

Снова в контртренде



Российские индексы на протяжении всего января показывали восходящую динамику, активная фаза роста пришлось на вторую декаду месяца. В феврале конъюнктура на финансовых рынках ухудшилась, но телеком-сектор двигался против тренда широкого рынка.



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

Отечественные индексы с начала года росли на новостях из США – экономика за океаном избежала угрозы «фискального обрыва», республиканцы решили проголосовать за повышение потолка госдолга. Дополнительную поддержку российским индексам оказал благоприятный ход сезона отчетностей в США, а также признаки оживления экономики в Китае, высокие цены на нефть (Brent в январе торговалась в коридоре \$113–115 за баррель) вкупе с укреплением рубля. Однако в феврале на финансовых рынках возобладал пессимизм, поводом для которого стали сообщения о падении ВВП США в IV квартале 2012 г. на 0,1% (по сравнению с IV кварталом 2011 г.) и негативной динамике ВВП еврозоны за аналогичный период (–0,6%).

Операторы – Олимпиаде и федеральным трассам

Капитализация «Ростелекома» за месяц снизилась почти на 5%. С начала года акции телекоммуникационного холдинга вели себя крайне волатильно, достигнув ценовой отметки в 125,9 руб. за бумагу в начале января и откатившись впоследствии до локального минимума – 117,9 руб. за одну обыкновенную акцию. Корпоративный новостной фон в рассматриваемый период выглядел весьма благоприятно. Холдинг продолжил активное развитие в регионах: в частности, была запущена сеть 3G в Приморском крае, а ФАС одобрила покупку «Ростелекомом» читинского оператора «Локтелеком» и новоуренгойского «Теле МИГ».

Определенное давление на котировки оператора могла оказать информация о том, что объем собственных инвестиций «Ростелекома» в проект Олимпиады 2014 в Сочи превысит 3 млрд руб. Средства будут направлены на развитие телекоммуникационной инфраструктуры и предоставление организаторам, участникам и гостям мероприятия современных услуг связи. Среди значимых корпоративных событий прошедшего месяца можно назвать и назначение директором департамента продуктов и маркетинга «Ростелекома» Ана-

толия Сморгонского, который ранее занимал должность директора по маркетингу Московского региона «ВымпелКома».

В прошлом месяце состоялся круглый стол с участием сотовых операторов, производителей оборудования и Минкомсвязи РФ, в рамках которого обсуждались проекты обеспечения федеральных трасс услугами сотовой связи. На нем было объявлено о том, что совокупный объем инвестиций в оснащение российских автодорог услугами сотовой связи в 2013 г. составит около 4 млрд руб. Несмотря на то что такие проекты для операторов не окупаются, их реализация обеспечивает завершенность сотовой сети. К тому же государство, ввиду высокой социальной значимости таких проектов, финансирует 50% совокупных затрат на их реализацию, снижая нагрузку на участников рынка мобильной связи.

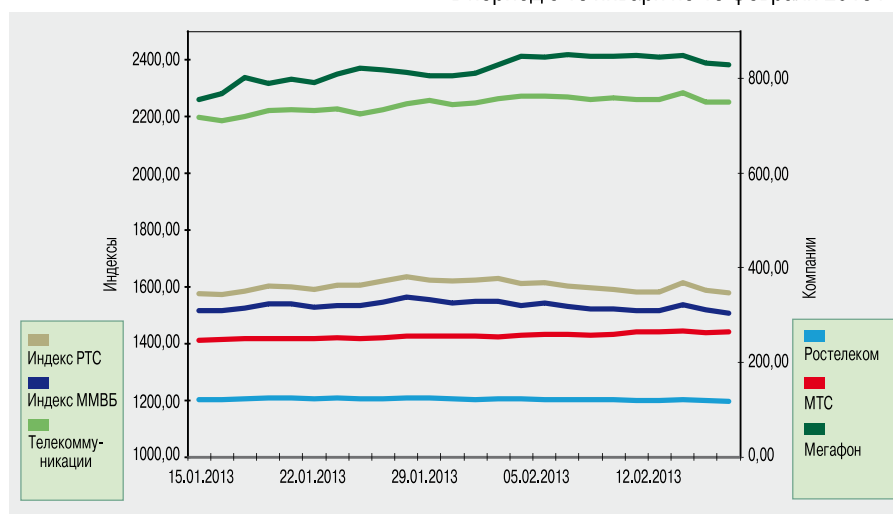
Акции МТС за рассматриваемый период подорожали на 6,44%, до 264,92 руб. Из негативных корпоративных событий следует выделить подачу узбекской «дочкой» МТС заявления о банкротстве. Причиной для этого стала невозможность «Уздунробиты» выполнять возложенные на нее Ташкентским городским судом финансовые обязательства в размере \$600 млн. Впрочем, МТС уже отразила в отчетности за II квартал 2012 г. обесценение долгосрочных активов компании в Узбекистане в размере \$579 млн и резерв в размере \$500 млн под возможные судебные разбирательства.

Справка ИКС



За период с 15 января по 15 февраля индекс ММВБ потерял 1,33% (до отметки 1508,17 пункта), а индекс РТС снизился на 0,72% – до 1577,26 пункта. Отраслевой индекс «ММВБ телекоммуникации» выглядел лучше широкого рынка, продемонстрировав за месяц прирост на уровне 3,2%, до 2251,27 пункта.

Динамика биржевых индексов и индексов телекоммуникационных компаний в период с 15 января по 15 февраля 2013 г.



В прошлом месяце на внеочередном общем собрании акционеры одобрили присоединение к МТС ЗАО «КР-1» и еще 12 региональных компаний. Параллельно ФАС удовлетворила ходатайство ОАО «Мобильные ТелеСистемы» о приобретении прав, позволяющих осуществлять функции единоличного исполнительного органа ЗАО «КОМСТАР-Регионы». Вероятно, активным покупкам бумаг МТС способствовала информация о том, что оператор может получить \$200 млн синергического эффекта за 2011–2012 гг. благодаря интеграции мобильных и фиксированных технологий и внедрению конвергентных сервисов. При этом розничная сеть МТС отчиталась о росте объема продаж через интернет-магазин в 2,5 раза по итогам 2012 г. По информации компании, такие темпы роста были достигнуты как за счет увеличения количества пользователей мобильного интернета, так и благодаря общему подъему российского рынка онлайн-торговли.

Более впечатляющую динамику продемонстрировали бумаги VimpelCom Ltd., подорожавшие на 14,14% (до \$12,27 за шт.). Оператор объявил о планах подконтрольного Orascom Telecom Holding S.A.E. по выкупу 99,3% акций канадской WIND Mobile, принадлежащих основателю и CEO компании. После того как канадские власти утвердят сделку, Orascom Telecom Holding будет владеть 65,1% в Globalive. В свою очередь, менедже-

мент норвежской Telenor заявил о том, что не планирует снижать долю в акционерном капитале «Вымпел-Кома», считая актив интересным с точки зрения инвестирования и поддерживая стремление компании к повышению стоимости. С другой стороны, фактором, сдерживающим интерес инвесторов к бумагам оператора, могла стать информация о том, что «ВымпелКом» не намерен увеличивать размер дивидендов до 2015 г., выплачивая в ближайшие годы \$0,8 на обыкновенную акцию.

Капитализация «МегаФона» выросла на 10,25%, до 829,6 руб. за акцию. Прошедший месяц не был насыщен корпоративными событиями; из числа наиболее значимых следует выделить внеочередное общее собрание акционеров компании, на котором им предстояло выбрать совет директоров мобильного оператора и одобрить договор с поставщиком биллинга «Петер-Сервис» на сумму 9,7 млрд руб.

No news – good news

Бумаги АФК «Система» подорожали за месяц на 8,04% – до \$26,7 за шт. Поводом для роста, вероятно, стали планы корпорации увеличить дивидендные выплаты акционерам в 2013 г. Следует отметить, что в 2011 г. объем дивидендов «Системы» составил 2,7 млрд руб. Влияние на котировки компании могла оказать и информация о продлении Верховным судом Индии срока действия лицензии «дочки» АФК «Система», Sistema

Shyam TeleServices Limited (SSTL), до следующего заседания суда – 11 марта нынешнего года. В феврале 2012 г. Верховный суд Индии аннулировал 122 региональные GSM- и CDMA-лицензии, выданные в 2008 г. 11 операторам, посчитав, что частоты достались им слишком дешево. У SSTL суд аннулировал 21 из 22 лицензий. В мае 2012 г. SSTL подала в Верховный суд Индии надзорную жалобу о пересмотре решения об отзыве лицензий.

В отсутствие каких-либо значимых новостей капитализация IBS Group выросла на 10,22% (до \$17,8), а холдинга РБК, напротив, сократилась на 3,7% (до 12 руб. за акцию).

Позитивные настроения преобладали в прошедшем месяце и в акциях подавляющего большинства интернет-компаний. Котировки бумаг Yandex N.V. выросли на 8,59% – до \$25,2 за шт. Основным драйвером роста, вероятно, стало ожидание инвестиционным сообществом финансовых результатов поисковика за последний квартал 2012 г., которые были опубликованы 19 февраля. Из менее значимых новостей, способных оказать влияние на динамику капитализации «Яндекса», можно выделить заключение соглашения с Европейским центром ядерных исследований (ЦЕРН) – в рамках сотрудничества поисковик будет предоставлять ученым-физикам свои вычислительные ресурсы и технологии обработки данных. Кроме того, «Яндекс» в прошлом месяце сообщил о запуске Wonder – первого приложения, ориентированного на американский рынок. К приложению могут подключаться учетные записи пользователя в Facebook, Twitter, Instagram и Foursquare, причем поиск информации ведется среди данных, которыми делятся друзья пользователя.

Капитализация Mail.Ru Group выросла на 9,48%, до \$35,8 за шт. Значимых корпоративных новостей за рассматриваемый период не случилось, за исключением информации о переходе Сергея Мартынова, руководителя основного сервиса компании – «Почты Mail.ru», в Минкомсвязь. В министерстве он займется развитием портала госуслуг. ИКС

Организатор



Партнер



Билайн®



Как машина – машине...

M2M – межмашинное взаимодействие – называют будущим телекома. И других приоритетных секторов экономики. По прогнозам к 2020 г. в мире будет до 50 млрд подключенных устройств, а людей – 7,3 млрд. Пропорции очевидны. Однако в ожидании «машинного бума» разумно выяснить: почему M2M-проекты не идут как по маслу? кому выгоден бизнес M2M? в каких отраслях эти услуги могут дать максимальный эффект?

Эти и другие вопросы «ИКС» задал профессиональному сообществу за круглым столом на тему «M2M. Чем и кому полезно межмашинное взаимодействие».



Н. КИЙ, «ИКС»

Наталья КИЙ, главный редактор, «ИКС»: Сектор рынка, о котором идет речь, в России достаточно молод, ему чуть больше 10 лет. Но именно сейчас он входит в фазу активного роста. Цифры пока не поражают: например, доля в структуре доходов оператора меньше одного процента, 10%-ное в среднем проникновение сим-карт. Но какая перспектива!

Рост выручки операторов от оказания услуг M2M – 70–80%, проникновение сим-карт увеличится в полтора десятка раз в первую пятилетку текущего десятилетия.

Поделюсь наблюдением, сделанным в ходе организационной подготовки к круглому столу. Приглашая аудиторию к участию, мы контактировали с довольно обширной базой вертикальных рынков, которая есть у журнала, – это преимущественно ИТ-директора, руководители технических служб, главные инженеры. Обнаружили, что осведомленность о существовании и возможностях M2M невелика и – как следствие – невелика заинтересованность потенциальных пользователей в межмашинном взаимодействии. Поэтому, во-первых, так важно мнение представителей разных секторов экономики, собравшихся за этим столом. А во-вторых, операторам и сервис-провайдерам M2M предстоит еще этот рынок формировать и воспитывать, что они за свою историю с успехом делали не раз.

Максим САВВАТИН, консультант, iKS-Consulting: На мировом рынке сегмент M2M продолжает

бурно развиваться. Темпы роста числа сим-карт с проникновением 2–2,5% остаются на уровне 40–50%. Объем рынка на конец 2012 г. оценим в \$68 млрд. M2M – это не рынок большого ARPU, здесь иллюзий нет. В среднем по миру получается \$5–6. Там, где трафик объемный (телематика, автотранспорт, видеонаблюдение), ARPU выше – до \$30–40 и больше.

Один из основных драйверов рынка – ЖКХ, сегмент умных счетчиков, смарт-грид-решений. Не везде дела идут гладко. Например, в США, инновационном лидере M2M, ряд потребителей коммунальных услуг выражали недовольство лишними расходами по смене счетчиков и подключению нового оборудования.

Лидируют на рынке M2M, разумеется, крупнейшие операторы – Vodafone, Orange и Telefonica, которые работают во множестве стран не только в Европе, но и в Латинской Америке.

А что происходит у нас? В России уже почти 4 млн сим-карт. Структура рынка в принципе схожа с корпоративным сегментом: более 85% абонентов контролируется операторами большой тройки. ARPU на европейском уровне – порядка 70–80 руб., в автомобильной навигации и трекинге – до 800 руб. В ближайшие три-четыре года ожидается 50–60%-ный рост рынка, который может многократно ускориться с вводом в действие проекта «ЭРА-ГЛОНАСС». Большое влияние на развитие M2M оказывает и еще окажет госсектор.



М. САВВАТИН, iKS-Consulting

А потребитель кто?



«ИКС»: Какие сегменты корпоративного рынка наиболее заинтересованы во внедрении M2M-решений? Какие из них проявили этот интерес, а кто еще об M2M не знает?



А. НАЗАРОВ, «ВымпелКом»

Алексей НАЗАРОВ, директор по маркетингу бизнес-сегмента, «ВымпелКом»: Я бы сказал, что M2M в России пока развивается стихийным образом. Бросили семечко – оно растет. Не могу сказать, что есть четкая стратегия, что государство, например, планирует развитие и поддержку M2M. В рамках нашего бизне-

са первые сим-карты межмашинного взаимодействия начали использоваться в банкоматах, что, признаюсь, было обнаружено постфактум. Пришло время определиться и с приоритетами, и с направлениями инвестиций в этот сегмент.

Сергей МИШЕНКОВ, советник министра, Минкомсвязь России: Межмашинное взаимодействие применяется с 40–50-х годов – при создании больших систем ПВО, ПРО, ПКО. Одни из первых M2M-решений строились на основе систем радиосвязи. Например, «Алтай» еще в досотовую эпоху контролировал состояние мостов.

Вячеслав АФАНАСЬЕВ, исполнительный директор, фонд «Инвестиции & Инновации & Технологии»: У меня есть не менее удивительная информация: первый российский GSM появился в виде межмашинного взаимодействия в Когалыме – там в 1993 г. нефтяники использовали это решение для управления своей сетью.

Александр КОЛОМЕНСКИЙ, руководитель интернет-проекта, GPS Club Россия: Возьмем диспетчеризацию – огромный рынок: такси, грузовики, логисты, кто угодно. Вы, наверное, видели: в такси стоят навигаторы с сим-картами. В геосоциальные сети уже вовлечены миллионы людей во всем мире. Они используют сим-карту с одной целью:



А. КОЛОМЕНСКИЙ, GPS Club Россия

чтобы выходить в интернет и посылать друг другу геолокационные сообщения. Самый большой взлет рынка M2M будет связан с системой «ЭРА-ГЛОНАСС» – это миллионы симок. В конце года в России появились китайские устройства с двумя симками, вторая предназначена для передачи данных – от трекера, информации о пробках и т.д. Рынок M2M намного больше, чем нам представляется, и надо на него смотреть более широко открытыми глазами, тогда к нему будет больше интереса.

Марк ВЕРЕЗУБОВ, начальник управления оперативного маркетинга, «Акадо Телеком»: По опыту нашей компании, один из основных интересов ис-

пользования M2M – это ЖКХ с мониторингом счетчиков в квартирах. Такой проект был запущен в Москве еще в 2006 г. В одном из районов Екатеринбурга в настоящее время выполняется проект интеллектуального города. Знаю, что программа «Умный город» будет реализовываться в Сколково. Решения в сфере интеллектуального города смогут дать всплеск M2M при условии бюджетной поддержки. Думаю, что и другие сферы услуг воспользуются предложением, например медицина, торговля.

Сергей МЕЛЬНИК, директор Центра сертификации, НТЦ «Комсет»:

Актуальный пример потребления M2M – передача в сервисный центр информации о состоянии агрегатов и передвижениях тяжелых машин. Понятное дело, что гарантийное обслуживание, которое приходится выполнять производителю после прогона экскаватора, гораздо дороже, нежели оснащение машины M2M-модулем, который в реальном времени передает координаты машины, данные о ее техническом состоянии и режиме использования в конкретный момент. В ближайшем будущем применение M2M на транспорте существенно расширится: недавно в Берлине, на конференции Qualcomm IQ-2012, компания Audi представила последнее поколение своих автомобилей, оснащенных системами определения дистанции и взаимодействия со светофорами по маршруту движения, передающими информацию на пункты сервисного обслуживания в реальном времени.

А. НАЗАРОВ: Готов поделиться забавным случаем. Несколько лет назад операторы, чего греха таить, любили запускать всякого рода лотереи. Одна машина, которая обслуживала лотерею, решила предложить сыграть в эту SMS-лотерею другой машине ☺. Та честно ответила, что команда не понята. В ответ на это первая бодро начислила ей некие бонусные баллы и предложила прислать в ответ еще одно SMS. В общем, этот датчик наверняка выиграл бы главный приз, так как диалог мог длиться бесконечно, но его удалось вовремя прервать...

Алексей ГЕРАСИМОВ, начальник отдела ВТ и телекоммуникаций, Роспромбанк: История с железками, которые играли в лотерею, случилась в нашем банке ☺.

А. НАЗАРОВ: Если серьезно, то в числе наших основных кейсов – мониторинг транспорта и других подвижных объектов, банкинг и платежные системы, системы безопасности, классическая телеметрия и другие сферы применения M2M-технологий, список которых растет год от года.



С. МЕЛЬНИК, НТЦ «Комсет»

Технологический фундамент



«ИКС»: Какие технологии и при каких условиях наиболее эффективны для обслуживания «железных» абонентов?

Сергей БАЛАШОВ, менеджер по продуктам телематических решений и сервисов, «ВымпелКом»: Будущее M2M, безусловно, за беспроводными технологиями: «фиксу» для удаленных объектов тянуть банально дорого, с подвижными объектами невозможно использовать в принципе, в то время как беспроводная связь гораздо проще и дешевле с точки зрения как организации, так и использования. Конечно, некоторые решения так навсегда и останутся фиксированными, например на крупных стационарных объектах, но это будет небольшая доля. В нашей практике наиболее распространена передача данных по GPRS, EDGE, 3G. На втором месте – SMS и как резерв – CSD (передача данных по голосовому каналу). CSD все еще распространена в России, что обусловлено либо устаревшим оборудованием, либо требованиями доступности – этот канал «отваливается» последним.



М. ВЕРЕЗУБОВ,
«АКАДО Телеком»

М. ВЕРЕЗУБОВ: Надо считать, что выгодно. У проводного оператора сеть есть в каждом доме, и он может предоставить услуги там, где отсутствует сотовая связь, – это подвалы, где, собственно, и находятся счетчики. Кроме того, он может предложить более выгодную цену. Это первое.

Второе. Мы работаем с сотней банков Москвы и области. Некоторые банки обращаются к нам с просьбой сделать резервный проводной канал для терминала в бизнес-центре, который уже оснащен сотовой передачей данных. Спрашиваешь, зачем. «На всякий случай» хотят иметь более качественный сигнал. Также необходимо учитывать объем информации, которую получа-



Ш. РЕЗНИКОВ,
«Интеллект-Телеком»

ет интеллектуальная машина. И после этого делать выбор.

Шагит РЕЗНИКОВ, директор департамента, «Интеллект-Телеком»: M2M M2M'у – рознь. На транспорте и в дистанционной медицине прежде всего востребована мобильная связь. А вот в ЖКХ не факт. Сейчас все фиксированные операторы строят GPON, EPON и т.д. Задача – добраться оптикой до квартиры. Здесь для компании-пользователя на первый план выходит и становится определяющей стоимость транзакции. По большому

счету неважно, как называется технология. Люди всегда будут считать деньги. Например, Мосгорэнерго имеет около 20 тыс. трансформаторных подстанций в городе и создала систему мониторинга расхода электроэнергии. Несмотря на то что у МОЭК в руках находятся все электрические сети и есть сети РЛТ, здесь все-таки остановились на мобильном решении, использующем сим-карты. Потому что для них это выгоднее.

Александр КРУПНОВ, президент, Инфокоммуникационный союз: Уместно вспомнить рекомендации МСЭ, который в развитии концепций M2M, умного дома и информационного общества давно обозначил приоритет беспроводных режимов, в том числе 3G и LTE. В пользу мобильных технологий говорит и соотношение мобильных и фиксированных абонентов в мире. И самое главное – частотный ресурс. По заключению мировых экспертов, для реализации глобальных задач человечеству нужно найти 1200 МГц спектра. Сегодня его нет нигде, ни в одной стране ☺. Эти разноплановые моменты надо учитывать при выборе технологических путей будущего.



А. КРУПНОВ,
Инфокоммуникационный Союз



«ИКС»: Какие характеристики сервисов M2M самые востребованные?

Сергей ПОНОМАРЕВ, директор по продажам, «Эшелон»: В аспекте противоугонных и мониторинговых систем первое и острое – это роуминг. Приходится находить какие-то решения: либо черный ящик, который накапливает события, пока нет связи; либо дорогостоящий тариф. Следующее – это зона покрытия и качество связи. Ведь если автомобиль находится вне связи, риск достаточно высок, потому что в этот момент автомобиль могут просто угнать. И мы вынуждены отвечать перед клиентом как оператор противоугонной системы.



С. ПОНОМАРЕВ, «Эшелон»

А. НАЗАРОВ: Среди всех характеристик я бы выделил вопрос стоимости решения, особенно в роуминге. Роуминг всегда был болевой точкой любого абонента, тем более абонента-машины, в этом случае проблема является чисто технической. Да, у нас есть хорошие тарифы, но если, например, M2M-устройство покидает пределы страны, продолжая работать, счет получается космическим. Для решения в том числе этой проблемы мы вошли в глобальный M2M-альянс, который объединяет семь мировых операторов связи. В рамках этого сообщества мы вместе прорабатываем тех-

ническое решение по автоматической смене профиля сим-карты при пересечении границы страны.



И. АСТАХОВ, МТС

Иван АСТАХОВ, руководитель группы развития М2М-решений, МТС:

По поводу роуминга. Мы уже сейчас имеем соглашение с Vodafone, правда, только на индивидуальной основе, и роуминг для М2М предоставляем на довольно выгодных условиях. По скорости передачи эта услуга отличается от того, что получают абоненты-люди (к сло-

ву, тарифы на передачу данных в Европе в разы выше, чем в России). Грубо говоря, мы переходим к разным уровням качества. Хотите полноценный сервис – это стоит дорого. Хотите дешево, низкую скорость и относительное покрытие – можем сделать, но соответственно и качество ниже. Думаю, операторам стоит на госуровне постараться решить вопрос о специальных принципах тарификации для М2М-абонентов, иначе одну и ту же сеть мы должны развивать под пользователей с очень разным объемом и характером трафика.

А. ГЕРАСИМОВ: Подключенная электронная книжка – это тоже М2М, вы согласны? У Amazon есть вариант платформы Kindle 3G, который работает за копейки, позволяя по 3G считывать kindle'овский кон-



А. ГЕРАСИМОВ, Роспромбанк

тент в любой точке мира. Контент там тяжелый, книжки по мегабайту. М2М-устройствам достаточно небольшой скорости, которая могла бы соответствовать копеечному тарифу. А пока по стране мы используем безлимитные опции тарифных планов операторов.

Илья ТИМОФЕЕВ, руководитель учебно-испытательного центра, «Вокзал-Инфоком»:

Мы с 2010 г. реализуем проект интегрированной комплексной системы безопасности в интересах Дирекции железнодорожных вокзалов ОАО «РЖД», где используются и М2М, и видеонаблюдение. На каждый вокзал из подключенных к проекту (Самара, Рязань-2, Смоленск, Новосибирск, Махачкала, Дербент и др.) заходит оптический канал 10–20 Мбит/с; резервный канал предусмотрен через маршрутизатор со слотом для сим-карты. Оператор центра мониторинга должен иметь возможность удаленно подключаться к камерам видеонаблюдения, участвовать в сеансах ВКС, получать сообщения по М2М от датчиков электроснабжения, температуры, влажности, задымления и т. д. При разрыве фиксированного канала связи (ТЗ это предусмотрено) по беспроводному сегменту должен пойти в основном трафик М2М и, как вариант, IP-телефония и ВКС. Нам важно регулирование качества услуг в зависимости от ситуации. Ведь если в случае ЧП лавина трафика обрушит фиксированный канал, то нагрузка ляжет на беспроводной, и приоритетный трафик пойдет по М2М-каналам.



И. ТИМОФЕЕВ, «Вокзал-Инфоком»



«ИКС»: Каковы перспективы технологий 3G и LTE для М2М-решений?

И. АСТАХОВ: Сети LTE еще строятся, покрытие небольшое, поэтому использование их в целях М2М ограничено. Есть сим-карты, использующие 3G, преимущественно для видеонаблюдения. Тормозит развитие то, что модем GPRS стоит до \$20, а 3G – \$60–100. Разумеется, компании экономят на оборудовании. Зарубежные эксперты прогнозируют, что и в 2016 г. 2G-модули будут все еще до-

минировать в М2М, 3G составят порядка 20% всего количества сим-карт. Разумеется, в 3G больше возможностей управления качеством обслуживания, выделения приоритетов и т.д. Если потребителям нужны качество сервиса, SLA, сбор информации с многих датчиков и ее моментальная передача, например в умном доме, то межмашинное взаимодействие в 3G это позволяет сделать.

Cui prodest



«ИКС»: Вряд ли кто будет возражать, что рынок М2М – это территория партнерства. Кто контролирует цепочку добавленной стоимости в этом сегменте? Как видоизменяются роли игроков?

Ш. РЕЗНИКОВ: Роль оператора важна, но во многих сегментах не определяющая. Трафик и сим-карты – далеко не все, что необходимо для запуска М2М на транспорте, в ЖКХ, телемедицине. Должны быть игроки, которые этот бизнес продвигают и используют то, что дают операторы. Например, почему не идет на ура очевидная задача мониторить все счетчики, которые есть в наших домах, все расходы ресурсов? Потому что нет компании, которая непосредственно на этом зарабатывает.

Телемедицина: о ней много говорится, но она существует в виде фрагментов. Потому что основные игроки во всем мире, которые играют на этом поле, а это в первую очередь страховые компании, еще спят. Да и на транспорте пока непонятно, кто должен это двигать. Государство, на мой взгляд, может этот момент регулировать путем постановки конкретных целей и сроков их выполнения.

С. МЕЛЬНИК: По оценкам М2М Global Alliance, для успеха проекта М2М в нем должны участвовать как ми-

нимум пять-шесть сторон: оператор, системный интегратор, транснациональные корпорации, которые являются основными потребителями M2M-трафика, обязательно соинвесторы, производители M2M-устройств, наконец, сервис-провайдеры.



С. БАЛАШОВ, «ВымпелКом»

С. БАЛАШОВ: «ВымпелКом» еще два года назад взял курс на то, чтобы в M2M развиваться как минимум в двух направлениях: продолжать свой основной бизнес – передачу данных, предлагая дополнительные услуги, и параллельно расширять охват этой цепочки ценностей, выступая в роли сервис-про-

вайдера, как делает ряд международных операторов, привлекая в качестве партнеров системных интеграторов.

Михаил КАШТАНОВ, ведущий специалист, «Геолоайф»:

Если раньше роль сервис-провайдера заключалась только в обслуживании своего узкого сегмента рынка, то сейчас от предложения конкретных, хорошо отработанных пакетов услуг происходит переход к совместному созданию новых сегментов рынка, именно в партнерстве с операторами и другими участниками.



М. КАШТАНОВ, «Геолоайф»

Бизнесу нужны правила



«ИКС»: Каковы регуляторные проблемы в секторе M2M? Как государство может помочь продвижению и развитию сегмента M2M?

В. АФАНАСЬЕВ: Европейский институт стандартизации в области связи имеет в своем составе два комитета – TS и TR, которые занимаются нормативным полем в области телематики, M2M. Нормативное поле России не соответствует тем документам, которые там создаются. Та же ситуация на межотраслевом уровне: документы, которые принимаются в здравоохранении или в сельском хозяйстве, не имеют «выходов» на сеть телематических услуг.



В. АФАНАСЬЕВ, фонд «Инвестиции в Инновации & Технологии»

Нормативное регулирование должно быть. Оно мало того что дает целеуказание. Оно еще и обязывает, в том числе и государство, следовать правилам, гарантирует отсутствие действий и документов «обратной силы». Нормативное регулирование должно обеспечить, например, достоверность информации и качество услуг в телемедицине,

чтобы к этой сфере было доверие в профессиональном сообществе и у пациентов. Если нам не хватает частотного ресурса, надо привлечь науку, определить новые направления, скоординировать их с мировыми. Нужна отраслевая и межотраслевая координация, комплексные концепции и планы.

С. МИШЕНКОВ: Разговоры о том, что объемы информации не имеют предела, наивны. Предел есть. Особенно для информации, которая полезна обществу. Честное слово, мне безразлично, в каком месте находится электрон в Альфе Центавра. И в ближайшую тысячу лет будет то же самое. Значит, требуемый объем полезной информации чем-то ограничен, правда? И вот давно пора операторам хотя бы для себя решить (но и другим сказать), какие объемы информации им будут нужны сегодня, завтра и через десять лет. И не

только по транспорту, по другим вопросам тоже! Иначе это выброшенные деньги.

С. МЕЛЬНИК: Есть действующие законы «О связи», «О техническом регулировании», «Об обеспечении единства и точности измерений». Если мы обратимся к букве этих законов, то увидим, что к области госрегулирования в сфере ИКТ относится регулирование, касающееся целостности, устойчивости и безопасности единой взаимоувязанной сети связи. Качество услуг связи, о котором мы сейчас говорим, не входит в область регулирования Минкомсвязи.

С одной стороны, государство говорит, что мы движемся к уменьшению роли госрегулирования, и хочет переложить ответственность на бизнес. А бизнес говорит о необходимости госрегулирования. Ничего сверхъестественного в этом нет – бизнесу нужны правила. Бизнес без правил очень дорогой. Применение стандартных решений всегда дешевле, чем разработка каждый раз новых. Кроме того, регулирование и разработка стандартов – удовольствие недешевое. Если каждая операторская компания будет работать по своим собственным стандартам, то не будет той самой целостности, которая нужна для стабильности работы сетей связи.

В рамках действующих законов эту роль разработки общих правил и стандартов могли бы взять на себя общественные организации, такие как Инфокоммуникационный союз или Международная академия информатизации, которые имеют для этого и требуемые интеллектуальные возможности.

А. НАЗАРОВ: Полностью поддерживаю: действительно, работать без стандартов очень дорого.

Подготовила **Наталья КИЙ**



С. МИШЕНКОВ, Минкомсвязь России

NB! Отличный клиентский опыт

В создающейся цифровой экономике клиентский опыт, т.е. опыт восприятия клиентом компании, ее продуктов и услуг, начинает определять успех или поражение в конкурентной борьбе.



Кит УИЛЕТТС,
председатель,
TM Forum

В цифровом мире самообслуживание – это норма. Клиенты, видя ваши сервисы так близко, что не остается потаенных мест, находятся при этом лишь в одном клике от ваших конкурентов. Формирование у клиентов хорошего впечатления – жизненно важная часть поддержания их лояльности. Оно выделит вас среди соперников, позволит создать сильный цифровой бренд и тем самым даст возможность устанавливать более высокие цены. Если клиенты чувствуют, что получают больше, они согласны больше платить – вот почему прибыли у Apple выше, чем у многих ее конкурентов.

Лояльные клиенты делятся впечатлениями с друзьями, и положительный опыт отзывается не в одном клиенте, а во многих. К сожалению, эта цепная реакция работает и в обратную сторону – о своем разочаровании клиент расскажет друзьям через блоги, Facebook и Twitter, а те – своим друзьям, и вскоре кто-нибудь запустит веб-сайт, куда выложит всю нелицеприятную информацию о вашей деятельности!

Эта цифровая цепная реакция очень важна: делайте все, как надо, и лояльность к бренду и доходность вырастут, отток клиентов уменьшится. При неверных действиях результатом будут неудовлетворенность клиентов, проблемы, разочарование, раздражение, ненужные траты, обесценивание бренда и потеря клиентов.

Компании, которые активно управляют клиентским опытом и инвестируют в него, поступают так, потому что руководствуются трезвым чувством бизнеса – привлечь клиента стоит дорого, и если вы потеряете его, а вслед за ним и других, то деньги будут потрачены зря. Клиентоориентированная организация – это та, у которой при принятии любого решения клиент находится на первом месте. Тем не менее руководители часто принимают решения, которые, казалось бы, не касаются клиентов напрямую, но очень негативно на них влияют.

Хороший клиентский опыт не появляется случайно

Хорошее или плохое впечатление не возникает у клиента само по себе: это следствие корпоративного духа компании и общей суммы взаимодействий с клиентом. Хороший клиентский опыт должен тщательно проектироваться и управляться так, чтобы каждая точка соприкосновения с клиентом была оптимальной – в противном случае вы ежемесячно рискуете потерять клиента и его друзей. Отправная точка может быть очень проста: **избавиться от того, что раздражает клиента.** Но чтобы соперничать с лучшими, следует стремиться **делать то, что доставляет клиентам удовольствие.**

Чтобы справиться с этой задачей, необходимо ясно представлять себе, что раздражает и что восхищает клиентов. В основе этого лежат анализ данных и бизнес-метрики, но абсолютных критериев для подобных вещей нет – они все время меняются по всему миру в зависимости от культуры и ожиданий и, как правило, от влияния других компаний, устанавливающих планку, относительно которой вы и делаете оценку.

Слишком часто корпорации руководствуются только внутренними интересами, когда каждый департамент стремится к своей собственной цели с небольшой долей заботы о клиенте. Именно по этой причине Стив Джобс отказался в Apple от постановки целей отдельных подразделений в пользу глобального подхода.

Не только говорите, но и делайте!

Компании, подобные Apple и Amazon, которые обеспечивают своим клиентам прекрасный пользовательский опыт, часто обсуждаются на конференциях и во многих статьях, например в этой. Однако, когда люди возвращаются к своей обычной работе, мало что меняется, если вообще меняется, за исключением случаев, когда есть сильное, дальновид-

У многих
компаний,
в том числе
у большинства
операторов связи,
физическое
взаимодействие
с клиентом –
это белое пятно

ное руководство и четкое указание поступать именно так.

Самоуспокоенность, высокомерие и просто плохой менеджмент можно пережить, когда конкуренция слабая, но поскольку цифровой торнадо набирает силу, бизнесу, который не обеспечивает того, что хотят клиенты, пощады, похоже, не будет. Раз и навсегда загладить плохое впечатление, произведенное на клиента, нельзя, и конечные пользователи легко могут вас покинуть, а вернуть себе репутацию компании, пекущейся о качестве и хорошем клиентском опыте, – задача непомерно сложная.

Пробуйте на себе

Опасность того, что клиентоориентированность будет поддерживаться только на словах, весьма реальна. Эту проблему не решить одной лишь воодушевляющей речью генерального директора. Важно, чтобы намерения подкреплялись действительными изменениями. Часто это означает фундаментальное переосмысление всей деятельности компании, которая так или иначе затрагивает клиента.

Также важно видеть жизнь глазами пользователя. Для этого персоналу и, что еще важнее, высшему руководству нужно попробовать потреблять продукты и услуги компании тем же самым способом, что и клиенты. А когда что-то случается, вместо того чтобы заходить «с заднего крыльца» и использовать неформальные пути решения проблем, персоналу необходимо действовать через обычные клиентские каналы и почувствовать, как вашу деятельность воспринимает клиент. Часто это очень показательно.

Плохо спроектированные веб-сайты и интерактивные системы голосового ответа – среди наиболее заметных источников раздражения клиентов. Внедренные для снижения расходов, они зачастую просто ужасны в качестве начала взаимодействия или разговора. Они бывают не только утомительны – иногда они не протестированы надлежащим образом и заводят вас в никуда. Когда вы в последний раз просматривали веб-сайт своей компании или звонили оператору в колл-центр?

Превращение свинца в золото

Непосредственный клиентский опыт, полученный вашими работниками, мо-

жет быть очень полезен, но есть много других источников сведений, которые также следует использовать. Фактически каждый аспект опыта клиента зависит от точности и доступности информации – огромного источника богатства, если вы сумеете правильно им распорядиться. Извлечение из незначащих данных полезной информации – это реализованная в 21-м веке мечта алхимиков о превращении свинца в золото.

Информация на кончиках пальцев о том, что в данный момент делают ваши клиенты, чего они сейчас хотят и к чему могут быть восприимчивы, станет огромным преимуществом, если вы сможете ею воспользоваться. Она позволит вам намного лучше понимать, как преподносить и позиционировать свои сервисы или сделать предложение в режиме реального времени – контекстное или основанное на местоположении. Вы получите ценную информацию, которая может быть монетизирована и для других клиентов.

Необходим проактивный и быстрый анализ того, что хочет клиент. Подходящие предложения в режиме реального времени, поддержка клиента в режиме реального времени и обработка в режиме реального времени могут оказать положительное влияние на опыт клиента и на итог взаимодействия с ним. Распутывать запутанную как спагетти информацию – задача сложная, но хорошее управление данными – ключевая компетенция успешного цифрового провайдера. Таким образом, инвестиции в интеллектуальные инструменты бизнес-аналитики помогают предложить клиентам высокоперсонализированную поддержку, хотя здесь важно не забывать о доходности.

Так что не случайно две самые «горячие» области в управлении клиентским опытом – это **анализ данных**, который помогает провайдерам понимать, что происходит, и **управление политиками**, которое помогает последовательно решать проблемы по мере их возникновения. Если данные – это основа хорошего клиентского опыта, то аналитика – это мозг, который преобразует данные в полезную информацию, а управление политиками – руки, которые выполняют работу.

Не забывайте, что клиенты часто имеют свои особенности и их персональный состав разнообразен; они могут ис-

пользовать ряд услуг совместно и при этом взаимодействовать с вами по разным каналам. Они могут находиться на работе или пользоваться услугами для себя лично, и в каждом из этих случаев у них будут разные ожидания. Еще труднее сформировать единый взгляд на клиента, когда отдельные департаменты используют разные идентификаторы клиентов или разные форматы. Но будьте уверены, пользователи быстро составят коллективный взгляд на неразбериху в вашем обслуживании!

Отсутствие единого мышления становится очень заметно в случае мультиканальных продаж, и клиенты начинают сильно раздражаться, когда получают различную информацию с сайта, из магазина или при разговоре с агентом. У этих каналов могут быть разные цены на один и тот же продукт или они могут относить его к разным продуктовым линейкам и предложениям, поскольку они находятся в ведении разных подразделений. В этом случае клиенту громко и четко заявляется, что провайдер не является единой организацией и не имеет профессиональных навыков в управлении клиентским опытом.

Доверие – главный приз

Все более актуальным и важным моментом для клиента становится конфиденциальность данных. Поскольку компании могут извлечь большие выгоды из клиентских данных, к их администрированию нужно относиться с должным вниманием, если провайдер собирается завоевать и сохранить доверие клиента.

Такие компании, как Facebook, LinkedIn и Sony, уже ощутили на себе, что ничто не вызывает такого шума в прессе, как потеря данных клиентов, и ничто не утрачивается так быстро, как их доверие. Вялые отклики типа «мы извлекли уроки из случившегося», в общем, не исправляют ситуацию, а повторные инциденты приводят к быстрой потере доверия клиента. Потеря доверия влечет за собой потерю лояльности, а это прямая дорога к забвению.

Витрина цифрового магазина

Розничный магазин – это лучшее место, где клиент провайдера может получить адекватный личный опыт. Отличным примером является компания Apple – ее магазины «заточены» не столько на продажу товаров, сколько на усиление бренда, его узнаваемость и формирование положительного опыта клиентов.

Но зачастую магазин способен только укрепить в мысли, что компания мало заботится о своих клиентах. У многих компаний, в том числе у большинства операторов связи, физическое взаимодействие с клиентом – это белое пятно. Спроектированные, возможно, исходя из специфических соображений выгоды, их магазины, как правило, плохо продуманы. Это унылые места, где используется множество запутанных технологий, они укомплектованы мрачными сотрудниками, которые зачастую мало знают о предлагаемых продуктах и услугах. Влияние таких магазинов на общее восприятие клиентами компа-

нии и ее бренда может быть огромным, но слишком часто отправной точкой является образ мышления подразделения, а не впечатление, производимое на клиента.

Хороший, плохой и ужасный

В цифровом мире витрина часто виртуальная и связана с социальными сетями. То, как вы реагируете на это, – ключевой фактор обеспечения хорошего клиентского опыта: все любят слушать, что говорят о них клиенты, если отзыв хороший, но если он негативный, то многие сразу отключаются и начинают объяснять, почему клиент неправ. Несмотря на то, что это может быть болезненно, слушать, когда о вас говорят хорошо, плохо или даже ужасно, просто необходимо для понимания того, что же надо изменить, чтобы направить клиентов по пути суперлояльности.

Легко сосредоточиться на негативных аспектах социальных сетей, но они могут быть использованы и для формирования у клиентов положительного отношения к вашим продуктам и услугам. Также они служат прекрасным средством узнать, что говорит о вас рынок.

Хороший пример – американский телеком-провайдер Comcast, который сумел превратить кошмар шумихи в социальных сетях и СМИ в триумф ComcastCares, своей службы поддержки абонентов на основе Twitter (в 2004 и 2007 гг. Comcast имел наилучший рейтинг удовлетворенности клиентов среди компаний и госорганизаций США, а в 2008 г. вошел в десятку лучших по этому показателю. – Прим. ред.). Его совет: **«Не удаляйте онлайн-критику, примите ее»** и, конечно, реагируйте на нее. Умение слушать, видеть проблемы и разбираться с ними сделало чудеса с имиджем Comcast.

Искусство и наука

В мире высоких технологий, каким становится наш мир, порой появляется искушение считать, что для каждой проблемы существует технологическое решение. И хотя анализ данных и управление политиками очень важны, но правильное управление опытом клиента – столько же искусство, сколько наука. Ведь вы имеете дело с людьми – их эмоциями, предрассудками и слабостями. Если центральное место во всех решениях, принимаемых вами и хоть в какой-то мере затрагивающих клиента, занимает не клиент, то вряд ли вы достигнете успеха.

В цифровом мире клиент – несомненно, король, и самый очевидный путь к прибыльности заключается в том, чтобы сделать клиентов, их друзей и семьи лояльными к вам, никогда их не разочаровывая и всегда обеспечивая по-настоящему прекрасный клиентский опыт.

В противном случае ждите провала! ИКС

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

Северный плацдарм для выхода на российский рынок

TelecityGroup, ведущий европейский оператор независимых от провайдеров дата-центров премиум-класса (их у компании 35), выходит на российский рынок. О том, почему было принято такое решение и что компания намерена предложить заказчикам в России, – Сами ХОЛОПАЙНЕН, директор по продажам TelecityGroup Finland.



Сами
ХОЛОПАЙНЕН

– В 2012 г. TelecityGroup приобрела двух ведущих финских операторов дата-центров с нейтральной доступностью – Teline Oy и Asademica Oy. ЦОДы, полученные компанией в результате поглощения, не только дают возможность свободного выбора поставщиков телекоммуникационных услуг, но и отличаются уникальным расположением – в непосредственной близости от российской границы.

Мы полагаем, что наряду со стремительным развитием индустрии ЦОДов в Западной Европе такие развивающиеся рынки, как Россия и Азия, обладают значительным потенциалом роста. Для TelecityGroup Северная Европа – это стратегически важное местоположение для предоставления полного комплекса услуг дата-центров и ИТ-услуг нашим клиентам из России, стран Балтии и Скандинавии. В Финляндии оптимальные климатические условия и географическое положение для строительства и обслуживания высококласных ЦОДов. Еще одним преимуществом является наличие развитой телеком-инфраструктуры, соединяющей Финляндию с соседними странами.

Как отметил генеральный директор TelecityGroup Finland Марко Ваннинен, мы видим повышенный интерес клиентов компании к высококачественным услугам дата-центров с нейтральной доступностью, расположенных рядом с находящимся на пике развития российским рынком. В TelecityGroup выход на этот рынок рассматривается как важная перспектива роста.

– Каких заказчиков вы планируете привлечь в России? В чем будут ваши конкурентные преимущества?

– Целевыми сегментами рынка для нас являются, например, операторы связи, контент-провайдеры и крупные и средние компании, которые нуждаются в надежной ИТ-инфраструктуре.

Наши конкурентные преимущества – это широкие возможности подключения, высокая эффективность логистики, информационная безопасность, профессионализм сотрудников.

Площадки TelecityGroup – одни из лучших в плане гибкости и ассортимента возможностей подключения. Для дата-центров коннективность связи – ключевой элемент. Нет высокоскоростной сети передачи данных – нет и бизнеса. Несмотря на новые технологии, постоянно появляющиеся на

рынке, скорость передачи данных по оптоволокну имеет свои пределы, что придает первостепенное значение тому, где находятся ваши данные. Меньше время ожидания – лучшее качество услуг.

Кроме эталонной инфраструктуры ЦОДа большую роль для нас играет организация эффективной логистической системы. Мы берем на себя организацию приезда специалистов компании-заказчика и доставку оборудования, гарантируя легкую доступность и 100%-ную надежность.

Очевидно, что при передаче критически важной бизнес-информации должна соблюдаться конфиденциальность. В ЕС и особенно в Финляндии законодательство в области защиты информации очень строгое. Секретность передачи информации в форме письменной и электронной корреспонденции или звонков, защита другой конфиденциальной информации прописана в Конституции Финляндии. Подобная защита охватывает все потоки информации, передаваемые через средства коммуникации.

TelecityGroup гордится своей профессиональной командой, служащей гарантом того, что ваша ИТ-инфраструктура круглосуточно доступна и надежно защищена.

Немаловажное обстоятельство: страны Северной Европы, где мы работаем, отличаются экономической и политической стабильностью. Это делает бизнес-планирование проще и сводит к минимуму такие неприятные сюрпризы, как неожиданные изменения в сфере регулирования бизнеса.

У Telecity имеется программа по расширению мощностей, одна из самых широкомасштабных в Европе. За счет расширения присутствия в европейских странах мы всегда можем обеспечить наших клиентов мощностями, необходимыми для их развития и достижения бизнес-целей. Множество площадок с грамотным расположением и тщательно подобранными вариантами подключения гарантирует гибкость при поддержании вашего роста и расширения.

Все наши дата-центры отвечают требованиям Tier 3 по стандартам Uptime Institute. Ценовая политика компании призвана обеспечить конкурентоспособность наших услуг и прежде всего учитывает фактическое использование ресурсов и мощностей.

– Каковы ваши ближайшие планы работы в России? Какие инвестиции здесь запланированы?

– Для TelecityGroup Финляндия – это своего рода плацдарм для выхода на рынки России и Прибалтики. В ближайшем будущем наша компания продолжит инвестировать средства в завоевание новых конкурентных позиций на российском рынке и укрепление позиции Хельсинки как ключевого международного интернет-хаба.

Приоритетными направлениями для нас являются, во-первых, удовлетворение растущего спроса на услуги по

размещению оборудования со стороны компаний, нуждающихся в связующем звене (service gateway) между Европой и Россией. Во-вторых, это предоставление наилучшего с точки зрения логистики расположения ЦОДа для российских клиентов в пределах ЕС и основы для европейских/американских компаний, ведущих свою деятельность рядом с российской границей и нуждающихся в современной телеком-инфраструктуре между Европой и Россией, с разнообразием способов подключения, малым временем ожидания и мощными оптоволоконными сетями связи.

– **Есть ли в ваших европейских дата-центрах российские клиенты?**

– Да, у нас много российских заказчиков, которые пользуются услугами наших дата-центров по всей Европе. Среди них ведущие телеком-операторы, контент-компании, крупные корпорации и предприятия среднего звена. Наши клиенты особенно высоко ценят надежность размещения оборудования в ЦОДах TelecityGroup, простоту логистики, а также масштабируемость решений, способных удовлетворять основные нужды международного бизнеса. Также для них важно, что TelecityGroup – заслуживающий доверия партнер, соблюдающий все договоренности. Другими словами, компании, которым доверяете вы, доверяют нам.

– **Какие услуги вы предоставляете в своих дата-центрах? Какие услуги, по вашему мнению, должны привлечь российских заказчиков? Планируете ли запускать какие-то новые сервисы?**

– В основе всей нашей деятельности – услуги размещения оборудования (colocation) и хостинга. Наша инфраструктура премиум-класса и отличные возможности подключения – залог высокого качества предоставления данных услуг.

Одним из наиболее интересных направлений нашей работы на российском рынке будет аварийное восстановление и защита данных. Полное резервирование ИТ-инфраструктуры компаний при помощи услуг аварийного восстановления на базе наших площадок в Северной Европе может оказать критически важным для непрерывного функционирования бизнеса заказчика в случае отказа в функционировании основного ЦОДа.

Наши эксперты готовы сориентировать заказчика по вопросам проектирования, модернизации и переноса дата-центра, а также познакомить его с другими нашими услугами, повышающими производительность хостинг-среды наших клиентов.

Мы предоставляем полностью резервированное подключение к интернету посредством нашей услуги IP Multihome либо возможность воспользоваться управляемой сетью Ethernet для консолидации ИТ-ресурсов в наших дата-центрах по всей Европе.

Наша многоуровневая система поддержки обеспечивает эффективность функционирования ИТ-инфраструктуры заказчика. Удаленное администрирование позволяет полностью обойтись без присутствия специалистов компании-клиента в дата-центре.

Кроме того, в наших ЦОДах обеспечивается полностью автоматизированное и управляемое резервное копирование и восстановление данных с диска на диск, с узлами хранения во множестве дата-центров. А наши услуги распределения нагрузки и управления серверами помогут повысить производительность ИТ-инфраструктуры и поддерживать ее на нужном уровне.

Время ожидания в сети

Хельсинки – Санкт-Петербург	8 мс
Хельсинки – Стокгольм	8 мс
Хельсинки – Амстердам	28 мс
Хельсинки – Франкфурт	35 мс
Хельсинки – Нью-Йорк	107 мс



– **Работаете ли вы на рынке облачных сервисов? Как вам представляется место оператора дата-центров на этом рынке? Какие перспективы в этой сфере вы видите для себя?**

– Сегодня компании все больше заинтересованы в облачных решениях. По своей природе облака требуют прочного фундамента для непрерывного функционирования. Они нуждаются в высококлассных и предлагающих различные варианты подключения ЦОДах, которые позволили бы компаниям-заказчикам и провайдером облачных сервисов свести к минимуму рост издержек, перенаправить ресурсы, нацеленные на администрирование и модернизацию оборудования, и сосредоточиться на профильном виде деятельности.

Помимо размещения оборудования в наших эталонных дата-центрах мы предлагаем решение «Инфраструктура как услуга» на базе динамического дата-центра (Dynamic Data Centre, DDC). Благодаря DDC мы можем предложить динамическую, полностью виртуализированную среду ИТ-инфраструктуры, масштаб которой можно с легкостью увеличивать или уменьшать и цена которой меняется в зависимости от потребностей заказчика. DDC позволяет сочетать элементы физической и виртуальной инфраструктуры для удовлетворения особых требований клиентов, а также при необходимости дает возможность выхода в DDC из colocation-среды TelecityGroup.

У нас широкий спектр потенциальных заказчиков. Разработчики облачных сред, провайдеры контента (в том числе мобильного), представители индустрии игр, компании, которым требуется гибкость и масштабируемость вычислительных ресурсов либо услуги аварийного восстановления, – все они заинтересованы в наших облачных решениях. Всем этим игрокам в конечном счете нужны ЦОДы с разнообразными вариантами подключения и малым временем ожидания.

Киберзащита конЦЕНТРируется

Для противодействия кибератакам во всем мире создаются центры реагирования на компьютерные инциденты – и Россия не исключение. Сотрудничество таких центров может сделать их работу заметно эффективнее.



Дмитрий КОСТРОВ,
ассоциированный
репортер
группы ИК 17,
МСЭ-Т

Центры реагирования в России

В настоящее время создается GOV-CERT.RU – центр реагирования на компьютерные инциденты в информационно-телекоммуникационных сетях (ИТС) органов государственной власти РФ, призванный решать следующие задачи: оказание консультативной и методической помощи при проведении мероприятий по ликвидации последствий компьютерных инцидентов в ИТС органов государственной власти; анализ причин и условий возникновения инцидентов в ИТС органов государственной власти; выработка рекомендаций по способам нейтрализации актуальных угроз безопасности информации; взаимодействие с российскими, иностранными и международными организациями, отвечающими за реагирование на компьютерные инциденты; накопление и анализ сведений о таких инцидентах.

Кроме того, в России уже действуют три аналогичных центра – CERT-GIB, WebPlus ISP и RU-CERT. Первый из тройки был создан совсем недавно, его основатель – компания Group-IB. Это частный центр реагирования, обслуживающий сторонние организации, но претендующий на звание «прогосударственного», так как именно с ним Координационный центр национального домена сети Интернет заключил соглашение о противодействии киберугрозам в доменах .RU и .RF (наряду с подразделением Лиги безопасного Интернета – фондом «Дружественный Рунет»). Центр работает в режиме 24x7 и оказывает услуги (на основе абонентского договора или договора оферты) реагирования на следующие типы инцидентов: отказ в обслужива-

нии (DoS, DDoS), компрометация информации, компрометация актива, внутренний или внешний несанкционированный доступ, создание и распространение вредоносного программного обеспечения, нарушение политик информационной безопасности, фишинг и незаконное использование бренда в интернете, мошеннические действия с системами ДБО и электронными платежными системами.

Центр WebPlus ISP CERT занимается обслуживанием только собственных ресурсов.

Четвертый центр, RU-CERT (Russian Computer Emergency Response Team) – это автономная некоммерческая организация «Центр реагирования на компьютерные инциденты», официально зарегистрированная как Computer Security Incident Response Team (CSIRT). RU-CERT занимается сбором и анализом информации по фактам компьютерных инцидентов (попыток или фактов нарушений российского законодательства или принятых международных нормативных правовых актов при обработке информации в открытых телекоммуникационных сетях, которые имеют отношение к сетевым ресурсам, расположенным на территории Российской Федерации), а также реагированием на них с целью выявления, предупреждения и пресечения подобной деятельности на территории РФ. RU-CERT на территории России также выступает в качестве контактной стороны для всех пользователей, которым необходимо содействие в обращении к российским интернет-провайдерам и официальным государственным структурам, проводящим предусмотренное российским законодательством расследование компьютерных преступлений. При этом RU-CERT не обладает правами на прекращение деятельности лиц, причастных к компьютерным инцидентам, закрытие ресурсов, блокирование адресов и т.п.

Кроме того, в настоящее время создается межотраслевой CSIRT на базе Ассоциации руководителей служб информационной безопасности.

Национальные центры: сотрудничество ради безопасности

Недавно в МСЭ-Т была принята международная рекомендация (проект которой активно продвигала Россия) X. NCNS-1 – Supplement on guidance for creating national IP-based public network security center for developing countries («Руководство по созданию Национальных центров безопасности сети связи общего пользования, базирующейся на протоколе IP, для развивающихся стран»). Рекомендация ориентирована на содействие обеспече-

нию безопасного и устойчивого функционирования национальной ИКТ-инфраструктуры, включающей сети операторов подвижной и фиксированной связи и национальный сегмент сети интернет. Ее концептуальный принцип – сотрудничество ради безопасности.

Рекомендация описывает структуру Национального центра и схему его внешних связей. Составляющие Рекомендации – организация функционирования межоператорской группы анализа инцидентов (МЕГА), интеграция функциональных компонентов и компонентов обеспечения безопасности, формирование координирующих воздействий для обеспечения непрерывности оказания услуг в рамках национальной ИКТ-инфраструктуры гражданам, бизнесу и органам государственной власти как в повседневном режиме работы, так и в условиях чрезвычайных ситуаций природного и техногенного характера.

В Рекомендации также описываются модели работы Национальных центров, которые можно использовать для обеспечения защищенности, стабильности и восстанавливаемости национальной ИКТ-инфраструктуры развивающихся стран, работающей на основе протокола IP. Эти модели могут быть федеративными или виртуальными и имплементироваться по отдельности или комбинированно. В рамках одного государства могут функционировать несколько подобных равнозначных центров.

Последовательное применение принципа «Сотрудничество ради безопасности» приводит к формированию распределенной, федеративной интеграционной среды (ФИС), или так называемого федеративного пространства доверия, где размещаются сервисы, доступные всем участникам системы коллективной безопасности на национальном уровне.

Наличие такой федеративной интеграционной среды обеспечивает операторам возможность присоединения к ней, размещения своих сервисов и получения доступа ко всем сервисам безопасности, развернутым в ФИС другими операторами и администрацией NCNS. Федеративная интеграционная среда организуется в виде стека управляющих плоскостей (control planes): Security Control Plane, Information Exchange Plane, Service Exchange Plane.

Принципы создания NCNS

NCNS проектируется и формируется как система организационно-технического управления национальной ИКТ-инфраструктурой в процессе межоператорского взаимодействия и включает и уже существующие центры управления сетями связи (NOC/SOC), и вновь создаваемые центры управления безопасностью операторов связи. NCNS обеспечивает координацию как в повседневной деятельности, так и во время чрезвычайных ситуаций.

Формирование NCNS предполагает создание специального пула операторов связи, отобранных и сертифицированных в соответствии с национальными требованиями и/или международными X.Sup2: ITU-T X.800-X.849 series – Supplement on security baseline for

network operators. Применение открытых и формализованных процедур и условий отбора операторов связи способствует расширению круга участников взаимодействия.

В основе создания NCNS лежат архитектура и методика организации и сопровождения системы поддержки операционной деятельности во взаимодействии с центрами управления сетями связи NOC/SOC, составляющими национальную ИКТ-инфраструктуру. Такой подход предполагает, что NCNS создается как распределенная система межоператорского взаимодействия.

В состав NCNS входят администрация центра, подразделение мониторинга и управления информационной безопасностью, подразделение анализа и развития. К функциям подразделения мониторинга и управления ИБ относят:

- создание и ведение базы данных по инцидентам безопасности на сетях связи, поддержка ее в актуальном состоянии;
- информационная поддержка протокольного обмена событиями безопасности и положительными практиками противодействия с другими центрами сетевой безопасности и с центрами безопасности взаимодействующих операторов;
- контроль (с применением технических и программных средств) состояния информационной безопасности сетей и систем существенных операторов;
- взаимодействие с оперативными подразделениями операторов при локализации и устранении аварий на сетях связи, вызванных деструктивными воздействиями на сеть и ресурсы систем управления сетью связи;
- организация взаимодействия с центрами безопасности взаимодействующих операторов при отражении массовых атак на системы управления сетями связи;
- организация взаимодействия с центрами компетенций и службами поддержки компаний – производителей телекоммуникационного и сетевого оборудования.

В функции подразделения анализа и развития входит:

- разработка нормативно-методической базы безопасности национальной ИКТ-инфраструктуры;
- анализ угроз безопасности и формирование мер и рекомендаций по противодействию им;
- формирование базы лучших практик и рекомендаций по обеспечению безопасности и реагированию на инциденты безопасности;
- разработка технических решений и сопровождение проектов и работ по информационной безопасности на сетях связи и информационных ресурсах;
- сертификация присоединяемых операторов.

Объектами информационного взаимодействия NCNS являются центры управления безопасностью операторов связи, другие NCNS, организации федеральных регуляторов в области безопасности и связи, центры ре-

агирования на инциденты безопасности (CERT, CSIRT, CIRT) и другие структуры, заинтересованные в повышении устойчивости сетей связи (вендоры, общественные организации и т.д.).

В целях информационного обмена NCNS с внешними объектами может быть использован весь спектр механизмов обмена информацией о событиях. В случае центров управления безопасностью операторов связи это протоколы взаимодействия, поддерживаемые операторскими системами управления и автоматизированными системами управления инцидентами. Для других NCNS предназначен новый протокол обмена, отвечающий требованиям взаимодействия NCNS. Обмен с организациями регуляторов в области безопасности и связи происходит в соответствии с национальным законодательством и особенностями технического оснащения регуляторов. Для взаимодействия с центрами реагирования на инциденты безопасности (CERT, CSIRT, CIRT и т.д.) используются механизмы обмена информацией, указанные в Рекомендации X.1500 (CYBEX). В случае вендоров, общественных и других организаций, заинтересованных в повышении устойчивости сетей связи, протоколы обмена целесообразно определять по договоренности с ними.

NCNS ведет собственную электронную базу данных об угрозах и методах защиты (с учетом национальных нормативных актов в части защиты конфиденциальной информации). Для автоматизации деятельности NCNS используется совокупность технических и программных средств.

МЕГА-подробности

Межоператорская группа анализа инцидентов (МЕГА) представляет собой архитектурную составляющую NCNS, выделенную для сбора, обработки и обмена информацией об инцидентах и событиях безопасности между операторами связи, потребителями услуг связи, производителями оборудования, государственными органами, а также для ведения базы данных «лучших практик» по выделенным инцидентам ИБ*.

Цель создания МЕГА – консолидация усилий по выявлению угроз информационной безопасности (кибербезопасности) национальной ИКТ-инфраструктуры, обнаружению и локализации инцидентов, относящихся к сфере информационной безопасности, принятию мер по устранению негативных последствий инцидентов и их недопущению в дальнейшем.

МЕГА формирует и рассылает присоединенным к NCNS операторам связи рекомендации по обеспечению базового уровня информационной безопасности (ITU-T X.800-X.849 series – Supplement on security baseline for network operators); проводит экспертизу и мониторинг инфокоммуникационных систем (по запросу) операторов связи на наличие уязвимостей и выдает рекомендации по их устранению и повыше-

нию уровня устойчивости предоставления услуг; оказывает поддержку пользователям – операторам связи в повышении устойчивости и информационной безопасности (консультирует их по вопросам борьбы с вредоносными программами, безопасных настроек, по случаям недоступности узлов и сегментов сети связи, нарушения авторских прав при работе в интернете и т.д.); принимает круглосуточно обращения операторов связи по поводу событий и инцидентов безопасности, в том числе жалобы на действия пользователей и операторов связи, а также на инциденты с использованием средств связи оператора (пример: фрод на сетях связи); ведет анализ (расследование) зафиксированных инцидентов и событий безопасности во взаимодействии с операторами связи, производителями оборудования, государственными органами и предоставляет оперативную информацию об угрозах, инцидентах и событиях безопасности для ликвидации их вредных последствий; организует взаимодействие между операторами связи и сервис-провайдерами при эксплуатации программно-технических средств поддержки информации об актуальности присоединенных сетей; способствует повышению устойчивости, а также информационной безопасности средств коллективного пользования; выдает рекомендации производителям оборудования в том, что касается требований к повышению устойчивости сетей связи и кибербезопасности средств связи; проводит информационно-аналитическую работу по сбору данных о произошедших атаках, актуальных методах атак, ресурсах злоумышленников, сигнатурах атак и т.д.

Список инцидентов, на которые реагирует МЕГА, включает (но не ограничивается ими) DDoS-атаки, несанкционированный доступ к сетевым ресурсам, наличие известной критичной уязвимости на имеющем существенное значение ресурсе, эпидемии компьютерных вирусов, функционирование в сети связи вредоносных программ, нарушение функций маршрутизации, приводящих к недоступности подсетей, сегментов, автономных систем, ошибочное или злонамеренное перекомфигурирование сетевого оборудования, приводящее к нарушению связности телекоммуникационных сетей, фишинг, рассылку различных видов спама, несанкционированный пропуск трафика («серый» трафик).



Принятие Рекомендации МСЭ-Т по созданию Национальных центров безопасности – важный этап формирования содружества государств в интересах обеспечения информационной безопасности на сетях связи. Теперь эффективность этого процесса зависит от дальнейшей разработки более конкретных стандартов на базе данного «зонтичного» стандарта, а также конкретных пошаговых руководств по их развертыванию. ИКС

*Инцидент информационной безопасности (инцидент ИБ) – одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации. Эти события указывают на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Перед рассветом ЛОКАЛЬНЫХ СЕТЕЙ

Как будет выглядеть самая локальная сеть – пользовательская – через три-пять лет.



**Константин
СЕРЕБРЯКОВ,**
директор
по работе
с операторами
связи, Qtech

В крупных городах подключение к безлимитному тарифу на скоростях 100 Мбит/с – уже не экзотика. Количество операторов, работающих в некоторых многоквартирных домах, превышает все мыслимые пределы (например, в доме, где проживает автор статьи, их более пяти), причем складывается впечатление, что тарифные планы для большинства из них создавали одни и те же специалисты. А учитывая доступность ноутбуков, смартфонов и прочей домашней компьютерной техники, пользователи предпочли сконцентрироваться не на поиске лучшего провайдера с идеальным соотношением цена/качество, а на обустройстве домашней сети.

Как начинались домашние сети

В ответ на потребности пользователей производители создали монструозные наборы девайсов, функции которых зачастую дублируют друг друга: плееры DVD или Blu-Ray для воспроизведения оптических дисков, медиаплееры для воспроизведения контента (в подавляющем большинстве нелегального), STB для просмотра IPTV... Можно также встретить компьютеры в виде медиацентров, игровые приставки, устройства типа Apple TV и т.д. Самое подходящее для всего этого описание – «путаница проводов» и «пылесборник». При этом некоторые девайсы могут простаивать неделями или даже месяцами, но они обязательно включены в домашнюю сеть. И если раньше было достаточно просто роутера, то такой парк техники уже порой требует неуправляемого коммутатора.

Основными «потребителями» беспроводного подключения стали смартфоны и планшеты. Часть перечисленных выше устройств тоже может подключаться по беспроводным каналам, но такое соединение не всегда обеспечивает надежную связь для передачи потокового видео или контента в HD-качестве.

С другой стороны, все большую популярность набирают домашние самосборные серверы и готовые NAS, на которые ложатся функции контент-библиотеки и медиасервера.



Все это многообразие привело к тому, что многие пользователи переходят на гигабитную домашнюю сеть, с беспроводными соединениями стандарта 802.11n. В большинстве случаев они самостоятельно выбирают домашние роутеры по цене от 1000 руб. и выше. Ряд таких устройств уже обладает функциями сетевого хранилища и медиасервера, но некоторое неудобство эксплуатации сдерживает их широкое применение.

Новый тренд – интеграция

Сейчас мы наблюдаем новый этап развития, для которого характерны интеграция все большего числа функций в новых моделях телевизоров и все большее распространение планшетов. Немаловажную роль играют снижение цен и, как следствие, доступность этих устройств. Более того, все чаще устройства оснащаются модулями беспроводной связи, что позволяет моментально интегрировать их в существующую инфраструктуру домашней сети.

В этих условиях пытливые умы нашли способ использовать медиацентры в качестве STB, да и производители данных устройств не чинят препятствий для такого (в большинстве случаев недокументированного) применения. Некоторые же практически перешли на использование телевизоров и в качестве медиацентров, и в качестве STB. Сегодня такое их применение ограничивается не столько недостатком знаний у пользователей (на форумах можно найти множество инструкций по настройке оборудования), сколько тем, что подбор необходимых компонентов требует значительных затрат времени и средств.

Другим ограничительным фактором становится все усиливающееся нежелание провайдеров превращаться в трубу. Эпоха расцвета провайдеров прошла, пользователи стали достаточно инертны, и их желание сменить провайдера даже ради экономии (часто незначительной) стремится к нулю. Поэтому сейчас провайдеры проводят достаточно агрессивную политику удержания абонентов и привлечения новых, предлагая им

Возможно,
мы увидим новый
подъем неболь-
ших провайдеров,
которые будут
лояльны к своим
пользователям
и не станут огра-
ничивать их доступ
к услугам, вынуж-
дая приобретать
дополнительное
оборудование

все больше и больше услуг. Если еще три года назад услуга IPTV имела не у каждого провайдера, то сейчас ее предлагают даже небольшие компании, обслуживающие один городской район. Крупные же провайдеры ради сдерживания оттока абонентов расширяют набор услуг: видео по запросу, сетевые хранилища, игровые приложения, игровые серверы и т.п. Наметилась и еще одна тенденция: провайдер готов оказывать ряд услуг без привязки к собственной сети, при этом абоненты данного провайдера получают услуги на льготных условиях, а остальные оплачивают их полностью.

Заглянем в будущее?

Темп жизни ускоряется в геометрической прогрессии, и рядовой покупатель уже не желает тратить время на создание домашней сети и подбор ее компонентов. Устройство должно работать сразу после включения в сеть, с минимальной тратой времени на его настройку.

Мы считаем, что в ближайшее время начнется массовое внедрение технологии 802.11ac, за счет чего повысятся скорости беспроводных соединений. К тому же в домашних роутерах появятся удобные и практичные функции контент-библиотеки и медиасервера. Немаловажную роль в этом сыграют производители программного обеспечения, которые стали уделять все больше внимания данному направлению. Все это даст возможность максимально эффективно использовать функции современных устройств, будь то телевизоры или смартфоны с планшетами. Отпадет и необходимость тянуть вечно мешающуюся витую пару, ускорится интеграция новых устройств в домашнюю сеть.

Производители же телевизоров перейдут на выпуск дешевых моделей с функциями медиаплеера, что кардинально снизит продажи отдельных устройств с подобным функционалом. Говорить о том, что медиаплееры совсем исчезнут с рынка, нельзя, так как парк уже приобретенных населением телевизоров без этой функции достаточно велик.

Мы также рискуем предположить, что телевизоры будут включаться все реже: основные функции «окна в мир» возьмут на себя планшеты, новый расцвет которых мы увидим уже в этом году с выходом операционной системы Microsoft Windows 8 и появлением все большего числа устройств на этой платформе.

Как отдельное направление будут развиваться домашние сетевые хранилища. К сожалению, их широкое распространение ограничат набирающие популярность интернет-кинотеатры и облачные хранилища, а также отсутствие легального способа наполнения их контентом.

Связующий стандарт для этих устройств уже существует и широко применяется — это DLNA. В альянс на сегодня входят более 200 производителей сетевых устройств, бытовой электроники и мобильной техники. Их усилиями стандарт стал общепризнанным и де-факто применяется в миллионах устройств и во многих программных продуктах. Именно DLNA окончательно создаст общедоступную и удобную экосистему. При этом технологии не стоят на месте, и следующий этап развития будет связан с массовым внедрением Wi-Fi Miracast — стандарта беспроводной передачи мультимедийного сигнала, утвержденного объединением Wi-Fi Alliance в сентябре 2012 г.

И для завершения обсуждения мы сознательно приберегли вопрос о роли провайдеров. Их отмечавшееся много раз нежелание превращаться в трубу, совмещенное со стремлением привязать пользователя к себе за счет «подаренного» роутера и STB, работающих только с определенным провайдером, может иметь очень интересные последствия. Фактически мы, возможно, увидим новый подъем небольших провайдеров, которые будут лояльны к своим пользователям и не станут ограничивать их доступ к услугам, вынуждая приобретать или брать в аренду дополнительное оборудование. Например, провайдеры все чаще дают возможность пользоваться услугой IPTV без приобретения STB, в ряде случаев достаточно функций, заложенных в новую модель телевизора.

Надеемся, что крупные провайдеры вовремя осознают желания пользователей, смогут договориться с производителями бытовой электроники и абонентского оборудования об интеграции своих сервисов и не станут чинить препятствия абонентам, ограничивая их доступ к сервисам контент-провайдеров.

Обычных же пользователей ждет избавление от множества разных устройств и мешанины проводов. Достаточно будет установить домашний роутер, настроить соединение и получить доступ ко всему многообразию контента из Всемирной паутины при помощи одного только телевизора, смартфона или планшета. ИКС

76 Н. ПРИВЕЗЕНЦЕВА. Системы хранения для «больших данных»
82 Система мониторинга центров обработки данных. Простота в надежности

84 Э. АЛЕХИН. Операционная устойчивость ЦОДа:
новое увлечение или реальная потребность? Окончание

86 Е. ВИШНЕВСКИЙ. Эволюция параметров
микроклимата ЦОДов

91 М. МАЛОВ. Видеосистемы без границ
94 Новые продукты

Системы хранения для «больших данных»

Надежда ПРИВЕЗЕНЦЕВА



Системы, растущие вместе с данными

Масштабируемость – одно из важнейших требований к корпоративной СХД. В связи с направлением big data внимание экспертов привлекают технологии горизонтально масштабируемых систем, известных как scale-out NAS.

Scale-out NAS представляют собой кластеры, состоящие из энного количества равноправных узлов, число которых можно легко наращивать и которые можно администрировать как единое целое. Отчасти это похоже на решение для виртуализации СХД, создаваемое с помощью специального устройства-виртуализатора – то же объединение множества систем хранения в единый пул с общим интерфейсом управления. Но есть и ряд существенных отличий.

Все узлы в кластерной NAS – от одного вендора, как правило, однотипные и одинаково сконфигурированные. В каждом узле содержатся и дисковая емкость, и кэш, и вычислительная мощность. Все узлы соединяются между собой выделенной высокопроизводительной сетью, обычно на основе Infiniband. А главное, такие кластеры изначально проектируются с единой файловой системой (ФС).

Традиционно для хранения файловых данных использовались NAS-системы, построенные в классической архитектуре: два контроллера, дисковые полки, RAID-группы и множество относительно небольших файловых систем. При необходимости работы с единым файловым хранилищем несколько таких систем могут объединяться в единое логическое пространство имен – с помощью распределенной файловой системы Microsoft DFS либо с использованием проприетарных вендорских технологий. Как поясняет Сергей Золотарев (EMC), снаружи такое хранилище выглядит как одна ФС, но внутри остается набором независимых файлов. Каждый каталог располагается только на одном из них, расположением каталогов, как правило, необходимо управлять вручную с учетом

«Большие данные» становятся все больше, говорят аналитики. К системам хранения предъявляются все более жесткие требования с точки зрения емкости, надежности хранения и производительности. Традиционные СХД не всегда показывают себя достаточно эффективными в новых условиях. Тема «больших данных» обуславливает интерес к иным механизмам и архитектурам хранения.

заполнения различных файловых систем и производительности. Администрируется такая система обычно тоже как набор независимых СХД со своими интерфейсами управления.

В отличие от такого рода решений scale-out NAS имеют по-настоящему единую ФС. Записываемые в нее данные равномерно распределяются между всеми узлами кластера в автоматическом режиме. Ярким примером такой системы является EMC Isilon: ее операционная среда OneFS объединяет в себе функциональность файловой системы, RAID-контроллера и менеджера томов.

По мнению Равиля Сафиуллина (IBM), именно ФС является ключевым компонентом решения для организации файлового доступа, определяющим его характеристики и возможности. Поэтому при создании такого решения выбирать следует скорее файловую систему, нежели модели устройств. Системы IBM базируются на параллельной ФС IBM GPFS, изначально создававшейся для применения в составе вычислительных кластеров, оперирующих большими объемами информации. За счет нее достигается функциональная совместимость различных устройств кластера и возможность поддержания единого рабочего пространства данных.

Одно из ключевых преимуществ scale-out NAS – простая масштабируемость с точки зрения как емкости, так и производительности, причем осуществляемая без остановки доступа пользователей к данным. Например, кластер EMC Isilon может содержать три узла в минимальной конфигурации и 144 в максимальной – это 20 Пбайт емкости в единой файловой системе. В отличие от традиционных систем, наращивание емкости которых упирается в производительность контроллеров, добавление нового узла в кластер увеличивает не только емкость системы, но и ее производительность.

Достоинство scale-out NAS и в том, что их высокая масштабируемость не оказывает пагубного влияния на

характеристики производительности, отмечает Андрей Новиков из Hitachi Data Systems, подчеркивая, что такие возможности присущи семейству решений Hitachi Network Attached Storage (HNAS). СХД семейства HNAS строятся на базе гибридной архитектуры – совместного использования процессоров общего назначения и программируемых логических интегральных схем (FPGA) для обработки низкоуровневых операций. Это дает возможность масштабировать систему до восьми узлов с совокупной емкостью до 16 Пбайт при сохранении очень высокой производительности.

Впрочем, к вопросу масштабирования СХД производители подходят по-разному, не все считают, что построение кластера из однотипных, специально предназначенных для этого узлов – оптимальный путь для заказчика, имеющего дело с постоянно растущими объемами данных. Например, Роман Ройфман (NetApp) считает, что должна быть возможность использовать в одной системе разнородные узлы разных поколений, добавлять ресурсы более старших или более новых систем. Одновременно он обращает внимание на то, что кластерная система должна обладать всеми возможностями и сервисами, присущими NAS-системе enterprise-уровня, такими как дедупликация, создание мгновенных копий, механизмы эффективного хранения (многоуровневого хранения на различных типах дисковых устройств).

Системы NetApp FAS и V-Series для унифицированного хранения данных легко масштабируются благодаря операционной системе Data ONTAP. Она позволяет расширить СХД, состоящую из пары контроллеров, до нескольких пар контроллеров и масштабировать дисковое пространство до десятков петабайт. При этом вся система будет управляться как единый логический пул ресурсов и единое пространство имен. В одном кластере могут сосуществовать системы разных поколений. Версия ONTAP 8.1 в сочетании с технологией Cluster-Mode (это один из режимов работы Data ONTAP, поддерживающий интерконнект узлов в кластере) позволяет создать кластер из 24 узлов (12 пар высокой доступности) для файлового доступа или четырех-узловой кластер для блочного доступа. В кластере выделяются один или несколько логических контейнеров (Vserver), содержащих ресурсы СХД, а также настройки безопасности (права доступа и пр.). При масштабировании контейнеры могут «растягиваться», вмещая больше файлов и данных.

Янис Кириакидес (Oracle) полагает, что scale-out NAS – не всегда оптимальный выбор для хранения «больших данных» и что сбрасывать со счетов традиционные системы хранения было бы неверно. Подход с использованием scale-out NAS оправдывает себя в тех случаях, когда разнотипные данные сильно смешаны, и требует высокой производительности в целом равномерно, без выраженных «горячих» и «холодных» участков. Однако стоимость хранения оказывается достаточно высокой: по сути, добавляя новые узлы в кла-

стер, мы добавляем в инфраструктуру новые серверы со своими вычислительными ресурсами и памятью, а также с потребляемой мощностью и выделяемым теплом. В традиционной системе можно ограничиться расширением дискового пространства путем добавления полки с дисками – дополнительные затраты минимальны. Традиционную СХД Oracle ZFS Storage Appliance специалист Oracle считает вполне достойной альтернативой scale-out NAS. Например, старшая в семействе система ZFS Storage 7420 доступна как в единичной, так и в кластерной конфигурации и масштабироваться может почти до 2,6 Пбайт. Для повышения эффективности хранения в Oracle ZFS Storage Appliance предусмотрены технологии компрессии и дедупликации на уровне блоков данных.

Контент, объекты или файлы?

Основную долю массива big data составляют неструктурированные данные (контент). Привычный вариант их хранения – в виде файлов. Однако файловое хранение имеет свои недостатки, один из наиболее очевидных связан с многообразием файловых форматов. Практически каждое приложение генерирует свой формат файлов, приложения со временем устаревают и уходят с рынка, с ними уходят и соответствующие форматы, и при долговременном хранении файлов (с учетом требований законодательства это могут быть десятки лет) вполне может оказаться, что в какой-то момент владелец данных часть из них просто не сможет прочесть.

Альтернативный подход к хранению данных – системы хранения с адресацией по содержанию (Content Addressable Storage, CAS) и объектные системы хранения (Object Storage). Архитектурно они похожи, как правило, и те и другие обходятся без файловой системы. Но, как поясняет Александр Зейников (LSI),

→ Приложения устаревают и уходят с рынка вместе со своими форматами файлов, и при долговременном хранении данных есть вероятность, что в какой-то момент владелец данных часть из них не сможет прочесть

разрабатывались они для разных целей. Решения Object Storage ставят своей главной задачей обеспечение максимальной производительности (отсюда их применение в высокопроизводительных вычислениях), а CAS-системы рассчитаны на максимизацию надежности хранения (поэтому их основное применение – онлайн-архив).

Комментируя различия CAS и Object Storage, Антон Банчуков (Dell) отмечает следующее: технология контентной адресации подразумевает, что для поиска данных используется не адрес их расположения на носителе или в системе хранения, а специально вычисленная хэш-функция, которая уникальным образом идентифицирует документ. С одной стороны, это позволяет получать быстрый доступ к конкрет-



ному документу или его содержанию, а с другой – быть уверенным в том, что документ не был изменен с момента последнего доступа к нему. Для архивов это очень важно. Объектное же хранение напоминает классическую ФС, но с той разницей, что если в файловой системе хранение происходит на уровне небольших блоков фиксированного размера, то Object Storage оперирует значительно более крупными единицами хранения информации – объектами. В их состав наряду с данными входят метаданные, которые могут содержать дополнительную информацию о хранимом содержимом: например, если речь идет о медицинском снимке, метаданные могут включать время его создания, информацию об аппарате, на котором он был сделан, имя врача, имя пациента, условия доступа к документу. Это позволяет применять к документам политику хранения (скажем, запрещать удаление документов «младше» пяти лет). При объектном хранении комбинируются преимущества обычных файлов с точки зрения скорости поиска и доступа с применением процедур, относящихся к типу документа. Сама компания Dell предлагает платформу объектной системы хранения данных Dell DX – ее базовая конфигурация состоит из одного сервера DX6000 и двух узлов хранения данных DX одинакового типа.

В основном эксперты сходятся на том, что системы Object Storage более перспективны, нежели CAS. Последние не приспособлены к работе с изменяющимися данными, поэтому если речь идет о решении для активных данных, а не об архивной платформе, CAS будет неэффективна. Объектные системы этого недостатка лишены. Кроме того, традиционные CAS-системы ориентированы прежде всего на локальное хранение, в то время как объектные системы могут иметь распределенную архитектуру и использоваться для облачного хранения. Да и объемы данных, которыми могут оперировать CAS, исчисляются максимум сотнями терабайт, в то время как разработчики объектных систем хранения уже замахиваются на эксабайты. Поэтому, по мнению Р. Ройфмана, CAS – это ушедшая с рынка технология, не нашедшая должного применения. Он напоминает и о том, что системы CAS предлагали собственный API, с которым должно было работать ПО архивирования (хотя попытка создать единый стандарт CAS API была). Объектные же системы хранения опираются на «понятные» облачным приложениям RESTful-сервисы, а процесс их стандартизации в SNIA идет полным ходом, поэтому есть реальный шанс получить работающую экосистему, открытую для различных производителей.

Впрочем, С. Золотарев замечает, что технологии CAS и Object Storage не исключают, а взаимно дополняют друг друга. Примерами решений, где обе технологии сочетаются, может служить классическая CAS-система EMC Centera, хранящая данные в виде объектов, или объектная система EMC Atmos, в которой, в числе прочего, применяется адресация по содержанию. Кстати, Atmos изначально разрабатывалась как облачная плат-

форма. Этот продукт позволяет строить географически распределенные системы с единым адресным пространством, с использованием политик адаптивного управления данными на основе метаданных, что позволяет автоматизировать процедуры хранения, распределения и управления информацией.

К семейству объектных СХД относятся и уже упомянутые системы HNAS, а также Hitachi Content Platform (HCP). Как указывает А. Новиков, в этих системах работа с метаданными хранящихся объектов происходит независимо от самих данных. Это позволяет избежать трудностей при использовании и хранении динамически изменяемых неструктурированных данных даже при очень больших объемах хранения. Эффективно работать с информацией в зависимости от ее типа, перемещать и извлекать данные исходя из их востребованности и динамики использования помогает продукт Hitachi Data Discovery Suite, с которым HCP и HNAS тесно интегрированы. Кроме того, механизмы интеллектуальной кэш-памяти на платформе HNAS позволяют кэшировать метаданные объектов, тем самым ускоряя работу с объектами в разы.

Высокомасштабируемую платформу для доступа к объектным данным и файлам недавно анонсировала компания HP. Ее система StoreAll Storage позиционируется как удобная основа для проектов big data и облачного хранения. Объектный режим, который реализован в новой версии операционной системы HP StoreAll OS v6.2 для StoreAll REST API, разрешает хранение файлов и объектов на одной платформе, а технология StoreAll Express Query обеспечивает быстрый поиск по метаданным. Как утверждают в HP, такой поиск происходит в 100 тысяч раз быстрее, чем при прежних методах поиска по файловой системе.

SSD: быстрее и экономнее

В современных системах хранения широко используются твердотельные, или флеш-накопители (SSD). В контексте big data интерес к ним еще более возрастает. Преимущество SSD – высокие скорости чтения, записи, поиска данных: они могут на порядки превышать аналогичные показатели для традиционных жестких дисков (HDD). На рынке уже появились модели систем хранения, полностью построенные на SSD: например, компания HP в прошлом году выпустила all-SSD-версию массива P10000 из семейства HP 3PAR. Но есть у технологии SSD и свои сдерживающие факторы.

Один из таких факторов – цена. Стоимость хранения гигабайта данных на SSD пока еще не может сравниться с таковой для HDD, не говоря уже о магнитных лентах. «Действительно, стоимость SSD достаточно высока по сравнению с традиционными дисками, – соглашается Я. Кириакидес, – но в ряде случаев такие инвестиции оправданы». Системы хранения данных можно сравнить с автомобилями: есть «грузовики», которые неспешно «перевозят» большие объемы при низкой стоимости на единицу «груза» (диски SATA или NL-SAS); есть «легковые машины», они менее вместительны, но более быстры (SAS либо FC); наконец, есть «спортив-

ные болиды» (SSD). Экономичного варианта использования SSD вполне можно добиться, если не пытаться «возить картошку на Ferrari».

Системы all-SSD (иначе, all-flash array, AFA) – на данном этапе решения нишевые. По мнению Александра Яковлева (Fujitsu), для ряда задач действительно экономически обоснованно приобретение небольшого по емкости массива из дисков SSD, который будет довольно дорогим, но покажет огромную производительность. В то же время существуют гибридные решения, сочетающие жесткие диски и флеш-накопители. Они позволяют реализовать автоматическое многоуровневое хранение данных: «горячие» данные автоматически перемещаются на наиболее быстрые носители, а менее востребованные мигрируют на недорогие и медленные. При таком подходе высокая стоимость SSD становится не так заметна.

Использование флеш-накопителей в гибридных системах возможно на нескольких уровнях, напоминает Р. Ройфман: 1) на уровне серверов для кэширования дисковых массивов (примером могут служить решения NetApp FlashAccel или Fusion-io directCache); 2) на уровне контроллеров СХД с использованием специальных кэширующих модулей (весьма успешный пример – FlashCache); 3) на уровне объединения HDD и SSD в единый пул (например, технология FlashPool). Все эти методы позволяют получить высокую производительность, не неся чрезмерных затрат на полную замену HDD на SSD. Для достижения

наилучшего результата методы можно комбинировать друг с другом.

А. Банчуков обращает внимание на такой механизм снижения стоимости хранения данных, как их дедупликация и сжатие. Для неструктурированной информации (файлов пользователей, текстовых документов, изображений и пр.) экономия может достигать десятков раз (т. е. в десять раз уменьшается физически занимаемое место). В подобном случае применение SSD вполне обоснованно, даже если это массив all-SSD. Если нет возможности сжимать данные (например, в случае потока видеофайлов, которые и так сжаты), применяют подход многоуровневого хранения.

Другим методом повышения экономичности СХД, в том числе на базе SSD, является технология выделения емкости по требованию – Thin Provisioning. В результате явления под названием over provisioning, когда емкость СХД резервируется за каким-либо приложением, но реально не используется, многие старые СХД хранят более чем на половине емкости пустые блоки, напоминает С. Золотарев. При этом пустые блоки нигде больше нельзя использовать. При помощи Thin Provisioning вся выделяемая емкость будет гарантированно использоваться, а все пустые блоки будут свободны для перераспределения между любыми серверами в корпоративной инфраструктуре.

Шагом к усилению позиций твердотельных дисков на рынке систем хранения стал переход многих производителей SSD с достаточно дорогой технологии

iKS-Consulting
предлагает Вашему вниманию
Аналитический отчет:



«Российский рынок коммерческих дата-центров 2012-2016»

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



Параметры отчета:

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

Подробная информация:

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

www.iks-consulting.ru

SLC (single-level cell) на более дешевую технологию MLC (multi-level cell). При этом, однако, диски MLC считаются менее надежными, у них больше время доступа к данным и меньше количество циклов перезаписи.

Как правило, производители СХД используют диски только одного типа. По мнению Я. Кириакидеса, это приводит либо к чрезвычайно высокой стоимости хранения, либо к недостаточной надежности. Но гибридный подход применим и здесь: компания Oracle в своих системах ZFS SA использует SLC-диски для кэширования операций записи (поскольку данные часто изменяются, и требуется обеспечить большое количество циклов перезаписи), а для кэширования операций чтения – MLC-диски большего объема.

Компания Hitachi использует именно MLC. Однако, как отмечает А. Новиков, разработка новых контроллеров для твердотельных накопителей и создание системы внутреннего дублирования ячеек, при котором часть из них изначально не используется, но динамически включается в работу при необходимости (например, при выходе из строя рабочей ячейки), позволяет успешно справляться с обозначенными проблемами.

Что касается наращивания производительности систем на базе SSD, то на данном этапе вопрос упирается не в сами SSD, а в другие компоненты и механизмы систем хранения. С. Золотарев считает, что основные ограничения в наращивании производительности СХД сейчас накладывает процессорная мощность контроллеров хранения традиционных двухконтроллерных СХД. По его словам, можно использовать хоть 16-ядерные контроллеры с SMP-архитектурой, но и они в конце концов станут узким местом. Очевидно, что наращивание количества ядер по традиционной схеме будет лишь временным решением. Назрела необходимость в новой архитектуре СХД, оптимизированной для использования твердотельных дисков. В компании EMC такой архитектурой считают scale-out – подход, позволяющий добавлять не ядра в контроллеры, а новые контроллеры для повышения производительности системы.

Однако производители контроллеров тоже не сидят сложа руки. Компания HDS выпустила для своей системы Virtual Storage Platform (VSP) специализированный модуль Hitachi Accelerated Flash, оптимизированный для монтажа в стойку. Он включает флеш-память (в начале было доступно 1,6 Тбайт, теперь речь идет о 3,2, а затем и о 6,4 Тбайт) и контроллер собственной разработки Hitachi. В контроллере реализован ряд новых возможностей, например сжатие информации в ходе записи, что помимо ускорения операции записи повышает срок службы флеш-памяти. Заявляется, что по сравнению с обычными SSD емкостью 400 Гбайт этот модуль позволяет в четыре раза увеличить производительность и на 46% снизить стоимость хранения данных.

Компания LSI выпустила в прошлом году RAID-контроллеры и хост-адаптеры с шиной PCI Express 3.0.

Они могут использоваться как с жесткими дисками, так и с твердотельными накопителями, демонстрируя очень высокую производительность. Как сообщает А. Зейников, такие контроллеры (например, PCI-E 3.0 LSI MegaRAID 9271) способны обслужить до 500 тыс. IOPS. Между тем производительность серверных устройств SSD составляет на данный момент порядка 30–50 тыс. IOPS. Таким образом, можно построить массив с использованием до 16 SSD на контроллер без потери производительности.

Помимо традиционной связки контроллер – SSD на рынке появились устройства в формате SSD-карт, вставляемых непосредственно в PCI-слот сервера (например, Nytro WarpDrive). Они позволяют добиваться высоких показателей IOPS без дополнительного конфигурирования и тюнинга устройства. Среди преимуществ таких решений – максимальное приближение устройства хранения к процессору и минимизация задержек привносимых RAID-контроллерами, сетевыми протоколами и пр.

Не ограничиваться рассмотрением SSD в факторе традиционных HDD призывает и Р. Сафиуллин. Недавно IBM приобрела компанию Texas Memory Systems, в портфеле которой имеются интересные разработки в области дизайна и организации ячеек памяти, алгоритмов записи/чтения данных и пр. Теперь «Голубой гигант» намерен представить под собственным брендом готовые решения уровня предприятия на базе твердотельных накопителей, которые обеспечат десятки терабайт доступного пространства с очень малым временем доступа к данным.

Флеш-технология – лишь один из вариантов реализации твердотельной памяти. Сейчас специалисты все чаще говорят о новом виде твердотельных накопителей, построенных на технологии памяти на базе фазового перехода (Phase Change Memory, PCM). Преимуществами PCM-накопителей являются не только значительно более высокое быстродействие самого носителя, но и отсутствие эффекта «выгорания», с которым приходится бороться разработчикам флеш-дисков. С. Золотарев полагает, что развитие технологий solid state-памяти (например, в сторону PCM) будет одним из направлений совершенствования накопителей, наряду с ростом емкости SSD и все более широким применением методов оптимизации использования твердотельных накопителей.



Технологический прогресс достиг сегодня такого уровня развития, что бизнесу стоит только «загадать желание». И, естественно, соотнести желания со своими возможностями, постаравшись выбрать экономически обоснованное решение. Несмотря на то что технологии постепенно дешевеют и делаются более доступными, хранение больших объемов данных требует значительных ресурсов. А значит, продуманная политика хранения не менее важна, чем современные технологии. ИКС



25-я международная выставка
телекоммуникационного оборудования,
систем управления, информационных
технологий и услуг связи

СВЯЗЬ- ЭКСПОКОММ

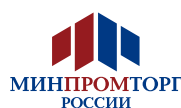
14–17.05.2013

www.sviaz-expocomm.ru

Центральный выставочный комплекс «Экспоцентр»



Министерство связи
и массовых
коммуникаций РФ



Министерство
промышленности
и торговли РФ



Официальный
информационный
партнер

Система мониторинга центров обработки данных Простота в надежности

В последнее время к системам мониторинга и управления центров обработки данных предъявляются все более высокие требования. Система Rittal CMC III этим требованиям отвечает.

Что диктует рынок, какие требования выдвигают сегодня потенциальные заказчики к мониторингу отдельной стойки и ЦОДа в целом? Максимальная надежность, моментальная реакция системы, экономичность, простота запуска и обслуживания, высокая точность снятия показаний, универсальность и масштабируемость – вот главные критерии для выбора системы мониторинга.

Рассматривая отдельную стойку как один из основных компонентов ЦОДа, выделим факторы возможного воздействия на нее: температура и влажность, дым и огонь, несанкционированное вскрытие, вандализм и т.д. Только представьте, что может случиться с вашим оборудованием, если, например, произойдет утечка в системе жидкостного охлаждения дата-центра или начнет распространяться дым, а вы об этом не будете вовремя осведомлены? Для того чтобы подобные нештатные ситуации не привели к необратимым последствиям, о них

формации пользователь может получить через веб-интерфейс. Также существует возможность интеграции в вышестоящие по иерархии системы управления ЦОДом с помощью протокола SNMP, например в ПО Rittal RiZone. Генерация сигналов тревоги обеспечивает своевременное оповещение администратора о выходе параметров за допустимые пределы по e-mail или посредством SMS-сообщений, в том числе в нерабочее время.

Внимание на самом главном

Важнейшим нововведением является использование шины Controller Area Network (CAN-Bus). Эта шина поддерживается центральным процессорным блоком, а также интеллектуальными датчиками Rittal, применение переходных блоков не требуется. Таким образом, датчики CAN-Bus подключаются к процессорному блоку последовательно: в каждом серверном

Rittal – The System.

Faster – better – worldwide.

IT-инфраструктура от элемента до системы.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

FRIEDHELM LOH GROUP

необходимо немедленно узнавать и максимально быстро на них реагировать. Из-за увеличения масштабов современных ЦОДов такая задача становится все более сложной и требует соответствующих технических средств.

Поэтому после тщательной разработки Rittal в 2012 г. представил новую систему мониторинга – CMC III, отвечающую всем современным требованиям и включающую инновационные решения в сфере мониторинга ЦОДов. С помощью этой системы можно непрерывно контролировать жизненно важные функции дата-центра в режиме онлайн.

Принцип действия CMC III прост: при помощи датчиков в серверных стойках и ЦОДе измеряются температура и влажность воздуха, скорость воздушного потока и другие параметры. Полученные значения параметров консолидируются и обрабатываются в центральном блоке системы. Доступ к собранной ин-

шкафу имеется датчик CAN-Bus, который соединяется шинным кабелем с датчиками в соседних шкафах. Данные пересылаются от датчика к датчику, прежде чем достигнут центрального блока. Поскольку датчики подключаются напрямую, снижается стоимость системы, обеспечиваются простота монтажа, обслуживания и масштабируемость системы в целом.

Rittal предлагает новое решение и в области датчиков: два важнейших – датчик температуры и инфракрасный датчик доступа к двери – интегрированы непосредственно в стандартный процессорный блок. Добавлена визуализация состояния каждого датчика: их состояние можно определить, не пользуясь веб-интерфейсом.

При этом CMC III гибко расширяется по модульному принципу: доступны счетчики расхода электроэнергии, датчики для фиксации актов вандализма и блок управления с восемью циф-

ровыми входами и четырьмя релейными выходами. Всего можно подключить до 32 датчиков. Кроме того, Rittal реализовал в СМС III две новые функции: появился датчик перепада давления, который контролирует степень изоляции холодного коридора ЦОДа, а также поддерживаются счетчики электроэнергии с выходом S0Bus. В ИТ-среде часто требуется определять или рассчитывать энергопотребление отдельных устройств или стоек. Благодаря интерфейсу S0Bus возможно считывание и отображение результатов измерений через СМС III.

Экономия места и электропитания

С учетом все возрастающих требований к вычислительной мощности ограниченное пространство ЦОДа следует использовать оптимальным образом. Поэтому был переработан и корпус блоков СМС: всю систему мониторинга можно разместить в одном юните или же на раме шкафа, не занимая полезного пространства в стойке. Для повышения надежности предусмотрено дублирование электропитания. В качестве альтернативы также возможно электропитание PoE – при наличии у коммутатора соответствующей функциональности.

Удобство: установка, конфигурирование, контроль

В качестве сетевого протокола пользователь может выбрать TCP/IPv4 и TCP/IPv6. Если система подключена к локальной сети, то конфигурирование производится с помощью удобного встроенного веб-сервера. Также предусмотрена возможность

подключения и многообразие используемый в СМС III протокол SNMP стал стандартом для многих ИТ-решений. Однако в промышленности и на производстве протокол SNMP распространен значительно меньше. Поэтому, если пользователь желает контролировать здание или промышленные установки (например, ГРЩ в ЦОДе) с помощью систем мониторинга, возникает проблема. Для ее решения система СМС III имеет встроенный OPC-сервер (Open Packaging Convention) от Microsoft.

Один в поле воин

Если есть необходимость в мониторинге отдельной стойки, Rittal предлагает систему в бюджетном варианте на базе процессорного блока Compact СМС III. В этом случае реализуются основные функции системы, причем помимо стандартных функций контроля температуры и доступа в шкаф имеется возможность подключения до четырех датчиков.

Автоматизированное управление в аварийных ситуациях

СМС III в сочетании с ПО для управления ИТ-инфраструктурой RiZone и Microsoft System Center Operations Manager предоставляет возможность автоматически принимать превентивные меры по обеспечению безопасности. Также в процессорном блоке СМС III предусмотрена возможность написания



подключения по miniUSB. С помощью USB-накопителя или карты памяти SD можно производить обновление программного обеспечения и вести долговременную архивацию данных с целью дальнейшего анализа (например, построения графиков температуры внутри шкафа).

У СМС III расширены возможности управления правами пользователей. Так, при увольнении ИТ-специалиста из компании его учетные записи приходится удалять отдельно из каждой системы мониторинга. СМС III поддерживает протокол Lightweight Directory Access Protocol (LDAP), который обеспечивает быструю централизованную обработку данных.

Применение СМС III в промышленности

Предлагая универсальную систему мониторинга, Rittal заботится не только об ИТ-секторе. Благодаря своей простоте, мо-

сценариев: например, при обнаружении дыма в стойке – отключить систему вентиляции. Аварийные ситуации выявляются без вовлечения персонала, а ответственные сотрудники оповещаются о них с помощью SMS или по электронной почте.

Комбинация СМС III, RiZone и SCOM представляет собой комплексное решение в области удаленного управления, которое контролирует все жизненно важные устройства ЦОДа, в том числе и тогда, когда сотрудники не находятся на рабочих местах.

ООО «Риттал»

125252, Москва, ул. Авиаконструктора

Микояна, 12, БЦ "Линкор", 4 этаж

тел. (495) 775-0230, факс (495) 775-0239

info@rittal.ru, www.rittal.ru

Операционная устойчивость ЦОДа

новое увлечение
или реальная
потребность?

Окончание. Начало см. «ИКС» № 1-2' 2012, с. 76.



Заурбек АЛЕХИН,
независимый консультант

Чтобы быть уверенным в высоком качестве функционирования ЦОДа, стандарт Tier Standard: Operational Sustainability необходимо применять последовательно и грамотно.

Порядок применения стандарта

Конечно, каждый сам может решить, как именно применять Стандарт операционной устойчивости для ЦОДов. И это будет от-

части верно. Мы же остановимся на «авторском» варианте применения стандарта.

Для начала следует определиться с целевым уровнем Tier. В целом Tier – это ожидания качества функционирования дата-центра. Например, по статистике Uptime Institute, дата-центр, соответствующий Tier II, по причинам, связанным с необходимостью обслуживания и ремонта инженерных систем, в среднем недоступен не более 22 часов в год. Аналогичное значение для Tier III – 1,6 часа. Кстати, раньше эти цифры явно указывались в Стандарте на топологию, но версия документа 2012 г. их уже не содержит.

Итак, предположим, что было принято решение о строительстве дата-центра некоего уровня. Был инициирован соответствующий проект, разработаны решения, подготовлен комплект документации, и проект ЦОДа успешно прошел сертификацию Uptime Institute на соответствие заявленному уровню надежности. Затем дата-центр был построен, т.е. построено (или реконструировано) помещение, подведены коммуникации, установлены и настроены соответствующие утвержденным проектным решениям оборудование и автоматизированные системы. Более того, ЦОД успешно прошел второй уровень сертификации Uptime Institute – сертификацию реализованных решений, и ему был присвоен ожидаемый уровень Tier.

Пока – всё, как принято у нас делать. Следующий шаг тоже наверняка ни у кого удивления не вызовет: передача построенного объекта эксплуатирующей структуре. Вот только в российской действительности, в отличие от зарубежной практики (которой мы еще коснемся), зачастую именно в этот момент и вспоминают об упомянутой структуре. Точнее – о необходимости ее наличия... Исключения, конечно, бывают, но при внимательном рассмотрении они часто оказываются не такими уж и исключениями.

Итак, объект построен, и с ним что-то надо делать. Делать у нас принято так: назначить ответственного за эксплуатацию, и пусть он сам со всем разбирается – разрабатывает предложения по организации, защищает бюджет,

формирует структуру команды, набирает персонал и ищет сервисных подрядчиков. Знакомая картина, не так ли?

И вот квалифицированный менеджер, получивший такой недешевый «подарок», приступает к делу. Прежде всего он выясняет, что хотя в мире дата-центров, имеющих сертификат Uptime Institute, существует множество, на одной шестой суши их общее число пока не превышает десятка (точнее, на момент написания статьи – всего два). А поскольку менеджер ответственный, он, конечно же, исследует доступные материалы этой организации, обнаруживает обсуждаемый нами стандарт и принимает решение учесть требования стандарта для своего ЦОДа. Каким образом ему лучше всего действовать с точки зрения рекомендаций стандарта?

Можно посоветовать следующий порядок действий, по существу являющийся высокоуровневым планом проекта:

1. Уточнить ожидаемые параметры обслуживания, убедиться, что они соответствуют заявленному Tier. Если это не так, дальнейшие шаги могут оказаться бессмысленны.
2. Понять, что собственно надо обслуживать: составить полный перечень систем и их компонентов, подлежащих обслуживанию и ремонту.
3. Выяснить, как правильно выполнять обслуживание и ремонт: разработать или получить иным способом технологические карты и описания операций обслуживания по всем системам и их компонентам.
4. Обеспечить надежное хранение и доступность всей документации по дата-центру, включая упоминаемую в п. 2.
5. Определить и описать основные операционные процессы: сформировать программу профилактического обслуживания, описать процесс устранения аварий и программу анализа отказов.
6. Разработать ресурсный план: определить необходимую численность и квалификационные требования к исполнителям, разработать организационную структуру и штатное расписание службы.
7. Организовать обеспечение реальными ресурсами: инициировать поиск и прием персонала, а также подбор подрядчиков.
8. Обеспечить развитие персонала и готовность к исполнению работ: внедрить процессы периодического обучения и порядок проведения инструктажей всех исполнителей, разработать полную программу обучения и повышения квалификации собственного персонала.

9. Принять решение о правилах взаимодействия с подрядчиками: подготовить соответствующие документы, договоры, SLA.

10. Построить систему управления обслуживанием: внедрить автоматизированную или чисто организационную систему контроля и управления исполнением операций обслуживания, обеспечить мониторинг основных параметров функционирования систем.

11. Сформулировать и зафиксировать правила поведения на объекте, порядок доступа, перемещения, размещения бытового оборудования, упаковки и т.д.

12. Обеспечить исполнение иных вспомогательных процессов и процедур: разработать и внедрить процессы управления финансами, мощностями, политики и процедуры функционирования объекта в целом.

13. Организовать переход к целевой операционной модели: провести начальное обучение персонала, обеспечить исполнение работ в соответствии с разработанными на предыдущих шагах элементами, образующими в совокупности целевую операционную модель.

14. Осуществить корректировку модели по итогам ее «опытной эксплуатации»: после того, как модель «притрется» и докажет свою работоспособность (на это может потребоваться более полугод), доработать ее с учетом внесенных практикой изменений и уточнений.

15. Сертифицировать операционную модель: провести аудит построенной операционной модели и ее реализации, получить сертификат Uptime Institute.

Этот план довольно объемный, но все же понятный и вполне реализуемый. Закономерны вопросы: каковы условия его успешности, возможные сроки, иные ограничения? Поскольку примеров построения такого рода модели в России пока нет, оценки попытаемся сделать на основании зарубежных проектов и практик. Итак, каким образом такого рода проект реализуется «там», в чем отличия и особенности?

По большому счету, план универсален. И, как обычно, сложности возникают в ходе его детализации.

Подводные камни внедрения

Как было сказано выше, основная отечественная проблема – это частичное или полное исключение периода эксплуатации и налагаемых им требований и ограничений из рассмотрения при планировании, проектировании и последующей реализации ЦОДа. В результате почти всегда происходит дублирование работы.

Действительно, в ходе строительства дата-центра без существенных дополнительных затрат времени и денег могут формироваться в нужных форматах и объемах и необходимая для последующей эксплуатации справочная и техническая документация, и требования к квалификации и ресурсному плану эксплуатирующей организации, и программа профилактического обслужива-

ния, и разнообразные процессы управления и обеспечения. Так ситуация выглядит при комплексном подходе.

У нас этого обычно не происходит, и организовывать эксплуатацию приходится с нуля, кропотливо выбирая из имеющегося набора документов необходимые данные, выявляя и заполняя пробелы. Особенно трудно бывает получить информацию по изменениям, внесенным в проект уже в ходе его реализации.

Другое существенное отличие – работа по общей регламентации деятельности: разработка планов, процессов и процедур и их документирование. Дело в том, что российская практика и требования регуляторов в отношении организации работ все еще носят строгий структурно-функциональный характер, который негибок, и часто при наложении на него процессной (по своей природе – матричной) модели возникают сложности. Здесь, как и при внедрении любых процессов, могут потребоваться значительные усилия.

Наконец, готовность к автоматизации. Хотя стандарт, рекомендуя строить систему управления обслуживанием, допускает ее реализацию «на бумаге», очевидно, что для крупных ЦОДов с большим числом элементов такой вариант будет неэффективен. Значит, нужна автоматизация, которая требует дополнительных затрат, усилий, конкретных знаний внедряемых продуктов. На Западе с этим как-то проще...

С учетом зарубежного опыта и перечисленных особенностей реализация представленного плана может занять от года до двух лет и более.

Основа успеха проекта – доступность необходимой информации, а также достаточная укомплектованность команды проекта работниками нужной квалификации. Команда проекта должна включать в себя специалистов, обладающих необходимыми знаниями по всем инженерным системам, специалистов по построению рекомендованных программ и процессов управления, специалистов по системам автоматизации управления обслуживанием и, конечно, группу управления проектом. Понятно, что даже талантливый и квалифицированный менеджер в одиночку с такой задачей за разумное время не справится. Ему однозначно потребуется помощь.

Что касается квалифицированных специалистов для построения службы эксплуатации, к счастью, у этой проблемы, помимо активного поиска и приема на работу такого рода сотрудников, есть еще одно надежное решение: соответствующие услуги готов предоставить сам Uptime Institute. Некоторые сложности, связанные с необходимостью адаптации документации к российскому законодательству, могут быть устранены силами российских компаний, имеющих соответствующий опыт. Несомненно, участие Uptime Institute в таком проекте обеспечит максимально высокое качество построенной операционной модели.

Дата-центры, сертифицированные по операционной устойчивости

Еще несколько лет назад Uptime Institute оценивал риски и перспективы обеспечения надежной эксплуатации дата-центра в рамках сертификации реализован-

ных решений ЦОДов. Одновременно с сертификационными документами эта организация предоставляла рекомендации по улучшению ситуации. Делалось это в качестве бонуса, скорее всего, поскольку на тот момент у Uptime Institute еще не было полной уверенности в полноте и достаточности требований для построения действительно хорошей операционной модели. Сегодня ситуация изменилась. Теперь есть отдельный стандарт, методика его применения, опыт сертификации.

Информация о дата-центрах, успешно прошедших сертификацию на соответствие требованиям операционной устойчивости, размещена на сайте Uptime Institute. На момент написания статьи их было пять: один – уровня Tier IV (дата-центр провинции Онтарио, Канада) и еще четыре – уровня Tier III (коммерческий дата-центр Fujitsu Services в Великобритании и три корпоративных ЦОДа: один – UnitedHealth Group и два – Target Corporation, все в США).

Напомним, ранее мы сделали предположение, что дата-центр имеет некоторый подтвержденный специальным сертификатом Uptime Institute уровень Tier. Это, безусловно, существенно сужает перечень потенциально заинтересованных в применении стандарта операционной устойчивости. В то же время многие положения стандарта будут полезны и при отсутствии у ЦОДа означенного сертификата. И хотя применять изложенные в стандарте идеи не возбраняется никому, но получить подтверждение правильности их применения без доброй воли Uptime Institute будет невозможно.

Понимая проблему, Uptime Institute совместно с представителями различных индустрий разработал отдельную специальную схему сертификации – Management and Operations Approval, предназначенную для оценки операционной модели действующих критичных дата-центров, не имеющих сертификата уровня Tier. Суть ее в следующем: в ходе сертификационного аудита оценива-

ется только операционная модель действующего дата-центра, в то время как по иным направлениям (характеристики здания и местоположение площадки) оценка не проводится. Выдаваемый в случае успеха по этой модели сертификат действует в течение двух лет. Действующий сертификат Management and Operations Approval на момент написания статьи имели восемь организаций – три в Великобритании (шесть площадок), три в США (три площадки) и две во Франции (восемь площадок).

Применимость стандарта для российских компаний

Как и всякое новое веяние, операционная устойчивость не может быть оценена однозначно. У нее будут как энтузиасты, так и критики. И кто победит, сказать сейчас трудно. В то же время не вызывает сомнения, что стандарт содержит действительно полезные идеи, которыми можно воспользоваться.

Будучи по сути документом отдельной коммерческой компании, стандарт не претендует на обязательность и не может быть в этом ключе рекомендован для применения на государственном уровне. Решение о его использовании и тем более – о необходимости сертификации на соответствие ему остается за менеджерами и владельцами конкретного дата-центра. С другой стороны, всё это не помешало получить фактическое признание стандарту Tier Standard: Topology. Поскольку Tier Standard: Operational Sustainability является его обоснованным продолжением, затрагивающим фазу эксплуатации дата-центра, без которой в целом теряется смысл усилий по строительству, логично предположить, что в ближайшей перспективе он также будет принят и признан за рубежом. А это, в свою очередь, позволяет надеяться, что в скором будущем мы станем свидетелями успешного применения стандарта Tier Standard: Operational Sustainability и в нашей стране. ИКС

Эволюция параметров микроклимата ЦОДов

Требования к микроклимату ЦОДов в последние годы неоднократно и существенно изменялись. Причина изменений – особенности дата-центров, учет и анализ которых позволяет обобщать основные направления развития систем их микроклиматической поддержки.



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

Современные ЦОДы, в которых используются вычислительные возможности стоечных (rack) и модульных (blade) серверов, работают при удельной мощности, превышающей 1080 Вт/кв.м. На сегодня, по данным Environmental Protection Agency, ЦОДы потребляют примерно 2% элект-

роэнергии, производимой в общемировом масштабе, а прирост их потребления составляет около 15% в год. Значительная доля расходуемой энергии приходится на климатическое оборудование, необходимость в котором очевидна, поскольку порядка 55% сбоев в работе электронного обо-

Эта статья стала последней для Е.П. Вишневого, нашего уважаемого, умного и интересного автора. Редакция «ИКС» приносит соболезнования коллегам и близким Евгения Петровича.

рудования связано с нарушением поддержания необходимой температуры (данные US Air Force Avionics Program). В связи с этим встает проблема оптимизации технологий и средств охлаждения воздуха, используемых в ЦОДах.

Требования к микроклимату

ЦОДы как объект микроклиматической поддержки имеют ряд характерных особенностей, параметры микроклимата в них существенно отличаются от общепринятых в практике кондиционирования воздуха. Во-первых, ЦОД – это по существу малообитаемый объект, поддержка микроклимата в котором, в отличие от обычных систем комфортного кондиционирования, имеет своей целью в первую очередь обеспечение работы ИТ-оборудования.

Во-вторых, предъявляются повышенные требования к надежности работы ИТ-оборудования, размещаемого в ЦОДах на условиях услуг colocation путем аренды стоек и занимаемых площадей. Показатели надежности, определяемые коэффициентом эксплуатационной готовности, достигают значений от 99,6712% для ЦОДа уровня Tier 1 до 99,9954% для ЦОДа уровня Tier 4. На перспективу основные ИТ-производители ведут разработку так называемой программы Five Nine, предусматривающей достижение коэффициента эксплуатационной готовности

Табл. 1. Классы микроклиматической поддержки ЦОДов

Зоны обслуживания	2004	2008	2011
Основные залы	REC	REC	REC
		1	A1
		2	A2
			A3
Вспомогательные помещения			A4
		3	B
		4	C

99,999%, что соответствует отсутствию эксплуатационной готовности каналов обработки информации не более 5,47 мин в году.

В-третьих, основной причиной сбоев в работе ИТ-оборудования являются нарушения электрических контактов из-за температурных деформаций многослойных плат и конструктивных элементов. Следовательно, с точки зрения микроклиматической поддержки важны не столько номинальные значения температуры и влажности, сколько их стабильность во времени и пространстве.

И наконец, большие финансовые вложения требуют максимально возможной экономической эффективности, что определяется как уровнем капитальных затрат, так и общей стоимостью владения

б и з н е с - п а р т н е р

Не меньше ответственности, а больше возможностей

Еще относительно недавно климатические параметры в ЦОДах регламентировались локальными нормами и специфическими требованиями поставщиков ИТ-оборудования. Нередко отсутствие общих норм приводило к противоречиям в локальных документах, кроме того, информация была чрезвычайно фрагментирована, что серьезно усложняло работу инженеров. Данный пробел был исправлен техническим комитетом TC 9.9 ассоциации ASHRAE, выпустившим директивы по выбору климатических параметров в ЦОДе.

В настоящий момент на рекомендации TC 9.9 широко опираются как поставщики оборудования по всему миру, так и инженерный персонал проектирующих организаций. Основной задачей, на которой сфокусировались специалисты TC 9.9, стало расширение допустимых пределов условий эксплуатации оборудования. В первую очередь последовательное расширение границ климатических параметров направлено на увеличение энергоэффективности решений, применяемых в ЦОДах.

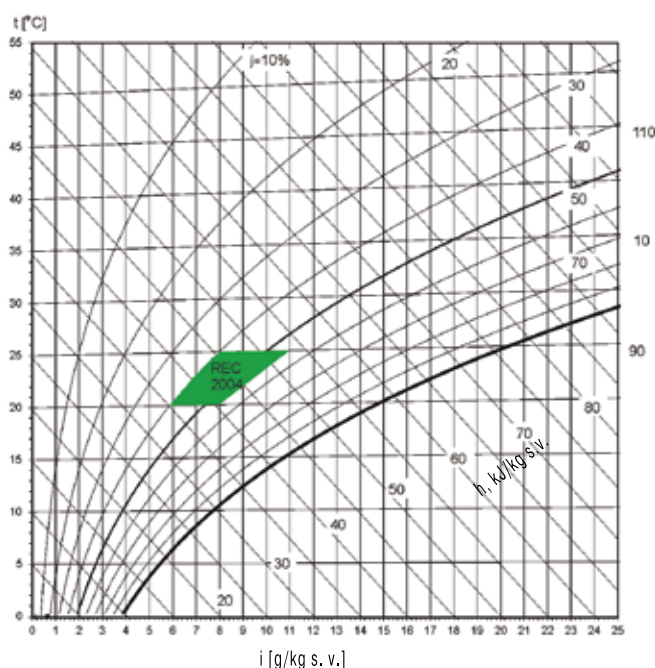
Но ошибочно полагать, что расширение пределов эксплуатации оборудования влечет за собой снижение ответственности, лежащей на системе кондиционирования ЦОДа. Напротив, перспективные нормы ставят перед производителями климатики новые задачи. Специалисты компании STULZ, которая находится в авангарде разработчиков систем прецизионного кондиционирования, предусмотрели возможность работы оборудования при высоких температурах возвращаемого воздуха. А использование систем свободного охлаждения, созданных компанией, в сочетании с расширением допустимых температурных интервалов в техническом помещении, позволяет достичь невиданных ранее показателей энергоэффективности. При этом, безусловно, стоит придерживаться рекомендуемого ASHRAE климатического диапазона и соблюдать разумный баланс между повышением PUE и сохранением уровня надежности оборудования.

Так, повышая допустимую температуру подаваемого в ИТ-оборудование воздуха, мы не только увеличиваем термодинамическую эффективность систем кондиционирования, но и существенно сокращаем время работы оборудования в режиме компрессорного охлаждения. В условиях Центрального региона России одна из наиболее эффективных в мире систем непрямого естественного охлаждения STULZ DFC (Dynamic Free Cooling) позволит экономить электроэнергию до 97% времени в году за счет работы в режиме свободного или смешанного охлаждения. А при использовании системы прямого естественного охлаждения STULZ DFC2 компрессоры можно не включать практически круглый год.



(495) 747-6000
www.stl-r.ru

Рис. 1. Область допустимых значений параметров микроклимата ЦОДа в рабочем режиме (норматив 2004 г.)



(ТСО), а они существенным образом зависят от обеспечиваемых параметров микроклимата.

Эволюция климатических параметров

Исходя из указанных особенностей, нормируемые параметры микроклимата ЦОДа за последние годы изменялись несколько раз. Из табл. 1 видно, как начиная с 2004 г. расширялось число классов микроклиматической поддержки ЦОДов, установленных техническим комитетом Американского общества инженеров по отоплению, холодильной технике и кондиционированию воздуха (American Society of Heating, Refrigeration, and Air-Conditioning Engineers; ASHRAE).

Табл. 2. Допустимые значения параметров микроклимата ЦОДа в рабочем режиме (норматив 2008 г.)

Класс	Параметры микроклимата: предельные значения (границы области допустимых значений)		
	DP, °C	t, °C	φ, %RH
REC 2008	>5,5; <15 (5,5; 5,5; -; 15; 15)	>18; <27 (18; -; 27; 27; -; 18)	>20; <80 (-; 20; 20; -; 80; 80)
1	<17 (-; -; 17; 17; -)	>15; <32 (15; 32; 32; -; 15)	>20; <80 (20; 20; -; 80; 80)
2	<21 (-; -; 21; 21; -)	>10; <35 (10; 35; 35; -; 10)	>20; <80 (20; 20; -; 80; 80)
3	<28 (-; -; 28; 28; -)	>5; <35 (5; 35; 35; -; 5)	>8; <80 (8; 8; -; 80; 80)
4	<28 (-; -; 28; 28; -)	>5; <40 (5; 40; 40; -; 5)	>8; <80 (8; 8; -; 80; 80)

Табл. 3. Допустимые значения параметров микроклимата ЦОДа в неработающем состоянии (норматив 2008 г.)

Класс	Параметры микроклимата: предельные значения (границы области допустимых значений)		
	DP, °C	t, °C	φ, %RH
1 и 2	<27 (-; -; 27; 27; -)	>5; <45 (5; 45; 45; -; 5)	>8; <80 (8; 8; -; 80; 80)
3 и 4	29 (-; -; 29; 29; -)	>5; <45 (5; 45; 45; -; 5)	>8; <80 (8; 8; -; 80; 80)

В 2004 г. был установлен единственный класс ЦОДов – рекомендуемый (Recommended; REC). Для него были заданы следующие предельные значения: температура $t > 20; < 25$ °C (границы области допустимых параметров* – 20; 25; 25; 20 °C); влажность $\phi > 40; < 55$ %RH (границы области допустимых параметров – 40; 40; 55; 55 %RH). Нормируемые значения микроклиматических параметров для этого класса в рабочем режиме детализирует рис. 1.

В 2008 г. число классов и нормируемых микроклиматических параметров существенно изменилось (табл. 2). Помимо нормируемых значений температуры t и относительной влажности ϕ введены ограничения для точки росы – Dew Point (DP, °C).

В дополнение к рабочему режиму установлены также нормируемые значения микроклиматических параметров для ЦОДа в неработающем состоянии (табл. 3), что соответствует периодам монтажа и демонтажа ИТ-оборудования, плановых профилактических работ.

В 2011 г. общее число классов в части нормируемых микроклиматических параметров вновь было увеличено (табл. 4). Были выделены классы микроклиматических параметров (обозначаемые буквами В и С) для вспомогательных помещений, к которым относятся рабочие места, оборудованные ПК, рабочими станциями и принтерами. Из рис. 2 видно, как были расширены области допустимых значений микроклиматических параметров основных залов ЦОДа и вспомогательных помещений в рабочем состоянии.

Изменились в 2011 г. и нормативные значения микроклиматических параметров ЦОДа в нерабочем режиме (рис. 3, табл. 5).

Некоторые тенденции

В предыдущих публикациях («ИКС» №4'2011, с. 85–88; №6'2012, с. 83–84; №11'2012, с. 83–87) мы обсуждали термодинамические аспекты использования свободного и адиабатического охлаждения ЦОДов в дополнение к традиционному механическому охлаждению или взамен него. Анализ описанных в настоящей статье изменений нормативов позволяет сделать следующие выводы.

* В качестве границы области допустимых параметров здесь и в таблицах указаны значения при обходе характерных точек контура области по часовой стрелке.

Табл. 4. Допустимые значения параметров микроклимата основных залов ЦОДа и вспомогательных помещений в рабочем режиме (норматив 2011 г.)

Класс	Параметры микроклимата: предельные значения (границы области допустимых значений)		
	DP, °C	t, °C	Ф, %RH
REC 2011	>5,5; <15 (5,5; 5,5; 15; 15; -)	>18; <27 (18; 27; 27; -; 18)	<60 (-; -; -; 60; 60)
A1	<17 (-; -; 17; 17; -)	>15; <32 (15; 32; 32; -; 15)	>20; <80 (20; 20; -; 80; 80)
A2	<21 (-; -; 21; 21; -)	>10; <35 (10; 35; 35; -; 10)	>20; <80 (20; 20; -; 80; 80)
A3	>-12; <24 (-12; -12; -; 24; 24; -)	>5; <40 (5; -; 40; 40; -; 5)	>8; <85 (-; 8; 8; -; 85; 85)
A4	>-12; <24 (-12; -12; -; 24; 24; -)	>5; <45 (5; -; 45; 45; -; 5)	>8; <90 (-; 8; 8; -; 90; 90)
B	<28 (-; -; 28; 28; -)	>5; <35 (5; 35; 35; -; 5)	>8; <80 (8; 8; -; 80; 80)
C	<28 (-; -; 28; 28; -)	>5; <40 (5; 40; 40; -; 5)	>8; <80 (8; 8; -; 80; 80)

1. Имеет место устойчивая тенденция расширения температурного и влажностного диапазонов в спецификациях основных поставщиков ИТ-оборудования, что обусловлено конструктивными и технологическими особенностями современных электронных плат (блейд-серверов) и их компаундной защиты.

2. Все более привлекательным становится использование систем свободного охлаждения (Free Cooling), и систем испарительного (адиабатического) охлаждения – прямого (Direct Evaporative Cooling) и косвенного (Indirect Evaporative Cooling), в которых входной и выходной потоки замыкаются внутри обслуживаемого помещения. Все шире ис-

б и з н е с - п а р т н е р

Расширение температурного диапазона в машзале ЦОДа – тренд настоящего времени



Владислав ЯКОВЕНКО,
руководитель отдела
инфраструктурных проектов,
ООО «Компания КОМПЛИТ»,
CDCDP, ATD

Для подклассов A3/A4 по стандартам ASHRAE 2011 диапазон температур уже настолько расширен, что сегодня в условиях Северо-Западного региона России системы охлаждения более 90% времени могут работать в режиме фрикулинга. И даже для наиболее строгих классов A1 и A2 настройка системы на большой градиент дает заметный выигрыш. Справедливости ради необходимо отметить, что при снижении затрат на саму систему охлаждения несколько увеличивается мощность, потребляемая серверами (в основном за счет усиленной работы вентиляторов оборудования).

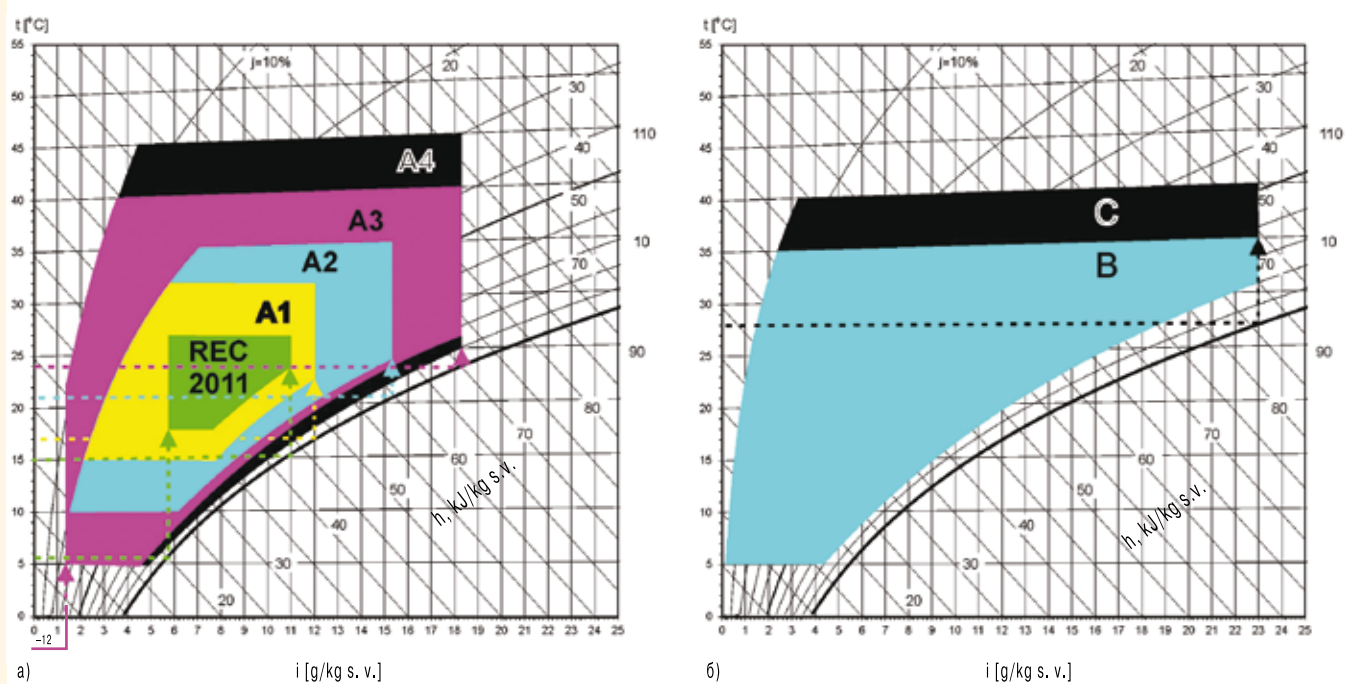
В будущем намечается развитие двух тенденций: с одной стороны, производители ИТ-оборудования будут постепенно повышать допустимую температуру воздуха на входе в серверы, с другой – помещения ЦОДов будут разбиваться на подтипы в зависимости от требований к надежности конкретного сервера. В ближайшие годы производители будут предлагать различные варианты компромиссов между стоимостью оборудования, его надежностью и производительностью.

Общее правило: чем строже требования к микроклимату, тем выше энергопотребление ЦОДа. Корпоративные ЦОДы high quality-сегмента останутся на площадках уровня Tier 3 с высокоточным поддержанием почти привычной температуры в +23–25°C. Все остальные ЦОДы, как коммерческие, так и операторские, постепенно начнут повышать температуру в машинных залах. Это значительно улучшит показатель PUE, а значит, позволит снизить совокупную стоимость владения и повысить рентабельность.

Один из вариантов экономии, даже в коммерческом ЦОДе, – это организация машзалов различной температуры внутри единого пространства дата-центра. Заметим, что первые реализации систем воздушного охлаждения с экономайзерами уже появились на нашем рынке. Не за горами строительство совмещенных (или расположенных рядом) объектов «ЦОД – здание» с перераспределением «бесплатной» тепловой энергии (класс W5 ASHRAE).

Резюмируя все вышесказанное, отметим, что нахождение компромисса между производительностью, стоимостью, энергопотреблением и надежностью объекта – одна из главнейших компетенций проектировщика дата-центров.

Рис. 2. Область допустимых значений параметров микроклимата основных залов ЦОДа (а) и вспомогательных помещений (б) в рабочем режиме (норматив 2011 г.)



пользуются и системы с разделенными потоками (Separated Evaporative Cooling), известные как KyotoCooling или, в отечественном исполнении, FFC (Full Free Cooling).

3. Поскольку требования к обеспечению стабильности поддерживаемых микроклиматических параметров неизменны (а в перспективе будут ужесточаться), применяемые системы охлаждения немеханического типа должны оснащаться развиты-

ми системами управления воздушными потоками, лабильными и малоинерционными по своей природе.

4. Роль механического охлаждения (Mechanical Cooling), используемого в системах чиллер – прецизионный кондиционер/фэнкойлы/холодные балки, сводится к снятию пиковых нагрузок в наиболее неблагоприятных условиях. В силу высокой теплоемкости жидкостного контура точность поддержания микроклиматических параметров при этом имеет ограничения.

Рис. 3. Область допустимых значений параметров микроклимата ЦОДа в неработающем состоянии (норматив 2011 г.)

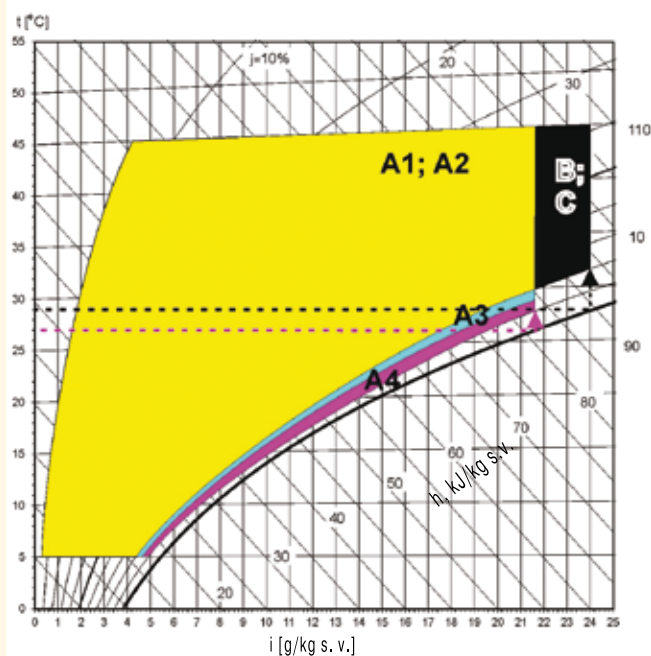


Табл. 5. Допустимые значения параметров микроклимата ЦОДа в неработающем состоянии (норматив 2011 г.)

Класс	Параметры микроклимата: предельные значения (границы области допустимых значений)		
	DP, °C	t, °C	Ф, %RH
A1; A2	<27 (-; -; 27; 27; -)	>5; <45 (5; 45; 45; -; 5)	>8; <80 (8; 8; -; 80; 80)
A3	<27 (-; -; 27; 27; -)	>5; <45 (5; 45; 45; -; 5)	>8; <85 (8; 8; -; 85; 85)
A4	<27 (-; -; 27; 27; -)	>5; <45 (5; 45; 45; -; 5)	>8; <90 (8; 8; -; 90; 90)
B; C	<29 (-; -; 29; 29; -)	>5; <45 (5; 45; 45; -; 5)	>8; <80 (8; 8; -; 80; 80)



Рассмотренные нами тенденции изменения нормативной базы в части параметров микроклимата ЦОДов открывают широкие перспективы использования возобновляемых энергоресурсов – свободного и адиабатического охлаждения, что будет способствовать повышению экономичности и экологичности современных проектов. ИКС

Видеосистемы без границ

Современные программно-аппаратные комплексы с доступом в систему из любой точки обеспечивают охранный видеоконтроль территориально распределенных объектов разного масштаба: и работу видеосистемы в штатном режиме, и реагирование на экстренные ситуации.

Для видеомониторинга крупных объектов и организаций с филиальной структурой целесообразно использовать распределенные сетевые системы. В подобных системах гарантированно не существует единой точки отказа, в ней реализовано несколько уровней резервирования, чтобы обеспечить максимум надежности и работоспособности. Такую систему легко масштабировать по количеству каналов, глубине архива и производительности, модифицировать и наращивать без остановки работы.

В рамках распределенной системы могут быть задействованы сотни и тысячи камер, гибридные и сетевые регистраторы, хранилища данных, посты мониторинга и др., при этом не существует ограничений на их физическое размещение. Все компоненты располагаются в любом удобном месте локальной/глобальной сети, и с каждого поста авторизованный оператор имеет к ним доступ. Не составит труда включить в единую систему вновь созданные объекты или добавить новые устройства.

Отметим также обширные возможности интеграции с другими системами, как на аппаратном, так и на программном уровне, и наличие готовых интеграционных решений.

Неограниченная масштабируемость

Наилучший выбор для создания сетевой системы видеонаблюдения территориально распределенного объекта – масштабируемая аппаратно-программная платформа с высоким уровнем резервирования и отказоустойчивости. Примером может служить Pelco Endura от компании Schneider Electric. Endura относится к решениям СТН для критически важных объектов: системы «Безопасный город», инфраструктурных проектов (аэропорты, транспортные магистрали, вокзалы), но может быть установлена и на крупных промышленных предприятиях, в торгово-офисных центрах, гостиницах и др.

Начиная с первого поколения Endura создавалась как комплексное решение для построения распределенных IP-систем видеонаблюдения, работающих в режиме 24x7. Она не имеет ограничений по количеству источников видеoinформации, рабочих мест операторов, по объемам видеоархива и, по сути, представляет собой набор компонентов, из которых строится индивидуальная система на базе сетевых протоколов.

Оптимальное решение для сравнительно небольшого объекта – система EnduraXpress, ядром которой являются автономные сетевые видеорегистраторы EE500.

Эти устройства предназначены для записи, хранения и просмотра видеопотоков с разрешением до HD, они используют кодеки H.264/MPEG-4, рассчитаны на работу с 32 или 64 потоками при общей скорости регистрации 250 Мбит/с и поставляются с лицензиями на рабочие станции Endura WS для организации рабочих мест операторов. NVR имеют встроенное ПО для конфигурирования системы, совместимы со всеми камерами и видеосерверами Pelco, а также других производителей, подключенными через модуль UDI5000-CAM.

EnduraXpress поддерживает прямое управление PTZ-функциями камер и цифровым зумом, а также функцию Zone of Interest («Зона интереса»): оператор может выделять и масштабировать определенные участки в кадре, сохраняя на экране отображение всей сцены целиком, причем в применении как к «живому» видео, так и к архивным видеофрагментам.

Для создания крупномасштабной видеосистемы необходима многокомпонентная версия Endura, позволяющая реализовать СТН на несколько тысяч камер (например, 4200 IP-камер функционируют в казино San Manuel в Калифорнии, 2700 – в Дубайском метро и т.д.) на оборудовании одного производителя, а при необходимости добавить дополнительные функции и провести интеграцию со сторонними системами.

Pelco Endura имеет открытую архитектуру. Минимально необходимый перечень компонентов включает System Manager SM5200 – аппаратно-программное устройство с удобным пользовательским интерфейсом для администрирования и конфигурирования системы, настройки сети, сервисов и т.д. и встроенным веб-сервером/браузером для просмотра «живого» видео, поиска и воспроизведения; сетевой видеорегистратор NSM5200, поддерживающий до 24 Тбайт встроенной памяти и массив RAID 6 (до двух дисков с «горячей заменой»); рабочую станцию WS5070, используемую в качестве поста наблюдения. Наряду с этим потребуются источники видеоданных, в качестве которых могут выступать сетевые камеры (Sarix, Spectra IP, Spectra HD, Sarix TI) и энкодеры Pelco (серии NET5400T) либо сторонних производителей.

Функционал системы весьма обширен, поэтому кратко перечислим основное. Предусмотрена поддержка видеокодеков MPEG-4, H.264 (Main, Base, High profile),



Михаил МАЛОВ,
ведущий эксперт,
«АРМО-Системы»



Универсальная видеосистема Endura обеспечивает безопасность критически важных объектов

трансляция многопоточного видео (в том числе с мегапиксельным разрешением), многоадресная маршрутизация Multicast (одновременная передача данных от одного источника на неограниченное число приемников, что позволяет видеть и записывать видеосигнал сразу на нескольких постах без увеличения нагрузки на сеть), запись звука. Имеется возможность использования электронных карт объекта, видеоаналитики, вывода изображений на видеостены и др.

К разряду уникальных относятся такие функции системы, как EnduraStor, которая оптимизирует объем памяти (уменьшает объем данных и позволяет обойтись меньшим объемом памяти), «прореживая» архивное видео по истечении заданного времени хранения и сохраняя только опорные кадры, а также EnduraView, которая автоматически подбирает оптимальные параметры видеопотока, уменьшая нагрузку на аппаратную платформу устройств и сеть передачи данных. В перспективе система будет развиваться в направлении возможностей доступа к видео из любой точки мира, работы с системой через приложение PelcoMobile для мобильных устройств под управлением Android и iOS. Немаловажно, что в будущем система станет ONVIF-совместимой.

Всё под контролем

Для организации централизованного и территориально распределенного видеонаблюдения на особо важных объектах предназначена система NiceVision Net компании Nice Systems. Это решение корпоративного уровня имеет открытую архитектуру, соответствует стандартам ONVIF и легко интегрируется с оборудованием сторонних производителей, системами безопасности и СКУД, различными средствами обнаружения, программными приложениями и модулями. NiceVision Net позволяет вести запись многопоточного видео от различных источников одновременно с визуализацией изображений на экране оператора и аналитической обработкой видеосигналов.

Система подходит для объектов различной сложности независимо от их размеров, окружающих условий, технологических сред и типов архитектур, отличается

высокой производительностью, надежностью, универсальностью, низкой совокупной стоимостью владения (ТСО). Она доступна в трех версиях: простейшая, eXpress, предназначена для относительно небольших объектов, с поддержкой до 64 камер и 10 клиентов; версия Professional – мультисерверное решение с поддержкой до 200 камер и 20 пользователей, обеспечивающее видеоконтроль транспортных узлов, электростанций и др. И наконец, Enterprise – система обеспечения безопасности особо крупных объектов, аэропортов, железнодорожных вокзалов, городских центров и др., поддерживающая неограниченное количество камер и одновременных подключений.

NiceVision Net, независимо от версии, предоставляет пользователям расширенные возможности видеомониторинга и такие функции, как ситуационный менеджмент, администрирование при помощи веб-браузера и мобильных устройств, поиск в архиве, автоматическая группировка событий по их важности/месторасположению, управление PTZ-камерами и др. Благодаря запатентованной технологии Zero Points of Failure система имеет повышенный уровень отказоустойчивости.

Интегрированный пакет программного обеспечения NiceVision позволяет организовать как локальный пост видеонаблюдения, так и глобальную мультисерверную систему видеомониторинга с неограниченным числом конечных устройств и удаленных пользователей, полностью настраиваемую с централизованного пункта управления. Ключевые функции ПО – удобная системная навигация, обеспечение доступа со смартфонов и через веб-клиенты, работа в режиме виртуального матричного коммутатора, вывод изображений на несколько мониторов, управление событиями (Event Management), экспорт и архивирование данных, визуализация и синхронизация видео и др.

Приложение Site DashBoard с интуитивно понятным интерфейсом обеспечивает централизованный видеоконтроль крупномасштабных объектов и территорий большой площади. Информационная панель оператора предоставляет доступ к видео от любой камеры одним щелчком мыши, обеспечивает просмотр текущего и архивного видео на одном мониторе, отображение



Профессиональная система NiceVision Net предназначена для видеонаблюдения на крупных объектах

информации о событиях, одновременно происходящих на удаленных друг от друга объектах, быстрое реагирование на нештатные ситуации.

В линейку NiceVision Net входят гибридные видеорегистраторы SVR-H, энкодеры NVE 1000, декодеры NVD1002 и NVD5104 и другие устройства. Одним из преимуществ системы является поддержка видеоаналитики NICE: выявление несанкционированного проникновения на закрытые охраняемые территории (Intrusion Detection), определение транспортных средств, припаркованных в неполюженном месте или создающих угрозу (Vehicle Detection), нахождение забытых/оставленных предметов, например багажа в аэропортах и транспортных терминалах (Baggage Detection), подсчет людей и транспортных средств и др.

NiceVision Net интегрирована с программной платформой Nice Situator, которая обеспечивает своевременное получение сигнала о возникновении тревожного события, предоставляет информацию о месте и времени происшествия, позволяет анализировать эти данные, выбирать алгоритмы реагирования, координировать действия сотрудников охраны. Благодаря интеграции с решением Nice Inform IP-видеосистема дает возможность управлять системами оповещения при возникновении тревожных ситуаций, использовать мультимедийные приложения и вести хронологическую регистрацию происшествия.

Комплексный подход

Многофункциональную систему видеомониторинга SkyPoint для крупных и территориально распределенных объектов разработала компания Lenel, входящая в корпорацию UTC (United Technologies Corporation) как часть UTC Climate, Controls & Security. SkyPoint предназначена для создания IP-видеосистем с большим числом каналов и включает в себя аппаратные и программные компоненты. Она может работать с неограниченным количеством аналоговых/IP-камер, видеосерверов и других устройств таких известных производителей, как Arecont Vision, AXIS, Bosch, Cisco, JVC, Pelco и др.

Система рассчитана на эксплуатацию на предприятиях, в транспортной инфраструктуре, крупных корпорациях и компаниях, государственных и коммерческих структурах и др. Она работает с сетевыми видеорегистраторами (NVR) и программным пакетом OnSSI для управления видеоданными: NetDVMS класса enterprise; NetDVR для односерверных средних/распределенных систем; ProSight-SMB для малого и среднего бизнеса. Кроме того, она совместима с Lenel Network Video Recorder (LNVR).

Система имеет открытую архитектуру, интуитивно понятный интерфейс, обеспечивает полнофункциональное администрирование и управление компонентами и данными, в том числе с помощью сенсорных панелей touchscreen. Простая навигация по камерам и узлам сети обеспечивается за счет поддержки иконок камеры/групп камер с масштабируемыми «привязан-

ными» картами: одним прикосновением к активной карте оператор может выбрать необходимые ему камеры, а также быстро получить доступ к планам помещений с указанием мест их размещения (поддерживаются карты на базе GIS).



Функция «Квантование времени» в системе SkyPoint позволяет быстро найти в видеозаписи момент, когда произошло событие

Среди задач, которые решает SkyPoint, – непрерывный видеомониторинг, мгновенное реагирование на тревожные события и архивирование аудио- и видеоданных независимо от количества подключенных к системе камер, удаленное управление PTZ-камерами (в том числе поворотными и Speed Dome, а также панорамными с объективом «рыбий глаз»), видеоаналитика и др. Интеллектуальный поиск в архиве обеспечивается функциями Smart Search, Scalable Kinetic Timeline (поиск с помощью навигационного инструмента «Кинетическая временная шкала») и Time Slicing (функция «Квантование времени» для немедленного доступа к видеозаписям момента, в который произошло событие).

SkyPoint работает с четырьмя типами клиентских приложений: базовое SkyPoint Client устанавливается на клиентском ПК; NetGuard Web Client предназначено для удаленного доступа к серверу и управления; NetCell и NetPDA Client – для мобильного видеоконтроля; NetMatrix и NetSwitcher имеют функции виртуального матричного коммутатора. Все приложения подключаются к единой, динамически обновляемой базе данных тревожных событий, обеспечивая скоординированную работу операторов, персонала и сотрудников службы безопасности.

Платформа Lenel SkyPoint позволяет не только вести видеонаблюдение, но и экспортировать данные в другие программные продукты, поддерживает конвертирование данных из других систем, включая средства анализа видеоизображений, управления доступом. При использовании в составе системы безопасности OnGuard она может быть интегрирована с другими системами, включая СКУД, ОПС, системы физической и логической безопасности. ИКС

Тонкие клиенты N-серии

предназначены для быстрой и недорогой виртуализации рабочих мест в территориально распределенных организациях.

N-серия тонких клиентов NComputing на базе процессора Numo 3 System-on-Chip включает модели N400 и N500. Их особенность – поддержка протокола HDX компании Citrix.



NComputing N400 – терминалы начального уровня. Основные характеристики: питание от Numo 3; энергопотребление < 5 Вт; резервное питание < 1,5 Вт; память DRAM – 256 Мбайт; дисплей с разрешением 1920×1080 (второй дисплей не

поддерживается). Устройство имеет порт 10/100 Ethernet (Wi-Fi не поддерживается), кардридеры и четыре порта USB 2.0 для подключения периферии. Терминал допускает запуск легких мультимедийных приложений в разрешении HD 720p с возможностью обработки графики на стороне сервера.

Старшая модель N500 самостоятельно справляется с рендерингом видео в разрешении 1080p и оснащена портом 10/100/1000 Ethernet. Опционально предусмотрена возможность беспроводного подключения по Wi-Fi и работы одновременно с двумя мониторами.

Терминалы NComputing позволяют сократить расходы на электроэнергию на 90% в сравнении с индивидуальными компьютерами, потребляющими 110 Вт и более.

Ориентировочная цена: N400 – \$129, N500 – \$199.

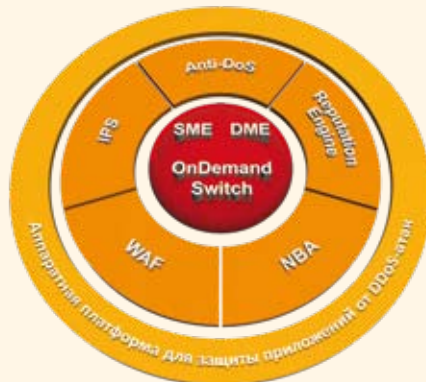
«Тайле»: +7 (495) 710-7125

Решение для противодействия кибератакам

Radware DefensePro x420 – аппаратная платформа для защиты приложений от DDoS-атак, способная справиться с атаками мощностью до 25 млн пакетов/с и 40 Гбит/с. Оснащена портами 10G и 40G.

DefensePro различает и разделяет аппаратным образом трафик легитимных пользователей и вредоносный трафик и обрабатывает каждый из них отдельно. Это обеспечивает сохранение качества обслуживания легитимных пользователей даже под массовой атакой на приложение.

В состав платформы входят модули проверки и анализа трафика, включая Anti-DoS, NBA, IPS, WAF и Reputation Engine, которые осуществляют постоянный мониторинг трафика и защищают сети, серверы и приложения от широкого спектра известных и новых видов кибератак. В DefensePro также используется запатентованная технология сигнатур реального времени на основе поведенческого анализа, по-



зволяющая за 18 с в автоматическом режиме обнаруживать начинающиеся атаки и успешно им противостоять.

Платформа включает два специализированных аппаратных компонента: DME (DoS Mitigation Engine) для предотвращения DoS/DDoS flood-атак и SME (StringMatch Engine) для защиты на основе сигнатур.

Механизм ответного реагирования в DefensePro может достигать производительности до нескольких миллионов ответных действий в секунду.

Radware: 8 (800) 100-6211

ERP-система

с отраслевыми модулями

В новой версии ERP-системы Microsoft Dynamics AX 2012 существенно изменен принцип комплектации продукта. В состав единой платформы кроме базовых функций, общих для компаний любой специализации, теперь включены пять отраслевых модулей, ранее поставлявшихся в виде отдельных решений. Эти модули предназначены для выполнения операций и управления бизнесом производственных компаний, дистрибьюторов, предприятий розничной торговли, государственных учреждений и компаний, предоставляющих профессиональные услуги. Такая универсальность позволит заказчикам не только сократить затраты на «дотачивание» решения в соответствии с особенностями своей деятельности, но и при необходимости быстро диверсифицировать бизнес. Для этого в ERP-системе есть средства для разворачивания дополнительных модулей и подключения их к уже работающему решению.

Наличие в едином продукте локализованных редакций для 36 стран мира, в том числе для России, упростит компаниям выход на внешние рынки и подключение филиалов, открываемых в других странах.

В новой версии ERP-системы улучшена масштабируемость – ее можно настроить для работы и в небольшой компании, и в крупном территориально распределенном холдинге.

По сравнению с предыдущей версией существенно изменена политика лицензирования Dynamics AX 2012. Новая ERP-система входит в комплект ПО от Microsoft, доступного в рамках корпоративного лицензионного соглашения Enterprise Agreement. Кроме того, если раньше заказчики могли купить лицензии только для одного вида пользователей, то теперь доступны сразу четыре вида лицензий с разным набором функциональных возможностей.

Microsoft: +7 (495) 967-8585

Full HD-видеокамеры

Видеокамеры HC-X920/X920M/X910 оснащены системой 3MOS PRO с поддержкой технологии BSI (Back Side Illuminated), существенно увеличивающей чувствительность сенсора 3MOS. Обновленная система 3MOS PRO состоит из объектива LEICA Dicomar F1.5, сенсора 3MOS и процессора изображения Crystal Engine Pro II. На переднюю линзу объектива LEICA Dicomar F1.5 нанесено нанопокрывание, которое повышает резкость и разрешение изображения. Процессор Crystal Engine Pro II обеспечивает эффективное подавление шумов.

Горизонтальное разрешение в 1080 строк позволяет снимать видео в разрешении Full HD. При помощи опционального 3D-конвертера VW-CLT2 возможна 3D-видеосъемка в разрешении Full HD. Доступны 5,1-канальная аудиозапись, зум и фокусировка микрофона, а также функция подавления шума ветра. Поддерживается возможность копирования информации на внешний жесткий диск.

Видеокамеры имеют широкоугольный объектив с фокусным расстоянием 29,8 мм и 25-кратным интеллектуальным зумом и сенсорный ЖК-экран с разрешением 1 152 000 точек и диагональю 3,5". Фотосъемка может осуществляться с разрешением 20,4 Мпиксел.

Модели серии 920 оснащены уровнем, который автоматически корректирует наклон изображения, незаметный человеческому глазу, а также пятиосной системой оптической стабилизации изображения HYBRID O.I.S., которая подавляет размытие изображения.



Для профессиональной видеосъемки предусмотрены кольцо ручного управления и электронный видоискатель (EVF) с разрешением, эквивалентным 263 424 точкам.

Модели HC-X920/X920M снабжены встроенным модулем Wi-Fi, который позволяет удаленно управлять видеокамерой с помощью смартфона, а также в реальном времени транслировать видео. Предусмотрена функция, отправляющая уведомление о начале трансляции на указанный заранее адрес электронной почты. С помощью приложения Panasonic Image App можно удаленно проверить аудиозапись, использовать зум и спустить затвор, полностью контролируя процесс съемки на экране смартфона или планшета. Также со смартфона или планшета можно включить функцию воспроизведения ключевых фрагментов.

Panasonic: +7 (495) 270-1635

Инструмент удаленного управления ИТ-инфраструктурой

Kaseya – модульная система для удаленной поддержки работоспособности и обслуживания ИТ-инфраструктуры, ориентированная на предприятия среднего и малого бизнеса. Все модули интегрированы между собой и управляются из единой веб-консоли.

Доступ к модулям и группам управляемых объектов регулируется гибкой системой прав. Kaseya собирает и обрабатывает результаты работы всех модулей в едином информационном центре, который генерирует отчеты на основе полученной информации. Механизм политик Kaseya позволяет автоматизировать применение конфигураций модулей на управляемых объектах. Задачи в модулях выполняются по расписанию. Расписания либо составляются администратором, либо задаются автоматически в соответствии с установленными политиками.

В Kaseya реализована модель превентивного и проактивного решения проблем. Превентивно выполняются установка обновлений, защита от вирусов и шпионов, резервное копирование данных и систем, мониторинг ключевых параметров и т.д.

Кроме инструментов безопасности в состав Kaseya входят модули, предназначенные для отслеживания изменений и поддержки имеющейся инфраструктуры. Модуль распространения ПО и распространения образов помогает ввести в эксплуатацию новый компьютер, установить новую программу или обновить уже установленную. Инвентаризация дает сведения об установленном аппаратном и программном обеспечении, используемых лицензиях. Модуль аудита выявляет изменения в аппаратной и программной частях, а также занятые или освобожденные лицензии. Модуль обнаружения сетевых устройств позволяет контролировать новые устройства, подключающиеся к локальной сети. Специальный модуль служит для управления и синхронизации объектов с доменом Active Directory. Также в Kaseya входят модуль расчетов с клиентами, система Help Desk и система учета времени, затраченного системным администратором на выполнение ИТ-задач.

Использовать Kaseya можно по лицензии, ежегодной или ежемесячной подписке – на своем оборудовании или по подписке в облаке по модели SaaS.

Sparxent Distribution: +7 (985) 960-6272

ДАТАЛАЙН

Тел.: (495) 784-6505
Факс: (495) 784-6506
E-mail: info@dtln.ru
www.dtln.ru с. 45

ИТ-ГРАД

Тел.: (812) 313-8815
E-mail: info@it-grad.ru
www.it-grad.ru с. 51

КОМПАНИЯ КОМПЛИТ

Тел.: (812) 740-3010
Факс: (812) 740-3011
E-mail: info@complete.ru
www.complete.ru с. 89

КРОК

Тел.: (495) 974-2274

Факс: (495) 974-2277
E-mail: croc@croc.ru
www.croc.ru с. 39

ЛАНИТ

Тел.: (495) 967-6650
Факс: (499) 261-5781
E-mail: lanit@lanit.ru
www.lanit.ru с. 52–53

САПРАН

Тел/факс: (495) 663-7759
E-mail: info@saprun.com
www.saprun.com с. 49

НПЦ СПЕКТР

Тел.: (846) 992-6746

Факс: (846) 992-0749
E-mail: spektr@mail.radiant.ru
www.spc.com.ru с. 13

ALADDIN

Тел.: (495) 223-0001
Факс: (495) 646-0882
E-mail: safe@aladdin.ru
www.aladdin.ru с. 43

ARINTEG

Тел/факс: (495) 221-2141
E-mail: sales@arinteg.ru
www.arinteg.ru с. 15

HP

Тел./факс: (495) 797-3900
www.hp.ru с. 41

IBM

Тел.: (495) 775-8800
www.ibm.com/ru 2-я обл.

IBS

Тел.: (495) 967-8080
Факс: (495) 967-8081
E-mail: ibs@ibs.ru
www.ibs.ru с. 55

MICROSOFT

Тел.: (495) 967-8585
Факс: (495) 967-8500
www.microsoft.com с. 9

RITTAL

Тел.: (495) 775-0230
Факс: (495) 775-0239

E-mail: info@rittal.ru
www.rittal.ru с. 23, 82–83

SONY ELECTRONICS

Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu с. 11

STL-R

Тел/факс: (495) 747-6000
E-mail: info@stl-r.ru
www.stulz.com с. 87

TELECITYGROUP FINLAND OY

Тел: +35 (0) 75 7570 400
E-mail: fi.info@telecit.com
www.telecitgroup.com . с. 68–69

Указатель фирм

«1С» 57	IBS Group 59	Softkey 6	«Газпром космические системы» 21	«ПетерСтар» 28
«1С-Битрикс» 50	IDC 12, 34	Softline 47	«Геолайф» 64	«Примсоцбанк» 12
24iMedia 18	iKS-Consulting 17, 20, 28, 60	Sony 19, 67	«Глобал Один» 6	«ПрограмБанк» 24, 25
500 Startups 14	IND Group 24	Sparxent Distribution 95	«Голден Телеком» 6	«Псковлайн» 28
Acme Packet 11	Infobox 55	SPB TV 20	ГПКС 21, 22	Псковская ГТС 28
Alaris Labs 15	FK InfoWatch 10	Sports Hub 15	«Группа ГАЗ» 13	Пушкинское высшее училище радиоэлектроники ПВО 6
Alcatel-Lucent 10	Intel 10, 15	STL-R 87	«Дружественный Рунет» 70	РБК 59
Allpoint Systems LLC 11	Intelsat 21	StrategyOne 26	«Инвестиции & Инновации & Технологии» 61	РЖД 11, 63
Amazon 35, 36, 63, 65	Intucel 11	StreamLabs 21	«Индайн Групп» 55	ГК «Рольф» 42
ApperCut Security 55	Irdeto 20	STULZ 87	Институт географии РАН 13	Роскосмос 8
Apple 21, 65, 67, 73	ISDEF 6	Target Corporation 86	«Интеллект-Телеком» 62	Роспромбанк 61
Apple Computer IMC 6	IVI.RU 19	Tekmi 14	«Интерспутник» 7, 8, 21, 22	Российский экономический университет им. Г.В. Плеханова 6
Arecont Vision 93	JVC 93	Tele2 5, 10, 28	«ИнфоВотч» 10	«Ростелеком» 4, 5, 10, 11, 13, 17, 28, 35, 37, 58
ASHRAE 86, 87, 89	LEICA 95	Telesonera 5	Инфокоммуникационный союз 62, 64	«РyСат» 12, 22
AT Consulting 57	Lenel 93	Texas Memory Systems 80	СП «Инфосервис» 11	Сбербанк 35
Audi 61	LinkedIn 67	TM Forum 65	«Инфосистемы Джет» 15, 56	«Синтерра» 28
Autodesk 11	LSI 77	TNS 14	«Истар» 12	АФК «Система» 59
AXIS 93	M2M Global Alliance 63	Trend Micro 15	«КаР-Тел» 10	«Ситроникс» 10
Backbase 24	Mail.Ru Group 59	T-Systems 15, 46	«Компания Март» 28	«Скай Линк» 28
Bosch 93	MassChallenge 14	United Technologies Corporation 93	КОМПЛИТ 89	«СКБ Контур» 38, 54
BP 15	FK MAYKOR 11	UnitedHealth Group 86	НТЦ «Комсет» 61	«Софткей» 44
British American Tobacco 15	MegaLabs 19, 38	Uptime Institute 11, 68, 84, 85, 86	«КОМСТАР-Регионы» 59	«СтарБлайзер» 12
BSC 24	Microsoft 21, 26, 35, 36, 38, 39, 47, 48, 54, 57, 74, 76, 83, 94	Uptime Institute Russia 11	ГК «КОРУС Консалтинг» 40, 56	«СТС Медиа» 10
BSS 14	Motorola Mobility 21	Verimatrix 20	КР-1 59	«Сумма Телеком» 14
CDNvideo 57	NetApp 77, 79	VimpelCom Ltd. 5, 59	КРОК 36	«СЦС Совинтел» 6
CERT-GIB 70	Netris 13	Vodafone 60, 63	«Лаборатория Касперского» 12	«Тайле» 94
Check Point Software Technologies 54	Newtec 12	WebPlus ISP CERT 70	ЛАНИТ 52	«ТБинформ» 38
Cisco 11, 56, 93	Ngenix 21	WIND Mobile 59	Лига безопасного Интернета 27, 70	«Телеинтерком» 6
Citrix 94	Nice Systems 92	Yandex N.V. 59	«Локтелеком» 58	«ТелеРосс» 6
Cloud Computing Association 36, 48	NIST 36	YouTube 27	«Лукойл» 15	«Телесети Плюс» 28
Comcast 67	Nokia Siemens Networks 10	ГК «Ай-Текс» 39, 57	«Лукойл-Интер-Кард» 15	«Телефонная связь Москвы» 6
Data+ 13	Oracle 11, 36, 77, 80	«Акадо — Екатеринбург» 15	«М2М телематика» 14	Технический центр телевидения и радиовещания Республики Саха (Якутия) 13
DataLine 56	Orange 5, 60	ГК «Акадо» 17, 18	«Манго Телеком» 47	«Техносерв Консалтинг» 67
Dell 77, 78	Orange BC 6	«Акцент» 12	МГТУ СТАНКИН 6	«Техносерв» 10, 57
Deutsche Telekom 5, 15	Orascom Telecom Holding S.A.E. 59	«Аладдин Р.Д.» 14, 43	МГУ 6	«Тинькофф кредитные системы» 24
Digital Design 57	Panasonic 12, 95	«Амфител Плюс» 11	МЕГА 71, 72	«Триколор ТВ» 14, 17, 18, 22
DigitalOctober 14	Parallels 34, 45	«Андек» 46	«МегаФон» 5, 13, 19, 20, 28, 35, 59	ТТК 11, 14, 17
EADS Astrium 21	Pelco 91, 93	«Анкей» 6	Международная академия информатизации 64	«Уздунробита» 58
Eaton 13	Presbyterian 15	АП КИТ 5	Международный институт управленческого развития IMD 6	Университет прикладных наук Сатакунта 6
EMC 37, 76, 78, 80	Qtech 73	«АРМО-Системы» 91	Международный М2М-альянс 14	УК «Финанс Менеджмент» 58
Ericsson 19	Radware 94	Ассоциация кабельного ТВ России 17	«Мобиль» 6	ГК «Финансовые информационные системы» 25
Esri CIS 13	Rambler 6	Ассоциация региональных операторов связи 4	Мосгорэнерго 62	Центр инновационного развития 14
Eutelsat 14, 21	RIT Technologies 14	Банк России 6, 48	МСЭ-Т 70, 72	«Центр прикладных исследований компьютерных сетей» 15
Facebook 24, 41, 59, 67	Rittal 82, 83	«Вайнах Телеком» 14	МТС 5, 6, 13, 17, 20, 35, 40, 58, 59, 63	«Центр реагирования на компьютерные инциденты» 70
Forbes 6	RU-CERT 70	«Вертолеты России» 13	НС Банк 14	«ЭР-Телеком» 17
Forrester 34	Russian Cloud Computing Professional Association 36	ВИМКОМ 21	«НТВ-Плюс» 18, 22	«Эшелон» 62
Fujitsu 86, 79	Safetech 14	«Воентелеком» 10	«Онланта» 52	«Яндекс» 15, 59
Fujitsu Technology Solutions 15	SAP 6, 10, 24, 38	«Возрождение» 6	«Основана Телеком» 5	
Gartner 34	SAS Institute 6	«Вокзал-Инфоком» 63	«Петер-Сервис» 59	
Georg Fischer 15	Schneider Electric 11, 91	ФГУП НИИ «Восход» 10		
Globalive 59	SEAT 15	ВТБ 39		
Google 19, 24, 39, 47	SES 21	«ВымпелКом» 4, 10, 13, 17, 19, 35, 54, 58, 59, 61, 62, 64		
GPS Club Россия 61	Shell 15			
Group-IB 26, 70	Sistema Shyam 15			
HandyBank 25	TeleServices Limited 59			
Hitachi Data Systems 77, 78, 80				
HP 36, 38, 41, 42, 48, 78				
IBM 36, 38, 48, 76, 80				

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство

«ИнформКурьер-Связь»:

127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 204; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:

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

МНТОРЭС им. А.С. Попова:

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