На фоне мировой коррекции

В разгар весны внешняя конъюнктура на мировых площадках не благоприятствовала росту на российском рынке акций: начавшаяся апрельская коррекция плавно перешла на май. На этом фоне бумаги телеком-компаний, прежде всего «Ростелекома», пользовались повышенным вниманием инвесторов.

Анна ЗАЙЦЕВА,
аналитик УК «Финам Менеджмент»

Коррекция на торгах была вызвана сразу несколькими факторами. Во-первых, это серия макроэкономических данных, показывающих, что в ряде развитых стран (США, Япония) экономика вновь начала торможение. Усугубила положение новость о понижении прогноза кредитного рейтинга США в конце апреля: это сообщение прокатилось коррекционной волной по всем мировым площадкам, в особенности пострадали российские биржи. Следующий фактор – ожидание постепенного окончания мягкой денежной политики основных центробанков и продолжающиеся долговые проблемы еврозоны. Дополнило все эти негативные моменты снижение цен на нефть и драгоценные металлы. В результате за период с середины апреля по середину мая отечественные индексы сильно просели.

«Ростелеком» – хороший рост при высоких объемах

Бумаги телекоммуникационных компаний – прежде всего «Ростелекома» – стали прекрасной инвестиционной идеей на фоне нестабильности мировых рынков, колебаний цен на сырье и валютных потрясений. Реорганизация «Связьинвеста» безусловно, привела к росту ликвидности бумаг «Ростелекома»: за рассматриваемый период они прибавили 5,66%, достигнув уровня 177,51 руб. за акцию. Во второй половине апреля бумаги компании на коррекционной волне сильно просели, опустившись к мартовским уровням поддержки в 158 руб., но смогли восстановить утерянные позиции уже в первые недели мая. С начала мая акции «Ростелекома» показывали хороший рост при высоких объемах.

С 12 мая на ММВБ начали торговаться новые акции «Ростелекома», в которые были конвертированы бумаги МРК в ходе реорганизации. Сейчас на рынке одновременно присутствует 18 выпусков акций объединенного «Ростелекома»: 16 из них были размещены в начале апреля после конвертации, один выпуск обыкновенных акций и один привилегированных торговались и ранее.

Среди корпоративных новостей стоит отметить публикацию сильной отчетности по МСФО за 2010 г. Согласно этим данным скорректированная чистая прибыль объединенного «Ростелекома» по МСФО в 2010 г. выросла на 49% – до 40,8 млрд руб. Выручка ОАО «Ростелеком» по итогам 2010 г. по МСФО увеличилась на 4% по сравнению с 2009 г. и составила 275,7 млрд руб. Показатель скорректированной OIBDA достиг 110,9 млрд

Справка ИКС

В период с 18 апреля по 13 мая индекс ММВБ потерял 8,32%, опустившись до отметки 1632,23 пункта. Индекс РТС снизился на 8,07% – до уровня 1866,30 пункта. Снижение показал и отраслевой индекс «ММВБ телекоммуникации», потеряв 5,87%; его значение составило 2405,48 пункта.
Следует отметить, что расчет индекса «РТС Телекоммуникации» был приостановлен с 16 марта 2011 г. решением биржи в связи с завершением реорганизации группы компаний ОАО «Связьинвест».

руб., показав прирост на 8% по сравнению с 2009 г. Рентабельность по скорректированной OIBDA выросла до 40,2% против 38,8% в 2009 г. Столь сильные результаты оправдали ожидания инвесторов и в дальнейшем могут послужить хорошим катализатором для роста спроса со стороны глобальных фондов.

У МТС все спокойно

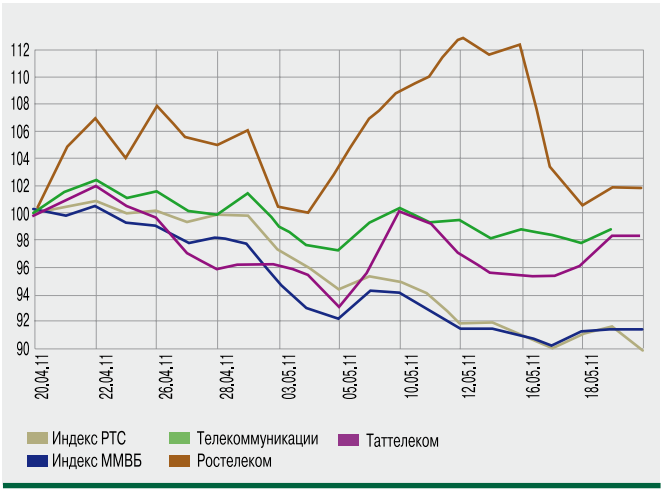
Акции сотового оператора МТС снизились в цене на 7,61% – до 237,39 руб. В целом бумаги компании вели себя довольно спокойно и ровно, резкое падение (около 4%) было отмечено только 10 мая после отсечки закрытия реестра акционеров. Среди корпоративных новостей стоит отметить публикацию нейтральной отчетности МТС в I квартале 2011 г., согласно которой чистая прибыль оператора составила 13 226 817 тыс. руб. против убытка в размере 7 700 151 тыс. руб. в IV квартале 2010 г. На увеличение чистой прибыли компании в I квартале оказали влияние волатильность курсов валют и отсутствие дополнительных обременительных обязательств. По сравнению с аналогичным показателем I квартала 2010 г. (10 598 046 тыс. руб.) компания увеличила чистую прибыль почти на 25%.

Бумаги телекоммуникационных компаний – прежде всего «Ростелекома» – стали прекрасной инвестиционной идеей на фоне нестабильности мировых рынков

ИТ-сектор в понижающем тренде

В апреле-мае бумаги АФК «Система» потеряли 8,06%, откатившись к отметке 29,702 руб. Согласно отчетности в IV квартале 2010 г. чистая прибыль компании по US GAAP до неденежных корректировок выросла на 18,8%, до $613 млн. Выручка в IV квартале увеличилась в долларовом эквиваленте на 19,5% год к году и на 5,1% квартал к кварталу, достигнув $7,7 млрд. В рублевом эквиваленте выручка составила 236 млрд руб. – это рост соответственно на 24,5 и 5,4%. Показатель EBITDA в IV квартале увеличился на 22,3% год к году, до $1,92 млрд. По итогам 2010 г. в целом выручка АФК «Система» выросла на 49,9% до $28,1 млрд, EBITDA – на 8,7%, до $7,31 млрд.

Динамика индексов РТС и телекоммуникационных компаний в период с 20 апреля 2011 г. по 18 мая 2011 г.



Акции «РБК ИС» потеряли 12,82%, упав в цене до 36,614 руб. за акцию. 19 апреля холдинг РБК сообщил, что продлевает обмен акций «РБК Информационные Системы» на акции ОАО «РБК» до конца мая 2011 г. Напомним, что ранее акции ОАО «РБК» были включены в «Список ценных бумаг, допущенных к торгам без прохождения процедуры листинга» на российских фондовых биржах ММВБ и РТС. Обмен акций проводится в рамках реструктуризации РБК. В результате последней ОАО «РБК» стало новой холдинговой компанией, в которой 51% принадлежит «Группе ОНЭКСИМ», а 49% обмениваются на 100% акций ОАО «РБК Информационные Системы». Обмен акций осуществляется в соотношении 1,116 акций РБК за 1 акцию «РБК Информационные Системы».

Капитализация «Ситроникса» снизилась более чем на 13%, до $0,0135. Компания опубликовала отчетность по US GAAP, согласно которой она, несмотря на рост прибыли, продолжает оставаться в убытке. Так, по итогам IV квартала 2010 г. чистая прибыль по US GAAP составила $19,2 млн против убытка годом ранее. Выручка в отчетном периоде увеличилась на 21% по сравнению с аналогичным периодом 2009 г. – до $484,5 млн. Показатель OIBDA составил $54,8 млн при рентабельности 11,3% по сравнению с убытком по OIBDA в $19 млн годом ранее. По итогам 2010 г. в целом выручка компании выросла на 14% – до $1,167 млрд. Чистый убыток снизился на 62%, составив $45,6 млн. Показатель OIBDA по итогам года был равен $105,6 млн при рентабельности 9,1%.

Исключением из общей тенденции к понижению стали акции Mail.ru Group, продолжившие рост на Лондонской фондовой бирже (LSE). За рассматриваемый период они прибавили 2,97% – до цены $35,01 за одну GDR. Компания смогла привлечь к себе внимание инвесторов публикацией сильной финансовой отчетности за 2010 г. Чистая прибыль контролируемых Mail.ru Group активов в прошедшем году выросла на 66% – до $77,3 млн. Выручка составила $324,7 млн, увеличившись на 64% по сравнению с 2009 г. Показатель EBITDA вырос на 77% – до $119,4 млн, говорится в официальном сообщении компании на сайте LSE. Выручка Mail.ru Group по итогам I квартала 2011 г. составила $110,6 млн, что означает рост на 69%.

Хочется верить, что акции IBS Group, прибавившие за рассматриваемый период 1,18% – до уровня $22,25, тоже покинули понижательный тренд. ИКС

Перенести нельзя отказать

Тема переносимости абонентского номера, или MNP, уже не на пике популярности у телекоммуникационной общественности. Впрочем, за пять лет с момента появления на российском телеком-рынке она пережила и взлет всеобщего интереса, и его охлаждение. Причиной тому и нерешительность регулятора, и запас контраргументов у «большой тройки» основных игроков.

Из всех участников некогда многочисленной рабочей группы сегодня идею MNP продолжают отстаивать энтузиасты из компании МТТ и нескольких их партнеров, совместными усилиями реализовавшие переносимость номера в опытной зоне, организованной в соответствии с рекомендациями ЦНИИС.

Какова ценность результатов этих испытаний для рынка телекоммуникаций? Есть ли у MNP надежда на поддержку со стороны операторского сообщества? Читатели «ИКС» смогут сами ответить на эти вопросы, ознакомившись с мнениями разных сторон, собранными Александрой КРЫЛОВОЙ.

Возможность, до которой рынок еще не дорос...

Что такое переносимость номера, об интересе к которой регулятор то заявляет, то забывает уже с 2005 г.? Бизнес-модель? Услуга? Может ли заработать на ней оператор? Ответы на эти вопросы – у Дмитрия ГУРКИНА, заместителя генерального директора МТТ.

Дмитрий ГУРКИН

– За переносимостью номера, безусловно, стоит бизнес-модель, поскольку для ее функционирования необходимо взаимодействие хозяйствующих субъектов, включающее и взаиморасчеты. Однако целью этой деятельности не является извлечение прибыли. Этот бизнес можно сравнить скорее с обязанностью обеспечить гражданам недискриминационный доступ к услугам связи.

– Почему, на ваш взгляд, переносимость номера воспринимается рынком так медленно и трудно?

Если взглянуть на зарубежный опыт, мы увидим, что инициатором и движущей силой внедрения переносимости были отнюдь не участники рынка, а зачастую и не регулятор. Осознание необходимости такого механизма приходило от осознания того, что это ограничивает права граждан в части свободы передвижения. Кроме того, привязка номера к оператору была признана фактором, ограничивающим конкуренцию. В такой ситуации инициатором внедрения переносимости номеров стали правительственные и законодательные органы, а на долю операторов выпала только практическая реализация требований в установленные сроки. Применительно к России такой подход можно сравнить с внедрением средств СОРМ в сети связи. Операторы в процессе, конечно, принимали живейшее участие, но скорее как исполнители, а не как инициаторы. Между тем в вопросах внедрения переносимости номеров ведущая роль у нас отдается именно операторам и регулятору. При этом регулятору тема MNP не вполне интересна, так как на данный момент нет предмета регулирования (нет собственно переносимости), а операторы вряд ли захотят сами себя к чему-либо обязывать. Вот и ходим по кругу с 2004 г.

Наверное, сегодня для России отсутствие переносимости номера – это не самая большая проблема, требующая пристального внимания со стороны исполнительной власти. Вот и получается, что «наверху» ее важность не видна, движения «снизу» тоже нет: абоненты не дозрели до понимания актуальности MNP.

Какова судьба подготовленного ЦНИИС по заказу МТТ отчета «Разработка предложений по реализации в РФ переносимости телефонного номера в сетях фиксированной и подвижной радиотелефонной связи»?

– Мы направили этот документ в Минкомсвязи РФ, где к нему отнеслись благосклонно. В частном по-

рядке нам было сказано, что MNP может стать темой одного из будущих заседаний НТС, для проведения которого необходимо собрать и подготовить дополнительные материалы. С этой целью мы организовали опытную зону в Самаре, о чем поставили Минкомсвязи в известность. По разработанной ЦНИИС методике провели первый этап испытаний, сделав упор на сетевые вопросы реализации MNP. Это был самый интересный для нас вопрос. Все результаты этих испытаний запротоколированы, и мы готовы вынести их на обсуждение профессионального сообщества.

– Какую роль видит для себя компания МТТ в схеме взаимодействия отдающего и принимающего операторов?

– В этой модели есть две возможные для нас роли. Первая – маршрутизирующий оператор, на средствах коммутации которого осуществляется запрос к базам данных при маршрутизации вызовов в сторону принимающего оператора. Вторая – оператор базы данных перенесенных абонентских номеров. Эта роль чисто технологическая, исполнять ее мы тоже можем, а вот хотим ли, я пока не знаю.

Как показывает мировой опыт, заработать на MNP держателю базы данных невозможно: оператор сотовой связи должен иметь выбор, с каким из держателей БДПН ему работать. И в итоге на рынке остается несколько игроков, которые покажут расходы на уровне справедливой компенсации фактически понесенных затрат. Вот почему переносимость номера для МТТ – это не способ заработать.

– Тогда что заставляет компанию шестой год отстаивать идею MNP и перед регулятором, и перед участниками рынка?

– В общем виде можно сформулировать так: наличие механизма переноса номеров делает рынок услуг связи более конкурентным, а значит, способствует уравниванию рыночных возможностей операторов. В такой ситуации участникам рынка будет логичнее сосредоточиться на своих основных видах бизнеса, больше внимания уделять работе с собственными абонентами, тем самым поднимая качество обслуживания. Таким образом, откроется больше возможностей для остальных игроков рынка, непрофильного для вышеупомянутых компаний. Рынок станет демократичнее.

– Иными словами, заработать на MNP вы не стремитесь?

– Хоть немного заработать всегда хочется. Компания, помогающая операторам снизить расходы на взаимодействие, вправе рассчитывать на какую-то маржу: «в ноль» никто не работает. Как минимум, мы займем своих людей, создадим какой-то новый рынок труда, но заработать на переносимости номера, сделать на ней бизнес, организовать компанию, которая занималась бы только ею, я думаю, нельзя.

– Тогда есть ли у вас сегодня основания для оптимизма?

– В России наблюдается движение в сторону гармонизации отечественного законодательства и европейских норм, а значит, в перспективе, через какое-то время, оно должно затронуть и телекоммуникации. ИКС

Елена ШМАТОВА, генеральный директор ОАО «ВымпелКом»

– Как на расстановку сил на рынке может повлиять введение MNP, Mobile Number Portability?

– Мы всегда говорили, что проект введения переносимости номера имеет право на существование, однако требует детальной проработки с точки зрения организационно-технических параметров внедрения.

Переносимость мобильных номеров, введение MNP потребует от операторов значительных затрат, в первую очередь на замену ИТ-платформ, на расширение емкости сигнальной сети, что может привести к росту стоимости услуг для конечных пользователей. Клиентская аудитория, заинтересованная в мобильных сетях, на наш взгляд, также неясна. К тому же уже сейчас существуют различные услуги, которые облегчают переход от оператора к оператору. Для удобства наших абонентов в мобильном сегменте мы предлагаем услугу «Легкий шаг в «Билайн», которая позволяет оповестить круг общения абонента о смене его номера: звонящие на старый номер получают информацию о новом номере в виде голосового сообщения или SMS.

Кроме того, для бизнес-пользователей, которых мы обслуживаем в фиксированных сетях, мы можем предоставить услугу, в рамках которой при переезде с места на место он сохраняет свой номер фиксированной связи, оставаясь нашим клиентом. Таким образом, мы как интегрированный оператор уже представляем нашим абонентам определенную гибкость в этом вопросе.

Валерий ЕРМАКОВ, первый заместитель генерального директора по операционной деятельности ОАО «МегаФон»

Стабилизация рынка – завершение формирования операторами связи собственных сетей ритейла, пропорциональный прирост абонентской базы и доходов у всех операторов – таковы условия, при которых переносимость номера, MNP, станет полезной для рынка. В этом случае она будет стимулировать перераспределение долей рынка между операторами и поддерживать высокий уровень конкуренции между ними. И очень может быть, тогда мы сами будем заинтересованы в том, чтобы обеспечить нашим абонентам такую возможность.

Если же внедрять MNP сейчас, то эффект утонет в лавине SIM-карт, которые дистрибутируются сегодня по всему рынку (только за прошлый год операторами «большой тройки» их было продано около 100 млн).

MNP отыграна успешно

Михаил НАУМЕНКО, руководитель проекта MNP компании МТТ

В опытной зоне по отработке реализации переносимости телефонного номера на сети подвижной связи, которую мы развернули в конце 2010 г. в Самаре, участвовали операторы мобильной связи СМАРТС и «Скай Линк», а также компании МТТ, «Техносерв» и «Протей». Первые два выступали в роли отдающих и принимающих операторов, МТТ – в роли маршрутизирующего оператора, «Техносерв» был интегратором проекта и отвечал за инженерную поддержку, а «Протей» поставил оборудование и программное обеспечение.

В соответствии с разработанной методикой испытаний из двух возможных способов обмена информацией о перенесенных номерах – централизованного и децентрализованного – в качестве модели был выбран централизованный, с учетом рекомендаций ЦНИИС. Использование в модели маршрутизирующего оператора позволило за счет централизации компетенций и операций снизить практически до уровня обычных текущих затрат расходы на реализацию MNP остальных участников процесса – операторов, отдающих и принимающих нумерацию.

День 21 декабря 2010 г. войдет в историю российских телекоммуникаций как дата установления первого вызова на «перенесенный» номер. СМАРТС и «Скай Линк» в опытной зоне «обменялись» десятью номерами из своих зон нумерации, смоделировав таким образом переход десяти абонентов из «Скай Линк» в СМАРТС и десяти – из СМАРТС в «Скай Линк». Тестовые испытания были успешно проведены с первой попытки, что говорит как о простоте выбранной модели сетевой реализации, так и о высокой квалификации сотрудников операторов, принявших участие в мероприятии. Компания МТТ продолжит тестировать модель, которая дает возможность всем участникам телеком-рынка обеспечить абонентам переносимость номера с минимальными затратами. ИКС

Переносимость номера: алгоритм взаимодействия

Всесторонне исследовав схемы реализации переносимости абонентского номера в сетях как фиксированной, так и подвижной связи, специалисты ЦНИИС предложили проект Свода правил по организационно-техническому взаимодействию всех участников процесса.

Согласно этим правилам для перехода от одного оператора связи к другому абонент подает принимающему оператору заявление о заключении договора на оказание услуг либо местной телефонной связи, либо подвижной радиотелефонной связи с использованием перенесенного абонентского номера – по форме, установленной оператором связи, в двух экземплярах (в числе прилагаемых документов должна быть копия договора с отдающим оператором).

Принимающий оператор регистрирует это заявление, чтобы в установленный срок направить заявителю уведомление о дате заключения договора либо мотивированный отказ в переносе абонентского номера.

При переносе номера из одной сети подвижной радиотелефонной связи в другую после заключения договора принимающий оператор выдает абоненту SIM-карту, которая будет активирована после завершения переноса. При заключении договора абонент оплачивает стоимость подключения.

В течение одного рабочего дня с момента получения заявления принимающий оператор обязан направить уведомление о переносе абонентского номера отдающему оператору. Получив этот документ, отдающий оператор точно так же, в течение одного дня, уведомляет принимающего оператора о возможности переносимости данного номера.

После этого оба оператора в установленный срок с момента получения подтверждения о возможности переносимости номера подают свои заявления в Россвязь для получения согласия на передачу абонентского номера из ресурса нумерации одного оператора связи другому оператору.

Если Россвязь дает согласие, принимающий оператор в течение одного рабочего дня с момента его получения сообщает маршрутный номер, дату, время переноса абонентского номера отдающему и/или маршрутизирующему оператору, а также держателю централизованной базы данных.

Получив этот документ, отдающий оператор в течение одного рабочего дня направляет принимающему оператору подтверждение даты и времени переноса.

В день и час, согласованные между операторами, выполняется техническая процедура переноса абонентского номера. После ее завершения принимающий оператор извещает абонента о моменте начала оказания ему услуг с использованием перенесенного номера. В сети подвижной радиотелефонной связи принимающий оператор направляет абоненту SMS с предложением установить в своем устройстве выданную при заключении договора SIM-карту и активирует ее.

Одновременно отдающий оператор расторгает договор с абонентом и возвращает ему неизрасходованные денежные средства (в случае переноса абонентского номера из одной сети подвижной радиотелефонной связи в другую отдающий оператор блокирует свою SIM-карту).

Время, в течение которого перенесенный абонентский номер по техническим причинам не обслуживался оператором связи, не должно превышать 10 мин.

А. К.

В преддверии информационной цивилизации

Год назад в беседах с Кириллом КОРНИЛЬЕВЫМ, вице-президентом IBM, гендиректором IBM в Восточной Европе и Азии, «ИКС» вел разговор о сути инноваций и задачах инноваторов (см. «ИКС» № 5'2010 с. 58, № 6'2010 с. 54). Тема нынешней беседы – ни много ни мало информационная цивилизация. Наш собеседник, состоящий в отряде ее созидателей, излагает свое видение меняющегося под воздействием ИТ мироустройства.

Кирилл КОРНИЛЬЕВ

– На запрос «информационная цивилизация» «Яндекс» выдал 9 млн ответов – энциклопедии, научные труды, статьи, конференции... Эта тема, похоже, на повестке дня во всем мире?

– За последнее десятилетие уже всем стало ясно, что информационные технологии вышли за пределы отраслевой науки и индустрии. ИТ больше, чем любая другая отрасль, участвуют в создании инструментов и ноу-хау, которые буквально меняют мироустройство – информационные технологии пронизывают все в этом мире. На них основаны системы и процессы, которые позволяют предоставлять услуги; они помогают разрабатывать, производить и продавать товары; они обеспечивают передвижение людей и самых разных объектов – грузов, нефти, воды и электронов; они влияют на работу и жизнь миллиардов людей. На каждого человека приходится почти миллиард транзисторов, и каждый из них стоит одну десятимиллионную долю цента. Во всем мире 4 млрд абонентов мобильной связи и 30 млрд радиометок. Эти метки впервые дают нам возможность наблюдать в режиме реального времени за поведением множества мировых систем – природных и антропогенных. Планета не только покрыта датчиками, она объединена каналами связи. Сегодня в Интернете 2 млрд человек – но и системы и объекты теперь тоже могут «общаться» друг с другом. Некоторые называют это «Интернетом вещей». Подумайте о возможностях обмена данными триллиона связанных между собой и оснащенных датчиками объектов – автомобилей, фотокамер, дорог, трубопроводов... и даже животных и фармацевтических препаратов. А с помощью передовых аналитических методов и все более мощных суперкомпьютеров мы можем превратить эти данные в знания.

– То есть этому надо все-таки обучиться?

– ИТ стали инструментом, которым должен владеть каждый руководитель. И я не имею в виду обучение тому, как использовать Twitter или iPad. ИТ – это не только инструмент бэк-офиса или бесконечный поток новых потребительских устройств. Информационные технологии – это то, как мы воспринимаем мир сегодня, в том числе в измерениях, невидимых для человеческого глаза; то, как мы отображаем и понимаем динамику сложных мировых систем; и это все в большей степени то, как мы принимаем решения – и претворяем их в жизнь. По всему миру мы видим дальновидных руководителей, которые овладевают этими новыми возможностями. Они применяют искусственный интеллект, чтобы сделать системы, процессы и инфраструктуру более эффективными, более продуктивными и способными быстро реагировать на изменения. Для тех, кто обладает мужеством и дальновидностью, переломный момент – это период новых возможностей. Будут победители и будут проигравшие. Некоторые компании и отрасли, некоторые страны и города будут сиять ярче других. И новые лидеры, которые появятся на этом глобальном этапе, чтобы победить, должны не просто пережить шторм, а изменить характер игры.

– О каком переломном моменте, о каком шторме вы говорите?

– Мы подошли к важному рубежу – точке перегиба. Мы переживаем переломный момент с точки зрения развития научной мысли и технологических возможностей. Завтрашние руководи-

тели индустрии должны осознать этот момент – не его механику, а его последствия – и учесть в своей будущей работе. Если судить об информационных технологиях по средствам массовой информации, то можно подумать, что их историю легко разделить на два этапа – сначала оборудование, потом программное обеспечение. Или на эпохи до Интернета и после. На самом же деле технический прогресс происходит не так. Это вовсе не «или-или», «то одно, то другое». И научное открытие – не просто «до и после». Это сложный, итеративный процесс постоянного развития. В этом году IBM отмечает свое 100-летие. За минувшие сто лет информационные технологии прошли путь от набора инструментов до целой индустрии и науки. Я хочу подчеркнуть, что ИТ – это больше, чем программы, и больше, чем устройства. Вы не сможете это оценить, если будете рассматривать технологию просто как множество гаджетов, веб-сайтов и очередных «классных продуктов». Взгляд в историческую перспективу помогает увидеть многомерную картину развития технологий и понять, как их основополагающие компоненты эволюционируют и рекомбинируются сегодня. Эти компоненты – датчики (механизмы для сбора в компьютеры информации о людях и событиях), память (способ хранения и доступа к информации в компьютерах), обработка (быстродействие и возможности компьютеров), логика (программное обеспечение и языки, которые позволяют компьютерам решать задачи), соединения (способы общения компьютеров с людьми и машинами), архитектура (меняющийся характер самих вычислений). И говоря о точке перегиба, я подразумеваю, что следующие 100 лет обещают быть не похожими на предыдущие.

– Какие задачи вы считаете актуальными для ИТ на пороге «следующих 100 лет»?

– Я хотел бы изложить три практических соображения по поводу задач управления. Во-первых, необходимы открытые стандарты. Конечно, значение стандартов широко известно – не только технических стандартов, но и новых глобальных правил в области торговой политики, интеллектуальной собственности и во многих других областях. Но если посмотреть на мир как на сложную систему взаимозависимых подсистем, понимаешь, что для нас вопрос стандартов приобретает весьма конкретное звучание. Речь идет об интерфейсах. Нам нужны стандартизованные интерфейсы между транспортной и энергетической системой, между системой образования и здравоохранения и между службами водоснабжения, безопасности дорожного движения, торговли, общественной безопасности и государственного управления. Они не появятся сами по себе. Я считаю, что на нашей отрасли лежит большая ответственность, но мы не можем действовать в одиночку. Потребуется новый уровень сотрудничества во всех секторах гражданского общества – в бизнесе, прикладной науке, государственном управлении, образовании, в неправительственных организациях и сообществах. Это выходит за рамки политики или идеологии и за рамки конкретных областей знаний. Но это – обязательное условие для построения глобально интегрированной, технологически оснащенной планеты.

Во-вторых, мы все должны осознать некоторые важные политические последствия этих технологических перемен. Веб-камеры помогают быстро предупреждать полицию и другие службы экстренного реагирования о чрезвычайных ситуациях. Это спасает жизни. Люди, использующие Twitter во время стихийных бедствий, передают в режиме реального времени информацию о причиненном ущербе, о пострадавших и местах расположения аварийно-спасательных служб. Это также может спасти жизни. Когда медицинские данные стали записываться и передаваться в цифровой форме, появилась возможность значительно уменьшить количество ошибок и повысить эффективность лечения. Но появились и опасения. Кто владеет всеми этими данными, как он ими распорядится, доверяю ли я ему? То же и в отношении информационной безопасности. Компании и правительства в восторге от конкурентных, экономических и экологических преимуществ интеллектуальной инфраструктуры – интеллектуальных сетей, железных дорог, коллекторов и зданий. Но значит ли это, что наша базовая инфраструктура безопасна и надежна? Насколько безопасен и надежен веб-сайт? Это серьезные вопросы. И они требуют детального рассмотрения всеми заинтересованными сторонами в обществе. Нам нужно построить не просто технологические и бизнес-системы. Мы должны построить социальную среду. И это подводит меня к третьему соображению: нам понадобится новая модель руководства.

В нашем традиционном понимании лидер – это некто, обладающий нечеловеческой прозорливостью, кто указывает на горизонт и ведет вперед, убеждая и вдохновляя других. По правде говоря, очень распространенная модель руководства в нашей отрасли. Но в мире, который стал глобальной системой систем, гораздо важнее руководить, прислушиваясь – воспринимая то, что эти многогранные экосистемы нам говорят. Нужно влиять, а не диктовать. Реальность настолько динамична и сложна, что к ней необходимо подходить с предельным вниманием, с намерением «служить, а не доминировать». И нам нужны системы управления, обеспечивающие участие в процессе, сотрудничество и прозрачность.

– Вы верите, что эта «триединая задача» выполнима?

– Я полон оптимизма. Главное, что в настоящее время существует ключевое условие для достижения реального прогресса – люди к нему стремятся. Мир стоит на пороге не просто новой технологической эры, но эры нового мышления.

Вопросы задавала **Лилия ПАВЛОВА**

Регулирование 2.0
С точки зрения сетевой нейтральности

«Конкуренция, ценообразование, надежность и безопасность – это наиважнейшие проблемы, лежащие «поперек» пути»
Н.С. Мардер
(Из выступления на конференции NGN'2009)

В последние годы в телекоммуникационной отрасли, особенно в США – на родине Интернета, идут споры по поводу концепции сетевой нейтральности. Ее защитники и противники находят все новые аргументы за и против, и эта проблема будет касаться всех стран и всех сетей.

Александр ГОЛЫШКО,
канд. техн. наук

Согласно концепции нейтральности Сети, весь интернет-контент должен рассматриваться поставщиками каналов широкополосного доступа одинаково, без какой бы то ни было дискриминации.

Защитники этой концепции считают, что крупные телекоммуникационные компании пытаются незаконно получить прибыль от своих инвестиций. Они, мол, хотят быть интернет-привратниками, которые сами решают, какие веб-сайты работают быстро, какие – медленно, а какие не будут загружаться совсем.

Противники сетевой нейтральности утверждают, что она не является необходимой и даже контрпродуктивна, поскольку всеобъемлющее и твердое законодательство о сетевом нейтралитете может привести к проблемам общественной и национальной безопасности; затруднить обеспечение защиты от вторжения в личную жизнь граждан; нарушить качество и ответные реакции Интернета; ограничить выбор потребителей; воспрепятствовать инвестициям в широкополосные сети.

Что же в итоге?

Скромное обаяние сетевых технологий

Да простят нас приверженцы технологической нейтральности, но для осознания регуляторных функций иногда приходится вникать в технологии. Современный набор сетевого оборудования связи у основных мировых поставщиков включает в себя так называемую интеллектуальную трубу (smart pipe), одной из базовых технологий которой является механизм углубленной инспекции пакетов данных (Deep Packet Inspection, DPI). С помощью этой относительно небольшой и, кстати, недорогой штуки оператор может не только определять вид трафика, проходящего через его сеть, но и гибко управлять им, меняя приоритеты обслуживания или полосу пропускания.

Еще раз напомним, что сегодня отрасль связи стоит на пороге мобильной интернет-революции, которая произойдет благодаря стремительному распространению IP-приложений, установленных на новых, интуитивно понятных пользовательских устройствах и сгенерированных в сервисных «облаках» вне зависимости от сетевой принадлежности. Однако, вникнув в сопутствующий отрасли информационный фон, можно сделать вывод, что и отраслевая терминология, и перспективные планы отрасли остаются в плену традиционных технологий, к примеру, радиодоступа в лице LTE (вот, мол, оно придет – и тогда «все будет». Кто помнит, так же говорили недавно про UMTS).

Но чтобы удовлетворить рыночный спрос на мобильный Интернет, необходимо учитывать лексикон, образ мыслей и поступки гораздо более широких кругов интернет-сообщества. Хотя бы тех, которые хорошо представляют себе, что такое «Интернет вещей». Поэтому, как считают специалисты, настала пора отделить радио от сетевых технологий и не фетишизировать мобильную связь в ущерб фиксирован-

ной. Даже если отвлечься от известной глобальной проблемы радиочастотного дефицита, следует понимать, что радиотехнологии не в состоянии поддерживать хостинг онлайнового магазина приложений, видеоконференции, электронную почту и высококачественную рекламу. Они также не поддерживают дифференцированные тарифные планы и оплату пользования чем-либо. Технологии радиодоступа не способны агрегировать интернет-трафик и не могут менять маршруты, дифференцировать и разделять потоки трафика, направляя их по разным сетевым каналам.

Зато у поставщиков оборудования (Alcatel-Lucent, Cisco, Ericsson, Huawei, Motorola…) появились решения, серьезно облегчающие жизнь всем внедряющим радиотехнологии. Эти решения поддерживают плавную модернизацию сетей от UMTS, HSPA, WiMAX до LTE и WiMAX 2.0 и одновременно позволяют операторам лучше контролировать, модернизировать и окупать быстро растущие объемы мобильного трафика, связанного с передачей видео и данных. Таким образом, транспортные IP-сети (в широком смысле) становятся солидной основой прибыльных операций в мобильном Интернете. Они способны в динамическом режиме менять маршруты трафика, оптимизировать рабочую нагрузку, мгновенно подключать новые радиоресурсы, дифференцировать гарантии качества услуг и непосредственно манипулировать оказанием услуг в зависимости от тарифов, состояния счета клиента и загрузки сети. Вот почему транспортные сети, составляющие основу национальной инфокоммуникационной инфраструктуры, заслуживают не меньшего внимания, чем традиционные радиотехнологии (которые, добавим, без соответствующего транспорта на массовом рынке – ничто). И одним из важных механизмов для работы с сервисами на транспортных сетях является smart pipe. Вопреки сложившимся представлениям, можно добиться более высококачественных услуг, если построить транспортные сети, базирующиеся на интернет- и интранет-моделях. Многие операторы сегодня стараются поступать именно так.

Механизм DPI не только обеспечивает работоспособность сети, спасая от перегрузок, но и поможет «договориться» с поставщиками контента и различных сервисов на предмет оплаты доступа к конкретным абонентам (а именно этот доступ и станет основной «валютой» инфокоммуникационного рынка). Таким образом, плату и с абонентов, и с источников сервисов за право пройтись по инфокоммуникационной магистрали смогут взимать и операторы, и государство (если оно также «вложится» в эту инфраструктуру).

Так ли хороша сетевая нейтральность, как ее малюют?

С большой вероятностью подход, опирающийся на DPI, многим не понравится: «халява» всегда превосходит любые другие тарифные предложения. Поэтому над многочисленными полками контент-провайдеров неизбежно будет поднято знамя сетевой нейтральности.

Разумеется, сторонники нейтральности сетей на самом деле скрывают за ней свои частные интересы. Однако для регулятора главное – это способность вопроса о нейтральности сетей лишить стимула инвестиции в развитие сетевой инфраструктуры. Ведь, будучи оператором, вы не можете, к примеру, применить нейтральность сети к HD IPTV. Допустим, вы вкладываете деньги, чтобы вывести на рынок конкурентоспособное ТВ-обслуживание. И если вы заявите, что нейтралитет будет касаться этого обслуживания (т.е. кто угодно помимо вас будет использовать эти каналы для передачи видео), то не найдете никакой жизнеспособной бизнес-модели, которая гарантировала бы вашим абонентам необходимые 25 Мбит/с. Сетевой нейтралитет, добавим, вредит и качеству предоставляемых услуг, поскольку подобен оживленному перекрестку без светофора. Быть может, регулятор с полосатым жезлом в подобной ситуации запретил бы качество, если бы не знал, как облегчает жизнь правильная организация дорожного движения. Заметим также, сами приверженцы сетевой нейтральности признают, что никто не станет строить сети, если их ресурс нужно будет отдавать «дяде». Но они и не строят.

А тем временем оператор должен поддерживать и постоянно модернизировать под растущий трафик инфраструктуру связи, подходящую к его абонентам. И вполне логично, что обеспечение доступа к ним (наряду с предоставлением им ШПД) постепенно станет одной из основных услуг связи и будет стоить денег. Причем вряд ли платить будут контент-провайдеры – чаще это придется делать пользователю. Но инвестировать в сети кому-нибудь кроме операторов точно придется.

Только отсутствие сетевой нейтральности позволяет оператору гарантировать QoS для «своих» сервисов на своей сети и доход от доставки своим абонентам «чужих» сервисов. Поэтому взвешенное отношение к сетевой нейтральности со стороны регулятора – последняя надежда операторов на получение каких-либо дивидендов от сетевых сервисов. Именно дозированная «нейтральность» может уберечь их от превращения в «битовую трубу». В настоящее время в условиях глобализации, подстегиваемой Интернетом, при действующих правовых нормах российского рынка связи в самом выигрышном положении находятся нерезиденты, которые действуют без учета российских реалий. Российским же компаниям, ограниченным нормативной и законодательной базой, вводить новые услуги на стыке теле- и инфокоммуникаций сложно и не всегда возможно. С внедрением smart pipe шансы на рыночный успех для всех поставщиков сервисов можно выровнять.

Чуть более года назад журнал Heavy Reading опубликовал результаты исследования, согласно которому более 70% опрошенных считают полезным разделение транспортных и радиотехнологий и пытаются осуществить это на практике. Появились наглядные доказательства того, что у операторов, разделивших радио- и транспортные технологии и отразивших этот подход в процессах приобретения, развертывания и эксплуатации сетей радиодоступа (RAN), доходы и уровень удовлетворенности абонентов выше, а совокупная стоимость владения ниже, чем у тех, кто настаивает на традиционном подходе. Крупнейшие поставщики традиционных мобильных радиорешений и мощные интернет-компании из Кремниевой долины могут дать операторам пищу для разработки стратегии отхода от транспортных традиций и разделения процессов развертывания радио- и транспортных сетей, чтобы получать лучшие решения из обоих миров.

Таким образом, строительство «интеллектуальной» транспортной сети для мобильного Интернета – это грамотное вложение средств в основы будущего прибыльного бизнеса, это эффективное средство для сетевого мониторинга и обеспечения надежности при перегрузках и это своеобразный регуляторный инструмент, которого до недавнего времени попросту не было на рынке связи. Поскольку же развитие мобильного Интернета напрямую связано с повсеместным доступом к IP-приложениям и устройствам, транспортные IP-сети уже сегодня показывают гораздо более высокую экономичность по сравнению с традиционными сетями TDM. Чем больше будут объемы мобильного интернет-трафика, тем эти преимущества ощутимее. Вот это и надо стимулировать регулятору.

Что делать

Но ведь дай операторам волю – они весь «чужой» трафик оттеснят в сторону, уберут конкуренцию, подгребут все доходы и, будучи по своей природе эгоцентристами, «свернут» IP-пространство. Правда, при этом они могут потерять значительную часть клиентской базы, и это, пожалуй, единственное, что их пока останавливает. С другой стороны, полный запрет на ограничение трафика будет ухудшать QoS для всех абонентов, «убивать» инвестиционную привлекательность и может даже полностью остановить сеть связи.

Так что же посоветовать регулятору в этой непростой обстановке? Теперь это уже не «бином Ньютона», посему:

- следует ввести в нормативную базу понятие механизма DPI в качестве кнута и легитимизировать ограниченную сетевую нейтральность в качестве пряника;
- необходимо разрешить операторам ограничивать сторонний трафик, но не ниже, чем до 20% общей пропускной способности каналов связи. Это оставляет надежду «независимым» контент-провайдерам с «легким» трафиком, тогда как обладателям «тяжелого» придется-таки договариваться с сетевиками о совместном расширении полосы пропускания или даже строить свои сети;
- операторы, не обладающие прозрачным механизмом мониторинга и приоритизации трафика, не должны иметь права на какие-либо его ограничения, т.е. для них вводится полный сетевой нейтралитет до тех пор, пока не обзаведутся указанным механизмом;
- в результате данного регуляторного компромисса низкоскоростные сервисы (планка может быть установлена, скажем, на 128 кбит/с), о которых говорил в прошлый раз Тим Бернес-Ли, все-таки могут получить определенный «нейтралитет» и стать соцпакетом;
- указанный сетевой мониторинг должен быть прозрачным для регулятора (надзорных органов) и может быть с успехом использован не только для контроля качества предоставления услуг, но и для создания центров мониторинга соответствующей инфраструктуры России в целях обеспечения ее целостности, защищенности и работоспособности (ну а за обман регулятор обязательно придумает наказание);
- предоставление тех услуг, которые невозможно проконтролировать, должно быть прекращено (к такому выводу пришел, в частности, индийский регулятор TRAI во время обсуждения ситуации, сложившейся с мониторингом Blackberry-сервисов). Именно так можно интегрировать обеспечение информационной безопасности в телекомсервисы в национальном масштабе (тут заодно получается и механизм отключения ресурсов и сервисов);
- вот, собственно, и все, если не считать СОРМ, которому также пригодится DPI.

Возможно, в зависимости от ситуации на рынке регулятор изменит соотношение 20:80. К примеру, если некоторые операторы окажутся неспособными далее самостоятельно развивать сервисы (такая тенденция имеется). И если компания Apple, не будучи оператором, но обладая всего двумя терминальными устройствами iPhone и iPad, захватила огромный рынок, то, быть может, «битовая труба» – это и есть их настоящее призвание? Пусть ею и остаются (а DPI установят, конечно).

Стоит только регулятору об этом заявить, и мы сами не заметим, как простимулируем операторов развивать дополнительные услуги. С партнерами и конкурентами, с Apple и Skype, хоть с самим дьяволом, лишь бы сохранить показатели доходности. А тут, глядишь, и государство с гражданами что-нибудь получат.

Впрочем, в Интернете не поставишь DPI, а всякую цензуру, как известно, Интернет воспринимает как повреждение на линии и ищет обходные маршруты. О том, как могут складываться взаимоотношения Telecom 2.0 и Интернета, – в следующий раз. ИКС

От доверительных отношений – к доверенному оборудованию

В сентябре этого года Crossbeam RT – СП американской компании Crossbeam Systems и РКСС – начнет выпуск платформ сетевой безопасности X-Series. Производство в России и получение статуса доверенного оборудования откроет ему шлюзы на рынки России и других стран СНГ, уверен Майк РАФФОЛО, президент и главный исполнительный директор Crossbeam.

Майк РАФФОЛО

– Итак, Crossbeam и «Российская корпорация средств связи» объявили о создании СП. Почему было принято это решение, чем объясняется выбор партнера?

– Мы заинтересованы в партнерских отношениях, позволяющих реализовать огромный потенциал российского рынка. Здесь работает много компаний, на которые как раз и ориентирована продукция Crossbeam: операторы связи, государственные организации, предприятия крупного бизнеса. Почему с РКСС? Для нас ответ простой: мы сотрудничаем с компанией больше двух лет и за это время у нас сложились хорошие доверительные отношения. Можно сказать и так: доверенные ☺. РКСС – первая в России компания, которая специализируется на производстве и разработке доверенного телекоммуникационного оборудования. Мы хотим вывести на российский рынок доверенные продукты, лучшие в своем классе.

– «Доверенное оборудование» означает, что исходные коды программного обеспечения, управляющего этим оборудованием, проверены сертификационными структурами ФСБ России на основе специальных методик и тестов, после чего выдается соответствующее заключение об отсутствии в данном ПО «недекларируемых возможностей». Эта сложная кропотливая работа занимает несколько месяцев, и далеко не каждый зарубежный вендор готов подвергнуть свою продукцию такой проверке. Почему вам это важно?

– Разумеется, не всем организациям требуется продукт, сертифицированный по высшему уровню защиты, можно продавать и «недоверенное» оборудование. Так мы и поступали до создания совместного предприятия. Но сертификация продукции Crossbeam RT и российская сборка (производство будет организовано на заводах Госкорпорации «Ростехнологии», в которую входит РКСС. – *Прим. ред.*) позволят увеличить продажи, в первую очередь в госсектор, поскольку в итоге решения будут отвечать жестким требованиям госорганов России по безопасности и надежности. Но и для операторов, и для корпоративных заказчиков статус доверенного оборудования, я думаю, будет серьезным аргументом в пользу выбора решений Crossbeam RT. Таким образом, создание совместного предприятия Crossbeam RT станет важным шагом в укреплении наших позиций на российском рынке вместе с партнером, который может обеспечить самые высокие стандарты производства, сертификации и поддержки для наших платформ сетевой безопасности X-Series.

– А чем, на ваш взгляд, объясняется выбор партнера со стороны РКСС?

– Задачи управления безопасностью ИТ-инфраструктуры сейчас очень остро стоят перед всеми компаниями мира – и мы помогаем их решить, минимизируя сложность ИТ-инфраструктуры и максимизируя ее производительность в защищенной среде. Без преувеличения, у нас лучшие в своем классе решения. На единой платформе сетевой безопасности Crossbeam X-Series может работать множество приложений от различных поставщиков – наших партнеров IBM, Check Point, McAfee, Actiance, Imperva, Sophos и Sourcefire. Их продукты оптимизированы для работы на платформе X-Series. Иными словами, мы даем заказчикам возможность выбирать самые лучшие программные средства любого производителя – это во-первых. Во-вторых, заказчики с помощью наших решений сокращают совокупную стоимость владения системами безопасности, консолидируя их в соотношении 50:1, когда «железо» 50 устройств заменяется единой платформой. И в-третьих, решение легко масштабируется без измене-

ния ИТ-инфраструктуры, что немаловажно с учетом постоянного роста объемов трафика данных в сетях большинства крупных компаний и операторов связи. Таким образом, мы даем компаниям удобный инструмент управления безопасностью очень сложной, нередко запутанной ИТ-инфраструктуры, ее масштабирования и повышения производительности в защищенной от киберугроз среде.

– Как рынок реагирует на это предложение?

– Сегодня решениям сетевой безопасности от Crossbeam доверяют более 900 глобальных компаний, операторов связи (включая 11 из 12 крупнейших в мире операторов) и поставщиков облачных услуг. В структуре бизнеса около 10% занимает облачный сегмент, примерно 40% – корпоративный и 50% – телеком. Мы присутствуем в 50 странах мира, работаем на рынке 11 лет, но рост был особенно быстрым в последние три года в силу обострившихся угроз информационной безопасности на сетях крупных компаний. И сейчас Crossbeam занимает лидирующее положение на мировом рынке систем сетевой безопасности для крупного бизнеса.

– Три года назад Crossbeam открыла свой офис в России, и к настоящему моменту у компании сложилась партнерская сеть из нескольких дистрибьюторов и реселлеров. Что произойдет с ними и как изменится модель продаж в связи с созданием совместного предприятия?

– Некоторые изменения произойдут, но они не будут драматическими. Договоры Crossbeam, ранее заключенные с российскими компаниями-партнерами, будут переведены на совместное предприятие Crossbeam RT. Если раньше они покупали оборудование непосредственно у Crossbeam, то теперь будут покупать у СП. Вероятно, со временем двухуровневая система продаж трансформируется в одноуровневую, когда Crossbeam RT будет выступать в качестве и производителя и дистрибьютора, а все остальные партнеры – в качестве реселлеров. Нет никакого смысла удлинять эту цепочку, тем более что с точки зрения их прибыли ничего не изменится.

– Возвращаясь к вопросу сертификации: а как быть с вашими технологическими партнерами – зарубежными поставщиками приложений, – если они не захотят участвовать в этом процессе, отдавать на проверку исходные коды своих программ?

– Каждый партнер будет решать сам: сертифицировать им или нет, открывать или нет. Мы ведь тоже, прежде чем принять решение об открытии исходных кодов, тщательно проанализировали ситуацию, взвесили все «за» и «против». И пришли к выводу, что сертификация поможет нам расширить продажи своих продуктов среди очень крупных российских предприятий. Поэтому начали процесс сертификации и намерены завершить его осенью этого года. Если наши технологические партнеры примут решение об открытии исходных кодов, это позволит и им расширить круг своих заказчиков. А мы, со своей стороны, предоставим им возможность участвовать в сертификационном процессе.

– По данным РКСС, первоначальные совместные инвестиции в СП на 2011 финансовый год составили 100 млн руб. В бизнес-плане совместного предприятия – окупить эти затраты в течение 24 месяцев, а к 2015 г. достичь оборота в 50 млн долл. Реально ли добиться таких объемов продаж в столь короткие сроки?

– На самом деле это очень реалистичный прогноз. Вообще, у совместного предприятия очень амбициозные планы: мы намерены занять серьезную долю на этом рынке в России и других странах СНГ. Прежде чем создавать СП, мы проделали большую работу, продумав и скрупулезно просчитав бизнес-план во всех аспектах. Эти цифры подтверждены потенциальными возможностями заказчиков, заказов, проектов и т.д.

Как самостоятельное юридическое лицо СП оформлено в виде общества с ограниченной ответственностью; в Совет директоров входят представители обеих сторон. В области разработок программного обеспечения мы видим хороший потенциал для работы с российскими партнерами. Планируем также внедрять уже существующие российские наработки; более того, в соответствии с нашим бизнес-планом со временем в совместное предприятие войдет группа российских программистов, которая будет заниматься адаптацией существующего программного обеспечения и разработкой новых приложений на базе Crossbeam X-Series, что, несомненно, значительно повысит российскую интеллектуальную составляющую в конечных продуктах.

– Но какая может возникнуть потребность в новых разработках, если уже сейчас на платформе собраны все возможные приложения?

– С точки зрения сетевой безопасности – да, на платформе есть все. Мы предлагаем лучшие в своем классе решения отдельных поставщиков: для предотвращения хакерских атак, вторжений, для управления системами информационной безопасности. Но платформа представляет собой уникальное произведение технологического искусства, этот оркестр играет любое музыкальное произведение. Обеспечение сетевой безопасности – изначальное и основное предназначение платформы, но в ней заложены и возможности решения многих других сетевых задач (например, трансформации данных). Возможности исключительно широкие, они ограничиваются разве что фантазией заказчика, и какие именно приложения будут разработаны и предложены российскому рынку – зависит только от желаний клиентов. Сейчас мы уже ведем переговоры в этом русле с рядом компаний в России, и могу предположить, что на рынке появятся действительно очень интересные решения – по прошествии некоторого времени, необходимого на документальное оформление желаний заказчиков, написание соответствующих программ и получение полного доверенного решения «внутри» Crossbeam X-Series.

Беседовала **Лилия ПАВЛОВА**

Проект дата-центра: советы для CIO

Российский рынок дата-центров после кризисного проседания вновь воспрянул. Стартуют и уже реализуются проекты все более крупных и технологически более сложных ЦОДов. Инвестиции в строительство и модернизацию дата-центров растут, но растут и требования заказчиков к эффективности этих инвестиций.

О том, как выбрать проект ЦОДа и исполнителей этого проекта, как увязать характеристики дата-центра с потребностями бизнеса компании, шла речь на круглом столе «Проект создания ЦОДа: вопросы для CIO», организованном журналом «ИКС».

Любой дата-центр – достаточно серьезный объект, срок окупаемости которого составляет обычно не один год. В таких проектах велики не только начальные капитальные затраты, но и расходы на эксплуатацию. Первыми это осознали компании, строящие крупные дата-центры: теперь они часто запрашивают расчет общей стоимости владения (TCO) для ЦОДа на период до 10(!) лет, чего раньше не бывало.

Консультант: необходимое и достаточное

ИТ-директора компаний, берущихся за создание собственных дата-центров, конечно, понимают, что подобные проекты требуют серьезного подхода и привлечения самых разных специалистов. Но далеко не все они осознают, что даже постановка задачи проектирования ЦОДа – дело непростое, тем более если необходимо спланировать его развитие на несколько лет вперед (кстати, многие ли догадывались три года назад о грядущем нашествии облачных вычислений?). Даже если ИТ-директор и его подразделение хорошо знают требования бизнеса компании и примерно представляют, как их можно реализовать в дата-центре, это не повод отказываться от услуг специалистов.

Денис ТУКАЛЕВСКИЙ (банк «Русский стандарт»): «Привлечение консультантов подразумевает внедрение каких-то новых технологий, иначе какой смысл?»

Помочь заказчику сформулировать базовые технические требования, из которых в дальнейшем вырастет грамотное техническое задание (ТЗ) на ЦОД, призваны профессиональные консультанты. Впрочем, отзывы о целесообразности их привлечения весьма неоднозначны в силу того, что роль консультанта (а также проектировщика, поставщика оборудования и исполнителя) у нас по традиции исполняют системные интеграторы, стремящиеся делать абсолютно всё. В любом случае компания должна оценить временные и финансовые затраты и сравнить, каковы они будут в вариантах участия консультантов или опоры на собственные силы, считает Дмитрий Тихович (Citrix Systems); и практика показывает, что в подавляющем большинстве случаев рекомендации консультантов оказываются более экономически выгодными, даже с учетом оплаты их услуг.

Дмитрий ЛИТОВЧИН («EMC Россия»): «Мы ожидаем от консультанта другого взгляда на нашу бизнес-задачу»

По словам генерального директора компании «Ди Си Квадрат» Александра Мартынюка, вопросы планирования и создания ЦОДа, выбора площадки и технического решения часто вводят неподготовленного заказчика в настоящий ступор. Поэтому консультант формально или неформально присутствует сейчас фактически в любом проекте строительства крупного ЦОДа. Именно консультант своими наводящими вопросами призван вывести заказчика из вышеупомянутого состояния и направить на путь истинный. Путь этот обычно долог и труден для всех участников: поиск ответов на множество вопросов, разработка вариантов строительства, откаты назад, новые варианты и т.д. Цель всех этих усилий по идее должна оправдать потраченные на них средства: чем конкретнее будет поставлена задача, тем быстрее заказчик сможет ее реализовать и начать возвращать деньги, вложенные в проект.

Конечно, опытная компания – к примеру, Mail.Ru, которая строит уже не первый и не второй свой ЦОД, – в принципе может обойтись без консультантов. Но это, несомненно, предполагает обстоятельный анализ совершенных ошибок и опыта, полученного в предыдущих

Сергей ПИСКУНОВ, директор по ИТ, «СОГАЗ»:

«Мы не ИТ-компания, а проекты у нас достаточно серьезные и требующие соответствующей компетенции, поэтому мы привлекаем консультантов, проводим тендеры, сравниваем разные варианты решений и при этом стараемся иметь дело только с теми компаниями, которые могут уверенно гарантировать результат».

проектах. В этом случае, как считает заместитель технического директора Mail.Ru Алексей Марухин, компания в состоянии не только профессионально сформулировать собственные технические требования к дата-центру, но и выступить генеральным подрядчиком в его строительстве. Рафаэль Сухов, генеральный директор Stack Labs, согласен с тем, что в проекте дата-центра необходимо участие консультанта, но роль последнего, по его мнению, весьма неблагодарна, поскольку бизнес-требования заказчика и его представления о проекте и распределении ролей его участников часто противоречат друг другу, а потому ключевым навыком консультанта должно быть умение находить компромиссы. Кроме того, консультант должен хорошо понимать особенности бизнеса, которому он помогает, и иметь глубокую техническую подготовку, чтобы свести воедино порой противоречивые требования заказчика. Правда, собственный опыт привлечения консультантов Stack Labs называет полезным, но неуспешным, самокритично признавая, что в этом, скорее всего, была вина обеих сторон: заказчик, возможно, не смог достаточно четко сформулировать саму задачу, а консультант, в свою очередь, не смог объяснить заказчику, что именно тот не понимает.

Конечно, вряд ли кто-то будет спорить, что в таком проекте, как новый мега-ЦОД Сбербанка (а это четырехэтажное здание, 15 тыс. кв.м машинных залов и 20 МВт подведенной мощности), консультант должен быть, и даже не один. В этом качестве сейчас выступают три организации из разных стран: одна отвечает за общую концепцию, вторая – за инженерную инфраструктуру, а третья (небезызвестный Uptime Institute) проверяет проектную документацию на предмет ее последующей сертификации на соответствие уровню надежности Tier III. Если еще учесть, что Сбербанк пожелал иметь максимально «зеленый» дата-центр с PUE = 1,3 и это потребовало применения новой пока для российского рынка технологии охлаждения KyotoCooling, а также что в этом ЦОДе необходимо обеспечить очень высокий уровень физической и информационной безопасности, задача у проектировщиков непростая. Да и у заказчиков тоже: ведь надо сохранить управляемость проекта и скоординировать действия трех организаций, каждая из которых является признанным в мире экспертом в своей области. Характерный штрих к описанию процесса создания этого дата-центра добавляют слова генерального директора компании ADM Partnership Максима Иванова: «Нам как проектировщикам интересно участвовать в проекте, где нашу работу проверяют сразу три консультанта».

По большому счету задача консультанта состоит в том, чтобы обеспечить заказчику непредвзятый взгляд на проект дата-центра с разных сторон, – а это требует понимания специфики его бизнеса. Дмитрий Литовчин («EMC Россия») подчеркивает, что прежний подход к построению ЦОДа как к набору из серверов, СХД, ИБП, системы охлаждения и фальшполов сейчас уже не позволяет создавать эффективные решения. Вся архитектура дата-центра должна строиться исходя из того, какую информацию имеет компания, что она с этой информацией собирается делать и какие результаты планирует получить. Иными словами, идти надо от бизнес-процессов, а не от серверных стоек.

Застывшая музыка ЦОДа

Еще одна важная задача, которую приходится решать ИТ-директору любой компании в связи с созданием нового ЦОДа, – это разработка архитектуры будущего дата-центра. Кроме всего прочего, в ней необходимо предусмотреть дальнейшее развитие и модернизацию ЦОДа с учетом новых технологических веяний и бизнес-трендов. Понятно, что если ЦОД для данной компании – это профильный бизнес, то скорее всего именно ИТ-директор будет тем самым архитектором проекта. Но если компания специализируется на каких-то других материях, то число кандидатур на должность архитектора сразу увеличивается: системный интегратор, уже упомянутый консультант, проектировщик, поставщик оборудования. Доводы в пользу всех перечисленных участников найти несложно, но, как предостерегает М. Иванов, почти всегда у всех у них есть тайный умысел склонить заказчика на ту или иную платформу или технологию и/или продать побольше оборудования либо услуг, а это чревато «пере-

Сергей КАРПОВ, начальник отдела архитектуры вычислительных комплексов, Альфа-банк:

«Архитектором дата-центра вполне может быть системный интегратор, но в этом случае ИТ-директор должен быть тем контролером, который не даст испортить проект».

косом» проекта и получением далеко не самого эффективного результата.

Если же брать компании, в основе бизнеса которых лежат специфические процессы, определяющие требования к ЦОДам (например, в банках дата-центр используется для обработки транзакций, у телекоммуникационных операторов – во главе угла биллинг и т.д.), существует вероятность, что именно руководство профильного бизнеса возьмет на себя функции архитектора ЦОДа. Последствия такого решения могут быть разными, но ответственность за работу готового дата-центра в любом случае придется нести ИТ-директору.

Конечно, заказчику важно получить нормально функционирующий ЦОД, и желание руководства компании поучаствовать в процессе задания параметров его работы вполне понятно, но, по мнению Р. Сухова, в идеале архитектором проекта должен быть интегратор, потому что именно он знает особенности всех технологических решений, плюсы и минусы всех инженерных систем и именно он, зная потребности заказчика, может выбрать необходимую конфигурацию дата-центра и построить его в соответствии с ТЗ. Хотя в принципе архитектором проекта может быть и ИТ-директор компании-заказчика, и технический директор, и главный инженер, лишь бы он осознавал пределы своей компетенции и прислушивался к мнению более квалифицированных в деле ЦОДостроения специалистов – консультанта и системного интегратора, а они, в свою очередь, должны учитывать интересы бизнеса заказчика. В общем, вариантов масса, главное – правильно оценить ситуацию.

CAPEX vs OPEX

Еще один вопрос, в ответе на который заказчики и проектировщики дата-центров часто расходятся между собой, – это баланс между первоначальными инвестициями в проект ЦОДа и затратами на его последующую эксплуатацию. Разговоры о том, что необходимо более эффективно использовать электроэнергию, у нас ведутся уже давно, но факт остается фактом: энергоэффективность российской экономики в разы ниже, чем в западных странах. Российские тарифы на электричество уже обогнали американские и уверенно держат курс на европейский уровень, вендоры наперебой расхваливают свои новые «зеленые» решения для электроснабжения и охлаждения дата-центров, а производители процессоров постоянно снижают энергопотребление своих изделий при сохранении или даже увеличении их производительности. Но приводит ли это к массовому «позеленению» российских дата-центров? Приходится признать, что нет. И уникальный проект ЦОДа Сбербанка погоды не делает.

Леонид ГОЛОВИН («Московская теплосетевая компания»): «Наверное, сейчас лучше не вкладываться в энергоэффективное оборудование, а покупать то, что дешевле»

С одной стороны, такая организация, как Сбербанк, может себе позволить потратиться на «зеленый» дата-центр хотя бы из чисто имиджевых соображений, а с другой – при общей подводимой мощности в 20 МВт даже не очень большое повышение энергоэффективности дает серьезную экономию. Владельцы более скромных дата-центров относятся к энергоэффективности весьма прагматично. «Наши расчеты показали, что при мощности ЦОДа порядка 1 МВт за счет установки энергоэффективного оборудования можно получить экономию в $10–20 тыс. в год. Много это или мало, каждая компания решает для себя сама, но если сравнивать с первоначальными затратами на дата-центр, то деньги совсем небольшие», – говорит Денис Тукалевский, начальник управления ДИТ банка «Русский Стандарт». «Компьютерные технологии развиваются очень быстро, и через год за те же деньги мы сможем купить вдвое более мощный сервер, имеющий такое же энергопотребление, что и нынешние модели, поэтому экономически эффективнее покупать сейчас то, что дешевле, а при необходимости через год-два делать апгрейд. Платить на 30–40% больше за более энергоэффективное оборудование не имеет смысла», – считает зам. главного инженера по ИТ «Московской теплосетевой компании» Леонид Головин. В целом корпоративный пользователь готов сейчас покупать более дорогое энергоэффективное решение только в том случае, если оно более надежно, т.е. параметр экономии энергопотребления рассматривается только при прочих равных условиях. Операторы коммерческих дата-центров смотрят на эту проблему со своей колокольни: энергоэффективное решение позволяет в рамках выделенного лимита дефицитной электрической мощности установить дополнительные стойки с полезной ИТ-нагрузкой, т.е. получить дополнительные деньги с клиентов.

Рафаэль Сухов (Stack Labs): «Не желая тратиться на энергоэффективность, вы снижаете потенциал роста полезной ИТ-нагрузки в условиях лимитирования электрической мощности»

Ответы на вопросы, касающиеся построения и эксплуатации дата-центров, упираются в модель бизнеса компании и, как следствие, – в цену простоя ЦОДа в течение некоего критичного для данной компании времени. Если эта цена известна, то ИТ-директору уже несложно решить, использовать ли новые технологии или ограничиться традиционными, привлекать сторонних специалистов или опираться на собственные силы, на чем можно сэкономить, а на чем – нет.

Евгения ВОЛЫНКИНА

MicroTCA готовит вторжение на рынок защищенных систем и спецприменений

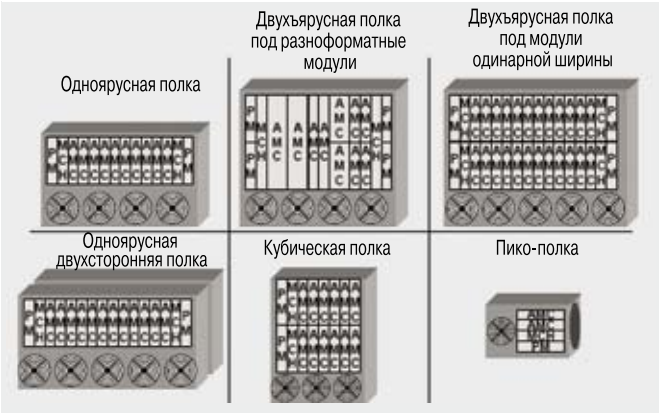
Сегодня стандарт MicroTCA стремительно набирает популярность не только в телекоме, но и во многих смежных отраслях: медицине, транспорте, промышленности, оборонной сфере. Наиболее захватывающих событий следует ждать в оборонно-аэрокосмическом сегменте, где MicroTCA начинает конкурировать как с унаследованными системными архитектурами CompactPCI и VME, так и с новым стандартом VPX.

Стандарт MicroTCA в свое время возник как попытка производителей оборудования, стремящихся на новые рынки, преодолеть изначальную ограниченность системной архитектуры AdvancedTCA/AdvancedMC рамками телекоммуникационных и близких к ним приложений класса high-end (подробнее см., например, «ИКС» № 9'2008, с. 86).

В архитектурном отношении работа над стандартом MicroTCA свелась к устранению промежуточного звена между объединительной панелью и модулями AdvancedMC. Избавив пользователей от необходимости иметь дело с громоздкими платами AdvancedTCA, которые с большим шагом устанавливаются перпендикулярно объединительной панели, стандарт MicroTCA позволил создавать компактные AdvancedTCA-подобные системы, не уступающие своим крупногабаритным собратьям практически ни в чем, кроме размеров (см. рисунок). В MicroTCA-системах высотой 3U или 4U с одной объединительной панелью и 12 процессорными модулями можно разместить 24 процессорных ядра в весьма небольшом пространстве уже в случае двухъядерных ЦП. При использовании же процессоров с четырьмя и более ядрами и/или многопроцессорных модулей плотность размещения обрабатывающих элементов увеличивается еще в несколько раз.

Таким образом, технология MicroTCA дает возможность реализовывать практически все преимущества архитектуры AdvancedTCA/AdvancedMC в корпусах меньших размеров и создавать гибкие высокопроизводительные системы с быстрыми последовательными соединениями между платами вместо параллельных шин. При этом модули AdvancedMC, имея компромиссные габариты, оказались очень хороши для построения компактных мультипроцессорных комплексов с повышенной механической прочностью. Применение высококачественных разъемов и компактных печатных плат весьма благотворно сказалось на механических свойствах конечных решений, в результате чего рынок AdvancedMC/MicroTCA начал тяготеть к системам повышенной надежности в целом и к защищенным системам в частности.

Стандартные типы корпусов MicroTCA



Справка

По данным аналитического агентства Venture Development Corporation, за период с 2007 по 2010 гг. объемы продаж оборудования AdvancedTCA/AdvancedMC/MicroTCA увеличились в 2,5 раза.

Актуальные тренды на рынке MicroTCA

В настоящее время в сегменте MicroTCA прослеживаются три основных тренда, обусловленных как эволюцией самого стандарта, так и меняющимися требованиями рынка. Во-первых, акцент с модулей одинарной ширины постепенно смещается на модули AdvancedMC двойной ширины, которые благодаря большей площади способны нести компоненты больших размеров и имеют более развитую функциональность. Например, холдинг Kontron выпускает в формфакторе AdvancedMC двойной ширины множество различных продуктов – от коммутаторов и сетевых плат с интерфейсами 10 Gigabit Ethernet до процессорных модулей.

Во-вторых, базовые аппаратные средства для построения систем MicroTCA, которые по-прежнему ориентированы на построение высокопроизводительных систем, работающих с интенсивными потоками данных, вслед за ростом процессорных мощностей и скоростей обработки данных активно обзаводятся быстрыми каналами 10 Gigabit Ethernet. Таков, в частности, модуль Kontron AM5030, выполненный на базе четырехъядерного серверного процессора Intel Xeon LC5518.

Третий и, пожалуй, самый важный тренд – это проникновение MicroTCA на рынок жестких специальных применений. Именно такую цель преследует создание спецификаций MTCA.1 (Air Cooled Rugged MicroTCA – защищенное оборудование MicroTCA с воздушным охлаждением), MTCA.2 (Hardened Air Cooled MicroTCA –

оборудование MicroTCA повышенной защищенности с воздушным охлаждением) и MTCA.3 (Hardened Conduction Cooled MicroTCA – оборудование MicroTCA повышенной защищенности с кондуктивным охлаждением). Первая спецификация, учитывающая требования мобильных решений и систем наружного базирования с охлаждением за счет конвекции, была принята консорциумом PICMG в 2010 г. и уже взята на вооружение ведущими производителями оборудования, третья принята в конце февраля 2011 г., в ближайшее время к ним должна присоединиться вторая. Спецификация MTCA.1 включает в зону ответственности MicroTCA оборонные приложения с классом окружающей среды EAC6 и классом вибрации V2 в терминологии ANSI/VITA 47. Спецификация MTCA.3 определяет интерфейс кондуктивного охлаждения, благодаря которому по своим термальным характеристикам, а также по устойчивости к ударам и вибрации оборудование MicroTCA сможет соответствовать самым «тяжелым» профилям стандарта ANSI/VITA 47 (иными словами, станет пригодным для создания герметичных систем с кондуктивным охлаждением, которые используются, в частности, на беспилотных летательных аппаратах и на других платформах с ограниченным свободным пространством). Переход плодов деятельности комитетов MTCA.1, MTCA.2 и MTCA.3 в статус утвержденных официальных документов консорциума PICMG – это мощнейший толчок к началу массового применения оборудования AdvancedMC/MicroTCA в некоторых очень интересных рыночных сегментах, включая аэрокосмический и оборонный.

Проникнуть на оборонно-аэрокосмический рынок мечтает любой производитель. А коли так, то вся многолетняя работа комитетов PICMG MTCA.1, MTCA.2 и MTCA.3 есть не что иное, как планомерная подготовка плацдарма для наступления на стандарт VPX – официально назначенный преемник системной архитектуры VMEbus, более трех десятилетий являвшейся для оборонно-аэрокосмической отрасли «своей». Разумеется, высоконадежное оборудование для жестких условий эксплуатации нужно не только космосу, авиации и оборонке: защищенные аппаратные средства с радостью принимают во многих других сегментах. Однако ценность приза, который получает поставщик, сумевший закрепиться в оборонно-аэрокосмическом сегменте, несопоставима с дивидендами от медицины и транспорта, которые, впрочем, в любом случае будут кстати.

Сильные стороны MicroTCA

Основное достоинство стандарта MicroTCA с точки зрения оборонных и аэрокосмических применений состоит в том, что он принадлежит к семейству стандартов нового поколения, исповедующих полный отказ от параллельных шин в пользу быстрых последовательных соединений между платами. Такие соединения могут реализовываться на базе Gigabit Ethernet, 10 Gigabit Ethernet, PCI Express, Serial RapidIO и некоторых других коммуникационных технологий. Топологически систему MicroTCA можно представить как сеть, узлами которой являются модули AdvancedMC, а роль коммутатора играет так называемый контроллер MCH, который реализуется либо как отдельный модуль AdvancedMC, либо как часть функций объединительной панели. Взаимодействие между слотами AdvancedMC по коммутируемым последовательным каналам создает условия для быстрого и беспроблемного наращивания производительности простым увеличением числа процессорных модулей.

Для разработчиков систем специального назначения представляют интерес и развитые функции системного управления MicroTCA, и поддержка «горячей» замены модулей. Специалистам, выбравшим стандарт MicroTCA, доступны широкий спектр изделий AdvancedMC на базе высокопроизводительных процессоров Intel Core Duo, Core 2 Duo и Core i7, передовых многоядерных ЦП с архитектурой PowerPC и сетевых процессоров, коммуникационные модули и модули накопителей, а также интегрированные платформы MicroTCA разных форм и размеров. При этом, как уже упоминалось, доля оборудования AdvancedMC/MicroTCA с поддержкой 10-гигабитных каналов постоянно растет.

Еще одно достоинство MicroTCA – его направленность на завоевание других рынков. Экспансия, расширение сферы применимости системной архитектуры AdvancedTCA/AdvancedMC – исходная цель стандарта MicroTCA и главный смысл его существования. Поэтому использование оборудования MicroTCA за пределами телекома с заходом в область высокопроизводительных промышленных, медицинских и оборонных приложений носит не спорадический, как в случае AdvancedTCA, а закономерный и ожидаемый характер. Диапазон текущих и будущих свойств оборудования AdvancedMC/MicroTCA в значительной мере пересекается с требованиями рынка спецприменений. Стандарт MicroTCA в своем исходном виде уже позволял решать довольно большой круг задач в оборонно-аэрокосмическом сегменте, спецификации же MTCA.1, MTCA.2 и MTCA.3 способны превратить MicroTCA в полноценного конкурента системной архитектуры VPX.

Фоном ко всему этому служит неуклонное увеличение числа поддерживающих технологию MicroTCA производителей и рост интереса к ней в нетелекоммуникационных секторах.

Весьма удачным следует признать и выбор момента для начала наступления стандарта MicroTCA на оборонно-аэрокосмический сегмент. При грамотных, в меру агрессивных действиях сил, продвигающих технологию MicroTCA на рынок систем спецназначения, ситуация «пересменки» между системными архитектурами VME и VPX позволит оборудованию MicroTCA захватить большую долю этого рынка, чем VME и VPX были бы готовы уступить ему при иных обстоятельствах.

Взвесим шансы на успех

Однако перечисленные выше преимущества стандарта MicroTCA в равной степени свойственны и системной архитектуре VPX, с которой он начинает вое-

вать за сегмент оборонных и аэрокосмических приложений. Архитектура VPX точно так же не обременена тяжелым наследием параллельных шин, позволяет использовать тот же набор коммуникационных технологий для организации взаимодействия между платами, поддерживает «горячую» замену, тыльный ввод-вывод и т.д., вплоть до наличия спецификаций, определяющих требования к защищенным решениям с кондуктивным и даже жидкостным охлаждением (стандарт VPX REDI, спецификация VITA 48).

На что же рассчитывают создатели спецификаций MTCA.1, MTCA.2 и MTCA.3, адресуя их рынку оборудования для систем спецназначения? Скорее всего, они полагаются на фактор массовости: поскольку стандарт MicroTCA родом с открытого и динамичного телекоммуникационного рынка, где работает много активно конкурирующих друг с другом независимых производителей, цена оборудования MicroTCA не может быть слишком высокой, чего нельзя сказать об аппаратных средствах VPX/VMEbus, существующих на значительно менее конкурентном рынке. Таким образом, аппаратные средства MicroTCA вправе претендовать на роль недорогой альтернативы сверхзащищенному оборудованию VPX. Альтернативы, способной обеспечивать высокую производительность, высокую готовность и чрезвычайно высокую пропускную способность при сравнительно малых размерах.

Под таким углом зрения затея с защищенными системами MicroTCA для оборонных приложений выглядит не столь уж безумной. Ведь ситуации, когда массовая технология вторгается в специальную прикладную область и противостоит там технологии эксклюзивной, глубоко в этой области укорененной, не так уж редки. Примерами могут служить конкуренция между системными архитектурами VME и CompactPCI и соперничество между процессорами x86 и PowerPC. Что-то подобное, на наш взгляд, должно произойти и с защищенными системами MicroTCA: со временем они займут на рынке спецприменений некоторую устойчивую нишу. VPX придется потесниться, и средняя стоимость решений на оборонно-аэрокосмическом рынке в результате снизится, равно как и порог вхождения на этот рынок для поставщиков оборудования. Еще более любопытных результатов можно ожидать от прихода защищенного оборудования MicroTCA на некоторые другие рынки (промышленный, медицинский), где нет ни безоговорочного доминирования каких-либо привилегированных системных архитектур, ни многолетних традиций, консервирующих исторически сложившееся положение вещей. В таких отраслях массовые недорогие аппаратные средства MicroTCA вполне способны устроить настоящий переворот и даже революцию, поскольку там переход на MicroTCA будет, по сути, эквивалентен движению в общем русле перехода с параллельных шин на быстрые последовательные соединения.

Беспроигрышная лотерея

Каковы могут быть итоги деятельного противостояния стандартов MicroTCA и VPX на рынке спецприменений? Спектр вариантов широк: от символического обозначения присутствия MicroTCA в исконных владениях VPX до почти равноправной конкуренции почти равноправных альтернатив. Правда, отход VPX под давлением MicroTCA на вторые роли представляется все же невероятным. Пока трудно сказать, какие аргументы из числа тех, что стандарт MicroTCA готов предъявить участникам оборонно-аэрокосмического рынка, окажутся убедительными, а какие – нет.

Но нужно учитывать и имиджевую составляющую: при любом исходе борьбы MicroTCA и VPX ее побочным результатом неизбежно станет рост авторитета MicroTCA абсолютно во всех сегментах компьютерной отрасли, включая медицинский, транспортный и промышленный, а также телекоммуникационный, с которого все и начиналось. В сущности, атака на рынок спецприменений является для стандарта MicroTCA этакой беспроигрышной лотереей с призом в виде роста продаж. Что, на наш взгляд, будет вполне справедливо. Ведь как стандарт весьма прогрессивный, позволяющий упаковывать производительность систем операторского класса в защищенные корпуса размером с обувную коробку, MicroTCA такого приза объективно достоин.

Владимир БРЕТМАН, директор направления базовых аппаратных средств ЗАО «РТСофт»
Леонид АКИНШИН, канд. физ.-мат. наук, обозреватель журнала «МКА: ВКС»
специально для «ИКС»

Облакам нужны специализированные бизнес-приложения

Подавляющее большинство облачных услуг, предлагаемых провайдерами, пока имеют весьма общий характер (хранение файлов, аренда виртуальных машин, антивирусная и антиспам-защита), т.е. ориентированы на широкий круг компаний. Об одном из редких примеров специализированных облачных сервисов рассказывает заместитель генерального директора компании DataLine Алексей СЕВАСТЬЯНОВ.

Алексей СЕВАСТЬЯНОВ

– Почему компания DataLine решила заняться облачными сервисами?

– DataLine всегда стремилась быть не просто оператором ЦОДов, сдающим площади под серверные стойки, а сервисной компанией, предоставляющей услуги ИТ-аутсорсинга. Поэтому с развитием технологий виртуализации мы стали предлагать своим клиентам и облачные сервисы. В мире и в России есть немало компаний, которые предоставляют услуги по аренде вычислительных ресурсов, но мы хотим пойти дальше и предложить заказчикам не просто аренду инфраструктуры, а инфраструктурные сервисы, нацеленные на решение конкретных бизнес-задач.

– С чего же решено было начать?

– С сервисов для медиакомпаний, которые периодически испытывают проблемы, обусловленные резким увеличением нагрузки на их онлайновые ресурсы. Известно немало примеров, когда самые разные сайты становились недоступными вследствие резкого возрастания нагрузки на них со стороны пользователей после публикации каких-то «горячих» материалов. Для таких случаев многие хостинг-провайдеры предлагают услуги по постоянному резервированию широких каналов связи, больших объемов памяти и вычислительных мощностей. Но это стоит немалых денег. Мы же предлагаем более гибкий подход: заказчик арендует у нас минимальный объем ресурсов, достаточный для нормальной повседневной работы, а при пиковых нагрузках он получает возможность быстро увеличить потребляемые мощности, заплатив в соответствии с «облачным» принципом только за их реальное использование.

– Как это работает?

– На нашем виртуальном кластере развертывается резервная площадка, на которую в штатном режиме по заданному заказчиком графику производится репликация его приложений и данных. Для передачи этих данных создается канал с минимально необходимой пропускной способностью, а в настройках DNS-сервера, который направляет пользователей на ресурс заказчика, устанавливается небольшое время обновления кэша (например, 10 минут). При возникновении пиковых нагрузок на DNS-сервере включаются альтернативные IP-адреса, расположенные на нашей резервной площадке, мощности виртуальной машины увеличиваются до требуемого уровня, а интернет-канал DataLine с необходимой пропускной способностью обеспечивает доступ пользователей к резервной копии сайта. Таким образом, происходит достаточно быстрое перенаправление трафика и запросов пользователей с основной площадки на резервную, а работоспособность и доступность ресурса восстанавливается.

При этом затраты заказчика сведены к минимуму. Во время работы онлайн-ресурса в штатном режиме с него взимается месячная абонентская плата за пользование виртуальной машиной небольшой мощности, дисковым пространством и достаточно узким каналом для репликации данных, а при пиковых нагрузках включается почасовая оплата виртуальной машины необходимой мощности и расширенного интернет-канала.

– Какие гарантии вы даете заказчику?

– В договор об уровне сервиса (SLA) записываются условия перехода в пиковый режим работы, которые определяются заданным максимальным временем отклика системы и/или минимальным превышением трафика над нормальным уровнем; параметры реакции нашей системы, т.е. какая доля трафика должна переместиться на нашу площадку в течение заданного промежутка времени; максимальные величины пропускной способности интернет-канала и компьютерных мощностей, предоставляемых заказчику в пиковом режиме; параметры работы и технического обслуживания резервной площадки в обычном режиме. Все эти характеристики постоянно контролируются и нами, и заказчиком.

– А как обстоят дела с больным для российских пользователей вопросом защиты данных от несанкционированного доступа со стороны обслуживающего персонала ЦОДа?

– Мы предлагаем целый ряд механизмов, которые должны убедить заказчика, что его данные будут в целости и сохранности. У нас есть специальные программные решения на базе технологии Cyber-Ark, которые позволяют осуществлять доступ администраторов ЦОДа к ресурсам заказчика только по так называемым псевдопаролям. Все действия администратора журналируются, есть также функция видеозаписи скриншотов с предоставлением клиенту AVI-файла. И, конечно, мы предоставляем все стандартные услуги по физической защите оборудования и каналов связи.

– Есть ли планы развития этого проекта?

– Да, теперь мы хотели бы предложить бизнес-ориентированные сервисы корпоративным заказчикам, работающим в других отраслях. Идеи уже есть, но о деталях говорить пока рано.

ЦОД·2011

6-я ежегодная международная конференция

издается с 1992 года
ИКС
www.iksmedia.ru

для профессионалов в области строительства и эксплуатации дата-центров
6 сентября 2011 года, гостиница Holiday Inn Sokolniki, Москва

Цели конференции:

- Обсудить в кругу профессионалов отечественной и зарубежной индустрии цодостроения актуальные вопросы строительства и эксплуатации ЦОДов
- Изучить лучшие зарубежные и российские практики
- Узнать о последних инновационных разработках в области цодостроения
- Рассмотреть эволюцию услуг ЦОДов
- Задать вопросы ведущим мировым экспертам и владельцам ЦОДов

Аудитория конференции: владельцы и руководители ЦОДов, ИТ-директора, директора по строительству, начальники служб эксплуатации, специалисты ИТ и инженерных служб. Всего более 400 участников.

Основные темы конференции

Оборудование и инфраструктура

- Кабельные системы
- Системы электроснабжения
- Климатическое оборудование
- Системы управления и мониторинга
- Системы физической безопасности
- Серверы, системы хранения, сетевое оборудование и ПО
- Виртуализация и консолидация
- ИТ-архитектура
- Информационная безопасность

Услуги

- Облачные сервисы
- ИТ-аутсорсинг
- SLA
- Managed Services

Управление и экономика

- Создание бизнес-концепций
- Типы ЦОДов
- Управление проектами создания ЦОДов
- Стандарты, сертификация
- Модернизация
- Аутсорсинг персонала
- Оптимизация затрат на инфраструктуру и ПО
- Повышение доходов от услуг
- Возврат инвестиций
- Энергосберегающие технологии

Инновации

- Модульные ЦОДы
- «Зеленые» подходы в ЦОДах
- Виртуальный ЦОД
- Новые инженерные решения

По вопросам спонсорского и делегатского участия обращайтесь в коммерческий отдел журнала «ИКС» по телефонам: (495) 229-4978, 785-1490, 502-5080 или факсу (495) 229-4976.

Более подробная информация на портале **www.iksmedia.ru/dpc_2011/dpc_conference_2011.html**

Организатор – журнал «ИКС»

Домовые сети Ethernet нового поколения

Локальные сети нового поколения (Next Generation LAN, NGL) не только позволят предоставлять широкополосный доступ в Интернет, ликвидировать нехватку IPv4-адресов и повысить безопасность пользования Всемирной паутиной, но и могут стать основой для построения новой глобальной сети связи – InterEthernet.

Сергей ЗАКУРДАЕВ,
независимый эксперт

Построение NGL

Первоначально компьютеры создавались для автономных вычислений, однако впоследствии возникла необходимость в их объединении в локальные сети (ЛВС). Так появилась технология Ethernet (стандарт IEEE 802.3); локальные сети в то время строились как одноранговые с разделяемой средой передачи, что резко снижало их эффективность.

Современные локальные сети на основе коммутаторов имеют архитектуру «клиент-сервер». При этом ПК играет роль универсального средства связи, обеспечивающего передачу данных, прием телевидения (IPTV) и телефонную связь (VoIP), а в перспективе, при оснащении всех ПК видеокамерами, можно будет организовать и видеосвязь по технологии Video Communications over IP (VCoIP). Сервер (кластер серверов-лезвий) локальной сети может выполнять разнообразные функции: осуществлять контроль и управление доступом в Интернет, динамическое назначение IP-адресов клиентам через службу DHCP, антивирусную защиту и контентную фильтрацию трафика; служить межсетевым экраном с поддержкой NAT, а также организовывать службы DNS, видеосвязи, видеоконференцсвязи, ТВ по требованию и виртуальные частные сети (VPN).

В коммутируемых локальных сетях порт коммутатора, соединенного с сервером, становится узким местом из-за угрозы его переполнения и возможности потери информации. Поэтому был разработан специальный протокол 802.3x, согласно которому на физическом уровне генерируются две команды: «Прекратить передачу» и «Разрешить передачу», что в итоге снижает эффективность работы всей сети.

Для организации эффективной работы локальной сети по схеме «клиент-сервер» необходимо обеспечить прямой и равноправный доступ каждого ПК-клиента к серверу, т.е. перейти от распределенной локальной сети на базе существующих коммутаторов к централизованной сети при сохранении в ПК существующих сетевых карт (network interface card), реализующих протокол Ethernet со скоростями 1/10/100 Мбит/с.

Это можно сделать путем использования нового класса устройств – семейства коммутирующих мультиплексоров («Декадный мультиплексор локальной сети», патент РФ № 2159511, 1999 г.), которые с целью обеспечения масштабируемости локальной сети нового поколения (NGL) на 10/100/1000 пользователей образуют иерархическую структуру.

При этом сетевым картам ПК в соответствии с процедурой LAA (locally administered address), предусмотренной стандартом IEEE 802.3, с помощью

Рис. 1. Структура иерархического MAC-адреса

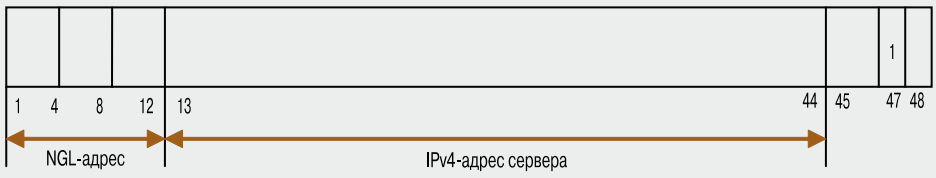
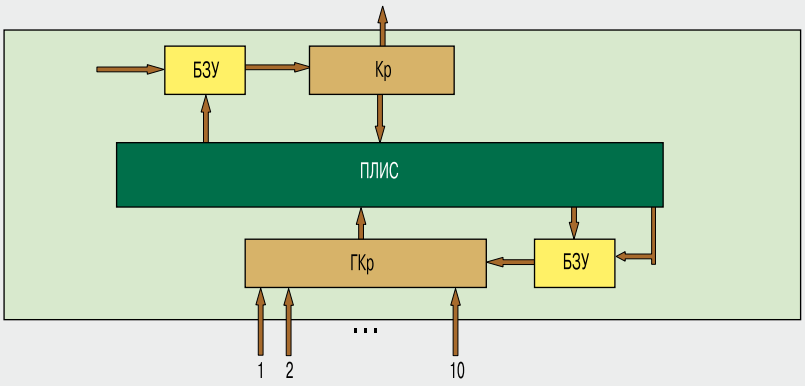


Рис. 2. Блок-схема коммутирующего мультиплексора



Кр – контроллер Ethernet 10*C* Мбит/с
ГКр – групповой контроллер Ethernet *C* Мбит/с
C = 1, 10, 100
БЗУ – буферное запоминающее устройство

утилиты SMAC назначаются новые иерархические гибридные MAC-адреса: три младшие тетрады (разряды 1–12) используются для коммутации в локальной сети; разряды 13–44 отводятся для размещения IPv4-адреса сервера, который в данном случае является групповым адресом для всех ПК локальной сети; разряды 45–48 – служебные, причем 47-й разряд устанавливается равным 1 (рис. 1).

Коммутирующие мультиплексоры (SWItching multiPLEX, SWIPLEX, SX) включают в себя семейство устройств – младшего (SX1), среднего (SX2) и старшего (SX3) уровней, обеспечивающих предварительную буферизацию кадров (рис. 2), которые поступают из 10 каналов Ethernet *C* Мбит/с, и затем их мультиплексирование в один канал Ethernet 10*C* Мбит/с (*C* = 1, 10, 100) для восходящего трафика к серверу по принципу FIFO («первым вошел – первым вышел»).

Коммутирование кадров, поступающих по одному каналу Ethernet 10*C* Мбит/с, в 10 каналов Ethernet *C* Мбит/с для нисходящего трафика от сервера производится простым преобразованием двоичного четырехразрядного кода соответствующей тетрады иерархического MAC-адреса назначения поступившего кадра Ethernet в десятичный код адреса предварительной буферизации (значения от 1 до 10): первой тетрады – в SX1, второй тетрады – в SX2, третьей тетрады – в SX3.

Аппаратная реализация функций мультиплексирования и коммутации основана на использовании программируемых логических интегральных схем (ПЛИС). Такие схемы содержат несколько миллионов «эквивалентных вентилей» и позволяют создавать логические и функциональные схемы любой сложности. Это даст возможность исключить генерацию и обработку таблиц MAC-адресов в каждом порту, которые в существующих коммутаторах осуществляются высокопроизводительными микропроцессорами. Коммутирующие мультиплексоры можно будет выполнить по технологии plug & play, что резко снизит их стоимость и упростит эксплуатацию.

Каскадирование данных устройств, реализованных в виде плат (bladeswiplex), позволит строить сети NGL, масштабируемые от 10 до 1000 пользователей, причем каждому из абонентских ПК будет предоставлен дуплексный канал Ethernet 1/10/100 Мбит/с для связи с сервером, что исключит необходимость управления потоком в сети (протокол 802.3x).

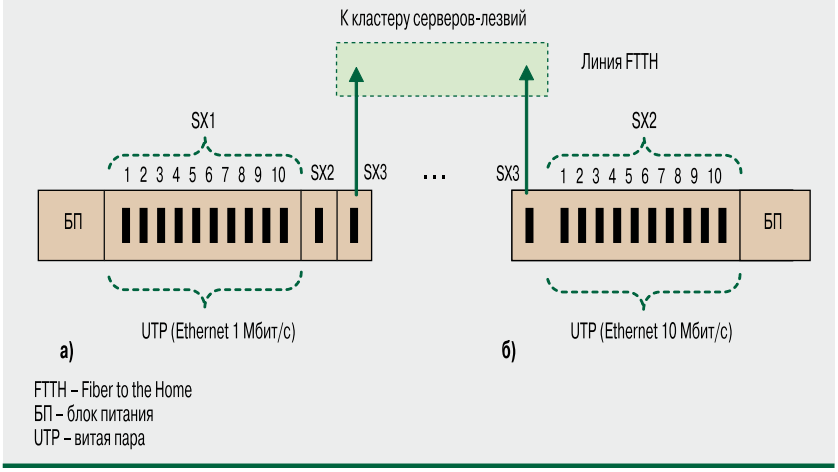
Благодаря наличию прямого соединения между сервером и ПК последние могут быть выполнены в виде тонких клиентов без жестких дисков и даже в виде одноплатных компьютеров со встроенной клавиатурой. ПО тонкого клиента включает лишь ядро ОС, которое требуется для обеспечения его работы, а другие необходимые программы может предоставить сервер. Это облегчает отказ от автономной (и рассчитанной на все случаи жизни) ОС и переход на свободное ПО.

От NGL к домовым сетям

NGL могут стать основой для построения сети Home Ethernet, объединяющей домашних пользователей, когда волоконно-оптический канал по протоколу Gigabit Ethernet от кластера серверов-лезвий провайдера подводится к дому к стеку коммутирующих мультиплексоров SX3 – SX2 – SX1. Возможны два варианта подключения.

По оценке экспертов, большинству домашних пользователей, уже имеющих телефонную связь и кабельное телевидение (30 каналов и более), достаточно получить канал доступа в Интернет со скоростью 1 Мбит/с по умеренной цене. Такую возмож-

Рис. 3. Схема подключения домовой сети Ethernet



FTTH – Fiber to the Home
БП – блок питания
UTP – витая пара

NGL могут стать основой для построения сети Home Ethernet, объединяющей домашних пользователей

ность обеспечивает подключение через коммутирующий мультиплексор SX1 (рис. 3, а) (число абонентов может наращиваться от 100 до 1000). Продвинутым пользователям (до 100 абонентов) может быть предоставлен канал Ethernet 10 Мбит/с, по которому организуется мультисервисное обслуживание (рис. 3, б).

Кроме того, продвинутые пользователи могут создать себе «умную квартиру» путем построения собственной локальной сети с помощью концентратора, который может подключить до 15 новых устройств (ПК, домашних кинотеатров, СВЧ-печей, других приборов), а также систем учета (электричества, воды) и контроля (охранной и пожарной сигнализации).

Число пользователей может быть кратно увеличено, поскольку волоконно-оптический кабель может состоять из нескольких десятков волокон, а число серверов-лезвий в кластере не ограничено (в разумных пределах).

Все ПК благодаря протоколу Ethernet 802.2 (LLC-SNAP) имеют возможность как непосредственно использовать мультимедийные протоколы прикладного уровня (SIP, SDP и др.), так и подключать стек протоколов TCP/IP (в этом случае SNAP имеет код 0800). При этом протокол IP не будет выполнять главных своих функций – маршрутизации и формирования адреса нового кадра, а будет служить лишь для подключения портов протокола TCP, необходимых для реализации технологии NAT.

■ ■ ■

В перспективе NGL, создаваемые по всему миру и прежде всего в России, могут быть объединены (по технологии NAT) в новую глобальную сеть связи – InterEthernet, число пользователей которой сможет превысить число существующих абонентов Интернета (IPv4) более чем в 1000 раз. Эту сеть целесообразно также назвать Интернет-3 – в отличие от Интернет-2, сети, использующей протокол IPv6. Интернет-3 может стать физической основой для построения глобального информационного общества. ИКС

ИКС pro технологии

ИБП: экономия и экология

Игорь КИРИЛЛОВ

Энергоэффективность сегодня рассматривается как одна из важнейших характеристик ИБП. Неудивительно, что все крупные мировые производители предлагают специальные технологии для улучшения этого показателя в своих системах. Но наряду с повышением КПД и экономией электроэнергии постепенно возрастает и роль экологической безопасности.

Отрасль ИТ идет в авангарде мировых технологических тенденций, среди которых – стремление к энергоэффективности и экологичности решений. Постоянное наращивание вычислительной мощности ИТ-систем требует самых эффективных средств энергоснабжения. Это в большой степени относится и к ИБП, особенно к тем моделям, которые применяют в дата-центрах. Поэтому многие производители сегодня стараются использовать в своих решениях специальные экологичные («зеленые») технологии, которые не только повышают КПД устройств, но и снижают количество вредных отходов в их производстве.

Кроме того, производители стремятся привести свою продукцию в соответствие с международными экологическими стандартами и требованиями независимых организаций, занимающихся вопросами экологичности ИТ-решений. В целом же вопросы энергетической эффективности и экологической безопасности выпускаемого оборудования для производителей ИБП относятся сегодня к числу наиболее приоритетных.

Эффективность в основе

Отметим, что первоначально понятие экологичного («зеленого») оборудования было синонимом энергоэффективных систем, влияние самих ИБП на окружающую среду фактически не учитывалось. И хотя постоянный рост цен на энергоносители делает именно энергоэффективность наиболее важным аспектом «зеленых» технологий, в последние несколько лет все крупные производители серьезно задумались над тем, чтобы подходы, используемые на всех этапах производства, эксплуатации и утилизации ИБП, были более «дружественными» для окружающей среды. И не только задумались, но и начали воплощать эти идеи в жизнь, чему способствуют и различные независимые организации, следящие за экологичностью в сфере ИТ: их рекомендации во многих случаях учитываются при разработке новых моделей ИБП. Сегодня невозможно стать ведущей компанией в сфере производства ИБП, не имея собственных разработок, направленных на повышение энергоэффективности и экологической безопасности.

Тем не менее любые «зеленые» технологии всегда преследуют главную цель – сделать инженерные системы более эффективными: ведь в больших вычислительных центрах и других крупных объектах энергоэффективность напрямую влияет на прибыльность проекта.

В энергоэффективных технологиях заинтересованы прежде всего компании, внедряющие крупные дата-центры с энергопотреблением более 1 МВт, отмечает Сергей Щербаков, руководитель группы системных инженеров APC by Schneider Electric в странах СНГ. В этом случае, учитывая масштаб проекта, экономия будет очевидной. Вместе с тем в Европе и Северной Америке сегодня крайне актуален вопрос минимизации вредного воздействия на окружающую среду. Во многих европейских странах невозможно получить одобрение надзорных органов для строительства нового ЦОДа, если его показатель энергоэффективности (Power Usage Effectiveness, PUE) выше 1,3.

К сожалению, в России применение энергосберегающих технологий на практике не является решающим фактором по причине относительно невысокой стоимости электроэнергии и достаточного количества природных ресурсов. В большинстве случаев заказчик обращает внимание на цену ИБП, а не на его энергоэффективность или тем более экологичность.

В то же время, как утверждает Андрей Вотановский, технический специалист по системам бесперебойного питания переменного тока Emerson Network Power, использование энергоэффективных систем сегодня влияет на имидж компании – фактор, который нельзя сбрасывать со счетов в условиях современного высококонкурентного рынка. Кроме того, применяя «зеленые» технологии, потребитель получит выгоду в будущем, а компании, которые сегодня не думают о будущем, завтра рискуют оказаться в прошлом.

«Зеленые» наблюдатели

Поскольку «зеленые» технологии превратились в модный тренд, возросла и роль независимых организаций, которые способны подтвердить экологичность и энергоэффективность того или иного изделия. Такие наблюдательные структуры пока что созданы только в США и наиболее развитых странах Европы. Пожалуй, наиболее значительной из них можно считать некоммерческую ассоциацию GreenGrid, которая разработала универсальную метрику энергоэффективности PUE. Это показатель эффективности всех инженерных систем, используемых в вычислительном центре.

Хотя ИБП не внесены в директиву Европейского сообщества RoHS (2002/95/EC «Ограничение использования некоторых вредных веществ в электронных устройствах»), некоторые производители, в частности Eaton и Chloride (в составе Emerson Network Power), на добровольной основе принимают меры к исключению веществ, перечисленных в этой директиве, из процесса производства ИБП. Кроме того, существует рекомендательная директива WEEE (2002/96/EEC «Отходы электрического и электронного оборудования»), в которой определены стандарты, относящиеся к сбору и переработке отходов от производства ИБП. Разработкой экологических стандартов и рекомендаций в сфере ИБП занимается, в числе прочих задач, и Европейский комитет производителей электрооборудования и силовой электроники (CEMEP).

В данном аспекте интересен опыт компании Chloride, установившей на основных производственных объектах систему тестирования «с нулевыми отходами», которая обеспечивает рециркуляцию всей электроэнергии, используемой в процессе тестирования оборудования, усиливая экологичность производства ИБП. Есть еще так называемый «Кодекс поведения» по системам бесперебойного питания – документ, подготовленный Европейской комиссией для разработчиков и производителей соответствующего оборудования. Он направлен на существенное сокращение потребления энергии при одновременном достижении максимального КПД систем бесперебойного питания.

Существуют и фирменные стандарты компаний; в частности, APC by Schneider Electric самостоятельно разработала систему оценки эффективности инфраструктуры ЦОДа – Data Center Infrastructure Efficiency (DCiE), которая активно используется в отрасли.

В погоне за КПД

Все производители ИБП стремятся предложить заказчику систему, которая имела бы наиболее высокий КПД, обеспечивая при этом качественное электропитание, надежность и приемлемую цену. Для сочетания всех этих факторов в одном устройстве используются специальные технологии и фирменные разработки. Все ведущие производители, заявляя об энергоэффективности и экологичности своих решений, как правило, имеют в виду, что их ИБП поддерживают особый, экономичный режим работы («экорежим»). Суть его

заключается в том, что питание оборудования происходит через статический байпас, без двойного преобразования, но если параметры входного напряжения превышают допустимые пределы, система немедленно переходит в режим двойного преобразования. При этом достигаются наиболее высокие показатели КПД – до 99%. Опасность такого подхода состоит в том, что в случае резкого скачка сетевого напряжения всплеск в любом случае пройдет на оборудование – ИБП физически не успеет перейти в режим двойного преобразования. Поэтому «чистый» экорежим рекомендуется только в том случае, если основная электрическая сеть стабильна и высоконадежна.

Однако здесь возможен компромисс: известные мировые производители предлагают специальные разработки, которые нивелируют эффект от скачков напряжения, при этом сохраняя КПД на уровне 96–98%. Это достигается, например, установкой пассивного сетевого фильтра на байпасе, который не пропустит всплески и провалы напряжения до момента перехода ИБП в режим двойного преобразования. Такой подход используется в ИБП Chloride Trinergy. Основная идея производителя заключается в следующем: зачем использовать преобразование из одного рода тока в другой и обратно, проигрывая в КПД, когда необходима лишь корректировка некоторых параметров сети?

Система Chloride Trinergy, способная работать в режимах, в которых не происходит постоянного двойного преобразования, самостоятельно может принимать решение о том, в каком режиме функционировать, в зависимости от состояния питающей сети и накопленной статистики. Для этой системы доступно три режима работы: VFI (максимальный контроль электропитания), VFD (максимальная энергоэффективность), VI (нечто среднее между двумя предыдущими), КПД которых достигает соответственно >95; 99 и 96–98%. ИБП Trinergy автоматически выбирает наиболее эффективный из них в зависимости от параметров электрической сети. По данным производителя, за счет комбинированного использования этих трех режимов в условиях ЦОДа можно достичь среднего показателя КПД почти в 98%.

У компании Emerson, которая в прошлом году приобрела Chloride и теперь имеет полное право позиционировать Trinergy как свое решение, есть и собственные разработки в сфере энергоэффективности, в частности система Liebert APM, представленная в 2010 г. Применение модульной архитектуры в совокупности с высокотехнологичной элементной базой и продуманной логикой управления позволило достичь высоких показателей энергоэффективности. Так, Liebert APM, обеспечивая максимальный КПД до 96% при двойном преобразовании, позволяет дополнительно оптимизировать энергопотребление за счет применения «спящего» режима для избыточных силовых модулей, с их последующей автоматической активацией, если потребуется дополнительная мощность. Вместе с тем практически все модели ИБП Emerson высокой мощности поддерживают работу в энергосберегающем режиме. Одним из примеров может служить Liebert Hipulse, где реализован режим Intelligent ECO Mode, позволяющий гибко и без вмешательства человека изменять режимы работы ИБП, увеличивая средний КПД системы до 98%.

Ключевая технология компании Eaton в сфере энергосбережения, позволяющая увеличить КПД ИБП до 99%, называется Energy Saver System (ESS). Благодаря специальным алгоритмам, реализующим технологию ESS, ИБП переходят в режим двойного преобразования только при реальной необходимости. В режиме двойного преобразования КПД таких моделей, как Eaton 9390 и Eaton 9395, составляет соответственно 94 и 94,5%. Кроме того, в ИБП Eaton имеется так называемая адаптивная система управления модулями (Variable Module Management System, VMMS), позволяющая системе бесперебойного питания автоматически определять, какие из силовых модулей (как в параллельных системах, так и в одиночных ИБП) могут работать в режиме ожидания, а какие будут использоваться для питания оборудования. В случае необходимости система задействует все силовые модули, а при низком уровне нагрузки (менее 40%) отключает резервные мощности, повышая общий КПД системы.

Похожим образом действуют и ИБП Socomec в режиме Energy Saver, когда работают только те ИБП, которые нужны для питания оборудования. Резервирование же обеспечивается тем, что дополнительный ИБП находится в режиме ожидания. Режим Energy Saver предназначен в первую очередь для комплексов, в которых потребляемая мощность часто изменяется. Он подходит для всех систем электропитания, содержащих не менее трех параллельно подключенных ИБП. Кроме того, ИБП Socomec поддерживают работу еще в двух режимах: Eco Mode и Always on, при этом максимальное значение КПД составляет более 98%.

Отметим, что энергоэффективный режим используется не только в ИБП корпоративного уровня. Так, все ИБП Powercom для сегмента SOHO поддерживают технологию Green Mode, которая может автоматически отключать ИБП в отсутствие нагрузки в случае работы от аккумулятора. Тем самым экономится как ресурс самого аккумулятора, так и электроэнергия при дальнейшей его подзарядке. Учитывая, что стоимость аккумулятора составляет около 20% цены всего ИБП, режим экономного энергопотребления позволяет снизить совокупную стоимость владения ИБП.

Система APC Symmetra PX, по заявлениям производителя, в нормальном режиме двойного преобразования обеспечивает КПД до 96–97%. Еще большей эффективности (до 98%) можно добиться в специальном экорежиме. Но, поскольку в этом случае оборудование подвергается опасности всплесков и провалов напряжения, использовать данный режим, особенно в условиях России, обычно не рекомендуется. Производитель делает

Уменьшение затрат на содержание ЦОД и снижение негативного воздействия на экологию.

Высокий КПД ИБП Eaton 9395 и уникальные технологии энергоэффективной архитектуры устройства позволяют значительно уменьшить расходы при эксплуатации ЦОД. Благодаря инновационному дизайну Eaton 9395 и использованию современных экологичных материалов, подлежащих вторичной переработке, снижается негативное воздействие на окружающую среду и расходы на последующую утилизацию. Компактные размеры и малый вес ИБП упрощают его транспортировку и инсталляцию.
Возможность фронтального подключения и обслуживания сводит к минимуму расходы на установку и экономит ценное пространство серверных комнат.

An Eaton Green Solution

EATON
Powering Business Worldwide

www.eaton.ru/ups

акцент на том, что реальной высокой эффективности удалось добиться даже при стандартной схеме двойного преобразования.

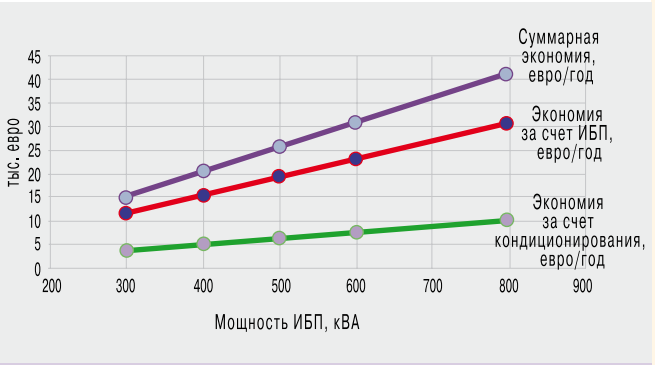
Немаловажную роль отводят производители интеллектуальным средствам управления системами электропитания. Ведь в сложной инженерной системе требуется согласованная работа отдельных компонентов – выпрямителей, зарядных устройств и т.д. Разработки в этом направлении в основном сконцентрированы вокруг «интеллектуальных» PDU (Power Distribution Unit). Такие системы позволяют централизованно контролировать энергопотребление, управлять электропитанием и вести мониторинг подключенного оборудования в большом количестве точек подключения, что повышает эффективность всей системы в целом. Такие решения сегодня предлагают APC by Schneider Electric, Eaton, Emerson, Rittal и другие.

Европейские инициативы и российские реалии

Все ведущие мировые производители реализуют в своих ИБП те или иные виды «зеленых» технологий, но распространение экологичных систем в значительной степени сдерживается экономическими факторами. Более высокая стоимость «зеленых» решений мешает им завоевать прочные позиции в российских проектах. При этом, как полагают эксперты, со временем вложения непременно окупятся, главным образом за счет экономии электроэнергии. Повышение КПД на несколько процентов, которое способен обеспечить экорежим, по оценкам европейских аналитиков, позволяет оправдать инвестиции в ИБП в течение 3–5 лет. Но пока цена электричества для потребителей остается на нынешнем уровне, российский заказчик в большинстве случаев не видит особой экономии, предпочитая более низкие первоначальные вложения.

Кроме того, имеет место недостаточная осведомленность потребителей как о самом режиме энергосбережения, так и об особенностях его применения, что снижает общую эффективность ИБП и не позволяет задействовать все его потенциальные возможности – такого мнения придерживается, в частности, директор корпоративного отдела Powercom Андрей Маркин.

Ежегодная экономия от применения режима ECO Mode на ИБП Liebert Hipulse 800 кВА в условиях Западной Европы



Источник: Emerson Network Power

В Западной Европе, откуда пришла к нам мода на «зеленые» технологии в ЦОДах, ситуация несколько иная. Стоимость электричества в разы выше, чем в России, и даже несколько дополнительных процентов КПД за год составляют солидные суммы. Это хорошо иллюстрирует расчет экономии, которую может дать экорежим ECO Mode на ИБП Liebert Hipulse в условиях западноевропейского ЦОДА (см. рисунок).

К тому же в Европе существуют ощутимые штрафы за расточительное потребление электроэнергии и, наоборот, финансовые выплаты или налоговые послабления, поощряющие использование энергосберегающих технологий. В России этот процесс только начинается, но первые шаги уже сделаны. К ним можно отнести, например, запрет мощных ламп накаливания. Возможно, последуют и другие, более ощутимые шаги, в том числе в сфере утилизации отработавшего оборудования.

Как бы то ни было, российские заказчики активно интересуются «зелеными» ИБП. По словам Анатолия Маслова, технического эксперта ООО «Клорайд Рус», некоторые заказчики начинают рассматривать варианты использования «зеленых» решений для крупных ЦОДов. Встречаются проекты, где вопрос энергоэффективности – один из главных. Выгоды потребителя в данном случае – экономия средств на эксплуатацию (снижается потребление электроэнергии) и страховка

на будущее от введения каких-либо нормативов энергоэффективности используемого оборудования. Однако потребительский сегмент пока что весьма невелик. Как полагает Наталья Маркина, советник главы российского представительства Socomec, основными потребителями «зеленых» ИБП в России являются прежде всего крупные ЦОДы, а также компании промышленного сектора – т. е. организации, способные ощутить эффект масштаба.

Использование энергосберегающих технологий однозначно снижает затраты на электроэнергию. Поэтому, как полагает Денис Андреев, руководитель департамента систем бесперебойного питания компании Landata, спрос на «зеленые» ИБП в России будет постепенно расти в соответствии с мировыми тенденциями. Но надо понимать, что их окупаемость будет ощутима минимум в среднесрочной перспективе, поскольку применение энергосберегающих технологий экономит 2–3% от общего потребления электроэнергии.

Применение подобных решений сейчас является одним из серьезных конкурентных преимуществ на рынке, но зачастую не основным. В странах с более высокой стоимостью электроэнергии «зеленые» технологии уже давно стали ключевым фактором при выборе ИБП, в то время как в России пользователи, особенно в корпоративном секторе, рассматривают всевозможные экорежимы лишь как дополнительное, но необязательное преимущество. Еще меньше внимания заказчики уделяют экологическим аспектам производства и утилизации ИБП. Но хочется думать, что ситуация постепенно изменится. ИКС

Электропитание в ЦОДах
Оценка возможностей постоянного тока

М. МЁРИЛЛ, менеджер по развитию DC-программ в индустриальном сегменте Emerson Network Power Energy Systems
Б. Дж. ЗОННЕНБЕРГ, менеджер по коммерческому развитию Emerson Network Power Energy Systems

Сегодня в ЦОДах основное внимание уделяется надежному обеспечению большей вычислительной мощности при меньших расходах и энергопотреблении. Электропитание постоянным током – практичный и доступный способ снижения сложности инфраструктуры ЦОДа и повышения КПД без ухудшения его эксплуатационных характеристик.

В последнее десятилетие резко выросла потребность в ИТ-системах, в частности в вычислительном оборудовании и системах хранения данных. Многие организации увеличили производительность и количество установленных у них серверов. Это привело к резкому повышению энергопотребления центров обработки данных. В 2004–2009 гг. рост плотности мощности и температуры в ЦОДах стал одной из основных проблем менеджеров, так как они стремились увеличить плотность размещения оборудования в стойках на 400–1000%. Параллельно росла и стоимость электроэнергии. На эти вызовы отрасль ответила повышенным вниманием к энергоэффективности ЦОДов. И в отдельных аспектах был достигнут значительный прогресс. Тем не менее в целом система электропитания ЦОДов все еще нуждается в оптимизации. Дело в том, что владельцы ЦОДов должны тщательно взвешивать все варианты компромиссов между энергоэффективностью и эксплуатационной готовностью. Сталкиваясь с таким выбором, многие продолжают использовать проверенные подходы, которые хотя и не гарантируют максимального КПД, но обеспечивают высокую эксплуатационную готовность. Однако во многих случаях можно повысить КПД без риска снижения этого важнейшего для ЦОДов показателя.

Стандартные схемы распределения питания в ЦОДе

Наиболее широко используемые в Северной Америке системы распределения питания переменного тока (AC) обеспечивают подачу тока 480 В на ИБП, где он преобразуется в постоянный ток для зарядки аккумуляторов, а затем снова преобразуется в переменный и его напряжение понижается в системе распределения до 208 В для подачи на ИТ-оборудование. Система питания ИТ-оборудования преобразует ток обратно в постоянный, а затем понижает его напряжение для питания процессоров, памяти и накопителей данных (рис. 1).

Рис. 1. Стандартная конфигурация системы питания ЦОД 480 В AC на 208 В AC

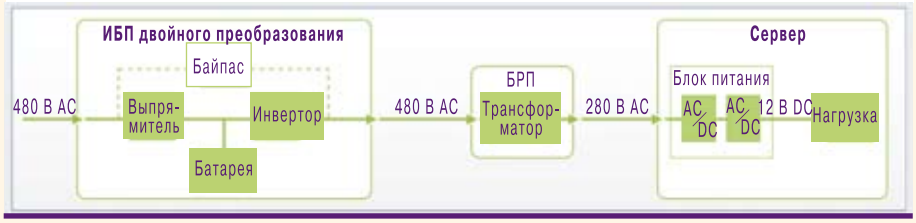


Рис. 2. В экономичном режиме поступающий ток не проходит через инвертор, увеличивая КПД системы ИБП

Когда ИБП переменного тока работает в экономичном режиме (рис. 2), его КПД повышается за счет шунтирования преобразования в инверторе. Однако это снижает надежность системы, так как критически важные нагрузки не будут изолированы от общей сети питания и колебаний напряжения, обычно сглаживаемых с помощью инвертора, а для обеспечения надежного перехода на последний требуются сложные цепи синхронизации. К тому же необходимо обеспечить быстрое включение инвертора в случае отключения питания и изолирование сети электропитания для предотвращения возникновения обратного тока в системе распределения. Независимо от скорости и надежности такого переключения риск его отказа в критический момент все равно существует.

В принципе схему распределения переменного тока можно упростить, устранив понижение в устройстве распределения и подавая ток более высокого напряжения (скажем, 277 В) с ИБП непосредственно на ИТ-оборудование (рис. 3). Однако этот подход в настоящее время по ряду причин не используется.

Во-первых, при подключении нагрузки «фаза-нейтраль» могут возникнуть дополнительные гармонические токи, которые частично нивелируют повышение КПД. Во-вторых, из-за более высокого напряжения в стойке могут возникнуть дуговые разряды, опасные для персонала, который выполняет в ней какие-либо работы. В-третьих, в настоящее время на рынке нет источников электропитания, которые могли бы обеспечить входное питание такого уровня. Таким образом, эта схема нуждается в дальнейшей проработке, прежде чем ее можно будет использовать на практике.

Поэтому наиболее реальной альтернативой распределению питания 480/208 В AC для организаций, которые стремятся оптимизировать надежность и КПД своих ЦОДов, сегодня оказывается питание постоянным током (DC) 48 В.

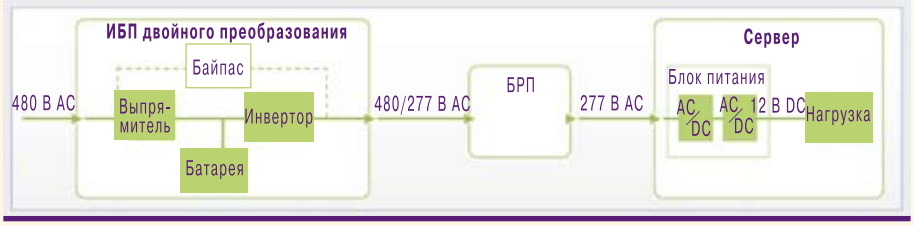
Практика организации питания ЦОДа постоянным током

В большинстве установок система питания –48 В DC состоит из трех элементов:

- модульной системы питания 480 В AC/ –48 В DC;
- аккумуляторных блоков для резервного питания (не менее 8 часов);
- шкафов распределения нагрузки.

Эти элементы соединены с медными шинами и проводами большого сечения, которые связывают различные участки предприятия для распределения питания –48 В на конечную нагрузку. Блоки питания понижают напряжение до 12 В DC и ниже для питания внутренних компонентов (рис. 4).

Рис. 3. Конфигурация системы питания ЦОДа 480/277 В AC



Применительно к ЦОДам преимущества такого подхода очевидны. После выпрямителей AC/DC питание полностью изолировано от внешней элект-

Историческая справка

Питание постоянным током 48 В давно применяется в телекоммуникациях. Оно отличается сравнительной простотой и надежностью, и ток в нем между сетью питания и конечной нагрузкой проходит малое количество стадий преобразования. Питание 48 В DC стало стандартом еще во времена Александра Белла. Аргументы в пользу этого были таковы. Постоянный ток, как тогда считалось, надежней переменного, поскольку его можно подавать с аккумуляторов резервного питания во время перебоев в питающей сети. А напряжение –48 В – оптимальный компромисс между эффективностью передачи тока на расстояние и безопасностью для человека, так как оно не представляет опасности при случайном касании токоведущих элементов.

Сегодня на АТС все еще используется питание –48 В DC, которое в нормальном режиме работы для обеспечения правильной зарядки резервных аккумуляторов фактически составляет от –52 до –54 В. Эти системы имеют очень высокую степень эксплуатационной готовности: согласно анализу 23 тыс. систем питания постоянного тока, производившемуся в течение 10 лет на предприятиях NTT, она достигает 99,9999999%*.

*Значение подтверждено расчетами.

росети и отличается «безопасным уровнем низкого напряжения» согласно IEC/UL 60950 и, следовательно, может обслуживаться во включенном состоянии обученным персоналом. Нет необходимости понижать мощность для баланса фаз или гармоник, которые отсутствуют в питании постоянным током. Кроме того, повышается безопасность персонала при обслуживании оборудования в стойке ввиду отсутствия дуговых разрядов при напряжении –48 В.

Но в ЦОДах, в отличие от АТС, отсутствуют мощные медные шины для распределения питания DC на стойки. К счастью, новая рядная топология ЦОДов не требует использования таких медных шин (рис. 5). В этой рядной конфигурации ток преобразуется из переменного в постоянный рядом с конечной нагрузкой, что снижает требования к сечению проводника из-за его малой длины.

Рис. 4. Стандартная компоновка элементов цепочки питания –48 В

Факторы, влияющие на выбор системы распределения питания

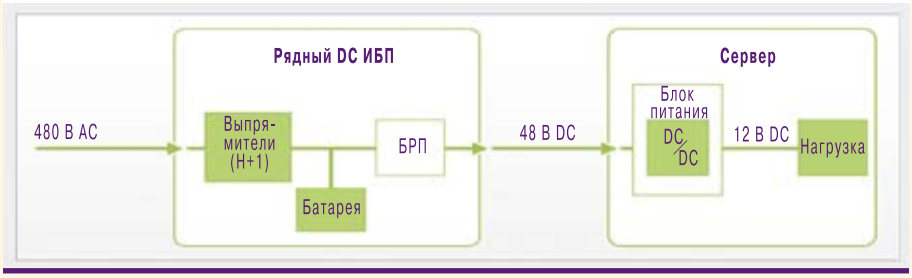
При выборе оптимальной архитектуры питания ЦОДа необходимо учесть ряд факторов. Понимание степени влияния каждого фактора – ключевой момент для принятия взвешенного решения.

КПД

Точный расчет общей энергоэффективности системы может оказаться трудной задачей из-за сложности и многообразия влияющих на нее факторов: требуемого уровня резервирования, наличия или отсутствия гармонических колебаний, вариаций нагрузки, а также дополнительных энергозатрат на охлаждение. Тем не менее такой расчет полезен для предварительной оценки КПД с учетом конкретных условий эксплуатации оборудования. Как показывает анализ, там, где эти факторы действуют, разрыв между эффективностью систем постоянного и переменного тока будет, скорее всего, более существенным.

- **Резервирование.** Уровень резервирования в системе распределения питания может влиять и на эксплуатационную готовность, и на КПД. Причем в системе распределении питания переменного тока более высокий уровень резервирования повышает эксплуатационную готовность, но снижает КПД всей системы. Максимальная эксплуатационная готовность достигается при резервировании по схеме 2N, когда каждый блок ИБП работает с нагрузкой не более 50%. Однако поскольку загрузка ЦОДа редко достигает пикового уровня, то резервирующие системы почти всегда функционируют с мощностью менее 50%. Таким образом, при работе одного ИБП максимальная мощность может приближаться к 40%, а в условиях нормальной эксплуатации каждый блок может быть нагружен на 20% и менее. У большей части оборудования кривые КПД сильно спадают при загрузке менее 30%, из-за чего фактический КПД оказывается значительно ниже того уровня, который достигается в идеальных условиях. В системах питания постоянного тока резервирование может быть полностью интегрировано в ИБП DC. Кроме того, в лучших системах DC-питания имеется функция оптимизации КПД, которая сохраняет пиковый КПД даже при загрузке системы всего в 5%, что позволяет одновременно обеспечить и высокий КПД, и высокую эксплуатационную готовность в реальных условиях.
- **Гармонические колебания.** Это искажения синусоидальной формы переменного тока при нелинейных нагрузках. В ЦОДах блоки питания серверов представляют собой нелинейную

Рис. 5. Рядный ИБП DC не требует длинных медных проводников, которые ранее ограничивали применение постоянного тока в ЦОДах



нагрузку, которая может стать причиной возникновения гармонических колебаний. Гармонические колебания накапливаются в нейтральном проводе, вызывая потери мощности при распределении и излишний нагрев системы. Если кумулятивный уровень гармонических колебаний (называемый также полным коэффициентом гармонических искажений) становится слишком высоким, это может привести к повреждению чувствительного электронного оборудования и потребовать снижения потребляемой мощности оборудования. В сложных распределительных системах переменного тока такие потери нелегко спрогнозировать, но их влияние может оказаться сильным.

В системах питания постоянного тока гармонические колебания отсутствуют по определению.

- **Колебания загрузки ЦОДа.** Многие ЦОДы большую часть времени работают при загрузке значительно ниже 100%. Кроме того, эта загрузка часто изменяется в реальном времени, что усложняет моделирование КПД. Так как серверы включаются, выключаются и используются с различной частотой, нагрузка на каждую фазу трехфазной системы питания меняется непредсказуемо, и это затрудняет согласование нагрузки между фазами. Несбалансированные нагрузки снижают общий КПД системы и вызывают образование дополнительного тепла. Кроме того, отслеживание базовых нагрузок по каждой фазе в заданный промежуток времени – непростая задача, требующая специальных инструментов.

  Опять же, проблемы с балансом нагрузок относятся только к трехфазному питанию переменным током, при использовании постоянного тока их нет.

- **Тепловые нагрузки, связанные с питанием.** Вторым крупнейшим потребителем энергии в ЦОДе после собственно ИТ-оборудования является система охлаждения. Охлаждение требуется для нейтрализации тепла, выделяемого ИТ-оборудованием, а также тепла, возникающего при работе преобразователей. Так как в системе постоянного тока выполняется меньше преобразований, а ее КПД выше, она производит меньше тепла, чем система переменного тока, что дает ощутимую экономию электроэнергии. Согласно приближенным подсчетам, уменьшение тепловыделения на 1 Вт позволяет сэкономить примерно 1,4–2 Вт при охлаждении.

Эксплуатационная готовность

Высокую эксплуатационную готовность могут обеспечивать системы питания и переменного, и постоянного тока. Максимальная эксплуатационная готовность, как уже отмечалось, обеспечивается при резервировании 2N, поскольку оно позволяет использовать архитектуру с двумя шинами, что исключает простои оборудования из-за отказов в цепи распределения энергии. Однако такая эксплуатационная готовность достигается как за счет установленного в системе оборудования, так и за счет снижения рабочего КПД системы. Многие организации достигают требуемого уровня эксплуатационной готовности с резервированием N +1, где резервирование обеспечивается на уровне блока.

На уровне блока повышению эксплуатационной готовности в системе питания постоянного тока способствуют два фактора. Во-первых, DC-система преобразования питания включает в себя меньше компонентов, чем сопоставимая AC-система, что увеличивает среднее время безотказной работы. Во-вторых, ИБП DC использует сеть дискретных выпрямителей для требуемого изолированного питания шины системы распределения. Эти выпрямители компенсируют отказ отдельного выпрямителя, давая возможность какое-то время работать без ущерба для производительности и мощности. Отдельные выпрямители могут быть безопасно заменены на работающем оборудовании в рабочих условиях, не влияя на работу системы. Таким образом, минимизируется среднее время ремонта системы, которое вносит основной вклад в показатель эксплуатационной готовности.

Масштабируемость

Система электропитания может стать фактором, ограничивающим установку дополнительного оборудования. Поэтому при создании и расширении ЦОДов все большую популярность приобретает модульный подход.

Если вся инфраструктура питания и охлаждения ЦОДа интегрирована в полностью замкнутый блок, то она может быть доставлена на место эксплуатации и быстро встроена в имеющиеся системы питания, связи и охлаждения, позволяя нарастить вычислительные мощности. Благодаря встроенным функциям резервирования и компактности ИБП DC хорошо подходят для такого применения.

Та же идея заложена в рядном расположении оборудования, дающем возможность поблочно расширять существующие мощности. Системы пи-

тания как переменного, так и постоянного тока обеспечивают масштабируемость рядного оборудования, но ИБП DC обладают преимуществом по резервированию и занимают как минимум на 50% меньше площади, чем аналогичная рядная AC-система.

Стоимость

Основная задача системы питания критически важных нагрузок – недопущение простоев оборудования из-за перебоев питания. Поэтому любое сравнение стоимости должно учитывать требуемый уровень эксплуатационной готовности и стоимость времени простоя. В целом рядные системы питания постоянного тока требуют меньше затрат на установку, эксплуатацию и техническое обслуживание, чем аналогичные AC-системы, и поддерживают уровень резервирования не менее N + 1. Экономический эффект может быть несколько размыт за счет стоимости ИТ-оборудования в DC-системе, так как стоимость серверов с источниками питания постоянного тока может быть на 10% выше, чем стоимость более распространенных серверов с AC-питанием. Но цена оборудования постоянного тока должна снизиться, когда эта технология получит более широкое распространение. В зависимости от многих факторов экономия, обеспечиваемая комплексной архитектурой питания на основе постоянного тока в сравнении с AC-системами, может достигать 20%.

■ ■ ■

В настоящее время питание всех критически важных нагрузок осуществляется постоянным током, блоки резервного питания также запитываются постоянным током. В сетях электропитания используется переменный ток. И оснований ожидать изменения этого положения в ближайшей перспективе нет. Соответственно возникает вопрос: где находится точка преобразования AC-питания из сети в DC-питание для современного электронного оборудования, оптимальная как с точки зрения энергоэффективности, так и защиты от перебоев электропитания? При слишком раннем преобразовании постоянный ток необходимо передавать на дальние расстояния, что требует проводников большого сечения для сокращения потерь. При слишком позднем преобразовании в процесс приходится вводить дополнительные ступени преобразования, что негативно влияет на КПД, надежность и уровень расходов.

Во многих областях применения оптимальная точка преобразования и хранения энергии должна находиться как можно ближе к нагрузке. В условиях ЦОДа ИБП на 48 В DC, устанавливаемые в ряд с серверными стойками, обеспечат наилучшие показатели КПД, надежности и гибкости. ИКС

Работа систем охлаждения в экстремальных погодных условиях

Эксплуатация систем охлаждения в тяжелых условиях лета-2010 дала инженерам ЦОДов бесценный опыт и показала эффективность некоторых практических приемов.

Сергей ЛЕБЕДЕВ, директор сервисного центра компании «ДатаДом»

Евгений КОЛПАЩИКОВ, ведущий инженер по холодильному оборудованию компании «ДатаДом»

Зачастую один из первых вопросов заказчика при выборе дата-центра: по какому принципу построена система охлаждения в ЦОДе? На сегодняшний день в московском регионе чаще всего встречаются два типа решений: на базе DX-кондиционеров (Direct eXpansion – прямое расширение) и построенные по схеме «чиллер – фанкойл» на основе CW-архитектуры (Chilled Water – охлажденная вода). Эти решения хорошо известны, у каждого есть свои преимущества и недостатки.

Выбор той или иной системы делается на этапе строительства и, как правило, зависит от конструктивных особенностей площадей, на которых планируется строить дата-центр, и от финансовых возможностей заказчика. Так, если нет свободной прилегающей территории для установки холодильных машин (чиллеров), то обычно принимается решение в пользу DX-кондиционеров с размещением выносных блоков на крыше (если нет, конечно, других ограничений, например по длине трассы). У чиллерных систем, в отличие от фреоновых кондиционе-

ров, длина трассы между чиллером и фанкойлом (внутренний блок кондиционера) может быть произвольной и ограничивается только мощностью насоса или насосной станции. Стоит также отметить, что система охлаждения на DX-кондиционерах дешевле, чем система чиллер – фанкойл, особенно если учесть необходимость резервирования инженерной инфраструктуры в ЦОДе. Необходимо предусмотреть установку дополнительной холодильной машины на случай ремонта или профилактических работ на основной (или основных) машинах. Все это приводит к существенному удорожанию систем охлаждения CW-архитектуры.

Но в рамках этой статьи мы не будем сравнивать эффективность работы систем охлаждения, построенных по разных моделям, а поговорим о практических задачах, с которыми сталкиваются инженеры при эксплуатации той и другой системы.

Система охлаждения, наряду с системой электропитания, требует постоянного внимания. Наши специалисты на протяжении нескольких лет обслуживают инженерные системы различных дата-центров: от крупных коммерческих (мощностью до 4 МВт) до относительно небольших, принадлежащих банковским структурам (мощностью до 400 кВт). За это время накоплен практический опыт в области эксплуатации систем кондиционирования, в том числе в критических для системы охлаждения ситуациях. Это, в частности, работа климатического оборудования в экстремальных погодных условиях.

При расчете систем кондиционирования берутся значения абсолютной минимальной и максимальной температуры воздуха для данной местности. Для московского региона это –42°С зимой и +37°С летом

Какие условия считать экстремальными?

Прежде всего, чтобы избежать непонимания, поясним, что мы подразумеваем под «экстремальными погодными условиями». Этим термином мы будем обозначать выход температурных параметров окружающей среды за верхнюю или нижнюю границу диапазона, в котором производитель гарантирует работу холодильного оборудования. Поясним на примере: если внешний конденсаторный блок DX-кондиционера рассчитан на температуру наружного воздуха от –30 до +30°С, то экстремальные погодные условия для данного кондиционера будут –30 и ниже или от +30 и выше. Если внешний конденсаторный блок рассчитан на работу в диапазоне от –30 до +35°С, то уличная температура в +30°С для него уже не является экстремальной – кондиционер должен работать.

Поскольку основная идея, лежащая в основе создания ЦОДов, – это обеспечение непрерывности работы клиентского оборудования, то уже при выборе системы охлаждения критически важно правильно указать расчетные параметры наружного воздуха. Ответ очевидный: чем шире диапазон, тем лучше. Но, как обычно, наши желания вступают в противоречие с нашими возможностями: оборудование с широким рабочим температурным диапазоном стоит дороже. Приходится идти на компромиссы, принимать на себя повышенные риски и т. д. В результате мы получаем, что несколько дней (недель) в году оборудование работает на пределе своих возможностей или даже за их пределом – в экстремальных погодных условиях.

Для каждого региона расчетные температурные параметры наружного воздуха можно взять в справочнике (СНиП 23-01-99 «Строительная климатология»). С учетом работы ЦОДа в режиме 24x7x365 при расчете систем кондиционирования берутся значения абсолютной минимальной и абсолютной максимальной температуры воздуха для данной географической местности. Для московского региона это –42°С зимой и +37°С летом.

Но даже если мы строго выдержали рекомендации справочника и правильно подобрали климатическое оборудование, это все же не дает 100%-ной гарантии спокойного существования. Справочник оперирует статистическими данными, исходя из того, что уже когда-то было. А что еще будет – неизвестно. Наглядный пример – лето 2010 г., когда температура переваливала за отметку в 37°С. Тем не менее мы рекомендуем при подборе климатического оборудования придерживаться данного СНиПа.

Эффективные приемы

Предположим, что у нас идеально построена система охлаждения ЦОДа. Это означает, что:

- рассчитаны мощности тепловыделения от оборудования;
- оборудование правильно подобрано по температурным параметрам согласно СНиПу;
- учтен необходимый резерв;
- составлен проект;
- монтаж оборудования выполнен квалифицированными специалистами с учетом рекомендаций завода-изготовителя;
- выполнены пусконаладочные работы;
- регулярно проводятся работы по техническому обслуживанию.

В таком случае вероятность стабильной и долгой работы климатического оборудования достаточно высока. Это в теории. Практика показала, что и в зимний, и в летний период есть много нюансов в работе даже таких «идеальных» систем, не говоря уже о достаточно типичной ситуации, когда климатическое оборудование с явно недостаточными характеристиками уже установлено. И что делать? Как минимизировать влияние экстремальных погодных условий?

Для начала рассмотрим летний период – лето нам сейчас ближе в буквальном смысле слова. Еще свежи

воспоминания лета 2010-го с его каждодневными температурными рекордами и ураганным ветром. Холодильное оборудование работало в экстремальных погодных условиях так часто, что фактически аварийная ситуация по перегреву уже не считалась чем-то особенным, стала восприниматься как штатная, как рутинная работа. Перед инженерами стояла задача не просто пережить один-два дня жаркой погоды, а сделать так, чтобы и сейчас, и завтра, и через неделю была обеспечена непрерывная работа холодильных машин в условиях длительной рекордно жаркой погоды.

Что можно сделать, допустим, для холодильной машины, рассчитанной на работу при температуре окружающего воздуха не выше +35°С, и, к примеру, для выносного блока фреонового DX-кондиционера, рассчитанного на температуру не выше +33°С? Рецепты «счастья» в обеих ситуациях примерно одинаковы.

Убрать все лишнее. Во-первых, лучше сразу начать с исправления ошибок, которые были допущены при проектировании или при строительстве/монтаже холодильной системы: расчистить площадь перед теплообменниками, чтобы по максимуму обеспечить свободный доступ воздуха к холодильному оборудованию и тем самым убрать эффект «теплового мешка». Температура конденсации фреона находится в диапазоне 45–55°С (мы, конечно, берем на себя большую смелость указывать температуру конденсации, не назвав ни давление конденсации, ни тип газа, но суть не в этом; все фреоны в физическом смысле ведут себя одинаково: чтобы перевести их из газообразного состояния в жидкое, их нужно сжать и охладить). Итак, если у нас оборудование зажато внешними строениями, коробками, другими предметами, то при отсутствии ветра часть отработанного воздуха (уже подогретого теплообменником холодильной машины с уличных 35 до 40°С и выше) захватывается вентиляторами и снова прогоняется через холодильную машину. В результате эффективность охлаждения самой машины резко снижается и холодопроизводительность ее падает. Поэтому надо обеспечить максимальный доступ свежего воздуха к машине.

Можно рассмотреть идею снятия защитных решеток с конденсаторных блоков. С одной стороны, решетки защищают оборудование от попадания посторонних предметов, но с другой – препятствуют продуву машины свежим воздухом. А когда борьба идет за каждый градус, мелочей уже не бывает.

Уменьшить локальный нагрев. Известно, что само солнце воздух практически не нагревает: солнце нагревает предметы (землю, асфальт, песок, воду и т.д.), а уж затем от них нагревается воздух. Так, температура асфальта летом в Москве легко может превышать 55°С, а температура газона в то же самое время будет около 30°С. Отсюда следует простой вывод: асфальтовое покрытие или черный гудрон – отнюдь не лучшее основание для размещения холодильного оборудования. Имеет смысл покрасить поверхность в белый цвет, насыпать щебенки, а еще лучше – посадить газонную траву, если есть такая возможность. Очень часто подобные задачи решают следующим способом: на предприятиях, где есть «дармовая» вода, под внешние блоки кондиционеров в жаркие дни на целый день включают воду, и она так и льется: по крыше, по стоку, в «ливневку» и далее на улицу. Так снимается локальный нагрев крыши, плюс увеличивается влажность воздуха, что также играет положительную роль при отводе тепла.

Проверить настройки. Необходимо проверить настройки каждого холодильного контура климатического оборудования: лучше придерживаться настроек, при которых оборудование работает максимально стабильно, без срывов в аварию по высокому давлению. Здесь основная задача – не допустить нестабильной работы компрессоров, их частого включения/выключения. При такой работе рывками есть риск просто «загнать» оборудование, и оно очень быстро выйдет из строя (надо ли говорить, что сломается оно в самый неподходящий момент?). В случае чиллера, кроме настроек работы компрессоров, необходимо подобрать оптимальный температурный баланс по входу/выходу воды (гликоля) из холодильной установки. Для этого можно аккуратно поднять температурную уставку по выходу на несколько градусов. Согласно справочнику «Система вентиляции и кондиционирования. Теория и практика» (в редакции от 2008 г.) при повышении температуры воды на выходе из чиллера на 1 градус холодопроизводительность машины увеличивается на 3%. Согласитесь, это неплохо. Но надо понимать, что повышение температуры воды — весьма ограниченный ресурс, так как холодильная машина проектируется на заводе под определенную температурную «вилку». Это, как правило, 12°С на вход чиллера и 7°С на выход, и нужно, не выходя за эти границы, подобрать температуру, при которой оборудование будет работать наиболее устойчиво.

Асфальтовое покрытие или черный гудрон – отнюдь не лучшее основание для размещения холодильного оборудования.

Очистить установку. Холодильное оборудование любит чистоту. Если конденсаторные блоки загрязнены, на них лежит слой грязи, перья, пушинки одуванчиков или плотное одеяло из тополиного пуха, можно даже не беспокоиться по поводу экстремальных погодных условий: оборудование перестанет работать гораздо раньше. Бесконтактная мойка (в том числе с «химией»), сухая чистка, чистка пылесосом должны проводиться в обязательном порядке

и на регулярной основе. Разница между работой оборудования с чистыми конденсаторными блоками и с грязными колоссальна. Во многих ситуациях хорошо выполненная чистка блоков решает проблемы жарких дней. Поэтому первым этапом подготовки климатического оборудования к жаркой погоде должна быть чистка, а лучше мойка конденсаторных блоков, причем мойка из аппарата высокого давления, с химией и – при необходимости – со снятием вентиляторов с холодильной машины для лучшего доступа к теплообменникам.

Рискованные меры

Если вышеуказанные мероприятия не помогли, и чувствуется, что кондиционеры (чиллеры) работают на грани возможностей и в любой момент готовы сорваться, можно попробовать еще несколько способов облегчить им жизнь. Но только к этим способам нужно относиться с осторожностью, учитывая некоторые нюансы. Как пишут в аннотациях к лекарствам: применять, если ожидаемая польза превышает потенциальный риск.

Во-первых, как ни удивительно это звучит, можно повысить температуру в модуле (в машзале, в гермозоне, словом, в помещении, где установлены сами стойки). До разумных пределов – например, до 25°C в холодном коридоре. Задача системы холодоснабжения в дата-центре – снимать теплопритоки. Если в помещение поступает неохлажденный уличный воздух из системы вентиляции или через входную дверь, то в модуль попадает теплый воздух, который тоже необходимо охлаждать. Получается, что система не только снимает теплопритоки в модуле, но и охлаждает улицу, а это совершенно лишнее. Надо снизить разницу между температурой в здании дата-центра и температурой в модуле, тогда на устранение поступающего извне тепла будет затрачиваться меньше энергии.

Холодильное оборудование любит чистоту. Если конденсаторные блоки загрязнены, можно даже не беспокоиться по поводу экстремальных погодных условий: оборудование перестанет работать гораздо раньше

Но надо понимать, что, повышая температуру в модуле, мы тем самым сужаем время реагирования на возможные проблемы в системе кондиционирования. В этом случае начальная точка отсчета температуры в модуле – не +21°C, а +25. И кратковременная остановка холодильной машины может привести к печальным последствиям, так как инерционность модуля по холоду мы практически свели на нет. Кстати, свойства инерционности модуля с температурной точки зрения мы успешно использовали прошлым летом во многих ЦОДах: ночью, когда не так жарко, принудительно охлаждали помещение до +18°C, а затем днем постепенно стравливали до +25°C, что помогало нам пережить особенно жаркие часы.

Многие наши коллеги, чтобы холодильное оборудование хоть как-то работало, поливают конденсаторные блоки из шланга водой: вот так с утра и до самого вечера непрерывно льют на них воду. Такой способ охлаждения имеет право на жизнь, но эффективность его не очень высока. Как известно из курса физики, теплоемкость воды равна 4,2 кДж/(кг·К), а удельная теплота ее испарения – 2500 кДж/кг. Очевидно, что если мы хотим отвести с помощью воды как можно больше тепла, то лучше воду испарять. Отсюда простой вывод: гораздо эффективнее не поливать конденсаторные блоки из шланга, а распылять воду в непосредственной близости от них. Так и расход воды меньше, и эффективность охлаждения выше. На одном из объектов мы собрали небольшую систему орошения на базе форсунок мелкодисперсионного распыления воды и с ее помощью добились образования устойчивого «тумана». Когда мы запустили систему в работу, результаты нас приятно удивили: с помощью системы орошения мы смогли локально понизить температуру окружающего воздуха на 8°C! На целых 8 градусов! Это, конечно, прекрасный результат.

С помощью системы орошения мы смогли существенно «отодвинуть» зону экстремальных температур и обеспечить стабильный режим работы холодильного оборудования. Но этот способ не панацея. При длительном использовании системы орошения на конденсаторных блоках образуется известковый налет: сначала теплообменники белеют, затем пластины оребрения покрываются твердой коркой солей кальция, которую потом очень трудно удалить. В итоге, постоянно распыляя воду, мы ухудшаем теплообмен, сами себе создаем проблемы в дальнейшей эксплуатации. Чтобы уменьшить налет, мы проводили водоподготовку, пропускали воду через фильтры, но полностью избавиться от известкового налета не получилось.

Зимой – свои проблемы

Несколько слов о зимнем периоде эксплуатации холодильного оборудования. Прошедшая зима не отличалась рекордами, в Москве не было тридцатиградусных морозов, зато случилось такое редкое явление, как ледяной дождь. Это явление опасно для выносных конденсаторных блоков кондиционеров, которые установлены параллельно земной поверхности – на выдув вверх. Если такой блок не работал во время ледяного дождя, то на нем могла образоваться замечательная ледяная «шуба», которая механически блокировала вращение вентилятора, и это могло привести к его поломке. Перед запуском такого кондиционера необходимо было очистить ото льда вентилятор внешнего блока. Мы размораживали такие внешние блоки теплой водой. Надо заметить, что при несильном намерзании льда внешний блок может сам разморозиться горячим фреоном. Для чиллер-

ных систем, работающих в режиме фрикулинга, особое внимание стоит обратить на сальники насосов. Если насосная группа установлена на улице, то сальниковое уплотнение должно быть рассчитано на работу в условиях сильных морозов, иначе они просто потекут.

■ ■ ■

Эксплуатация систем охлаждения больших промышленных объектов, таких как ЦОДы, включает в себя как техническое обслуживание силами собственных инженеров на объекте, так и обслуживание с привлечением специалистов сервисных компаний. Обслуживание на регулярной основе с соблюдением графиков планово-профилактического ремонта минимизирует вероятность аварий оборудования. Надо стремиться к тому, чтобы инженеры службы эксплуатации могли предвидеть возможные аварийные ситуации и были к ним готовы. Еще лучше – чтобы они могли устранить причину возможной аварии. А это достигается с опытом, через шишки и подзатыльники, каждодневной работой. По другому – никак. ИКС

Установки пожаротушения для ЦОДов

Проблема пожара для ЦОДов более чем реальна, и единственно возможное решение проблемы – системы газового пожаротушения. Существуют разные их типы, со своими особенностями.

Павел ИВАНОВ,
ведущий инженер
ООО «Пожтехника»

По мере роста бизнеса растет и объем используемой им информации, и в какой-то момент приходит время консолидировать обработку данных и централизованно управлять ИТ-инфраструктурой и информационными системами. Для этого нужен центр обработки данных (ЦОД). В первую очередь ЦОДы необходимы компаниям, для которых критичны высокая степень готовности, отказоустойчивость, надежность информационных систем. Это крупные компании, эксплуатирующие сложные бизнес-приложения (ERP-, CRM-системы и т.д.), операторы связи, банки, страховые компании.

Основные составляющие инфраструктуры ЦОДа – информационная, телекоммуникационная и инженерная инфраструктура. Первые две оставим профессионалам в области ИТ, а мы поговорим об инженерной составляющей, в частности об установках газового пожаротушения.

Итак, проблема возгорания в ЦОДах реально существует и единственное возможное решение – это система газового пожаротушения. Водяные, порошковые, пенные установки нет смысла рассматривать, поскольку ущерб для ЦОДа от таких установок сопоставим с ущербом от пожара.

Применительно к ЦОДам существуют два варианта газового пожаротушения. Наиболее распространенный способ – **объемное газовое пожаротушение.** В этом случае газом заполняется весь объем помещения. Второй способ – **газовое пожаротушение отдельных стоек**. Это компактное решение, при котором тушится только стойка, но в таком варианте стойки должны быть герметичными. В данной статье мы рассмотрим только объемное газовое пожаротушение.

Пожары в ЦОДах – это реальность

27 марта 2010 г. случился пожар в Одессе, в ЦОДе, расположенном в бизнес-центре «Фабрика Бизнеса». Именно там на втором этаже находится дата-центр одного из крупных хостинг-провайдеров Украины. Установка пожаротушения не сработала. Пожарные, прибывшие на место происшествия, не имели газовых огнетушащих веществ. В результате серверы пострадали и от огня, и от воды. В ЦОДе при тушении выбиты окна. Ущерб, нанесенный пожаром, исчисляется миллионами долларов.

30 мая 2008 г. из-за короткого замыкания произошёл пожар в ЦОДе The Planet (Хьюстон, шт. Техас, США). Огонь не дошел до серверов, где хранятся данные клиентов, но из-за него было прервано энергоснабжение. В общей сложности пострадало 9 тыс. серверов, где находились данные 7,5 тыс. клиентов провайдера. Но поскольку The Planet состоит из шести ЦОДов, после пожара данные клиентов частично переместили в другие ЦОДы.

Устройство установки пожаротушения

Любая установка газового пожаротушения состоит из двух частей: электротехнической и технологической.

Электротехническая часть (рис. 1) отвечает за своевременное обнаружение пожара, оповещение соответствующего персонала, а также за выдачу сигнала на запуск пожаротушения. В ее состав входят:

- прибор управления АУГПТ;
- пожарные извещатели;
- оповещатели;
- табло;
- клапан сброса избыточного давления;
- система раннего обнаружения дыма.

Рис. 1. Электротехническая часть установки газового пожаротушения

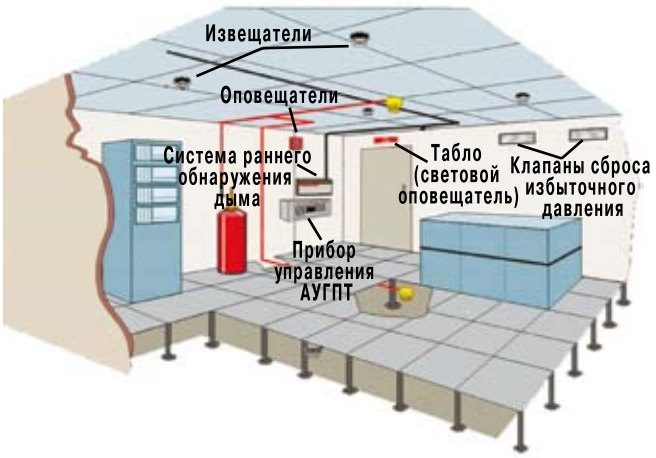
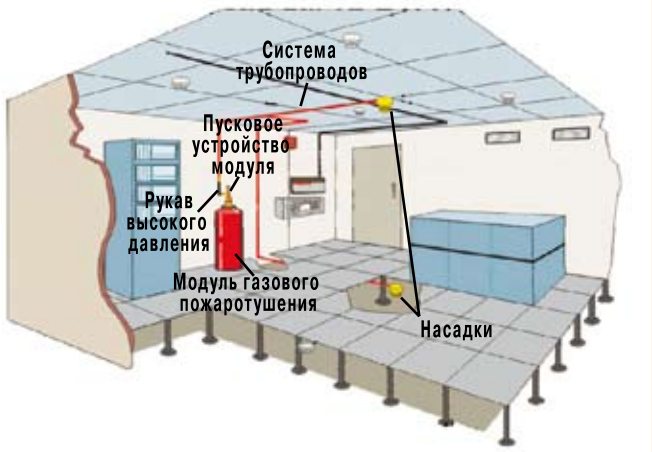


Рис. 2. Технологическая часть установки газового пожаротушения



Так как стоимость электротехнической части составляет не более 10% стоимости технологической, многие проектировщики и заказчики не очень ответственно относятся к выбору оборудования для нее. Но на самом деле газовое пожаротушение – это пожаротушение на ранней стадии. Поэтому к выбору пожарных извещателей и прибора управления нужно подойти со всей тщательностью.

В помещениях серверных и ЦОДов за счет работы систем кондиционирования и охлаждения формируются сильные потоки воздуха. Поэтому эффективность обычных точечных пожарных извещателей крайне мала. Любой дымовой извещатель работает как оптическое устройство: в дымовую камеру извещателя попадает дым, луч света отражается от него и попадает в приемник, вследствие чего происходит выдача сигнала «ПОЖАР». Иными словами, точечный дымовой извещатель «ждет», пока до него дойдет дым. Однако в условиях мощных потоков воздуха дым до него просто не доходит.

Решение этой проблемы – аспирационные извещатели. В них используется «активный» способ обнаружения, при котором не надо ждать, пока дым дойдет до отверстия. Такие извещатели состоят из системы ПВХ-трубопроводов с отверстиями, через которые происходит забор проб воздуха из помещения, и блока управления, в котором находится насос для забора воздуха и лазерная камера для его анализа.

Конечно, стоимость аспирационных систем в сотни раз превышает стоимость традиционной пожарной сигнализации (цена точечного извещателя – до 500 руб., а аспирационного – от 2500 евро), но зачем ставить точечные извещатели, если они не будут работать? Цена на аспирационные извещатели, пусть и высокая, все же несравнима с тем ущербом, который может нанести пожар, да и в общей смете строительства ЦОДа стоимость аспирационных систем будет составлять лишь несколько процентов.

Технологическая часть (рис. 2) отвечает за хранение газового огнетушащего вещества, а также за его выпуск из модулей. В ее состав входят:

- модуль газового пожаротушения;
- пусковое устройство модуля;
- рукав высокого давления;
- система трубопроводов;
- насадки-распылители.

Средства тушения

К применению на территории России разрешено множество газовых огнетушащих веществ (ГОТВ). Они перечислены в Своде правил СП5.13130.2009. Все эти ГОТВ эффективно тушат пожар, однако есть отличия в механизмах тушения и в способах реализации той или иной установки.

Давайте разбираться. На сегодняшний день известны четыре способа тушения пожара (возможны и комбинации этих способов).

1. **Охлаждение.** Скорость любой химической реакции, в том числе и горения, зависит от температуры. Эта зависимость описывается известным уравнением Вант-Гоффа:

$$v_2 = v_1 \times g^{(T2 - T1)/10},$$

где g – температурный коэффициент со значением от 2 до 4. Из этого уравнения следует простой вывод: при снижении температуры на 10°С скорость реакции падает в 2–4 раза. Это снижение весьма существенно, особенно для цепных реакций (а именно к таким реакциям относится горение). Цепные реакции развиваются лавинообразно и так же лавинообразно угасают. Поэтому резкое охлаждение зоны горения приводит к полному прекращению горения.

По методу охлаждения действуют в основном сжиженные газы. Такие ГОТВ отличаются низкой огнетушащей концентрацией, а следовательно, для них нужно меньшее количество модулей, что очень важно для ЦОДов.

2. **Изоляция.** Все реакции развиваются на границе раздела фаз, проще говоря, на поверхности. В реакции горения участвует не само вещество, а газообразные продукты, переходящие из него в зону

Масштабируемая адресно-аналоговая пожарная сигнализация ESSER

Сетевая система пожарной сигнализации ESSER для защиты магазинов, офисных зданий и промышленных предприятий

ТОВАР СЕРТИФИЦИРОВАН

Серия пожарных панелей IQ8Control C

Особенности системы пожарной сигнализации ESSER:

- Семейство ПКП разной емкости для применения на небольших, средних и крупных объектах;
- Модульная архитектура сигнализации позволяет легко и быстро нарастить систему;
- Возможность объединения до 31 панели в единую сеть essernet;
- Организация интегрированной системы безопасности с помощью ПО WINMAG;
- Максимальная длина кольцевых шлейфов до 3,5 км;
- Интеграция панелей пожаротушения 8010 в кольцевой шлейф esserbus.

Технические характеристики ПКП ESSER:

- К одному ПКП может быть подключено до 40 кольцевых шлейфов esserbus;
- Широкий выбор лицевых панелей управления с отображением информации на русском языке;
- Поддержка беспроводных устройств IQWireless;
- В одном колцевом шлейфе можно объединить:
  - 127 адресных устройств / групп извещателей;
  - 32 транспондера / адресных устройства оповещения серии IQ8Alarm;
  - 48 автоматических извещателей серии IQ8Quad со встроенными устройствами оповещения.

Автоматические извещатели:

- Встроенный изолятор короткого замыкания в каждом извещателе серии IQ8Quad;
- Широкий ассортимент автоматических извещателей (дымовые, термомаксимальные, термодифференциальные, мультисенсорные, со встроенными устройствами оповещения);
- Извещатели для специальных применений (линейные дымовые, линейные тепловые, извещатели открытого пламени, извещатели для взрывоопасных применений, аспирационные извещатели и т.д.)

Транспондеры для подключения периферийных устройств

- Гибкое программирование отдельных входов и выходов транспондеров;
- Большой выбор транспондеров (12 реле, 4 входа/2 реле, 1 вход, коммуника-ционный транспондер, транспондеры для подключения сторонних извещателей и т.д.)

www.armosystems.ru

армо-системы
105066 г. Москва, ул. Спартаковская, д. 11,
Бизнес-центр "Немецкая Слобода", под.2.
Тел.: (495) 787-3342, 937-9057
Факс: (495) 937-9055
e-mail: armosystems@armo.ru
http://www.armosystems.ru

армо-петербург
196084 г. Санкт-Петербург,
ул. М. Митрофаньевская, д. 1, лит.А
Тел.: (812) 449-1435, 449-1436
Факс: (812) 449-1437
e-mail: armo-spb@armo.ru
http://www.armospb.ru

армо-урал
620028, г. Екатеринбург,
ВИЗ-Бульвар, д. 13, корп. 1, оф. 101
Тел./факс: (343) 372-7227, 359-5667, 263-7917
Факс: (343) 359-5567
E-mail: armo-ural@armo.ru
http://www.armoural.ru

454021, г. Челябинск,
ул. Ворошилова, д. 35,
Торгово-офисный центр «Зенит», оф. 2.2
Тел./факс: (351) 247-14-40/41/42
E-mail: armo-ural@armo.ru
http://www.armoural.ru

горения. Это могут быть пары самого вещества или продукты его разложения (первичные продукты горения). С другой стороны, для развития горения требуется постоянная подпитка зоны горения кислородом. Если воспрепятствовать этим процессам, реакция затухает.

3. **Разбавление.** Содержание кислорода в атмосфере – всего 21%. Остальные компоненты воздуха не поддерживают горение, но участвуют в газообмене на границе раздела фаз, конкурируя с кислородом. Поэтому для прекращения горения не обязательно полностью убрать кислород из атмосферы, достаточно снизить его концентрацию примерно до 12%.

Итак, в обычном воздухе содержится 21 об. % кислорода. Нужно разбавить его до 12%: 21/X = 12; X = 21/12 = 1,75, т.е. огнетушащая концентрация (ОТК) газа-разбавителя должна быть равной примерно 75 об. %. На практике используют даже более низкие концентрации, поскольку газовые огнетушащие вещества реализуют несколько механизмов тушения.

ГОТВ, действующие по механизму разбавления, являются экологически чистыми веществами, потому что состоят из газов, которые присутствуют в атмосфере. Но стоит отметить, что высокая огнетушащая концентрация требует большого количества модулей; необходимы также клапаны сброса избыточного давления. К примеру, на помещение в 100 куб. м необходимо приблизительно 50 куб. м газа «Инерген». Если помещение полностью герметично, то эти 50 куб. м газа могут вызвать разрушение помещения, поэтому для «разбавителей» клапаны сброса обязательны.

Водяные, порошковые, пенные установки для тушения пожаров в ЦОДах нет смысла рассматривать, поскольку ущерб для ЦОДа от таких установок сопоставим с ущербом от пожара

4. **Ингибирование.** Это процесс, замедляющий основную реакцию. Суть дела в том, что при горении лавинообразно растет количество активных частиц – радикалов. Например, при воздействии кислорода на углеводород образуются две активные частицы-радикала. Каждая из них, атакуя нейтральную молекулу углеводорода, образует еще два радикала – и цепная реакция пошла... Теперь введем в зону реакции ингибитор, например трифторметан, известный как хладон 23. Его реакция с радикалом уничтожает радикал, и образуются две нейтральные молекулы. Таким образом, количество активных частиц в зоне реакции снижается, следовательно, реакция угасает. На практике все происходит сложнее, но суть процесса от этого не меняется.

При химической реакции ингибирования возможно выделение побочных продуктов, которые могут быть опасными для людей, а также оставляют налет на защищаемом оборудовании.

По действующим в России нормативным требованиям (СП5.13130.2009) запрещено выпускать газовое огнетушащее вещество в помещение, если там находятся люди. И это ограничение совершенно правильное. Как показывает статистика, причиной гибели людей на пожарах более чем в 70% случаев становится отравление продуктами горения. Но если обнаружить пожар на ранней стадии, то негативных последствий можно избежать.

Конечно, предпочтительней использовать безопасные для людей газы, которые, к примеру, при ложном выпуске не оказывают воздействия на здоровье человека. Особенно это важно для больших ЦОДов, где возможно присутствие в залах обслуживающего персонала*.

Типы установок

Установки газового пожаротушения делятся на два типа: централизованные и модульные. В централизованных установках баллоны с газом размещены в помещении станции пожаротушения и тушат сразу несколько помещений или одно из них. Модульные установки пожаротушения состоят из одного или нескольких модулей, объединенных единой системой обнаружения пожара и приведения их в действие. Модули способны самостоятельно выполнять функцию пожаротушения и размещаются в защищаемом помещении или рядом с ним.

Выбор типа установки газового пожаротушения зависит, во-первых, от количества защищаемых помещений на одном объекте, во-вторых, от наличия свободного помещения, в котором можно разместить станцию пожаротушения.

Если защите на объекте подлежат три и более помещений, расположенных друг от друга на расстоянии не более 100 м, с экономической точки зрения предпочтительнее централизованные установки. Причем стоимость защиты одного и того же объема снижается с увеличением количества помещений, защищаемых одной станцией пожаротушения.

Вместе с тем централизованная УГП по сравнению с модульной имеет свои недостатки: приходится прокладывать по зданию трубопроводы от станции пожаротушения к защищаемым помещениям; требуется выполнять множество требований СП5.13130.2009 к станции пожаротушения.

В следующих статьях мы более подробно разберем типы установок, их преимущества и недостатки в применении к ЦОДам, а также коснемся компактных установок пожаротушения, которые постепенно приобретают популярность на российском рынке. ИКС

* См., например, С. Дауэнгауэр, «Сравнение систем пожаротушения», «Алгоритм безопасности», №3'2009.

Биометрические системы контроля доступа в ЦОД

В современных дата-центрах сконцентрировано большое количество дорогостоящего оборудования, там же хранится пользовательская информация, ценность которой порой превосходит стоимость «железа». Поэтому наряду с системами пожарной сигнализации, пожаротушения и охраны ЦОДам требуются системы контроля доступа, и самые прогрессивные из них – биометрические.

Вячеслав ПЕТИН, ведущий эксперт компании «АРМО-Системы» по системам контроля доступа

От кого же мы защищаем ЦОД? Во-первых, от злоумышленников, проникающих на охраняемую территорию с конкретными вредительскими целями. Но не только. Нанести непоправимый ущерб сложным и чувствительным к механическим воздействиям системам можно и по некомпетентности, из самых лучших побуждений. В общем, необходимость установки системы контроля доступа (СКД) в дата-центре, на наш взгляд, сомнений не вызывает. Однако чтобы применение технических средств ограничения доступа имело смысл, нужно позаботиться и о надежной конструкции самого помещения. Проще говоря, и стены, и двери должны быть достаточно прочными.

Технологии ограничения доступа

Среди систем контроля доступа наиболее широко распространены системы, работающие с проксимити-картами или смарт-картами. Популярность СКД на основе бесконтактных карт основана на их относительно низкой стоимости и простоте внедрения. Но не секрет, что проксимити-карту можно передать другому человеку или клонировать. Смарт-карты частично решают проблему с клонированием, однако возможность передачи пропуска другому лицу остается. Учитывая ценность хранимых в ЦОДе данных и оборудования, мы считаем, что целесообразно обратить внимание на биометрические системы контроля доступа, которые обеспечивают действительно высокий уровень безопасности. Ведь подделать отпечаток пальца или форму лица намного сложнее, нежели клонировать или передать карту. К тому же ряд устройств обладает способностью определения ложных биометрических признаков. Например, считыватели отпечатков пальцев Sagem (устройство MA521+) или Bioscript (устройство 4G V-Station Extreme) могут с высокой долей вероятности отличить настоящий палец от поддельного «мертвого», отлитого из пластика или резины.

Сегодня становятся все популярнее системы на основе сканирования рисунка сосудов пальцев, обеспечивающие более высокий уровень безопасности по сравнению с системами на базе отпечатков пальцев. В последние годы активно развивается технология идентификации по геометрии лица. Однако данный метод гораздо сложнее остальных в плане технической реализации, а кроме того, он требует большего отрезка времени для идентификации пользователя, чем, например, сличение шаблонов отпечатков пальцев. Но поскольку для ЦОДов высокая пропускная способность системы не нужна, в них эта технология вполне может применяться.

Основные мировые производители биометрического оборудования – компании ZK Software, Smartec, Sagem, Identix, Bioscrypt, Recognition Systems и LG Electronics.

Необходимо отметить, что к установленным на предприятии биометрическим системам доступа сотрудники иногда относятся с недоверием и неохотно предоставляют свои идентификационные данные. Такое отношение вряд ли оправданно, поскольку все биометрические характеристики хранятся в памяти считывателей или в базе данных СКД в виде специальных ша-

Рис. 1. Считыватель отпечатков пальцев

блонов. Шаблоны же сформированы таким образом, что восстановить из них исходный биометрический признак, будь то отпечаток пальца или изображение лица, невозможно. Поэтому применение биометрической СКД не представляет для сотрудников никакой опасности с точки зрения возможной утечки их персональных данных.

Особенности применения

В биометрических системах контроля доступа биометрический считыватель для ввода того или иного признака может иметь встроенный контроллер управления дверью. Однако в безопасных решениях использование встроенного контроллера недопустимо, поскольку это дает злоумышленнику возможность демонтировать устройство и, замкнув провода, напрямую управлять замком двери. Устранить подобную уязвимость позволяет Wiegand-интерфейс, через который биометрический считыватель подключается к управляющему модулю системы контроля доступа. В этом случае управление замком двери осуществляется модулем, расположенным в безопасной зоне, т.е. внутри защищаемого помещения. Причем считыватели разных технологий могут работать в составе практически любых СКД, чье аппаратное обеспечение поддерживает Wiegand-интерфейс.

При подобной архитектуре системы контроля доступа в памяти считывателя помимо биометрического шаблона хранится Wiegand-код, который посылается во внешнюю СКД при успешной идентификации биометрического признака. И уже внешняя система принимает решение, предоставить пользователю доступ на объект или нет. Помимо описанных вариантов, существуют биометрические считыватели с выносным контроллером двери, который может быть расположен в защищенной зоне.

Хотя при защите ЦОДов рекомендуется использовать считыватели с внешними контроллерами, отметим, что практически любой биометрический ридер имеет датчик вскрытия, срабатывающий при демонтаже устройства. При этом генерируется сигнал тревоги, который поступает как на локальные устройства оповещения, так и в глобальные системы мониторинга, где оператор выбирает соответствующий способ реагирования на тревогу. Срабатывание датчика вскрытия также может активировать дополнительное запирающее устройство.

Один из важнейших элементов любой биометрической системы – программное обеспечение для ввода биометрических шаблонов, регистрации и сбора событий, настройки, мониторинга и обслуживания системы. Если биометрические считыватели подключаются к контроллерам внешней системы, то возможны два варианта работы с ПО.

Первый вариант: комплексная система имеет два различных программных интерфейса. Через программный интерфейс биометрической системы производится регистрация шаблонов и присваивание им соответствующих кодов, а через программный интерфейс системы контроля доступа назначаются уровни доступа, формируются отчеты и осуществляется мониторинг системы в целом.

Второй вариант: комплексная система имеет единый программный интерфейс для СКД и биометрической подсистемы. Такой вариант удобнее и потому предпочтительнее. Например, при добавлении сотрудника в систему все операции по вводу пользовательской информации и биометрических шаблонов, назначению уровней доступа, добавлению фотографий и т.п. выполняются из одного интерфейсного окна.

На что обратить внимание при выборе оборудования

При организации системы контроля доступа особенно важны следующие параметры биометрических считывателей.

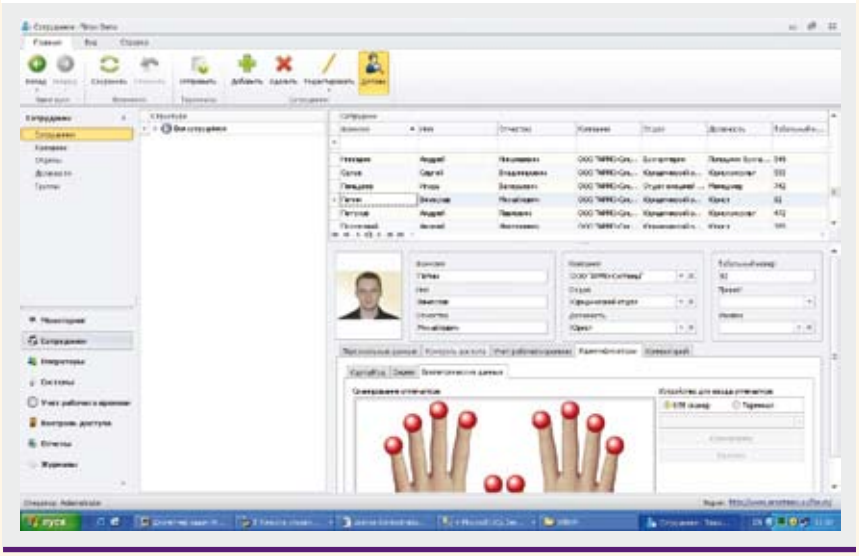
Тип сканера (для идентификации по отпечаткам пальцев). На рынке наиболее широко представлены устройства с емкостными и оптическими сканерами отпечатков пальцев. Емкостные сканеры чувствительны к статическому электричеству и имеют низкую разрешающую способность. С помощью оптических сканеров биометрические шаблоны получаются значительно более качественными. Существуют также ультразвуковые, полупроводниковые, радиочастотные и другие сканеры отпечатков пальцев. У каждой технологии – свои преимущества и недостатки. Например, ультразвуковые сканеры дают высокое качество шаблона, но очень дороги.

Сколько лет биометрии?

Не многие знают, что биометрию человечество применяет как минимум с XIV века. Уже тогда отпечаток пальца служил купцам вместо подписи на торговых соглашениях. В 1880 г. доктор Генри Фолдс опубликовал в научном журнале статью с идеей использования дактилоскопии как способа идентификации личности в криминалистике. А в 1905 г. математик Карл Пирсон превратил идентификацию по отпечаткам пальцев в стройную научную дисциплину. С тех пор биометрия сделала большие успехи, и помимо единственной технологии идентификации по отпечаткам пальцев сейчас существуют десятки методов, которые продолжают развиваться и совершенствоваться. В их числе – идентификация по форме кисти руки, голосу, почерку, сетчатке и радужной оболочке глаза, рисунку сосудов пальцев и форме лица.

В 1947 г. в Вудс-Холле (США) прошла Первая международная биометрическая конференция, где было организовано Международное биометрическое общество, съезды которого проходят каждые четыре-пять лет. Биометрические технологии, отличавшиеся ранее дороговизной, сегодня становятся все более доступными для малого бизнеса и даже для домашнего применения.

Рис. 2. Программный интерфейс системы контроля доступа на основе биометрических параметров



Емкость базы данных шаблонов. Биометрические считыватели редко имеют большую память для хранения шаблонов. Ограничения на размер памяти накладывает главным образом быстродействие процессора устройства, так как выполняемая им задача идентификации весьма ресурсоемкая: считыватель должен сравнить один шаблон с множеством других. Обычно память рассчитана на сотни, иногда тысячи шаблонов. При использовании считывателей отпечатков пальцев нужно учитывать необходимость хранения нескольких шаблонов для одного человека, поскольку пальцы подвержены различным повреждениям. Среди считывателей с увеличенной памятью отметим модель MA500 от Sagem, которая может обслуживать до 50 тыс. пользователей (по два отпечатка пальца на каждого), и считыватель 4G V-station от Bioscrypt с памятью на 500 тыс. шаблонов.

Многофакторная идентификация. Наличие такой возможности значительно повышает уровень безопасности системы. Так, при работе в режиме «код + биошаблон» пользователь должен и предъявить биометрический признак, и ввести код доступа. Также очень распространен режим «карта + биошаблон». Существует и трехфакторная идентификация, например «карта + код + биошаблон». Для реализации подобных режимов работы большинство биометрических считывателей опционально имеют встроенный считыватель проксимити- или смарт-карт. Некоторые устройства со встроенными считывателями смарт-карт позволяют хранить биометрические шаблоны не в памяти считывателя, а на самой смарт-карте. Этот метод нивелирует влияние ограниченной памяти устройства, поскольку при сравнении предоставленного биометрического признака с биометрическим шаблоном последний берется не из памяти считывателя, а со смарт-карты. Данный режим эквивалентен двухфакторной идентификации – для получения доступа пользователь должен предъявить и карту, и биометрический признак. Некоторые биометрические считыватели имеют клавиатуру для ввода PIN-кода и/или программирования устройства.

Скорость идентификации (время считывания и распознавания шаблона). Обычно высокая пропускная способность нужна на проходных крупных предприятий. Доступ в помещения ЦОДа требуется только обслуживающему персоналу, соответственно, пропускная способность не является критическим параметром. Именно поэтому здесь могут использоваться биометрические считыватели, скажем, на основе идентификации по форме лица или по сетчатке глаза, работа которых занимает чуть больше времени, чем работа считывателей отпечатков пальцев.

Wiegand-интерфейс (вход/выход). Wiegand-выход позволяет подключать биометрические считыватели к широкому спектру систем контроля доступа. Также к Wiegand-входу биометрического считывателя можно подключать внешние считыватели проксимити- или смарт-карт и использовать карты в качестве дополнительного фактора идентификации.

Коэффициент ложного пропуска (FAR). Важный параметр любой системы безопасности. Он показывает, насколько велика вероятность того, что неправильный биометрический шаблон будет определен как правильный. Значение данного параметра не должно превышать 0,0001 (т.е. на 10 тыс. попыток может произойти одно ошибочное определение биометрического шаблона).

Коэффициент ложного отказа (FRR). Этот параметр показывает, насколько велика вероятность того, что правильный биометрический шаблон будет определен как неправильный. Поскольку в ЦОДе не требуется высокая пропускная способность, параметр не очень важен: при неверной идентификации биометрического признака сотруднику не составит труда пройти идентификацию еще раз, потратив чуть больше времени.

■ ■ ■

Биометрические технологии все шире распространяются на профильных рынках. Это обусловлено и более высоким уровнем защиты, обеспечиваемым биометрией по сравнению с системами на основе бесконтактных карт, и удобством ее применения.

Биометрические системы наиболее полно отвечают высоким требованиям безопасности, предъявляемым к системам контроля доступа таких важных объектов, какими являются ЦОДы. Быстрое развитие биометрических технологий обязывает нас при планировании комплексной системы безопасности подобных объектов тщательно изучить текущее состояние отрасли с тем, чтобы выбрать наиболее подходящие технологии и функциональное оборудование. ИКС

Коммутатор для предприятий малого и среднего бизнеса

Коммутатор Web Smart DES-1210-08P оснащен восемью портами 10/100 Мбит/с с поддержкой технологии PoE (IEEE 802.3af) и имеет расширенные функции управления и безопасности. В устройстве также реализована функция энергосбережения, с помощью которой можно отключить питание портов в заданное время.

DES-1210-08P поддерживает такие функции, как VLAN на основе стандарта IEEE 802.1Q, динамическое агрегирование каналов, Spanning Tree, Loopback Detection, IGMP Snooping, Port Mirroring и LLDP, а также функцию диагностики кабеля. Аутентификация 802.1x на основе портов, функции Port Security, DHCP Server Screening, ACL, ARP Spoofing Prevention и Safeguard Engine обеспечивают управление доступом пользователей к сети и защиту от вредоносного трафика.

Коммутатор поддерживает функции Auto Surveillance VLAN (ASV) и Auto Voice VLAN для приложений VoIP и развертывания системы видеонаблюдения. ASV гарантирует качественную передачу видео в режиме реального времени, присваивая сетевому трафику тот или иной уровень сервиса, а функция управления полосой пропускания позволяет сетевым администраторам обеспечить максимальный приоритет приложениям, требующим высокой пропускной способности.

Управление коммутатором осуществляется через Web-интерфейс, компактный интерфейс командной строки по протоколу Telnet или утилиту SmartConsole.

Рекомендованная розничная цена – $266.

D-Link: (495) 744-0099

Однофазные ИБП

ИБП серии Amplon RT – онлайновые ИБП мощностью 5,6 и 10 кВА с двойным преобразованием, высоким коэффициентом мощности (на входе > 0,99) и малыми гармоническими искажениями входного тока (iTHD < 5%). Устройства оборудованы русскоязычным ЖК-дисплеем, отличаются компактностью (габаритные размеры – 440 x 671 x 89 мм (Ш x Г x В)) и допускают как горизонтальную (в стойку), так и вертикальную установку. Для повышения надежности ИБП можно установить по схеме 1 + 1 параллельного резервирования.

Также можно увеличить количество подключенных батарейных модулей, чтобы обеспечить необходимое время работы критически важных приложений. Широкий диапазон входного напряжения и регулируемый ток заряда увеличивают срок службы батарей. Для сокращения времени перезарядки используется дополнительное зарядное устройство.

ИБП Amplon RT пригодны для защиты серверного, сетевого и телекоммуникационного оборудования в ЦОДах.

ООО «Дельта Энерджи Системс»: (495) 644-3240

ИБП для операторов связи

«Форпост» – источник бесперебойного питания 220 (380) В / 48 В – 140 А. Он предоставляет возможность выбора выходного напряжения – 48 В или 60 В, подключения до 10 нагрузок и работы с двумя группами аккумуляторных батарей, имеет масштабируемую архитектуру. Размеры устройства – 480 x 352 x 360 мм.

Для обеспечения безаварийной эксплуатации в ИБП используются микропроцессорное управление, внутренний мониторинг, комплекс автоматических защит, журналы состояний источника и аккумуляторных батарей в реальном времени, система автоматического содержания и заряда АКБ, формирование сигналов телеметрии, подключение внешних датчиков, звуковая и световая сигнализация об аварии.

Конфигурирование и управление осуществляется по Ethernet через интерфейс LAN, а также по интерфейсам CAN или RS-232. При управлении по LAN оператор через веб-браузер подключается к выбранному им ИБП и может проконтролировать напряжение питающей сети, выходное напряжение и температуру всех выпрямителей; номер основного выпрямителя; наличие батареи; ток и напряжение батареи и нагрузки; емкость, температуру и процент заряда батарей. При необходимости оператор также через Интернет может изменять приоритет выпрямителей БПС, включать и отключать их; запускать процессы выравнивания заряда аккумуляторных батарей. Количество ИБП в системе дистанционного контроля оператора практически не ограничено. Помимо этого возможно управление при помощи графического ЖК-дисплея и навигационного меню.

«Оптимальные Коммуникации»: (495) 730-6363

Система экономного охлаждения ЦОДа

EcoBreeze – воздушная система охлаждения, устанавливаемая за пределами ЦОДа и способная осуществлять автоматическое переключение между прямым воздушным и косвенным испарительным теплообменом.

При достаточно низкой температуре окружающей среды EcoBreeze использует прямой воздушный теплообмен, обеспечивая минимальный расход электроэнергии. При этом горячий воздух от компьютерного оборудования ЦОДа прокачивается электронно-коммутируемыми вентиляторами через внутренние каналы косвенного испарительного охладителя (IEC). После первоначального охлаждения воздух от компьютерного оборудования выходит из IEC, проходит через змеевик охлаждения и возвращается в центр обработки данных.

Если температурные условия делают такое охлаждение недостаточно эффективным, система автоматически переходит в режим косвенного испарительного теплообмена: тепло горячего воздуха, поступающего от компьютерного оборудования ЦОДа, удаляется за счет испарения воды с наружной стороны каналов теплообменника. Однако при любом режиме охлаждения EcoBreeze устраняет контакт наружного воздуха с воздухом внутри ЦОДа.

EcoBreeze включает пропорциональную систему подачи хладагента R410a и встроенную систему водоподготовки, исключающую необходимость в химической обработке воды.

EcoBreeze – модульное решение: блоки системы охлаждения мощностью 50 кВт могут объединяться в группы до четырех (200 кВт) или восьми (400 кВт) модулей. EcoBreeze соответствует стандартам энергоэффективности ASHRAE 90.1/TC 9.9 и подходит для работы в странах с холодным климатом. Доступны варианты системы с различными мощностью, напряжением и числом фаз электропитания.

APC by Schneider Electric: 8(800) 200-2722

Терминал для HD-видеоконференцсвязи

Aastra BluStar 8000i Media Phone – это специализированное высокопроизводительное настольное устройство для видеоконференций со средствами совместной работы. Оно объединяет настольный телефон, 13-дюймовый цветной сенсорный экран с разрешением видеоизображения 1280 x 720 пикселов и поддержкой перьевого ввода, широкоугольную HD-камеру с углом обзора 70° и разрешением 720 пикселов, матрицу из четырех управляемых микрофонов, следящих за перемещением говорящего в пространстве для устранения нежелательного фонового шума, три высококачественных громкоговорителя (левый/правый и центр/бас) и сканер отпечатков пальцев.

Благодаря поддержке стандарта H.264 для видео, протокола SIP – для управления вызовом и широкополосного аудиокодека G.722, медиафон обеспечивает HD-видеоконференцсвязь с частотой 30 кадров/с. Скорость потока – от 128 кбит/с до 5 Мбит/с. Возможен как полноэкранный режим работы, так и режим с разбивкой экрана.

Помимо видеозвонков в режимах «точка–точка» и многоканальной видеоконференции (до 100 участников) поддерживаются опции совместной работы: передача файлов с ПК, сотовых телефонов и других устройств по Bluetooth-интерфейсу, совместный просмотр документов, выведенных на экран с компьютера. С системой могут быть интегрированы пользовательские приложения, обеспечивая отображение дополнительной информации из различных источников. Для интеграции приложений сторонних производителей предоставляются API и SDK.

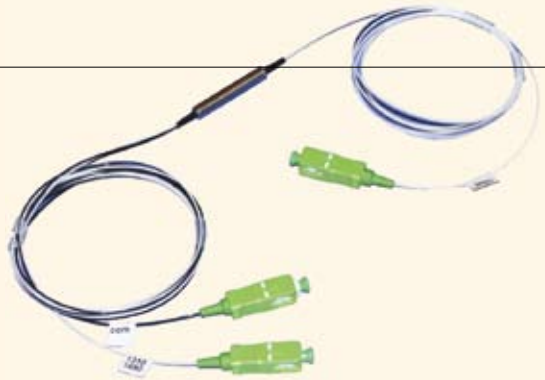
Идентификация пользователей для входа в систему осуществляется с помощью сканера отпечатков пальцев. Шаблоны отпечатков пальцев хранятся в устройстве. Имеется также голосовая идентификация.

Физические интерфейсы: два порта Gigabit Ethernet, разъем RJ9 для гарнитуры, разъем 3,5 мм для микрофона (полоса пропускания 18 кГц), разъем 3,5 мм для гарнитуры (полоса пропускания 18 кГц), два порта USB 2.0

Aastra BluStar 8000i Media Phone полностью интегрируется с платформами Aastra MX-ONE и A5000.

Aastra: (495) 287-3035

Оптический мультиплексор



Мультиплексор PWD-02FF5L12 предназначен для передачи аналогового телевизионного сигнала на длине волны 1550 нм при построении сетей FTTH (PON).

Мультиплексор состоит из корпуса и оптических ввода-выводов (полюсов) с длиной волокна 1 м. Поставляется оконцованным любым типом оптических разъемов (SC, FC, LC, ST) с любым типом полировки (UPC, APC). Монтируется в 19-дюймовые конструктивы 1U, 2U и 4U (изделие ПОР-РМ), которые устанавливаются в большой оптический кросс КМО или в 19-дюймовый шкаф вместе с активным оборудованием.

Оптические характеристики:

- рабочий диапазон длин волн 1550 нм – 1540–1560 нм;
- рабочие диапазоны длин волн 1310 и 1490 нм – 1260–1360 и 1480–1500 нм;
- максимальные вносимые потери для диапазона 1550 нм – 0,50 дБ;
- максимальные вносимые потери для диапазонов 1310 и 1490 нм – 0,40 дБ;
- минимальная изоляция для диапазона 1550 нм – 35 дБ;
- минимальная изоляция для диапазонов 1310 нм и 1490 нм – 25 дБ;
- поляризационные потери – 0,1 дБ;
- оптические возвратные потери – 50 дБ.

Малое значение затухания на мультиплексоре (менее 0,8 дБ) позволяет подключить 64 абонента на одну линию от OLT без ущерба для оптического бюджета линии. PWD-02FF5L12 имеет декларацию о соответствии (№ ОК-1696) и может применяться на сетях связи.

НТЦ «ПИК»: (8332) 37-6140

Решение для веб-конференций

OpenScape Web Collaboration предоставляет возможности организации мультимедийных совещаний для предприятий всех размеров.

Решение OpenScape Web Collaboration поддерживает до 250 параллельных пользователей на одном сервере, до 1000 пользователей мобильных клиентов/веб-браузеров или 100 собственных клиентов в одном сеансе. До восьми участников сеанса могут передавать видео (кодек H.264). Сервер OpenScape Web Collaboration может быть установлен в среде VMware ESX(i) 4.x.

Пользователь может определить, будет ли он представлять свой рабочий стол или просматривать чужой. Пользователи могут загружать документы в хранилище файлов и указывать участников, которым разрешено эти файлы скачивать. Имеется функция чата для обмена текстовыми сообщениями.

Опция электронной доски позволяет создавать эскизы на виртуальной панели. Они могут быть сохранены как графические файлы для дальнейшей работы. Сеанс веб-конференции может быть записан и сохранен в защищенном от несанкционированного использования формате.

Безопасность обеспечивается 256-битным AES кодированием. Используется протокол HTTP с SSL-кодированием. Также может быть установлен пароль для присоединения к сессии. Решение OpenScape Web Collaboration имеет сертификат TÜV Süd (DIN:ISO/ IEC 25051:2009).

Siemens Enterprise Communications: (495) 737-1215

ИБП с измерением потребляемой мощности

Eaton 5PX – серия ИБП мощностью от 1,5 до 3 кВА, выполненных по линейно-интерактивной технологии. Выходной коэффициент мощности – 0,9, КПД может достигать 99%.

ИБП позволяет измерять потребляемую мощность до уровня групп розеток. Результаты измерений могут быть выведены на ЖК-экран 5PX или загружены с помощью ПО управления питанием Eaton Intelligent Power Software Suite.

В ИБП реализовано управление сегментами нагрузки, что дает возможность сначала завершать работу некритичного оборудования и таким образом увеличивать время работы критичного оборудования от батарей.

5PX предлагает подключение по COM- и USB-портам, а также имеет дополнительный разъем для опциональных коммуникационных плат (включая плату SNMP/ Web или плату релейных контактов).

Заряд батарей производится по трехэтапной технологии, при которой батарея заряжается только в случае необходимости. В результате батареи меньше подвергаются разрушению и общий срок их службы увеличивается до полутора раз. Поддерживается «горячая» замена батарей.

Устройства имеют универсальный корпус, поэтому могут быть установлены как в стойку, так и вертикально.

Eaton: (495) 981-3770

Блог, еще раз блог!

Владимир ЛИТВИНОВ

История – залог самостоятельности

>>>> Вчера в истории развития телекоммуникаций произошло уникальное событие. Впервые, по-моему, за двадцать лет в телеэфире Первого канала программы «Время» появился сюжет о юбилейной дате в истории развития отечественной связи.

...Интересная деталь. Там, где компании (МГТС, «Центральный Телеграф») хранят историю развития предприятий, а значит, чтут традиции, продолжается относительно самостоятельное их функционирование в сложнейших условиях перехода к рыночной экономике. Я с болью вспоминаю, с какой легкостью на «междугородке» мы отправляли на металлолом и драгметаллы шнуровые и бесшнуровые коммутаторы, декадно-шаговые искатели, междугородные таксофоны и т.д., ничего не оставляя для потомков. Может, поэтому и судьба предприятия делает такой крутой поворот от крупнейшего на сети Союза до 74-го филиала «Ростелекома».

Конечно, новый «Ростелеком» с 20-летней историей и постоянно меняющимся менеджментом живет сегодня другими задачами (консолидация активов, диверсификация бизнеса и т.д.). Тем не менее он сформирован из старейших предприятий связи, а открытию первого междугородного сообщения (Москва – Петербург) в этом году исполнилось 112 лет. В распоряжении «Ростелекома – ММТ» находится уникальный с точки зрения места для будущего музея объект (здание по адресу Арбат, 46), расположенный в пешеходной зоне старого Арбата.

Такая получается история. О юбилейных датах дальней связи вспоминают в телеэфире, но не имеют представления в «Ростелекоме», как, впрочем, и в «Связьинвесте». Да и обратиться там по существу некуда, по крайней мере в Москве...

комментировать

Михаил ЕМЕЛЬЯННИКОВ

Велик могучий русский языка!

>>>> Законы наряду с двумя главными общеизвестными бедами нашей страны, похоже, уверенно становятся третьей.

...Долго, хором и поодиночке, читали часть 12 ст. 9 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (ФЗ-294): «О проведении плановой проверки юридическое лицо, индивидуальный предприниматель уведомляются органом государственного контроля (надзора), органом муниципального контроля не позднее чем в течение трех рабочих дней до начала ее проведения». Я не верю в опечатки в законах. Они проходят через такое количество и таких рук, что опечатка там невозможна в принципе. Так что же тогда имели ввиду авторы под словами «не позднее, чем в течение трех рабочих дней»? Эта фраза на русский язык не переводится никаким образом. За один час предупредить можно? Это же не позднее? А за неделю? Это позднее или раньше?

Дальше – больше. ФЗ-294 обязывает органы контроля и надзора согласовывать планы проверок с прокуратурой, Генпрокуратура и контролирующие органы должны размещать планы проверок на своих сайтах. Такие планы есть. На сайте Роскомнадзора – в явном виде, на сайте Генпрокуратуры – в виде поисковой формы. Они не совпадают! В плане Роскомнадзора проверка конкретной организации есть, в сводном плане Генпрокуратуры – нет. И что из этого следует? Можно проводить проверку или нет? Законна ли она? В ФЗ-294 ответа снова нет...

Ах, как прав был безвременно ушедший Александр Иванов: «Велик могучий русский языка!». На нем можно писать законы, понять которые нельзя, а чиновник тем не менее всегда оказывается прав. А все остальные, соответственно, неправы...

комментировать

Геннадий ФОКИН

Управление рисками правообладателей

>>>> На рынке (в частности, софтверном и наукоемкой высокотехнологичной продукции) сложилась парадоксальная ситуация – желание работать с интеллектуальными правами огромное, а навыков и необходимой документации у правообладателей, как правило, нет. Немудрено – патенты (правоустанавливающие документы) охватывают не более 15% объема оборота интеллектуальной собственности и на программы для ЭВМ, базы данных не распространяются, а практикуемые свидетельства о регистрации программ для ЭВМ и баз данных правоустанавливающими документами не являются. Таким образом, один из самых высокотехнологичных бизнесов является и одним из самых незащищенных.

Имущественные интеллектуальные права – «золотовалютный запас бизнеса». Интеллектуальные права появляются только в отношении результатов интеллектуальной деятельности. Однако не каждый результат может стать «интеллектуальным активом», ему нужна «оправа» – надлежаще оформленные документы, подтверждающие наличие и использование интеллектуальной собственности без нарушения интеллектуальных прав.

Каждый выходит из положения как может...

Не нужно бояться трудностей – «поводырем» правообладателя может стать ассоциированная система менеджмента качества результатов научно-технической деятельности, организованная и функционирующая по стандарту СТО.9001-08-2011 серии «Интеллектуальная собственность и инновации».

комментировать

Реклама в номере

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

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

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

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