Линейно-интерактивные ИБП Eaton 5P имеют мощность от 650 до 1550 ВА, КПД до 98% и формируют на выходе чистый синусоидальный сигнал. Встроенная функция измерения мощности позволяет точно измерить энергию, подводимую к нагрузке. Кроме того, ИБП оснащены функцией сегментации нагрузок, которая дает возможность отключать неприоритетные нагрузки, продлевая время работы основных систем при отключении электропитания. ИБП имеют графический ЖК-дисплей, на котором в реальном времени отображается подробная информация о состоянии системы.

ИБП 5P поставляются с ПО Eaton Intelligent Power, которое обеспечивает простую интеграцию с платформой управления виртуализацией VMware vCenter Server и платформами виртуализации с открытым исходным кодом, включая Citrix XenServer, Microsoft SCVMM, Red Hat и др. При отключении электропитания эта интеграция обеспечивает автоматический и прозрачный для пользователя перенос виртуальных машин на не затронутые отключением серверы, а также корректное завершение работы виртуальных машин и серверов в случае продолжительного отключения.

Eaton: +7 (495) 981-3770

Реклама в номере

Указатель фирм

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.