Обгоняя растущий рынок

В феврале российский рынок акций – включая и телеком-сектор – чувствовал себя достаточно уверенно, хотя и замедлил темпы роста. С наступлением же первого весеннего месяца на рынке усилилась волатильность в преддверии президентских выборов.

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

Однако итоги президентской кампании и признание В.В. Путина победителем выборной гонки не оказали существенного влияния на биржевые индексы, поскольку эти результаты преимущественно уже были заложены в рыночных ценах. Поддержку отечественным площадкам оказало разрешение проблемы реструктуризации греческого долга и выделение Афинам очередного финансового транша помощи от Евросоюза.

Операторы подводят итоги

Бумаги российского телекоммуникационного сектора пользовались высоким спросом у инвесторов во многом благодаря своим традиционным защитным свойствам. Восходящая динамика наблюдалась в акциях МТС, которые в итоге прибавили в цене 6,68% – до 233,5 руб. Причиной роста послужила публикация позитивной отчетности по итогам 2011 г. по US GAAP, согласно которой консолидированная выручка оператора выросла на 9,1% – до $12,3 млрд. Чистая прибыль за прошлый год достигла $1,44 млрд, что на 5% выше показателя 2010 г. Показатель OIBDA в 2011 г. вырос на 5,6%, до $5,14 млрд; рентабельность по OIBDA – 41,8%. Чистый денежный поток компании за 2011 г. был равен $1,026 млрд. Капитальные затраты группы МТС за тот же период составили $2,585 млрд или 21% от выручки компании.

Акции «Ростелекома» потеряли за месяц 1,04%, остановившись на отметке 150,02 руб. Просадка бумаг оператора началась во второй декаде февраля и продлилась до первой декады марта (по итогам торгов 7 марта они откатились к отметке 143 руб. за акцию). Оттолкнуться от минимума котировкам помог ряд корпоративных новостей: во-первых, информация о том, что «Ростелеком» завершил сделку по приобретению 28,2% акций ОАО «НТК» за 13,8 млрд руб. В результате с учетом 71,8% акций, купленных в феврале 2011 г., стоимость приобретения 100% акций ОАО «НТК» составила 41,7 млрд руб. Эффект от полной интеграции группы «НТК» оценивается примерно в 2 млрд руб. в период до 2015 г. Во-вторых, у акций ОАО «Ростелеком» появился новый долгоиграющий драйвер роста – планы оператора совместно с большой тройкой создать единую инфраструктурную компанию, куда будут переданы антенно-мачтовые сооружения участников проекта.

Распродажи были зафиксированы и в бумагах VimpelCom Ltd, которые за рассматриваемый период потеряли 4,67%, снизившись до отметки в $11,42 за акцию. И если вторую половину февраля акции компании еще находились в восходящем тренде, то в начале марта, после публикации отчетности за IV квартал 2011 г. по US GAAP, котировки поползли вниз. Чистый убыток Vimpelcom Ltd, включая ОАО «Вымпелком», составил $386 млн против чистой прибыли в $461 млн за аналогичный период 2010 г. При этом чистая прибыль Vimpelcom по итогам 2011 г. составила $488 млн, что на 71% меньше показателя предыдущего года ($1,673 млрд). Выручка Vimpelcom в IV квартале выросла в 2,1 раза, достигнув $5,87 млрд, а по итогам 2011 г. составила $20,25 млрд, что в 1,9 раза больше, чем год назад.

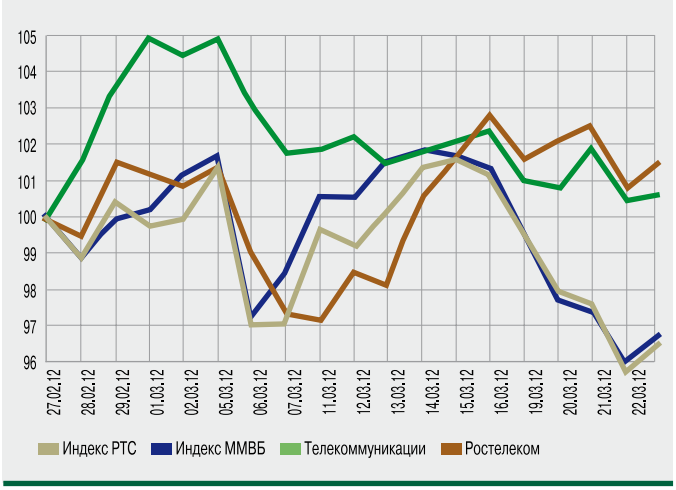
Неожиданный рекорд

Ростом на 12,55% завершили торги бумаги АФК «Система», закрывшиеся на уровне 29,6 руб. А поводом для этого ста-

Справка ИКС

За месяц, в период с 15 февраля по 15 марта, индекс ММВБ прибавил 4,13% – до 1626,63 пункта, индекс РТС вырос на 5,6%, до 1751,67 пункта. Отраслевой индекс ММВБ «Телекоммуникации» показал рост в 6,16%, остановившись на отметке 2 400,63 пункта.

Динамика биржевых индексов и индексов телекоммуникационных компаний в период с 27 февраля по 22 марта 2012 г.



ла информация о планах компании выкупить свои акции с открытого рынка. Менеджмент «Системы» считает, что, несмотря на рост стоимости на 20–30% со времен выкупа, проведенного осенью 2011 г., капитализация компании по-прежнему ниже стоимости ее активов. Вопрос о начале нового выкупа бумаг пока обсуждается только на уровне менеджмента и еще не выносился на совет директоров.

В свою очередь, акции входящего в АФК «Система» концерна «Ситроникс» за месяц потеряли 1,89%, снизившись в цене до $0,52 за шт. Поводом для падения послужило решение РТИ, дочернего предприятия АФК «Система», выкупить 3,5 млрд акций, или 36,9% уставного капитала «Ситроникса». Тем самым РТИ планирует консолидировать 100% акций компании (напомним, что в настоящий момент РТИ принадлежит 63,07% ее акций, в свободном обращении – 17,82%). Оферта будет выставлена миноритариям «Ситроникса» после получения одобрения ФСФР.

Скромный прирост капитализации показал российский холдинг IBS Group. Его акции подорожали на 1,92%, до отметки $18,85. Акции компании росли на позитивной отчетности за III квартал 2011 г.: консолидированная выручка IBS Group выросла на 26,3%, составив $277,3 млн. Другим хорошим поводом для роста акций могли послужить планы вывода компании Luxoft на IPO. Однако не слишком успешное февральское размещение конкурента Epam, вероятно, заставило IBS пересмотреть эту идею и перенести сроки.

Рекордный рост показали акции РБК: они прибавили 49%, превысив отметку в 23,234 руб. за акцию. Котировки этих бумаг нарисовали три ярко выраженные белые «свечи», за одну торговую сессию они набирали более 12% капитализации, причем в отсутствие каких-либо значимых новостей. В остальном же котировки акций РБК двигались умеренными темпами. Среди корпоративных новостей стоит отметить решение медиахолдинга продолжить наращивать структуру за счет перспективных активов. Так, РБК заинтересовался динамично растущим рынком купонных сервисов – компания приобрела 33% акций в «КупонГиде», с планами дальнейшего увеличения пакета до 73% в течение двух лет.

Новые вершины интернет-компаний

Благоприятно проходили торги для публичных российских интернет-компаний. В частности, высоким рыночным спросом пользовались акции Mail.ru Group – они выросли до отметки $38,93, прибавив 14,5%. На покупки инвесторов спровоцировала публикация сильных результатов за 2011 г., согласно которым суммарная сегментная выручка Mail.Ru выросла на 58,6% – до $514,9 млн, а чистая прибыль компании увеличилась в 2,5 раза, до $207,6 млн. Показатель EBITDA за прошедший год вырос до $282,8 млн, свободные денежные средства компании по состоянию на 31 декабря 2011 г. составляли $154,3 млн. Ежемесячная аудитория портала Mail.Ru, по данным TNS Russia, в декабре 2011 г. достигла 30 млн российских пользователей.

Бумаги отечественного интернет-поисковика Yandex продолжили покорять новые вершины. Акции Yandex N.V. подорожали за месяц на 11,12%, до уровня $23,97, а с начала года бумаги компании прибавили около 22%. Поддержку им оказала публикация финансовых результатов за IV квартал 2011 г. и год в целом: выручка компании выросла на 60%, до $622,2 млн, чистая прибыль — на 51%, до $179,3 млн, однако рентабельность по чистой прибыли сократилась на 1,2 п. п. – до 28,8%. ИКС

Комплексные решения для ЦОДа в контексте CeBIT'2012

В этом году на выставке CeBIT было показано немало решений для дата-центров. Наиболее исчерпывающей стала экспозиция немецкой компании Rittal GmbH.

Уже много лет подряд каждую весну сотни тысяч людей со всего мира устремляются в немецкий город Ганновер, чтобы посетить одно из наиболее грандиозных мероприятий в жизни hi-tech-индустрии – выставку CeBIT. В этом году она собрала около 340 тыс. посетителей из 90 стран и более 4200 компаний, в том числе 94 из России.

Большое внимание на выставке было уделено центрам обработки данных. Наиболее масштабную экспозицию, посвященную этой теме, представила компания Rittal, которая отметила в прошлом году свой полувековой юбилей. Помимо решений для ЦОДов Rittal выпускает широкий ассортимент продукции, и для доставки экспонатов на выставку понадобилось 40 грузовиков, а общая площадь стенда компании превысила 2,5 тыс. м^2. За время работы CeBIT'2012 экспозицию Rittal посетили десятки тысяч человек.

В 2012 г. исполняется десять лет с момента открытия представительства Rittal в России. Rittal зарекомендовал себя на российском рынке с наилучшей стороны высоким качеством, разнообразием и продуманностью решений.

Корпусные системы и системы питания

Многим потребителям компания известна, в первую очередь своими серверными шкафами. В этом году на CeBIT Rittal впервые показала новую модификацию популярной модели шкафов TS 8 – TS IT, нагрузочная способность которой достигает полутора тонн на 19" плоскость. Изменена базовая комплектация: боковые стенки стали двухсекционными, задние двери – двустворчатыми, увеличена степень перфорации фронтальной двери (теперь она достигает 85% против 78% в предыдущей модификации). Установка основных аксессуаров в TS IT осуществляется быстро и без применения инструментов.

В составе экспозиции были и другие типы шкафов – компактные навесные (для операторов связи), всепогодные, антивандальные, со встроенными системами активного охлаждения и др. Также демонстрировались многочисленные модели открытых стоек для телеком-сферы. Отметим, что в рамках партнерских соглашений Rittal выпускает шкафы для таких компаний, как Dell, Cisco, HP, IBM, NetApp.

На CeBIT'2012 компания Rittal показала разнообразные модели ИБП и систем распределения электропитания. В их число вошли новые модульные источники PMC120 мощностью до 120 кВт, которые благодаря относительно небольшому размеру, энергоэффективности, надежности и сниженной по сравнению со старшими моделями стоимости могут использоваться в дата-центрах любого уровня. Что касается давно зарекомендовавших себя модульных ИБП Rittal для ЦОДов серии PMC200, то их мощность может достигать 200 кВт. При этом до пяти источников могут быть объединены в общую систему, что позволяет достичь мощности до 1 МВт.

На отдельном стенде экспонировались новинки – вертикальные модули распределения питания PDU. Имеется широкий выбор модулей – с разными количеством и типами розеток. Каждый тип PDU может быть выполнен в четырех вариантах: базовом (только распределение питания), с измерением (появляется возможность измерения тока на каждой фазе и суммарной мощности), с переключением (добавляется возможность управления отдельными блоками розеток) и с полным управлением (добавляется еще возможность измерения и управления для каждой розетки). Все модули с возможностью измерения могут подключаться к сети Ethernet и удаленному мониторингу. Также функционал модулей можно расширить путем подключения к ним датчиков системы CMC III. Кроме PDU на выставке была представлена новая версия классической шины PSM, адаптированной для работы с новой системой CMC III.

Системы охлаждения и мониторинга

На стенде Rittal демонстрировалась новая уникальная модель внутрирядного прецизионного кондиционера LCP CW InLine. На данный момент это самая мощная система охлаждения такого типа и размера из представленных на рынке. Судите сами: при габаритах 300×2000×1200 мм система может отвести до 60 кВт тепла. Предыдущая модель обладала вдвое меньшей холодопроизводительностью. Благодаря специальной системе распределения воздуха охлажденный поток подается в стороны по всей высоте кондиционера. В результате оборудование, размещенное в шкафах, охлаждается равномерно, независимо от того, на какой высоте оно находится. Модуль охлаждения LCP CW InLine оснащен шестью вентиляторами, каждый из которых отводит до 10 кВт тепла и может быть заменен в «горячем» режиме. Подобная конструкция дает возможность добавлять вентиляторы по мере роста тепловой нагрузки в дата-центре. Кондиционеры снабжены контроллерами управления и встроенным ПО, что

позволяет интегрировать их в общую систему мониторинга и управления ЦОДа. Посредством SNMP они могут взаимодействовать со всеми популярными системами удаленного управления. Для тех, кто предпочитает решения от одного производителя, Rittal предлагает собственную комплексную систему мониторинга и контроля инфраструктуры ЦОДа под названием RiZone. Для повышения эффективности охлаждения дата-центра компания выпускает системы изоляции «холодного коридора», которые могут применяться в сочетании с внутрирядными или зальными кондиционерами.

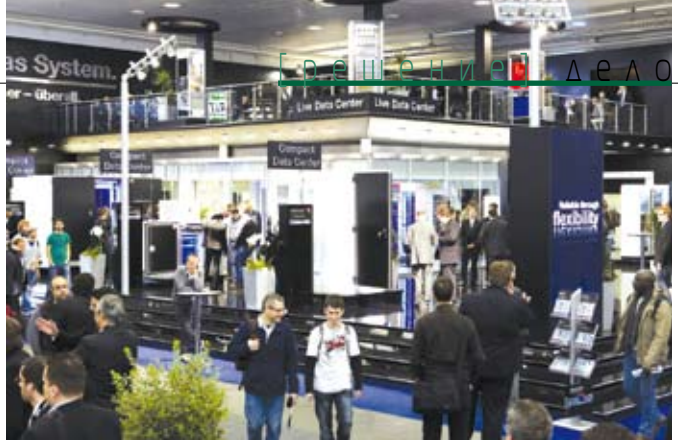
Надежность кондиционеров LCP CW InLine обусловлена не только качеством каждого отдельного компонента, но и резервированием наиболее критичных компонентов. Потенциальной точкой отказа является только контроллер управления, что, кстати, характерно для всех присутствующих на рынке внутрирядных кондиционеров. В упомянутых решениях Rittal эта проблема решена весьма оригинальным способом. В случае выхода из строя системы микропроцессорного управления LCP не теряет функциональности. При отказе контроллера управления кондиционеры автоматически включаются на полную мощность и одновременно с этим подают аварийный сигнал по всем доступным каналам.

Такая же схема действует и для чиллеров, которые Rittal разрабатывает и производит самостоятельно. Холодопроизводительность одной машины достигает 0,5 МВт, восемь чиллеров могут быть объединены в общую систему с централизованным управлением. Отметим, что холодильные машины Rittal поддерживают функцию фрикулинга, что значительно повышает их энергоэффективность. На CeBIT'2012 компания Rittal представила несколько собственных моделей зальных кондиционеров мощностью до 108 кВт (на водяном охлаждении) и 54 кВт (на фреоне).

Для организации эффективного охлаждения в наборе решений Rittal есть еще одна интересная разработка – пассивный теплообменник LCP Passive, устанавливаемый вместо задней двери шкафа и способный отвести до 20 кВт тепла. В этом решении нет собственных вентиляторов, вместо них используются те, что есть в активном оборудовании.

Другая важная новинка – компактная система мониторинга CMC III для ЦОДа. В основе решения – управляющий (процессорный) блок, использующий шину CAN Bus, к которому можно подключить до 32 различных датчиков – температуры, влажности, задымления, открывания дверей и др. В предыдущей модели – CMC-TC – для подключения датчиков требовались специальные промежуточные блоки, теперь все датчики передают информацию и получают питание по CAN-шине. Процессорный блок имеет возможность питаться как от сети переменного тока (при помощи блока питания), так и с помощью PoE. Он подключается по SNMP или каналам Ethernet к рабочему месту оператора либо интегрируется в комплексную среду мониторинга ЦОДа. Центральный блок CMC III может быть подключен к двум источникам электропитания и содержит встроенные датчики температуры и доступа. Дополнительно может быть установлена SD-карта для записи и хранения истории событий.

Все упомянутые разработки могут использоваться как отдельно, так и в рамках целостной концепции построения ЦОДа, которая известна под торговой маркой RimatriX. Отметим, что в отличие от некоторых конкурентов, которые также предлагают комплексные решения для дата-центров, Rittal производит и собственные системы пожаротушения на безопасном веществе Novec 1230, которые тоже можно было увидеть на стендах CeBIT'2012.



Преимущество комплексных решений

В последние несколько лет Rittal активно развивает направление готовых комплексных решений для создания инженерной инфраструктуры ЦОДа. В рамках концепции выпускается целая серия интересных решений, рассчитанных на потребителей разного масштаба. В этом году в рамках выставочной экспозиции компания представила пять таких систем.

Комплексное решение начального уровня – мини-ЦОД в «коробке» – рассчитано в первую очередь на операторов связи. Это вандалозащищенный сейф полезной емкостью 15U. Корпус шкафа отвечает требованиям IP55 и WKII (по взломостойкости), а также обеспечивает защиту от пожара класса F90 в соответствии с DIN 4102 (30 мин в пределах значений стандарта EN 1047-2). Кроме стойки для оборудования там размещается вся необходимая инфраструктура – кондиционер холодопроизводительностью до 4 кВт, ИБП мощностью до 3 кВА, системы мониторинга и пожаротушения. Есть и более емкие решения, позволяющие разместить внутри защищенного сейфа до 47U оборудования.

Rittal предлагает подобные комплексные решения и для установки в помещении. В этом случае система может состоять даже из нескольких шкафов с общими системами охлаждения, мониторинга, ИБП.

■ ■ ■

Развитие индустрии цодостроения в мире идет в сторону предложения комплексных решений от поставщика, имеющего компетенции во всем спектре инженерных систем ЦОДа. Такие решения позволяют удовлетворять высокие требования заказчиков по надежности, масштабируемости, управляемости, энергоэффективности, удобству эксплуатации и срокам реализации проектов. Продемонстрированные в нынешнем году на выставке решения Rittal полностью подтверждают эту тенденцию и открывают новые возможности в создании такого сложного продукта, как центр обработки данных.

Двое на одном стуле

Ситуация парадоксальная: одна и та же область общественных отношений сегодня находится под контролем сразу двух органов исполнительной власти – Федеральной антимонопольной службы (ФАС) и Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор).

Алексей МИШУШИН

Уж сколько копий сломано в полемике о чрезмерных контроле и надзоре, установленных над российским бизнесом! Связь и телекоммуникации по степени внимания государственных органов к деятельности участников рынка давно стали притчей во языцех. Но в некоторых сферах даже знатокам телекома скучать не приходится, так много здесь открытий приготовили нам отечественное регулирование и судебная практика.

В соответствии с п. 5 Положения, утвержденного Постановлением Правительства РФ от 30.06.2004 № 322, Роспотребнадзор осуществляет надзор и контроль за исполнением обязательных требований законодательства Российской Федерации в области.... защиты прав потребителей и потребительского рынка, в том числе:

- государственный контроль за соблюдением законов и иных нормативных правовых актов Российской Федерации, регулирующих отношения в области защиты прав потребителей;
- контроль за соблюдением правил продажи отдельных предусмотренных законодательством видов товаров, выполнения работ, оказания услуг.

Перечисленного достаточно, чтобы понять, что рассмотрение любых нарушений Правил оказания услуг связи, будь то телематические услуги или услуги кабельного телевещания и др., относится к компетенции Роспотребнадзора. Необоснованно приостановил предоставление абоненту услуг местной телефонной связи или выставил счет на неожиданно высокую для абонента сумму? Включил в договор с абонентом условие о необходимости получения утраченного счета в офисе оператора связи? Манипуляции с тарифами на услуги? Будь готов объяснить свою позицию надзорному органу. И если оказался неправ, ответишь по всей строгости КоАП РФ.

Но вот в чем фокус. Заметная часть подобных нарушений может также стать предметом разбирательства, возбужденного антимонопольной службой, которая согласно Положению, утвержденному Постановлением Правительства РФ от 30.06.2004 № 331, является уполномоченным федеральным органом исполнительной власти, осуществляющим функции по принятию нормативных правовых актов и контролю за соблюдением антимонопольного законодательства. Поскольку в соответствии с п. 1 ст. 10 ФЗ «О защите конкуренции» запрещаются действия (бездействие) занимающего доминирующее положение хозяйствующего субъекта, результатом которых являются или могут являться недопущение, ограничение, устранение конкуренции и (или) ущемление интересов других лиц, антимонопольный орган может взять к своему производству самые разнообразные дела, в которых обнаружит «ущемление интересов других лиц».

Напрашивается вопрос: каких именно интересов? Каких именно «других лиц»? Нет ответа в законодательстве!

Пояснение пришло из зала суда. В постановлении Президиума Высшего арбитражного суда РФ от 05.04.2011 № 14185/10, принятом по спору ОАО «РЖД» с ФАС, говорится: согласно Указу Президента РФ от 09.03.2004 № 314 «О системе и структуре федеральных органов исполнительной власти» ФАС России переданы функции по контролю и надзору упраздненного Министерства по антимонопольной политике и поддержке предпринимательства за исключением функции в сфере защиты прав потребителей, которая наряду с функцией по контролю и надзору в сфере санитарно-эпидемиологического надзора передана Федеральной службе по надзору в сфере защиты прав потребителей и благополучия населения.

Проще говоря, Президиум ВАС РФ признал неправомерной попытку ФАС вторгнуться в компетенцию Роспотребнадзора в области потребительского рынка и защиты прав потребителей при одновременном отсутствии со стороны правонарушителя действий, влекущих недопущение, ограничение, устранение конкуренции или нарушающих законодательство о естественных монополиях. Высший судебный орган, по сути, ограничил ФАС в возбуждении дел по жалобам потребителей, не связанным с вопросами конкуренции или нарушением законодательства о естественных монополиях. А таких дел в практике ФАС много, и в ряде случаев правонарушителю может грозить оборотный штраф, исчисляемый сотнями тысяч, а иногда и миллионами рублей.

Решение суда совершенно логично и естественно, хотя оно не является решением описанной правовой коллизии (постановлением суда закона не перешибешь!). ИКС

FMC в эпоху универсализации

Технологическая и сервисная конвергенция – одна из очевидных целей универсализации бизнеса операторов. Однако сказать, что этот тезис подтвержден жизнью, пока нельзя. Стал ли былью миф о FMC? Или ее удел – оставаться блестящей пряжкой на портфеле большого бизнеса? Практика универсальных операторов дает на эти вопросы разные ответы.

Четыре года назад и отнюдь не в первый раз «ИКС» писал («Fixed Mobile Convergence по-русски», см. № 1'2008) о том, что ни операторы, ни производители терминальных устройств, ни потенциальные потребители не готовы к реализации концепции Fixed Mobile Convergence.

За прошедшее с тех пор время ситуация изменилась: в результате сделок M&A операторы мобильной связи стали универсальными, объединив свои сети с сетями приобретенных фиксированных игроков, появились iPhone и iPad, создается инфраструктура для облачных сервисов.

Что представляет собой конвергенция в новом контексте операторского бизнеса? «Сегодня FMC-услуги предлагаются большой тройкой в корпоративном сегменте, – комментирует Максим Савватин, аналитик iKS-Consulting. – Дальше всех продвинулся по этому пути «ВымпелКом», поскольку первым по нему пошел. «МегаФон» (с учетом «Синтерры»), у которого конвергентные услуги только появляются, сильно активизировался в бизнес-сегменте. МТС пока готовит почву для конвергенции, не более того».

И операторы и аналитик сходятся во мнении, что до сих пор рынок конвергентных услуг остается непрозрачным, единообразных методик подсчета не выработано, как, впрочем, и общепринятого определения понятия «конвергентные услуги».

Есть и достижение – спрос корпоративных заказчиков на FMC-сервисы. «Спрос на конвергентные услуги сейчас большой, – отмечает М. Савватин, – причем не только у крупных корпораций, но и у SMB-компаний».

В настоящее время наличие таких сервисов в продуктовом предложении оператора – признанный всеми эффективным инструмент привлечения новых клиентов и удержания уже имеющихся. Превратятся ли они наконец в генератор дополнительной выручки ставших теперь универсальными операторов?

Конвергенция начинается с бизнес-модели

НИКОЛАЙ МАЗУР

В гонке универсализации «МегаФон» стартовал третьим, предусмотрительно пропустив вперед двух конкурентов. Результат объединительных процессов – переход оператора к новой посегментной бизнес-модели. Что она собой представляет? – спросили мы у Николая МАЗУРА, руководителя департамента по управлению продуктами для федеральных корпоративных клиентов и операторов связи ОАО «МегаФон».

– В рамках новой бизнес-модели был сформирован объединенный маркетинг «МегаФона» и «Синтерры» для сегментов B2B, B2G и B2O. Именно в его структуре сегодня разрабатываются и реализуются продукты для каждого из них.

Переход к этой модели потребовал проведения работ и по объединению сетей обеих компаний, и по передаче части клиентов «Синтерры» в «МегаФон». И хотя у мобильного оператора к тому времени уже была своя магистральная сеть, его отдельные филиалы предоставляли услуги фиксированной связи, а некоторые – и конвергентные услуги, первоочередной нашей задачей была реализация в «МегаФоне» всех продуктов, которые были доступны в «Синтерре». Поскольку за основу брались наработки «Синтерры», это удалось сделать быстро. Потребовалось лишь решить технические вопросы, необходимые для запуска тех или иных услуг фиксированной связи.

– Клиенты из каких бизнес-сегментов остались в «Синтерре»?

– Перед «Синтеррой» стоит стратегическая задача ускоренного развития сегмента B2G, который является ее отдельной от «МегаФона» компетенцией. При этом как часть объединенной компании «Синтерра» предоставляет госзаказчикам услуги мобильной связи от имени «МегаФона» по агентской схеме. Такая организация работы способствует тому, что менеджеры объединенной компании постепенно становятся универсальными.

– Какие конвергентные продукты, объединяющие возможности сетей мобильной и фиксированной связи, появились в результате универсализации бизнеса оператора?

– Наличие двух сетей, при взаимодействии которых не требуется производить прямые выплаты другим операторам (интерконнект), позволило нам предложить клиентам, пользующимся мобильной и фиксированной связью от «МегаФона», совершать звонки «внутри себя» по льготной цене. Нашу услугу «Корпоративный прио-

ритет» можно рассматривать как «легкую», «тарифную» конвергенцию. Что касается более глубокой, «технологической» конвергенции, то, для примера, мы даем возможность клиенту с мобильного телефона звонить по короткому номеру на фиксированный телефон и обратно, оптимизируя тем самым его бизнес-процессы.

– Как бы вы оценили спрос корпоративных клиентов на конвергентные продукты?

– Спрос нужно формировать, потому что изначально его нет, это с одной стороны. С другой стороны, наличие таких услуг очень важно в работе с нашими клиентами, которые стремятся оптимизировать свои телеком-бюджеты, а иногда и отличаться от конкурентов инновационными решениями, созданными «только для них». Поэтому мы и взращиваем у себя такую компетенцию. По сути, конвергентные услуги сегодня – это дополнительная возможность привлечь клиента и удержать его в своей базе.

– Какие перспективные конвергентные продукты могут изменить эту ситуацию?

– По большей части все наши идеи таких услуг связаны с оптимизацией бизнес-процессов клиента и удовлетворением его запросов, например на удаленное управление объектами, их мониторинг посредством SIM-карт, на определение местоположения его сотрудников, транспортных средств и т.д. или на организацию физического доступа с использованием QR-кодов или технологии NFC.

В конце 2011 г. была создана 100%-ная дочерняя компания «МегаФона» – MegaLabs. Это экспериментальная площадка, в задачи которой входят разработка и быстрый вывод на рынок инновационных продуктов и услуг в смежных с мобильной связью сегментах.

– Каковы, на ваш взгляд, обязательные условия успешной универсализации оператора?

– Нужно дать клиенту «единую точку входа», поддержав ее неким набором продуктов и решений. На достижение этой цели должно быть направлено все: и система продаж, и система обслуживания и поддержки клиентов, и информационные веб-ресурсы.

Конвергенция растет, как мобильный Интернет

ЕВГЕНИЯ ГРИГОРЬЕВА

Для «ВымпелКома» путь к универсализации начался чуть ли не десять лет назад с предоставления FMC-услуг в партнерстве с компаниями «Голден Телеком» и «Эквант». О том, как развивается это направление сегодня в рамках единого интегрированного оператора, рассказывает Евгения ГРИГОРЬЕВА, руководитель департамента по продуктам мобильной связи бизнес-сегмента ОАО «ВымпелКом».

Объединение сотовой и фиксированной сетей в рамках универсального оператора сняло ограничения на функционал FMC-услуги, которые имела партнерская схема. Оно позволило нам предоставить компаниям, пользующимся нашими услугами фиксированной и мобильной связи, льготные условия тарификации. В конце 2011 г. в ряде регионов мы запустили услугу «Единый межгород», подключив которую клиент получает возможность совершать международные и междугородные звонки с фиксированных и мобильных телефонов по единой цене.

Также мы смогли обеспечить дальнейшее технологическое развитие конвер-

Унифицированный биллинг как основа конвергенции

Компания МТС готовится предоставить абонентам, пользующимся его услугами фиксированной и мобильной связи, возможность оплачивать их по единому счету. Важным шагом в этом направлении стал перевод абонентов всех филиалов компании «Комстар-Регионы» на унифицированную биллинговую платформу.

Внедрение решения LANBilling Supervise на всей территории действия компании «Комстар-Регионы», т.е. более чем в 100 городах России, позволило обеспечить единые стандарты обслуживания абонентов фиксированной связи группы МТС, в том числе «единую точку входа» для их коммуникаций с оператором.

Теперь пользователи услуг проводного ШПД и платного телевидения смогут контролировать баланс лицевого счета, решать вопросы с кредитованием, заказом услуг и изменением их набора в контактном центре МТС или в любом из салонов оператора по всей России. А оператор получил возможность в кратчайшие сроки запускать общефедеральные маркетинговые программы, делать абонентам выгодные предложения, включая пакетные, ориентируясь на единый стандарт качества и обслуживания.

Таким образом, переход на унифицированную интеграционную биллинговую платформу стал своего рода подготовкой почвы для оказания конвергентных услуг абонентам МТС – физическим лицам на основе единого счета.

Что касается подобных услуг для корпоративных пользователей, то их потребности в конвергентных решениях оператор удовлетворяет, создавая индивидуальные комплексные решения на базе стандартизованных продуктов «@втосекретарь», FMC, VPBX. Вектор их развития направлен в сторону стирания границ между фиксированной и мобильной составляющими услуги. Цель – предоставить клиенту виртуальные сервисы, позволяющие объединить все его терминалы, реализовав возможность доступа к ним как из мобильной и фиксированной сетей связи, так и через Интернет.

По материалам, подготовленным пресс-службой МТС

гентных услуг, расширение их функционала для клиентов из разных отраслей и пошли в сторону предоставления комплексных решений. Для банков, например, которые сейчас расширяют сети мини-офисов по всей стране, мы пакетируем FMC-услугу с сервисом BlackBerry. В результате появляется комплексное решение: доступ к почте и возможность по единой цене звонить по коротким внутренним номерам любому коллеге в пределах России.

При этом наш анализ профиля таких клиентов показывает, что они экономят до 30% затрат на связь, не уменьшая ни количества SIM-карт, ни количества стационарных телефонов – просто за счет оптимизации маршрута звонка.

Конечно, продавать FMC-услуги непросто, поскольку далеко не все компании могут сами оценить эффект, который от них получат. Мы целенаправленно проводим разъяснительную работу на примерах наших текущих FMC-клиентов – компаний с похожим профилем потребления из тех же отраслей. О том, что такой подход работает, свидетельствуют итоги 2011 г. Количество клиентов конвергентных услуг в «Билайн» Бизнес выросло на 65%, а выручка от них – на 74%. Темпы роста такие же, как и у мобильного Интернета, который вырос на 67% (в абсолютных цифрах прирост конвергентных услуг, конечно, более скромный), при том что с технической точки зрения FMC-услуги гораздо сложнее, требуют вовлечения топ-менеджмента, развертывания инфраструктуры, обучения людей. Принятие решения об их внедрении занимает в среднем четыре-шесть месяцев.

Сегодня у нас более 20 тыс. кросс-клиентов, примерно 8% нашей базы бизнес-клиентов, а начинали мы с 7–8 тыс. Понятно, что профили их абсолютно разные и показатель ARPU тоже разнится в зависимости от набора услуг и характера их потребления. Одно дело – совершать льготные звонки с фиксированного телефона на мобильный на короткие номера в сети «Билайн», другое – полностью задействовать возможности конвергентных услуг для всех корпоративных коммуникаций, дополнив традиционную фиксированную телефонию и заменив ими телефонию стандарта DECT.

Клиентов привлекают комплексные, законченные решения: это и голосовой тарифный план, и цена передачи данных, и скидки на оборудование, и многое другое в одном пакете. Конечно, в большинстве своем крупные корпоративные клиенты приходят к нам не только из-за наличия у нас услуги FMC. Но есть пул клиентов, которых мы получили благодаря конкурентным преимуществам как интегрированного оператора, и были случаи, когда благодаря наличию в портфолио услуги FMC мы выигрывали серьезные тендеры.

За рубежом сегодня движутся в сторону unified communications. В России еще рано говорить о готовности рынка к подобным сервисам, но потенциал с каждым годом растет. И мы готовимся к тому, чтобы предложить SMB-клиенту всё – и instant messaging, и передачу данных, и корпоративную почту, и короткую нумерацию. То есть создать вокруг него «поле» сервисов.

Подготовила **Александра КРЫЛОВА**

Регулирование 2.0
С точки зрения сервиса

Привычка есть привычка, ее не выбросишь за окошко,
а можно только вежливенько, со ступеньки на ступеньку, свести с лестницы.
Марк Твен

Современная инфокоммуникационная сеть позволяет сгенерировать любой сервис, поэтому инфраструктуру целесообразно отделить от сервисов законодательно, введя для них раздельное лицензирование. А появление новых сервисов у участников отечественного ИКТ-рынка надо всячески поощрять и поддерживать.

Александр ГОЛЫШКО,
канд. техн. наук

Общие принципы и немного магии

Мы уже неоднократно отмечали, что текущее отраслевое регулирование базируется на сепаратном сервисном лицензировании, выросшем из более чем векового узкоспециализированного сетевого строительства: «телефонного» или «телевизионного». А уж если передача данных, то как-нибудь поверх указанного выше. Наступающие в отрасли новые времена, о которых давно рассказывают не только специалисты, вышли из современных «всеядных» мультисервисных технологий, однако отраслевое лицензирование они пока не затронули. Последнее же действует по старинке: к лицензии на оказание услуг прилагается техническое дополнение с предписанием, каким именно способом эти услуги оказывать. И в результате значительная часть усилий лицензиата нацелена не на развитие сервиса, а на бюрократическое обоснование этого развития в рамках имеющихся или требуемых документов.

При этом большая часть операторов уже не ограничивается оказанием услуг голосовой телефонной связи, но обеспечивает и доступ в Интернет, и сопутствующие IP-сервисы. Поэтому предоставление ими собственных Voice & Video-over-IP сервисов – логичное расширение линейки операторского продуктового предложения.

Ну а никем не ограничиваемые интернет-компании еще раньше научились не только дублировать «традиционные» телекоммуникационные сервисы вроде телефонии и ТВ-вещания, но и добились определенных успехов в части их качества. С развитием ШПД последнее неуклонно растет. Следствий такой ситуации для «традиционного» телекомрынка два: потеря динамики потенциального операторского бизнеса и общий «конвергентный» ИКТ-проигрыш (т.е и оператора, и потребителей, и государства) от недополученных услуг и денег. Ведь над конкурентами из лагеря ИТ не стоят с занесенным топором регуляторы, а развитие ШПД только укрепляет их позиции. Так что же делать?

Первое, что часто приходит на ум, – запретить интернет-сервисы вместе с Интернетом. Однако человек разумный скорее вспомнит один из законов Мэрфи, гласящий, что если открыть банку с червями, то собрать их можно только в банку большего размера. Поэтому, прежде чем погружаться в дебри ИКТ-сервиса, давайте внимательно прочитаем три широко известных закона Артура Кларка:

1. Когда уважаемый, но пожилой ученый утверждает, что что-то возможно – он почти наверняка прав. Когда он утверждает, что что-то невозможно – он, весьма вероятно, ошибается.
2. Единственный способ обнаружить пределы возможного – отважиться сделать шаг в невозможное.
3. Любая достаточно развитая технология неотличима от магии.

Нетрудно видеть, что все вышесказанное как нельзя лучше относится к современным инфокоммуникационным сетям, у руля которых пока еще стоят если не ученые, то весьма сведущие люди. В этих сетях в настоящее время может быть сгенерирована абсолютно любая

услуга (точнее, не противоречащая законам физики, на которых основана сама сеть). На маркетинговом отрицании этого факта уже прогорело немало сетевых операторов. И если мы хотим заглянуть в будущее отрасли, мы должны экстраполировать существующие ИКТ-тренды в направлении самых эффективных средств коммуникации.

«Шаг в невозможное» регулярно совершают сервисные креативщики, из которых достаточно упомянуть коллег Стива Джобса. Приложения компании Apple вот уже несколько лет занимают значительную часть мирового рынка, включая, разумеется, и доходы.

Что же касается магии, то в процессе развития каждая технология становится незаметной для пользователя, которого по обыкновению более всего интересует соотношение цена/услуга. К хорошему привыкаешь быстро. А картины, возникающие сегодня с помощью неуловимых движений пальцев на экране смартфона, в самом деле могли показаться магией владельцу сотового телефона всего каких-нибудь 12–15 лет назад. Причем к магии относились бы как сами картины, так и движения пальцев. Не меньшее удивление вызвал бы у тогдашних сотрудников Минсвязи вопрос современного смартфона в ответ на попытку совершить звонок: «Как будем говорить – по ТфОП или через Skype?». В общем, сегодня подобная «магия» – обычное дело.

Итак, в современной и тем более будущей инфокоммуникационной сети можно сгенерировать любой сервис, о чем, впрочем, давно говорит нам концепция NGN. Поэтому в условиях такой сети (т.е. без фрагментов TDM и других рудиментов XX века), где все сервисы отделены от инфраструктуры, целесообразно и законодательно отделить инфраструктуру («трубу») от сервисов (контента, приложений и пр.) путем введения раздельного лицензирования – инфраструктурного и сервисного. Соответственно на рынке будут присутствовать как инфраструктурные операторы, так и сервисные. Причем никто не мешает инфраструктурным операторам иметь обе лицензии. Таким образом, сфера ИКТ-услуг разделится на чисто коммуникационные услуги, связанные с формированием инфраструктуры, и дополнительные услуги, включающие в себя все, что может быть доставлено поверх нее.

Инфраструктура общего пользования

Инфраструктурный оператор формально участвует в предоставлении любой услуги/сервиса и получает лицензию на создание инфраструктуры в виде сети передачи данных. То есть на создание современной мультисервисной инфраструктуры, а не, к примеру, телефонной или телевизионной сетей (именно это и следует контролировать надзорным органам). Заметим, что в условиях быстрого движения в направлении создания сетей All-IP телекоммуникационный регулятор может сконцентрироваться на весьма ограниченном перечне инфраструктурных (коммуникационных) услуг: присоединении сетей (причем без указания маршрута трафика), организации заказанного соединения и пропуска трафика, предоставлении инфраструктуры в аренду, обеспечении доступа к абоненту (ШПД), обеспечении качества предоставляемых услуг, роуминге и информационной безопасности. О двух последних услугах – подробнее.

Во-первых, в стране с такой территорией, как у РФ, существует необходимость организации межсетевого роуминга при отсутствии покрытия сети данного оператора в конкретном регионе. Во-вторых, по мере развития транспортных сетей операторов мобильной связи целесообразна поэтапная отмена внутрисетевого роуминга. Действительно, в настоящее время внутрисетевой роуминг позволяет поддерживать низкие тарифы на вызовы в домашнем (дотационном) регионе. С другой стороны, наличие внутрисетевого роуминга у оператора, позиционирующего себя в качестве глобального игрока, – нонсенс. Великие не должны размениваться на мелочи. Они строят сети будущего, а сеть будущего должна быть однородной с точки зрения получения любого сервиса в любой точке страны. И в целях стимулирования такого перехода регулятор может установить план поэтапной (по регионам) ликвидации внутрисетевого роуминга с тем, чтобы через три-четыре года операторы перестроили свои бизнес-процессы и это явление было ликвидировано в национальном масштабе.

Что касается информационной безопасности, то сегодня необходимо осознать ее неразрывную связь с понятием инфокоммуникационного сервиса. Отныне она – неотъемлемая составная часть IP-коммуникаций и IP-сервисов. В противном случае, с одной стороны, будет желание собирать деньги и ни за что не отвечать, а с другой – все это обеспечивать и довольствоваться оставшимся. И еще очевидно, что необходим концептуальный переход от понятия «сети связи общего пользования» к «инфраструктуре общего пользования».

Все остальные услуги/сервисы следует считать принадлежностью сервисного слоя: сервисного и контентного уровней, а также уровня приложений. Можно даже придерживаться следующей логики при обозначении услуг/сервисов: то, что сгенерировано на инфраструктурном уровне, называется услугой, а то, что вне его (т.е. на трех других уровнях), – сервисом. В результате инфраструктурные операторы могут предоставлять как услуги, так и сервисы, тогда как остальные провайдеры занимаются только сервисами. В целом же различия между так называемыми услугами связи и так называемыми информационными услугами должно постепенно стираться – ведь для всех них нужны сетевые ресурсы.

Сервисы как наше всё

Итак, применительно к сети будущего слой сервиса будет находиться в другой (глобальной) плоскости государственного регулирования. Подобный подход позволит «разгрузить» регулирование от излишней технологичности, справедливо критикуемой сегодня рыночным сообществом.

При этом следует иметь в виду, что основная «сервисная проблема» сетей будущего – не в регулировании какого-либо национального сервиса, а в разделе грядущего глобального сервисного пространства в масштабах планеты между национальными регуляторами.

Уникальность текущего момента в ИКТ-отрасли заключается в том, что современные операторы подобны советским женщинам эпохи развитого социализма, которые, как гласил известный анекдот, были озабочены двумя взаимоисключающими проблемами: как похудеть и где достать продукты. Точно так же операторы находятся в непрерывном поиске: чем наполнить свои сети и как увеличить их пропускную способность. О том же задумываются поставщики оборудования и ПО, в том числе занимающиеся облаками. Уже сегодня многие интернет-сервисы более чем успешно конкурируют с «традиционными» услугами (телефония, ТВ-вещание), а теряющие доходы «традиционные» инфраструктурные операторы чрезвычайно заинтересованы в диверсификации сервиса в сторону VAS.

Заветная мечта любого поставщика сервиса – создание «сервисного супермаркета». «Супермаркет» не у каждого получится, но с точки зрения государственных интересов следует приветствовать появление любого нового ИКТ-сервиса и соответствующего бизнеса. А тем временем сервисы (и «супермаркеты») становятся глобальными. К примеру, если до последнего времени немногие отечественные разработчики контента могли похвастаться наличием бизнеса за рубежом, то теперь любой продукт, попавший в магазин приложений, будет представлен по всему миру.

Быстрое развитие облачных сервисов стирает границы между чисто коммуникационными услугами и интернет-сервисами. Если в 2010 г. этот рынок в РФ составил $30 млн, то уже к 2015 г. может достигнуть $1 млрд (IDC). Сегодня практически всё может быть предложено клиенту в виде облачного сервиса: инфраструктура (IaaS), платформа (PaaS), ПО (SaaS), Web (WaaS), бизнес-процессы (BPaaS) и пр. и пр. В частности, сервисы, доступные по модели SaaS, предлагают клиентам услуги IP-телефонии, унифицированных коммуникаций и совместной работы над проектами.

Неожиданным следствием облачных вычислений может быть «смерть» прикладного программирования и подъем рядового пользователя до уровня поставщика сервисных приложений. Не исключено, что вскоре все пользователи станут потенциальными разработчиками, способными создавать собственные приложения по принципу Lego из кодов или программ, которые отыщут в Интернете самостоятельно. Таким же образом может измениться и сам Интернет – из инструмента, доступного только для чтения, благодаря развитию Web 2.0 он может трансформироваться в нечто другое, где каждый гражданин сможет писать, редактировать и вносить свою лепту в общее дело. В результате, как говорят специалисты, пользователи перестанут быть пассивными потребителями приложений и станут конечными пользователями-программистами. И это тоже серьезно расширит сервисное ИКТ-пространство.

Перспективные сетевые технологии предоставляют широкие возможности интеграции сервисов. Так, Unified Communications позволяют осуществлять прием и генерацию вызовов с любого терминала. Все сервисы могут быть кастомизированы под требования пользователей, причем будет доступна полная интеграция голоса, SMS, VoIP, IM и социальных сетей. В свою очередь, Unified Media дают пользователю возможность контролировать медийный поток. В частности, любой поток может быть принят на любом устройстве с адаптацией контента, а остановленный по какой-либо причине поток может быть возобновлен на другом устройстве. Подобные технологии нельзя разделить на отдельные услуги/сервисы – формально это просто мультисервис поверх скоростной сети передачи данных. Причем набор технологий, поддерживающих такое обслуживание, на самом деле не важен никому. А еще формально все эти «пируэты» незаконны – согласно действующему законодательству для каждой услуги должен быть свой отдельный терминал.

Порой XXI век наступает слишком быстро для многих «людей XX века», и они просто не успевают за сменой трендов и технологий. Взять хотя бы такую «древнейшую» связную услугу, как радиовещание. Как это было раньше? Радиочастоты, передатчики, комплексы студийной аппаратуры, хранилища аудиозаписей, инженеры, радисты и т.д. А что теперь? Интернет-вещание, которое хочешь – аудио, хочешь – видео. Многие УКВ-радиостанции вещают в Интернете. КВ-вещание целиком уходит в Интернет. Страшно представить – имея ШПД, вы имеете все вещание мира (и это, заметим, – реальное цифровое вещание). Практически любой ТВ-канал можно найти в Сети. Будущие пользователи ИКТ-услуг – наши дети – уже перестали смотреть в «тот самый ящик» (он у них другой, и гораздо лучше). Впрочем, современные телевизоры следуют за трендом, и теперь они вовсе не телевизоры, а компьютеры с дополнительной опцией приема ТВ-вещания. Существуют «радиостанции» и «ТВ-каналы», которые осуществляют свою деятельность исключительно в Интернете, а термин «радио» имеет лишь маркетинговое значение. Организовать собственную интернет-радиостанцию может любой желающий, поскольку не нужно никаких студийных комплексов, а в самом простом случае достаточно либо ПК и гарнитуры, либо сервера и некоего ПО. Все остальное есть в Сети или в голове «вещателя». А еще в Интернете имеется много ресурсов, которые предлагают стать «радиовещателями» всем желающим, и через них работают десятки «радиостанций». И попыток создать собственный канал интернет-ТВ с каждым годом будет предприниматься все больше. Прогноз таков – сотни миллионов людей во всем мире будут пробовать свои силы в создании собственной интернет-радиостанции, интернет-телестудии и собственного канала интернет-ТВ. Основную роль во всем этом будет играть не техника, а креативность, оригинальность, бренд и репутация, которые позволят им стать конкурентоспособными или хотя бы интересными какой-то группе слушателей/зрителей. И за-

метим, что ничто из перечисленного выше не может быть создано по приказу или за деньги.

Десять непрошеных советов

Ну а теперь, учитывая, что возглавить всегда продуктивнее, чем бороться, регулятору целесообразно сделать следующее.

- Оперативно снять существующие ограничения на предоставление инфраструктурных услуг (отмена зонового принципа, обязательных требований по присоединению сетей и пропуску трафика), поскольку они серьезно тормозят развитие всего «инфраструктурного крыла» ИКТ-отрасли.
- Перенести перекрестное субсидирование национальной инфраструктуры на фонд универсальной услуги (т.е. на оплачиваемое право доступа к ней всех субъектов рынка).
- Стимулировать инфраструктурных операторов не к созданию дополнительных преград сторонним поставщикам интернет-сервисов, а к развитию собственного сервисного пакета, т.е. вместо запретов нужна поддержка рыночной конкуренции.
- Приветствовать появление любого нового сервиса у любого сервис-провайдера, присутствующего на отечественном ИКТ-рынке, поскольку развитие ИКТ-сервисов является одной из основных целей современного государства.
- Установить и поддерживать универсальное и формализованное отношение регулятора к сервис-провайдерам, в роли которых могут выступать любые субъекты рынка – инфраструктурные операторы, MVNO, интернет-компании и даже физические лица без деления сервис-провайдеров по принципу мобильности, доминирующего положения на рынке и т.п.
- Постановить, что выдача отдельных лицензий на предоставление каких-либо услуг с точки зрения стимулирования ИКТ-отрасли (особенно в среде телеком-операторов) контрпродуктивна.
- Считать полезным для всей ИКТ-отрасли уравнивание в правах всех субъектов рынка в том, что касается создания любых ИКТ-сервисов, не нарушающих другие законы РФ (кроме «телефонного» закона «О связи»). Для выхода на указанный сервисный рынок всем им необходимо получить **единую мультисервисную лицензию, дающую право предоставлять любой сервис** (включая телекоммуникационные услуги, технологическая основа которых отныне не важна регулятору), а де-факто являющуюся просто **разрешением на доступ в национальную ИКТ-инфраструктуру со своими сервисами (любыми)**. Иначе говоря, подключился к «трубе» – имеешь определенные потенциальные возможности. Если «труба» «интеллектуальная» (со счетчиком), то ее владелец может выстроить с пользователем определенные отношения в части потребления ресурсов. Если «интеллекта» нет – это проблема владельца «трубы». Если работаешь поверх «трубы» (общедоступного Интернета) без лицензии, твой трафик может быть подвергнут ограничениям (вплоть до полной остановки или увеличения потери пакетов) любым инфраструктурным оператором.
- Считать наличие или отсутствие каких-либо услуг/сервисов у оператора не регуляторной проблемой, а дополнительной прибылью или упущенной выгодой сервис-провайдера. Это будет стимулировать диверсификацию сервисов при относительно равных возможностях участников ИКТ-рынка.
- Внести в лицензионные условия обязательства (их нужно разработать) обеспечения определенного уровня информационной безопасности с соответствующей ответственностью перед потребителем.
- Признать и установить «сетевое» равенство в обслуживании абонентов вне зависимости от их перемещения по территории РФ – одинаковые услуги должны иметь одинаковые тарифы, что будет означать отсутствие национального внутрисетевого роуминга, о чем говорилось выше.

В общем, ничего особенного. Просто воплощаются в жизнь идеи разработчика первых компьютерных программ Дж. Маккарти о том, что хранение и обработка информации однажды превратятся в коммунальную службу, и информация будет доступна так же, как вода, свет, газ. Очень скоро будет котироваться только одна ИКТ-услуга под названием «связь» в самом широком понимании этого слова. ИКС

Как организовать DNS в интересах блогосферы

Система доменных имен (DNS) – исключительно важный компонент инфраструктуры интернет-провайдера. Шрини АВЕРНЕНИ, вице-президент по защите интересов клиентов и инновациям компании Nominum дает пошаговые рекомендации по разработке, созданию и эксплуатации DNS-инфраструктуры в условиях активной блогодеятельности абонентов.

Шрини АВЕРНЕНИ

Для DNS обычно используются две формы организации – авторитетная (authoritative) и кэшированная (caching). Серверы авторитетной DNS содержат домены вида www.yourcompany.com и соответствующие ресурсные записи, а также, благодаря привязке имен хостов к их IP-адресам, информацию о месте их расположения.

Кэшированные серверы DNS помогают приложениям и сервисам – браузерам, VoIP, IPTV и пр. – перемещаться по иерархии DNS для нахождения соответствующего авторитетного сервера и в итоге – хостового компьютера искомого домена.

С чего начать?

При разработке и развертывании кэшированной DNS-инфраструктуры в первую очередь нужно прояснить следующие вопросы.

- Какому количеству абонентов планируется предоставить доступ к ресурсу? 100–150 тыс. на сервер – это типичный максимум для высокопроизводительного программного обеспечения, работающего на современной аппаратной платформе.
- Каким ожидается прирост абонентской базы? Хорошо бы увязать рост числа абонентов с циклом обновления оборудования (три-четыре года). Приняв максимальное число абонентов равным 100–150 тыс., можно высчитать их начальное число.
- Насколько распределенной хотелось бы видеть инфраструктуру? Обычно это определяется топологией сети. Размещение DNS-кластеров/серверов как можно ближе к конечным пользователям позволяет предоставить наилучший из возможных вариантов доступа в Интернет.
- Какие дополнительные функции (типа IPv6 или DNSSEC) должны быть задействованы?
- Какие дополнительные решения – например, редирект, идентификацию и подавление ботов – предполагается реализовать на платформе?
- Какие количественные показатели следует предоставлять внутренним системам? Какая связанная с DNS статистика собирается в настоящее время и будет ли полезна новая статистика, предлагаемая новой платформой?
- Есть ли планы развертывания новых услуг, которые станут факторами роста DNS? Каковы иные движущие силы роста бизнеса?
- Как служба эксплуатации будет управляться с новой инфраструктурой?
- Какие процессы и процедуры должны быть внедрены для поддержки новой (или обновленной) платформы?

Найдя ответы на поставленные вопросы (а, возможно, и на некоторые другие, обусловленные спецификой информационной среды), можно приступать к реализации своих планов. Так как возможно, что инфраструктура создается с нуля или модернизируется уже существующая, целесообразно проанализировать, как потребности бизнеса соотносятся со стоимостью и возможностями выбранного решения. Нужно учесть число абонентов и производительность системы, взвесить факторы, влияющие на качество, воспринимаемое абонентами, например время ожидания, а также стоимость.

Разработка и создание кэширующего DNS-сервера

Когда решения относительно масштабирования, допустимого времени ожидания и дополнительной функциональности, основанной на DNS, приняты, можно переходить к следующим уровням детализации системы.

Аппаратная платформа. Потребуется быстрая процессорная архитектура Intel/AMD. Оперативная память – 2 Гбайт. Но если планируется реализовать дополнительные функции – редирект или широкомасштабную статистику, то нужно иметь 8 Гбайт или больше. Также необходим гигабитный интерфейс.

Конфигурация сервера. Ее целесообразно задать следующим образом:

- каждому источнику запроса должен назначаться отдельный IP-адрес;
- объем кэш-памяти в зависимости от среды может варьироваться от 500 до 1500 Мбайт. На выбор данного конфигурационного параметра существенно влияет число абонентов, имеющих доступ к серверу;
- значение параметра Recursive contexts (рекурсивные контексты – RC) должно быть низким. Рекурсивный контекст – это цепочка команд, которая используется для выполнения процедуры рекурсии (процедуры, при которой сервер выполняет от имени клиента полный поиск нужной информации во всей системе DNS, при необходимости обращаясь к другим DNS-серверам). Чем меньше число рекурсивных контекстов, тем больше число удачных обращений к кэшу. При оптимизации сервера кэширования эти два параметра идут рука об руку;
- для допустимого времени хранения ответов (TTL) в кэше в большинстве случаев используется значение по умолчанию. Малое TTL критично для большинства ресурсных записей (RR) глобальных объектов. Это значение лучше держать низким, порядка 15–45 минут.

Безопасность. Придерживайтесь следующих рекомендаций:
- не разворачивайте межсетевой экран перед кэширующими DNS-серверами (при необходимости можно установить систему предотвращения вторжений или аналогичную ей);
- задайте список управления доступом (ACL), совпадающий с диапазоном адресов абонентов, которым разрешен доступ к серверу;
- установите максимальное число портов (16) для рандомизации UDP-порта источника, чтобы обеспечить максимальную защиту от спуфинга;
- используйте метод рандомизации запроса, известный как 0x20. Убедитесь, что сервер может работать (через TCP) без рандомизации, чтобы обслуживать небольшое количество авторитетных серверных имен, которые не зеркалируют запросы.

Резервирование. Это критичный показатель при создании надежной инфраструктуры с кэшированием. Для резервирования хорошо иметь в наличии несколько разных сетей и несколько дата-центров. При этом потребуются как минимум два логических кэширующих сервера, по крайней мере один из которых нужно располагать по возможности ближе к абонентам – так, чтобы задержка не превышала 20 мс.

Доступность. Для того чтобы воспринимаемое абонентами качество взаимодействия с Интернетом было высоким, кэширующая инфраструктура должна быть доступной всегда. Возможны несколько моделей развертывания DNS-инфрастуктуры, но лучше всего следовать топологии сети и соответствовать ожидаемым абонентами качеству и стоимости:
- модель на основе балансировки нагрузки. Эта модель допускает горизонтальное масштабирование в насыщенных средах. При необходимости также появляется возможность дополнительного контроля списков ACL на аппаратных средствах. Издержки этого подхода – высокий уровень компетенции, требуемый от балансировщика нагрузки для управления средой;
- модель на основе групповой рассылки. Это очень распространенная модель реализации. Она позволяет отдельным серверам выступать в роли узлов DNS в сети. Трафик DNS маршрутизируется к ближайшему серверу в сети;
- гибридная модель – групповая рассылка с балансировкой нагрузки. Используется в крупномасштабных средах. Обеспечивает гибкое масштабирование узла во множество серверов в зависимости от плотности абонентов и объемов трафика.

Производительность. Масштабируемая инфраструктура должна справляться с отказами сети и/или оборудования. У сервера всегда должен иметься достаточный запас производительности на случай потери сайта или сервера, а также для проведения регламентных работ на сайте или сервере.

Установка пороговых значений. Этот шаг позволит центру управления сети превентивно решать проблемы, пока они не приобрели угрожающего характера:
- загрузка процессора не должна превышать 40, 50 или 60%;
- запуск контекстов рекурсии должен осуществляться при примерно 20%-ном использовании ресурсов, 50%-ная загрузка должна вызвать отправку уведомления, а 75%-ная требует разбирательства в создавшейся ситуации;
- нужно задать число запросов в секунду на одного клиента.

DDoS. Для предотвращения DDoS-атак следует ограничивать интенсивность запросов по IP, использовать распределенные серверы и лучшие типы кэширующих серверов.

Процесс развертывания. Старайтесь упростить процесс развертывания, чтобы оперативнее устанавливать патчи и обновлять программное обеспечение. Будьте готовы быстро пересобрать операционную систему, установить патч или обновить ПО.

Запуск кэширующего DNS-сервера

Итак, новая DNS-инфраструктура «поднялась» и заработала. Теперь нужно обеспечить выполнение следующих требований:
- процесс DNS должен работать на сервере при загрузке процессора не более 20%;
- нужно максимизировать число удачных обращений к кэшу путем управления его размером;
- рекурсивные контексты должны быть установлены на уровне 10–15% общей поддерживаемой доступности RC;
- ресурсы следует распределить, насколько это возможно;
- серверы должны быть максимально приближены к абонентам;
- если позволяют условия эксплуатации, полезно использовать несколько операционных систем и разнотипное оборудование. Зачастую это трудно осуществимо и может быть экономически невыгодно ввиду отсутствия ресурсов, работающих под разными ОС, необходимости поддержки разных эксплуатационных процедур и моделей развертывания, а также дороговизны эксплуатации. Количественные показатели производительности могут меняться в зависимости от использования конкретного типа ОС и/или оборудования.

Для поддержания надежности работы окружения на уровне 99,999% очень важно обеспечить контроль доступности системы и измерение параметров функционирования программного обеспечения. В число наиболее важных показателей мониторинга входят:
- загрузка процессора, памяти, дискового пространства;
- состояние подсистемы ввода-вывода;
- статистика интерфейсов;
- процесс кэширующего сервера;
- статистика рекурсивных контекстов;
- число запросов в секунду;
- список клиентов, генерирующих наибольшее число запросов к DNS;
- список наиболее часто посещаемых доменов.

При установке патчей и обновлений по возможности предварительно проверьте их в лабораторных условиях. Сначала установите их на один сервер или сайт и дайте ему поработать в течении некоторого времени, согласованного со службой эксплуатации. Методики и процедуры, выполняемые службой эксплуатации, при добавлении новых функций и/или особенностей работы также следует обновить.

Мониторинг безопасности из облака

Собственный Центр оперативного мониторинга и управления инцидентами информационной безопасности (Security Operations Center, SOC) может себе позволить далеко не каждая компания. А если сервисы SOC вынести в облако? По мнению Эльмана БЕЙБУТОВА, руководителя направления безопасности БД и SOC компании «Инфосистемы Джет», новая модель предоставления услуг будет востребована не только SMB, но и крупным бизнесом.

Эльман БЕЙБУТОВ

– Что представляет собой «классический» SOC, и какие его компоненты можно вынести в облако?

– SOC – это система сбора, корреляции и хранения событий информационной безопасности, позволяющая оперативно выявлять инциденты ИБ и реагировать на них. Для получения полноценной картины инцидентов обычно к SOC подключают имеющиеся системы информационной безопасности, сканеры уязвимостей, средства защиты СУБД, серверы приложений и веб-серверы, рабочие станции привилегированных пользователей и сетевое оборудование. В облако можно перенести основные сервисы SOC: мониторинг событий и уязвимостей ИТ-активов, мониторинг конфигураций ИТ-активов и внешнее тестирование защищенности ИТ-систем, мониторинг обращений к СУБД и защиту веб-сервисов. Вне облака, пожалуй, имеет смысл оставить лишь реагирование на инциденты.

– Как возникла идея облачных сервисов SOC?

– Многие крупные заказчики пошли по пути создания SOC на собственной площадке. Но за последние год-полтора подобные системы стали пользоваться спросом и среди небольших банков, страховых компаний, ритейловых организаций и промышленных предприятий. В их числе компании, активно использующие веб-приложения для бизнеса, которым необходим обмен данными через Интернет, компании сектора SMB, уже имеющие опыт работы с провайдерами ИТ-сервисов. Это также быстрорастущие компании, в которых развитие бизнеса опережает развитие систем безопасности, средние и малые компании, не имеющие возможности приобрести ИБ-продукты корпоративного уровня. Альтернативой для них становится получение по подписке сервиса того же уровня, что и у владельцев собственных SOC.

Но следует отметить, что и enterprise-заказчики, желающие вынести ряд функций информационной безопасности во внешнюю организацию, заинтересовались облачными сервисами SOC. Они получают возможность контроля инцидентов безопасности и управления эффективностью работы службы ИБ.

– SOC из облака – чья это «тема»? Вендоров, интеграторов или телекомов?

– Сегодня крупные телекоммуникационные компании активно предоставляют различные сервисы безопасности своим абонентам. Уже сейчас телекомы осваивают этот рынок, предлагая облачные услуги антивируса, «чистого Интернета» и межсетевого экранирования. Я думаю, что это направление в телекоммуникационном бизнесе будет развиваться и далее. Что касается вендоров, то при всем их желании ресурсов для оказания подобных услуг у них недостаточно. Если говорить об интеграторах, то сейчас лишь несколько ведущих компаний на российском рынке строят SOC для крупных заказчиков. Но в качестве облака сервисы SOC предлагает пока только одна компания: на нашем рынке это ноу-хау принадлежит «Инфосистемам Джет». Возможно, через некоторое время количество такого рода предложений увеличится.

– Подписываясь на облачные сервисы SOC, что получают компании кроме собственно сервисов?

– Вообще говоря, интегратор «с консалтинговой начинкой» предоставляет не просто сервис, а сервис, настроенный под клиента: со своим SLA, с набором правил и политик ИБ в привязке к

ИТ-инфраструктуре заказчика, с регламентами разрешения инцидентов внутри организации. Что касается стратегических выгод, то для клиентов это в первую очередь возможность сконцентрироваться на основном бизнесе и сократить капитальные вложения в создание собственных систем безопасности. Не менее значимо в данном случае и снижение затрат на поддержку систем безопасности при незапланированных изменениях в ИТ-инфраструктуре. Заказчик оплачивает только объем сервисов, необходимый для текущей ИТ-инфраструктуры.

Кроме того, компания получает ряд технологических преимуществ: это более современные технические и технологические решения в области ИБ и услуги более высокого качества, чем реализованные собственными силами. Заказчик может также пользоваться услугами квалифицированных специалистов провайдера, обеспечивающих обслуживание и поддержку систем абонента, а при необходимости предлагающих их оперативную модернизацию. Наконец, неоспоримым преимуществом является доступность услуг и удобство сервисов: управление качеством и набором услуг, быстрота и легкость подключения и регулирования параметров услуг, их оплаты, просмотра отчетов и пр.

– Как происходит подключение к облаку? Требуется ли устанавливать системы на стороне клиента?

– В «классическом» облаке клиент просто заходит через свой веб-браузер на портал – и в этом портале работает. При реализации SOC в облаке есть отступление от «классики»: в ряде случаев мы ставим оборудование на стороне заказчика для того, чтобы иметь возможность обрабатывать там большие потоки данных, например при мониторинге всех обращений к СУБД. Обычно к базам данных идет большой трафик от серверов приложений, и для сбора «сырых» данных на стороне клиента ставится специальный компонент системы безопасности, который перенаправляет эти данные на центральную консоль в облако. Они фильтруются по правилам и политикам безопасности, и заказчику поступает уже сводка событий и инцидентов, требующих реагирования. Защита веб-сервисов выделяется в отдельный блок услуг. По аналогии с сервисом мониторинга обращений к СУБД мы смотрим, какой трафик идет от рабочих станций клиента к серверам приложений. Эта дополнительная информация позволяет понять, какого вида атаки на них были предприняты, определить уровень защищенности веб-серверов и более тонко настроить правила корреляции.

В то же время, например, услуга по сканированию уязвимостей предоставляется без отступлений от классического варианта – мы просто запрашиваем доступ к внешним IP-адресам и через защищенный интернет-канал сначала проводим сканирование собственно компонентов ИТ-инфраструктуры, а затем сканируем их на наличие уязвимостей, неправильной конфигурации. В результате заказчик получает отчет о найденных уязвимостях и рекомендации по их устранению.

Подключение клиентов к облаку осуществляется стандартно, после подписания SLA, в котором фиксируются договоренности, границы предоставления услуг и перечень объектов мониторинга с помощью облака. Цена подписки на каждую услугу по соответствующей модели расчета формируется на срок, предварительно оговариваемый с клиентом.

– Какие существуют модели расчета стоимости услуг?

– Модели различаются по основным параметрам в зависимости от типа услуги. Для защиты баз данных важно знать средний объем трафика, идущего от серверов приложений к СУБД, поскольку этот показатель влияет на затраты поставщика услуг по хранению данных. Для сканирования уязвимостей расчет строится исходя из числа сканируемых узлов, по которым мы должны будем собирать сводки и анализировать конфигурации. После определения базовой стоимости сервиса модель расчетов индивидуализируется в соответствии с запросами каждого клиента.

Могу сказать, что весомую долю стоимости могут составлять услуги консалтинга: проработка критичности угроз, правил корреляции, составление регламентов инцидент-менеджмента на стороне заказчика и реагирования на тот или иной инцидент, вплоть до распределения ролей внутри организации.

– Какова ваша оценка перспектив развития облачных сервисов ИБ в России?

– На мой взгляд, в ближайшие два-три года в России облачные услуги безопасности будут так же востребованы, как сейчас в странах Европы и США. В России о подобных сервисах впервые заговорили в 2008 г., и первая реакция на них была очень настороженной. Более того, эти услуги воспринимались скорее «в штыки». Но не прошло и двух лет, как ситуация изменилась на прямо противоположную: клиенты посмотрели вокруг и увидели, что весь мир «меняет парадигму», это коснулось даже крупных корпораций (например, автоконцернов). По уровню безопасности – равно как и с точки зрения выгоды – облачные услуги не уступают системам, построенным на собственных площадках, поэтому, скорее всего, востребованность подобных сервисов и в нашей стране будет увеличиваться, а в секторе SMB всплеска их популярности можно ожидать уже в ближайшие полгода-год. Потому мы и считаем свой выход на рынок облачных сервисов ИБ своевременным и многообещающим.

– Объем всего российского рынка информационной безопасности (услуги и ПО) оценивается примерно в $700 млн. Как вы считаете, велик ли будет вклад SOC-Cloud в общую копилку?

– К объему рынка ИБ этот сегмент в ближайшие годдва, вероятно, много не прибавит, но значительно увеличит качество предоставления услуг клиентам, которые хотят при небольших инвестициях получать надежный сервис.

Беседовала **Лилия ПАВЛОВА**

DLP: куда утекают данные

От утечек данных не застрахован никто. Если компания не хочет, чтобы ее ценная информация стала «достоянием общественности», DLP-система должна стать неотъемлемой частью ее корпоративной сети.

Ирина МОМЧИЛОВИЧ,
генеральный директор Rainbow Security

Если положить на одну чашу весов продукты и услуги компании, ее финансовые и трудовые ресурсы, а на другую – ценную информацию, то весы, скорее всего, придут в равновесие. И это неудивительно. В современном мире информация – один из самых ценных активов. Клиентские базы, финансовая информация и отчетность, бизнес-планы – основа деятельности любой организации. Но у медали есть и оборотная сторона. Кража или случайная утечка данных могут привести к серьезным последствиям: судебному расследованию, срыву запланированных сделок, ущербу репутации организации, потере доверия клиентов и партнеров.

Наиболее эффективным средством борьбы с такими угрозами являются системы класса DLP (Data Leakage Prevention). Спрос на эти решения среди организаций всех отраслей быстро растет. Особый интерес к DLP проявляют банки, международные платежные системы, государственный сектор и медицинские учреждения. Они чаще других работают с личными данными клиентов, привлекающими злоумышленников.

С помощью DLP-решений компания получает четкое понимание:

- **где** хранится ценная информация;
- **куда** перемещаются конфиденциальные данные;
- **как** и когда они используются;
- **кто** из сотрудников имеет к ним право доступа.

Как вода сквозь пальцы

Чем быстрее развиваются информационные технологии, тем больше появляется возможностей для «просачивания» ценных данных компании за пределы ее информационной среды. В основном утекают персональные данные клиентов и сотрудников (по нашим оценкам – 62,6%). Чаще всего утечки происходят через следующие каналы.

Мобильные носители. USB-накопители, флэш-карты, съемные жесткие диски, карты памяти – лидеры рейтинга самых опасных каналов с точки зрения утечки информации. Утечка может быть результатом как случайных, так и умышленных действий (потери, передачи или кражи съемных носителей). Простейший способ передать файлы другому человеку – записать их на USB-устройство.

Электронная почта. Даже в почтовой системе, надежно защищенной от спама, вредоносных атак, вирусов, сотрудник может прикрепить к письму не тот документ или отослать сообщение с ценными данными неверному адресату.

Службы мгновенных сообщений, социальные сети, форумы, блоги. ICQ, Skype, Mail.ru Агент, Google Talk, AOL AIM и пр. – эти средства общения, давно превзойдя по популярности электронную почту, располагают сотрудников к неофициальному и, как они полагают, анонимному общению. А в результате – разглашение конфиденциальной информации и распространение ее на просторах Интернета. Полностью запретить использование подобных средств невозможно, поскольку зачастую они необходимы компании для осуществления бизнес-коммуникаций.

А виноват ли сотрудник?

Еще одна проблема – «человеческий фактор». Под этим понятием чаще всего подразумеваются халатность, невнимательность, небрежность сотрудников, злоупотребление полномочиями и прочие неприятные для компании действия.

Собственные работники компании могут нанести корпоративным данным гораздо больший урон, чем внешние атаки. Сотрудники ИБ-служб прилагают массу усилий, стараясь обезопасить информационную среду компании от хакерских атак. Но не упускают ли они при этом из вида самую опасную угрозу – инсайдеров? По оценкам Rainbow Security, 42% утечек информации происходит по вине инсайдеров, и только 23% – по вине хакеров.

Имея законный доступ к конфиденциальной информации, сотрудники беспрепятственно используют эти данные в личных целях, копируя их на съемные носители, передавая по электронной почте, через файлообменники, публичные FTP-серверы и пр.

Причем бизнес-данные нередко утекают за границы информационной среды компании не в результате злого умысла, а по невнимательности или неосведомленности сотрудников. Иногда работник просто не знает, что пересылает кому-то конфиденциальную информацию. Кроме того, многие сотрудники берут работу на дом. Для этого они, как правило, отправляют необходимую рабочую информацию на свой личный почтовый ящик, взломать который гораздо проще, чем корпоративный.

Что уж говорить об уволенных сотрудниках, которые уносят с собой данные о клиентах, проектах, бюджетах и пр. Нетрудно догадаться, что потом может произойти с этой информацией: базы данных клиентов, поставщиков, сотрудников очень востребованы на черных рынках. Номера банковских карт могут быть опубликованы

в Интернете, что повлечет за собой атаки на счета клиентов и сотрудников компании. Базы ГИБДД, налоговой инспекции, банковских организаций реально приобрести всего за несколько сотен долларов, хотя такая информация по определению является конфиденциальной. Кто выносит ее за пределы компании? Рядовой сотрудник, ставший брешью в «крепостной стене» организации.

Остается одно – контролировать каналы передачи информации с целью предотвращения утечки, и лучшее решение этой задачи – установка современной DLP-системы.

Как устранить «течь»

Сегодня на рынке информационной безопасности представлено множество DLP-систем, отличающихся друг от друга и функционально, и технологически, однако основной принцип их работы един и сводится к трем основным функциям.

1. Мониторинг и контроль перемещения конфиденциальной информации по сетевым каналам связи:
- анализ исходящих сообщений электронной почты и блокирование передачи ценных данных;
- блокирование передачи конфиденциальных данных, осуществляемой с помощью средств мгновенного обмена сообщениями (ICQ, Skype, Google Talk и пр.);
- перехват и анализ текста, вводимого в веб-интерфейс письма публичной почтовой службы (mail.ru, yandex.ru и пр.);
- блокирование отправки конфиденциальных данных на мобильные носители через беспроводные интерфейсы (Bluetooth, Wi-Fi и т.д.);

2. Контроль действий пользователей на рабочих станциях:
- контроль и разграничение прав доступа пользователей к конфиденциальной информации;
- блокирование копирования в буфер обмена определенных данных – например, запрет копирования через буфер обмена информации, содержащей словосочетание «банковские счета», из программы Microsoft Excel в Microsoft Word;
- контроль перемещения ценной для компании информации между пользовательскими компьютерами, а также ее копирования на съемные носители;
- блокирование печати документов, содержащих конфиденциальную информацию;
- блокирование выполнения фотографий экранов (скриншотов) некоторых приложений.

3. Аналитическое сканирование важнейших ресурсов предприятия: веб-порталов, файл-серверов, CRM-систем, конечных рабочих станций с целью выявления неупорядоченного хранения конфиденциальных данных.

Пять признаков «правильной» системы

Выбрать максимально эффективное DLP-решение и не запутаться в огромном многообразии представленных на рынке систем – задача непростая. При выборе корпоративной системы защиты от утечек данных необходимо ориентироваться на следующие основные критерии.

1. Работа с максимально возможным количеством каналов утечки данных. Чем большее число каналов контролирует DLP-решение – тем лучше. Если хотя бы один канал не отслеживается системой, то именно через него сотрудник может передать конфиденциальную информацию.

2. Мощные фильтры анализа информации. Это главная часть решения DLP. С их помощью DLP-система может обнаруживать конфиденциальную информацию в анализируемых данных. Чем более мощным будет подобный функционал, тем выше уровень защиты информационной среды. DLP-решения предотвращают утечку данных, используя «отпечатки», регулярные выражения, ключевые слова и метаданные. По-настоящему эффективная DLP-система способна сканировать и контролировать все вложения в письме, а также обнаруживать в передаваемом трафике даже те данные, которые были сильно видоизменены пользователями. Чтобы корректно работать со всей анализируемой информацией, DLP-решение должно обладать еще одним свойством: возможностью морфологической обработки данных на множестве языков. Поиск конфиденциальной информации должен производиться с учетом морфологии и синтаксиса текста.

Автоматическое блокирование и перенаправление писем, расширенные возможности карантина, создание скрытых копий и шифрование писем – все эти функции также должны быть реализованы в DLP-решении.

3. Обучаемость и гибкость системы. Система DLP должна уметь классифицировать типы конфиденциальных данных и обучаться тому, на что надо обращать внимание и какие действия необходимо предпринять при обнаружении попытки утечки информации.

Кроме того, DLP-решение должно гибко управлять использованием съемных носителей. К примеру, копирование конфиденциальной информации на USB-накопители, флэш-карты и пр. должно запрещаться, но не для всех. Исключение нужно делать для лиц, обладающих соответствующими должностными полномочиями, например для руководителей.

Еще одна немаловажная характеристика DLP-системы – возможность задания различных политик и прав доступа для отдельных компьютеров и групп пользователей, для доверенных и недоверенных почтовых доменов.

4. Архивирование анализируемых данных. Важная составляющая любой системы DLP – это возможность расследования инцидентов. Для этого необходимо архивирование перехваченной и заблокированной информации. Ведение архива позволяет проанализировать активность пользователей за определенный временной интервал и понять, что на самом деле было заблокировано.

5. Соответствие стандартам. Выполнение требований таких международных стандартов, как GLB, HIPAA, PCI, позволит успешно использовать решение коммерческим компаниям, организациям здравоохранения, банковским и государственным учреждениям.

Полный перечень требований, предъявляемых к решениям DLP, конечно, гораздо шире. Но соответствие приведенным выше критериям для любой современной DLP-системы обязательно. ИКС

Закон «О персональных данных»: поправки приняты, концепция не изменилась

Окончание. Начало см. «ИКС» № 3, с. 60.

Ключевые определения закона «О персональных данных» и связанные с ними конституционные понятия нуждаются в приведении в единую систему с четко очерченными различиями, совпадениями и пересечениями. Возможно, для этого понадобится ввести новые, дополнительные или альтернативные понятия.

Василий ЛЕВЧИК, руководитель рабочей группы по нормативным правовым вопросам Ассоциации региональных операторов связи

Коллизия с конституционными нормами

1. Целью ФЗ «О персональных данных», согласно его ст. 2, является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну», т.е. ценностей, защищаемых ст. 23 ч. 1 Основного закона:

Ст. 23 ч. 1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Однако далее к этим понятиям федеральный закон нигде не обращается – вместо этого законодатель ввел понятие «персональные данные», определив его настолько широко, что в него попадает и информация о частной жизни, и информация, составляющая личную и семейную тайну. Это приводит к коллизиям с конституционными нормами, которые, безусловно, законодателем не предполагались.

Очевидно, что публичный интерес предусматривает множество случаев, когда персональные данные должны быть обработаны без согласия их субъектов. Возможность ограничения прав и свобод граждан, в том числе и вышеуказанных, предусмотрена ст. 55 ч. 3 Конституции:

Ст. 55 ч. 3. Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В соответствии с этим ФЗ «О персональных данных» устанавливает случаи, когда персональные данные могут быть обработаны без согласия их субъектов. Желая максимально защитить интересы граждан, законодатель в некоторых важных нормах использует оговорку о том, что при этом не должны нарушаться права субъектов персональных данных:

Ст. 1. ч. 2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, ***если при этом не нарушаются права субъектов персональных данных;***

Ст. 4 ч. 2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты... по отдельным вопросам, касающимся обработки персональных данных. Такие акты ***не могут содержать положения, ограничивающие права субъектов персональных данных...***

Ст. 6 ч. 1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей ***при условии, что при этом не нарушаются права и свободы субъекта персональных данных;***

8) обработка персональных данных необходима для осуществления профессиональной деятельности журнали-

ста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности ***при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;***

Ст. 18 ч. 4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, ***если при этом не нарушаются права и законные интересы субъекта персональных данных;***

Однако каждый случай обработки персональных данных без согласия их субъекта сам по себе уже является нарушением его права, зафиксированного ст. 23 ч. 1 Конституции РФ, а в силу прямого действия ее норм вышеперечисленные оговорки лишены нормативного смысла и юридически ничтожны.

Для преодоления этой коллизии подобные оговорки следовало расширить упоминанием о том, что нарушения прав, предусмотренные настоящим законом, все-таки допустимы, сделав это, например, таким образом: «если при этом не нарушаются права и законные интересы субъекта персональных данных **иным, чем предусмотрено настоящим законом, образом».** Более сложный путь обхода этой проблемы использован в ст. 16 ч. 1 и ч. 2 закона.

Продолжая анализ ст. 1 ч. 2 закона, отметим, что содержащаяся в ней оговорка о нераспространении сферы закона на обработку персональных данных «исключительно для личных и семейных нужд» не вполне обоснованна с точки зрения ст. 23 ч. 1 и ст. 24 ч. 1 Конституции. Действительно, в Основном законе установлен безоговорочный характер неприкосновенности частной жизни, личной и семейной тайны, а также абсолютный запрет на доступ к информации о частной жизни лица без его согласия – безотносительно целей, для которых такая информация узнается другим лицом, включая и обычное любопытство.

2. Проблемы несоответствия ФЗ «О персональных данных» ст. 23 ч. 1 Конституции хотя бы понятно, как решать, а вот ее ст. 24 ч. 1 лишает юридической силы гораздо больше положений закона.

Во всеохватывающее понятие «персональные данные» формально попадает и «информация о частной жизни» – по крайней мере до тех пор, пока в законе не будет проведено какое-либо разграничение между ними. Однако такая информация дополнительно защищена ст. 24 ч. 1 Конституции РФ, устанавливающей для этого случая непреодолимый запрет:

Ст. 24 ч. 1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

При этом существенно, что если возможность и условия ограничения конституционных прав и свобод федеральными законами предусматриваются процитированной выше ст. 55 ч. 3 Основного закона, то подобной универсальной нормы для снятия своих же запретов Конституция не содержит, а возможность их преодоления (если таковая предусмотрена) явно оговаривается в каждом отдельном случае (табл. 3).

Получается, что ст. 6 и другие статьи закона «О персональных данных», устанавливающие случаи, в которых возможна обработка персональных данных (а значит, и информации о частной жизни) без согласия их субъекта, противоречат непреодолимому запрету ст. 24 ч. 1 Основного закона. Однако публичный интерес требует регулирования, предусмотренного законом, поэтому во избежание нарушения Конституции в законе нужно явным образом отделить «персональные данные» от «информации о частной жизни».

Табл. 3. Некоторые примеры конституционных запретов*

Абсолютные (непреодолимые) конституционные запреты	Запреты, для которых Конституция предусматривает механизмы их преодоления
Ст. 4 ч. 4. Никто не может присваивать власть в Российской Федерации. Захват власти или присвоение властных полномочий преследуется по федеральному закону	**Ст. 22 ч. 2.** Арест, заключение под стражу и содержание под стражей допускаются только по судебному решению. **До судебного решения лицо не может быть подвергнуто задержанию на срок более 48 часов**
Ст. 6 ч. 3. Гражданин Российской Федерации не может быть лишен своего гражданства или права изменить его	**Ст. 23 ч. 2.** Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только **на основании судебного решения**
Ст. 14 ч. 1. Российская Федерация – светское государство. Никакая религия не может устанавливаться в качестве государственной или обязательной	**Ст. 25.** Жилище неприкосновенно. Никто не вправе проникать в жилище против воли проживающих в нем лиц **иначе как в случаях, установленных федеральным законом, или на основании судебного решения**
Ст. 24 ч. 1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются	**Ст. 35 ч. 3.** Никто не может быть лишен своего имущества иначе как по решению суда. **Принудительное отчуждение имущества для государственных нужд может быть произведено только при условии предварительного и равноценного возмещения**

* Левчик В. Конституционные запреты. «Современное право» № 8'2011, с. 48.

Следует также учитывать, что Конституция не содержит явного указания на то, считать ли сведения, составляющие «личную и семейную тайну», особо защищаемой частью «информации о частной жизни», или же нужно считать эти понятия частично перекрывающимися или совпадающими (например, информация о супругах или детях обычно не считается тайной, однако некоторые обстоятельства женитьбы/замужества или факт усыновления/удочерения вполне могут быть таковой).

Но в любом из этих случаев запрет ст. 24 ч. 1 Основного закона распространяется и на сведения, составляющие «личную и семейную тайну», – до тех пор, пока в самой Конституции или в федеральном законе не будет явно установлено, что означенные сведения не являются информацией о частной жизни. Сделать же это совсем не просто.

Нестыковки с Уголовным кодексом

Декларированная в ст. 2 ФЗ «О персональных данных» цель в настоящее время не поддержана наличием какой-либо, хотя бы административной, ответственности за нарушение прав субъектов персональных данных. Фактически закон безосновательно предполагает, что если уполномоченные на то госорганы разработают систему адекватных мероприятий по защите, операторы персональных данных будут ей следовать, а контрольно-надзорные органы будут проверять их выполнение, то нарушения прав субъектов персональных данных не произойдет.

Реально же утечки баз персональных данных происходят, в том числе из недр весьма серьезных государственных органов и учреждений, причем при формальном соблюдении ими «установленных требований». А применение ст. 137 ч.1 УК РФ («Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации...») наталкивается на серьезные трудности из-за юридической неопределенности защищаемых этой статьей ценностей – личной и семейной тайны (но не «информации о частной жизни» в целом, см. ст. 24 ч. 1 Конституции РФ).

Представляется, что отсутствие в Уголовном кодексе ответственности за нарушение еще более строгого (абсолютного) запрета ст. 24 ч. 1 Конституции вызвано как раз опасением того, что под понятие «информации о частной жизни» могут быть подведены любые сведения о гражданине.

Эта же проблема встанет и при включении в законодательство ответственности за нарушение прав субъектов персональных данных – как в силу отмеченной выше их «всеохватности», так и из-за сохраняющейся юридической неразличимости с «информацией о частной жизни».

Как исправить ситуацию?

Все вышеизложенное свидетельствует о необходимости законодательно определить (возможно, в законе «Об информации, информационных технологиях и защите информации») конституционные понятия «личная тайна», «семейная тайна», «информация о частной жизни», явным образом установив границы их пересечения/совпадения.

1. Поскольку сведения, составляющие «личную тайну» и «семейную тайну», являются частью более общей «информации о частной жизни» (такова трактовка ст. 137 ч. 1 УК РФ – см. выше), то для обеспечения возможности их раскрытия придется обойти запрет ст. 24 ч. 1 Конституции РФ путем как можно более узкого определения в законе понятия «информация о частной жизни». За «частной жизнью» следует оставить лишь небольшую сферу, вторжение в которую действительно не может быть оправдано никаким публичным интересом.

Если же считать, что, наоборот, «информация о частной жизни», как более защищаемая непреодолимым конституционным запретом, является особой частью «личной и семейной тайны», то все равно эти понятия придется законодательно разделить.

При этом «личную тайну» целесообразно соотнести с другими конституционными тайнами (тайной связи, убеждений, национальности), а также с профессиональными тайнами, введенными федеральными законами (врачебной, банковской, налоговой, патентной, усыновления, завещания и т.п.), и определить, что из всего этого может быть действительно отнесено к «информации о частной жизни».

Возможно, для этих же целей в закон придется ввести альтернативное понятие **«информация о социальной жизни»** – так, чтобы она не попадала в «информацию о частной жизни».

2. Состав «личной и семейной тайны» может быть установлен как исчерпывающим перечнем, так и определением круга тех сведений, которые не могут быть тайными в этом смысле.

3. В самом законе «О персональных данных» следует явным образом соотнести «персональные данные» с «информацией о частной жизни», не допуская их совпадения. Возможно, здесь как раз и поможет новое понятие «информация о социальной жизни».

Но даже и в этом случае представляется целесообразным введение в закон понятия **«широко известные персональные данные»**, которые являются таковыми де-факто, безотносительно воли их субъекта или дозволения закона, – для защиты прав и интересов их обладателей. Например, факт обучения лица в таком-то классе такой-то школы такого-то города известен довольно широкому кругу лиц – как минимум всем соученикам и преподавателям этого лица. Возможно, это понятие будет как-то соотноситься с «общедоступными персональными данными». ИКС

ИКС pro

Технологии

70 В. ГАВРИЛОВ. Погода для ЦОДа. Нетрадиционные системы охлаждения

73 И. КИРИЛЛОВ. ДГУ в дата-центре: акцент на мощность и безотказность

77 А. ЛАСЫЙ, П. ВАШКЕВИЧ. Резервы повышения энергоэффективности ЦОДа

78 Р. НЭЙМЕК, Э. ФУРНЬЕ. Как снизить энергопотребление ЦОДа за счет выбора параметров работы чиллера

83 А. МАРТЫНЮК, И. АНИСИМОВ. Модернизация классики цодостроения: модульные дата-центры

88 В. МАКСИМОВ, П. ИВАНОВ. Новые подходы к пожаротушению в современных ЦОДах

92 Новые продукты

Природа для ЦОДа

Нетрадиционные системы охлаждения

Виктор ГАВРИЛОВ,
технический директор компании «АМДтехнологии»

Необходимость сокращения затрат на содержание ЦОДов заставляет искать новые пути для снижения энергопотребления. Ни для кого не секрет, что после серверного оборудования основной потребитель электроэнергии в ЦОДе – система кондиционирования. Именно поэтому во многих проектах упор делается на использовании альтернативных систем охлаждения.

Оптимизация системы охлаждения позволяет значительно снизить затраты на электроэнергию и повысить эффективность работы ЦОДа. По этой причине пересматриваются международные стандарты, регламентирующие параметры микроклимата в серверных помещениях. Так, в стандарте ASHRAE TC 9.9 с 2008 г. допустимая температура воздуха в помещении ЦОДа поднята до 27°C. Ведущие производители серверов, идя в ногу со временем, разрешают эксплуатацию серийно выпускаемого оборудования при повышенной температуре воздуха в «холодном» коридоре, а перепад температуры входящего и выходящего воздуха на блейд-серверах составляет от 20 до 30°C. Все это дает проектным организациям возможность при построении систем охлаждения ЦОДов применять новейшие технологии.

Тепло – на ветер

Однако так же полезно вспомнить хорошо забытое старое и обратиться к приточно-вытяжным установкам, чтобы снимать теплопритоки за счет холода наружного воздуха. В последнее время подобные технологии распространяются все шире. Известные вендоры серийно выпускают оборудование, позволяющее большую часть года охлаждать ЦОД, используя разность температур на улице и в помещении. Такие системы продвигают компании Kyoto Cooling, Colt Data Center Services, APC by Schneider Electric (модульная система охлаждения EcoBreeze), Stulz (система Direct free-cooling). Есть в их рядах и отечественные производители, в частности компания «Аякс Инжиниринг», разработавшая систему FFC, и другие. При разных подходах к построению систем охлаждения принцип у всех один – холодильные машины, входящие в состав установок, должны работать минимально возможное время, а свободное охлаждение задействуется по максимуму.

Однако полностью отказаться от холодильных машин можно не всегда, хотя это создает определенные неудобства. Ведь несмотря на то что холодильная машина включается только при пиковых нагрузках в самый теплый период года, а все остальное время простаивает, для ее работы все равно приходится выделять электрическую мощность, да и сама покупка таких машин потребует немалых затрат.

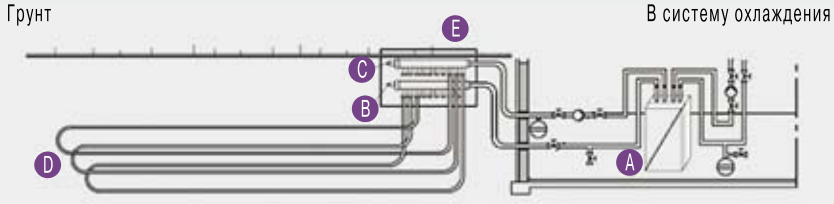
Проектные организации ищут решения, которые позволят полностью отказаться от холодильных машин для ассимиляции теплопритоков в серверных помещениях. В Европе уже несколько лет функционируют ЦОДы, круглогодично использующие стандартное климатическое оборудование, но без холодильных машин. Речь идет о двух центрах обработки данных в Германии, применяющих систему геотермального охлаждения.

Тепло унесет подземная река

Первый ЦОД находится в Мюнхене, он принадлежит страховой компании WWK и расположен в офисном здании. При строительстве фундамента здания была обнаружена подземная река, протекающая на небольшой глубине. И тогда родилась идея воспользоваться подземными водами для холодоснабжения будущего ЦОДа. Причем сама вода из реки не забирается. Во-первых, получение разрешений у служб экологической безопасности представляло определенные сложности, а во-вторых, это потребовало бы дополнительных затрат на фильтрацию и очистку воды. По этим причинам была выбрана замкнутая система охлаждения с горизонтальными земляными коллекторами (рис. 1).

Во время заливки фундамента были заложены коллекторы из поли-

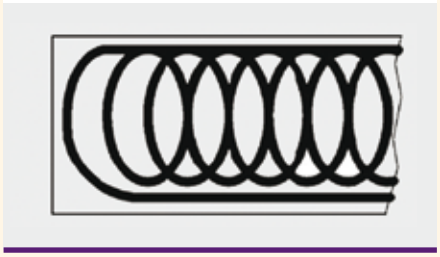
Рис. 1. Принципиальная схема системы геотермального охлаждения



A – пластинчатый теплообменник гликоль – вода
B – распределительный коллектор – обратная магистраль
C – распределительный коллектор – подающая магистраль
D – земляной коллектор
E – технологическое помещение

этиленовых трубопроводов длиной 100 м каждый (рис. 2). Длина трубопроводов определялась исходя из оптимального гидравлического сопротивления участка таким образом, чтобы не увеличивать потребляемую мощность циркуляционного насоса. Суммарная длина всех коллекторов достигает нескольких километров. На концах трубопроводы объединены распределительными гребенками подающей и обратной магистралей. Для обеспечения высокой надежности системы каждый трубопровод снабжен отсекающими вентилями. Трубопроводы наружного контура заполнены теплоносителем – раствором пропиленгликоля (температура замерзания – минус 10°С), который благодаря охлаждению грунтовыми водами в течение всего года имеет температуру около 12°С. Насос заставляет теплоноситель циркулировать по замкнутому контуру. Жидкость поступает в промежуточный пластинчатый теплообменник гликоль – вода, в котором и происходит отвод тепла от серверного оборудования. Во вторичном контуре циркулирует вода с температурой 14–16°С. Помещения ЦОДа расположены на цокольном и на третьем этажах здания. Оборудование установлено в серверные шкафы с водяным охлаждением Knuerr CoolTherm с закрытой архитектурой охлаждения. Тепловыделение одной стойки составляет 8–16 кВт, суммарная холодопроизводительность системы – 400 кВт, при этом имеется резерв мощности как минимум 100 кВт.

Рис. 2. Земляной коллектор



В результате общая схема системы холодоснабжения выглядит следующим образом:

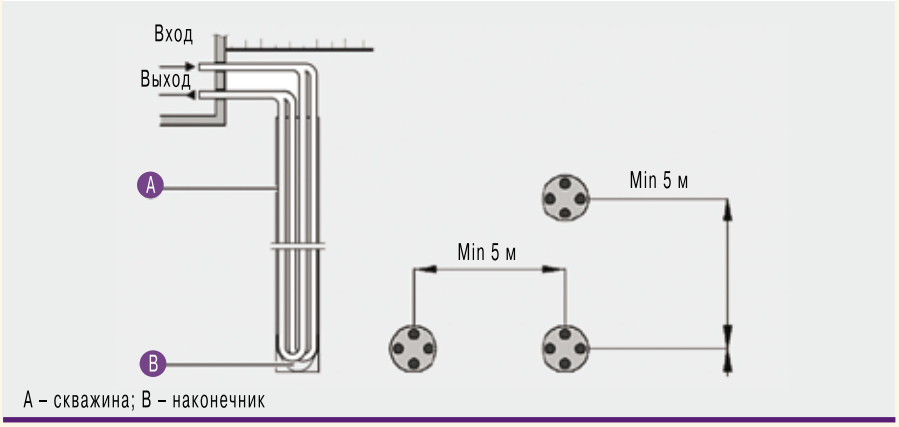
Грунтовые воды ⇔ Теплообменник ⇔ ЦОД

Такая система охлаждения ЦОДа вне зависимости от времени года обеспечивает значение показателя PUE на уровне 1,09. Это неудивительно, поскольку фактически единственными потребителями электроэнергии системы холодоснабжения являются два циркуляционных насоса.

Тепло зароем в землю

Похожая схема геотермального охлаждения, но несколько в другом исполнении реализована в центре обработке данных компании Toshiba, расположенном неподалеку от Мюнхена. Однако здесь ЦОД создавался в существующем здании, и устраивать горизонтальные коллекторы было нерентабельно. Поэтому было принято решение использовать вертикальные земляные тепловые зонды, состоящие опять же из заполненных пропиленгликолем полиэтиленовых труб. Для их установки пробурили четыре скважины на глубину 100 м. В каждую скважину опустили параллельно четыре трубы, образующие двойные U-образные зонды (рис. 3). Раствор пропиленгликоля поступает по двум трубам от распределителя вниз и возвращается по

Рис. 3. Устройство U-образного трубчатого земляного зонда



A – скважина; B – наконечник

двум другим трубам обратно вверх к коллектору. Все промежутки между трубами и грунтом заполнены материалом с хорошей теплопроводностью – бетонитом. Температура в верхних слоях почвы меняется в зависимости от сезона, ниже границы промерзания температурные колебания значительно уменьшаются. Так, на глубинах 10–15 м и ниже температура грунта на протяжении всего года держится около +10°С.

Холодопроизводительность системы – 80 кВт, в качестве внутренних блоков системы кондиционирования применены межрядные кондиционеры CoolLoop, а также изолированный холодный коридор CoolFlex.

Особенность этой схемы в том, что система охлаждения ЦОДа совмещена с системой отопления здания (рис. 4), тепло в которую поступает через тепловой насос производительностью 100 кВт (потребляемая мощность – 25 кВт). В теплый период года тепловой насос не работает, отвод тепла из ЦОДа осуществляется только за счет геотермального охлаждения. В холодное время, когда здание необходимо отапливать, в работу включается тепловой насос, и для отопления используется тепло, отводимое от серверного оборудования. Земляные зоны подключаются только тогда, когда при малой загрузке серверное оборудование выделяет тепла значительно меньше расчетной тепловой нагрузки.

На эффективность данной схемы сильно влияют теплофизические свойства почвы – ее объемная теплоемкость и теплопроводность, которые, в свою очередь, зависят от состава и состояния грунта. Теплопроводность грунта тем больше, чем выше содержание в нем воды, чем больше доля минеральных компонентов и чем меньше пористость. Чтобы воспользоваться описанным решением, перед проведением буровых работ необходимо получить данные геологической разведки выбранного места. Из карты разреза станет понятно, на какую глубину можно бурить скважины и каковы термические свойства грунта.

Тепло – на обогрев здания

Чтобы использовать тепло, отводимое от серверного оборудования, для работы теплового насоса, вовсе необязательно бурить скважины или прокладывать земляные коллекторы. Равно как нет необходимости отказываться от свободного охлаждения ЦОДа, если основным источником холода служат чиллеры.

Понятно, что при работе компрессоров чиллера получить нагретую воду довольно просто. Но компрессоры работают только в теплый период года. При температуре наружного воздуха ниже 5°С компрессоры останавливаются, и холодильные машины переходят в режим свободного охлаждения. Тепло от серверного оборудования передается теплоносителю и далее фактически выбрасывается на улицу. Непосредственно использовать это тепло не удастся, так как температура жидкости составляет лишь 15–18°С. Но эта вода вполне пригодна для работы теплового насоса. Из системы охлаждения отепленная вода поступает в тепловой насос, где охлаждается и подается обратно в систему холодоснабжения ЦОДа. С другой стороны теплового насоса происходит нагрев воды до 50°С, далее вода может нагреваться в накопительном или проточном бойлере до 90°С. Дополнительным источником тепла могут стать электроэнергия, газ, жидкое или твердое топливо, а также система центрального теплоснабжения. Впрочем, воду с температурой 50°С можно напрямую использовать для отопления технологических помещений (рис. 5), а также для нагрева воздуха в системах приточной вентиляции и воздушного отопления. Применение теплового насоса по-

Рис. 4. Принципиальная схема использования геотермального охлаждения и системы отопления здания

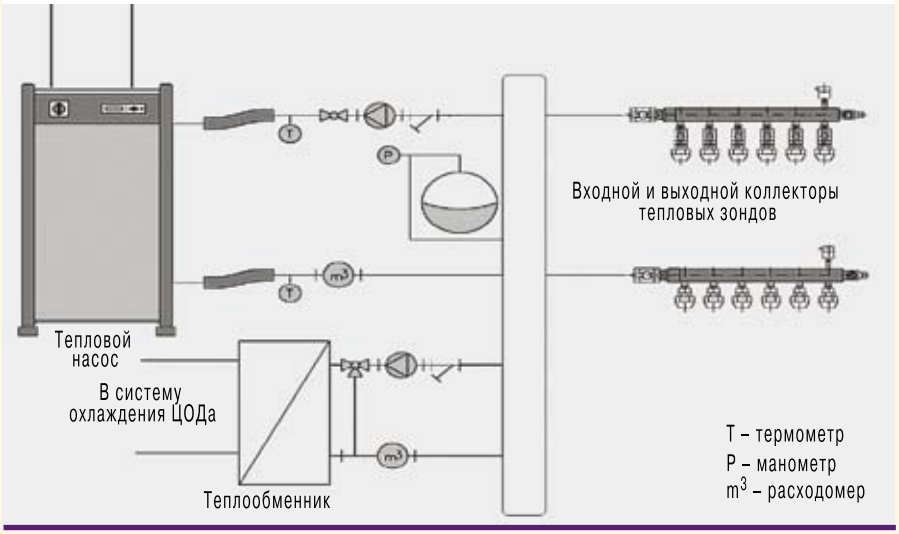
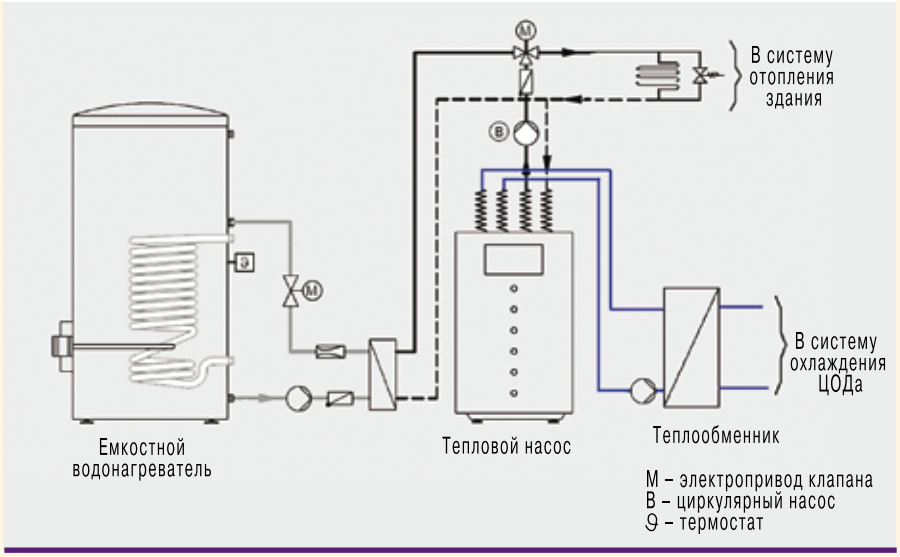


Рис. 5. Принципиальная схема использования теплового насоса для отопления здания



зволит сэкономить до 70% энергии, требуемой для отопления здания.

Описанная схема использования теплового насоса не требует проведения земляных работ, обустройства вертикальных или горизонтальных земляных коллекторов. Главное условие – тепловыделение ЦОДа должно быть равно или больше количества тепла, необходимого для отопления здания. При построении системы холодоснабжения ЦОДа, базирующейся на чиллерах внутренней установки, тепловым насосом может служить один из чиллеров.

В любом случае возможность и рентабельность применения тепловых насосов для отопления здания определяется на этапе проектирования. Данный способ рекуперации тепла при эксплуатации ЦОДа весьма эффективен и не требует больших капитальных затрат.

■ ■ ■

Безусловно, не всегда и далеко не везде подобные системы можно и целесообразно применять. Все зависит от конкретного объекта, его расположения, строительной готовности и т.д. Однако, как нет предела совершенству, так нет предела стремлениям проектировщиков осуществить свой замысел, найти новые пути повышения энергоэффективности системы, разработать принципиально новые схемы или нетрадиционным образом использовать хорошо известные технологии. Не существует рецепта построения идеального ЦОДа. И это хорошо, значит, всегда есть место творчеству, возможность комбинировать различные методы, оптимизируя оборудование разных производителей для решения конкретной задачи. ИКС

ДГУ в дата-центре

Акцент на мощность и управляемость

Игорь КИРИЛЛОВ

Дизель-генераторные установки используются повсеместно – от частных домов до международных аэропортов и крупных дата-центров. Каково же текущее положение и перспективы российского рынка ДГУ и какие требования предъявляются к дизель-генераторным установкам в контексте их использования в ЦОДах?

На одних объектах дизель-генераторные установки служат резервным источником электропитания, а на других – основным. Несмотря на концептуальную схожесть всех ДГУ, каждая ниша применения диктует свои требования к оборудованию. Этим объясняется многочисленность производителей и широкий модельный ряд оборудования. На российском рынке сегодня можно найти устройства в диапазоне мощности от нескольких киловатт до мегаватта и выше, которые представляют десятки зарубежных компаний и их отечественных партнеров. Кроме того, свою продукцию предлагают и российские разработчики.

Российский рынок ДГУ-2011

По оценкам экспертов, общий объем российского рынка ДГУ составил в 2011 г. $480–500 млн, а рост по сравнению с 2010 г. – 20–25%. Спектр решений, присутствующих на российском рынке, включает в себя сотни моделей, поставляемых десятками известных и не очень известных производителей. Для удобства разобьем все ДГУ на две большие группы – однофазные (мощностью до нескольких десятков киловатт) и более «серьезные» трехфазные. Последние, в свою очередь, также будем подразделять на системы малой, средней и высокой мощности (до 250 кВА, 250–550 кВА и свыше 550 кВА соответственно).

Рост рынка ДГУ оказался неоднородным. Сегмент малой мощности и однофазных решений вырос в денежном выражении почти на 50%, средней – на 15–20%, а поставки наиболее «тяжелых» систем увеличились на 7–10%. Наибольшим спросом во всех сегментах пользовались разработки зарубежных производителей, таких как Aksa, Caterpillar, Cummins, FG Wilson, Gesan, SDMO, хотя все чаще встречалась и продукция российских компаний. При этом у каждого вендора сложился свой набор моделей, которые были популярны в разных сегментах (см. таблицу).

Наиболее популярные модели ДГУ на российском рынке в 2011 г.*

Производитель	Однофазные	Трехфазные		
		Небольшой мощности (< 250 кВА)	Средней мощности (250–550 кВА)	Большой мощности (> 550 кВА)
Caterpillar (США)	–	Olympian GEP150	3406 365 кВА	3516B-HD 2500 кВА
Cummins (США)	–	C150D5	C550D5	C1400D5
FG Wilson (Великобритания)	–	P33-1	P250H2	P635P5
Gesan (Испания)	DPA/S 16-35E MF	Серия Energy 15-65 кВА, двигатель Perkins, DVA/S 140E – DVA/S 220E	DVA/S 275E – DVA/S 550E, двигатель Volvo Penta	DVA/S 660E, DVA/S 700E, DPA/S 1100E, DPA 1400E, DTA 2200E
GMGen (Италия)	GMM12M	GMJ66	GMV350	GMM1400
SDMO (Франция)	SH 6000 E, T9KM	J110, T12K	V350, V275	V630, V700

*Источник: исследование «ИКС», февраль 2012 г.

Крупнейшими потребителями ДГУ в 2011 г. стали организации, представляющие государственный сектор, добывающую отрасль, промышленное производство, телекоммуникации. Много заказов поступало от предприятий сферы торговли и обслуживания (в частности, отелей), финансовых структур и бизнес-центров.

Наиболее активный рост инсталляций отмечался в банковской сфере, поскольку с развитием филиальных сетей и ужесточением требований к непрерывности бизнес-процессов выросла и потребность в системах резервного электроснабжения. В частности, одним из крупных заказчиков ДГУ стал Сбербанк России. Он завершает сейчас создание системы резервного электроснабжения для своего центра обработки данных, который претендует на звание самого крупного в Европе. В рамках этого проекта компания «Хайтед» (российский дистрибьютор производителя FG Wilson) поставила ему 12 контейнерных высоковольтных (10,5 кВ) электростанций по 2500 кВА каждая (общая мощность энергоцентра достигает 24 МВт). По оценке Михаила Лобанова из «Хайтеда», наибольшим спросом в 2011 г. пользовались ДГУ мощностью от 700 кВА и выше.

Рост интереса к устройствам большой мощности и параллельным системам ДГУ отметил и Олег Четвер-

гов, заместитель гендиректора компании «Абитех». По его данным, сегодня на многих предприятиях производится замена эксплуатировавшихся дизельных генераторов на более мощные модели или установка дополнительных ДГУ. Ощущается и тенденция к снижению стоимости владения системой посредством оптимизации затрат на обслуживание и сервис, а также использования новых более технологичных и экономичных двигателей известных мировых производителей. Направлением, в котором ДГУ будут развиваться в ближайшей перспективе, О. Четвергов считает их интеллектуализацию.

Среди компаний, осуществляющих поставку и установку дизель-генераторов российским потребителям, по мнению экспертов, наиболее заметны были интеграторы IBS, Stins Coman, «Астерос», «ГрандМоторс», «Инфосистемы Джет», КРОК, «Ланит», «НГ Энерго», «Президент-Нева», «Сиэтл-ДМО», «Техносерв», «Хайтед», «Энвижн Груп».

Если говорить о дополнительных характеристиках ДГУ, которые больше всего привлекают российских клиентов, то участники рынка в первую очередь назвали качество изготовления, богатую базовую комплектацию, доступность сервисной базы, возможность организовать мониторинг состояния дизеля без лишних затрат. Так, Сергей Костиков из компании «Синергетика» (мастер-дистрибьютора концерна SDMO Industries в России) отмечает, что наибольшим спросом на рынке в 2011 г. пользовалось (и, по всей вероятности, будет пользоваться в дальнейшем) оборудование с хорошим соотношением цена/качество и развитой сервисной гарантийной и постгарантийной поддержкой. Весомым аргументом в пользу выбора той или иной модели служат также наличие всепогодных и шумозащитных кожухов и дополнительные опции, предлагаемые производителем, в частности встроенные баки большой емкости. И конечно же покупатель обращает внимание на сроки поставки и наличие оборудования на региональном складе. Перечисленные аспекты и обусловили популярность продукции вышеупомянутых производителей, а также лидерские позиции интеграторов.

Емкими и быстрорастущими сегментами российского рынка ДГУ являются направление коммерческих и корпоративных ЦОДов и решения для операторов связи.

Какие ДГУ подойдут для ЦОДа

Несмотря на то что принципиальная схема ДГУ разных производителей практически идентична, сфера их применения обусловливает некоторую специфику устройств. Так, по мнению Станислава Коларжа, коммерческого директора «ГрандМоторс», типичные требования к ДГУ для ЦОДов заключаются в следующем: относительно большая мощность единичной установки (500–2000 кВА), хорошие коммуникационные способности контроллера для организации удаленного мониторинга, наличие возможности построения синхронизированных резервируемых систем.

Дизель-генераторная установка как резервная система подачи электроэнергии для ЦОДа должна работать безотказно и в случае выхода из строя основного источника обеспечивать вычислительное и телекоммуникационное оборудование комплекса питанием необходимого качества в течение длительного времени – от нескольких часов до нескольких суток и более. Отметим, что согласно требованиям TIA-942 ЦОД уровня Tier I не предполагает использования ДГУ, но комплекс Tier II должен быть оснащен хотя бы одной дизель-генераторной установкой. Дата-центры более высоких уровней должны содержать минимум по два ДГУ, поскольку в Tier III подразумевается схема резервирования N + 1, а в Tier IV – 2N.

Модели генераторов, устанавливаемых в ЦОДах, должны быть рассчитаны на подачу синусоидального тока, который необходим для ИБП или ИТ-оборудования. Таким образом, важным аспектом является согласование параметров ИБП и ДГУ, работающих на объекте. К тому же резервный генератор должен питать не только вычислительное и телекоммуникационное оборудование, но и довольно энергоемкие инженерные подсистемы, в частности кондиционирование и вентиляцию. При этом нужно учитывать, что кондиционеры в дата-центрах оснащены электродвигателями, которые, как известно, создают в момент включения большие пусковые токи (превышающие номинал в 3–5 раз). К тому же современные системы охлаждения, используемые сегодня во многих российских дата-центрах включают/отключают кондиционеры и вентиляторы в зависимости от тепловой нагрузки в машинном зале. Так что пиковые пусковые токи возникают не так уж редко. Это обстоятельство заставляет выбирать для ЦОДа установки только с синхронными генераторами, соответственно исключая асинхронные системы.

Нельзя упускать из виду и рост энергопотребления ИТ-систем ЦОДа в будущем, по мере развития комплекса. Поэтому, выбирая ДГУ, необходимо изначально закладывать большой запас мощности с учетом вышеупомянутых факторов. Кроме того, на выходе каждого электрогенератора должно быть установлено устройство подавления переходных помех. Как правило, все процедуры, связанные с введением ДГУ в работу в случае аварии на основной сети, выполняются автоматически; тем не менее, если речь идет о дата-центре, необходимо предусмотреть и возможность ручных манипуляций – синхронизации или переключения байпаса каждого отдельного генератора.

Также следует обратить внимание на скорость вращения электродвигателя. Модели, рассчитанные на постоянную работу (24/365), как правило, обладают показателем в 1500 об./мин. Более высокие скорости (3000 об./мин и выше) в данном случае не подходят. К тому же, если подразумевается возможность длительной работы, дизель-генератор должен быть оснащен системой жидкостного охлаждения, поскольку модели на воздушном охлаждении требуют периодической остановки (на 2–3 часа примерно раз в 10 часов). Важным показателем является и время наработки на отказ – у лучших образцов зарубежного производства он достигает 40 тыс. часов и более. Если предполагается, что ДГУ должен работать круглосуточно в течение длительного времени, то нужно выбирать модели с бесщеточными генераторами, которые не требуют частого проведения регламентных работ.

Дополнительные характеристики ДГУ, рассчитанных на работу в ЦОДах, – наличие удаленной системы мониторинга, защиты от перегрузок, индивидуального заземления, термокожухов, систем звукоизоляции (что особенно актуально в условиях города) и т.д. Еще один важный момент – топливные баки большой емкости. Некоторые модели вмещают суточный запас топлива для дизеля. Однако ни один ДГУ не может обеспечить надежность, равную 100%, поэтому на особо ответственных объектах дизель-генераторные установки дублируются.

ДГУ, отвечающие вышеперечисленным требованиям, могут применяться в дата-центрах любого типа. Наиболее популярны в российских ЦОДах установки в мощностном диапазоне 200–1400 кВА.

Какие ДГУ нужны операторам связи

Узловые объекты операторов связи по своим эксплуатационным характеристикам весьма близки к ЦОДам, поэтому и требования к ДГУ для них сходны с требованиями к ДГУ для ЦОДов. Дополнительно в них может быть включена система GSM-мониторинга. По словам Сергея Меликьянца («Цеппелин Русланд»), у операторов связи наибольшим спросом пользуются системы мощностью от 12 кВА до 2,5 МВА. Заказчики в первую очередь обращают внимание на надежность ДГУ, наличие развитой сервисной базы, способность интегратора предложить любые решения «под ключ», включая системы ИБП, распределения электропитания и т.д.

А по наблюдению С. Коларжа, операторами связи востребованы две основных группы ДГУ: в мощностных диапазонах 10–30 кВА (для резервирования электропитания мелких узлов и базовых станций) и 200–1000 кВА, которые применяются на коммутаторах и крупных узлах связи.

■ ■ ■

Рынок дизель-генераторных установок растет. В текущем году эксперты прогнозируют увеличение спроса примерно на 20% по сравнению с 2011-м. Быстрее всего по-прежнему будет расти сегмент ИКТ. Продолжающиеся развитие этой отрасли, а также стойкая тенденция к централизации вычислительных ресурсов ведут к тому, что все большее число объектов, таких как дата-центры или узлы операторов связи, попадают в категорию бизнес-критичных. Соответственно, здесь все чаще востребованы надежные, мощные и отказоустойчивые системы гарантированного электропитания, незаменимым элементом которых является ДГУ. ИКС

Резервы повышения энергоэффективности ЦОДа

Повысить энергоэффективность дата-центра можно как путем оптимизации инженерных систем, так и путем оптимизации загрузки процессоров.

Александр ЛАСЫЙ, технический директор департамента интеллектуальных зданий компании КРОК

Петр ВАШКЕВИЧ, главный инженер департамента интеллектуальных зданий компании КРОК

Наилучших результатов в снижении энергопотребления в ЦОДе можно достичь за счет систем охлаждения и вентиляции. Поскольку в России большую часть года температура воздуха не превышает 20–22°С, то до 85% времени в году можно использовать свободное охлаждение (фрикулинг).

Долгое время в нашей стране температура в «холодных коридорах» составляла 17–24°С, тогда как в современных зарубежных ЦОДах она может достигать 27°С, а производители серверов разрешают до 32–35°С. Поэтому сейчас повсеместно намечается тенденция к подъему температуры в ЦОДе – это позволит расширить диапазон работы свободного охлаждения и снизить затраты на электроэнергию. К примеру, в данный момент КРОК реализует проект по созданию ЦОДа в Восточной Сибири с расширенным температурным диапазоном в машинных залах. В результате до 99% времени в году охлаждение дата-центра будет работать в режиме фрикулинга.

Система энергоснабжения даже в небольшом ЦОДе получается сложной. Это обусловлено наличием в нем потребителей, которые различаются по мощности, характеру нагрузки и требованиям к непрерывности питания. Отметим, что заложить высокоэффективные инженерные решения можно только на этапе проектирования, особенно при строительстве корпоративного ЦОДа, когда заранее планируется удельное энергопотребление, близкое к реальности.

Для бесперебойного гарантированного электропитания ЦОДа сегодня используют два подхода: классическую схему на основе статических ИБП в сочетании с дизель-генератором и другой вариант – на основе дизельных динамических ИБП.

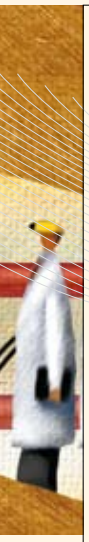
В ЦОДе КРОК «Волочаевская-2» установлено четыре таких ДДИБП

Первыми в России в промышленную эксплуатацию ДДИБП на базе оборудования производства Hitec Power Protection запустила наша компания в аутсорсинговом ЦОДе КРОК «Волочаевская-2». В дата-центре размещено четыре установки, мощность каждой – 1000 кВА. Дизельные динамические ИБП позволяют обеспечить бесперебойность электроснабжения всех типов потребителей, как ИТ-систем, так и вспомогательного оборудования ЦОДа, причем их не требуется разделять, как раньше.

На стадии проектирования ЦОДа КРОК «Волочаевская-2» мы провели анализ этого решения в сравнении с аналогичной площадкой со статическими ИБП, и выяснилось, что классический вариант имеет ряд недостатков. Статический ИБП вместе с дизель-генератором занимает примерно в 2 раза больше площади, чем ДДИБП. Классическая схема обладает более низким КПД, ей требуется специальная климатическая установка для охлаждения ИБП и регулярная замена батарей, стоимость которых может превышать стоимость самого ИБП. Но главный минус классической схемы – это медленный заряд батареи, что может сказаться на непрерывности электропитания в случае повторного отключения электроэнергии. В то же время дизельные динамические ИБП заряжаются в течение 10 мин, имеют более высокий КПД, срок эксплуатации 25 лет, не требуют сложной системы охлаждения. Используя ДДИБП, можно обеспечить бесперебойное электроснабжение и при кратком, и при длительном отключении внешнего питания, а также осуществлять «кондиционирование» электроэнергии, подавая потребителям «чистую» электроэнергию.

■ ■ ■

В последнее время во всем мире чаще стали задумываться над оптимизацией загрузки процессоров в центрах обработки данных, одним из путей которой стала организация облачных вычислений. Именно здесь кроется еще один мощный резерв для повышения энергоэффективности ЦОДа.



Как снизить энергопотребление ЦОДа за счет выбора параметров работы чиллера

Рэмзи НЭЙМЕК, директор по проектированию компании Total Site Solutions,
Эрик ФУРНЬЕ, старший инженер-механик компании Total Site Solutions

Ослабление требований к температурным параметрам, в расчете на которые традиционно проектируются и эксплуатируются ЦОДы, в сочетании с оптимизацией устройства коридоров между рядами серверных стоек позволяет существенно снизить мощность, потребляемую чиллерной установкой, и следовательно, сэкономить энергоресурсы.

В помещениях, где размещается компьютерная техника, важнейшая задача – недопущение перегрева и выхода из строя микропроцессорных чипов. Для этого к серверам подается поток холодного воздуха. Однако не следует, стремясь добиться комфортных по охлаждению условий, ставить перед собой цель подавать воздух с температурой 55°F (12,8°C). Это приведет к завышению мощности холодильных установок и к излишнему расходу электроэнергии. И руководящие указания ASHRAE TC9.9, и публикации Национальной лаборатории им. Лоуренса в Беркли* допускают, чтобы на серверы поступал воздух с температурой до 27°C. Исследования, проведенные фирмами – производителями серверов, показали, что их оборудование способно безотказно работать при более высоких температурах входного охлаждающего воздуха. Поскольку львиная доля нагрузки по охлаждению в ЦОДе приходится на отвод явного тепла, а тепловые нагрузки, обусловленные скрытой теплотой, весьма незначительны, то повышение температуры охлаждающей воды является гарантированным способом снижения энергопотребления холодильной установки. Достигается это благодаря уменьшению разности давления хладагента в конденсаторе и в испарителе чиллера и благодаря тому, что в процессе отвода явного тепла удается избежать ненужного осушения воздуха.

Проектировщики приняли во внимание рекомендации ASHRAE, и в результате был разработан вариант размещения охлаждаемого оборудования в ЦОДе по схеме «горячий коридор» (HAC) – «холодный коридор» (CAC). Эта схема размещения способствует подаче требуемого количества холодного воздуха к фронтальным панелям серверов и минимизирует вредное перемешивание потоков горячего и холодного воздуха в проходах, что является шагом в правильном направлении.

К сожалению, проектировщики и службы эксплуатации не спешат с внедрением двух мероприятий, направленных на экономию электроэнергии. Первое сводится к повышению температуры охлаждающей воды на выходе из чиллера (Leaving Chilled Water Temperature – LCHWT) и температуры охлаждающего воздуха, подаваемого в помещение ЦОДа. Второе состоит в увеличении разности между входной (Entering Chilled Water Temperature – ECHWT) и выходной LCHWT температурами охлаждающей воды (ΔT), которая в традиционной практике находится в диапазоне от 5,6 до 6,7°C.

Повышение LCHWT

Переход на более высокие температуры охлаждающей воды и воздуха в ЦОДе имеет целый ряд полезных следствий для экономии энергоресурсов. Работа на воде с более высокой температурой на выходе холодильной установки (LCHWT) – один из способов уменьшить разность давлений хладагента холодильной машины. В практике охлаждения промышленных объектов с целью обеспечения комфортных условий упор делается на понижение перепада давления путем изменения температуры воды в конденсаторе в зависимости от температуры окружающей среды при поддержании постоянной температуры воды в испарителе. В результате давление на стороне конденсатора понижается. В ЦОДе охлажденная вода, поступающая из холодильной установки, может иметь более высокую температуру (LCHWT), что позволяет понизить перепад давлений со стороны испарителя, повысив давление хладагента в испарителе, и добиться того же самого эффекта уменьшения перепада давлений хладагента холодильной установки в целом. Переход на более высокое значение LCHWT в данном случае оказывается возможным благодаря тому, что, как говорилось выше, охлаждение в ЦОДе осуществляется путем отвода в основном явного тепла.

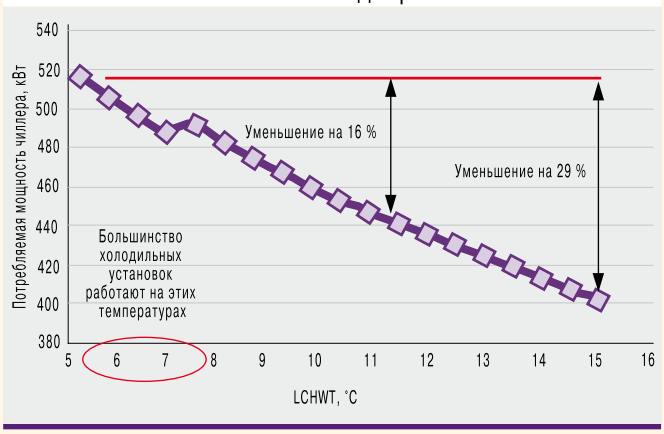
О других положительных эффектах повышения температуры охлаждающей воды и воздуха можно сказать следующее. Переход на более высокие температуры воздуха приводит к уменьшению потреб-

*High Performance Data Centers, LBNL and Pacific Gas and Electric Study, 2006.

ности в охлаждении потоков воздуха, а это означает, что снижается энергопотребление вентиляторов. Повышение температуры как воздуха, так и воды увеличивает продолжительность эксплуатационного периода, когда можно включать экономайзеры на стороне воды или на стороне воздуха. Компрессор либо стоит, либо работает на неполной нагрузке на протяжении всего или существенной части периода работы в режиме естественного охлаждения (фрикулинга), что также означает сокращение энергопотребления. Кроме того, уменьшение расхода электроэнергии на чиллер позволяет использовать для удовлетворения потребностей ЦОДа электрогенератор меньшей мощности. Если говорить в современных терминах, то все вышеперечисленное сводится к повышению эффективности использования энергии в ЦОДе и к уменьшению вредных экологических последствий его функционирования.

В качестве примера рассмотрим центробежный чиллер производительностью 1000 тонн холода США* (3513 кВт), у которого параметр LCHWT варьируется в диапазоне от 5,6 до 15,6°C с шагом 0,55°C. Температурный дифференциал испарителя

Рис. 1. Профиль мощности чиллера для разных значений LCHWT



поддерживается постоянным на уровне 7,8°C; аналогично температурный дифференциал конденсатора сохраняется равным 6,7°C при температуре воды 36,1°C на входе и 29,4°C на выходе. Эксперимент с указанным изменением температуры воды на выходе чиллера LCHWT проводился на машине семейства Trane. Полученные результаты вполне предсказуемы. При повышении температуры охлаждаю-

* 1 тонна холода США – это количество энергии, которое необходимо отобрать, чтобы 1 т воды при температуре 0°C за 24 ч превратить в лед при температуре 0°C. – *Прим. ред.*

Как сделать чиллерные системы конкурентоспособными

Виктор ГАВРИЛОВ, технический директор компании «АМДтехнологии»

В борьбе за повышение энергоэффективности ЦОДа можно выделить два основных направления. Первое – это прямой фрикулинг, при котором для отвода тепла используется наружный воздух, и второе – это применение холодильных машин, работающих с повышенной температурой воды. У каждого способа есть свои достоинства и недостатки.

Так, установки с прямым фрикулингом большую часть года работают без включения холодильных машин, что значительно снижает мощность, потребляемую системой охлаждения. Вместе с тем эти системы более металлоемкие, что накладывает определенные ограничения на их инсталляцию в существующих зданиях. В зависимости от выбранной схемы установки могут возникать проблемы с работой в холодный период года, с поддержанием влажности, а также с возможностями зонального регулирования температуры в обслуживаемом помещении.

Чиллерные системы несколько проигрывают в энергетической эффективности системам с прямым фрикулингом, однако использование высокой температуры воды позволяет им успешно конкурировать. С помощью холодильных машин можно строить гибкие и масштабируемые системы охлаждения, разбивать машинный зал на различные климатические зоны, оптимизировать распределение воздуха в зале, использовать различные типы кондиционеров в зависимости от тепловой нагрузки.

На европейском рынке большую популярность приобретает технология Cold Logic, основанная на поддержании давления воды в контуре холодоснабжения ниже атмосферного. В случае утечки вода не попадет на оборудование, а наоборот – воздух будет подсасываться в систему. Температура воды в контуре динамически изменяется в зависимости от тепловой нагрузки. При грамотном проектировании система кондиционирования, построенная на чиллерах, способна успешно конкурировать с системами, использующими прямой фрикулинг, при этом коэффициенты энергетической эффективности будут соизмеримы, а стоимость киловатта холода может быть значительно ниже.

Табл. 1. Базовый вариант моделирования при ΔT = 5,6°C

LCHWT, °C	5,56	6,67	7,78	8,89	10	11,11	12,22	13,33
Средняя температура возвратного воздуха на блоках CRAH, °C	25,6	26,7	28,3	29,4	31,1	32,2	33,9	35
Энергопотребление механических систем								
Вентиляторы испарителя, кВт	4 384 061	4 802 728	4 658 993	4 569 237	4 378 787	4 378 787	4 133 578	3 578 039
Чиллеры, кВт	18 060 694	16 946 670	16 642 845	16 507 812	15 967 679	15 461 305	15 056 205	14 870 534
Градирни, кВт	838 747	838 747	838 747	838 747	838 747	838 747	838 747	838 747
Насосы, кВт	2 217 071	2 217 071	2 217 071	2 217 071	2 217 071	2 217 071	2 217 071	2 217 071
Суммарная мощность механических систем, кВт	**25 500 573**	**24 805 216**	**24 357 657**	**24 132 867**	**23 402 284**	**22 895 910**	**22 245 601**	**21 684 391**
Годовая экономия, кВт	(695 357)	0	447 560	672 349	1 402 932	1 909 307	2 559 615	3 120 825
Годовая экономия, $	(55 629)	0	35 805	53 788	112 235	152 745	204 769	249 666

щей воды с 5,6 до 15,6°C потребляемая мощность чиллера уменьшилась примерно на 115 кВт, т.е. на 29% (рис. 1). Исходя из того, что большинство холодильных установок работают (при постоянном значении ΔT) на LCHWT в диапазоне 5,6–7,8°C, перевод LCHWT в окрестности 12,8°C позволяет сократить расход электроэнергии на 14–18%. А если пойти на более «агрессивный» вариант и повысить LCHWT до 15,6°C, то можно добиться еще более существенного снижения энергопотребления – до 25–32%. При правильном размещении оборудования по схеме CAC/HAC и хорошем автоматическом регулировании чиллера повышение температуры охлаждающей воды и соответствующее повышение температуры воздуха, подаваемого в ЦОД, не только допустимо, но и дает значительный экономический эффект в виде экономии потребляемой электроэнергии.

Увеличение разности температур воды на входе и выходе чиллера

Еще один способ экономии электроэнергии при работе чиллеров – увеличение разности температуры воды на входе и выходе чиллера (ΔT = ECHWT – LCHWT). Расход воды и параметр ΔT связаны между собой обратной зависимостью в соответствии с формулой:

$$\text{Массовый расход} = \frac{\text{Тепловая нагрузка}}{\text{Удельная теплоемкость} \times \Delta T}.$$

При постоянной тепловой нагрузке холодильной установки с ростом ΔT расход воды уменьшается линейно (1:1). Однако мощность насоса (HP) связана с массовым расходом кубической зависимостью (GPM – расход в г/мин):

$HP_1 / HP_2 = (GPM_1 / GPM_2)^3$.

С уменьшением расхода требуемая мощность насоса соответствующим образом уменьшается. Это приводит к значительному сокращению энергопотребления всей установки в целом. Далее, уменьшение расхода и возможность использования насосов меньших габаритов позволяют устанавливать менее мощные частотно-регулируемые приводные электродвигатели и применять на объекте трубопроводы меньших диаметров.

В качестве примера рассмотрим холодильную установку производительностью 4000 тонн холода США (14 052 кВт), функционирующую в ЦОДе площадью примерно 9300 м² с тепловыделением поряд-

Табл. 2. Альтернативный вариант моделирования при ΔT = 8,9°C

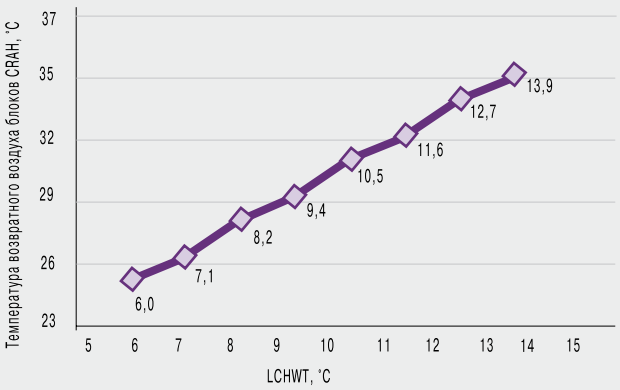
LCHWT, °C	5,56	6,67	7,78	8,89	10	11,11	12,22	13,33
Средняя температура возвратного воздуха на блоках CRAH, °C	25,6	26,7	28,3	29,4	31,1	32,2	33,9	35
Энергопотребление механических систем								
Вентиляторы испарителя, кВт	3 580 379	3 698 985	3 876 014	3 442 172	3 629 544	3 629 544	3 350 360	3 350 360
Чиллеры, кВт	18 060 694	17 284 253	16 705 758	16 541 570	16 001 437	15 528 821	15 123 721	14 778 171
Градирни, кВт	838 747	838 747	838 747	838 747	838 747	838 747	838 747	838 747
Насосы, кВт	1 393 278	1 393 278	1 393,278	1 393 278	1 393 278	1 393 278	1 393 278	1 393 278
Суммарная мощность механических систем, кВт	**23 873 099**	**23 215 264**	**22 813 798**	**22 215 768**	**21 863 007**	**21 390 390**	**20 706 107**	**20 360 556**
Годовая экономия, кВт	932 118	1 589 952	1 991 418	2 589 448	2 942 210	3 414 826	4 099 109	4 444 660
Годовая экономия, $	74 569	127 196	159 313	207 156	235 377	273 186	327 929	355 573

ка 1,6 кВт/м² (реальная установка находится в Вашингтоне, округ Колумбия). Объект обслуживается четырьмя 1000-тонными центробежными чиллерами, четырьмя 1000-тонными башенными градирнями и насосной системой переменной производительности. Параметр LCHWT изменялся в диапазоне от 5,6 до 13,3°C с шагом 1,1°C.

Было проведено компьютерное моделирование с двумя значениями параметра ΔT, что позволило получить данные для достаточно точной интерполяции в пределах диапазона изменения LCHWT. В базовом варианте (табл. 1) моделирование проводилось для значения ΔT = 5,6°C. В альтернативном варианте было взято значение ΔT = 8,9°C (табл. 2). В обоих случаях параметр ΔT для воды на стороне конденсатора был принят равным 6,7°C, при этом температура воды на выходе конденсатора была равна 29,4°C. Стоимость электроэнергии принята равной $0,08 за 1 кВт (т.е. цене, по которой электроэнергия отпускается на коммунальные нужды).

Прежде чем анализировать данные о суммарной экономии электроэнергии для обоих значений параметра ΔT, обратим внимание на один важный момент. Температура возвратного воздуха на блоках вентиляционного агрегата компьютерного зала (CRAH) увеличивается пропорционально росту LCHWT (рис. 2). Температура возвратного воздуха может служить мерой средней температуры воздуха

Рис. 2. Корреляция между LCHWT и температурой возвратного воздуха блоков CRAH



в помещении, и нужно подчеркнуть прямую корреляцию этой величины с параметром LCHWT, что может оказывать отрицательное влияние на температурный режим в ЦОДе. На практике это означает, что надлежащее размещение рядов стоек по схеме HAC/CAC с тем, чтобы направлять горячий воздух обратно на блоки CRAH, является обязательным. Если этого не сделать, то потребуется установить большее число этих блоков, чтобы компенсировать более высокую температуру возвратного воздуха. В результате электродвигатели вентиляторов блоков CRAH будут потреблять электроэнергии больше,

Рис. 3. Зависимость эффективной мощности насоса охлаждающей воды от параметра ΔT

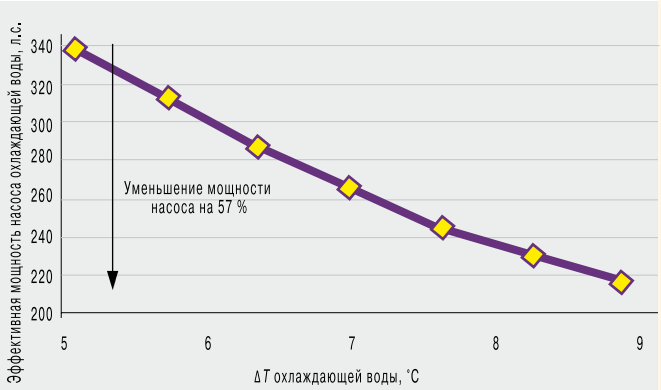
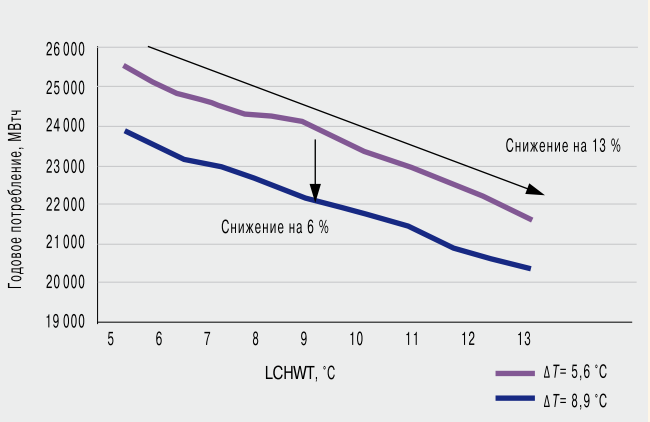


Рис. 4. Зависимость годового энергопотребления от параметров LCHWT и ΔT



чем чиллеры и насосы. Наша компьютерная модель схему размещения оборудования в ЦОДе учитывала, поэтому температура возвращаемого воздуха менялась с изменением LCHWT, но это не потребовало повышения мощности вентиляторов блоков CRAH.

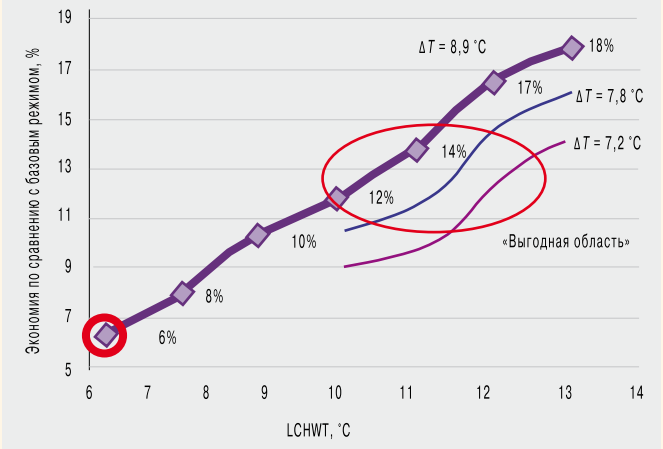
А вот зависимость мощности насоса охлаждающей воды от параметра ΔT обратная: при повышении ΔT от 5,6°C до 8,9°C мощность снизилась на 57% (рис. 3). Как будет показано ниже, такое уменьшение мощности значительно снижает энергопотребление объекта в целом.

Суммарное потребление электроэнергии в ЦОДе при повышении температуры воды на выходе чиллера снижается на 13% при обоих вариантах значения параметра ΔT (рис. 4). Однако при переходе от базового (ΔT = 5,6°C) к альтернативному варианту (ΔT = 8,9°C) энергопотребление сокращается еще на 6–8%.

Большинство существующих чиллерных установок рассчитаны на работу в режиме, который можно назвать базовым: LCHWT = 6,7–7,2°C, ΔT = 5,6°C. Поэтому у пользователей может появиться естественное желание посмотреть, какую экономию электроэнергии можно получить, если при любом допустимом значении LCHWT перейти на ΔT = 8,9°C. Экономия может составить от 6 до 18% (рис. 5). Зону, где LCHWT находится в диапазоне 10–12,8°C, а экономия электроэнергии – 10–14%, назовем «выгодной областью». Такой термин используется потому, что переход на соответствующий температурный режим по LCHWT довольно легко реализовать без отрицательных последствий для качества автоматического регулирования работы чиллера и без существенного ухудшения теплового режима в помещении ЦОДа. Дальнейшее повышение LCHWT от 12,8 до 15,6°C «с хвостиком» обеспечивает еще большую экономию электроэнергии – между 15 и 18%. На практике это достижимо, но только при условии тесного взаимодействия с фирмой – изготовителем чиллера, поскольку необходимо предотвратить риски, связанные с работой в режиме малой разности давления хладагента в конденсаторе и в испарителе.

На рис. 5 показаны также линии, отвечающие двум еще более низким значениям параметра ΔT. Моделирование соответствующих вариантов не проводилось. Эти линии нанесены на график только для того, чтобы показать, где будут находиться промежуточные значения процента экономии электроэнергии и что соответствующие графики можно получить методом интерполяции.

Рис. 5. Экономия энергопотребления при ΔT = 8,9 °C по сравнению с базовым режимом (LCHWT = 6,7 °C, ΔT = 5,6 °C)



Инженеры-проектировщики и службы эксплуатации могут добиться существенной экономии электроэнергии и, соответственно, денежных средств выбором оптимальных значений температуры воды на выходе из чиллера и разности температур охлаждающей воды на входе в чиллер и выходе из него. Идеальными «кандидатами» на работу в режиме с LCHWT в диапазоне 10–12,8°C при более высоком, нежели традиционно, значении ΔT являются ЦОДы. Переход на такие значения указанных параметров в «умеренном» варианте может дать экономию энергоресурсов на 10–14%, а в «агрессивном» – 15–18%. ИКС

Модернизация классики цодостроения

Модульные дата-центры

По мере развития новых требований и подходов к проектированию и эксплуатации технологических площадок всё заметнее становится интерес к модульным дата-центрам. И здесь у России есть шанс успешно конкурировать с западными разработками.

Александр МАРТЫНЮК, директор проекта ЕРЦОД компании «Ростелеком»

Игорь АНИСИМОВ, директор департамента инженерных систем NVision Group, ATD

Новые запросы нового века

В начале 2000-х стало очевидно, что классическая концепция дата-центра перестала соответствовать реалиям рынка и ей необходимо найти более жизнеспособную альтернативу. Сначала на Западе, а потом и в России задачи бизнеса и условия конкуренции начали требовать от компаний развертывать дата-центры более оперативно, чем позволяли традиционные технологии. Иногда это была временная мера, которая давала возможность выдержать темп развития бизнеса в ожидании ввода в действие строящейся площадки либо обеспечить решение краткосрочных бизнес-задач с заданным качеством и к нужному сроку. В других случаях компании были заинтересованы в быстром создании постоянного дата-центра, пусть даже ценой более высоких затрат на строительство. В ответ на эту потребность в 2005–2007 гг. в США (эта страна – безусловный лидер на международном рынке дата-центров), а затем и в Западной Европе сформировались два типа услуг: «дата-центр напрокат» и «дата-центр в контейнере». Первую модель с успехом начала практиковать SunGuard – она вот уже более двух лет предлагает своим заказчикам полную линию разных по масштабам законченных решений: от одного фургона (SunGard Mobile Data Center), готового к размещению 25 рабочих мест, до целого автопарка, предназначенного для развертывания полноценного мобильного офиса (SunGard Mobile Metro Center), в котором достаточно комфортно могут разместиться 175 рабочих групп. Со второй пионером была компания APC (автор концепции InfraStruXure Express Medium Density On-demand Mobile Data Center), конкуренцию которой вскоре составил инфраструктурный комплекс ISE Cube, а также решения мировых ИТ-грандов – Sun Microsystems (ныне подразделение Oracle), IBM, HP, Microsoft.

В России на тот момент рынок услуг дата-центров как самостоятельное направление ИТ-бизнеса только начал зарождаться. Произошло это на фоне активного насыщения разных секторов экономики вычислительными системами и «железом» новых поколений. Большинство корпоративных площадок с морально устаревшей инфраструктурой не соответствовало требованиям к эксплуатации этих систем. И хотя поначалу вал проектов строительства коммерческих дата-центров был остановлен несоответствием пред-

ложения требованиям клиентов, все же дело сдвинулось с мертвой точки. Сегодня Россия уже является активным участником дискуссий и изысканий на тему модульных дата-центров (МДЦ).

Еще одной, не менее важной предпосылкой появления МДЦ стал активный рост потребления ИТ-продуктов разных поколений. В разных дата-центрах мира рядом с морально устаревающим «юнитовым железом» появились «лезвия» и программно-аппаратные комплексы с высокой вычислительной плотностью. Этот тренд особенно четко прослеживался в крупных коммерческих дата-центрах, а также в высокотехнологичных сегментах экономики, где в 2007–2010 гг. активно шла консолидация ИТ-активов. По мере увеличения числа стоек с блейд-системами и их аналогов в классических серверных залах, рассчитанных на стойки с энергопотреблением 3–5 кВт, становилась очевидной необходимость новых подходов к ЦОДостроению. Рынок сегодня демонстрирует заинтересованность в компактных площадках, пригодных для размещения стоек и оборудования с высоким энергопотреблением и при этом оснащенных энергоэффективными и экологичными инженерными системами, способными отводить большое количество выделяемого тепла.

Три типа модульных решений

На сегодняшний день термин «модульный дата-центр» применяют к технологическим площадкам трех типов. Это:

- комплексные решения на основе «дата-центров в коробке» – они имеются у Microsoft, HP, Rittal, Google;
- модульные здания ЦОДов со стандартизованной инфраструктурой, современные аналоги классических стационарных площадок с зональным распределением вычислительных ресурсов и единым инженерным ядром – примером такого дата-центра является «бабочка» HP;
- «легоподобные» энергоэффективные комплексные решения из модулей заводского изготовления – за рубежом такие решения выпускаются под брендами BladeRoom, Colt, AST SSD, HP EcoPOD, I/O Anywhere, в России о завершении собственной разработки этого класса заявила в 2010 г. компания Stack Labs.

О достоинствах и специфике использования контейнерных решений в свое время говорилось и писалось довольно много. С технической точки зрения эти решения довольно привлекательны — в момент поставки заказчик получает почти готовое к эксплуатации решение, который может функционировать и как самостоятельная единица, и как квант крупного дата-центра. Но не стоит упускать из виду, что за этим «почти» стоит необходимость подготовки ровной площадки, подключения электроэнергии, каналов связи, воды, канализации, наличия свободных мощностей на холодильной машине (а если мобильный ЦОД должен быть отказоустойчивым, то на двух холодильных машинах). К тому же, если такой квант рассчитан на напряжение 110 В, как в случае Sun Blackbox, то еще придется поставить трансформаторы. И хорошо, если обо всех этих нюансах вендор известит заказчика заранее.

Существенным фактором, сдерживающим использование контейнерных решений, является их высокая себестоимость. Но несмотря на это, решения данного класса пользуются заслуженным успехом у крупных ИТ-компаний и операторов связи, а также в тех отраслях, специфика которых требует регулярно оперативно развертывать территориально удаленные узлы корпоративной инфраструктуры. Наглядный пример тому – признание российской версии контейнерного МЦОД Daterium, разработанного компанией «Ситроникс».

Опыт, полученный ИТ-рынком на этапе создания модульных дата-центров контейнерного типа, позволил двигаться дальше в поисках решения, отвечающего ожиданиям рынка. Ключевыми ориентирами в этом поиске стали доступная стоимость владения дата-центром, универсальность по отношению к системам с разной вычислительной плотностью, а также снижение коэффициента PUE.

В этом плане обращает на себя внимание HP POD 240a (EcoPOD), представляющий собой сборку из двух 40-футовых модулей для размещения ИТ-оборудования, которая выполняется по конвейерному принципу на специальной площадке в Хьюстоне. Отличие EcoPOD от более старших моделей – использование не водяного, а воздушного охлаждения. Благодаря этому удалось существенно повысить энергоэффективность дата-центра и обеспечить отвод до 44 кВт тепла от каждой из 44 50-юнитовых стоек. Именно на блейды и аналогичные им решения с высокой вычислительной плотностью была сделана ставка при разработке HP POD 240a – размещение в нем стоек со стандартным оборудованием экономически невыгодно.

ЦОД в контейнере (HP EcoPOD)

Модульные решения Blade Room

Что касается модульных решений принципиально нового типа, аналогия с конструкторами «Лего» неслучайна: такие решения позволяют в короткие сроки создавать из типовых стандартных элементов дата-центры с технологическими параметрами по «лекалам» заказчика. Начнем обзор с разработки британской компании BladeRoom, которая в течение 20 лет специализируется на предоставлении технически сложных модульных установок заводского производства заказчикам, работающим в сфере здравоохранения, в оборонной и государственной отраслях и т. д. Энергоэффективное решение (PUE 1,13), созданное этой компанией, позволяет реализовать дата-центр любого масштаба — от 10 до 240 и более стоек. Допустимая нагрузка на стойку – от 1 до 24 кВт, причем никаких ограничений на размещение по соседству решений с разной вычислительной плотностью нет. Мощности такого дата-центра вводятся в эксплуатацию не единовременно, а по мере необходимости; в случае готовности площадки новый модуль может быть развернут в течение 12 недель. Дизайн дата-центра BladeRoom сертифицирован Uptime Institute на соответствие Tier III. Компания позиционирует свою разработку как оптимальное start-up решение для малого и среднего бизнеса либо как инфраструктуру для организации удаленного резервного узла поставщиков услуг colocation.

Аналогичные параметры заявлены и для дата-центра IO Anywhere, созданного в США в 2007–2010 гг. Его коэффициент PUE составляет 1,17, что достигается во многом за счет использования высокоэффективных систем для отвода тепла от модулей, заполненных вычислительными системами.

Модули IO Anywhere представляют собой сборные стальные конструкции заводского производства. Они сейсмически устойчивы, что позволяет разворачивать дата-центры даже в регионах, подверженных землетрясениям. Внутри каждого модуля имеется фальшпол, способный выдержать физическую нагрузку до 700 фунтов на квадратный фут.

Первый проект с использованием этого решения был реализован в прошлом году в Нью-Джерси (США), где всего за 90 дней был развернут дата-центр с общим энергопотреблением 3,6 МВт. Комплекс модулей IO Anywhere был произведен и укомплектован на фабрике IO в Финиксе (шт. Аризона), а затем доставлен на трейлерах в модульный центр IO в Эдисоне (шт. Нью-Джерси).

Еще один красивый проект ввода в эксплуатацию модульного дата-центра был закончен в начале нынешнего года в Исландии. Речь идет о технологической площадке Verne Global площадью 500 кв. м, для размещения которой была выбрана территория бывшего командного центра НАТО площадью 18 га. Весь цикл строительства объекта, собранного из 37 модулей Colt Data Center Services, занял четыре месяца. Особенность этого дата-центра – 100%-ное потре-

бление энергии от возобновляемых источников кампуса Кефлавик. Новый форм-фактор модулей Colt (представленный в 2011 г.) позволяет создавать гермозоны площадью 125, 250 и 375 кв. м и впоследствии постепенно наращивать их дополнительными модулями, а также регулировать диапазон плотности электропитания – от 750 Вт до 3 кВт на квадратный метр. На конференции DataCentres Europe 2011 компания отчиталась о результатах глобальной модернизации действующих дата-центров, позволившей сократить величину PUE на 10%, за что ей была присуждена премия за энергоэффективность ЦОДов – The European Award for Energy Efficiency in Data Centres.

Экологичность и энергоэффективность

Тема экологичных и энергоэффективных решений все явственнее переходит из разряда поисков и дискуссий в сферу практической реализации – равно как и проблема оптимизации инфраструктурного базиса дата-центров, возможность его использования при развертывании облачных сред. К примеру, компания Huawei заявила в конце прошлого года о создании серии интеллектуальных ЦОДов нового поколения (Intelligent Data center Solution – IDS), включающей мобильные ЦОДы (IDS1000) и дата-центры модульного типа (IDS2000). В числе достоинств IDS1000 – возможность использования вне помещений и снижение потребляемой энергии вдвое по сравнению с классическими дата-центрами, а также способность работать в условиях стихийных бедствий, масштабных мероприятий или военных операций. В IDS2000 интересны современные технологии охлаждения, в том числе принцип разделения потоков холодного и горячего воздуха, точная подача воздуха и наружное охлаждение, что обеспечивает коэффициент энергопотребления PUE менее 1,2. Интеллектуальная система управления Huawei iFOS динамически регулирует энергоснабжение и охлаждение в соответствии с нагрузкой платформы облачных вычислений.

Строительство ЦОДа Verne Global в Исландии

Впрочем, вопрос о необходимости эффективного управления воздушными потоками в дата-центре занимает не только западные компании: в России свое решение этой проблемы предложили сразу два игрока ИТ-рынка. В 2011 г. компания «Аякс-Инжиниринг» завершила проект строительства дата-центра для «Яндекса» с мощностью ИТ-нагрузки 2,2 МВт. В проекте была использована запатентованная система охлаждения ЦОДа Full freecooling (FFC), которую специалисты компании создали на базе промышленного образца теплообменника Kyoto Cooling. Использование восьми таких установок на 280 кВт (по две FFC на каждый из четырех машинных залов) позволило разместить в дата-центре 96 средненагруженных стоек по 12 кВт и 72 высоконагруженные стойки по 15,5 кВт. Расчетный PUE нового дата-центра «Яндекса» составляет 1,11–1,49, среднегодовой PUE равен 1,17.

Не исключено, что подход к организации охлаждения в высоконагруженных дата-центрах «Аякс-Инжиниринг» составит достойную альтернативу решению, задействованному в комплексной разработке модульного дата-центра другой российской компании – Stack Labs. Летом 2010 г. она объявила об успешном тестировании прототипа модульного энергоэффективного дата-центра со среднегодовым значением PUE 1,2 и ниже (вплоть до 1,02). Базовыми элементами этого МДЦ служат стандартизованные модули заводского производства. Как следует из отчета по результатам апробации решения, его ключевое достоинство – комплекс интегрированных систем мониторинга и управления эксплуатационными параметрами дата-центра. Они позволяют в режиме реального времени выстраивать оптимальный алгоритм межсистемного взаимодействия на уровне ключевых для дата-центра элементов инженерной инфраструктуры.

Интеллектуальная система диспетчеризации, предусмотренная в таком МДЦ, позволяет консолидировать поступающую информацию и автоматически «выдавать системам указания» о порядке необходимых операций. Скажем, при изменении характера нагрузки на стойки в серверных залах система кондиционирования, основанная на принципе фрикулинга, автоматически адаптирует режим воздухообмена в ЦОДе. В дата-центрах, которые, как ожидается, уже в 2012 г. пополнят ресурсы сети Stack Data Network, можно будет размещать стойки любой энергонагруженности — от стандартных 5–6 кВт

SMARTER

DATA CENTER INFRASTRUCTURE.
WE'RE IN IT.

Наши уникальные разработки и технологическое сотрудничество с ведущими производителями активного сетевого оборудования помогают предвидеть Ваши будущие требования к кабельной инфраструктуре.

Наши инвестиции в региональное присутствие обеспечивают Вам нашу компетентную и своевременную техническую поддержку.

Создавая динамичный и высокоэффективный ЦОД, выбирайте продукцию TE Connectivity!

www.datacenteragility.com

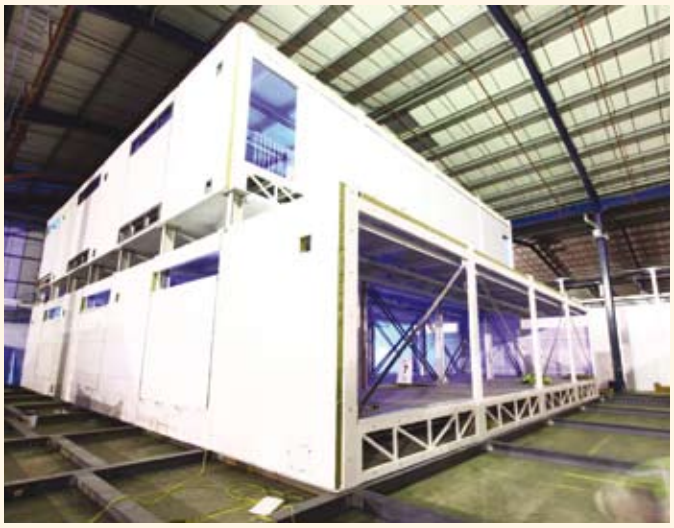
Коммутационная система UCP и шкафы NETpodium для ЦОД:

- Наилучшее решение для объединения «медных» и оптических портов
- Единая коммутационная панель для всех подключений
- Коммутация за пределами 19"-конструктива
- Экономия монтажного пространства и снижение трудозатрат
- Поддержка приложений от 1 до 100 Гбит/с
- Малое время монтажа без использования инструментов
- Оптимальная организация коммутационных шнуров при высокой плотности портов

AMP NETCONNECT

Представительства:
Москва: (495) 790-7902
Екатеринбург: (343) 253-1153
Новосибирск: (383) 230-4099
www.ampnetconnect.ru

TE connectivity



Модульный ЦОД Colt в процессе сборки

на стойку до 40 кВт; есть и возможность повышения уровня отказоустойчивости площадки без перерыва в предоставлении сервисов. Впрочем, насколько все эти параметры будут выдерживаться на практике, реально можно будет судить только после запуска площадок.

Хорошие перспективы?

Даже беглый обзор форм-факторов МДЦ, доступных сегодня на международном рынке, не оставляет сомнений в том, что классические дата-центры, которые на протяжении многих лет успешно выполняли возложенные на них функции, будут все более активно вытесняться принципиально новыми решениями. Даже убежденные приверженцы «классики» вынуждены отдавать предпочтение более современным проектным решениям – как на этапе начала строительства, так и в процессе эксплуатации площадки.

Столь обширный спектр концепций создания ЦОДов: решения на базе классического подхода, контейнерные решения, адаптивные модульные конфигурации – по большому счету свидетельствует о высоком уровне зрелости международного рынка дата-центров. Потенциальный владелец площадки имеет достаточную свободу выбора, чтобы найти оптимальное для себя решение. Но наиболее перспективным на сегодняшний день, по мнению аналитиков, является все же модульный подход. Он позволяет в будущем существенно сократить затраты на развертывание дата-центра и наиболее близок по своим функциональным характеристикам к требованиям облачных сред. Не случайно на предстоящем аналитическом симпозиуме Uptime Institute в качестве best practice анонсированы именно модульные дата-центры.

Пусть пока проекты, демонстрирующие на практике преимущества модульных подходов, единичны. Но они, во-первых, уже есть. И это свидетельствует о том, что ИТ-рынок постепенно готовится отвечать на новые – как правило, неожиданные – вызовы технического прогресса.

Во-вторых, впервые за многие годы география смелых ИТ-инноваций охватывает не только США и Западную Европу, но и Россию. Как тут не вспомнить годы, когда отечественные НИОКР успешно конкурировали с изысканиями западных научных лабораторий. И это вселяет оптимизм. Похоже, у России действительно есть серьезные шансы вернуть себе утраченные позиции достойного интеллектуально-технического оппонента Запада. ИКС

Новые подходы к пожаротушению в современных ЦОДах

С появлением новых ИТ-сервисов, новых технологий меняется сама концепция построения ЦОДов. Требованиям новой концепции должны соответствовать и системы газового пожаротушения – как неотъемлемая часть современной серверной или дата-центра.

Владимир МАКСИМОВ,
генеральный директор
«Нонфаир»

Павел ИВАНОВ,
технический директор
«Нонфаир»

Появление новых подходов к построению ЦОДов вызвано несколькими причинами; в первую очередь это нехватка свободных мощностей электроснабжения. В современном дата-центре приходится рационально использовать электрические мощности для нужд ИТ, а не для вспомогательной системы охлаждения, что привело к изменению концепции воздухообмена и кондиционирования.

Развитие систем охлаждения сегодня идет в сторону максимально эффективной доставки холодного воздуха к серверным стойкам и эффективного отвода тепла к охладителю. Это привело к тому, что использование обычных кондиционеров потеряло смысл, поскольку

происходило смешивание потоков холодного и горячего воздуха. В настоящее время предпочтение отдается системам с разделением потоков – с организацией в помещении «холодных» и «горячих» коридоров, которые выполняют роль воздуховодов.

Наконец, от дата-центров сегодня требуется постоянная доступность. Развитие информационных услуг достигло такого уровня, что отключение ЦОДа всего на несколько минут может привести к катастрофическим последствиям для бизнеса компании.

Названные причины не просто изменили подходы к построению систем вентиляции и электроснабжения, но и потребовали изменений в других сферах технологического оснащения серверных и ЦОДов, в частности в системах обнаружения пожара и автоматического пожаротушения.

Для организации надежно работающей системы пожаротушения в современных ЦОДах необходимо учитывать большее количество параметров, нежели раньше. Мы покажем, какие именно характеристики ЦОДа влияют на построение системы автоматического газового пожаротушения (ГПТ) и на каких стадиях проектирования необходимо совместно выбирать оптимальные решения для раннего обнаружения возможного очага пожара и его тушения.

Применение фрикулинга

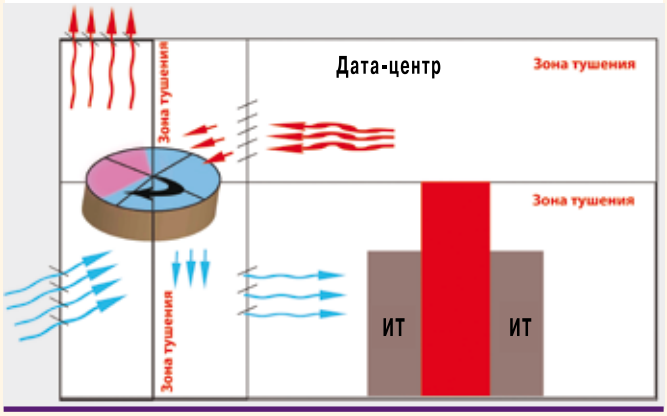
В целях существенной экономии электроэнергии сегодня широко применяется технология свободного охлаждения – Full Freecooling (FFC), согласно которой помещение ЦОДа охлаждается за счет более прохладного воздуха с улицы. Система FFC представляет собой два разомкнутых отдельных контура: наружный и внутренний. Во внутреннем контуре циркулирует воздух ЦОДа, в наружный контур подается уличный воздух. Основным элементом системы является роторный регенератор, в котором происходит теплообмен между воздухом окружающей среды и воздухом в помещении ЦОДа. Задача роторного регенератора заключается в том, чтобы охладить воздух в ЦОДе от +37 до +24°С наружным воздухом с температурой до +22°С.

Такое построение системы охлаждения приводит к тому, что при расчетах установки газового пожаротушения следует учитывать не только объем помещения ЦОДа, но и объем воздуховодов и объем венткамеры внутреннего контура системы FFC (см. рисунок).

Важно отметить, что применение огнезадерживающих клапанов в данном случае неприемлемо, так как системы FFC используются на объектах, остановка которых недопустима даже в критических ситуациях. Герметичность же при тушении достигается остановкой и блокированием ротора рекуперации, но вентиляторы внутреннего контура при этом работают, а охлаждение переходит на классическую схему кондиционирования.

Использование FFC предусматривает организацию в ЦОДе «горячих» и «холодных» зон или коридоров. Такое планировочное решение влечет за собой определенные требования к размещению насадок установки

Типовая схема системы охлаждения Full Freecooling



ГПТ. Точнее, может возникнуть заблуждение о том, что допустима установка насадок-распылителей только у нагнетающего вентилятора, за счет которого произойдет заполнение огнетушащим газом всего защищаемого объема. Такое техническое решение подкупает простотой реализации и минимумом монтажных работ, но может привести к отказу в самый ответственный момент при срабатывании установки ГПТ: при внештатной остановке нагнетающего вентилятора тушение будет неэффективным. Не стоит возлагать функции транспортировки газа для пожаротушения на другие, не предназначенные для этого системы, это не обеспечит равномерного заполнения объема огнетушащим составом за нормативное время. Поэтому при проектировании установок ГПТ необходимо располагать насадки согласно их характеристикам и действующим нормам непосредственно в защищаемом объеме.

Система вентиляции

Неотключаемая система замкнутой вентиляции или охлаждения при выпуске газового огнетушащего вещества (ГОТВ) не противоречит действующим нормам, а лишь требует согласования данного решения в установленном порядке. Немного сложнее ситуация в случае общеобменной системы вентиляции и кондиционирования, где нет возможности установить огнезадерживающие клапаны и отключение вентиляции невозможно по технологическому процессу. В этом случае расчеты выполняются по методикам, разработанным для конкретного объекта, согласно СП5.13130.2009 п. 8.14.3.

Ряд зарубежных специалистов, проводивших натурные испытания «чистых газов», склоняются к тому, что работающая при выпуске ГОТВ система замкнутой циркуляции воздуха не ухудшает, а наоборот, улучшает эффективность тушения, даже без применения повышающих коэффициентов. С зарубежными специалистами можно согласиться, по крайней мере, в случае применения газовых составов с более высокой плотностью, чем у атмосферного воздуха.

При проектировании установок газового пожаротушения в таких помещениях следует рассматривать два случая: работающей системы замкнутой вентиляции и полной остановки воздухообмена. В обоих случаях насадки следует располагать в каждом объеме: и в зонах

«горячих», и в зонах «холодных» коридоров, чтобы обеспечить максимально быстрое создание огнетушащей концентрации в случае отказа вентиляционной системы. Однако если вентиляционная система продолжает работать, не следует при выполнении гидравлического расчета отдавать предпочтения выходу газа за малый промежуток времени. Следует стараться, чтобы время выхода было максимально возможным для данного случая по нормативным документам. Например, для модульной установки время выхода ГОТВ – не более 10 с; следовательно, нужно стремиться к максимально возможному времени 9,9 с.

Используя эти особенности, можно добиться того, чтобы время циркуляции воздуха по замкнутой системе было равно или меньше времени выхода ГОТВ, за счет чего достигается равномерное смешивание ГОТВ в воздухе. Создание огнетушащей концентрации будет равномерным как в случае остановки вентиляции, так и в случае ее работы по замкнутому контуру.

В любой ситуации, когда разрабатывается установка газового пожаротушения для ЦОДа с неотключаемой замкнутой вентиляцией, необходимо учитывать весь объем ЦОДа, вентиляции и венткамеры – физически это один объем. Но при этом необходимо, чтобы и венткороба и венткамера обеспечивали необходимый предел огнестойкости, как, собственно, и сам ЦОД.

Крайне важно также обеспечить герметичность всего этого объема. Обращаясь к опыту зарубежных специалистов, отметим, что для них выполнение проекта невозможно без предварительного теста на герметичность помещения и определения реальной негерметичности и времени удержания в этом помещении нормативной огнетушащей концентрации. Хотя в российских нормативных документах и указаны допустимые уровни негерметичности, но остается открытым ряд вопросов: как точно вычислить негерметичность помещения? насколько расчетная негерметичность будет отличаться от реальной после выполнения строительных работ? Если такие вопросы возникают по отношению к помещению в статическом состоянии (в нормах рассматривается вариант без принудительной циркуляции воздуха), то чего ожидать от помещения, которое по расчетам герметично, а фактически параметры негерметичности при работе замкнутой системы вентиляции неизвестны? Следовательно, при проектировании установки ГПТ с рабочей системой замкнутой вентиляции не стоит полагаться на утверждение строителей о том, что помещение абсолютно герметично; вместо этого стоит провести аппаратный тест на герметичность. Такие тесты в России пока не очень распространены, но постоянно усложняющиеся задачи заставляют прибегать к нему (подробнее о тесте на герметичность см. статью А. Анненкова «Противопожарная защита ЦОДов: нужен ли тест на герметичность», ИКС № 1-2'2012, с. 77).

При проектировании таких сложных объектов с общим объемом циркуляции воздуха ставится еще одно условие: применение насадок одного типоразмера (СП5.13130.2009 п. 8.11.6), поскольку нельзя рассматривать каждый выделенный «горячий» и «холодный» коридоры как независимые объемы. Возможность применения насадок разного типа рассматривается в каждом конкретном случае отдельно.

Ошибки проектирования

Перед реализацией архитектурно-планировочных решений ЦОДа необходимо совместно со специалистами газового пожаротушения проработать возможные варианты размещения оборудования, в частности определить место размещения модулей газового пожаротушения, проанализировать нюансы, связанные с воздушными потоками, выполнить гидравлические расчеты, подтверждающие возможность реализации сложных трубных разводок. Основная ошибка здесь – когда планировки выполнены с учетом требований ИТ и уже реализованы, а место для размещения технологического оборудования либо не предусмотрено, либо его выделено недостаточно, а значит, невозможно установить полноценную систему пожаротушения, удовлетворяющую многочисленным требованиям и нормам. Кроме того, необходимо сразу предусмотреть помещение для хранения резервного запаса, если на объекте предусматривается модульная установка ГПТ.

Еще ряд ошибок при строительстве ЦОДов связан с отсутствием клапанов сброса избыточного давления либо с невозможностью их установить, так как на стадии проектирования про них просто забыли или выполнили не все расчеты. Это же касается и установок газоудаления после срабатывания установок ГПТ. Для больших помещений, в том числе и ЦОДОв, предпочтение следует отдавать стационарным установкам, обеспечивающим удаление ГОТВ в короткий промежуток времени без необходимости их сборки и установки, что характерно для переносных дымососов.

При разработке планировочных решений необходимо также определить, строить ли один большой зал или разделить его на ряд небольших помещений огнестойкими ограждающими конструкциями. Такие конструкции позволяют рассматривать каждый зал как самостоятельную зону пожаротушения. Эти решения помогут уменьшить затраты как на строительство, так и на дальнейшую эксплуатацию установок ГПТ.

Кроме технологической части газового пожаротушения, ряд особенностей имеет и электротехническая часть, особенно при проектировании установок пожаротушения в помещениях с постоянным замкнутым воздухообменом.

Не секрет, что при больших воздушных потоках точечные дымовые извещатели не обеспечивают эффективное обнаружение дыма на ранних стадиях, поскольку их место установки по нормативным документам может находиться в стороне от сильных воздушных потоков. В большинстве случаев потоки воздуха просто не успевают подняться до точечного извещателя, установленного на потолке. На обнаружении возгорания негативно сказывается и высокая скорость потоков воздуха, которая препятствует попаданию частиц дыма в оптическую камеру точечного извещателя. Таким образом, пассивный способ определения дыма

(т.е. извещатель «ждет», пока до него дойдет дым) не подходит для определения возгорания в современном ЦОДе. В нашем случае единственным проверенным решением является активное обнаружение дыма, т.е. извещатель должен сам взять пробы воздуха и проанализировать их на задымленность.

Таким требованиям удовлетворяют аспирационные извещатели с установкой воздухозаборных трубок на пути воздушного потока, например в вытяжном венткоробе. Гибкие настройки аспирационных извещателей позволяют достоверно определить уровень задымленности помещения даже при высоких скоростях потоков воздуха. Но применение аспирационных извещателей обеспечит безотказное обнаружение только при нормально действующей установке вентиляции и кондиционирования, а что будет, если вентиляционная система отключена? Как показывает опыт, оптимальным решением в таких случаях является применение аспирационных извещателей совместно с точечными извещателями; это обеспечит раннее обнаружение дыма в любом состоянии системы вентиляции и кондиционирования.

В заключение хотелось бы еще раз отметить, что на данном этапе, при большом интересе компаний к новым технологиям охлаждения, для правильного выбора технического решения установок ГПТ необходимо рассматривать большее количество факторов. Кроме «голых» архитектурных планировок помещений будущего ЦОДа проектировщику системы газового пожаротушения необходима информация о предполагаемой системе вентиляции, о размещении оборудования в ЦОДе, схеме организации выделенных объемов «холодных» и «горячих» коридоров, функциональном назначении фальшполов и фальшпотолков, возможности или невозможности отключения вентиляции и системы кондиционирования. Место для размещения оборудования ГПТ и трассировку трубопроводов лучше определить на ранней стадии подготовки архитектурно-планировочных решений. Следует также по предварительным расчетам совместно определить количество и место расположения клапанов сброса избыточного давления и системы газоудаления. Крайне важно, на наш взгляд, провести тест на герметичность по завершении общестроительных работ, чтобы иметь возможность внести изменения в проектируемую установку пожаротушения.

Все перечисленные характеристики помещений ЦОДа необходимо учесть в совокупности на ранних стадиях проектирования. Опыт показывает, что чем раньше при проектировании сложного объекта уделяется внимание вспомогательным системам, в том числе системам безопасности, тем более органично они вписываются в общую инфраструктуру объекта и тем лучше выполняют свои функции. ИКС

Пожарная безопасность ЦОДов: актуальные вопросы

Антон АННЕНКОВ,
исполнительный директор
ГК «Пожтехника»

При создании системы пожарной безопасности ЦОДа абсолютно оправдано применение высокочувствительных аспирационных дымовых детекторов типа VESDA в комбинации со стандартными адресно-аналоговыми детекторами дыма. В современной практике такое решение стало фактически типовым: при высокой интенсивности воздухообмена в помещении ЦОДа лазерная аспирационная технология – едва ли не единственный способ раннего (а значит, своевременного) обнаружения дыма. Технология VESDA позволяет создать систему, способную обнаружить начальную стадию задымления даже в каждой отдельной стойке – для этого потребуется детектор специального исполнения с 15 отдельными адресными аспирационными каналами.

Как известно, выделению дыма предшествует довольно длительная стадия нагревания неисправного элемента внутри юнита. Пока не началось выделение дыма, выявить проблему могут только газоанализаторы, настроенные на монооксид углерода CO (выделяется любым источником перегрева) и водород (выделяется при перегреве аккумуляторов и элементов питания). Аспирационный датчик-газоанализатор VESDA, встроенный в ту же систему, что и дымовой датчик, на ранней стадии способен обнаружить проблемы в юните. Разумеется, применение газоанализаторов увеличивает стоимость системы безопасности, но выводит отказоустойчивость ЦОДа на более высокий уровень.

Вопрос о реальной степени герметичности помещений ЦОДа, защищенных системой автоматического газового пожаротушения, действительно встал на российском рынке относительно недавно – с приходом крупных западных подрядчиков с их стандартами и опытом. Специалисты ГК «Пожтехника» провели серию испытаний на герметичность в ЦОДе DataSpace как перед монтажом системы пожаротушения, так и после. Тест на герметичность может дать возможность существенно сэкономить, в частности, избежав установки или сведя к минимуму число клапанов сброса избыточного давления (правда, в сочетании с применением огнетушащих веществ с минимальной объемной рабочей концентрацией, таких как 3M Novec 1230).

А наиболее важная, на мой взгляд, мысль, которая прозвучала в статье, – это тезис о том, что для разработки качественных решений для пожарной безопасности ЦОДа необходимо учитывать критичные характеристики помещений на ранних стадиях принятия проектных решений и обязательно анализировать эти характеристики в совокупности. Только такой подход позволит создать действительно надежную и эффективную систему пожарной безопасности – и при этом даже сэкономить порой весьма значительные средства.

Модульная корпусная система

Система TS IT состоит из стойки для сетевого или серверного оборудования и стандартизированных аксессуаров с уменьшенной сложностью и поддержкой технологии скоростной сборки Plug & Play.

Аксессуары, такие как приборные полки и раздвижные направляющие, могут быть смонтированы одним человеком без инструментов. Расстояние между 19" монтажными уровнями также может быть изменено без инструментов, а ширина шкафа может составлять также 21", 23" или 24". Допустимая нагрузка на один 19" уровень – 1500 кг.

В комплект ИТ-шкафа входят универсальный 19" монтажный уровень, двухсекционные боковые стенки с быстрозажимным креплением и оптимизированные щёточные кабельные вводы.

Двери могут быть перфорированными или сплошными. Перфорированные, с площадью вентиляции 85%, используются в помещениях с климат-контролем. Все двери открываются на 180 градусов. Задние двери в шкафах TS IT – двустворчатые. Шкаф имеет достаточно плотные прокладки, чтобы использовать газовый огнетушитель в случае пожара, а также позволяет установить корпусную систему климат-контроля.

В качестве альтернативы обычным цоколям для TS IT доступна система Flex-Block, которая может быть легко собрана. Кабельные направляющие и ролики могут быть быстро добавлены к цоколю.

Шкаф TS IT может быть адаптирован для автоматизированной инвентаризации установленного в него оборудования – серверов и коммутаторов – добавлением полосок с RFID-метками.

«Риттал»: (495) 775-0230

Система управления инфраструктурой ЦОДа

В программно-аппаратный комплекс CenterMind входят следующие подсистемы.

CenterMind G+ постоянно (24/7) в режиме реального времени предоставляет информацию о параметрах окружающей среды в серверной комнате или ЦОДе. Подсистема может использоваться как для мониторинга одного шкафа в удаленном филиале, так и для комплексного обслуживания крупного ЦОДа. В CenterMind G+ входят контроллеры и набор датчиков для измерения параметров окружающей среды (температуры, влажности, воздушного потока, утечки воды, пожарный, открытия двери и т.д.). Поддерживаются датчики двух типов: аналоговые (измеряющие точное значение заданного параметра) и пороговые (срабатывающие на определенное событие). К одному контроллеру в зависимости от его типа может подключаться от 4 до 32 датчиков.

Подсистема CenterMind P+ позволяет организовать удаленный мониторинг энергопотребления отдельно для каждого устройства в ЦОДе. Подсистема базируется на линейке блоков распределения питания (PDU), от простых розеточных блоков до интеллектуальных, предоставляющих данные об энергопотреблении на каждую розетку и позволяющих дистанционно отключать оборудование или перезагружать серверы. Блоки PDU выпускаются с различной плотностью розеток, как одно-, так и трехфазных. Они могут быть смонтированы сбоку или сзади шкафа, экономя дорогостоящее монтажное пространство.

Подсистема PatchView контролирует кроссовые поля СКС ЦОДа, определяет состояния подключения коммутационных шнуров и идентифицирует медные и оптические панели.

Доступ к контроллерам подсистемы CenterMind G+ и контроль над PDU (CenterMind P+) осуществляется как через встроенное ПО, так и через внешнее ПО CenterMind. Встроенное и внешнее ПО построены на основе веб-технологий и не требуют установки клиентского ПО.

ПО CenterMind обеспечивает интеллектуальное управление инфраструктурными системами ЦОДа через единый графический интерфейс.

RiT Technologies: (495) 684-0319

Гигабитный стекируемый коммутатор
второго уровня

ECS4810-28TS – продукт серии ECS 4500, нацеленный на рынок бизнес-пользователей. Устройство имеет 24 порта 1000BASE-TX и четыре гигабитных комбо-порта (RJ-45/SFP). Отличается расширенным диапазоном рабочих температур (–20–65°C). Может управляться напрямую через команды CLI или через простой графический веб-интерфейс.

Коммутатор обеспечивает гибкое стекирование до 16 устройств с общей полосой пропускания до 4 Гбит/с и возможностью управления через один IP-адрес. IEEE 802.1w Rapid Spanning Tree Protocol обеспечивает работу сетей без образования петель и создает резервный маршрут с быстрой сходимостью. Протокол IEEE 802.3ad Link Aggregation (LACP) через объединение нескольких физических каналов в один логический создает более широкую полосу пропускания. IGMP Snooping ограничивает полосу интенсивного видеотрафика, исходя из запросов пользователей.

ECS4810-28TS применяет Class of Service (CoS) стандарта 802.1p, а также задействует поле DSCP в заголовке IP-пакета для классификации передаваемой информации. Четкое формирование приоритетных очередей гарантирует, что трафик с высоким приоритетом обслуживается первым.

Для безопасности портов коммутатор использует IP Source Guard и Port Security, обеспечивая доступ к своим портам на базе MAC-адреса, может ограничивать число подключенных устройств и защищает от атак MAC flooding. В дополнение могут быть задействованы три типа списков контроля доступа (ACLs) для отклонения пакетов на основе MAC-адреса, IP-адреса или портов TCP/UDP. Поддерживается функция DHCP Snooping, которая позволяет отправлять запросы DHCP только конкретному серверу.

В коммутаторе ECS4810-28TS реализована функциональность IPv6, включая стекирование по двойному протоколу (IPv4 и IPv6), и поддержка функций управления IPv6 для SNMP, Telnet и TFTP.

Edge-Core Networks Corporation: (916) 685-8272

Серверы с возможностями самодиагностики

В серверах линейки ProLiant Gen8 реализованы технологии Active Health и Insight Online, которые позволяют им автоматически анализировать собственное состояние по 1600 параметрам. Технология Insight Online опирается на одноименный портал по управлению ИТ-ресурсами и поддержке, основанный на облачных технологиях. Кроме того, архитектура ProActive Insight обеспечивает автоматизацию жизненного цикла серверов: контролирует их исправность, расход электроэнергии и другие аспекты производительности. Технология HP 3D Sea of Sensors выявляет перегруженные серверы в реальном времени, что на 70% повышает коэффициент производительности на ватт по сравнению с моделями ProLiant G7.

В линейку ProLiant Gen8 входят шесть моделей: ML 350p в корпусе «башня» для филиалов и удаленных офисов; DL 380p и DL 360p для монтажа в стойку; блейд-серверы BL 460c для конвергентной архитектуры, готовой к развертыванию облака; масштабируемые серверы SL 230s и SL 250s для поддержки веб-приложений, облачных технологий и высокомасштабируемых сред.

В частности, блейд-серверы BL 460c оснащены процессорами Intel Xeon серии E5-2600, имеют 16 слотов четырехканальной памяти DDR3, расширение до 512 Гбайт. Может использоваться память HP, способная работать на частоте 1600 МГц при пониженном энергопотреблении (1,35 В). Имеются три слота расширения PCIe x3; съемная карта сетевых подключений Flexible LOM (LAN on Motherboard) позволяет менять доступные сетевые порты (от Ethernet до Infiniband). Подсистема хранения данных: контроллер Smart Array с флешем 512 Мбайт, до двух жестких дисков. Блейд-серверы рассчитаны на использование с внешними системами хранения данных.

Система удаленного управления и мониторинга iLO Management Engine является развитием системы iLO, которая использовалась в предыдущих поколениях серверов HP ProLiant.

HP: (495) 797-3500

Блог, еще раз блог!

Владимир ЛИТВИНОВ

Салат «Столичный» от «Ростелекома»

>>>>...Из «курицы, несущей золотые яйца» в 90-х годах и принесшей при вхождении в «Ростелеком» почти 50% дополнительных доходов, ММТ за десятилетие функционирования в составе «Ростелекома» благополучно превратился в «пятое колесо» московской телекоммуникационной «телеги».

Я не собираюсь в сжатом блоге анализировать причины стремительного падения компании (отсутствие преемственности и постоянная чехарда с назначениями топ-менеджеров, привлекательные для продажи непрофильные активы ММТ, борьба с издержками при отсутствии диверсификации бизнеса...). Результатом стало малопонятное включение филиала ММТ в состав другого макрорегионального филиала «Центр» «Ростелекома» (честно говоря, плохо понимаю такое структурное построение), объединяющего еще 17 филиалов Центрального региона. При этом филиал «Междугородный и Международный Телефон» еще и переименовали в филиал «Столичный» – это решение принял совет директоров в связи с тем, что «старое название не в полной мере соответствует целям и задачам компании в столичном регионе». Таким образом, некогда известный в Москве бренд, как «не соответствующий», прекращает свое существование. Позвольте, а бренд «Центральный телеграф», «МГТС» или, например, «Московский комсомолец» соответствует «целям и задачам» современного периода? Старому бренду ММТ можно было бы придать современное звучание (например, Московские МедиаТехнологии), все-таки товарный знак «Столичный» является интеллектуальной собственностью совсем другого, ликеро-водочного бизнеса. Может быть, имело смысл вернуть историческое название ЦМТС, как любовно называют родное предприятие ветераны (например, Центр Московского Телекоммуникационного Сервиса), что более органично вписалось бы в МРФ «Центр» «Ростелекома».

Конечно, новоиспеченному совету директоров «Ростелекома», похоже, не имеющему представления об истории отечественной связи, в период тотальной инсталляции вебкамер на избирательных участках, консолидации активов и международной экспансии «Ростелекома» обращать внимание на имена филиалов...

Меня, например, раздражает, когда в подвале здания Министерства связи на Тверской, 7 (построено в 1930 году и получило имя «Дом связи им. Подбельского») функционирует ресторанчик со странным именем «Старый телеграф», как будто есть «новый телеграф»...

комментировать

Геннадий ФОКИН

Менеджмент интеллектуальных ресурсов ВПК

>>>> Служебная интеллектуальная собственность является частью производственных ресурсов, НИОКР и проектных работ предприятий, результатов интеллектуальной и научно-технической деятельности работников, объектом менеджмента качества наукоемкой высокотехнологичной продукции. Особое значение менеджмент интеллектуальных ресурсов имеет в военно-промышленном комплексе, где реализуются последние достижения науки и техники, а производство регламентируется национальными и корпоративными стандартами предприятий ВПК.

...

Закономерно возникают вопросы:

— Почему к результатам интеллектуальной деятельности, которым предоставляется правовая охрана, причислены «нововведения, техническая информация, научно-технические и программные разработки, отчеты, знаки, логотипы и аналогичная информация, которая относится к действующему бизнесу работодателя»?

— Почему работодателю принадлежат исключительные права на интеллектуальную собственность, созданную до оформления трудовых отношений (подписания трудового договора с работником)?

— Почему работодателю принадлежат авторские права, которые являются личными неотчуждаемыми интеллектуальными правами физических лиц — авторов?

— Почему патентные заявки принадлежат работодателю до отчуждения права патентования?

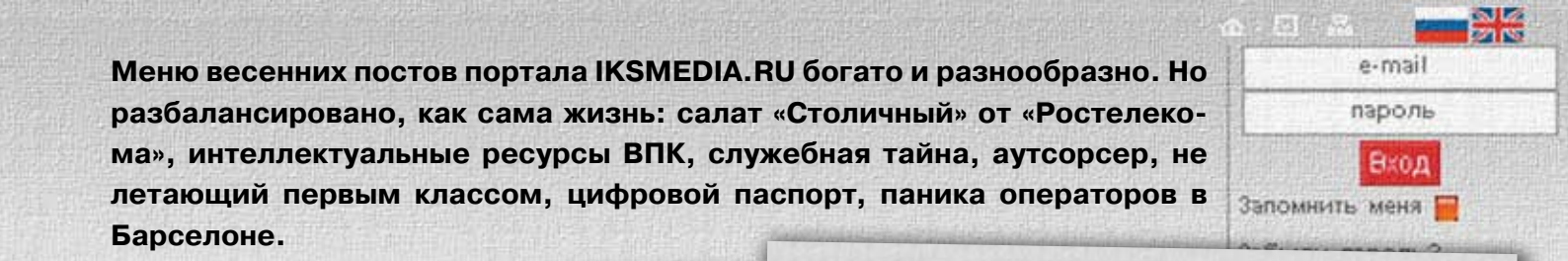
— Каким образом отчуждается (переходит) к работодателю исключительное право на служебную интеллектуальную собственность, созданную в порядке трудовых отношений и служебных заданий работнику?

— Является ли согласие работника в вопросе о принадлежности работодателю интеллектуальной собственности, созданной до оформления трудовых отношений, оформленное подписанием такого договора, понуждением к нарушению законодательства со стороны работодателя и фактическим присвоением имущественных интеллектуальных прав на интеллектуальную собственность?

Указанные вопросы – не предмет трудовых споров. Это предмет внимания прокуратуры, органов лицензирования видов деятельности и сертификации СМК предприятий. Приведено это в качестве иллюстрации небрежности юридических и некомпетентности кадровых служб, необходимости внимания со стороны проверяющих, целесообразности активизации постоянно действующих комиссий по качеству (ПДКК)...

комментировать

Меню весенних постов портала IKSMEDIA.RU богато и разнообразно. Но разбалансировано, как сама жизнь: салат «Столичный» от «Ростелекома», интеллектуальные ресурсы ВПК, служебная тайна, аутсорсер, не летающий первым классом, цифровой паспорт, паника операторов в Барселоне.



Михаил ЕМЕЛЬЯННИКОВ

Доколе, Катилина, мы будем жить без служебной тайны?

>>>> В середине первого века до нашей эры (до Р.Х.) Цицерон в своей речи осаживал честолюбивого Луция Сергия Катилину: «Доколе, Катилина, будешь ты злоупотреблять терпением нашим?». Почему-то именно это вспомнилось после прочтения в «Ведомостях» о том, что вице-премьер «Сечин выступил за тайну собственной переписки».

Действительно, утечки информации из органов государственной власти, о которых идет речь в статье, а тем более из Правительства РФ – не только не допустимы, но и крайне опасны, вызывая резонанс в общественном сознании. Если можно там – то почему нельзя нам?

Вот только приводимые изданием слова вице-премьера «Зачастую такая переписка имеет различные грифы, ограничивающие ее открытое использование, а предавать ее огласке указания не давалось» вызывают некоторое недоумение.

С грифами государственной тайны все понятно – разглашение ее составляет уголовное преступление, преследуется по закону и недопустимо ни при каких обстоятельствах. А вот какие еще грифы имелись в виду?

О мифах, стереотипах и менталитете

>>>> Знакомый топ-менеджер одного из крупнейших мировых банков, работающий в Лондоне, рассказывал про отношение к аутсорсерам. Оказывается, аутсорсеров надо беречь, холить и лелеять, постоянно работая над повышением их лояльности. Потому как они, в силу особых отношений с заказчиками, допущены к самому святому, к самому тайному, о котором и в самом банке почти никто не знает. Поэтому хорошо бы аутсорсера периодически приглашать на финалы «Формулы-1» в разных городах мира, на центральные матчи где-нибудь на стадионе Уэмбли или на премьеру в венской опере. Заодно снимать ему номер в соответствующем отеле. За счет заказчика, конечно. А вот билеты на самолет покупать нельзя. Это не комильфо, на коммерческий подкуп смахивает, а не на выражение признательности за многолетнюю лояльность. Серьезный аутсорсер никогда за счет заказчика первым классом не полетит. Он себя уважает.

Мифы и стереотипы иногда могут завести далеко в сторону от реальности, а воспитанный ими менталитет – сыграть злую шутку. Может оказаться, что модель поведения, созданная посконным и домотканым этим самым менталитетом, безнадежно устарела. И лучше ее менять.

комментировать

Петр ДИДЕНКО

Про доверие, онлайн-паспорт и врагов

>>>> Помню, еще 6 августа 2010 года был я в эфире гостеприимной радиостанции «Вести ФМ», и там меня всё пытали, мол, что, электронная подпись – это цифровой паспорт гражданина и такая форма надвигающейся цензуры? Без паспорта в Интернет теперь не войдешь? Есть много ответов на эти вопросы и степень хардкора в них зависит от текущего градуса желания глумиться над вопрошающим, признаюсь ☺.

ОК, я согласен что нельзя всех заставлять носить с собой паспорт (хотя в России без него почти никак, да в США есть один изобретательный штат...). Говорят, «свобода одного человека заканчивается там, где начинается свобода другого». То есть в ситуациях, где «не поставить настоящую подпись» значит «иметь возможность нанести вред», надо что-то придумывать.

А вообще, весь вопрос не в паспорте или электронной подписи, а именно в доверии. Если мы друг другу доверяем – всё это не нужно. Если мы враги – надо все время смотреть в паспорт, справку, счет-фактуру и прочие глупости. Думаю, настоящие враги общества – это те, кто целенаправленно разрушает доверие, нарушая закон, занимаясь вот так обманом, чтобы потом было проще воровать и скрывать это. Аминь.

комментировать

Крис ОЗИКА

Лавина данных обрушит операторский бизнес?

>>>> На Всемирном мобильном конгрессе-2012 в Барселоне я увидел главного «возмутителя спокойствия» – планшетный компьютер с установленными на нем ресурсоемкими мультимедийными приложениями. Феноменальный успех устройства iPad и последовавшее за ним быстрое распространение устройств с операционной системой Android изменили поведение пользователей: теперь они готовы часами смотреть видео в любом месте и в любое время. И хотя фильм на планшетнике – совсем не то же самое, что в широкоформатном кинотеатре с объемным звуком, увеличенный экран предоставил зрителю вполне приемлемое сочетание качества изображения, мобильности и комфорта.

У операторов же мобильной связи эта ситуация вызвала настроение, близкое к панике. Неожиданно – будто кто-то открыл огромные шлюзы – сети захлестнула лавина видеотрафика. К тому же на рынке появилось множество приложений для смартфонов и планшетных компьютеров, которые стали генерировать еще больше трафика, создавая огромную нагрузку на сети и днем и ночью.

комментировать

Реклама в номере

АБИТЕХ
Тел./факс: (495) 234-0108
www.abitech.ru . . . . . .с. 85

АМДТЕХНОЛОГИИ
Тел.: (495) 963-9211
Факс: (495) 225-7431
E-mail: info@amd-tech.ru
www.amd-tech.ru . . . . . .с. 71

КРОК
Тел.: (495) 974-2274
Факс: (495) 974-2277
E-mail: croc@croc.ru
www.croc.ru . . . . . .с. 75

ГК ЛПМ
Тел.: (495) 979-9901
Факс: (495) 739-0566
E-mail: market@lpm.su
www.lpm.su . . . . . .с. 13

ГК ПОЖТЕХНИКА
Тел.: (495) 687-6949
Факс: (495) 687-6943
E-mail: info@firepro.ru
www.firepro.ru . . . . . .с. 91

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

СИНЕРГЕТИКА
Тел./факс: (495) 786-4813
E-mail: info@synergetika.ru
http://synergetika.ru . . . .с. 80

СОКК
Тел./факс: (846) 955-0963
E-mail: sales@soccom.ru
www.soccom.ru . . . . . .с. 19

ЭР-ТЕЛЕКОМ
Тел.: (342) 246-2233
Факс: (342) 219-5024
E-mail: info@ertelecom.ru
www.ertelecom.ru . . . . 4-я обл.

AASTRA
Тел.: (495) 287-3035
Факс: (495) 287-3036
E-mail: info.ru@aastra.com
www.aastra-cis.ru . . . . . .с. 17

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

EUROLAN
Тел.: (495) 287-0758
E-mail: info@eurolan.se
www.eurolan.se . . . . . .с. 77

HP
Тел./факс: (495) 797-3900
www.hp.ru. . . . . с. 11

NOMINUM
Тел: +1-650-381-6000
www.nominum.com . . с. 60–61

POWERCOM
Тел.: (495) 651-6281
Факс: (495) 651-6282
www.pcm.ru . . . . . .с. 81

RIT
Тел./факс: (495) 684-0319
E-mail: marketing@rit.ru
www.rit.ru . . . . . с. 83

RITTAL
Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru . . 1-я обл., с. 50–51

SONY ELECTRONICS
Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu . . . . . .с. 55

TE CONNECTIVITY/ AMP NETCONNECT
Тел.: (495) 790-7902
Факс: (495) 721-1894
www.ampnetconnect.ru . . .с. 87

Указатель фирм

2ГИС 45
ADM Capital 16
Aerofirst 9
Aksa 73
Alcatel-Lucent 13
Amazon 7
AOL 64
APC by Schneider Electric . 17, 70, 83
Apple 6, 7, 23, 26, 35, 57
Arvato Digital Services 17
ASHRAE 78
Avaya 14
Beeline 12
BlackBerry 55
BladeRoom 84, 85
Broadcom 35
Capman 27
Caterpillar 73, 74
Chloride Rus 13
Cisco 13, 15, 16, 50
Citrix 21
Cognitive Technologies 16
Colt Data Center Services . . . 70, 84, 85, 86
Compaq 10
CSS 9
Cummins 73, 74
DataLine 21
DataSpace 91
Dell 50
Deutsche Telekom 6
DevBusiness.ru 20
Digital Design 21
EADS Astrium 15
Edge-Core Networks Corporation . 93
Emerson Network Power 81
EMC 10
Epam 49
EpicorSoftware 12
Ericsson 13, 18
Ernst & Young 16
Esri CIS 43
Explay 41
FG Wilson 73, 74
FinamShape 12
Garmin 41
Genesys 13
Gesan 73, 74
GMGen 74
Good Line 27
Google 6, 26, 64, 65, 84
Hitachi Data Systems 10
HP . . . 10, 12, 26, 50, 83, 84, 93
Huawei 18, 35, 86
IO Anywhere 84, 85
IBM 13, 15, 50, 83
IBS 49, 75
IDC 18, 58
iKS-Consulting 23, 27, 53
Intel 15, 20, 21, 60, 93
Intracom Telecom 13
Italtel 27
J'son & Partners 23
Knuerr 71
Kyoto Cooling 70
Lightwire 13
Logitech 12
Luxoft 49
Macquarie Renaissance 16
Mail.Ru Group 12, 49
Mediamarkt 14
MegaLabs 54
Micron Technology 12
Microsoft 6, 7, 16, 17, 26, 65, 83, 84
Moko-Consulting 24
Motorola 35
Motorola Solutions 16
Navteq 41
NDS Group 13
NetApp 50
NIS GLONASS Pvt Ltd 34
NIST 20
Nokia 35
Nokia Siemens Networks 16
Nominum 60, 61
Oracle 15, 83
Orange Business Services 16
Panasonic 16
Parallels 26
Permira Funds and Technology Crossover Ventures 13
Polycom 18
Prestigio 41
Prology 41
Qualcomm 18, 35, 44
Rainbow Security 64
Reliance 7
RiT Technologies 92
Rittal 50, 51, 84
Rydra Trading Company 13
Samsung 35
SAP 12, 15, 21
SAP Labs СНГ 12
SDMO 73, 74, 75
SECURIT 18
Skype 7, 64, 65
Sony 13, 35
Sony Ericsson 13
SPIRIT Telecom 8, 43
Stack Labs 84, 85
Stins Coman 75
Stulz 70
Sun Microsystems 83
Symantec 14
Tele2 16
ИАА TelecomDaily 41
Telefonica 6
The Uptime Institute . . . 74, 85, 88
TM Forum 1, 6
TNS Russia 49
Toshiba 71
Total Site Solutions 78
Trane 79
Tvigle Media 22
UFG Private Equity 16
Verizon 7
VimpelCom Ltd 48
Vodafone 7
WWK 70
Yahoo! 12
Yandex 49, 65
Yota 16
YouTube 23
Zecurion 18
ZTE 35
«Абитех» 75
«АвиаТел» 24
«АвтоВАЗ» 35
«Автоспутник» 41
«АвтоТрекер» 8, 18
Агентство стратегических инициатив 16, 33, 34
Академия космонавтики им. К.Э. Циолковского 8
«Акадо» 23
«АМДтехнологии» 70, 79
«Астерос» 75
«Аякс Инжиниринг» 70, 86
Банк России 26
«Белый ветер – Цифровой» . . . 14
«Водоканал Санкт-Петербурга» . 16
Военная академия имени Ф.Э. Дзержинского 8
ВЦ Главного военного клинического госпиталя им. Бурденко 9
ВЦ Института физико-технических проблем 9
«ВымпелКом» 15, 16, 18, 23, 27, 48, 53, 54
«ГеоСтар навигация» 44
ОКБ «Гидропресс» 15
ГИЦИУ КС 8
ГКНПЦ им. М.В. Хруничева . . . 8
«ГЛОНАСС/ГНСС-Форум» 36
«Голден Телеком» 54
ВНИИ «Градиент» 15
«ГрандМоторс» 75
«Грузия-Россия» 16
ЕБРР 16
«Евросеть» 14
«Е-Лайт Телеком» 27
ЕТК 27
«Инлайн Груп» 15
«Интеллект Телеком» . . . 8, 35, 43
«Инфомир» 24
«Инфосистемы Джет» . . 18, 62, 75
«Кар-Тел» 12
Клуб-ком.рф 24
«Коминфо Консалтинг» 24
«Компания КОМПЛИТ» 26
Компания ТТК 15, 27
«Комстар-Регионы» 54
Координационный центр национального домена сети Интернет 16, 12
«Корбина Телеком» 23
ФГУП «Космическая связь» . . . 15
КРОК 75, 77
«КупонГид» 49
«Ланит» 75
«Локис» 9
«М.Видео» 14
ГК «М2М телематика» 8, 33, 34, 40, 43
МАИ 8
МГТУ им. Н.Э. Баумана 8
МГУ 9
«МегаФон» 12, 14, 15, 16, 18, 26, 53, 54
МИСиС 8
МТС 15, 18, 27, 48, 53, 54
МЭСИ 9
«Навиком» 41
«Навител Навигатор» 41
«Национальные телекоммуникации» 13, 48
«НГ Энерго» 75
НИИ КС 8
«НИС ГЛОНАСС» 32, 33, 34, 35, 45
«Новотелеком» 27
«Нонфаир» 88
НПФ «Гейзер» 8
«Открытые Технологии» 17
ГК «Пожтехника» 91
«Президент-Нева» 75
«Прогород» 41
«Разумный Интернет» 16
«Райтек Текнолоджис» 47
РБК 49
РЖД 52
«Риттал» 92
Российская академия космонавтики им. К.Э.Циолковского 8
«Российские космические системы» 8, 33, 36
«Ростелеком» 12, 13, 14, 15, 16, 27, 48, 83
РТИ 13
«РуСат» 18
«РУСЛАН Коммуникейшнз» 8
«Русские башни» 16
«Русские навигационные технологии» . . . 8, 18, 32, 34, 42
«Русско-итальянская компания по телефонизации» 27
РЦТК 27
«Сага Телеком» 16
Банк «Санкт-Петербург» 15
Санкт-Петербургская радиокоммуникационная компания 16
Санкт-Петербургский государственный университет 15
Сбербанк России 74
«Северен-Телеком» 13
Северо-Восточный федеральный университет 15
«Сибсвязь» 27
«Синергетика» 74, 75
«Синергия» 8
«Синтерра» 53
АФК «Система» . . . 13, 34, 48, 49
«Систематика» 13
СитиГид 41
«Ситроникс» . . . 13, 35, 43, 49, 84
«Сиэтл-ДМО» 75
«Скай Линк» 27
«Сколково» 12, 16
«СОЦПРОФ» 15
«СТС Медиа» 22
«Стэп Лоджик Групп» 13
НПП «Тест» 15
«Техносерв» 18, 75
«Томтел» 27
«Триколор ТВ» 23
ФГУП НИИР 8
УК «Финам Менеджмент» 48
«Фонд посевных инвестиций Российской венчурной компании» 8
«Хайтед» 74, 75
«Цеппелин Русланд» 76
«Эквант» 54
«Экстатик» 13
«Электросвязь» 27
«Эльбрус Капитал» 27
«Эльдорадо» 14
«Энвижн Груп» 12, 75, 83
НПО «Энергия» 9
«Энтер» 13
«Яндекс» 26, 86

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 212; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:
127254, Москва, Огородный пр-д, д. 5, стр. 3; тел.: (495) 785-1490, 229-4978.

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка, д. 6/9/20, стр. 1; тел.: (495) 921-1616.