Начало делового сезона: настроение позитивное

В сентябре, с наступлением нового делового сезона, российские фондовые индексы, несмотря на повышенную волатильность, демонстрировали довольно уверенный рост. Росли и акции телеком-компаний.

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

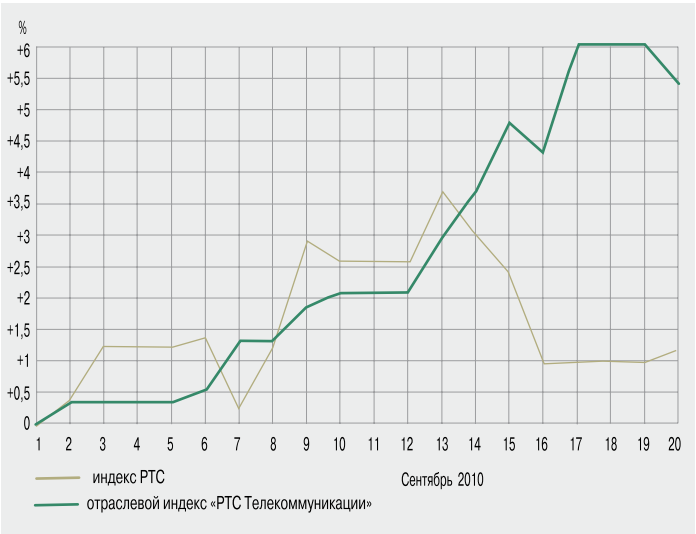
Так, в период с 1 по 20 сентября индекс ММВБ прибавил 4,23%, до отметки 1426,84 пункта, а индекс РТС – 3,17%, до 1467,11 пункта. Отраслевые индексы выросли еще больше – капитализация индексов «ММВБ Телекоммуникации» и «РТС Телекоммуникации» увеличилась на 4,98% (2236,54 пункта) и 5,55% (222,77 пункта) соответственно.

Ключевым событием месяца стал уход генерального директора госхолдинга «Связьинвест» Евгения Юрченко. Потеря – в самый разгар преобразований – сильного лидера, который возглавил команду «Связьинвеста» непосредственно перед началом реорганизации активов компании и чьей основной задачей являлось проведение этой реорганизации, может помешать ее нормальному ходу. Активная же борьба претендентов за вакантное место способна поставить под вопрос успех всей реформы, поскольку несет в себе потенциальные угрозы не только для «Связьинвеста», но и для «Ростелекома», на базе которого идет интеграция активов госхолдинга. Тем не менее за рассматриваемый период капитализация «Ростелекома» увеличилась на 9,53% до отметки 136,25 руб.

Акции «Сибирьтелекома» подорожали на 5,35%, достигнув в цене 1,91 руб. Компания объявила аукцион на привлечение двух кредитных линий по 1 млрд руб. Две пятилетние невозобновляемые кредитные линии планируется привлечь по ставке не более 8,7 и 8,5% годовых. Учитывая масштабы бизнеса оператора и его финансовые показатели, с высокой долей вероятности можно предположить, что эти кредиты по обозначенной ставке он получит.

Бумаги «ЦентрТелекома» выросли на 8,72%, достигнув уровня 26,31 руб. за акцию. Поддержку акциям оказала публикация позитивной отчетности по МСФО за I полугодие 2010 г., согласно которой чистая прибыль компании по сравнению с аналогичным периодом 2009 г. (2927 млн руб.) выросла на 42% и составила 4155 млн руб. Выручка от реализации увеличилась по сравнению с аналогичным периодом прошлого года (18 212 млн руб.), составив 19 976 млн руб. Также стало известно, что совет директоров «ЦентрТелекома» принял решение отложить рассмотрение вопроса об участии общества в Akado International Limited. Такое решение было принято в связи с поступлением информации о том, что компания Renova Media Enterprises готова обсудить альтернативную структуру сделки.

Динамика индексов и инструментов РТС



За рассматриваемый период бумаги «Дальсвязи» подорожали на 11,56%, до отметки 110,15 руб. Компания сообщила о сокращении чистого долга за I полугодие 2010 г. по МСФО на 7,3% – до 5,504 млрд руб. Чистая прибыль в I полугодии по МСФО выросла на 0,6% по сравнению с аналогичным показателем I полугодия 2009 г. и составила 1,444 млрд руб. Выручка оператора в отчетном периоде увеличилась на 5,2% по сравнению с аналогичным показателем I полугодия прошлого года, достигнув 8,987 млрд руб. Рост выручки компания объясняет увеличением доходов от услуг передачи данных и телематических услуг (Интернет); выросли (на 176 млн руб.) и доходы от местной телефонной связи в результате повышения тарифов с 1 марта 2009 г. – на 8,7% у ОАО «Дальсвязь» и на 6,3% у ОАО «Сахателеком».

Котировки акций «Северо-Западного Телекома» прибавили 8,72%, до уровня 25 руб. Оператор подвел итоги финансово-хозяйственной деятельности за I полугодие 2010 г. в соответствии с МСФО. Чистая прибыль компании за тот же период в соответствии с МСФО составила 2474 млн руб., увеличившись более чем вдвое по сравнению с I полугодием прошлого года. При этом маржа по чистой прибыли заметно выросла по сравнению с предыдущим периодом и составила 17,6%.

Наибольшим спросом пользовались бумаги «Уралсвязьинформа», прибавившие 11,94%, до 1,209 руб. Компания представила консолидированные неаудированные финансовые результаты за январь–июнь 2010 г. в соответствии с МСФО. Так, выручка от реализации в I полугодии 2010 г. увеличилась на 6%, достигнув 21 308 млн руб. Операционные расходы снизились на 2,9%, до 16 411 млн рублей. Показатель EBITDA составил 9732 млн руб.; прибыль от операционной деятельности – 5 561 млн руб. По итогам I полугодия выручка от нерегулируемых услуг превысила половину общего объема выручки «Уралсвязьинформа» и составила 53,4% (47,0% в I полугодии 2009 г.).

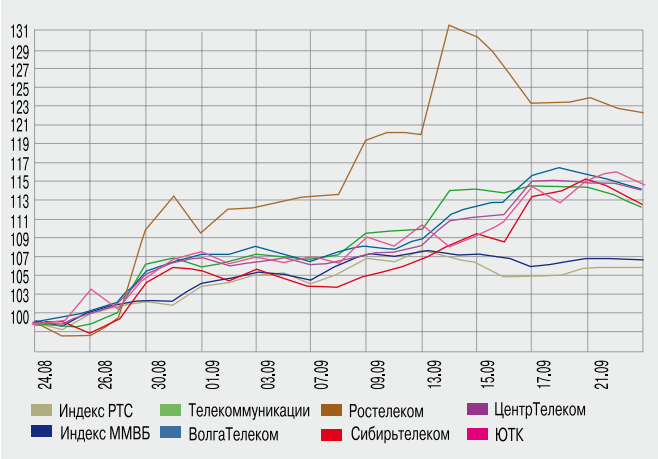
Капитализация «ВолгаТелекома» выросла на 10,23% до отметки 115,3 руб. за акцию. Чистая прибыль ОАО «ВолгаТелеком» по МСФО в I полугодии 2010 г. увеличилась на 52,6% и составила 2,816 млрд рублей, говорится в отчете компании. Выручка от реализации группы за 6 месяцев этого года увеличилась по сравнению с аналогичным периодом прошлого года на 6,1%, составив 17 095 млн руб. Прибыль от операционной деятельности за отчетный период выросла на 20,2% и достигла 4120 млн руб. Компания также исполнила в полном объеме свои обязательства по выкупу у миноритариев акций на общую сумму 2,46 млрд руб., говорится в материалах «ВолгаТелекома»: выкуплено 3 450 386 штук обыкновенных акций на сумму 333,790 млн руб. 64 коп. и 21 978 733 штук привилегированных именных бездокументарных акций типа «А» на сумму 2,126 млрд руб. 42 коп. Выкуп акций происходил в соответствии с отчетом об итогах предъявления акционерами требований о выкупе принадлежащих им акций, утвержденным решением совета директоров ОАО «ВолгаТелеком» 10 августа 2010 г.

Активная борьба претендентов за вакантное место гендиректора «Связьинвеста» способна поставить под вопрос успех всей реформы холдинга

Сотовые операторы продемонстрировали более скромный рост. Котировки МТС прибавили 1,65% до отметки 254,99 руб. Агентство Fitch Ratings подтвердило долгосрочный рейтинг дефолта эмитента МТС в иностранной валюте на уровне «BB+» со «Стабильным» прогнозом. Кроме того, Fitch подтвердило краткосрочный РДЭ МТС в иностранной валюте на уровне «B» и приоритетный необеспеченный рейтинг в иностранной валюте на уровне «BB+», а также национальный долгосрочный рейтинг на уровне «AA(rus)» со «Стабильным» прогнозом.

Бумаги АФК «Система» выросли на 1,52% – до уровня 26,55 руб. за акцию. Чистая прибыль по US GAAP по итогам II квартала 2010 г. составила $144 млн, что на 41,5% меньше показателя аналогичного периода прошлого года, говорится в отчете компании. Консолидированная выручка увеличилась на 11,5% по сравнению с I кварталом 2010 г. и составила $6,9 млрд. Показатель OIBDA достиг $1,9 млрд, на 14,3% по сравнению с первым кварталом 2010 г., маржа OIBDA – 27,0%. Операционная прибыль выросла на 21,9% по сравнению с I кварталом 2010 г. – до $1,1 млрд, операционная маржа составила 16,4%. ИКС

Динамика индексов РТС и телекоммуникационных компаний в период с 24 августа по 21 сентября 2010 г.



Как ускорить развитие российских телекоммуникаций в русле мировых тенденций

Сколько уже копий сломано о вечную тему соответствия регулирования отечественной телекоммуникационной отрасли современным тенденциям развития рынка и техники... Многие, и не без оснований, говорят о том, что модель регулирования следует изменить. Однако самое сложное – это определить направления и последовательность таких изменений.

Алексей РОКОТЯН,
первый заместитель гендиректора компании «Норильск-Телеком», канд. техн. наук

Автор данной статьи тоже посвятил ряд публикаций этой теме – и в журнале «ИКС», и на портале IKSMEDIA (см. онлайн-трактаты «От «телекома» к «инфокому»» и «Как нам реорганизовать... телефонию»). В этом материале сделана попытка обобщить и консолидировать ранее высказанные предложения о подходах к построению перспективной регуляторной модели.

В последние годы у многих людей, связанных с телекоммуникационной отраслью, все чаще возникают вопросы, ответ на которые в рамках сегодняшнего отраслевого регулирования как минимум неочевиден. Например, такие:

- Зачем пользователю современных инфокоммуникационных услуг иметь несколько договоров на оказание услуг связи? Как операторам на практике пакетировать услуги?
- С точки зрения пользователя услуги мобильной и фиксированной телефонии во многом сходны и взаимозаменяемы. Почему регулирование подотраслей фиксированной и мобильной связи столь различно?
- Как реально обеспечить приток инвестиций в развитие инфраструктуры связи в «невыгодных» районах?
- Как сделать взаиморасчеты операторов прозрачными и недискриминационными? Как перестать подталкивать их к объективно бесполезным проектам, рассчитанным не на расширение возможностей для пользователей, а на использование перекосов системы взаиморасчетов?
- Чем отвечать на вызов Skype и других служб IP-телефонии? Как в перспективе будет выглядеть рынок голосовых услуг?
- Каков реальный эффект либерализации рынка дальней связи? Стоит ли рассматривать этот рынок как перспективный?
- В чем смысл лицензирования в связи?
- Как телеком-операторы взаимодействуют с потребителями своих услуг в инфокоме? Что это за услуги? За что платит клиент оператору в инфокоме?
- Рано или поздно ответ на эти вопросы нужно будет найти. Чем раньше удастся это сделать и внедрить новые принципы в практику, тем ниже будут отраслевые издержки и выше конкурентоспособность российского телекома.

Добавляет проблем и операторам, и абонентам ряд решений последних лет, касающихся регулирования телефонии и голосовых услуг вообще. Общепризнанны технические проблемы, обусловленные неудачным способом выбора оператора дальней связи, невозможностью рационально строить голосовые сети на базе пакетных технологий. В этом же ряду находятся неоправданно усложненные взаимоотношения с пользователями, в том числе:

- многочисленные договоры на оказание услуг телефонии, дорогое их администрирование;
- трудности взыскания дебиторской задолженности в ситуации, когда услуги местной и междугородной связи оказывают разные операторы;
- уже упоминавшиеся проблемы с пакетированием услуг.

Следует также иметь в виду, что операторы местной связи имеют возможность воздействовать на выбор абонентом оператора дальней связи и на практике влияют на развитие рынка дальней телефонии, причем далеко не всегда в интересах абонентов и самого рынка.

Много противоречий между участниками рынка создают перекосы цен на услуги по пропуску трафика, практически сохраняющие перекрестное субсидирование, а также существенная неодинаковость требований, предъявляемых к разным операторам (и к тому же не слишком явно зафиксированных в НПА) по таким аспектам, как живучесть сетей, содержание мобилизационных резервов, социальная нагрузка.

В результате у нас, в частности, нет серьезного потенциала снижения цен на дальнюю связь, что фактически играет на руку службам типа Skype, которые, по сути, находятся вне правового поля, но пользуются все большей популярностью.

Отдельный блок проблем связан с неэффективным использованием фонда универсальных услуг.

Ну и наконец отметим, что реализованная в России в 2005–2006 гг. «горизонтальная» модель рынка голосовых услуг совершенно не вписывается в объективную тенденцию к вертикальной интеграции.

Теперь от констатации общеизвестных проблем пора перейти к конструктиву и предложить ряд мер, реализация которых, по мнению автора, позволит ускорить развитие российского телекоммуникационного рынка в русле общемировых тенденций.

Регулирование телефонии и голосовых услуг

Итак, в телефонии представляется целесообразным:

1. В качестве первой и срочной меры устранить формальные препятствия к эффективному внедрению оборудования NGN/IMS на сетях связи, называемых сейчас телефонными. Это прежде всего коррекция «Требований к построению телефонной сети связи общего пользования». Проект такого документа по поручению Минкомсвязи России уже разработан функционирующей на базе АДЭ рабочей группой РГ-1 при активном участии автора.

2. Осуществить переход от иерархического построения традиционных телефонных сетей к неиерархическим сетям нового поколения, прежде всего на уровне сетей одного субъекта РФ (т.е. решить так называемую проблему зоновых сетей).

3. Трансформировать модель рынка телефонных услуг, завершив балансировку тарифов и отказавшись от попыток решать экономические проблемы методами технологического регулирования.

В более широком смысле задача состоит в переходе от модели регулирования, удобной отдельным операторам (что самое обидное, удобной только на конкретной, уже миновавшей стадии развития рынка), к модели, ориентированной на удобство клиента. Следующим шагом нужно разобраться с ролью, которую играет в инфокоммуникациях бизнес, основанный на телекоммуникационной инфраструктуре, и закрепить эту роль в нормативной базе.

Здесь нужно отметить, что уже в ближайшей перспективе голосовые службы перестанут быть «лицом» телекоммуникаций, это лишь одна из составляющих пакетного предложения услуг («...voice is just another application...»). Фиксированная и мобильная телефония должны рассматриваться и регулироваться одинаково, как частные случаи услуг мультисервисной сети связи. Основным источником доходов инфраструктурных операторов, располагающих развитыми сетями электросвязи, становятся локальные сервисы, в том числе голосовые. Основными «базовыми» услугами, предоставляемыми сетями связи, будут являться подключение терминалов клиентов к сети и сеансы связи в широком смысле. Телефонный сеанс (соединение) – это частный, хотя и важный случай.

Добавим, что бизнес, связанный с Интернетом, уже достаточно давно живет по подобной модели, начала постепенно приближаться к ней и мобильная телефония. И только отечественная фиксированная телефонная связь пытается отрицать очевидное и собирать заметную долю доходов с дальней телефонии и межоператорских услуг, представляя собой жесткую конструкцию, постепенно покрывающуюся трещинами и разрушающуюся под ударами рыночной стихии...

Что касается услуг междугородной и международной телефонии, то в перспективе просматриваются два типа сервисов дальней голосовой связи: условно бесплатный без гарантий качества (Skype и аналоги) и с гарантиями качества при ограниченной оплате (традиционное соединение).

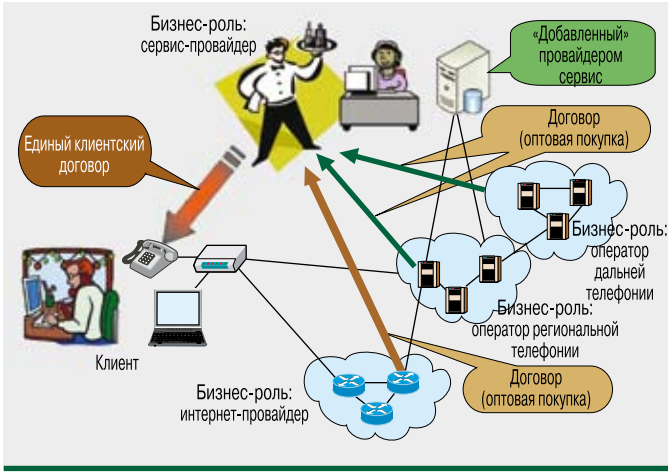
Автор убежден, что сегодняшний рынок дальнего голосового трафика долгосрочной перспективы не имеет, а его искусственная поддержка вредна для отрасли. Превращение дочерних компаний «Связьинвеста» в единую операционную компанию, слияние сотовиков из «большой тройки» с крупными операторами фиксированной связи практически не оставляет шанса на сколько-нибудь существенную долю рынка многочисленным владельцам сетей междугородной и международной связи, вышедшим на рынок после 2006 г. Да и сам этот рынок, скорее всего, скоро съежится в разы под воздействием крупных вертикально интегрированных компаний, контролирующих всю цепочку взаиморасчетов и имеющих возможность делать гибкое тарифное предложение пользователям на весь комплекс голосовых услуг.

Отделим сеть от сервисов

Результатом действия сегодняшних тенденций должно стать изменение модели рынка. Бизнес, непосредственно базирующийся на сетевой инфраструктуре, станет оптовым бизнесом по транспорту информации, организации стандартных сеансов связи, фактически «трубой битов». А взаимодействие с пользователями будет осуществляться в рамках бизнес-роли сервис-провайдера (см. рисунок).

По мнению автора, ключевой принцип инфокоммуникационного рынка заключается в том, что сеть и сервис – это разные бизнесы, они строятся

Модель рынка инфокоммуникационных услуг



и, соответственно, регулируются совершенно поразному. Сервис – это один из пользователей услуг сети связи и в то же время способ розничной продажи услуг, в том числе и услуг, предоставляемых сетевой инфраструктурой. При этом модель регулирования должна быть ориентирована на возможность и удобство продажи пользователям в первую очередь пакетного предложения сетевых и информационных услуг.

Важнейшим принципом для инфокоммуникаций должна стать сетевая нейтральность: любой сервис технически доступен абоненту любой подходящей по параметрам сети связи. В то же время сети связи должны стать универсальными и мультисервисными, время «моносервисных» сетей, ориентированных на один доминирующий тип передаваемой информации, давно ушло (на рисунке такие сети показаны в качестве предельного случая).

Исходя из чисто транспортной роли сетевого оператора, стоит закрепить в нормативной правовой базе положение о том, что ответственность за содержание информации, передаваемой по сети связи, включая соблюдение авторских прав, несет ее источник: сервис-провайдер или сам абонент. Дело инфраструктурного оператора – подключать терминалы и организовывать сеансы связи. Все технические ограничения на доступность тех или иных сервисов должны вводиться только в рамках установленных законом процедур.

При этом конкретная компания, безусловно, вправе сочетать бизнес-модели сетевого оператора, сервис-провайдера, контент-провайдера – разумеется, при выполнении требований, предъявляемых к каждому из этих бизнесов. Именно на этих путях операторам следует искать ответ на падение маржинальности телекоммуникационного бизнеса. Оптовый инфраструктурный бизнес объективно не может быть высокоприбыльным, но у него и риски не столь велики. Вместо набивших оскомину причитаний о том, что превращение в «трубу битов» неприемлемо, связистам нужно понять, что остановить внедрение в отрасли глобального разделения труда невозможно. А разделение бизнес-ролей инфраструктурного и сервисного операторов и есть для телекоммуникаций глобальное разделение труда, давно ставшее привычным во многих других отраслях. Линию развития конкретной компании стоит выстраивать на основании известных в стратегическом маркетинге механизмов вертикальной интеграции, позволяющих скомбинировать высокомаржинальные и высокорисковые бизнес-роли розничных продаж с гораздо более устойчивым, но и менее прибыльным инфраструктурным бизнесом.

Городу универсальная услуга не нужна

Настала пора изменить способ использования фонда универсальной услуги (ФУУ). ФУУ должен поддерживать реально востребованные услуги, а не искусственную конструкцию, полезность которой несопоставима с затратами на ее содержание. При этом оказание услуг, субсидируемых ФУУ, должно быть выгодно инфраструктурному оператору. ФУУ целесообразно ориентировать прежде всего на обеспечение поддержки сервиса в труднодоступных и малонаселенных районах, а применение в этих целях перекосов в тарифах или технических ограничений нужно прекратить как можно скорее.

Предлагается направить ФУУ на прямое субсидирование оказания по доступным тарифам услуг, имеющих социальное значение, в труднодоступных и малонаселенных районах, где объективно высоки затраты на инфраструктуру, а конкуренция невысока. В крупных же городах и коттеджных поселках универсальная услуга не нужна.

Механизм работы ФУУ видится следующим:

- ФУУ покрывает разницу между средней себестоимостью услуги с учетом небольшой прибыли и ценой, доступной для пользователя и одинаковой на территории региона;
- основанием для получения субсидий являются выставленные и оплаченные абонентами счета за услуги;
- любой инфраструктурный оператор, оказывающий услуги доступа к сети, на обслуживаемой территории не вправе отказать абоненту в подключении к сети и предоставлении услуг, поддерживаемых ФУУ.

В число услуг, поддерживаемых ФУУ, может входить подключение к сети фиксированной связи для обеспечения телефонии и доступа в Интернет с небольшой скоростью. В этом случае к универсальным услугам будут относиться предоставление доступа к сети, местные телефонные соединения (для труднодоступных районов – и междугородные), а также социальный доступ в Интернет. Поскольку обязательство оказания универсальных услуг ложится на всех инфраструктурных операторов, имеющих локальные сети, то тем самым обеспечивается равенство социальных обязательств для всех участников рынка.

Установление государством тарифов на фиксированную телефонию – атавизм

Важнейший элемент перспективной модели регулирования – это отказ от прямого установления цен на услуги фиксированной телефонии для конечных пользователей. Конкуренция с сотовыми сетями и механизм универсальных услуг удержат операторов местной телефонии от неоправданного завышения цен, а для удаленных районов предлагается установить максимальную допустимую разницу в ценах для различных направлений при оказании услуг междугородной связи. Это позволит исключить установление демпинговых цен для «выгодных» направлений и заградительных для «невыгодных».

Нужно сближать подходы по регулированию цен для всех межоператорских услуг по передаче голоса с гарантированным качеством, и фиксированных, и мобильных:

- предельные цены на межоператорские голосовые услуги должны регулироваться для операторов сетей всех типов;
- оператор сотовой сети должен иметь единую предельную цену завершения вызова на свою сеть в пределах региона;
- для фиксированных сетей на переходный период может сохраняться возможность иметь две предельные цены завершения вызова в пределах региона – «внутригородскую» и «внутрирегиональную», а от понятия «уровень присоединения» стоит постепенно отказываться;
- для межрегиональных вызовов также возможны два уровня предельных цен: между густонаселенными регионами и в удаленные и трудно доступные регионы.

При этом принципиальным является отказ от технологических и коммерческих ограничений на маршруты пропуска голосового трафика для всех типов сетей.

За единую лицензию на услуги связи

Исходя из вышеизложенного, можно совершенно по-новому определить роль и цель лицензирования оказания услуг связи. Цель этого института – фиксация равных условий деятельности для всех инфраструктурных операторов. В эпоху мультисервисных сетей лицензия на услуги связи должна быть единой и давать оператору возможность предоставлять все типы сетевых подключений и сеансов связи.

Предметом лицензирования должно являться оказание услуг, непосредственно опирающихся на использование сетевой инфраструктуры («базовых» услуг), т.е. предоставление доступа к сети связи и организация сеансов связи (любых).

В лицензии должны фиксироваться существенные условия, сопровождающие деятельность по оказанию «базовых» услуг связи, а именно:

Обязательства:

- ✓ оказание универсальных услуг;
- ✓ реализация функции СОРМ;
- ✓ локализация расположения терминала;
- ✓ выполнение требований по совместимости (целостности);
- ✓ выполнение требований по безопасности;
- ✓ выполнение требований по устойчивости;
- ✓ выполнение требования сетевой нейтральности;
- ✓ обеспечение недискриминационных условий присоединения и пропуска трафика для других операторов связи.

Права:

- ✓ пользование конкретными полосами радиочастотного спектра;
- ✓ получение возмещения из ФУУ за реально оказанные услуги, отнесенные к универсальным;
- ✓ взаимодействие с другими сетевыми операторами на недискриминационных условиях;
- ✓ доступ к хозяйственной и сетевой инфраструктуре на недискриминационных условиях.

Назрело

Кардинальное изменение подходов к регулированию рынка телекоммуникаций:

Переход к лицензированию только одного вида деятельности – оказания «базовых» услуг связи с целью фиксации обязательств и прав инфраструктурных операторов.

Отказ от «горизонтальной» модели рынка голосовых услуг, переход к вертикальной структуре:

- ❍ сетевой оператор как владелец сетевой инфраструктуры (локальный/региональный или межрегиональный);
- ❍ сервис-провайдер, предлагающий весь комплекс голосовых и иных услуг связи в рамках пакета инфо- и телекоммуникационных сервисов.

Отказ от прямого регулирования клиентских тарифов на услуги электросвязи.

Регулирование предельных цен на межоператорские услуги для всех типов компаний.

Перенос основной доли доходов, получаемых при оказании услуг связи, на локальные сервисы. При этом бизнес-модель магистрального оператора основана на максимизации пропускаемого трафика и получении доходов по взаиморасчетам от локальных операторов. Она предполагает большие объемы при низкой марже.

Переход к использованию фонда универсальной услуги для прямого субсидирования фактически оказанных услуг в труднодоступных и малонаселенных районах.

Объективная роль сетей связи в инфокоммуникациях – **инфраструктура для инфокоммуникационных сервисов,** «труба битов». В этом нет ничего страшного, если правильно выстроены подходы к регулированию.

Операторские и провайдерские компании могут эффективно **сочетать различные бизнес-роли,** обеспечивая развитие всех бизнесов, которыми занимаются инфраструктурный оператор, сервис-провайдер и поставщик контента. ИКС

Практический семинар

«Выбор, создание, обслуживание ЦОД. Подходы, модели, стоимость»

Уникальное событие! Впервые в России!

Автор семинара:
Джерри Галлахер – исполнительный директор, президент Total Site Solutions (TSS), a Fortress International Group и выдающийся специалист, обладающий более чем 30-летним опытом в области создания, эксплуатации и модернизации ЦОД и иных критически важных объектов. Г-н Галлахер входит в круг общепризнанных мировых экспертов и традиционно является участником крупнейших мероприятий, проводимых AFCOM, Uptime Institute и другими организациями.

Пять причин, почему важно участвовать:

- рассмотрение реальных инструментов снижения затрат на ЦОД
- анализ моделей создания дата-центров
- формирование бюджета на строительство и эксплуатацию ЦОД
- набор практических рекомендаций с конкретными стоимостными оценками для эксплуатирующих организаций
- возможность получить ответы на вопросы, касающиеся стратегии развития Ваших проектов в области ЦОД

Семинар рассчитан на профессиональную аудиторию, эксплуатирующую и строящую дата-центры в России и странах СНГ.

ПРОГРАММА СЕМИНАРА

9:00-10:00	**Начало регистрации и утренний кофе**
10:00-11:00	Выбор площадки под создание ЦОД. Важные критерии отбора. Как оценить и правильно расставить приоритеты?
11:00-11:15	Вопросы слушателей
11:15-12:15	Пять основных моделей создания ЦОД. Характеристики, стоимость и особенности для заказчика
12:15-12:35	**Кофе-брейк**
12:35-13:35	Операционная деятельность ЦОД с точки зрения управления и эксплуатации инженерной и другой инфраструктуры. Стоимость операционной деятельности инфраструктуры ЦОД. Эксплуатационный ежегодный бюджет ЦОД
13:35-14:00	Вопросы слушателей, обсуждение
14:00-15:00	**Обед**

Для регистрации на семинар необходимо обратиться в редакцию журнала «ИКС» по тел.: +7 (495) 229-4978, 785-1490 или отправить заявку по адресу: expo@iksmedia.ru
Менеджер мероприятия: Анна Скрипник

Стоимость участия в семинаре одного слушателя составляет 21240 руб. с НДС.

издается с 1992 года ИКС www.iksmedia.ru

Дата проведения семинара: 3 ноября 2010 г., начало регистрации в 9-00.
Место проведения: гостиница «ХОЛИДЕЙ ИНН ЛЕСНАЯ», Москва, ул. Лесная, д. 15.

data centers design & consulting [dc]² www.dcxdc.ru | www.dcxdc.com

Защищенность IP-телефонии в историческом и практическом контексте

IP-телефония медленно, но верно идет к тому, чтобы полностью заместить традиционные архитектуры телефонии (кроме сотовой). Вопрос о ее защищенности в сравнении с системами традиционной телефонии хотя и остывает, но периодически еще вызывает ожесточенные споры.

Сергей РЯБКО,
президент группы компаний «С-Терра», канд. физ.-мат. наук

Споры эти редко политически нейтральны, аргументы их часто нецелостны и в устах разных авторов приобретают различный смысл. Да и сравнивают, надо сказать, соленое с зеленым. Поэтому прежде всего давайте определимся с предметом оценки, ведь за время своего существования техника телефонии (и, следовательно, ее безопасность) изменилась радикально.

О безопасности телефонии

Безопасность систем телефонии (рис. 1) определяют:

- свойства центрального коммутационного узла (АТС);
- методы настройки его емкости, номерного плана и услуг (условно назовем эту сферу администрированием);
- свойства терминалов и способы взаимодействия с ними.

Обобщая, задачи АТС можно описать как управление вызовами, коммутацию соединений абонентов и транковую связь с другими АТС по магистральной линии.

Герой, он же «уходящая натура»: фрикер

Взлом телефонии – почтенное занятие в техноандеграунде. Примечательно, что два старейших американских хакерских издания подчеркивают свое родство с телефонным жульничеством: журнал «2600» (www.2600.net) назван в честь частоты тонального сигнала АТС 2600 Гц, а название пережившего было клиническую смерть, но возродившегося журнала Phrack (www.phrack.org) происходит от слова phreaking – взлом телефонии.

Благородный хакер старого закала декларировал свои цели как некий информационный анархокоммунизм. Фрикер был более приземленным жуликом. Но, в отличие от хакера, программиста, фрикер должен был понимать автоматику, физику сигналов и уметь спаять примитивный (или не очень) инструментарий.

Целью большинства фрикерских трюков было обычное воровство телефонного ресурса: звонок с таксофона забесплатно, за чужой счет и т.п.

Механизм «обмана» АТС (преимущественно стандартов 1950–1980-х гг.) основывался на системе сигнализации между терминалом и АТС. Инструментами служили так называемые боксы – простейший «черный», более развитые «красный» и «синий». Боксы имели стандартные схемы, выдавали импульсные и тоновые сигналы с целью заставить АТС в нужный момент «подумать», что разговор оплачен, или, менее благородно, но проще – переписать биллинг на другой номер.

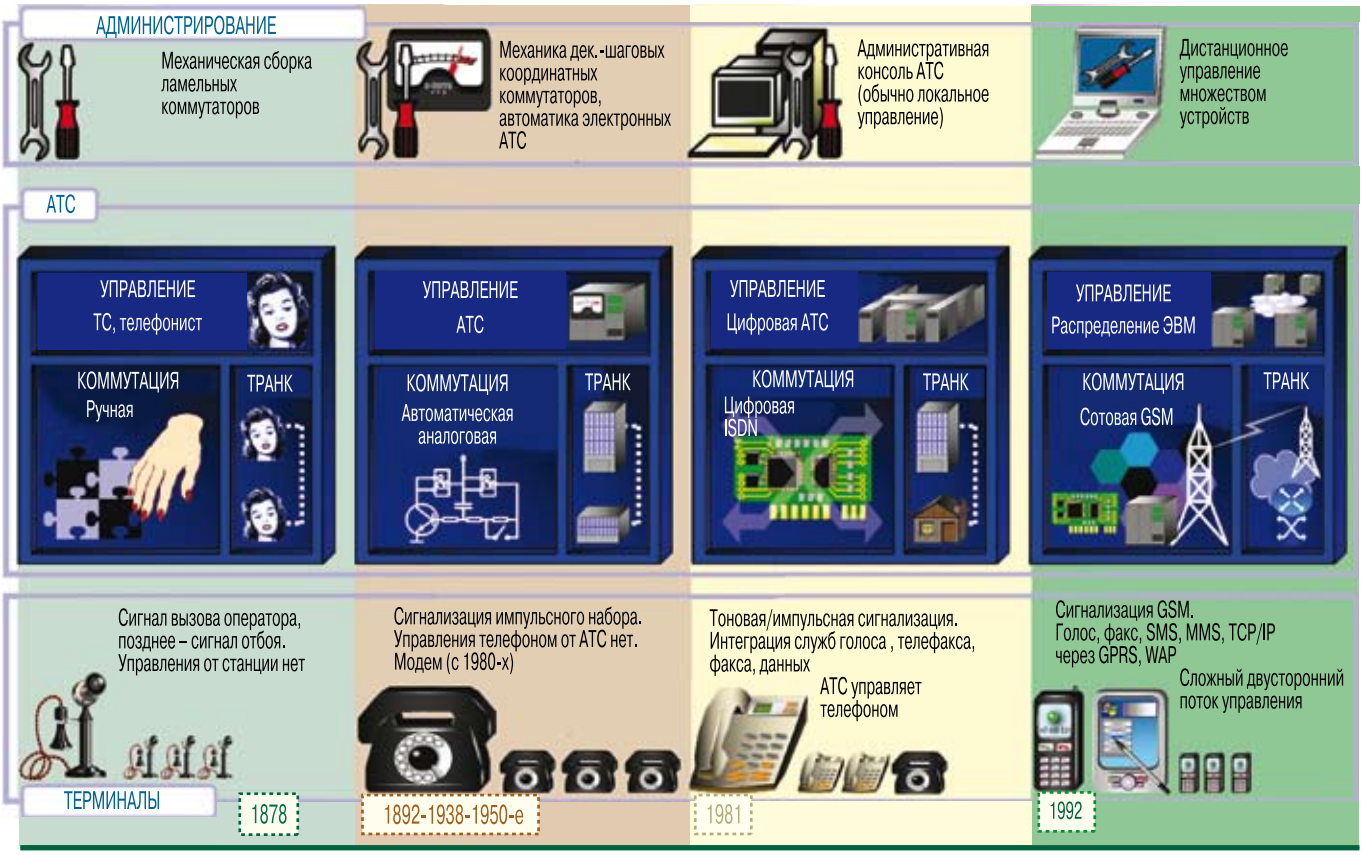
С приходом цифровой телефонии методы фрикинга начали меняться. В сотовой телефонии заработала криптографическая защита. Бокс без SIM-карты стал бесполезен, фрикер с боксом ушел в историю. На смену ему пришел «черный» оператор, втихую зарабатывающий вполне промышленного масштаба деньги на переговорах обитателей черкизоновских андеграундов с родственниками и партнерами во Вьетнаме, Таджикистане или Молдове. Но этот персонаж – уже не предмет технологического исследования, а фигурант дела Управления «К». Расстанемся с ним, пожелав успехов нашим милиционерам.

Забавы «больших братьев» и маленьких негодяев: прослушка

Перехват переговоров следует разделить на два класса: операторский и, условно, частный.

Операторская прослушка существовала еще в первых станциях с ручной

Рис. 1. Эволюция систем телефонии



коммутацией. В них сигнализация терминала, за исключением вызова телефонистки, отсутствовала. Поэтому, чтобы отследить отбой, телефонистка должна была постоянно или периодически прослушивать все линии. Можно предположить, что это услаждение природного женского любопытства смягчало тяготы однообразного труда и строгий отбор при приеме на работу (по тогдашним объявлениям о найме, от телефонистки требовались: красивый голос, разборчивая речь и размах рук не менее 154 см).

В современной телефонии операторская прослушка приобрела организованный характер оперативно-розыскного мероприятия. В сотовых сетях, где применяется стойкое шифрование трафика абонентов, существует антитеррористический режим, при котором абонентское шифрование в целях отлова террористов регламентно снимается.

Ну, это в интересах служб, призванных обеспечить нашу безопасность. А вот может ли прослушать линию частный субъект?

Может. Способы: несанкционированное подключение (два «крокодила» на контакты в подъезде или в подвале плюс телефонная трубка), подкуп оператора, перехват радиоканала, включение в поток. «Жучок» как шпионскую технику не трогаем, поскольку защита от нее – предмет отдельного разговора.

Сложность и стоимость частной прослушки со временем растут, но в доцифровую эпоху атака была доступна человеку с доходами ниже среднего. Поэтому такие системы следовало бы считать полностью открытыми.

В этой связи интересны два вопроса. Первый: мог ли фрикер перехватывать разговоры кого угодно с кем угодно?

Эти возможности были весьма ограничены. Несанкционированное подключение – простая, но все-таки оперативная работа. «Частник» может ее выполнить в среде своего обитания, единовременно в одном месте. Ограничен он и в скрытности операции.

Что же до дистанционного перехвата, то он возможен, скорее, теоретически. Опыт случайного включения в разговор есть у каждого пользователя старых городских АТС. Есть фрикерские легенды о дистанционном перехвате. Но в доступной фрикерской литературе описаний процесса подключения к чужому разговору я не нашел. Из чего можно сделать вывод о том, что перехват был случаен, критическим образом зависел от марки и настроек конкретного оборудования. То есть технологии дистанционного перехвата телефонных разговоров у фрикеров не было.

Вопрос второй: мог ли гражданин защититься от прослушки?

Ответ: нет, не мог. Защищенную связь могли себе позволить спецслужбы и правительство, но и они предпочитали выделенные спецсети («Кремлевка», «Искра»). Гражданам же (из склонных к паранойе) оставалось только развивать интуицию с тем, чтобы по шумам, щелчкам и эхо-эффектам линии судить о том «слушают ли меня сейчас?».

Забавы вендоров

Со временем в цифровой телефонии обозначился новый класс устройств – УАТС, учрежденческая АТС. К этому моменту сложность АТС возросла, а дизайн ее элементов (кремний и программное обеспечение) перестал быть прозрачным. Существенно усложнилась сигнализация между АТС и терминалом, поскольку вычислительная машина АТС уже не только «понимала» примитивные сигналы «запрос-отбой», но и стала управлять телефонами абонентов.

Появились сведения о специальных («полицейских») режимах АТС. В 1997 г. я слышал леденящую кровь историю о том, как служащий крупного финансового учреждения, погруженный в размышления, конечно, о макроэкономике, задумчиво барабанил пальцами по клавишам выключенного телефона. И вдруг телефон ожил и начал в режиме громкого вещания транслировать секретнейший разговор Председателя с Вице-президентом... Служащий случайно набрал код доступа к «полицейской» прослушке!

Миф эта история или правда, но «полицейские» режимы присутствуют как в числе документированных функций АТС, так и в виде недекларированных возможностей оборудования. Поэтому, например, при сертификации УАТС практикуется «стерилизация» умных телефонов. Боевые советские офицеры (в прошлом), а ныне предприниматели покупают такие телефоны и впаивают в «шибко умного» герконовый прерыватель. Положит трубку абонент, и цепь питания (или цепь микрофона) физически разорвана. Нехай враг послушает!

Покупает такие телефоны массовый потребитель? Нет. Тогда пусть впишет в перечень некомпенсированных рисков телефонии и прослушку со стороны оператора, сисадмина или «частника», знающего код «полицейского» режима.

Забавы админов

Лакомой добычей злоумышленника является перехват прав управления системой.

В телефонии здесь все относительно благополучно. Дело в том, что в ранних системах задачи настройки системы коммутации, формирования номерного плана, биллинга решались методами механического монтажа. Защита была естественной: «не давать отвертку в руки врага».

На этапах поздней автоматизации и ранней «цифры» управление стало производиться с персонального компьютера. Но и в это время все было неплохо: консоль управления располагалась рядом с АТС, формула защиты была «не пускай врага в спецпомещение». Ну так кто ж его пустит...

Но с ростом числа УАТС, с распространением цифровой телефонии распределенность управления начала расти. Предельным случаем стала сотовая телефония, где контроллеры и коммутаторы базовых станций – это десятки тысяч автономных вычислительных комплексов, работающих в единой инфраструктуре масштаба страны. Локальное управление такими системами в принципе невозможно. Соответственно, возникла задача защиты управления.

К чести телефонистов (операторы связи – знатоки сетевой безопасности), их системы в основном выполнены в технологии «выделенная виртуальная сеть управления» и достаточно защищены. Взлом их – дело весьма трудное. Единственное, на что можно посетовать, – криптография на страже сети там почти повсеместно западная, следовательно – нелегитимная.

Средства аутентификации, управления, мониторинга и аудита целесообразно выделять в отдельный защищенный сетевой периметр

Забавы вокруг биллинга

Если с защитой сетевого управления в цифровых системах все относительно хорошо, то с биллингом таки возникают проблемы. Обычно они лежат в плоскости прикладной логики и не связаны со свойствами инфраструктуры. Сценарии различны: prepaid-карты и пополнение счетов, кража реквизитов эккаунтов, обман систем роуминга с «подставными» SIM-контрактами. Схемы объединяют мошеннический social engineering и знание уязвимостей биллинга. Желания публиковать детали, характерного для «старых» хакеров и фрикеров, у всех участников процесса – мошенников, операторов связи и следователей органов – немного. Типовые схемы надо восстанавливать по косвенным признакам.

Забавы с мобильниками

Сотовая связь, в сравнении с традиционной, даже цифровой, телефонией, существенно децентрализуется. Это промежуточная стадия эволюции между телефонией и сетью данных. Транковая

линия здесь уже не многожильный кабель между АТС и не цифровой поток в оптическом волокне, а просто IP-сеть с поддержкой QoS. На IP часто вынесены также задачи регистрации мобильных абонентов, аутентификации, управления, биллинга. Говорить о защищенности этих подсистем «в сравнении с IP-телефонией» бессмысленно: это одинаковые системы.

Однако у сотовых систем следует отметить важную особенность – громадный интеллект терминала и лавинное увеличение сложности взаимодействия с ним. Отсюда возникают принципиально новые, невиданные для телефона, но вполне привычные для сети данных угрозы: вирусопоражение, спам и т.п.

О безопасности IP-телефонии

Традиционная телефонная сеть и IP-сеть (рис. 2) обладают рядом кардинальных различий, которые сказываются, помимо прочего, и на безопасности.

Прежде всего, по частям исчезает главный узел – телефонная станция. Центральный элемент, к которому следует обратиться при необходимости совершить звонок, остается. Это сервер вызовов. Но, обработав вызов и соединив абонентов, он уходит из процесса. Далее трафик передается по IP-сети непосредственно между абонентами. Транковые сети подключаются к различным маршрутизаторам через соответствующего типа адаптеры. Таким образом, и коммутацию, и транкинг берет на себя не дорогущий и трудно масштабируемый центральный узел, а произвольная по конфигурации и размеру IP-сеть, включенная в сферу обслуживания одного сервера вызовов. В этом – залог гибкости, масштабируемости и дешевизны систем IP-телефонии.

Рис. 2. Схема системы IP-телефонии

Безопасность сети

Будучи по природе своей IP-сетями, сети IP-телефонии подвержены тем же атакам, что и сети данных. И меры защиты они берут из арсенала IP-сетей.

Вкратце они состоят в следующем.

Для сети телефонии проводится спецподготовка коммуникационной среды, а именно:

- Закрывается доступ к оборудованию с целью защиты от несанкционированных подключений.
- На уровне активного сетевого оборудования запрещаются все неиспользуемые протоколы. Применение служебных протоколов защищается.
- На уровне системного ПО настройки переводятся в состояние разрешительной политики доступа («все, что не разрешено явно, – запрещено»), удаляются все неиспользуемые приложения, закрываются неиспользуемые порты, проводится инспекция учетных записей пользователей и администраторов, контроль качества паролей.
- По мере возможности разграничиваются права доступа администраторов, операторов и аудиторов систем, обеспечивается раздельное администрирование систем управления и аудита.

Сегментируются сети голоса и данных, обеспечивается управление адресными пространствами, налаживается контроль доступа средствами коммутации ЛВС (VLAN), а при выходе в WAN-сеть – средствами пакетной фильтрации.

Для IP-телефонов используются внутренние планы IP-адресов, а на периметре – трансляция адресов (NAT). Это исключит возможность утечки голосового трафика «наружу».

Организуется контроль за физическими подключениями. Для этого применяются технологии так называемой MAC-аутентификации, мониторинг событий динамического конфигурирования IP-адресов по протоколам DHCP, ARP и системы IDS/IPS. При правильном применении этих средств несанкционированное подключение будет автоматически обнаружено и выведено из обслуживания, а информация о событии немедленно поступит к администратору безопасности.

Технологии VPN позволяют строго аутентифицировать как пользователей, так и устройства, обеспечить конфиденциальность и целостность трафика, построить криптографически стойкий контроль доступа (в виртуальную защищенную сеть может проникнуть только владелец секретного криптографического ключа, что обеспечивает практическую изоляцию сетевого периметра VPN).

Стандартные VPN-продукты естественным образом интегрируются в существующие инфраструктуры аутентификации, управления, мониторинга и аудита.

Сети и атаки

Атака	Аналоговая телефония	Цифровая телефония	Сотовая телефония	IP-телефония	IP-телефония с применением VPN
Перехват разговора внешним злоумышленником	Открыт для имеющего доступ к линии и/или системам коммутации, прочие режимы затруднены	Теоретически возможен для имеющего доступ к линии. Требует спецоборудования для декодирования уплотненного потока	В штатном режиме исключен (шифрование радиоканала)	Затруднен для не имеющего доступа к трафику. Открыт для имеющего доступ к IP-трафику (если не используется телефон с шифрованием; сертифицированной защиты нет)	Исключен
Перехват разговора оператором (администратором сети)	Открыт	Открыт	Открыт	Затруднен (оператор IP-АТС может не иметь прямого доступа к трафику телефонов)	Исключен
Несанкционированное подключение к сети	Открыто. Требует подключения к линии. Контроль отсутствует	Затруднено. Требует подключения к линии. Контроль ограничен	Исключено	Затруднено или исключено (в зависимости от дизайна мониторинга)	Исключено
Имперсонация терминала (перевод биллинга на другой номер)	Открыта для имеющего доступ к линии или владельца бокса	Открыта для имеющего доступ к линии. Затруднена для владельца бокса. Требует технических средств	Исключена	Практически исключена	Исключена
«Полицейский режим» терминала	Отсутствует в силу примитивности терминала	Возможен	Практически исключен для простых моделей. Для смартфонов и КПК теоретически возможен (хотя весьма затруднен) путем внедрения опасного мобильного кода	Теоретически возможен, затруднен	Исключен
Перехват управления системой	Невозможен	Теоретически возможен, затруднен	Теоретически возможен, на практике весьма затруднен	Теоретически возможен, но весьма затруднен при правильной эксплуатации систем аутентификации	Исключен
Атаки путем манипуляции с персональным идентификатором	Отсутствуют	Отсутствуют	Затруднены, но возможны за счет обмана систем роуминга	Исключены (при правильной эксплуатации систем аутентификации)	Исключены (при правильной эксплуатации систем аутентификации)
Аномальное поведение абонента	Не детектируется	Может быть обнаружено	Детектируется системой обслуживания вызовов и биллинга	Надежно детектируется в различных точках сети	Надежно детектируется в различных точках сети

Для защиты телефонии VPN-продукт должен вносить минимальные задержки, исключать потери данных, не нарушать стабильность потока пакетов.

В контексте построения защиты персональных коммуникаций подчеркнем интересные особенности технологий IPsec VPN:

- Обеспечивается сквозная конфиденциальность переговоров двух абонентов. Разговор не может прослушать никто посторонний (даже если он – пользователь той же защищенной сети).
- Шифрование трафика в стандартных протоколах реализуется на основе временных (сессионных) ключей, которые сменяются через определенное время. В режиме IPsec perfect forward secrecy практически исключена возможность их восстановления в будущем. Это означает, что шифрованный голос существует в открытом виде только во время его звучания.

Защита инфраструктуры

Средства аутентификации, управления, мониторинга и аудита целесообразно выделять в отдельный защищенный сетевой периметр. Организовать его помогут уже упоминавшиеся технологии VLAN и VPN.

Для систем мониторинга и аудита особенно важна централизация: данные о единичном событии на единичном устройстве часто не говорят ни о чем. Централизацию обеспечат протоколы Syslog и SNMP. Но ограничиваться ими не стоит: они позволяют распознать факт атаки после ее завершения. Сегодня их полезно усилить средствами проактивного контроля аномальных активностей и средствами обнаружения и подавления атак, работающими в реальном времени.

Сравним несравнимое

Итак, мы увидели, что сети традиционной телефонии и IP-телефонии – это физически и логически очень разные объекты. Атакуют в них разнородные ресурсы, и типы атак существенно разнятся. Что может дать их сравнение?

Первое. IP-сеть подвержена большему числу атак, чем даже сотовая телефонная сеть.

Второе. По количеству доступных средств защиты, их мощи и комплексности IP-сети превосходят любые телефонные сети.

Результат? Неоднозначен. Представим его в виде таблицы, и пусть каждый делает выводы сам. ИКС

О чем не знают пользователи корпоративной IP-телефонии

Узнать прогноз погоды и биржевые котировки, в чрезвычайной ситуации передать экстренное сообщение по громкой связи, вести учет рабочего времени сотрудников – для всего этого и многого другого достаточно лишь IP-телефона...

Александр АНОШИН, директор компании «БКС-АйТи»

С каждым годом для все большего количества российских служащих IP-телефон становится рабочим инструментом: по оценке J'son & Partners, в 2009 г. 39% предприятий, расположенных в городах-миллионниках, использовали IP-телефонию, и ожидается, что к 2013 г. эта цифра возрастет до 68%. Львиная доля компаний среднего и малого бизнеса отдала предпочтение VoIP-технологиям исключительно с целью снижения затрат на междугородную и международную связь. Однако большинство крупных предприятий внедряют IP-телефонию как более эффективную систему корпоративных коммуникаций, позволяющую уменьшить расходы на связь между удаленными офисами, сэкономить на обслуживании корпоративной сети связи, организовать единый контакт-центр и расширить возможности маршрутизации звонков и организации совещаний.

Остановиться ли этим предприятиям на достигнутом? Или, получив в свое распоряжение столь богатый инструментарий, им стоит задуматься о том, как его применить для решения еще большего количества актуальных задач?

В этой статье мы обсудим перспективы расширения базовых возможностей уже построенной корпоративной сети IP-телефонии с помощью сервисов унифицированных коммуникаций. Описанные решения довольно широко распространены за рубежом, однако российский рынок с ними только знакомится.

Справочная информация на дисплеях IP-телефонов

Практически в каждом бизнесе существует определенный набор вопросов, на которые нужно незамедлительно получать ответы из своевременно обновляемых корпоративных справочников и внешних источников. Оказывается, во многих случаях для этого необязательно прибегать к помощи компьютера, достаточно лишь IP-телефона.

Так, используя IP-телефон, сотрудник банковской организации может получить актуальную информацию о биржевых индексах и курсах валют. Владелец гостиничного бизнеса, оборудовав номера IP-телефонами, сможет повысить уровень обслуживания, предложив постояльцам посмотреть прогноз погоды, ознакомиться с услугами гостиницы, списком развлекательных учреждений и ресторанов.

Одним нажатием кнопки на дисплей IP-телефона вызываются обновленные данные по основным показателям эффективности деятельности компании или нужный контакт в ее едином телефонном справочнике, содержащем номера телефонов партнеров, клиентов, поставщиков и сотрудников всех филиалов. Причем информация в справочнике может и должна регулярно обновляться при помощи импорта данных из системы управления кадрами, CRM-приложений и прочих корпоративных источников.

IP-телефония как инструмент службы безопасности

Корпоративная сеть IP-телефонии может внести свою лепту и в повышение уровня безопасности предприятия. Во-первых, это трансляция экстренных оповещений по телефонной сети при возникновении чрезвычайной ситуации. В этом случае все IP-телефоны предприятия переводятся в режим «спикерфон», текущие разговоры – в режим ожидания, и через внешние динамики IP-телефонов на максимальной громкости передается экстренное сообщение. Причем система рассылки объявлений может задействовать имеющиеся устройства громкой связи – таким образом, объявления будут транслироваться на группу IP-телефонов плюс установленные внешние динамики. Также система оповещения может быть интегрирована с различными системами безопасности предприятия. Используя эту функцию, можно, к примеру, мгновен-

но оповестить всех ответственных лиц о нарушении периметра контролируемого объекта – их телефоны «взорвутся», транслируя предзаписанное голосовое объявление о нарушении.

Во-вторых, это возможность видеонаблюдения, когда экран IP-телефона используется для быстрого доступа к изображениям с видеокамер. Этот сервис будет особенно полезен на стройках, больших производственных площадках, в системах контроля доступа (чтобы получать снимок с камеры за дверью перед тем, как ее открыть).

В-третьих, особую помощь сотрудникам отдела безопасности могут оказать возможность фильтрации «подозрительных» звонков (т.е. звонков на определенные номера или типы номеров, о которых немедленно извещается служба безопасности) и запись разговоров сотрудников.

Наконец, службе безопасности будет доступно прослушивание телефонных переговоров сотрудников компании.

Новые возможности корпоративных коммуникаций

Многим компаниям будет интересна возможность привилегированного управления звонками. Руководители подразделений, а также сотрудники службы безопасности нуждаются в возможности незаметно подключиться к установленному соединению для прослушивания разговора, а супервайзерам часто требуется принять участие в диалоге неопытного сотрудника с клиентом, чтобы своевременно повернуть ход беседы в нужную сторону.

Помимо этого, топ-менеджеры хотят иметь возможность мгновенно связаться со своими подчиненными, даже если их линия в это время занята, или своевременно оповестить сотрудников о предстоящем мероприятии, отправив им текстовое или голосовое сообщение, получение которого необходимо подтвердить.

Решить эти задачи и таким образом повысить эффективность корпоративных коммуникаций можно с помощью специальных сервисов IP-телефонии: системы групповой рассылки голосовых и текстовых объявлений, трансляции экстренных оповещений в режиме реального времени через динамики IP-телефонов, сервиса VIP-управления звонками, автодозвона.

IP-телефония как средство автоматизации бизнес-процессов

IP-телефоны предоставляют базовые возможности ввода-вывода информации, которые можно использовать для разработки интерфейса к корпоративным информационным системам. Таким образом, IP-телефон может стать инструментом автоматизации ряда простых, рутинных бизнес-процессов, которые есть практически в любом производстве. Приведем несколько примеров.

В большинстве организаций нужно вести учет рабочего времени. Для этого тоже могут пригодиться IP-телефоны. Время начала и завершения работы, а также перерывы на обед, перекур и прочее могут регистрироваться непосредственно с IP-телефонов сотрудников, а затем полученные данные будут автоматически экспортироваться в систему учета рабочего времени или систему управления проектами.

Также немаловажно отслеживать телефонные переговоры сотрудников. Используя специальное приложение для корпоративной IP-телефонии, можно вести тщательный учет звонков, на основании которого оценивать эффективность каждого сотрудника: определять процент звонков личного характера, привязывать совершенные телефонные переговоры к клиенту или проекту и формировать отчет о звонках в разрезе сотрудников, клиентов или текущих проектов.

Помимо этого, сейчас все чаще предлагается применять IP-телефон как интерфейс для управления бытовыми устройствами (одна из концепций «умного дома»), будь то осветительные приборы, системы климат-контроля или запорные устройства.

Здесь же уместно вспомнить о возможности бронирования с помощью IP-телефона переговорных комнат, автотранспорта и совместно используемого оборудования.

Для полноты картины приведем узкоспециальный пример: IP-телефон как интерфейс к корпоративной информационной системе в гостиничном бизнесе. Оснащение номеров IP-телефонами позволит не только увеличить количество услуг для гостей, но и оптимизировать работу персонала: через IP-телефон горничная сможет отметить время начала и окончания уборки, указать готовность номера к заселению, направить запрос для пополнения бара и пр.

Подведем итоги...

Итак, внедрение дополнительных программных сервисов в функционирующую сеть корпоративной IP-телефонии может помочь:

- ускорить доступ к часто изменяющейся справочной информации, обеспечив при этом ее своевременную актуализацию;
- повысить уровень безопасности предприятия;
- сделать внутрикорпоративное общение более эффективным;
- автоматизировать ряд бизнес-процессов, не требующих передачи большого объема данных.

Конечно, решить эти задачи можно и «традиционными» методами – с помощью программного обеспечения, установленного на персональном компьютере. Но в ряде случаев IP-телефоны будут эффективнее: например, на производстве, где большинство рабочих мест оснащено телефонами, а не персональными компьютерами, или в отделе продаж, где телефон – наиболее привычное орудие труда каждого сотрудника, а, значит, возможность использовать именно его для доступа к наиболее востребованной информации поможет существенно повысить производительность труда.

Можно привести еще много примеров рационального использования внедренной сети корпоративной IP-телефонии, но цель этой статьи – лишь предоставить пищу для размышления и помочь шире взглянуть на то, чем вы привыкли пользоваться каждый день... ИКС

Ведущий дистрибутор AVAYA
AURA/Communication Manager/IP Office
AVAYA Data Solutions

Комфортное партнерство

- Программа поддержки новых партнеров
- Сертификация компаний и специалистов
- Специальные программы для операторов связи
- Поддержка проектов
- Центр Экспертизы Решений
- Учебный Центр (десятки учебных программ)
- Испытательная Лаборатория

COMP TEK

AVAYA

Абонент хорошей АТС редко помнит ее название. Он просто звонит.

142784, Москва, Киевское шоссе,
бизнес-парк «Румянцево»,
стр. 1, подъезд 5, этаж 8.
тел.: (495) 789-6565,
факс: (495) 278-3053
www.comptek.ru
e-mail: sales@comptek.ru

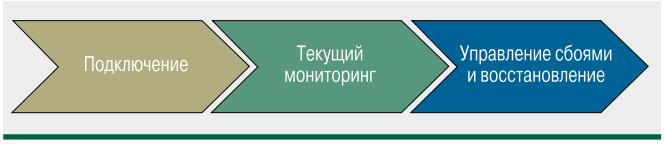
Возможности управления жизненным циклом услуг Carrier Ethernet

По мере того как услуги Carrier Ethernet все чаще применяются в коммерческих приложениях и для передачи сотового трафика, операторы связи начинают испытывать потребность в наборе инструментов для более эффективного предоставления, мониторинга и управления услугами E-Line, E-Tree и E-LAN. Эти возможности могут обеспечить демаркационные устройства Ethernet с поддержкой тестирования.

Кроме оптимизации сетевых процессов и повышения качества услуг до соответствия ожиданиям потребителей, такие инструменты позволяют существенно снизить расходы и найти источники прибылей. В частности, операторы могут ускорить выведение услуги на рынок за счет уменьшения усилий и времени, необходимых для запуска; сократить число выездов на места, вызовов технических специалистов и обращений по поводу сбоев благодаря удаленному тестированию, сквозному обзору и проактивному мониторингу; свести к минимуму штрафы за нарушения SLA (соглашения об уровне обслуживания); снизить отток абонентов благодаря понятным и четким отчетам по оказанным услугам и меньшему количеству споров об оплате.

В критических точках жизненного цикла услуги оператору нужно применять различные процедуры тестирования. Вот некоторые практические рекомендации.

Этапы жизненного цикла услуги



Подключение услуги

Управляемое внедрение новой услуги обычно включает установку, тестирование линии и услуги и приемочные испытания, призванные показать, что услуга работает правильно и в соответствии с параметрами QoS (качество обслуживания) и CoS (класс обслуживания), определенными в SLA. На этом этапе тестирование служит также для формирования основных параметров производительности, с которыми будут сравниваться результаты будущих проверок. В частности, для сквозной пропускной способности определяются ключевые индикаторы производительности (KPI): коэффициент доставки пакетов, задержка и джиттер. Результаты этих измерений сохраняются для отчета потребителям, сравнения с требованиями SLA и другого использования в будущем, например, оценки параметров услуги после модернизации или восстановления. Для точной настройки услуги проводятся испытания при максимальной нагрузке в течение 24–72 ч перед предоставлением линии для критически важных приложений.

Например, в случае услуги 3-CoS EVPL (Ethernet Virtual Private Line) между несколькими пунктами – центральным офисом предприятия, удаленными филиалами и ЦОДом – некоторые из пунктов могут находиться вне зоны покрытия сети оператора, и для их подключения придется воспользоваться участками сети другого поставщика услуг связи. Оператор в таком случае должен быть уверен, что EVC работает без сбоев, что каждый тип трафика соответствует записанным в SLA гарантиям QoS и что существует сквозной обзор всего пути прохождения трафика услуги, включая участки чужой сети, так что можно точно установить причины возможных неполадок и быстро их устранить.

Функция	Инструмент
Верификация соединения	Проверка целостности (Unicast/Multicast) согласно Y.1731/IEEE 802.1ag
	Кольцевая проверка (MAC Ping, Unicast/Multicast) согласно Y.1731/IEEE 802.1ag
Диагностические проверки	L1 кольцевая проверка физического интерфейса
	L2/3 кольцевая проверка каждого потока на скорости линии или меньше, с переключением MAC/IP
Нагрузочные испытания	Измерения пропускной способности и тест BER согласно RFC-2544
Верификация SLA	Потеря пакетов, задержка пакетов, вариация задержки пакетов согласно RFC-2544

Текущее управление услугой и мониторинг

Измерения KPI осуществляются и на постоянной основе, для мониторинга состояния сети и обеспечения QoS в соответствии с описанным в SLA классом обслуживания. Непрерывный мониторинг необходим для обнаружения деградации услуги и сетевых заторов. Соответствующие оповещения показывают оператору, где необходимо улучшить пропускную способность. Когда нарушается соединение или работа услуги, выполняются соответствующие действия по устранению сбоев. Собранные данные интегрируются системами бэк-офиса, отчеты о состоянии сети и услуги доступны предприятию периодически или по запросу. Тесты OAM проводятся с такой частотой, которая оптимальна для быстро-

Функция	Инструмент
Мониторинг производительности	Потеря и задержка пакетов, вариация задержки пакетов на EVC.CoS согласно ITU-T Y.1731
	Доступность согласно G.826
Отчеты о порогах SLA	Отчеты через EMS согласно Y.1731
Статистические отчеты	Отчеты через EMS с помощью TFTP, SNMP согласно Y.1731

го обнаружения и устранения проблем, но соответствует желанию оператора ограничить использование ресурсов сети и пропускной способности на тестирование.

Управление сбоями и восстановление

Важное место в управлении жизненным циклом услуги занимает возможность выявлять проблемы, влияющие на работу услуги, находить их точное место и оповещать о них. Самое важное место в этом процессе отводится демаркационным устройствам в точках передачи трафика услуги. Чтобы устранить возникшую проблему и упредить дальнейшую ее эскалацию, демаркационные устройства осуществляют определение и изоляцию сбоя, удаленное тестирование и восстановление. Проводится набор удаленных тестовых операций до выезда технического персонала на место сбоя. Это снижает среднее время до восстановления работоспособности услуги (MTTR) и уменьшает воздействие сбоя на потребителей. Операционные расходы сокращаются, поскольку дорогостоящие выезды техников не производятся без необходимости.

Функция	Инструмент
Определение и изоляция сбоя	Проверка целостности или кольцевая проверка (MAC Ping) согласно Y.1731/IEEE 802.1ag
	Трассировка линии (MAC Trace-route) согласно Y.1731/IEEE 802.1ag
	L3 Ping и Trace-route
Оповещение и передача сигнала о неисправности	Отключение пользовательского порта
	Аварийная индикация, индикация удаленной неисправности согласно ITU-T Y.1731
	Отправка сигнала перед отключением, SNMP-прерывание согласно IEEE 802.3ah
Диагностические проверки	L1 кольцевая проверка физического интерфейса
	L1 IEEE 802.3ah кольцевая проверка
	L2/3 кольцевая проверка каждого потока в процессе работы услуги
Восстановление	G.8031 защитное линейное переключение Ethernet (ELPS, EVC Protection)
	IEEE 802.3-2005 (ранее 802.3ad) защита порта на основе агрегации каналов
	G.8032 защитное кольцевое переключение Ethernet (ERPS)

Демаркационные устройства Ethernet с поддержкой тестирования

Развитые возможности тестирования снижают общую стоимость владения при внедрении услуг Carrier Ethernet. Реализация в одном устройстве функциональности и самой услуги, и тестирования позволяет обойтись без дополнительного оборудования и процедур для тестов. Такие устройства, работая с другими оконечными сетевыми устройствами или тестовыми системами, генерируют тестовый трафик или выполняют функции тестового зонда. Управление трафиком и тестирование для каждого потока снижают стоимость в расчете на один порт и устраняют проблемы с доступностью порта при установках и запусках. Модернизация услуг на таких устройствах легко производится программным способом. И, конечно, их применение кардинально снижает необходимость выездов технического персонала.

Нет нужды говорить, что описанные выше функции не поддерживаются ни медиаконвертерами Ethernet, ни стандартными коммутаторами Ethernet. Такой функциональностью обладают специализированные демаркационные устройства, в частности интеллектуальное оборудование семейства EtherAccess производства RAD Data Communications. Например, операторы первого и второго уровня во всем мире применяют оборудование Carrier Ethernet ETX-204A, RICi-16 и LA-210 для Ethernet-доступа по любой инфраструктуре – оптике, меди или xDSL.

Подобные демаркационные устройства незаменимы в условиях, когда трафик проходит через различные сети и необходимо в любой момент иметь полный обзор всего пути услуги. Кроме того, очень быстрая обработка трафика, основанная на аппаратных особенностях этого оборудования, позволяет немедленно обнаружить потерю целостности и произвести резервное переключение менее чем за 50 мс. Устройства проводят очень точное измерение потерь пакетов при тестировании на реальном трафике. Измерения задержки выполняются с точностью более 1 мкс. Мониторинг на уровне потока пакетов позволяет одновременно осуществлять сотни сессий OAM.

При внедрении услуги имеет значение даже физическая конструкция демаркационных устройств Carrier Ethernet. В повседневной операторской практике нередки случаи несоответствия формулировки технического задания на установку или тестирование, которое получает технический персонал, и реального состояния оборудования в точках доступа к услуге. Это приводит к потерям времени и повторным выездам на места. Часто случаются даже простые ошибки в определении типа порта или режима электропитания. Благодаря продуманному дизайну обслуживание демаркационных устройств EtherAccess производства RAD меньше подвержено влиянию подобных ошибок. Вся необходимая информация расположена на передней панели, устройства имеют два режима электропитания и комбинированные порты UTP/SFP.

Демаркационные устройства, обладающие функциями тестирования для каждого потока, такие как семейство оборудования RAD EtherAccess, позволяют операторам связи упростить внедрение, мониторинг и поддержку услуг Carrier Ethernet. Тестирование услуг, которое осуществляется автоматически и независимо от происхождения сетевого оборудования, позволяет операторам снизить расходы, оптимизировать процедуры и повысить прибыльность услуг.

Услуги triple play на сетях доступа FTTx

Быстрый рост абонентской базы ШПД и высокие требования к организации последней мили заставляют операторов связи все чаще отказываться от развития классических технологий доступа, таких как ADSL. Альтернативой им становятся сети FTTx, в которых для доставки трафика используется оптическая линейная инфраструктура.

Константин СИЛИВЕРСТОВ,
менеджер отдела продуктов и решений для сетей передачи данных Huawei CIS

Основные проблемы ADSL заключаются в серьезных ограничениях по полосе пропускания канала, низкой его стабильности и высоких операционных затратах, обусловленных необходимостью поддерживать приемлемое для данной технологии качество проводной инфраструктуры. Этих недостатков лишены архитектуры доступа на базе Ethernet или семейства протоколов PON (GEPON).

Общее в этих решениях – использование оптической линейной транспортной инфраструктуры для доставки трафика потребителям (технологии FTTx). В обоих случаях поддерживаются древовидные и кольцевые топологии оптических каналов. В GEPON разветвление оптики обеспечивается за счет использования на узловых точках оптических пассивных разветвителей, а разделение каналов – за счет механизмов мультиплексирования. В случае «чистого» Ethernet для разветвления транспортных каналов на узловых точках устанавливают активное оборудование коммутации Ethernet.

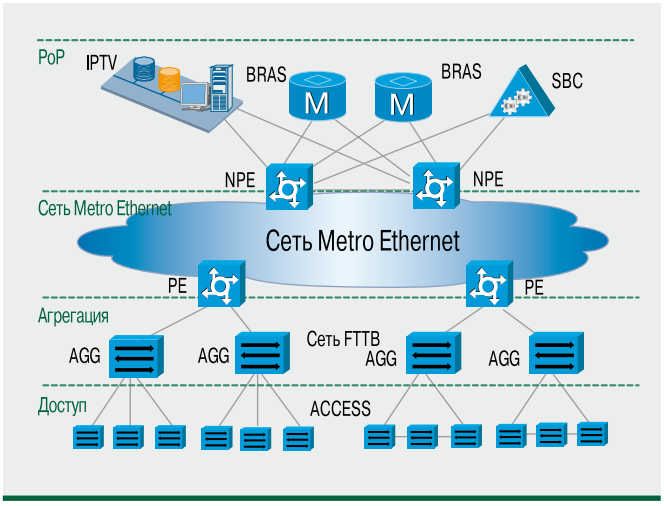
Как GEPON, так и Ethernet имеют хорошие перспективы развития на российском телекоммуникационном рынке для построения сетей FTTx. К преимуществам GEPON можно отнести большую отказоустойчивость, обусловленную применением пассивных оптических разветвителей. Кроме того, технология не требует установки активного оборудования, а значит, нет и сопутствующих проблем. Главным недостатком решений на базе GEPON является более высокая их стоимость по сравнению с решениями Ethernet и меньшая гибкость при реализации схем резервирования. Хотя есть все основания в скором времени ожидать серьезного удешевления решений GEPON, на сегодняшний день сети доступа на базе Ethernet доминируют на российском рынке благодаря гораздо более низкой стоимости решений.

При построении сетей доступа FTTx в России в основном используется архитектура FTTB (оптика до здания). Учитывая широкое распространение сетей FTTB с использованием активного сетевого оборудования Ethernet и особой актуальности вопросов реализации на данных сетях конвергентных услуг, мы сделаем особый акцент на услугах в рамках модели triple play.

Архитектура мультисервисной сети

В последние годы крупные операторы связи все чаще при строительстве сети исходят из централизованной модели предоставления серви-

Рис. 1. Типовая сеть передачи данных



сов, что обусловлено существенным снижением капитальных и операционных затрат на построение и эксплуатацию сети. Как правило, всю централизованную телематическую инфраструктуру оператора связи можно разделить на логические уровни (рис. 1).

PoP (Point of Present). Это уровень предоставления сервиса потребителям услуг. Как правило, оборудование данного уровня располагается на одном центральном узле оператора. В соответствии с моделью triple play потребителям телематических сервисов могут предоставляться следующие услуги:

- передачи данных HSI (High Speed Internet);
- передачи видео BTV (Broadcast TV), VOD (видео по запросу);
- передачи голоса VoIP (IP-телефония).

Каждый из этих сервисов имеет свои специфические требования к сети передачи данных. Так, HSI обеспечивает высокоскоростной доступ к ресурсам Интернета, коммерческим телематическим сервисам компании, межпользовательский обмен трафиком. На уровне доступа используются протоколы IPoE и PPPoE, сервис в большинстве случаев предоставляется агрегаторами трафика широкополосного доступа (BRAS). Для него обычно обеспечивается базовое качество сервиса.

Сервис BTV – это предоставление услуг телевещания, базирующихся на многоадресной рассылке (Multicast). Источником трафика является BTV-система. Для данного типа трафика наиболее критична потеря пакетов.

Сервис VOD – предоставление услуг телевещания, базирующихся на целевой одноадресной рассылке по запросу со стороны пользователя. Источником трафика является централизованная VOD-система. Как и BTV, данный тип трафика чувствителен к потерям пакетов.

Сервис VoIP предоставляется инфраструктурой NGN. Стык с сетью передачи данных организуется через пограничный контролер сессий (SBC). Данный тип сервиса наиболее требователен к задержкам и джиттеру на сети.

Магистраль Metro Ethernet. Основная задача данного уровня – агрегация трафика и надежная его доставка в соответствии с вышеперечисленными требованиями от уровня предоставления сервиса (PoP) до уровня доступа и обратно. В большинстве современных операторских сетей в качестве транспортного протокола на сети Metro Ethernet используется IP/MPLS. Для агрегации трафика служит технология VPLS/HVPLS.

Уровень доступа (сеть FTTB). Основные задачи данного уровня – обеспечение пользователям услуг triple play доступа к телематическим сервисам, агрегация трафика пользователей, транспорт трафика до пограничных коммутаторов магистральной сети Metro Eternet и обратно.

Архитектура сети FTTB

Как правило, сеть доступа FTTB хорошо вписывается в двухуровневую модель, включающую уровень агрегации трафика и уровень доступа. В соответствии с данной моделью разделяются задачи активного оборудования сети доступа.

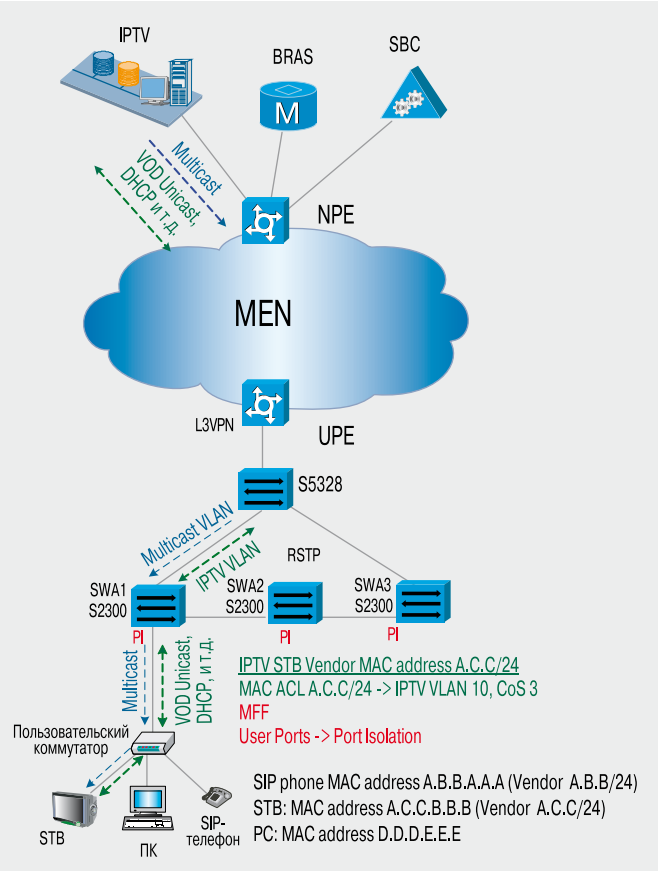
Задачи коммутаторов уровня агрегации:

- агрегация оптических каналов от коммутаторов уровня доступа по оптимальной цене;
- доставка трафика телематических услуг до магистрального коммутатора сети Metro Ethernet в соответствии с требованиями, определяемыми моделью triple play;
- при необходимости – обеспечение резервирования транспортного пути и механизмов защиты от петель на базе протоколов семейства STP;
- реализация политик управления пользовательским трафиком в соответствии с сервисной моделью, используемой в сети оператора.

Задачи коммутаторов уровня доступа:

- доставка трафика телематических услуг до потребителей телематических сервисов, включая классификацию трафика в зависимости от типа сервиса triple play и обеспечение качества обслуживания в соответствии с требованиями для каждого типа сервисов;
- минимизация рисков несанкционированных действий со стороны пользователей, влекущих за собой нецелевое использование ресурсов сети доступа;

Рис. 2. Модель реализации услуг IPTV



- при необходимости – резервирование транспортных путей до агрегирующих коммутаторов сети доступа;
- защита от возможных петель трафика и вызванного ими флаппинга MAC-адресов со стороны пользователей.

Большинство из перечисленных задач уровня доступа достаточно просто решается в рамках классического функционала L2-коммутации и не представляет технических сложностей. Однако решение некоторых задач не столь очевидно. Наибольшую сложность может вызвать совместное решение задач классификации входящего от пользователя трафика в соответствии с моделью предоставления конвергентных услуг и минимизации рисков, вызванных несанкционированными действиями со стороны пользователей.

Рассмотрим модель предоставления сервисов triple play и вариант построения модели доступа для конвергентных услуг, которые предлагает компания Huawei Technologies.

Модели сервисов triple play на сети Ethernet

Сервис IPTV

Для сервиса IPTV, модель предоставления которого приведена на рис. 2, доставка трафика, в зависимости от типа, имеет следующие особенности:

Сервис **BTV** базируется на многоадресной рассылке (Multicast). На сети доступа для доставки трафика пользователям используется механизм Multicast VLAN. Трафик BTV в направлении сети доступа на пограничном магистральном коммутаторе Metro Ethernet маркируется приоритетом 802.1p CoS 3.

Сервис **VOD** базируется на целевой рассылке (Unicast). На сети доступа для доставки трафика пользователям используется выделенный сервисный IPTV VLAN. Трафик VOD в направлении сети доступа на пограничном магистральном коммутаторе Metro Ethernet,, как и в случае BTV, маркируется приоритетом 802.1p CoS 3.

Служебный трафик (DHCP, HTTP, TFTP и т.п.) доставляется по той же модели, что и VOD. Если необходимо использовать для SBC протокол DHCP, то на пограничном магистральном коммутаторе в сервисном VLAN IPTV настраивается DHCP relay на платформу IPTV.

Классификация трафика. Клиентские порты на коммутаторах доступа настраиваются в режиме 802.3 (access). Определяются диапазоны MAC-адресов, используемые производителями терминального оборудования IPTV (Set To Box STB).

На портах доступа в направлении от клиента создаются правила классификации трафика на основе маскируемых списков доступа (MAC ACL), в которые попадают фреймы с MAC-адресами STB. Для входящего трафика с MAC-адресов, принадлежащих диапазону STB, добавляется внешний тег 802.1q IPTV vlan (например, 10). Чтобы обеспечить приоритет служебному трафику, этот тип трафика маркируется CoS 3.

Защита сети доступа от петель трафика и флаппинга MAC-адресов. Для сервиса IPTV риск деградации сервисов минимален, поскольку MAC ACL предотвратит попадание MAC-адреса шлюза (PE) в IPTV VLAN.

Сервис VoIP

Для этого сервиса, модель реализации которого приведена на рис. 3, доставка трафика различных типов имеет следующие особенности:

Сервис **SIP** (сигнализация) базируется на целевой рассылке (Unicast).От платформы SBC до пограничного магистрального коммутатора Metro Ethernet трафик обычно доставляется с использованием L3VPN. На сети доступа для доставки трафика пользователям используется выделенный сервисный голосовой VLAN (Voice VLAN). Трафик на магистральном маршрутизаторе в направлении сети доступа в голосовом VLAN маркируется приоритетом 802.1p CoS 5. SBC работает в режиме SIP Proxy.

Служебный трафик (DHCP, HTTP, TFTP и т.п.). Механизмы его доставки и приоритизации полностью аналогичны транспортной модели для SIP. Если необходимо использовать для SIP-телефонов протокол DHCP, то на пограничном магистральном коммутато-

Рис. 3. Модель реализации услуг VoIP

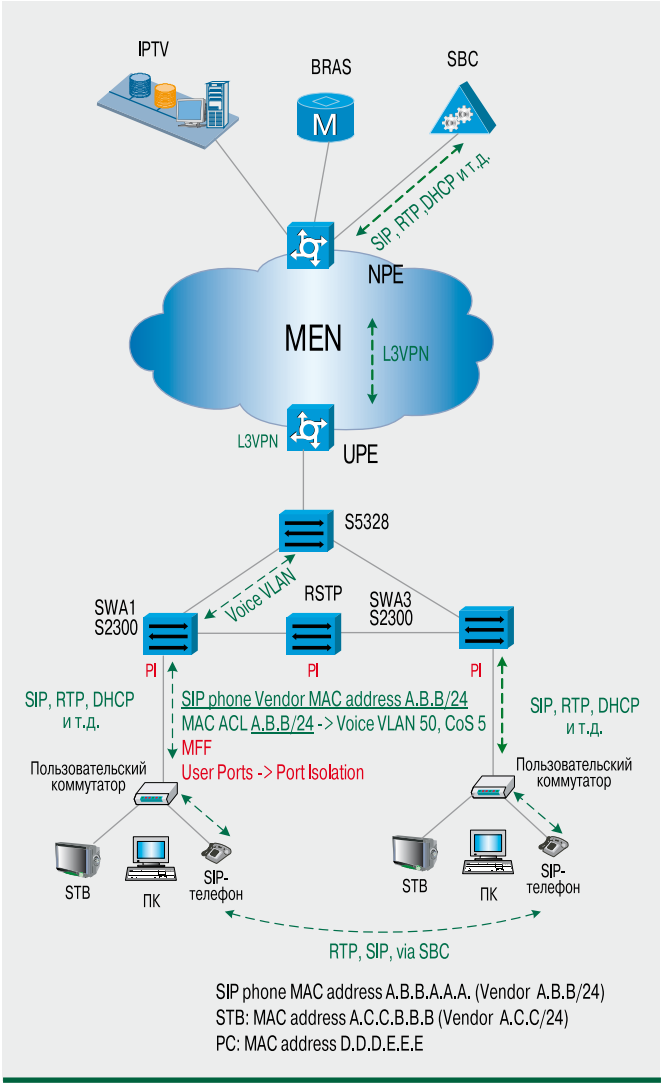
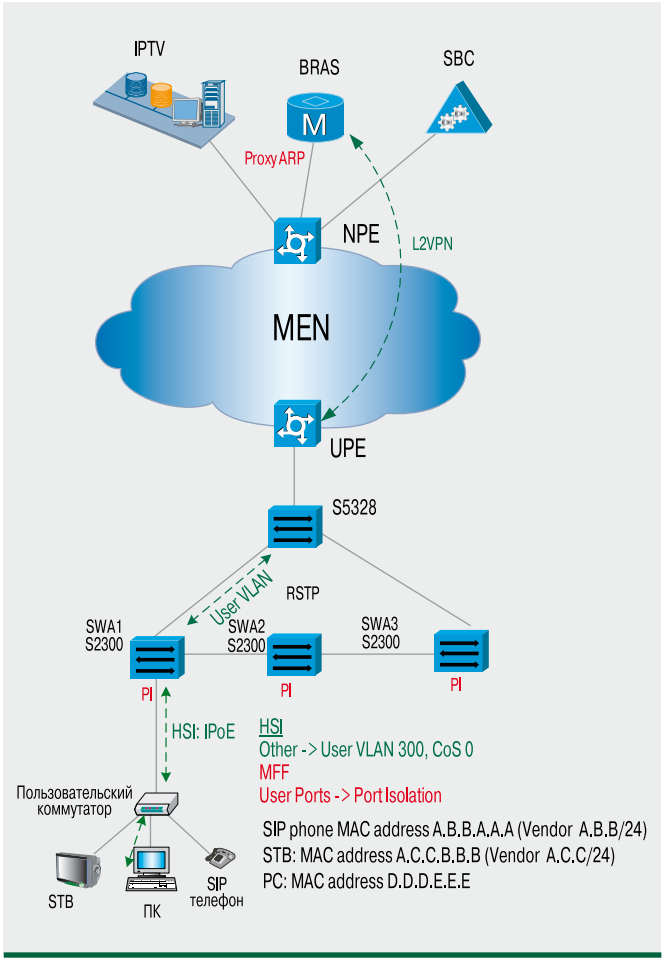


Рис. 4. Модель сервиса HSI



ре в сервисном Voice VLAN настраивается DHCP relay на платформу SBC.

Трафик RTP (голосовой). Механизмы его доставки и приоритизации также аналогичны механизмам доставки SIP и служебного трафика. Хождение трафика между пользователями на коммутаторах агрегации и доступа блокируется функционалами Port Isolation и MFF (см. выше, модель IPTV). Для обмена RTP-трафиком между SIP-телефонами на терминирующем пограничном маршрутизаторе, в голосовом VLAN, активизируется функционал Proxy ARP.

Классификация трафика. Клиентские порты на коммутаторах доступа настраиваются в режиме 802.3 (access). Определяются диапазоны MAC-адресов, используемые производителями терминального оборудования SIP-телефонов. На портах доступа в направлении от клиента создаются правила классификации трафика на основе MAC ACL, в которые попадают фреймы с MAC-адресами SIP-телефонов. Для входящего трафика с MAC-адресов, принадлежащих диапазонам SIP-телефонов, добавляется внешний тег 802.1q Voice VLAN (например, 50). В целях приоритизации голосовой трафик маркируется CoS 5.

Сервис HSI (передача данных)

Для сервиса HSI, модель которого приведена на рис. 4, классификация трафика организована следующим образом. Клиентские порты на коммутаторах доступа настраиваются в режиме 802.3 (access). Определяются диапазоны MAC-адресов, используемые производителями серверов широкополосного доступа (BRAS). На портах доступа в направлении от клиента создаются правила классификации трафика на основе списков MAC ACL, в которые попадают фреймы с любых MAC-адресов, за исключением MAC-адресов BRAS. Данное правило важно для предотвращения возникновения петель на уровне доступа. Правило классификации трафика HSI должно работать только после того, как трафик проклассифицирован согласно правилам классификации для сервисов IPTV и VoIP. Для входящего трафика HSI добавляется внешний тег пользовательского VLAN (например, 802.1q 300) и устанавливается приоритет 802.1p CoS 0.

Минимизация рисков НСД

Для всех трех типов сервисов triple play характерен один и тот же типичный сценарий несанкционированного доступа со стороны пользователей. Так, в случае сервиса IPTV он выглядит следующим образом: пользователь, находящийся в одном бродкастовом домене, подменяет на клиентской стороне MAC-адрес на адрес из диапазона STB. Затем он подменяет IP-адрес и пытается использовать сервисный VLAN IPTV для обмена трафиком в бродкастовом домене IPTV.

Предлагаемое решение задачи: в IPTV VLAN на коммутаторе доступа активизируется функционал MFF (имеется у коммутаторов Huawei S5300, S2300). Данный механизм перехватывает все ARP-запросы и перенаправляет их на MAC-адрес интерфейсной карты магистрального коммутатора Metro Ethernet, где терминируется IPTV VLAN (MAC-адрес шлюза обнаруживается автоматически). На терминирующем IPTV VLAN магистральном коммутаторе в IPTV VLAN выключается механизм Proxy ARP, что исключает обмен трафиком через магистральный коммутатор. На пользовательских портах активизируется также механизм Port Isolation (исключает хождение трафика L2 между портами, на которых активизирован данный функционал), в результате чего пропускается только IP-трафик.

Для сервисов VoIP и HSI предлагается аналогичное решение, базирующееся на функционале MFF и Port Isolation коммутаторов Huawei S5300 и S2300.

■ ■ ■

Безусловно, рассмотренный в статье вариант реализации услуг triple play на сетях доступа Ethernet – не единственно возможный. Существуют альтернативные варианты решения задачи классификации и разделения трафика, например посредством организации на клиентском интерфейсе коммутатора доступа транка 802.1q, с последующим разделением сервисов по VLAN, но надо отметить, что такой вариант будет гораздо более затратным. ИКС

За госуслугой в МФЦ

Грядущий переход органов госвласти к предоставлению услуг в электронной форме не означает их отказа обслуживать граждан, обратившихся очно. Для повышения комфортности получения государственных и муниципальных услуг в регионах РФ создаются многофункциональные центры. О роли, которую они могут сыграть в построении информационного общества, – Михаил ИВАНКОВ, заместитель гендиректора аудиторско-консультационной группы «Развитие бизнес-систем».

Михаил ИВАНКОВ

Препятствия на пути к информационному обществу

весьма многообразны. Они носят технический, правовой, организационный и даже ментальный характер.

Так, в отдаленных населенных пунктах еще слабо развита сетевая инфраструктура. Для оказания многих государственных и муниципальных услуг в электронном виде требуется внести в нормативную правовую базу изменения, которые уравняли бы в правах бумажную и электронную форму документа.

Большая часть населения нашей страны пока не умеет и психологически не готова получать государственные и муниципальные услуги через Интернет: 92% граждан из тех, кто регулярно пользуется интернет-ресурсами, после ознакомления со справочной информацией о порядке получения услуги на официальном портале органов власти все равно предпочитают пойти в само учреждение уточнить и перепроверить полученные сведения. А органы власти всех уровней еще не осознали необходимость систематически обновлять информацию, размещаемую ими на своих веб-сайтах.

Не появился до сих пор орган, выступающий в роли администратора процессов оказания сложных услуг (тех, в предоставлении которых участвуют несколько органов власти), а попытки преодоления межведомственной разобщенности имеют несистемный характер и осуществляются в инициативном порядке.

Да и перевести абсолютно все госуслуги в электронный вид не представляется возможным: для получения паспорта или свидетельства регистрации собственности гражданину все равно придется идти за готовым документом.

Новый тип учреждений поможет их преодолеть

Опыт 35 регионов РФ показывает, что все вышеперечисленные проблемы решаются при создании многофункциональных центров предоставления государственных и муниципальных услуг.

Задача этих учреждений – в максимально комфортной для граждан обстановке оказывать в режиме «одного окна» услуги всех уровней (федерального, регионального, муниципального) по единым стандартам и регламентам, в соответствии с унифицированными административными процедурами.

Обеспечить скоординированное, своевременное и качественное оказание услуг населению позволяет автоматизированная информационная система поддержки деятельности МФЦ (АИС МФЦ). Она включает в себя три подсистемы: информационно-справочную, подсистему автоматизации и контроля процесса оказания государственных и муниципальных услуг, а также сервер форм.

АИС МФЦ помогают быстро и качественно исполнять сквозные административные регламенты, которые закрепляют единую последовательность действий различных органов власти, участвующих в оказании одной услуги. В результате между ведомствами ходит не заявитель и не посредник, а соответствующая информация. Таков вклад многофункциональных центров предоставления государственных и муниципальных услуг в налаживание межведомственного взаимодействия.

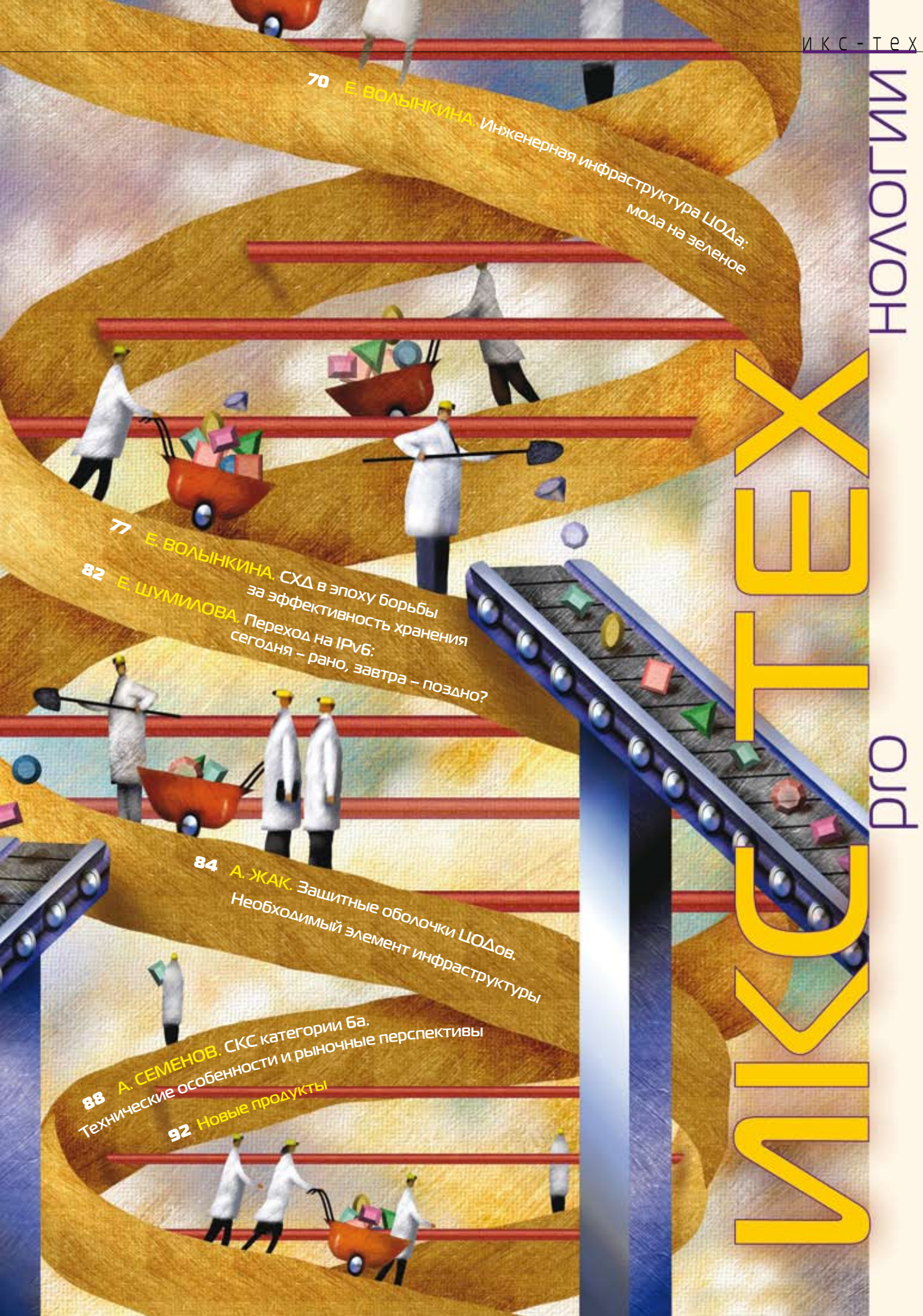
МФЦ наряду с центрами телефонного обслуживания и представительствами органов власти в Интернете – один из основных коммуникационных каналов между государством и гражданами. Вместе они являются воплощением внедряемой сегодня вневедомственной модели взаимодействия государства с населением, когда граждане общаются не с отдельным органом власти, а с государственной системой в целом.

Многофункциональные центры снабжены доступом к порталу госуслуг. Граждане, приходящие в МФЦ, могут также воспользоваться терминалами для доступа к порталу госуслуг в Интернете. Тем, кто не чувствует уверенности в работе с новыми технологиями, помогают сотрудники учреждения. Таким образом МФЦ способствуют повышению уровня компьютерной и правовой грамотности населения, преодолению цифрового неравенства.

Развертывание сети МФЦ позволяет оптимизировать бюджетные расходы на предоставление качественных государственных услуг гражданам, поскольку в этом случае существенно снижаются трудозатраты работников органов власти на обслуживание населения: большая часть их функций передается «универсальным» специалистам многофункциональных центров.

О том, что органы власти в российских регионах приходят к пониманию полезности этих новых учреждений, лучше всего свидетельствует тот факт, что сегодня многофункциональные центры уже предоставляют государственные и муниципальные услуги жителям 35 субъектов РФ. И до конца 2010 г. обязательства по развертыванию системы МФЦ взяли на себя еще 47 регионов РФ. ИКС

ИКС pro технологии



Инженерная инфраструктура ЦОДа: мода на зеленое

Евгения ВОЛЫНКИНА

О том, как повысить энергоэффективность инфраструктуры дата-центров и каковы экономические последствия внедрения технологий энергосбережения, шла речь на 5-й Международной конференции «ЦОД-2010», организованной журналом «ИКС».

Для нормальной работы современных компьютеров необходима серьезная инженерная инфраструктура, которая вносит весомый вклад в и без того внушительное энергопотребление дата-центров. Развитые страны, где ЦОДы в их нынешнем понимании появились гораздо раньше, чем у нас, уже давно обеспокоены их энергопрожорливостью. В 2007 г. американское Агентство по защите окружающей среды (U.S. Environmental Protection Agency) представило Конгрессу США специальный доклад об эффективности серверов и дата-центров, где указывалось, что в 2006 г. на потребление американских ЦОДов пришлось 1,5% всей вырабатываемой в США электроэнергии, что составило 61 млн МВт•ч, а потрачено на это было $4,5 млрд. Причем почти 10% этой электроэнергии «съели» серверы и дата-центры государственных федеральных организаций, на что из карманов налогоплательщиков пошло около $450 млн. В том же докладе была отмечена тенденция удвоения энергопотребления ЦОДов каждые 5–6 лет и сделан прогноз на 2011 г.: если рост энергопотребления будет идти такими же темпами, то доля дата-центров в общенациональном потреблении электричества даже при использовании технологий виртуализации и повышения энергоэффективности серверов достигнет 2,9%, что составит 100 млн МВт•ч, или $7,4 млрд в год. Иначе говоря, при сохранении тех же пропорций энергопотребления частных и государственных ЦОДов затраты федерального бюджета США составят $7,4 млрд, а это деньги налогоплательщиков, к которым там относятся трепетно. Не менее трепетно относятся к своим деньгам и владельцы корпоративных и коммерческих дата-центров. Усилия «Гринписа» и партий «зеленых» тоже не проходят даром (в Европе их позиции очень сильны, да и цены на электричество там выше, чем в США), так что борьба за снижение энергопотребления и повышение энергоэффективности в развитых странах имеет уже не только экономическую подоплеку.

Первым делом надежность, но...

Всем известна разработанная Uptime Institute классификация дата-центров по уровням надежности Tier I, II, III и IV, которая определяет зависимость среднего времени простоя ИТ-оборудования ЦОДа от структуры инженерных систем и уровня их избыточности. При сертификации проектов дата-центров и готовых площадок Uptime Institute всегда ставил и ставит во главу угла их надежность. Надежность требует резервирования инженерных систем, а резервному оборудованию нужно электропитание, поэтому дата-центр уровня Tier III и IV не может иметь рекордно низкого PUE просто по определению.

Однако такая приверженность надежности не означает, что Uptime Institute не интересуют проблемы энергоэффективности дата-центров. Интересуют и даже очень: начиная с 2007 г. главными темами всех ежегодных симпозиумов Uptime Institute были энергосбережение, энергоэффективность и зеленые технологии. Кроме того, вот уже три года подряд Uptime Institute присуждает призы Green Enterprise IT (GEIT) Award дата-центрам, в которых реализова-

ны инновационные идеи и технологии, позволившие достичь заметных результатов в деле экономии электроэнергии. Подать заявку может дата-центр любой страны, любой мощности, любого размера и уровня надежности, и для этого совсем не надо иметь сертификат Tier Standard: Topology от Uptime Institute. Кстати, обладателей таких сертификатов как раз и нет среди лауреатов премии GEIT. Основная цель этого конкурса – обмен опытом и распространение лучших практик использования технологий энергосбережения.

О некоторых лауреатах 2010 г. рассказал на конференции Алесдер Мелдрум, ведущий эксперт Uptime Institute. Среди них были и уже известные широкой публике проекты, и те, о которых мало кто знает. В числе первых стоит упомянуть дата-центр, расположенный под Успенским собором в Хельсинки. В системе его охлаждения с ноября по май используется морская вода, а в остальное время года – абсорбционные чиллеры. Но самой смелой идеей является использование тепла, выделяемого оборудованием ЦОДа, для отопления жилых домов. В результате всех этих мер затраты на охлаждение дата-центра сократились на 80%, его PUE оказался меньше 1(!), а энергопотребление всего города Хельсинки сократилось на 1%.

Еще один проект, ставший уже фактически притчей во языцех, это дата-центр Microsoft в Чикаго, представляющий собой ангар, в котором находятся контейнеры с серверами и собственными системами охлаждения. В ангаре площадью около 30 тыс. м² можно установить до 56 контейнеров, каждый из которых может содержать до 2400 серверов. По заявлению Microsoft, текущие операционные расходы на содержание такого ЦОДа на 30% ниже, чем в дата-центре традиционной архитектуры с той же мощностью. Uptime Institute при присуждении приза GEIT оценил в этом проекте величину коэффициента PUE (для каждого контейнера он составляет всего 1,15) и такой метод улучшения энергоэффективности, как повышение температуры воды в чиллерах с 8 до 18°C.

Обладателем приза GEIT стал также известный дата-центр компании HP в Виньярде (Великобритания), в котором главной экономной технологией выступает фрикулинг. Местный климат позволяет 98% времени в году использовать для охлаждения только внешний воздух. В течение оставшихся 2% времени (чуть более недели в году) этот ЦОД работает от чиллеров. В режиме фрикулинга PUE составляет 1,16, а его среднегодовое значение – 1,2. Примечательно, что стоимость строительства этого ЦОДа составила около $15 тыс. на 1 кВт мощности ИТ-оборудования, что всего на 10% дороже, чем у обычного ЦОДа той же мощности. За первый же год эксплуатации экономия на электроэнергии достигла $4 млн, а в дальнейшем, после выхода на полную мощность, ожидается вдвое большая экономия – $8 млн в год; как результат, срок окупаемости объекта должен составить всего 2 года. Таким образом, этот проект полностью опровергает уже устоявшееся мнение, что технологии энергосбережения при всей своей прогрессивности и экономии на OPEX настолько сильно увеличивают CAPEX, что заметно удлиняют срок окупаемости объекта.

Дата-центр SwitchNAP компании Switch Communications, который расположен в Лас-Вегасе (шт. Невада, США), вышеупомянутой награды Uptime Institute не имеет, зато является исключением из правила несовместимости энергоэффективности и надежности. Как рассказал Алексей Солодовников, руководитель подразделения Schneider Electric Datacenter Solution Team (компания Schneider Electric была поставщиком части оборудования для инженерной инфраструктуры этого ЦОДа), дата-центр SwitchNAP является чемпионом мира по подведенной электрической мощности (250 МВт, при этом выходная мощность ИБП составляет 84 МВт) и по плотности этой мощности в расчете на квадратный метр. Охлаждение этого да-та-центра обеспечивают четыре си-

стемы, которые могут включаться по отдельности и в любой комбинации в зависимости от ситуации за бортом: чил-леры, фреоновая система, система прямого забора внешнего воздуха и теплообменники. Система охлаждения полностью зарезервирована, но это не помешало создателям добиться среднегодового PUE, равного 1,21 (и это в условиях жаркого климата!). Свой вклад в это достижение внесли системы от APC by Schneider Electric – ИБП с КПД, равным 97%, и устройства распределения питания с КПД 98,6%. Особо стоит отметить, что создателям удалось сэкономить не только на OPEX, к которым относятся и счета за электричество, но и на CAPEX: на строительство было потрачено $350 млн, что при выходной мощности ИБП в 84 МВт дает порядка $4200 на 1 кВт (для сравнения: по статистике Uptime Institute, 1 кВт мощности дата-центра уровня Tier III или IV обходится при строительстве более чем в $20 тыс.). При этом SwitchNAP гарантирует своим заказчикам (и это указано в SLA, предусматривающем серьезные штрафные санкции) полностью безотказную работу. Иначе говоря, коэффициент готовности равен 100%(!), тогда как для дата-центра уровня Tier IV он составляет «всего» 99,995%. Для владельцев SwitchNAP это уже седьмой построенный ими дата-центр, так что можно предположить, что ими накоплен немалый опыт, который позволит выдержать заявленный уровень сервиса.

> Надежность требует резервирования, а резервному оборудованию нужно электропитание, поэтому дата-центр уровня Tier III и IV по определению не может иметь рекордно низкого PUE

У нас экологическое сознание пока не овладело широкими массами. По словам Алексея Городецкого, старшего менеджера по развитию бизнеса компании Linxtelecom, имеющей целую сеть географически распределенных дата-центров, клиенты сейчас требуют проверенных решений, поэтому не стоит делать культа из PUE. Тем не менее в последнем дата-центре компании в Петербурге, который скоро должны запустить в тестовую эксплуатацию, использованы и изолированные горячие и холодные коридоры, и чиллеры с фрикулингом. Но дефицит электроэнергии в местах скопления дата-центров (т.е. в Москве) и постоянный рост тарифов на электричество заставляют думать об энергоэффективности и российских владельцев ЦОДов. Конечно, сейчас в России есть немалый спрос на услуги дешевых дата-центров в «базовой комплектации», но в них проблема минимизации энергопотребления решается за счет надежности. Однако на российском рынке уже есть решения, обеспечивающие заданный уровень надежности при ограничениях на электрические мощности и занимаемую площадь и при этом еще позволяющие сэкономить на эксплуатационных расходах.

Экономим с ИБП...

Тем, кто задумал строить серьезный дата-центр с подведенной мощностью более 1 МВт, стоит присмотреться к системам бесперебойного и гарантированного электроснабжения на базе дизельно-роторных ИБП (их еще называют динамическими ИБП). Как считает Рене Лацина, руководитель по международным продажам Hitec Power Protection, при мощностях выше 1 МВ•А динамические ИБП представляют собой самое экономичное и энергоэффективное решение для ЦОДов уровня Tier III и IV. Эта экономичность и энергоэффективность достигается в первую очередь за счет упрощения инфраструктуры дата-центра при использовании таких ИБП. В состав классической системы бесперебойного и гарантированного электропитания должны входить дизель-генераторная установка (ДГУ), электрические фильтры, ИБП, аккумуляторные батареи, система кондиционирования для ИБП, распределительные щиты и система компенсации реактивной мощности. В системе с динамическим ИБП бесперебойное, непрерывное и резервное электроснабжение обеспечивают только ДГУ и электромагнитный накопитель кинетической энергии, реализованные в одном устройстве. Аккумуляторных батарей – одного из серьезных антиэкологических факторов – в них нет. Р. Лацина также подчеркивает простоту конструкции динамического ИБП: «Все его основные элементы – синхронный генератор, ротор накопителя энергии и дизель – собраны на одной раме и соединены простой соосной механической связью. При такой конструкции нет необходимости в преобразовании энергии во внутренних силовых электрических соединениях и в коммутационной аппаратуре. Эта простота дает максимальную надежность, официальный срок службы такой системы составляет 25 лет». Кроме того, для размещения систем электропитания, построенных на базе динамических ИБП, требуется на 40–60% меньше площади, чем для систем со статическими ИБП.

Компания Hitec Power Protection выпускает динамические ИБП в диапазоне мощностей от 500 до 3000 кВ•А и напряжений от 0,4 до 20 кВ, их КПД составляет 97–98%. Такие устройства от Hitec уже используются в целом ряде крупных ЦОДов, в том числе в сертифицированных в Uptime Institute по категориям Tier III и Tier IV. Например, в Великобритании в дата-центре Fujitsu London North, имеющем сертификат Tier III, установлено семь машин мощностью 1670 кВ•А каждая, которые работают на напряжении 11 кВ при частоте 50 Гц. Средний PUE этого ЦОДа составляет 1,27. Есть динамические ИБП от Hitec и в двух дата-центрах, проекты которых сертифицированы на уровень Tier IV, в ОАЭ и в Голландии. По словам Р. Лацины, традиционные решения для систем электропитания этих дата-центров были бы конструктивно более сложными и более дорогими по исполнению.

Но хоронить традиционные системы бесперебойного электропитания конечно же рано. В конце концов даже сам производитель динамических ИБП заявляет об их преимуществах перед традиционными системами лишь при мощностях более 1 МВт. А в России подавляющее большинство составляют сейчас как раз ЦОДы меньшей мощности. Классические системы ИБП с аккумуляторными батареями пока вполне поддаются модернизации и совершенствованию с целью повышения энергоэффективности, снижения общей стоимости владения (TCO) и текущих эксплуатационных расходов. Один из вариантов – использование модульных ИБП, о преимуществах которых на конференции рассказал Иван Мельников, менеджер по развитию бизнеса компании «ЭкоПрог», продвигающей на российский рынок ИБП производства Newave. Даже если брать во внимание только надежность работы системы ИБП (а именно это прежде всего требуется в дата-центре), преимущества модульных ИБП налицо: при равном времени наработки на отказ у одиночных и модульных ИБП время восстановления при выходе из строя у последних существенно меньше (на замену модуля уходит примерно 30 мин, а среднее время восстановления работоспособности одиночного ИБП составляет 6 ч), и за счет этого заметно возрастает уровень готовности всей системы бесперебойного электропитания. CAPEX для модульных ИБП тоже должен быть ниже, так как они имеют вертикальную топологию и по идее занимают меньше места. Что касается энергоэффективности, то и здесь модульные ИБП выигрывают, поскольку имеют существенно более гибкие возможности масштабирования для настройки мощности в соответствии с имеющейся нагрузкой – со всеми вытекающими отсюда последствиями для КПД, который при недозагрузке ИБП, как правило, заметно снижается. Ну, а снижение КПД означает непроизводительный нагрев атмосферы. Таким образом, вывод напрашивается однозначный: модульные ИБП хороши со всех точек зрения, в том числе и из экологических соображений.

Дата-центр HP в Виньярде опровергает устоявшееся мнение, что технологии энергосбережения при всей своей прогрессивности и экономии на OPEX очень сильно увеличивают CAPEX

Справедливости ради стоит отметить, что производителям традиционных ИБП тоже не чужды идеи повышения энергоэффективности и снижения TCO. Во-первых, они уменьшают размеры моноблочных ИБП, которые требуют теперь гораздо меньше места для обслуживания (примерно на 50%). Во-вторых, на рынке уже есть ИБП, КПД которых почти не деградирует при изменении нагрузки в довольно широких пределах. В качестве примера Василий Лапшин, руководитель направления дистрибуции GE DE компании «Абитех», приводит онлайновые ИБП серии SG от General Electric, КПД которых не опускается ниже 94% при нагрузке, варьирующейся в диапазоне от 40 до 80% от максимальной (в ИБП предыдущего поколения КПД не превышал 92%). Кроме того, в системах с параллельным подключением нескольких ИБП применяется технология энергосбережения IEMi, которая при падении нагрузки ниже заданного уровня отключает избыточные ИБП, тем самым повышая нагрузку и соответственно КПД работы оставшихся. Использование на входе ИБП IGBT-выпрямителей тоже снижает энегопотребление. Они вносят существенно меньшие по сравнению с тиристорными выпрямителями гармонические искажения напряжения, а это означает, что нет необходимости сильно завышать мощность ДГУ и непроизводительно тратить электроэнергию и деньги. И еще одна отличительная особенность современных ИБП – возможность эффективной работы и с индуктивной, и с емкостной нагрузкой (а серверы как раз являются емкостной нагрузкой), что также сокращает потери электроэнергии.

... и с системами охлаждения

Сокращение потерь электроэнергии в системах электропитания ЦОДа – это, конечно, важное дело, но на них обычно приходится не более 10% общего энергопотребления современного дата-центра, поэтому гораздо большего эффекта следует ожидать от снижения энегопотребления системы охлаждения, которая в среднем «съедает» около 30% электроэнергии, потребляемой ЦОДом.

Сократить потери можно, например, используя в системах охлаждения предлагаемые компанией Cofely Refrigeration чиллеры Quantum с повышенной энергоэффективностью. Эти чиллеры (с водяным или воздушным охлаждением) продвигает на российский рынок компания «Термокул». Чиллеры Quantum с водяным охлаждением выпускаются в диапазонах мощностей от 250 кВт до 3 МВт и от 2 до 5 МВт, мощность чиллеров с воздушным охлаждением охватывает диапазон от 200 кВт до 1,4 МВт. Сниженное энергопотребление чиллеров Quantum достигается за счет использования центробежных компрессоров Turbocor с магнитными подвесами. Благодаря такой подвеске между движущимися частями компрессора практически нет трения, а, следовательно, и потерь мощности. Эта конструкция позволяет отказаться и от смазки, что добавляет системе экологичности. Еще одним крупным достоинством чиллеров Quantum управляющий директор европейского филиала по строительству заводов компании Cofely Refrigeration Юрген Ферле считает их чрезвычайно высокую эффективность при частичной нагрузке (а именно в таких режимах чаще всего приходится работать холодильным машинам). Кроме того, при запуске чиллера в электрической сети не возникает броска тока, что тоже вносит свой вклад в экономию электроэнергии.

Заметного сокращения энергопотребления системы охлаждения дата-центра (вплоть до 50%) можно до-

биться, используя технологию фрикулинга. Самая распространенная на сегодня реализация этой технологии в мире – чиллеры с системой динамического фрикулинга и турбокомпрессорами. Такие системы охлаждения есть и в российских дата-центрах. При внешней температуре ниже +15°C они работают в режиме фрикулинга, используя холод уличного воздуха или другого природного источника холода, а выше этой температуры включаются чиллеры. Если учесть, что, по статистике, 82% времени в году в средней полосе России температура не поднимается выше +15°C, то экономия электроэнергии может оказаться весьма внушительной, достигая 45% по сравнению с обычными фреоновым DX-системами охлаждения. Но и это не предел. В мире уже разработан целый ряд технологий, позволяющих расширить температурный диапазон применения фрикулинга и таким образом добиться еще большей энергоэффективности систем охлаждения. Например, в упомянутом выше дата-центре SwitchNAP в Лас-Вегасе системы полного фрикулинга работают при температуре за бортом до +24°C, благодаря чему энергопотребление системы охлаждения оказывается на 70% ниже, чем с DX-системами.

Система FFC (Full Freecooling), разработанная российской компанией Ayaks Engineering, работает в режиме фрикулинга до температуры +23°C. Для охлаждения в ней используется внешний приточный воздух и вращающийся регенеративный теплообменник. Максимальная экономия по сравнению с DX-системой составляет 65%. Заместитель коммерческого директора Ayaks Engineering Денис Беляев представил расчеты общей стоимости владения систем охлаждения трех разных типов (DX-система, чиллерная система с динамическим фрикулингом и система FFC) для виртуального дата-центра, в котором общая мощность ИТ-нагрузки составляет 2 МВт. Предполагалось, что во всех трех случаях используется далеко не самое дешевое оборудование: в DX-системе – блоки Emerson L99 (HCE 74), собранные по схеме N+1, в чиллерной системе – чиллеры Emerson SBS063 R407C с внутренними блоками Emerson L10 и резервированием по схеме N+1, в системе FFC (N блоков по 500 кВт) – чиллеры Emerson SBS059. Оказалось, что капитальные затраты на все эти системы отличаются не так уж сильно: система FCC на 6% дороже чиллерной системы с фрикулингом и на 26% дороже DX-системы. Операционные расходы подсчитывались, исходя из цены 1 кВт•ч электроэнергии в 2,9 руб. Здесь самой экономичной оказалась система FCC, эксплуатация чиллерной системы с фрикулингом обошлась на 45% дороже, а OPEX DX-системы – на 64% выше, чем у FCC (только на оплате электроэнергии, по расчетам, экономится более 12 млн руб. в год). Подсчет общей стоимости владения показал, что экономическая выгода установки системы FCC по сравнению с DX-системой становится очевидной уже через 1,2 года (выравнивание с чиллерной системой с фрикулингом достигается через 8 месяцев), а через 5 лет экономия составляет уже 60 млн руб. (разница с чиллерной системой – около 36,6 млн руб.).

Таким образом, начальные вложения в «зеленые» системы фрикулинга оказываются ненамного выше, чем в традиционные системы охлаждения, но их эксплуатация обходится существенно дешевле, что позволяет получить немалый выигрыш в общей стоимости владения.

«Зеленая» защита

«Зеленые» технологии продвигаются в дата-центры и на других фронтах. Дошли они и до систем пожаротушения. В большинстве российских ЦОДов, где есть хоть какие-то системы пожаротушения, стоят баллоны с хладоном, а над дверями можно увидеть грозные табло «газ, выходи!», которые вместе с сиреной должны предупредить персонал об опасности, если система пожаротушения зафиксирует возгорание. Хладон – очень вредное вещество, наверное, даже более опасное для человека, чем сам пожар. Поэтому разработка компанией 3M нового тушащего вещества Novec 1230, безопасного и для человека, и для компьютерного оборудования, и для окружающей среды, было встречено с большим энтузиазмом. При использовании Novec 1230 не выделяется никаких токсичных веществ, а атмосфера в помещении остается пригодной для дыхания. Вот только высокая цена системы пожаротушения с Novec 1230, появившейся на российском рынке около 3 лет назад, довольно долго отпугивала многих потенциальных покупателей. И вот наконец у этой безвредной бесцветной диэлектрической жидкости появились перспективы распространения не только в системах пожаротушения «крутых» банков. По словам Натальи Хазовой, генерального директора компании «Пожтехника», в которой появилась первая в России заправочная станция для систем с 3M Novec 1230, выбор нового экологичного тушащего вещества уже оправдан не только из соображений безопасности, но и с экономической точки зрения. Начальные затраты, конечно, пока заметно выше, чем для систем с хладоном, но затраты на обслуживание оказываются существенно меньше. Кроме того, перезаправку Novec 1230 можно проводить непосредственно на объекте, что с хладоном просто исключено. Стимулировать внедрение новых систем пожаротушения должен и тот факт, что трубопровод хладоновой системы пожаротушения несложно адаптировать для использования жидкости Novec 1230.

Подсчет общей стоимости владения показал, что экономическая выгода установки системы Full Freecooling по сравнению с DX-системой охлаждения становится очевидной уже через 1,2 года

В общем, от пожара внутри защита есть. Правда, как предупреждает генеральный директор ООО «Эксол» Станислав Заржецкий, в 80% случаев пожары возникают не в серверных залах, а в прилегающих помещениях, в связи с чем очень актуальной представляется внешняя защита дата-центра. Причем защита нужна не только от огня, но и от проникновения воды, коррозийных газов, электромагнитного излучения, пыли, падающих обломков и т.п. Самая известная торговая марка на рынке средств физической защиты для ЦОДов – это Lampertz, но на нем есть и другие достойные бренды. Например, в категории средств средней степени защиты по своим параметрам лидирует система ProRZ F90+, а Lampertz занимает второе место. А вот в категории средств максимальной защиты первое место занимает Lampertz/Rittal – LSR 18.6E. Во всяком случае, это единственное по-настоящему модульное решение, которое можно построить без отключения компьютерного и сетевого оборудования.

■ ■ ■

В очень многих странах мира есть законодательные нормы, ограничивающие энергопотребление и стимулирующие внедрение технологий энергосбережения. На первый взгляд, они должны усложнять жизнь владельцев дата-центров. Но стоит признать, что развитие «зеленых» технологий уже дошло до той стадии, когда цена их внедрения не кажется чрезмерной, а их использование порой заметно снижает затраты на эксплуатацию и общую стоимость владения ЦОДом. Из моды на «зеленое» начинают вырастать успешные бизнес-кейсы. Это уже не «от кутюр», а гораздо более практичное «прет-а-порте». ИКС

СХД в эпоху борьбы за эффективность хранения

Евгения ВОЛЫНКИНА

По данным IDC, объем информации, записанной на самые разные компьютерные носители, растет сейчас в мировом масштабе со скоростью 60% в год, а затраты на ее хранение – на 50% в год. Поэтому технологии, которые позволяют повысить эффективность работы систем хранения данных, очень актуальны. Об остроте проблем, стоящих перед производителями СХД, говорят и последние события на этом рынке.

Конец лета – начало осени нынешнего года ознаменовались на рынке СХД короткой, но напряженной борьбой Dell и HP за небольшую (во всяком случае в сравнении с вышеупомянутыми гигантами) компанию 3Par, которая известна специалистам своей предназначенной для дата-центров платформой хранения данных 3Par Utility Storage. Эта платформа построена на базе собственных серверов 3Par, в ней используется фирменная операционная система и разработанная еще в 2002 г. технология Thin Provisioning для динамического выделения приложениям дискового пространства по требованию. Она очень важна для повышения эффективности использования дисковой памяти, виртуализации и модных ныне облачных вычислений. Основное достоинство Thin Provisioning – в более тонкой «нарезке» ресурсов СХД по сравнению с традиционными технологиями, которые выделяют ресурсы с «запасом» в расчете на возможное увеличение потребностей в будущем и, следовательно, требуют более емких и дорогих систем хранения. По заявлению самой компании 3Par, с помощью ее решений капитальные расходы на покупку систем хранения можно сократить на 75%, а затраты на управление и администрирование СХД – аж на 90% (!).

Компании Dell и HP, бившиеся за возможность использовать разработки 3Par в своих продуктах, в пылу борьбы несколько раз поднимали ставки, и в итоге первоначальная цена в $1,15 млрд, предложенная Dell, увеличилась более чем вдвое. Поле битвы осталось за HP, заявившей о готовности заплатить за 3Par $2,35 млрд (и это за компанию, которая имеет годовой доход немногим более $240 млн!). Правда, многие эксперты считают, что цена 3Par явно завышена, несмотря на неоспоримые достоинства технологии Thin Provisioning и на то, что обладание ею может выдвинуть HP в лидеры рынка виртуализированных СХД для систем облачных вычислений (если, конечно, HP в ближайшей перспективе правильно распорядится своим приобретением). В принципе, у HP есть собственная технология того же назначения – HP EVA (Enterprise Virtual Array), которую компания продвигает на рынок крупных корпоративных СХД, но она далеко не столь эффективна, как решение от 3Par. Кроме того, платформа 3Par Utility Storage позволит HP отказаться от использования в своих больших системах класса предприятия СХД производства Hitachi Data Systems (сейчас HP является фактически их реселлером).

От high-end к SMB

Ну а пока HP расширяет ассортимент предлагаемых СХД «снизу»: представленные в этом году системы HP StorageWorks P2000 G3 Modular Smart Array (MSA) и HP StorageWorks P4000 G2 SAN ориентированы на малые и средние предприятия. Можно сказать, что они являются еще одной иллюстрацией уже сформировавшейся традиции переноса функций и возможностей, ранее присущих крупным корпоративным системам, на уровень SMB. Например, стандартной функцией в системе StorageWorks P2000 G3 стала функция репликации данных Remote Snap, позволяющая восстанавливать данные при сбоях. Remote Snap делает мгновенные «снимки» данных и переносит их на второй массив P2000 G3 (так что малому предприятию, желающему обезопасить свои данные, придется раскошелиться и на резервную СХД). В комплект поставки системы также входит специальное ПО Volume Copy, которое автоматически создает локальные копии данных, и лицензия на 64 мгновенных «снимка», что должно гарантировать восстановление данных в случае какой-либо аварии. Набор поддерживаемых интерфейсов тоже как у «больших»: SAS, iSCSI, SATA и Fibre Channel (FC) 8 Гбит/с. Причем в СХД есть комбинированные контроллеры FC/iSCSI Combo, с 8-гигабитными портами FC и гигабитным iSCSI. Опять же по традиции увеличена общая емкость СХД: массив может содержать SAS-диски общей емкостью до 57,6 Тбайт и SATA-диски емкостью до 192 Тбайт.

HP позиционирует СХД StorageWorks P4000 G2 SAN как систему для рынка SMB и при этом заявляет, что с ее помощью можно создавать виртуализованные среды, т.е. вездесущая виртуализация уже дошла и до «низов». Теперь малому и среднему бизнесу предлагаются СХД с избыточными блоками питания и вентиляторами, RAID-массивами, с поддержкой технологий Network RAID 5 и 6, сокращающих объем потребляемой памяти, с интеллектуальным анализатором эффективности использования СХД под названием Best

Practice Analyzer, с функциями удаленного копирования и клонирования приложений и уже упомянутыми возможностями делать мгновенные снимки данных. Трудно сказать, насколько это сейчас актуально для массового малого и среднего бизнеса, но он наверняка оценит возможность наращивать емкость системы хранения с относительно небольшим шагом 12 Тбайт.

Никаких дублей

Кстати, миллиардные покупки компаний на мировом рынке СХД случаются уже не в первый раз. Аналогичная схватка с участием других очень известных участников рынка систем хранения – компаний EMC и NetApp – произошла летом прошлого года. Тогда предметом торга была компания Data Domain, продукция которой олицетворяет другую тенденцию развития современных СХД, а именно использование технологий дедупликации данных. Эти технологии позволяют избавиться от дублирования, порой многократного, одних и тех же данных и существенно сократить не только физический объем корпоративной СХД, но и время, необходимое на создание резервных копий хранимых данных. Дедупликацию сложно назвать новой технологией, она известна довольно давно, но на фоне постоянного снижения цен на дисковые носители и стоимости хранения 1 Гбайт данных компании до поры до времени особенно не беспокоились о хранении избыточной информации и об эффективности использования своих СХД. Но вышеупомянутый 60%-ный рост объема хранимых данных в немалой степени обязан увеличению количества избыточной информации, так как по данным той же компании IDC, около 70% данных дублированы. Затраты на хранение и управление этими огромными массивами информации становятся для компаний довольно чувствительными. Очевидным следствием является заметное повышение ценности дедупликации и спроса на нее. Поэтому «цена вопроса» в споре за разработчика этой технологии оказалась немалой: ставшая победителем компания EMC заплатила за Data Domain $2,1 млрд. Теперь она предлагает СХД, использующие технологии Data Domain, сохранив ее торговую марку.

> Около 70% данных дублированы... Очевидным следствием является заметное повышении ценности дедупликации и спроса на нее

В исполнении EMC дедупликация уже «спустилась» до СХД среднего класса, коей является новая система EMC Data Domain DD670, представленная в июле нынешнего года. DD670 выполняет внутреннюю дедупликацию со скоростью 5,4 Тбайт в час и поддерживает репликацию и автоматическое восстановление данных в случае сбоя в 90 удаленных офисах с помощью систем Data Domain меньших размеров – DD140 или DD610. Конечно, компанию с таким количеством удаленных офисов трудно назвать средней, но базовая модель Data Domain DD670 предназначена именно для таких компаний (ее характеристики: двухстоечное шасси, 12 Тбайт дискового пространства, поддержка модулей расширения с дисками SATA емкостью 1 или 2 Тбайт и уже почти обычный 8-гигабитный интерфейс Fibre Channel). Поставки систем EMC Data Domain DD670 должны начаться в III квартале 2010 г.

Справедливости ради стоит отметить, что проигравшая в тех торгах компания NetApp и без технологий Data Domain очень успешно работает на рынке СХД с дедупликацией. В мае этого года она объявила о том, что стала первым в мире поставщиком, на СХД которого хранится в общей сложности более 1 эксабайта дедуплицированных данных (приблизительно 1 млн Тбайт).

Дедупликацией активно занимается и компания Symantec, которая встроила соответствующие функции в целый ряд своих программных продуктов для защиты, хранения и резервного копирования данных для СХД разных размеров, в частности в NetBackup, Enterprise Vault и Backup Exec. А в начале сентября 2010 г. Symantec анонсировала специальное устройство NetBackup 5000 с предустановленным ПО, позволяющее производить дедупликацию со скоростью 4,3 Гбайт в час. Кроме того, оно предназначено и для репликации данных с диска на диск (и в последнем качестве оно является альтернативой ленточным устройствам резервного копирования данных). Это устройство с резервированием дисковых накопителей по технологии RAID 6 поставляется с дополнительными вентиляторами и источником питания, его емкость в зависимости от конфигурации может варьироваться от 16 до 96 Тбайт. Причем компания Symantec подчеркивает, что не собирается становиться поставщиком «железа» для СХД и по-прежнему остается разработчиком ПО для защиты данных, а NetBackup 5000 – это только ответ на запросы клиентов, которые желают получить продукт, требующий минимальных усилий по его внедрению. Надо полагать, что большинство таких заказчиков составляют компании категории SMB, которые не могут себе позволить лишних затрат на обслуживание систем хранения данных. Для них же предназначено и «облачное» предложение Symantec: в пользовательский интерфейс новых версий ПО резервного копирования NetBackup и Backup Exec включена опция cloud-storage, при выборе которой будет производиться автоматическое подключение корпоративной СХД к облачному распределенному сетевому хранилищу Storage Delivery Network компании Nirvanix.

Курс на SSD

Компания Huawei Symantec, совместное предприятие Huawei Technologies и Symantec, предлагает собственную «облачную» СХД. Причем ее платфор-

Профессиональное оборудование для охранных IP-систем видеонаблюдения

Smartec

STC-IPM3096A

Мегапиксельная 1.3 Mpx IP-камера «день/ночь», 1/3" (ExViewHAD Progressive CCD), M-JPEG/MPEG-4; до 15 fps (1280x960); 0.4лк (цв.), 0.06 лк (ч/б), 0.003 лк (ч/б, Slow Shutter); поддержка SD-карт; 12VDC/24VAC/POE

Весь товар сертифицирован

STC-IPM3095A

Мегапиксельная 1.3 Mpx IP-камера, программный «день/ночь», 1/3" (ExViewHAD Progressive CCD), M-JPEG/MPEG-4; до 15 fps (1280x960); 0.4 лк (цв.), 0.02 лк (ч/б, Slow Shutter); поддержка SD-карт; 12VDC/24VAC/POE

STC-IPM3595A

Мегапиксельная 1.3 Mpx IP-камера купольного типа, программный «день/ночь», 1/3" (ExViewHAD Progressive CCD), M-JPEG/MPEG-4; до 15 fps (1280x960); объектив 2.7-9 мм с АРД; 0.4 лк (цв.), 0.02 лк (ч/б, Slow Shutter); поддержка SD-карт; 12VDC/24VAC/POE

STC-IPX3062A (с видеоаналитикой VCA)

IP-камера «день-ночь» с режимом WDR, 1/3" (Sony Double Scan CCD), H.264/MPEG-4/M-JPEG (2-потоковая передача); 25 fps (720x576); 0.3лк (цв.)/0.002лк (ч/б, Slow Shutter); слот для SD-карт; 12VDC/POE

STC-IPX3562A (с видеоаналитикой VCA)

Купольная вандалозащищенная IP-камера«день-ночь» с режимом WDR, 1/3" (Sony Double Scan CCD), H.264/MPEG-4/M-JPEG (2-потоковая передача); 25 fps (720x576); 0.3лк (цв.)/0.002лк (ч/б, Slow Shutter); слот для SD-карт; 12VDC/POE

NetStation

ПО сетевой записи/наблюдения для IP-камер Smartec, Axis, Sanyo, Pelco, JVC, Arecont Vision и др.; до 64 каналов на один сервер. Поддержка мультисерверных и гибридных конфигураций, карт объекта. Клиентское ПО для PC, КПК и смартфонов

реклама

- Всегда на московском складе
- Программа развития дилеров
- Инструкции на русском языке
- Техническая поддержка
- Гарантийные/сервисные услуги

армо-системы
www.armosystems.ru

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

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

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

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

ме облачного хранения Oceanspace T3000, выпущенной в 2009 г., недавно пришло на смену второе поколение в виде систем T3200 и T3500 G2. Предназначаются они для дата-центров, в которых вопрос снижения энергопотребления стоит очень остро, поэтому в системах Oceanspace используются разнообразные технологии энергосбережения, в том числе плавный запуск жестких дисков, автоматическое повышение и понижение скорости их вращения в зависимости от нагрузки, регулировка скорости вращения вентиляторов в зависимости от окружающей температуры, использование твердотельных накопителей (SSD) и процессоров с низким энергопотреблением и др. Правда, пока в системах T3200 и T3500 G2 поддерживается установка только двух SSD-накопителей емкостью 100 или 200 Гбайт каждый, а основной объем хранения обеспечивают обычные жесткие диски с интерфейсами SATA емкостью 1 или 2 Тбайт каждый или SAS (от 300 до 600 Гбайт), и таких жестких дисков в СХД T3200 установлено 12 шт., а в системе T3500 G2 – 24 шт. В итоге при установке только однотерабайтных дисков в режиме ожидания энергопотребление у обеих СХД составляет 50 Вт, а в рабочем режиме соответственно 260 и 360 Вт.

Но конечно же SSD-накопители устанавливаются в современные системы хранения данных не столько ради снижения энергопотребления, сколько для ускорения доступа к тем данным, к которым часто приходится обращаться (у современных SSD скорость чтения составляет порядка 250 Мбайт/с). Поэтому SSD-накопители присутствуют сейчас во всех современных СХД корпоративного класса с многоуровневой архитектурой хранения. Хранение данных даже на очень дорогих SSD-накопителях вполне экономически оправдано в приложениях, критичных к скорости выполнения операций ввода-вывода. Но, как правило, в корпоративных информационных системах работают и другие приложения, менее или вовсе не требовательные к скорости чтения/записи данных. На них рассчитаны СХД типа предлагаемой IBM дисковой системы DS8700. Для организации многоуровневого управления данными в ней используется технология IBM System Storage Easy Tier. Она позволяет автоматически вести непрерывный мониторинг работы СХД, перемещать данные повышенного спроса на более быстрые SSD-носители, а остальные отправлять на традиционные жесткие диски с интерфейсами Fiber Channel или SATA (в зависимости опять же от спроса на эти данные).

Тенденции те же

По оценке IDC, лидером по поставкам внешних СХД в Россию сейчас является компания EMC, ее доля составляет 38%, второе место с 22% рынка – у HP. Вообще же российский рынок систем хранения, как и весь ИТ-рынок, постепенно оправляется от кризиса, но его рост пока далек от поступательного. По данным той же IDC, объем продаж СХД в I квартале 2010 г. составил немногим более $48 млн, что на 60% больше, чем за аналогичный период прошлого года, хотя и на 35% меньше, чем в IV квартале 2009 г. Если исходить из этих показателей, то рост объема рынка за год должен составить 103%. Цифра весьма внушительная, если учесть, что компании стали гораздо более осторожно подходить к выбору любых ИТ-решений. Правда, в списке требований к СХД первым пунктом уже не всегда стоит цена. Заказчиков все чаще интересуют срок возврата инвестиций, общая стоимость владения, совместимость с имеющимся оборудованием, скорость доступа и безопасность данных.

Российским производителям СХД, конечно, сложно тягаться с мировыми грандами в секторе корпоративных систем высшего класса, они работают для тех заказчиков, для которых основным критерием при выборе любого компьютерного оборудования является как раз цена, т.е. для малых и средних компаний. Но тут наши производители не отстают от мировых тенденций, предлагая технологии, уже спустившиеся в нижний и средний ценовой сегмент. Например, компания DEPO Computers в этом году представила комплексные решения для систем распределенного хранения данных, поддерживающих возможность их использования вместе с системами виртуализации от VMware и Microsoft. Они построены на базе серверов DEPO Storm и СХД DEPO Storage Server с применением разных технологий репликации (синхронной и асинхронной, блочной и файловой, а также – в качестве адаптации к российским реалиям – репликации с использованием медленных беспроводных каналов связи). Старшая модель этой СХД DEPO Storage Server 3124 допускает установку до 24 жестких дисков с интерфейсом SAS или SATA. В «средне-тяжелых» СХД DEPO Storage 5000 теперь есть 8-гигабитные интерфейсы Fiber Channel, а двухтерабайтные SATA-диски устанавливаются не только в старшие модели СХД DEPO Storage, но и в те линейки, что предназначаются для небольших компаний, рабочих групп и даже для персонального использования (DEPO Storage 1004). В качестве следующего шага, наверное, стоит ожидать появления SSD-накопителей. Хотя их стоимость в расчете на 1 Гбайт емкости снижается далеко не так быстро, как у традиционных жестких дисков, и даже через пару лет их цены, по прогнозам, будут различаться на порядок, но спрос на приложения, требующие высоких скоростей чтения/записи данных, явно будет способствовать распространению SSD-носителей. ИКС

Хранение данных даже на очень дорогих SSD-накопителях вполне экономически оправдано в приложениях, критичных к скорости выполнения операций ввода-вывода

DEPO Storage 6000

DEPO computers

Решения для создания сетей хранения данных масштаба предприятия

DEPO Storage 6312 – система хранения данных начального уровня

- Интерфейсы FC, iSCSI
- Макс. дисковая емкость 96 Тб
- 2 контроллера, кэш (на контроллер/на систему) – 4Гб/8Гб
- Порты передачи данных,варианты: 8x4Гб FC, 4x12Гб SAS, 8xGE iSCSI, 4x4Гб FC + 4xGE iSCSI

от 350 000 руб.

DEPO Storage 6324 – система хранения данных среднего уровня

- Интерфейсы FC, iSCSI
- Макс. дисковая емкость 480 Тб
- 2 контроллера, кэш (на контроллер/на систему) – от 4 до 16Гб/от 8 до 32Гб
- Порты передачи данных,варианты: 12x8 Гбит/с FC, 4x8 Гбит/с FC + 4x10 Гбит/с iSCSI

от 477 000 руб.

DEPO Storage 6600 VIS – отказоустойчивый контроллер виртуальной SAN

- Интерфейсы FC, iSCSI
- Интеграция СХД различных производителей в единую SAN
- Сервисы репликации данных как внутри SAN, так и в удаленном ЦОД

от 3 611 000 руб.

Новая линейка продуктов DEPO Storage 6000 включает системы хранения данных и специальное оборудование для виртуализации, позволяющее интегрировать различные устройства хранения данных, упростить управление и построить многоуровневые системы резервирования. Централизованная архитектура хранения и рациональное использование ресурсов снижают общую стоимость владения.

Модели линейки DEPO Storage 6000 могут быть приобретены как отдельными позициями, так и в составе комплексных решений DEPO, включая услуги по установке и настройке оборудования.

Компания DEPO Computers
комплексные IT-решения • системная интеграция • компьютерные системы
тел. (495) 969-22-22, www.depocomputers.ru

Товар сертифицирован. Реклама

МЫ ИХ СДЕЛАЛИ! ДЛЯ ВАС!

Переход к IPv6: сегодня – рано, завтра – поздно?

Евгения ШУМИЛОВА, эксперт отдела технического консалтинга компании АМТ-ГРУП

Большинство экспертов сходится во мнении, что свободные адреса в рамках протокола IPv4, имеющиеся в распоряжении IANA, закончатся в середине 2011 г., у региональных интернет-регистраторов – в 2012 г. Лекарство от этой «болезни» известно – переход на IPv6. Но когда именно и как оператор связи должен осуществить переход на новый протокол?

По результатам опроса 31 интернет-провайдера разных сегментов рынка* на предмет готовности к повсеместному внедрению IPv6 выяснилось следующее: большая часть провайдеров склоняется к мнению, что их адреса, предназначенные для самой сети и ее обслуживания, закончатся, возможно, году к 2020-му или позже, так как многие используют для своей сети не более 1% адресов. А вот исчерпать запасы адресов IPv4 для клиентов основная масса провайдеров собирается до 2015 г. Единого для всех операторов «Дня Икс», конечно, не будет, размеры блоков адресов у всех разные, да и темпы прироста клиентов сильно отличаются, но мысль, что адреса закончатся, в среде интернет-провайдеров уже укоренилась.

Есть ли реальные драйверы для IPv6?

Для пользователей огромным стимулом к переходу на IPv6 послужило бы наличие интересных сервисов на основе IPv6 и конкурентоспособные цены на них. С точки зрения контент-провайдеров стимулом являются огромные массы пользователей, имеющих подключение по IPv6 и готовых потреблять IPv6-сервисы. Налицо ситуация «Курица или яйцо?»: пока контент-провайдеры ждут появления пользователей, заинтересованных в IPv6, потребители телекоммуникационных услуг (домашние, мобильные, бизнес-пользователи, госструктуры, M2M) ожидают появления IPv6-контента.

До некоторой степени увеличению IPv6-трафика способствуют правительственные и национальные программы. К ним относятся принятая в 2008 г. правительством США программа, требующая от всех федеральных агентств обеспечить в своих сетях поддержку IPv6, а также тестирование и исследования под эгидой NIST в США и Китае, программа планирования масштабного внедрения IPv6 в Европе (i2010), соответствующие программы в Малайзии, Японии и других странах.

Рассуждать на тему, кто должен проявить инициативу, можно сколь угодно долго. При этом процесс уменьшения количества свободных адресов IPv4 не останавливается ни на минуту, и в первую очередь операторам связи придется так или иначе справляться с этой проблемой. Первый вариант – выдавать адреса только при крайней необходимости. Но это и так давно принятая практика, и она не меняет кардинально общую картину. Второй вариант – развивать всевозможные механизмы трансляции (NAT44, NAT444 и пр.), но этот метод далеко не всегда оптимален. Он требует немалых затрат на дополнительное оборудование, внедрение трансляторов и т.д., но не ведет к увеличению доли трафика IPv6 в Сети.

Одним из стимулов третьего варианта – внедрения IPv6 – для оператора может стать экономия на IPv4-трансляции в обозримом будущем. Рост скоростей неминуемо приведет к росту стоимости электронной коммутации и в большей степени электронной обработки данных (NAT, DPI). В случае пакетной коммутации намечается долгосрочный тренд уменьшения количества узлов электронной коммутации и применения оптической коммутации, в перспективе очевидным представляется исключение трансляции как таковой. Рано или поздно затраты на трансляцию превысят затраты на внедрение IPv6 (так, в случае NAT444 количество последовательных трансляций увеличивается до двух, не считая трансляции на стороне абонента). Этот момент времени для каждого оператора свой и зависит от множества факторов, включая темпы роста абонентской базы, скоростей и доли IPv6-трафика.

IPv6 в действии

Одна из областей, где IPv6 более эффективен, чем IPv4, – сенсорные сети (беспроводные сети, состоящие из распределенных автономных устройств и подключенных к ним датчиков для мониторинга физических и экологических условий). Пример такой сети – 6lowpan, взаимодействие по IPv6 поверх маломощных беспроводных сетей стандарта IEEE 802.15.4.

Интересна программа правительства по распространению IPv6 в Японии, где для мониторинга температуры коров развернута пилотная сеть. Животных снабжают специальным чипом, в результате чего каждая корова имеет свой IPv6-адрес. В городе Нагоя IPv6 применяется в сенсорной сети датчиков на стеклах такси. Датчики передают информацию о скорости движения дворников автомобилей на сервер, и в те районы города, где идет дождь, направляются дополнительные машины.

* Emerging Service Provider Scenarios for IPv6 Deployment (draft-ietf-v6ops-isp-scenarios-00). https://datatracker.ietf.org.

Проблемы внедрения

Внедрение IPv6 или, тем более полный переход на IPv6, осуществляется, конечно, не за день и не за год. С его внедрением у большинства конечных пользователей, подключенных по IPv6, с доступом к нативному IPv6-контенту проблем не будет, а вот обеспечение доступа к IPv4-контенту потребует некоторых усилий со стороны операторов.

Операторы крупных сетей сталкиваются в процессе перехода с довольно серьезными проблемами. «Масштаб бедствия» для них не ограничивается модернизацией самой сети, при переходе так или иначе будут затронуты все подсистемы. Внедрение нового протокола влечет за собой неизбежную модернизацию системы и политик безопасности – в IPv6 добавляются новые возможности, а вместе с ними, соответственно, появляются новые уязвимости. Система управления и биллинга должна быть готова к поддержке IPv6 на всех уровнях для обеспечения мониторинга, сбора статистики, учета трафика и проч. Необходимая доступность сети должна быть поддержана созданием отказоустойчивого решения: защита от всевозможных отказов IPv6-сегмента сети, варианты доступности ресурсов по IPv4. Полноценное внедрение протокола не может происходить без адаптированных систем СОРМ, IDS/IPS, DPI, инфраструктурных DNS, DHCP и др.

Таким образом, интернет-операторы tier-1 рассматривают вторжение IPv6 в свою сеть осторожно, осознавая связанные с переходом проблемы: чем больше сеть, тем они серьезнее. Для подготовки к внедрению IPv6 им требуется множество мероприятий, аудитов и обследований, а также долгосрочное планирование мероприятий, модернизация существующих и закупка дополнительных ПО и оборудования, обучение большого количества персонала, ведение проекта со всеми его затратами на разработку и осуществление. Всё это означает инвестиции внушительных размеров, которые не являются краткосрочно прибыльными.

У небольших сервис-провайдеров (до 10 тыс. абонентов) трудности при внедрении невелики: обучение персонала, организация пиринга по IPv6 с соседями, модернизация ПО и оборудования (хотя зачастую уже всё IPv6-ready) – затраты минимальны. У таких сервис-провайдеров IPv6 зачастую уже внедрен, и даже не по инициативе руководства, а силами самого персонала из академического интереса.

В наименее выгодном положении находятся сервис-провайдеры среднего размера. С одной стороны, поджимает постоянно увеличивающееся количество домашних абонентов, а с другой – количество свободных адресов всё уменьшается и уменьшается.

А как внедрять?

Внедрение IPv6 представляет собой процесс, который согласно RFC5211 условно делится на три этапа. На первом этапе интернет-провайдеры должны подготавливать свою сеть и инфраструктуру к внедрению IPv6, разворачивать пилотные зоны и предоставлять желающим клиентам тестирование (возможно, некоммерческое) новых услуг. У многих провайдеров интернет-услуг на данный момент нет возможности тратить время на пилотирование. Адреса заканчиваются слишком быстро, потребности клиентов растут, и очевидно, что для многих время первого этапа уже прошло.

Второй этап подразумевает активное внедрение IPv6 в широкие массы. И если провайдер, до сих пор не задумавшийся о переходе на новый протокол, спросит, когда же внедрять, то ответом будет: «Сейчас!». Сейчас самое время заняться предоставлением коммерческой услуги IPv6 для всех категорий абонентов.

Третий этап – тотальное внедрение, при котором подавляющее большинство новых пользователей будет подключено по IPv6, почти все сервисы будут адаптированы под новый протокол, а количество IPv4-пользователей и сервисов будет стремительно уменьшаться. Но до этого пройдет еще немало лет.

Стратегия – способ достижения сложной цели

Для сети оператора переход на новый протокол – длительный и ресурсоемкий процесс, и поэтому для перехода на IPv6 рекомендовалось проведение предварительного тестирования. Но сегодня широкомасштабное и длительное тестирование уже невозможно для тех операторов, которые стоят перед необходимостью предоставлять услугу в ближайшем будущем (например, в следующем году). Для компенсации отсутствия первого этапа могут быть проведены испытания в рамках тестирования по проекту внедрения.

Ключевым моментом в проекте внедрения, безусловно, является планирование. На данном этапе определяются важнейшие стратегические задачи, унифицируются методы и подходы, используемые на протяжении всего проекта внедрения, вырабатываются технические решения по распределению адресного пространства, взаимодействию IPv4- и IPv6-ресурсов, адаптации затрагиваемых систем и подсистем, как инфраструктурных, так и сервисных. Поскольку модернизация сети, сервисов и связанных подсистем не может быть произведена одномоментно, один из наиболее важных моментов – проработка этапности внедрения. Этот процесс индивидуален для сети каждого оператора.

АМТ-ГРУП использует передовые мировые практики в области внедрения IPv6 при разработке и реализации проектов на сетях операторов связи разного масштаба. Высокопрофессиональный и детальный подход команды специалистов позволяет всесторонне изучить все затрагиваемые внедрением IPv6 процессы, осуществить стратегическое планирование и внедрение в соответствии с современными требованиями к телекоммуникационным сетям.

Лёд тронулся!

Процесс перехода на IPv6 набирает обороты, и его, похоже, не остановить. Операторы готовят свои сети к коммерческой эксплуатации IPv6 в ближайшие годы, а десятки провайдеров во всем мире уже предоставляют IPv6-сервисы тысячам домашних пользователей и бизнес-абонентам. Главное – не опоздать!

Защитные оболочки ЦОДов
Необходимый элемент инфраструктуры

Александр ЖАК,
технический директор
компании «ДатаДом»

Требования к надежности и бесперебойности функционирования ЦОДов непрерывно растут. Добиться уровня доступности, соответствующего Tier III (незапланированные простои – в среднем 1,6 часа в год, доступность – 99,98%) и тем более Tier IV можно только при обеспечении должной физической защиты оборудования дата-центра от внешних неблагоприятных факторов. Именно для этого ЦОДам и нужны защитные оболочки.

Из всех возможных неблагоприятных факторов, воздействующих на ЦОД, самый опасный и тяжелый по последствиям – внешний пожар. А с учетом наших российских особенностей и менталитета он опасен вдвойне. Подробнее неблагоприятные воздействия, которые необходимо учитывать при устройстве защитных оболочек (ЗО), описаны в статье С. Заржецкого «Огонь, вода и коррозийный газ. Угрозы физической безопасности ЦОДа» («ИКС» № 3'2010, с. 85–87).

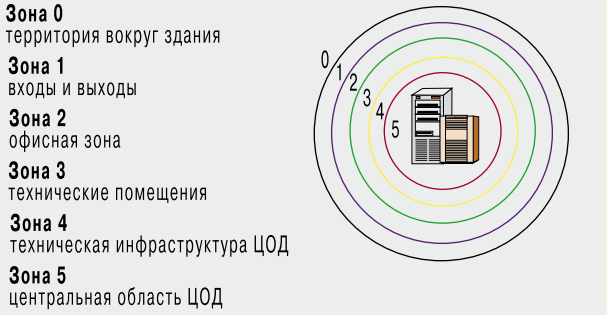
Еще одна важная функция ЗО – физическое разграничение зон ответственности ЦОДа. Российские нормативные документы – ВНП 001-01/Банк России, РД 78.36.003-2002/МВД России – определяют минимум три зоны ответственности на объектах категории А (ЦОД в целом – подгруппа AI, серверное помещение, машинный зал – подгруппа AII). За рубежом, в частности в Германии, практикуется и более жесткий подход с большим количеством зон (рис. 1).

Договоримся о терминах

Центр обработки данных (дата-центр, ЦОД) – совокупность спланированных определенным образом территорий, внешних площадок (анклавов), строений, помещений, с установленными инженерными системами обеспечения и обслуживающим персоналом, образующих общее физическое пространство и технологическую среду для размещения компьютеров, электронных и иных средств приема, передачи, обработки, хранения информации и обеспечивающих заданную степень доступности (готовности) размещенного оборудования в заданном режиме функционирования.

Защитная оболочка (ЗО, IT security room) – специально проектируемое и устанавливаемое помещение, предназначенное для размещения, функционирования и хранения электронного оборудования и носителей информации в заранее определенных условиях и технологических режимах, обеспечивающее защиту содержимого от заранее определенных неблагоприятных воздействий в режиме 24 ч в сутки, 7 дней в неделю, 365 дней в году.

Рис. 1. Зоны ответственности ЦОДа



Источник: Информационный центр IZB

Краткая история

Понятие «защитная оболочка» появилось в середине 70-х годов 20-го века. До начала 80-х гг. ЗО создавались на основе технологий построения банковских хранилищ, в основном из сталефибробетона, что было дорого и далеко не всегда оправдано экономически. Такие ЗО использовались, как правило, силовыми ведомствами и крупными государственными учреждениями.

Впервые в Европе ЗО, изготовленную из специальных материалов и предназначенную для физической защиты содержимого от неблагоприятных внешних факторов, спроектировала и в 1982 г. установила немецкая фирма Lampertz GmbH & Co. KG, входящая в концерн Friedhelm Loh Group и занимавшая к тому времени лидирующие позиции в производстве сейфов для носителей информации. Первоначально защитные оболочки предполагалось размещать исключительно внутри здания; значительно позднее, уже в нашем веке, появились решения, которые позволяют возводить ЗО под открытым небом.

Первая ЗО была модульной, но сварной конструкцией, в отличие сборно-разборных ЗО, выпускаемых фирмой с 1987 г. Таких защитных оболочек было создано порядка пяти-шести единиц.

Параллельно разработки в этой области вела компания Firelock Fireproof Modular Vaults (США). В 1986 г. она установила первую ЗО в Америке. Это была модульная сборно-разборная конструкция.

В 1987 г. фирма Lampertz инсталлировала свою первую полностью модульную ЗО сборно-разборной масштабируемой конструкции.

Основные игроки рынка ЗО

Наименование фирмы, страна	Что производит и продает
Adolphs Ageless Safes GmbH, Германия	Сварные сейфы для оборудования и носителей информации
Brodinger IT Sicherheitstechnik, Австрия	Каркасные неразборные модульные ЗО, сварные контейнеры ЗО наружного исполнения
Firelock Fireproof Modular Vaults, США	Бескаркасные сборно-разборные модульные масштабируемые ЗО
Lampertz GmbH & Co. KG, Германия	Бескаркасные сборно-разборные модульные масштабируемые ЗО, модульные и сварные сейфы для оборудования и носителей информации, сварные контейнеры ЗО наружного исполнения
MS Protect AG, Швейцария	Бескаркасные неразборные модульные ЗО
PriorIT AG, Германия	Каркасные и бескаркасные сборно-разборные модульные масштабируемые ЗО, элементы ЗО (двери, люки, клапаны, кабельные вводы, кабельные каналы)
proRZ Rechenzentrumsbau GmbH, Германия	Бескаркасные сборно-разборные модульные масштабируемые ЗО, модульные сейфы для оборудования, контейнеры ЗО наружного исполнения
RemTech Limited, Англия	Бескаркасные сборно-разборные модульные масштабируемые ЗО, элементы ЗО (двери, люки, клапаны)
SecuraCorp International Pty. Ltd., Австралия	Каркасные неразборные модульные ЗО, элементы ЗО (замки, электронные системы)
Sistemas Mecánicos para Electrónica,S.A. (SME), Испания	Каркасные неразборные модульные ЗО, сварные сейфы для оборудования и носителей информации

На российском рынке работают фирмы Lampertz, RemTech Limited и SME.

Технология и материалы

Опыт работы компании «ДатаДом» показывает, что применение в качестве строительного материала ЗО бетона, кирпича и гипсокартонных листов во всех случаях нецелесообразно, а в большинстве случаев – недопустимо (подробнее см., в частности, вышеупомянутую статью С. Заржецкого).

До появления первых защитных оболочек для защиты от пожара, воздействия высоких и низких температур использовались материалы разной степени горючести с низким коэффициентом теплопроводности – пакля, минеральная вата, вермикулит, пенополиуретан и др. Вначале они служили заполнителями межстеночных пустот в готовом помещении. Потом стало очевидно, что если заключить наполнитель в каркас из тонкого листового металла, получится панель (сэндвич), которую можно применять как самостоятельный строительный элемент.

Первыми изготавливать и применять теплоизолирующие сэндвич-панели в качестве конструкционных элементов помещений (стены, потолок, пол) начали компании, строящие промышленные здания-холодильники долгосрочного хранения.

В настоящее время разработаны специальные негорючие материалы с теплопроводностью в 2–2,5 раза ниже, чем у пенополиуретана, не выделяющие газов и жидкостей в виде пара при их нагревании (например, PYROFOAM, используемый в сэндвич-панелях RemTech Limited).

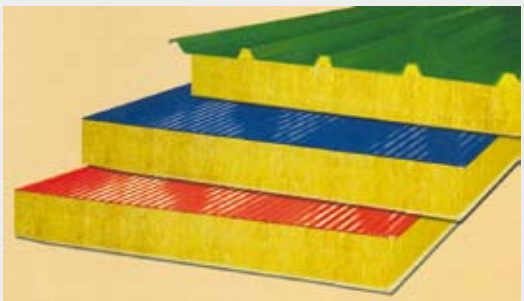
Наиболее подходящим строительным материалом для ЗО являются специальные многослойные панели с различными наполнителями. Сертифицированные по нормам ИТ-безопасности ГОСТ Р 52919-2008 (DIN 1047-2-2000) «Информационная технология. Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость. Комнаты и контейнеры данных» помещения из такого сорта импортных панелей (например, производства Lampertz), а также отдельные сертифицированные панели и элементы помещения (например, продукция RemTech Limited) имеют отличные эксплуатационные характеристики, но достаточно дороги.

Российская промышленность также выпускает многослойные панели различного (в основном общестроительного) назначения. Эти панели значительно дешевле, чем зарубежные аналоги, но они не сертифицированы по ГОСТ Р 52919-2008 и не обладают необходимой прочностью для защиты от «силовых» воздействий (взлома, обрушения, взрыва, стрельбы).

Кроме того, согласно общестроительному нормативу ГОСТ 30247.0-94 (ИСО 834-75) при воздействии на внешнюю поверхность компьютерного помещения температуры в 945°С температура в 140°С на внутренней необогреваемой поверхности считается допустимой. Относительная влажность в помещении при этом не нормируется.

Рис. 2. Примеры сэндвич-панелей

Сэндвич-панели TRIMO (Россия)



Сэндвич-панели «Венталл» (Россия)

Нормы ИТ-безопасности существенно жестче: при воздействии на внешнюю поверхность компьютерной комнаты температуры в 945°С ГОСТ Р 52919-2008 в качестве допустимой для внутренней необогреваемой поверхности называет температуру в 50°С при относительной влажности не более 85%.

Поэтому для использования тех или иных строительных материалов в создании защитной оболочки ЦОДа наличия одного российского общестроительного сертификата пожарной безопасности недостаточно. Обязательна сертификация по ГОСТ Р 52919-2008 или аналогичным стандартам. Причем выбранный материал оболочки-саркофага ЗО должен обеспечивать соблюдение внутри помещения тепловлажностных характеристик в соответствии с ГОСТ Р 52919-2008 при внешнем воздействии на оболочку пожара с температурой 945 °С в течение 30 мин (предпочтительнее – 60 мин).

Правильно спроектированная и инсталлированная ЗО должна, как минимум, включать в себя:

- герметичное масштабируемое помещение;
- систему экранирования помещения («клетка Фарадея»);
- систему электронного контроля параметров помещения;
- систему основного и аварийного освещения;
- автоматическую дверь с электронным и механическим замками;
- автоматический люк регулирования давления в гермозоне при срабатывании системы газового пожаротушения;
- автоматический люк забора внешнего воздуха;
- систему газодымоудаления из гермозоны;
- систему герметичных огнеупорных муфт и кабельных вводов.

По опыту компании «ДатаДом» для создания защитных оболочек в российских условиях наиболее подходит продукция следующих фирм-производителей (в порядке убывания цены и качества):

- Lampertz – ЗО, контейнеры, сейфы;
- RemTech Limited – ЗО;
- TRIMO – строительные трехслойные панели;
- «Венталл» – строительные трехслойные панели.

Сейфы для защиты оборудования, данных и носителей информации

Для небольших объектов (одна-две стандартные 19-дюймовые стойки) используются специальные аппаратные сейфы, обеспечивающие необходимые параметры защиты и функционирования установленных в них стоек с оборудованием.

В качестве примера можно привести аппаратные модульные и сварные сейфы фирм Lampertz, proRZ Rechenzentrumsbau GmbH и Adolphs Ageless Safes, оснащенные всеми системами жизнеобеспечения и обла-

Не забывайте о физической безопасности ЦОДов!

Станислав ЗАРЖЕЦКИЙ,
генеральный директор
ООО «Эксол»

Изложенная автором информация для российского рынка строительства ЦОДов очень важна. Хочется сказать Александру Жаку отдельное СПАСИБО за созданный им труд «ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ВЫБОРУ И СТРОИТЕЛЬНОЙ ПОДГОТОВКЕ ТЕРРИТОРИИ И ПОМЕЩЕНИЙ ДЛЯ ЦЕНТРА ОБРАБОТКИ ДАННЫХ (ЦОД)». Автору удалось собрать воедино огромное количество разрозненной информации, проанализировать ее и привести к стройной структуре, позволяющей читателю четко уяснить основные требования и условия, необходимые для построения ЦОДа. Ранее мне не встречался труд такого уровня содержательности и целостности. Хотя подобная работа была необходима рынку, поскольку интерес к построению ЦОДов возник у заказчиков достаточно давно, но до сих пор, по сути, не было систематического представления о том, КАК это нужно делать, чтобы получить в результате надежно защищенный от неблагоприятных внешних воздействий дата-центр.

В данной статье Александр снова обращается к вопросам создания защитных оболочек для ЦОДов. Приятно, что автор дает весьма полный обзор решений, не концентрируясь при этом на тех или иных производителях. Независимый обзор нужен сегодня нашим ИТ-интеграторам для того, чтобы видеть реальную ситуацию на рынке такого рода решений.

Касаясь рисков, которые могут в той или иной степени нарушить бесперебойную работу ЦОДа, автор совершенно справедливо подчеркивает необходимость обращать на физическую безопасность дата-центров самое пристальное внимание.

Компания «Эксол» уже много лет работает в области решений по обеспечению физической безопасности ЦОДов. Мы хорошо знаем тенденции рынка нашей страны в этом направлении. Исходя из своего опыта, мы можем сказать, что значимость труда Александра Жака трудно переоценить.

дающие такими же характеристиками физической защиты, как и более масштабные решения.

Для хранения особо важных документов и носителей информации служат специальные герметичные сейфы, гарантирующие полную сохранность данных и физических носителей, в том числе бумажных, при пожаре пятой категории.

Характеристики и конструктивные особенности различных защитных оболочек ЦОДов

Сэндвич-панели, из которых монтируются защитные оболочки, у разных производителей обладают разными защитными и эксплуатационными характеристиками. Посмотрим, какие решения доступны в России.

Самые качественные и дорогие изделия из представленных на российском рынке принадлежат фирме Lampertz. Они обеспечивают защиту почти от всех видов угроз, включая взрывы в непосредственной близости от ЗО и стрельбу из стрелкового оружия в стены и в потолок практически в упор. Пожаростойкость по ГОСТ Р 52919-2008 – до 180 мин, степень защиты по ГОСТ 14254-96 (МЭК 529-89) – IP56. В качестве последнего штриха можно добавить, что эти решения еще и бескаркасные. К недостаткам таких ЗО, по мнению автора, относятся большой удельный вес панелей, достигающий 60 кг/м², и как следствие – невозможность ручного монтажа панелей без подъемных приспособлений и высокая стоимость. Высота стеновых и длина потолочных панелей – 2350–3500 мм, ширина – 600 мм (или по заказу – 1200 мм для «легких» решений), толщина – 100–120 мм, удельный вес – 20–60 кг/м² в зависимости от степени защищенности. Защитные оболочки помещений, у которых и длина, и ширина превышают 3500 мм, нуждаются во внутренних стойках-опорах. Для своих решений Lampertz выпускает полный набор необходимых элементов – двери с автоматическими доводчиками, замки, автоматические люки забора воздуха, сброса давления и дымоудаления, систему освещения, автоматику СКУД и реакции на нештатные ситуации. Для организации кабельных вводов используются элементы от сторонних производителей.

Более дешевые решения фирмы RemTech Limited создаются на основе сертифицированных по пожарным ИТ-нормам сэндвич-панелей с наполнителем из специального полимера. Пожаростойкость по ГОСТ Р 52919-2008 – до 90 мин, степень защиты по ГОСТ 14254-96 – IP56. Защитная оболочка конструктивно бескаркасная. Базовое решение обеспечивает защиту от пожара и некоторую (невысокую) взломостойкость, впрочем, несколько более высокую, чем у российских панелей. Специальные исполнения имеют высокую взломостойкость при сохранении всех остальных параметров. Взрывозащищенностью и пулестойкостью панели, в том числе специального исполнения, не обладают. Длина стеновых и потолочных панелей – до 6000 мм при стандартной ширине 1140 мм (ширина

может быть меньше), толщина – 100 мм. Панели базового решения допускают возможность резки прямо на месте монтажа общестроительным инструментом. Удельный вес панели базового решения около 22 кг/м². Панели специального исполнения армированы изнутри профилированной мелкоячеистой стальной решеткой. Резать такую панель также можно на месте монтажа, но только специальным инструментом и с малой скоростью. Удельный вес панели специального исполнения около 26 кг/м². Для устройства ЗО шириной более 6000 мм используют либо внутренние стойки-опоры, либо специальный подвес к верхнему перекрытию, на который опирается стык торцов двух потолочных панелей. Из фирменных элементов предлагаются автоматические люки забора воздуха, сброса давления и дымоудаления, остальные элементы от – сторонних производителей.

Самые недорогие решения – ЗО из российских общестроительных сэндвич-панелей производства TRIMO или «Венталл» с наполнителем из минеральной ваты на предварительно смонтированом каркасе из стальных труб квадратного сечения. Они не имеют сертификации ни в отношении пожаростойкости (по ГОСТ Р 52919-2008), ни в отношении степени защиты, обеспечиваемой оболочками (по ГОСТ 14254-96). На их основе принципиально невозможно сделать взломозащищенную конструкцию. К сожалению, нужно констатировать, что кроме низкой стоимости и возможности резки панелей прямо на месте монтажа общестроительным инструментом этим решениям совершенно нечего противопоставить их зарубежным конкурентам. Размер панелей может достигать 12000 мм в длину при ширине 1100 мм, толщина 120 мм. Удельный вес панелей порядка 20–21 кг/м². В целом такие характеристики не должны особенно удивлять, поскольку эти панели исходно позиционировались как общестроительные и не предназначались для создания ЗО дата-центров. Однако, при всех недостатках – повторюсь – эти панели однозначно лучше подходят для устройства защитных оболочек ЦОДов, нежели кирпич, бетон или гипсокартон.

Наиболее подходящим строительным материалом для ЗО являются специальные многослойные панели с различными наполнителями

■ ■ ■

Во второй части статьи будут затронуты вопросы выбора помещения для установки ЗО, строительной подготовки, проектирования и логистики. ИКС

СКС категории 6а

Технические особенности и рыночные перспективы

Кабельная техника категории 6а – на сегодня наиболее совершенный тип СКС массового использования. Основная область ее применения – ЦОДы. Какую долю эта техника может занять в общем объеме рынка СКС?

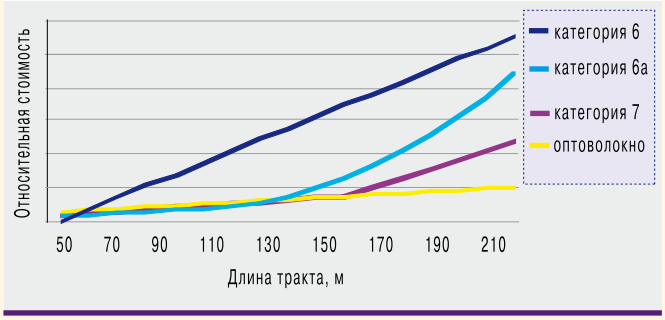
Андрей СЕМЕНОВ,
директор по развитию
«АйТи-СКС»

Структурированные кабельные системы в той их части, которая реализуется на основе симметричного кабеля, в соответствии с принятым в нашей стране американским подходом делятся по так называемым категориям. С увеличением номера категории или появлением у нее буквенного индекса-расширителя улучшаются передаточные параметры системы, в том числе растет максимально допустимая скорость передачи информации. Однако одновременно с этим повышается стоимость компонентной базы, а также сложность монтажа и тестирования готового объекта, что серьезно увеличивает его полную стоимость. В настоящее время наиболее совершенным типом СКС массового применения является техника категории 6а, поэтому сосредоточимся именно на ней.

Предпосылки появления

Техника категории 6а была создана в ответ на острую потребность в кабельных системах общего назначения, обеспечивающих передачу информационных потоков со скоростью не менее 10 Гбит/с. Первоначально считалось, что естественный кандидат на эту роль – серийная техника категории 7, разработанная еще в середине 90-х гг. прошлого века. Однако она оказалась функционально избыточной и вследствие этого слишком дорогой с точки зрения построения сетей массового применения.

Рис. 1. Относительная стоимость линии 10G, реализованной на разных типах элементной базы, в зависимости от ее протяженности



Дело в том, что техника категории 7 разрабатывалась в первую очередь для поддержки сетевых интерфейсов ATM-622. Поэтому в ней не использовалась схема параллельной передачи и применялось бинарное кодирование линейных сигналов. Таким образом, в СКС категории 7 характеристики приемопередатчиков активного сетевого оборудования и пассивной линейной части канала связи изначально не были согласованы. В результате теоретическая шенноновская пропускная способность, которая для техники категории 7 на стометровом каноническом тракте с четырьмя соединителями достигает примерно 55 Гбит/с, использовалась чуть больше чем на 10%. При столь низком КПД кабельного тракта ожидать от него хороших экономических параметров было бы верхом наивности.

В то же время техника категории 6а с системной точки зрения существенно более точно согласована с типовой областью применения. Она создавалась с прицелом на передачу сигнала 10-гигабитного Ethernet на расстояние 100 м. Шенноновская пропускная способность такого тракта составляет 18 Гбит/с (некоторые современные серийные системы в экранированном исполнении позволяют получить 30–40 Гбит/с). Это гарантирует как нормальное функционирование интерфейса, так и хорошие стоимостные параметры решения в целом (рис. 1). Здесь же отметим, что техника категории 7 изначально не позволяла строить неэкранированные СКС.

Проблемы технического плана

Сетевые интерфейсы 10G Ethernet максимально полно используют потенциальную пропускную способность современных кабельных трактов. Достигается это благодаря применению многоуровневого кодирования для ограничения ширины полосы канала связи, коррекции и компенсационных механизмов для выделения информационного сигнала из шумов, а также ряда других технических приемов. Тем не менее, для того чтобы в 10 раз увеличить скорость передачи этого активного сетевого оборудования по сравнению с решениями Gigabit Ethernet, потребовалось более чем в 4 раза повысить верхнюю граничную частоту спектра линейного сигнала. Нарушение пропорциональности объясняется переходом от кода PAM-5 в Gigabit Ethernet к линейному коду PAM-16 в системах 10G Ethernet.

Использование неэкранированных кабельных трактов в расширенном до 500 МГц частотном диапазоне привело к появлению ощутимых межкабельных (в общем случае – межэлементных) переходных влияний. А это, в свою очередь, вынудило расширить список параметров, которые должны контролироваться перед сдачей линии в эксплуатацию, включив в него межкабельное переходное затухание в обычном и суммарном вариантах.

Область применения

Наращивание быстродействия канала связи, по которому происходит подключение к ЛВС на нижнем уровне информационной системы, до уровня свыше нескольких десятков мегабит в секунду в настоящее время признано нецелесообразным. Выдвигавшееся еще полтора десятка лет назад и выполненное на рубеже веков требование об обязательном увеличении скорости до 1 Гбит/с сегодня снято с повестки дня: видеоконференции, фактически единственное реально востребованное пользовательское приложение, требующее столь широкополосного канала, так и не получили ожидаемого развития и массового внедрения.

Отсюда немедленно следует, что областью применения техники категории 6а являются те линии СКС, в которых принципиально отсутствуют скоростные

ограничения системы «человек–машина». Такие линии могут организовываться на магистральных уровнях традиционных офисных СКС и в центрах обработки данных.

Магистрали крупных СКС можно сразу исключить из дальнейшего рассмотрения. Это связано с необходимостью выполнения обязательных требований обеспечения гальванической развязки между отдельными техническими помещениями. Поэтому главным и фактически пока единственным объектом, где возможно массовое применение СКС категории 6а, являются ЦОДы.

Оценка объема рынка СКС категории 6а

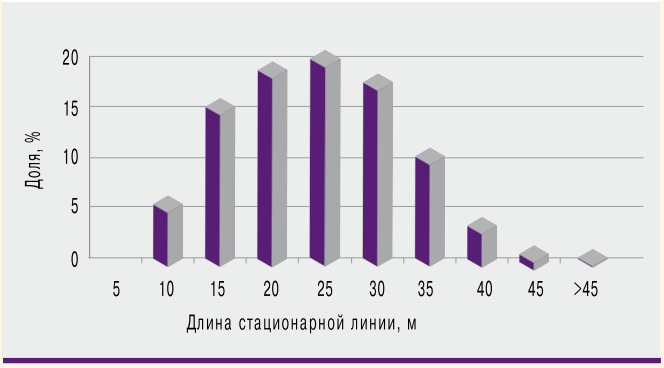
Наличие четко очерченной области применения и некоторые ее технические особенности позволяют достаточно точно оценить объем рынка СКС категории 6а в регионах с высоким уровнем информатизации. К последним можно смело отнести и Россию.

Теоретические расчеты и практика реализации кабельных систем офисного типа свидетельствуют о том, что затраты на построение магистральной части правильно спроектированной СКС категории 6а составляют примерно 15–20% общей стоимости СКС объекта. Кабельную систему ЦОДа с точки зрения построения информационной системы в целом можно рассматривать как удаленное отображение магистральной части классической СКС. Линии СКС в ЦОДе используются для соединения серверов с коммутаторами ЛВС и накопителями массовой памяти. Поэтому названную цифру можно удвоить.

Из полученной таким образом оценки следует вычленить средства, затрачиваемые на приобретение оптической техники. Существенным преимуществом оптической элементной базы, компенсирующим ее несколько худшие экономические параметры (см. рис. 1), является меньшее энергопотребление сетевых интерфейсов, что для ЦОДов критически важно. Однако реализовать это преимущество на практике в полной мере не получается, и вот почему. Средняя длина стационарной линии СКС в ЦОДах несколько меньше 30 м (рис. 2) – вместо 40 м, типичных для крупных офисных кабельных систем. Обусловлено это двумя факторами: во-первых, компактностью ЦОДа как архитектурного объекта, проистекающей из дороговизны подобных зданий; во-вторых, исходным наличием в нем большого количества кабельных трасс под обязательным фальшполом и на каблегонах, устанавливаемых поверх монтажных шкафов. Широкий выбор возможных кабельных трасс при прокладке линейного кабеля дает большие возможности для минимизации протяженности стационарной линии.

При столь малых длинах типовой стационарной линии межножильный интерфейс сетевого оборудования, как правило, может работать в режиме Short reach. В этом случае оптические интерфейсы теряют свое преимущество в отношении потребляемой мощности.

Рис. 2. Распределение длин стационарных линий кабельной системы ЦОДа (на примере СКС с 700 портами)



Исходя из вышеизложенного, можно предположить, что количество медножильных и оптических линий в ЦОДах будет примерно одинаковым. А с учетом несколько более высокой стоимости элементной базы категории 6а (она на несколько десятков процентов дороже соответствующих аналогов категории 6) объем рынка СКС этой разновидности можно в первом приближении оценить как одну треть суммарного объема рынка офисных кабельных систем категории 5е и 6.

Оборудование категории 6а и развитие техники СКС

В процессе развития техники категории 6а был сделан ряд оригинальных разработок, которые не имеют аналогов в СКС предыдущих поколений. Прежде всего хочется отметить так называемую полуэкранированную технику, т.е. кабельные системы, у которых отдельные компоненты стационарной линии и тракта снабжены незаземленными экранами пленочного типа. Металлизация такого экрана имеет разрывы, препятствующие образованию токовых петель, но не мешающие нормальному функционированию экрана на частотах свыше 300 МГц.

Добавление пленочного экрана в конструкцию линейных кабелей, розеточных модулей и коммутационных шнуров не ухудшает их массогабаритных характеристик, но повышает стойкость к внешнему мешающему электромагнитному излучению. Это происходит за счет увеличения примерно на 10 дБ величин параметров ANEXT и AFEXT в обычном и суммарном вариантах.

Основное преимущество полуэкранированной техники заключается в том, что она может монтироваться по правилам неэкранированных кабельных систем. Для нее не является критически важным наличие качественного телекоммуникационного заземления, эффективно выполняющего свои функции на частотах в сотни мегагерц.

С технической точки зрения использование полуэкранированной техники, которая не требует заземления, эффективно решает проблему создания необходимого «запаса прочности» по межкабельной помехе, которой уже нельзя пренебрегать в верхней половине

рабочего частотного диапазона сетевых интерфейсов 10G Ethernet. С практической точки зрения полуэкранированная техника выгодна тем, что ее повышенная помехоустойчивость заметно ускоряет и упрощает монтаж.

Уже упоминавшиеся особенности распределения длин линий кабельных систем в ЦОДах стали причиной появления техники неофициальной категории «квази 6а». Речь идет о кабелях, которые по ряду важных параметров (в первую очередь затуханию и сопротивлению шлейфа) не соответствуют стандартам офисных СКС и СКС для ЦОДов, построенных по стандарту TIA-942. Однако, если длина стационарной линии не превышает 60 м (что с большим запасом перекрывает практические потребности в отношении кабельных систем для ЦОДов), тракт на их основе вполне обеспечивает требуемое качество передачи. А из-за отсутствия реальных потребителей техника PoE, для которой важно сопротивление шлейфа, в ЦОДах неактуальна.

Существенный выигрыш от применения изделий «квази 6а» вместо стандартной техники категории 6а обусловлен их заметно меньшим диаметром (чуть более 5 мм). В результате улучшаются их массогабаритные характеристики и в значительной степени нивелируется значимое для ЦОДов преимущество оптических линий по этому параметру.

Особо отметим, что, несмотря на массовый характер предложения данных изделий со стороны производителей, в известных редакциях нормативных документов они пока не упоминаются.

Подведем итоги

Техника категории 6а – продукт оптимизационного согласования параметров пассивной линейной части и активного сетевого оборудования, выполненного с целью получения новых свойств комплексного продукта.

Четко очерченная нишевая область применения СКС категории 6а – нижний уровень кабельных систем ЦОДов.

Объем потребления техники категории 6а в настоящее время должен устойчиво расти, однако в обозримой перспективе его величина ограничена примерно третью объема потребления СКС категорий 5е и 6.

В процессе создания техники категории 6а был выполнен и внедрен в практику построения кабельных систем ряд новых разработок, которые уже в ближайшее время могут привести к пересмотру некоторых фундаментальных положений действующих редакций профильных стандартов. ИКС

Автор выражает признательность И.Г. Смирнову за предоставленные статистические данные по кабельным системам ЦОДов.

Правильный выбор категории СКС оптимизирует стоимость проекта

Александр ЛАСЫЙ,
технический директор департамента интеллектуальных зданий компании КРОК

При реализации структурированной кабельной системы мы всегда принимаем в расчет срок и условия ее функционирования. Пожалуй, это главные критерии выбора категории СКС.

Для зданий, которые планируется эксплуатировать длительное время (10–15 лет), целесообразно выбрать СКС категории 6а, чтобы обеспечить запас производительности на такой период и беспроблемный переход на скорость 10 Гбит/с. В этом случае предпочтительны системы SYSTIMAX GigaSpeed X10D. В магистралях таких сетей лучше использовать многомодовые оптоволоконные линии OM-3 с той же производительностью, но имеющие возможность передавать сигналы на расстояния до 350 м. Комбинация в СКС кабелей этих категорий позволяет оптимизировать стоимость проекта.

Для серверных помещений и центров обработки данных применение медной СКС категории 6а стало уже практически стандартом. На магистральных линиях в ЦОДах мы обычно устанавливаем многоволоконные претерминированные кабели, например, SYSTIMAX InstaPatch. Они позволят плавно и без серьезной первоначальной реконструкции СКС перейти на агрегированные линии со скоростями 40 Гбит/с и более. Так, недавно мы завершили проект для крупной консалтинговой компании, в ходе которого оснастили ее офис в деловом центре «Москва Сити» интеллектуальной СКС iPatch категории 6а (GigaSpeed X10D). Проект рассчитан на перспективу и дает возможность развивать локальную сеть без глобальной реконструкции СКС.

СКС категории 6а широко применяются в ЦОДах еще и благодаря тому, что они существенно снижают общие затраты за счет более низкой стоимости сетевого оборудования. Например, конструкция и технические показатели СКС GigaSpeed X10D компании Commscope позволяют сократить минимальную длину горизонтальных кабелей до 5 м, что важно для ЦОДов, где коротких кабелей много, а минимальная длина по стандарту – 15 м. Поэтому данный продукт имеет очень хорошие перспективы в своем сегменте рынка. В компактных ЦОДах с максимальной длиной кабельных пробросов 20–25 м, работая с кабелем марки 3091, можно сократить количество прокладываемого кабеля почти вдвое. Более того, в комплекте с розеточными модулями MGS600 и кордами 360GS10E этот кабель допускает четыре коммутации на 90 м линии, а значит, в ряде случаев можно отказаться от активного сетевого оборудования и использовать для администрирования пассивную коммутацию.

Климатический шкаф с установкой электропитания

Установка электропитания «Штиль» PS48-0400 (4/2500) в климатическом антивандальном шкафу ШТК-103 КТН-02С предназначена для организации новых и модернизации существующих узлов связи стандарта GSM. Двухсекционный антивандальный шкаф ШТК-103 КНТ-02С в качестве системы поддержания микроклимата оснащен кондиционером с теплообменником, что позволяет значительно экономить электроэнергию, затрачиваемую на поддержание рабочей температуры в шкафу. Антивандальная защита обеспечивается двойными стенками шкафа, трехточечными замками, скрытыми петлями дверей и невозможностью разборки шкафа снаружи.

ШТК-103 КНТ-02 оснащен датчиками (открытия двери, дыма, влажности, температуры), а также системами поддержания микроклимата и контроля температуры внутри шкафа. Все данные мониторинга объекта связи, осуществляемого встроенным в установку электропитания «Штиль» контроллером, передаются по каналу на пульт диспетчера технической службы оператора связи. Для удобства регулярного обслуживания доступ к оборудованию осуществляется с фронтальной стороны, все подключения выведены на лицевую панель системы электропитания.

Комплексное решение позволяет размещать внутри шкафа не только систему электропитания постоянного тока 48В «Штиль» PS48-0400 (4/2500) мощностью 10 кВт с аккумуляторными батареями, но и активное оборудование оператора связи. Шкаф с оборудованием можно устанавливать под открытым небом: степень защиты – IP 55, а допустимый диапазон температур – от –40 до + 40°С.

Группа компаний «Штиль»: (4872) 24-13-62

Агент газового пожаротушения

Газовое огнетушащее вещество (ГОТВ) Novec 1230 относится к разряду перфторированных кетонов и представляет собой бесцветную прозрачную жидкость со слабовыраженным запахом, которая тяжелее воды в 1,6 раз и не проводит электричество. Диэлектрическая проницаемость Novec 1230 равна 2,3 (за единицу принята проницаемость осушенного азота).

Novec 1230 быстро переходит из жидкого состояния в газообразное и активно поглощает тепловую энергию огня. Поскольку температура кипения этого ГОТВ при давлении 1 атм составляет 49,2°С, оно мгновенно испаряется, не вступая ни в какие химические реакции, и его использование не наносит ущерба оборудованию и не приводит к короткому замыканию, даже если сжиженный газ выливается прямо на электрические розетки или контакты.

Коэффициент безопасности Novec 1230 равен 2,38 (его предельно допустимая концентрация – 10%, расчетная – 4,2%). Это позволяет применять ГОТВ для пожаротушения в помещениях, где постоянно находятся люди, – в диспетчерских, аппаратных, центрах управления полетами, ситуационных центрах и т.д.

Каждый модуль представляет собой баллон емкостью от 8 до 180 л, в котором в жидкой фазе хранятся Novec 1230 и газ-вытеснитель (в этом качестве используется осушенный азот 5-й категории с точкой росы –55°С), поднимающий давление в баллоне до 24,8 бар при температуре + 20°С. ГОТВ Novec 1230 заливается в баллон в количестве, необходимом для тушения конкретного помещения. Выпуском огнетушащего газа управляет запорно-пусковое устройство с соленоидным, пневматическим или ручным приводом.

«3М Технологии для электронной промышленности»: (495) 784-7479

Магистральный маршрутизатор

Brocade MLXe входит в линейку маршрутизаторов MLX Series. Он способен работать с пропускной способностью до 15,36 Тбит/с, обрабатывать до 4,8 млн пакетов в секунду и поддерживает интерфейсы 100GE. Позиционируется для ЦОДов и сервис-провайдеров.

Маршрутизатор выпускается с 4, 8, 16 и 32 слотами, в которые помимо модулей с интерфейсами 10GE, 1 GE, SDH-16, SDH-64, можно устанавливать модули, обеспечивающие передачу на скорости до 100GE. Эти модули снабжены двумя портами 100GE.

Фабрика коммутации имеет резервирование по схеме N + 1. Распространение воздушного потока организовано по схеме «все назад». MLXe сертифицирован по стандарту NEBS level 3.

Основные технические характеристики:

- до 32 портов 100 GE на систему;
- до 256 портов 10 GE или 1536 портов 1 GE на систему;
- до 64 портов OC-192 (SDH-64) или 256 портов OC-48 (SDH-16) на систему;
- агрегация VLAN (Q-in-Q);
- поддержка протоколов Layer 2: MRP, VSRP, RSTP, MSTP;
- поддержка IEEE 802.1ad Provider Bridges;
- соответствие сертификации MEF 9 и MEF 14 для Carrier Ethernet;
- поддержка агрегации до 64 потоков 10 GE/OC-192;
- поддержка мультитерабитных транков путем агрегации портов 100 GE в LAG group;
- маршрутизация на скорости линии;
- поддержка MPLS, в том числе IP over MPLS, Virtual Leased Line, Virtual Private LAN Service, BGP/MPLS VPN и Multi-VRF.

Маршрутизаторы MLXe полностью совместимы со всеми модулями MLX и NetIron XMR.

Brocade: (495) 937-8319

Мультимедийные микрокиоски самообслуживания

Микрокиоск MK500 – это многофункциональное устройство, предназначенное для проверки цен на товары путем считывания штрихкода, а также способное организовать интерактивное общение с клиентом, предоставляя ответ на запросы, вводимые нажатием на сенсорную панель или кнопку. Оно комплектуется лазерным сканером для считывания кодов 1D или фотосканером для кодов 1D, 2D и PDF417. MK500 снабжен цветным сенсорным ЖК-дисплеем (диагональ 3,5", разрешение QVGA 320 x 240 пикселов) с тремя программируемыми кнопками и встроенными стереодинамиками. Возможность расширения обеспечивают слот для карт MicroSD, а также порт Ethernet RJ-45 и три порта Mini USB 1.1 (2.0-совместимый) для подключения периферийных устройств, включая принтеры, клавиатуру, устройства для считывания магнитных карт и т.п. Подключение к локальной сети предприятия может осуществляться по Ethernet со скоростью 10/100 Мбит/с (802.3) либо по беспроводному каналу 802.11a/b/g (до 54 Мбит/с), питание осуществляется от сети 220 В или через Ethernet (802.3af). Вес устройства – 320 г.

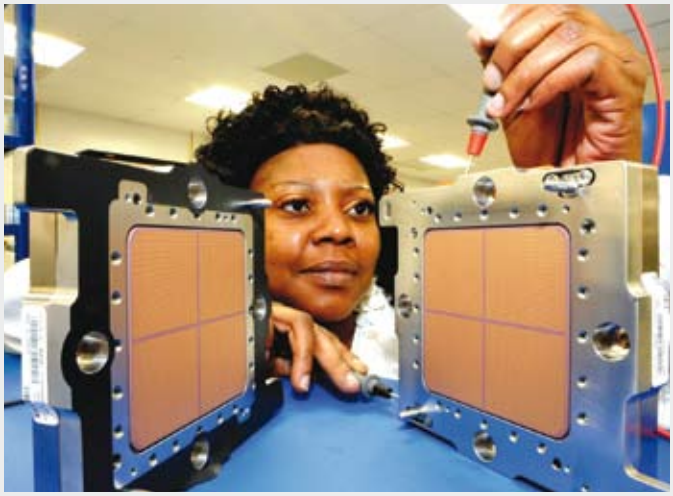
MK500 является полноценным мультимедийным устройством и способен воспроизводить аудио- и видеофайлы. Микрокиоск работает под управлением ОС Windows CE.NET 5.0 и обладает встроенной поддержкой Internet Explorer 6.0 и Symbol Pocket Browser. Комплект ПО включает в себя Web Kiosk с исходными кодами, AirBEAM Smart и Rapid Development Client. Совместимость с платформой мобильных сервисов Motorola (MSP) дает возможность удаленной первоначальной настройки, установки ПО, мониторинга и поиска неисправностей. В число средств разработки входят Microsoft eMbedded Visual C++ 4.0 SP3 и Visual Studio .Net 2005.

Старшая модель MK4000 имеет расширенные возможности по сравнению с MK500. Она снабжена цветным сенсорным ЖК-дисплеем с диагональю 12,1" и разрешением 800x600 пикселов (SVGA), лазерным сканером для 1D-кодов или имидж-сканером для кодов 1D, 2D и PDF417, двумя встроенными громкоговорителями и микрофоном. Вес – 1,99 кг.

Motorola: (495) 785-0150

Мэйнфрейм zEnterprise 196

содержит 96 микропроцессоров, работающих на тактовой частоте 5,2 ГГц и способных выполнять свыше 50 млрд команд в секунду. Чип произведен с использованием 45-нанометровой процессорной технологии SOI («кремний на изоляторе»).



Процессор мэйнфрейма использует запатентованную IBM технологию встраиваемой памяти DRAM (eDRAM), позволяющую размещать динамическую кэш-память с высокой плотностью в тех же чипах, что и высокоскоростные микропроцессоры.

Микропроцессорная технология поддерживается программным обеспечением для оптимизации исполнения рабочих нагрузок с большими объемами данных, что обеспечивает повышение производительности до 60% при исполнении рабочих нагрузок с интенсивной обработкой данных и Java-нагрузок.

Система на 60% мощнее своего предшественника, мэйнфрейма System z10, при приблизительно одинаковом потреблении электроэнергии.

IBM: (495) 775-8800

Корпоративная система защиты конфиденциальной информации

Secret Disk Enterprise (SDE) – корпоративная система защиты конфиденциальной информации с централизованным управлением – позволяет отслеживать состояние зашифрованных носителей, уменьшает риск ошибочных действий пользователя и снимает нагрузку с информационных служб предприятий.

Система обеспечивает решение следующих задач корпоративных заказчиков:

- защиту от несанкционированного доступа и раскрытия конфиденциальной информации, находящейся на компьютерах пользователей;
- централизованное управление защищенными дисками на компьютерах пользователей;
- единый мониторинг и диагностику состояния защищенных дисков на рабочих местах пользователей;
- разграничение прав пользователей продукта, в том числе и системных администраторов, при доступе к защищенным данным;
- сокращение нагрузки на службы поддержки и администрирования за счет выполнения большинства операций через административный веб-портал.

Функциональные возможности Secret Disk Enterprise:

- шифрование разделов на жестких дисках, защита системного раздела, создание виртуальных зашифрованных дисков;
- двухфакторная аутентификация пользователей с помощью электронного ключа eToken как для загрузки операционной системы, так и для доступа к защищенным дискам;
- работа с защищенными данными вне корпоративной сети;
- аудит использования защищенных ресурсов и действий пользователей;
- безопасное резервное копирование защищенных данных сторонними продуктами для динамических виртуальных зашифрованных дисков.

Прозрачная работа продукта незаметна для пользователей системы. Поддерживаются несколько алгоритмов шифрования, в том числе AES-256, Triple DES и отечественный алгоритм ГОСТ 28147-89. Для пользователей существует возможность оперативного восстановления доступа к данным в случае утери или поломки электронного ключа. Тиражирование клиентского программного обеспечения выполняется средствами системы управления SDE, что существенно упрощает и ускоряет развертывание системы на предприятии.

Aladdin: (495) 223-0001

Блог, еще раз блог!

Александра КРЫЛОВА

Apple услышала разработчиков

>>>> Распространенное на российском телекоммуникационном рынке мнение о замечательных отношениях между компанией Apple и разработчиками программных продуктов для ее AppStore оказалось, мягко говоря, преувеличением.

Да, действительно, за два года количество приложений, размещенных в Apple AppStore, достигло 250 тыс., количество их загрузок перевалило за 6,5 млрд, а разработчики ПО на платформе iOS заработали на приложениях для iPhone свыше $1 млрд.

Однако далеко не все партнеры были удовлетворены условиями сотрудничества, а точнее, теми требованиями, которым должны соответствовать программные продукты, размещаемые в AppStore. Недавно компания Apple объявила о том, что приняла жалобы разработчиков приложений для iPhone и iPad близко к сердцу и учла некоторые из них в новом руководящем документе, призванном ослабить часть ограничений. Речь идет прежде всего об ограничениях на использование средств разработки для iOS. Отныне они не распространяются на разработчиков, чьи приложения не требуют загрузки обновлений. Также у партнеров Apple появилась возможность использовать в своих программах технологию Adobe Flash. Правда, это не означает, что владельцы iPhone или iPad смогут просматривать созданные при ее помощи веб-страницы.

...Стремление Apple пойти навстречу партнерам, поставляющим приложения для AppStore, можно понять: время, когда ее магазин был единственным на рынке, прошло. Сегодня сотрудничество разработчикам программных продуктов для мобильных устройств предлагают и Google для Android, и RIM с Blackberry App. Вдруг они предложат более интересные условия?

комментировать

Александр МАРТЫНЮК

То, о чем так долго говорили... свершилось

>>>> Конференция «ЦОД 2010» прошла. Что можно о ней сказать, пока воспоминания свежи?

Уровень мероприятия заметно вырос. Это видно во всем:

– участников – более 300 человек;

– докладчиками были не только отечественные специалисты, но и зарубежные эксперты;

– темы докладов аналогичны тем, что делались в этом году на международных мероприятиях AFCOM, Uptime Institute и Gartner;

– зал не просто слушал лекции, но и задавал вопросы...

Уровень понимания рынком сложности проблемы и важности обсуждаемых вопросов вырос.

В целом впечатление очень хорошее. И от организации, и от докладов, и от обсуждавшихся на круглом столе вопросов.

Чего бы хотелось еще от этой конференции?

Конечно, большей активности участников. Невольно приходится сравнивать с зарубежными конференциями, и в этом плане их участники более активны. В чем? В количестве и качестве задаваемых вопросов, ответов на анкеты по каждому выступлению, активности на круглых столах.

Хотелось бы больше узнать о реализованных в России и за рубежом проектах.

Искренне хочется верить, что популизм и желание продать постепенно уступят место серьезной дискуссии специалистов, что приведет к росту качества и количества ЦОДов.

Впрочем, все эти желания будут упираться в готовность заказчиков потреблять качественные и недешевые услуги.

комментировать

Андрей ЕГОРОВ

Ужасы нашего хостинга

>>>> Рынок хостинга нечасто радует отечественного пользователя какими-либо громкими событиями и новостями. Разве что дата-центр останется без электричества или хозяйствующие субъекты между собой государственных денег не поделят и начнут веерные отключения и временные ограничения доступа к пользовательским сайтам, и тогда вся хостинговая и околохостинговая тусовка с интересом следит за развитием событий.

Крупных покупок и поглощений среди отечественных хостеров не было последние три-четыре года, не считая странных обсуждений на форуме хостобзора (hostobzor.ru) о продаже сферических компаний в вакууме или забавных «оферт» о скупке мелких хостингов, как на сайте компании «Спринтхост».

...Хочется заметить, что российский пользователь достаточно стойко переносит разного рода невзгоды, связанные с низким качеством сервиса или отсутствием такового. Показателен пример с почти недельной недоступностью ресурсов российского хостинг-провайдера «Мак-Хост», после которого тот лишился 30% своей клиентской базы и, возродившись, как птица феникс, где-то на амстердамских просторах, продолжил свое движение вперед.

...Интересно, каким будет рынок хостинга через 5–10 лет? Уже не первый год эксперты предрекают ему скорую стагнацию и чудесное превращение хостинг-провайдеров в провайдеров готовых SaaS-решений. Продолжение процесса объединения хостинговых компаний после кризиса можно считать важным сигналом на пути эволюции отечественного хостинга.

комментировать

Реклама в номере

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

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

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

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