Телекомы отстали от «широкого» рынка

С середины октября по середину ноября акции российских компаний телеком-сектора торговались преимущественно в «зеленой» зоне и на позитивном фоне. Капитализация отечественных телеком-компаний неплохо выросла, особенно это касается бумаг «ЦентрТелекома», «Дальсвязи», «Уралсвязьинформа» и «Волгателекома».

Анна ЗАЙЦЕВА,
аналитик УК «Финам Менеджмент»

Российский фондовый рынок в середине осени демонстрировал позитивную динамику. Решение Федеральной резервной системы США о дальнейшем смягчении кредитно-денежной политики позволило российским индексам покорить максимумы двухгодичной давности. Однако затем игроки пожелали зафиксировать прибыль, так что в конечном счете индексы несколько растеряли свои завоевания.

Хроника реорганизации. Продолжение

Основным событием в секторе по-прежнему остается процесс реорганизации «Связьинвеста», который обрастает новыми подробностями. В частности, 26 октября завершилась процедура выкупа акций у миноритарных акционеров дочерних компаний госхолдинга – на эти цели «дочки» «Связьинвеста» потратили более 15,6 млрд руб. Кроме того, 10 ноября состоялось заочное внеочередное общее собрание акционеров «Ростелекома». Его основные акционеры, холдинг «Связьинвест» (владеет 50,7% обыкновенных акций) и ВЭБ (контролирует 39,9% обыкновенных акций), проголосовали против принятия поправки в устав «Ростелекома», предусматривающей, что величина дивидендов по привилегированным акциям будет определяться как величина в 10% чистой прибыли по итогам последнего финансового года, деленная на общее число размещенных привилегированных акций.

Среди других важных корпоративных новостей, влиявших на ситуацию на фондовом рынке, можно выделить покупку у «Газпромбанка» компанией Marshall Capital Partners фонда, который владеет акциями «дочек» «Связьинвеста» – семи МРК и «Ростелекома». На указанном фоне акции «Ростелекома» выросли за месяц на 2,08%, достигнув цены в 140,59 руб.

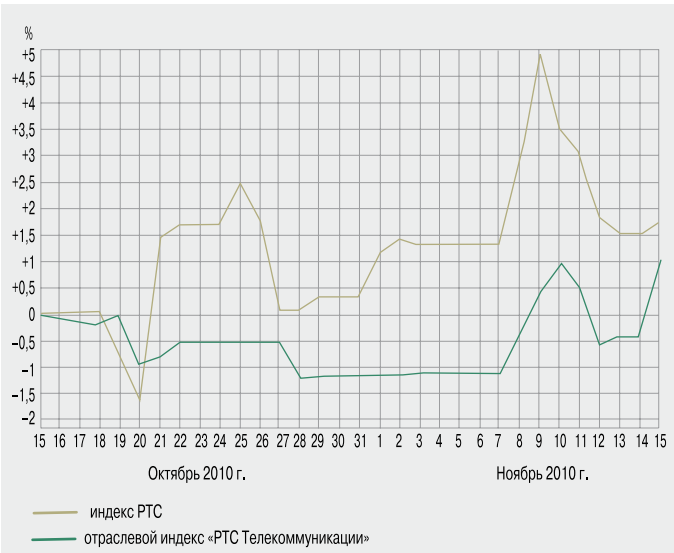
Традиционные тяжеловесы растут

У «Сибирьтелекома» капитализация увеличилась на 7,21%, составив 2,364 руб. Поддержку котировкам акций компании оказала публикация позитивной

Справка ИКС

С 15 октября по 15 ноября индекс ММВБ прибавил 4,51% до отметки 1556,18 пункта, а индекс РТС – 1,41%, до 1609,43 пункта. Отраслевые индексы также зафиксировали рост: индекс «ММВБ телекоммуникации» поднялся на 3,69%, до отметки 2282,29 пункта, индекс «РТС Телекоммуникации» вырос на 1,05%, достигнув 234,58 пункта.

Динамика индексов и инструментов РТС



отчетности за 9 месяцев 2010 г. по РСБУ. Так, чистая прибыль оператора за 9 месяцев увеличилась на 83,4% по сравнению с аналогичным периодом прошлого года и составила 3185,5 млн руб., что обусловлено увеличением прибыли до налогообложения. Маржа чистой прибыли выросла на 6,455 процентных пункта – до 14,7%. Доходы «Сибирьтелекома» без учета дочернего бизнеса за 9 месяцев текущего года достигли 21 643,7 млн руб., увеличившись на 3,7% по сравнению с аналогичным периодом прошлого года.

Акции «ЦентрТелекома» за прошедший месяц прибавили 9,29% – до уровня 29,2 руб. Компания продолжает демонстрировать стабильно высокие результаты: согласно отчетности по РСБУ, за 9 месяцев 2010 г. ее чистая прибыль составила 5 320 738 руб., увеличившись за год более чем на 30%. Среди корпоративных событий стоит отметить сообщение о том, что акционеры «ЦентрТелекома» одобрили выплату дивидендов по итогам 9 месяцев нынешнего года в размере 0,5085555 руб. на одну обыкновенную акцию и 1,1163016 руб. – на привилегированную. Как говорится в сообщении компании, сумма выплат на простые акции составит 798,111 млн руб. (15% чистой прибыли общества по результатам 9 месяцев 2010 финансового года), на «префы» – 532,075 млн руб. (10% прибыли). Срок выплаты дивидендов – до 7 января 2011 г.

Обыкновенные акции «Дальсвязи» выросли на 7,21%, превысив отметку 116,67 руб. Акционеры компании определились с выплатой дивидендов по итогам 9 месяцев: из расчета 3,432 руб. на обыкновенную и 6,857 руб. на привилегированную акцию номиналом 20 руб. Чистая прибыль общества за 9 месяцев 2010 г. составила 2172,812 млн руб., а на выплату промежуточных дивидендов по итогам 9 месяцев будет направлено 480,8081 млн рублей. Дивиденды будут выплачены до 12 января 2011 г.

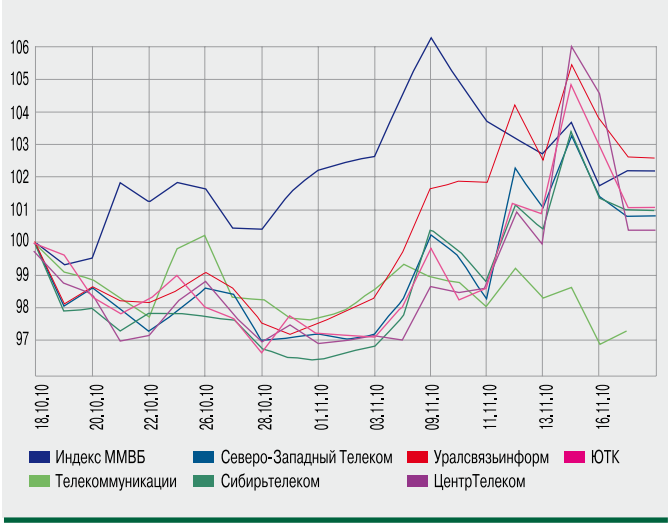
Бумаги «Северо-Западного Телекома» подорожали на 6,27% – до уровня 26,616 руб. Поддержку им оказала публикация позитивной отчетности по РСБУ за 9 месяцев 2010 г., согласно которой чистая прибыль оператора выросла на 18,4% (до 3,725 млрд руб.) по сравнению с аналогичным периодом прошлого года. Выручка от продаж по сравнению с тем же периодом 2009 г. увеличилась на 7,5% и составила 20,858 млрд руб., в том числе от услуг связи – 19,149 млрд руб. Что касается решения о выплате дивидендов, то акционеры «Северо-Западного Телекома» по итогам 9 месяцев определили их размер в 0,6 руб. на обыкновенную акцию и 1,3 руб. на привилегированную.

Капитализация «Волгателекома» выросла на 8,02% до отметки 125 руб. за акцию. Федеральная антимонопольная служба разрешила оператору приобрести 100% голосующих акций ОАО «Радиотелефонная компания» (основные виды деятельности – услуги местной телефонной связи и телематических служб). Компания также сообщила об увеличении чистой прибыли за 9 месяцев 2010 г. на 38,6% – до 4403,1 млн руб. Выручка «Волгателекома» составила 21 264,3 млн руб., увеличившись на 6,0% по сравнению с аналогичным периодом 2009 г. Доходы от услуг связи возросли на 5,4%, до 20 103,7 млн руб.

> Важным событием для МТС стало вступление в альянс Wholesale Applications Community, нацеленный на создание глобальной открытой платформы для разработки и продажи мобильных приложений

Акции «Уралсвязьинформа» поднялись на 8,61%, достигнув 1,287 руб. Компания показала нейтральные результаты по РСБУ за 9 месяцев 2010 г. Так, в январе–сентябре выручка составила 32,05 млрд руб. (+6% к соответствующему периоду 2009 г.), при этом благодаря жесткому контролю компания снизила затраты на 4,6% по сравнению с январем–сентябрем 2009 г. Показатель EBITDA вырос до 14,2 млрд руб. (+23,1%), чистая прибыль компании достигла 6,07 млрд руб. (+105,6%).

Динамика индексов РТС и телекоммуникационных компаний в период с 18 октября по 16 ноября 2010 г.



У сотовиков рост скромный

Бумаги сотового оператора МТС отметились наиболее скромным ростом, прибавив 2,23%, что составило 255,58 руб. за акцию. Компания сообщила об увеличении чистой прибыли за 9 месяцев 2010 г. по РСБУ с 26,852 млрд руб. до 35,129 млрд руб. Выручка увеличилась с 146,163 млрд руб. до 159,048 млрд руб. Важным для компании событием стало вступление в международный телекоммуникационный альянс Wholesale Applications Community (WAC), нацеленный на создание глобальной открытой платформы для разработки и продажи мобильных приложений.

Обыкновенные акции АФК «Система» выросли на 2,86%, достигнув цены в 26,757 руб. Компания сообщила о приобретении 51% акций «Навигационно-информационных систем», из которых 25,5% акций принадлежали ОАО «Концерн «РТИ Системы» и 25,5% акций – ОАО «Ситроникс». ИКС

Защитим электронный документооборот

Лозунг из заголовка – требование момента. Особенно с вступлением в действие федеральной системы межведомственного электронного взаимодействия (см. «ИКС», № 11'2010, с. 6). Что представляет собой такая защита, рассказал Алексей САБАНОВ, заместитель гендиректора компании «Аладдин Р.Д.».

Алексей САБАНОВ

– Насколько велика сегодня потребность российских органов власти в системах защищенного документооборота? В каких случаях, на каком уровне госуправления их использование необходимо?

– Можно выделить несколько причин, по которым именно сейчас организация защищенного электронного документооборота становится объектом пристального внимания. Во-первых, при непосредственном участии руководителей государства интенсифицируется переход к оказанию госуслуг в электронном виде. Обмен электронными документами быстро набирает «критическую массу», при которой неизбежно встают вопросы защиты конфиденциальной информации, в частности, персональных данных. Услуги, предоставляемые в электронном виде, должны базироваться на защищенном электронном документообороте, поскольку формированию электронного документа для физического или юридического лица, как правило, предшествует обмен документами нескольких ведомств. И этот процесс не должен быть общедоступным.

Во-вторых, госорганизации, работающие с гражданами и юридическими лицами, в массе своей начинают осознавать необходимость внедрения электронного документооборота. При этом первостепенный вопрос – применение средств защиты для обеспечения целостности и конфиденциальности информации, содержащейся в электронных документах, а также подтверждения их авторства. Появляется реальная потребность в наделении электронных документов юридической силой наравне с бумажными.

Защищенный документооборот нужен сегодня на всех уровнях госуправления. Другое дело – на всех ли этих уровнях необходима юридическая значимость электронных документов? В первую очередь она нужна для документов, которые могут иметь правовые последствия для граждан и организаций.

– Каков пул поставщиков таких решений? Отмечаете ли вы тенденцию к его расширению?

– Рынок разработчиков систем электронного документооборота в настоящее время близок к насыщению. Наиболее известные игроки объединились в Гильдию управляющих документацией. В нее входят ведущие практики и ученые, руководители делопроизводственных подразделений федеральных и региональных органов законодательной и исполнительной власти, крупных компаний, предприятий, банков. Цель работы Гильдии – обмен опытом и координация деятельности профессионалов в области СЭД, содействие своим участникам, а также широкой профессиональной общественности в распространении передового отечественного и мирового опыта в сфере управления документацией и электронного документооборота.

Поскольку сегодня интерес к системам защищенного документооборота растет, не исключена возможность появления новых, хорошо подготовленных и агрессивных игроков. Системы электронного документооборота внедрялись у нас несистемно, поэтому существует много отраслевых ниш, пока не заполненных специализированными, полностью «обкатанными» решениями.

Почти у всех разработчиков есть системы в защищенном исполнении. Но что понимается под защитой? Некоторая часть разработчиков СЭД уверена, что, «прикрутив» электронную подпись и даже не пройдя испытаний на корректность использования средств криптографической защиты информации (СКЗИ) по требованиям ФСБ России, они предоставляют рынку систему защищенного документооборота. Это не так. Именно по этой причине внедрение защищенного документооборота в органах государственной власти, как правило, выполняют интеграторы, имеющие в штате высококвалифицированных специалистов по защите информации, а также обладающие опытом и соответствующими лицензиями ФСБ и ФСТЭК России.

Вторая проблема заключается в том, что «коробочную» версию, пригодную для внедрения в любом органе госвласти, создать весьма непросто. Зачастую отечественные разработчики начинают с заказной системы документооборота, предназначенной для одного клиента, пусть даже крупного и имеющего разветвленную инфраструктуру и различные прикладные системы. Если заказчик внедрением доволен, у разработчика возникает уверенность, что программный продукт «встанет» и в других организациях. Однако, оказывается, что для каждого отдельного заказчика требуется доработка продукта с учетом особенностей бизнес-процессов, инфраструктуры, возможностей интеграции с существующим системным и прикладным ПО.

– Каким набором сертификатов и других разрешительных документов должен обладать поставщик СЭД, позиционирующий свое решение как защищенное?

– По-хорошему, разработчику систем защищенного электронного документооборота надо получить две основные лицензии ФСТЭК России: на деятельность по разработке и/или производству средств технической защиты конфиденциальной информации и на деятельность по технической защите конфиденциальной информации – в случае самостоятельных внедрений и последующего оказания услуг.

Если поставщик СЭД встраивает СКЗИ в свое ПО, то ему необходима лицензия ФСБ России на разработку и производство средств криптографической защиты. В этом случае нужно исходить из того, что компания планирует делать, так как в лицензии могут содержаться разные формулировки (разрешения). Например, только разработка и производство или разработка и производство информационных или телекоммуникационных систем с использованием криптосредств и т.п. В лицензии могут быть использованы все формулировки, относящиеся к разработке и производству.

Для того чтобы продавать СЭД со встроенными СКЗИ, собственные или сторонних фирм, в том числе иностранных, разработчику требуется лицензия ФСБ России на распространение СКЗИ. Если же разработчик планирует оказывать дополнительные услуги – предоставление защищенных каналов передачи данных, ключевой информации (удостоверяющие центры) или обслуживание криптосредств сторонних организаций, то ему понадобится лицензия на предоставление услуг в области шифрования информации. Для оказания услуг сопровождения и обслуживания криптосредства или информационных систем разработчику необходима лицензия на техническое обслуживание. Кроме того, в ряде случаев могут потребоваться сертификаты ФСБ России на разработанные средства технической защиты информации.

Как правило, разработчики привлекают для выполнения работ по встраиванию криптосредств лицензиатов ФСБ России, поскольку самим получать указанные лицензии слишком долго и дорого. К тому же в штате надо иметь обученных специалистов.

– Какие организационные и технические меры должны приниматься для защиты внутриведомственного и межведомственного документооборота?

– Хотелось бы, чтобы в каждом ведомстве защищенный документооборот строился на основе классического подхода к созданию защищенных систем: оценка рисков – концепция безопасности – модель угроз – модель нарушителя – модель защиты – выбор средств защиты и построение комплекса средств ИБ – управление безопасностью – аудит – совершенствование комплекса средств ИБ. По поручению Минкомсвязи за проект системы межведомственного электронного взаимодействия энергично взялась команда профессионалов «Ростелекома» и компании РНТ. Теперь вопросы информационной безопасности поставлены во главу угла. В докладе Валерия Зубахи, директора проекта «Электронное правительство», на состоявшемся в Санкт-Петербурге PKI-форуме сообщалось, что 15 из 19 федеральных органов власти уже начали межведомственный обмен по защищенным каналам. Это вселяет оптимизм.

– Как, по вашей оценке, решаются сегодня проблемы информационной безопасности, возникающие при взаимодействии органов государственной власти, МФЦ и граждан?

– К сожалению, в абсолютном большинстве случаев эти проблемы остаются за кадром. Те ведомства и подчиненные им предприятия, которые реально защищали свои базы данных, их передачу и обработку до появления требований ФЗ-152 «О персональных данных», продолжают это делать и сейчас. Многие компании, которые до 2006 г. не уделяли пристального внимания вопросам защиты, ФЗ-152 заставил этим заниматься, и положительная динамика налицо. Однако темпы выполнения законодательных требований в области защиты персональных данных, о которых можно судить по количеству уведомлений в адрес Роскомнадзора, не устраивают ни граждан, ни регуляторов. Один из важных моментов деятельности электронного правительства – доверие к его технологиям со стороны граждан и юридических лиц. Доверие в данном случае может быть основано на использовании проверенных временем и сертификационными испытаниями технических средств защиты при организации защищенного документооборота и межведомственного обмена электронными документами. Степень доверия будет повышаться, если о применяемых для защиты персональных данных средствах защиты будут знать все участники информационного обмена. ИКС

Руководящие документы в сфере межведомственного взаимодействия

- Постановление Правительства РФ № 931 от 25.12.2007 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям».
- Постановление Правительства РФ № 477 от 15.06.2009 «Об утверждении правил делопроизводства в федеральных органах исполнительной власти», содержащее раздел «Особенности работы с электронными документами» и перечень обязательных сведений об электронных документах.
- Приказ Минкомсвязи № 41 от 23.03.2009 «Об утверждении Требований к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра».
- Постановление Правительства РФ № 697 от 08.09.2010 «О единой системе межведомственного электронного взаимодействия».

Контроль доступа к конфиденциальным документам

Попадание многих электронных документов в чужие руки может иметь для компании неприятные последствия. Обеспечить конфиденциальность критичной информации как раз и призваны системы управления правами доступа к документам.

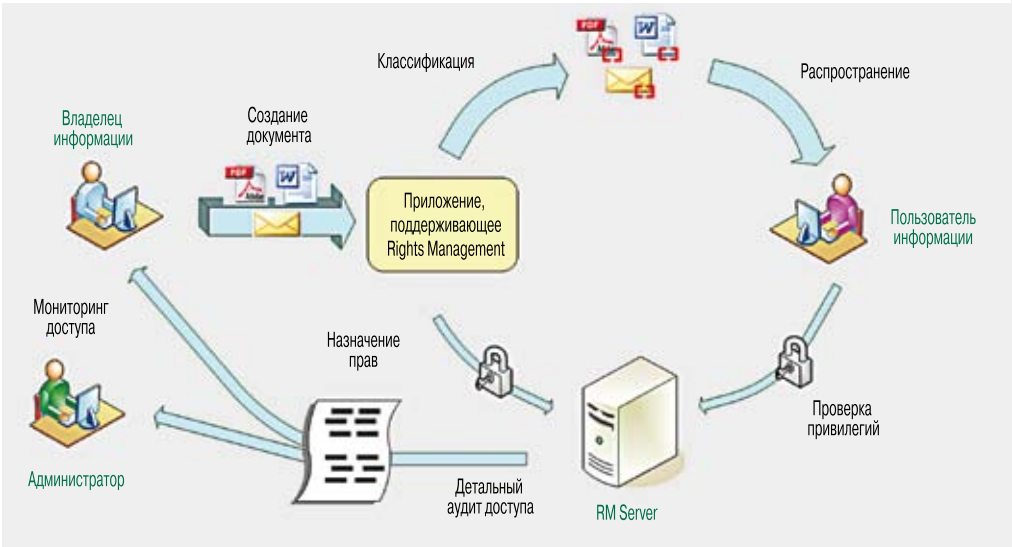
Алексей СОВА,
компания
«Информзащита»

Однажды в далеком 2003 г. Стив Баллмер, главный исполнительный директор Microsoft, долго искал один важный документ. И был совсем не рад, когда нашел его на одном из внутренних серверов в открытом виде. Правда это или нет, никто не скажет, но именно компания Microsoft одной из первых создала программный продукт для управления доступом к содержимому документов – Windows Rights Management Services (RMS). Поскольку задачи ограничения доступа к конфиденциальным документам стоят не только перед Microsoft, разработка была выпущена в виде коммерческого продукта и какое-то время была единственной на рынке. Сегодня существует уже несколько успешных реализаций таких систем от крупных производителей программного обеспечения – EMC Documentum, Oracle, HP, Liquid Machines.

Системы класса Rights Management (управление правами доступа) во многом схожи между собой. В их основе лежит шифрование защищаемой информации и разграничение доступа к содержимому документов на основе ролевой модели. Как правило, используется клиент-серверная архитектура (см. рисунок), в которой сервер отвечает за хранение политик, ключей шифрования, аутентификацию пользователей, а клиентские модули обеспечивают применение политики к той или иной информации, а также взаимодействие с сервером.

После создания документа автор при помощи клиентского приложения обращается к серверу. Это можно делать как в ручном режиме прямо из приложения, в котором создан документ (MS Office, редакторы изображений, CAD и др.), так и в автоматическом, например при получении документа из базы данных. Клиентский модуль устанавливает защищенное соединение с сервером. Пользователь после прохождения аутентификации выбирает требуемые параметры защиты документа («гриф

Типовая архитектура системы Rights Management



секретности»). Для аутентификации могут использоваться существующие механизмы, включая LDAP, процедуру регистрации Windows, аутентификацию на основе имени пользователя и пароля, веб-аутентификацию, цифровые сертификаты и токены. Затем сервер случайным образом генерирует ключ, сохраняет его локальную копию и копию политики и отправляет ключ клиентскому приложению. Клиентский модуль шифрует (или, по терминологии компании Oracle – запечатывает) документ соответствующим ключом шифрования, а затем удаляет его. Таким образом, ключ и политика хранятся только на сервере. У пользователя остается лишь зашифрованный документ, ему не доступны ни ключ, ни исходный документ.

Запечатанный документ можно безопасно распространять любым удобным способом – отправлять по электронной почте, выкладывать на сервер, передавать на съемном носителе.

При попытке получателя открыть защищенный документ автоматически вызывается клиентский модуль системы. Модуль устанавливает защищенное соединение с сервером, обеспечивает аутентификацию пользователя и посылает запрос на получение ключа шифрования. При успешном прохождении аутентификации сервер отправляет клиенту ключ и набор политик. Клиентский модуль ограничивает возможности приложения, используемого для работы с документом, в соответствии с политикой, расшифровывает документ, отображает его на экране и незамедлительно уничтожает дешифрованный документ и полученный ключ. Защищенное соединение, которое устанавливается между клиентским модулем и сервером, имеет два уровня защиты. Во-первых, это зашифрованный с помощью SSL канал, что гарантирует аутентификацию сервера и защиту передаваемой информации. Во-вторых, внутри SSL-туннеля создается еще один туннель на уровне приложений для обмена ключами шифрования документов.

В повседневной деятельности любой организации системе управления правами доступа к документам можно найти множество применений:

- **Рассылка писем руководства внутри компании.** Сотрудники могут читать защищенное письмо, но не могут его копировать, сохранять, редактировать или пересылать.
- **Работа в группе.** Руководитель группы устанавливает ограниченные права доступа к документам и назначает срок действия этих прав. По истечении установленного времени доступ к документам прекращается.
- **Публикация конфиденциальных данных на корпоративном портале.** Доступ обеспечивается через стандартный веб-браузер; данные можно просмотреть, но нельзя распечатать, скопировать или вставить в другую программу.
- **Работа с партнерами и контрагентами.** На доступ к документу накладываются ограничения, предотвращающие его передачу сторонним лицам и устанавливающие разрешенное время доступа. Уполномоченные сотрудники заказчика могут только ознакомиться с переданным документом и высказать свои пожелания.

Основное достоинство систем управления правами доступа – это повышение безопасности. Но есть еще два параметра, по которым продукты от разных производителей могут различаться достаточно сильно, – это удобство использования и управляемость. В этом плане Oracle Information Rights Management (IRM), например, выигрывает у Windows Rights Management Services (RMS), поскольку в IRM можно оперировать группами документов, пользователей и администраторов, а не устанавливать права отдельно для каждого документа или пользователя, как в RMS. С учетом того, что внедрение таких систем, как правило, происходит на этапе, когда пользователей уже много, а документов еще больше, работа с группами серьезно сокращает затраты.

Однако какой бы выбор ни был сделан, установка подобной системы существенно снижает риск утечки конфиденциальной информации. Это обеспечивается за счет шифрования данных, контроля действий, производимых с документом (печать, копирование, пересылка), регистрации событий доступа к информации и возможности централизованно изменить или аннулировать доступ к документу, даже если он уже вышел за пределы контролируемого периметра. ИКС

Установка системы управления правами доступа существенно снижает риск утечки конфиденциальной информации

Симметричный ответ на новые угрозы безопасности

Новые виды сетевых угроз требуют комплексной защиты в режиме реального времени. Radware готова такую защиту предоставить.

Новые тенденции в области атак

За последние годы значительно расширился круг потребителей, имеющих онлайновый доступ к корпоративным сетевым ресурсам, – это клиенты, партнеры, поставщики и вообще любые пользователи Интернета. Доступность сети превратилась в фактор, провоцирующий злоумышленные атаки. Тем не менее система защиты сетевой инфраструктуры, обеспечивая безопасность коммуникаций, не должна их ограничивать.

Системы предотвращения вторжений (IPS) сличают сигнатуры (образцы известных атак на разного рода уязвимости) с входящим сетевым трафиком и блокируют трафик, который выглядит нежелательным.

Лазейка, используемая хакерами, – это легитимные виды коммуникаций, отвечающие правилам приложений и незаметные для систем сетевой защиты, отслеживающих превышение пороговых объемов трафика или сигнатуры атак. Многие современные угрозы сетевой безопасности имеют динамическую природу, и с ними нельзя справиться с помощью статических устройств IPS на основе сигнатур. Эти угрозы в целом не связаны с необычно большим объемом трафика, не содержат нелегитимных запросов к приложениям и не используют уязвимости в программном обеспечении.

В попытке противостоять этим новым типам угроз администраторы сетей стараются реактивно просматривать журналы регистрации и вручную устанавливать фильтры и пороговые значения трафика для сдерживания атак. Но если установить слишком жесткие ограничения, то нормальные пользователи будут лишены доступа, а слишком мягкие ограничения не защитят корпоративную сеть от атак. В то же время немногие предприятия готовы непрерывно заниматься такой тонкой настройкой.

Для успешной борьбы с современными угрозами необходимы новые технологии предотвращения вторжений, дополняющие существующие IPS на основе сигнатур.

Эффективная система защиты должна автоматически определять и отражать широкий спектр атак в режиме реального времени, не оказывая негативного влияния на работу обычных пользователей. Поскольку модели прохождения нормального сетевого трафика часто изменяются, система должна быстро адаптироваться к происходящему без участия администратора.

Механизмы автоматического обнаружения должны различать нормальное и ненормальное поведение пользователя, даже если разница в поведении не очень велика.

На случай неправильной оценки какого-либо трафика система защиты должна иметь механизм самокоррекции для сведения к минимуму ошибочного доступа к сети.

Более того, система должна выбрать оптимальный метод реагирования, чтобы остановить атаку с минимальным участием администратора. Реагирование должно динамически самостоятельно подстраиваться под изменение условий и параметров атаки.

Угрозы и риски на уровне сети

Угрозы на уровне сети включают атаки, приводящие к неправильному функционированию сетевых ресурсов. Довольно старый, но до сих пор применяемый метод использования слабых мест в IP-инфраструктуре – атака DDoS (распределенная атака типа «отказ в обслуживании»).

Атаки DDoS обычно подразумевают проникновение в сотни или тысячи компьютеров в Интернете. Такое проникновение может осуществляться вручную или автоматически, с помощью, например, червей или других вредоносных программ, которые распространяются самостоятельно или могут быть загружены пользователем по неосторожности. Любой уязвимый компьютер может быть инфицирован, и после успешного взлома на нем устанавливаются вредоносные средства для DDoS и бот, с помощью которого хакер контролирует все зараженные машины и координирует производимые с них атаки.

Увеличение числа ботов приводит к росту сетевых атак типа DoS. Такие атаки обычно отнимают стековые ресурсы оперативной памяти, загружают маршрутизаторы и коммутаторы ненужной обработкой и/или потребляют пропускную способность, мешая нормальным коммуникациям в атакованной сети.

Кроме переполнения, ведущего к отказу в обслуживании, угрозы сетевого уровня включают традиционные атаки против слабых мест в операционной системе. Каждый элемент сети, будь то маршрутизатор, коммутатор или защитный экран, имеет свой набор уязвимостей. Если любая из уязвимостей используется злонамеренно, то вся IP-инфраструктура подвергается опасности и могут быть нарушены функционирование соответствующего элемента сети и целостность бизнес-процессов.

Угрозы и риски на уровне сервера

Угрозы на уровне сервера четко подразделяются на две категории: атаки на уязвимости в стеке TCP/IP и атаки на уровне приложений.

Атаки на уязвимости в стеке TCP/IP направлены на транспортные ресурсы сети, они создают помехи нормальному установлению TCP-соединений и транзакциям приложений, для которых эти соединения ис-

пользуются (например, транзакции HTTP, загрузка файлов по FTP, почтовые сообщения и т.д.). Довольно просто полностью занять ресурсы TCP на сервере с помощью нескольких видов атак, например, переполнения TCP Syn или заданием слишком большого числа TCP-соединений. Атака последнего вида легко реализуется, и ее нельзя эффективно отследить и предотвратить с помощью основной массы существующих решений сетевой безопасности. Такая атака, потребляющая большой объем серверных TCP-ресурсов, может прервать или сильно затруднить работу серверов. Этот вид атак необязательно имеет большие размеры, что усложняет его обнаружение и предотвращение.

Так же, как и в случае атак сетевого уровня, угрозы для стека TCP/IP включают и более традиционные атаки на работу операционной системы. Каждая из общеупотребительных ОС имеет свои уязвимости, использование которых ухудшает работу сервера и опасно для приложений.

Атаки уровня серверных приложений

Угрозы для серверных приложений с использованием уязвимостей – наиболее распространенный тип атак. Если атаки направлены на заранее известные уязвимости приложений, то более или менее понятно, как с ними бороться. Но когда в программном обеспечении обнаруживается новая уязвимость, хакер может воспользоваться этим слабым местом прежде, чем производитель программы или разработчик средств безопасности сумеет защититься от атаки, распознав ее сигнатуру или выпустив программную заплатку, закрывающую эту уязвимость. Атака, происходящая в то время, пока разрабатываются средства защиты или заплатки, относится к типу zero minute.

Типичные категории известных атак и атак zero minute уровня серверных приложений включают в себя атаки на уязвимости, связанные с переполнением буфера, внедрение SQL-кода, XSS – межсайтовый скриптинг, руткиты и «черви».

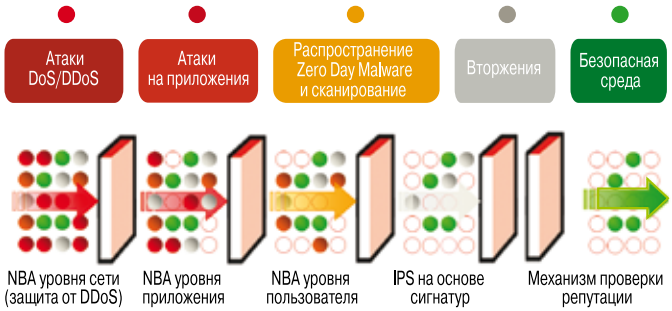
Угрозы серверным приложениям, не связанные с уязвимостями, нацелены на слабые места в серверных приложениях, которые не подпадают под определение уязвимости. Для этих угроз характерна последовательность легитимных событий, с помощью которых взламывается сервер (точнее, механизмы аутентификации), и приложение сканируется на предмет обнаружения уязвимостей. Эти уязвимости в дальнейшем могут использоваться для получения контроля над работой приложения. Более сложные виды атак, не связанных с уязвимостями, состоят из специально подобранных повторяющихся комбинаций легитимных запросов к приложению, которые злоупотребляют ресурсами памяти и процессора сервера, приводя приложение в состояние частичного или полного отказа в обслуживании.

По мнению исследовательского агентства IDC, «хакеры продолжают искать способы злоупотребления чужим программным обеспечением. Когда-то они использовали уязвимости, но теперь найдены возможности получения контроля над ПО без уязвимостей».

Эти развивающиеся угрозы серверным приложениям, выглядящие как обычные запросы, не обязательно связаны с большим объемом трафика, что позволяет хакерам смешаться с потоком полностью легитимных коммуникаций, соответствующих правилам приложения, так что системы сетевой безопасности не распознают действия вредителей с точки зрения пороговых значений трафика или известных сигнатур атак.

Такие атаки производят сканирование приложений, прямой подбор пароля и подбор по словарю, переполняют приложение сессионными запросами, а также устанавливают в зараженной системе боты, способные интегрировать разные средства атаки и угрожать приложениям.

Предотвращение атак – разные уровни защиты



Новые методы защиты

Чтобы выявить и предотвратить сегодняшние и будущие атаки, устройство Radware DefensePro, кроме детерминистского подхода защиты от известных атак с помощью проактивных обновлений сигнатур и ограничения трафика с аномальным объемом и неправильным использованием протоколов, реализует уникальный метод. Преимущество Radware – это метод автоматической генерации сигнатур в реальном времени для предотвращения атак zero minute, не основанных на уязвимостях, без вмешательства администратора сети. Сигнатуры создаются в реальном времени специальным механизмом принятия решений на основе методов fuzzy logic, позволяющих точно определять и останавливать атаки за считанные секунды. Механизм опирается на данные модулей поведенческого анализа, исследующих трафик на уровне клиента, сервера и сети и посылающих оповещения встроенной системе отражения атак при обнаружении аномальных моделей.

Эффективно обезопасить сеть современного предприятия можно только с помощью высокотехнологичных решений, интеллектуально применяющих комплексные методы защиты и не препятствующих легитимной работе корпоративных приложений.

На весах инноваций и традиции

Производители оборудования и проектировщики дата-центров постоянно предлагают рынку новые и с разных точек зрения более эффективные технологические решения для инженерной инфраструктуры ЦОДов. Но далеко не каждый владелец ЦОДа согласится на эксперименты с непроверенными технологиями. Интриги выбору решений для дата-центров добавляют и превратности климата.

Об извилистых путях внедрения новых технологий на объектах, от которых требуется бесперебойная работа, шла речь на круглом столе «Инженерные решения для ЦОДов: инновации или традиции?», организованном журналом «ИКС» совместно с компаниями КРОК и APC by Schneider Electric.

Каштаны из огня

Слово «инновации» сейчас в моде, и никто не спорит, что инновации крайне важны для развития информационных технологий, но, как подчеркнул генеральный директор компании ADM Partnership Максим Иванов, ЦОД в подавляющем большинстве случаев – ответственный объект, который должен обеспечивать заданный, и часто очень высокий, уровень надежности и функциональности. Стремление инженеров попробовать применить на практике новые оригинальные технологические идеи вполне понятно, но на другой чаше весов обычно лежат требования заказчика, который не хочет рисковать без весомых на то оснований, в первую очередь экономических.

Максим ИВАНОВ: «Это лето подарило нам шанс задуматься о том, каков запас прочности у наших ЦОДов»

Ответ на вопрос о том, где проходит грань разумного риска, для каждого ЦОДа приходится искать заново. В стане «осторожных консерваторов» вполне ожидаемо находятся крупные организации, чей бизнес весьма критичен к простоям дата-центров. Это подтверждают слова директора проектов управления технических средств и телекоммуникаций Сбербанка России Дмитрия Рожнова: «Мы стремимся к инновациям, но это не первоочередная задача. Основной критерий нашей работы – надежность».

Не столь категоричны компании, для которых критически важны экономическая эффективность всего бизнеса и снижение операционных расходов. К последним как раз относятся затраты на электроэнергию. Как сказал директор по строительству компании «МегаФон» Виталий Дубинин, классические технологии, конечно, позволяют спать спокойно, но бизнес требует эффективности и, значит, внедрения соответствующих энергосберегающих технологий. Правда, «МегаФон» как компания, имеющая дата-центры разных размеров в разных регионах страны, может себе позволить проводить эксперименты на новых площадках, а потом обкатанные технологии внедрять в своих крупных ЦОДах.

Экспериментами занимается и компания КРОК, которая, будучи системным интегратором, предлагает заказчикам новые решения, уже испытанные на себе. Как сообщил заместитель директора департамента интеллектуальных зданий КРОК Александр Ласый, сейчас компания строит два дата-центра, и меньший из них станет полигоном для тех инновационных решений, которые в дальнейшем планируется тиражировать.

Ну а большинство владельцев ЦОДов, в первую очередь корпоративных, предпочитают учиться на чужих ошибках: «каштаны из огня пусть таскает кто-нибудь другой, а мы пока поглядим».

Вместе с тем на рынке дата-центров появился целый ряд решений и технологий, уже долгое время работающих в совсем других отраслях. В качестве примеров генеральный директор компании «Ди Си квадрат» Александр Мартынюк привел динамические дизельно-роторные ИБП, которые несколько десятков лет используются в качестве источников электропитания в армиях многих стран мира, и системы отвода тепла на морской воде, давно применяемые компаниями, ведущими шельфовую добычу полезных ископаемых. Аналогичными «пришельцами» в мире ЦОДов являются и некоторые технологии кондиционирования и охлаждения, в частности всем нынче известные роторные теплообменники компа-

нии Kyoto Cooling. С одной стороны, эти технологии проверены временем и многочисленными инсталляциями, но с другой стороны, для данного рынка они новые, и отношение к ним, как и к любым другим новинкам, довольно осторожное.

Только для больших

Удерживает от внедрения новых технологий, в частности дизельно-роторных ИБП и фрикулинга, также и то, что их применение экономически оправдано пока только в крупных по российским понятиям ЦОДах с подводимой мощностью не менее 1 МВт. В качестве показателя энергоэффективности дата-центров часто используют коэффициент PUE, который все стараются максимально снизить. За рубежом уже есть ЦОДы, где он равен 1,12 и даже 1,08. Однако руководитель подразделения Schneider Electric Datacenter Solution Team Алексей Солодовников предупреждает, что подобных значений PUE можно достичь лишь в мультимегаваттных ЦОДах, так как на максимально высокие уровни энергоэффективности современные системы электропитания и холодоснабжения выходят лишь при мощностях в несколько мегаватт. На малых системах, к которым относится подавляющее большинство российских дата-центров, где мощность 1 МВт все еще редкость, таких величин PUE достичь невозможно. В небольших ЦОДах пока лучше и дешевле действовать с другой стороны: с помощью виртуализации повышать загрузку серверов с традиционных 10–15% до 50–60%. Кроме того, обладателям даже крупных дата-центров стоит помнить, что повышать энергоэффективность ЦОДа без ущерба для операционной устойчивости можно только до определенного предела, а основная задача этого объекта – все-таки обеспечение непрерывности бизнеса, а не экономия электроэнергии.

Владельцам небольших российских ЦОДов хотелось бы посоветовать не ждать, когда новые технологии «спустятся» до уровня массового рынка, а использовать опыт таких же небольших зарубежных дата-центров (ведь на Западе есть не только «монстры» на многие десятки мегаватт). ЦОДов там намного больше, чем у нас, соответственно, наработана хорошая статистика применения разных решений. К тому же то новое оборудование, которое привозят к нам зарубежные вендоры, к моменту его появления в России, как правило, уже имеет немало инсталляций в Европе и США, и этот опыт позволит минимизировать испытания на себе.

Александр ЛАСЫЙ: «Несмотря на глубокие изменения на рынке услуг ЦОДов за последние три-четыре года, оценка рисков при строительстве дата-центров остается серьезной проблемой»

Гром не грянет...

Долгое время относительно низкая стоимость электроэнергии у нас в стране была тормозом для внедрения новых энергоэффективных технологий в дата-центрах, но усилия российских энергетиков по постоянному повышению тарифов заставили многих заинтересоваться достижениями прогрессивной технической мысли. Кроме того, недавно в России появился еще один стимул к инновациям, а заодно и к ужесточению требований к надежности инфраструктуры ЦОДов. Речь идет об испытаниях, которым подверглись многие дата-центры из-за сильных морозов зимой и аномальной жары летом 2010 г. Во-первых, они показали, что уровень проектирования и строительства российских ЦОДов за последние годы заметно повысился: ни одной крупной аварии во время долгой летней жары зафиксировано не было, хотя в предыдущие годы аварии случались и при более низких температурах.

Дмитрий РОЖНОВ: «Мы стремимся к инновациям, но это не первоочередная задача. Основной критерий нашей работы – надежность»

Во-вторых, погодные эксцессы заставили задуматься о запасе прочности оборудования систем охлаждения дата-центров не только сотрудников служб эксплуатации, но и руководителей компаний. Практически всем стало ясно, что при строительстве и реконструкции ЦОДов необходимо учитывать климатические реалии, а температурные рекорды этого московского лета должны стать весомым аргументом при обосновании бюджетов на строительство или модернизацию. Кроме того, превратности климата показали правильность требований стандарта TIA-942 к системам кондиционирования и охлаждения ЦОДов: они должны быть рассчитаны на максимальную и минимальную температуры воздуха, зафиксированные в данном регионе. Как отметил директор компании «Вентспецстрой» Петр Ронжин, выполнение этих требований раньше ставило его компанию в заведомо худшие условия при переговорах с заказчиками, поскольку «правильные» системы стоили дороже. Но теперь стало очевидно, что только такой подход позволяет создавать действительно отказоустойчивые дата-центры. С ним согласен и А. Ласый: заказчики, которых в свое время не удалось убедить в том, что при проектировании серверных комнат и дата-центров нужно закладываться на температуры выше +35°C летом и ниже –35°C зимой, теперь готовы переделать свои системы с учетом новых климатических условий.

Многие компании уже корректируют корпоративные требования к системам охлаждения. Например, в новом варианте технического задания на строительство ЦОДа Московской объединенной энергетической компании в требованиях к системе кондиционирования фигурирует температурный диапазон от –40 до +45°С. Правда, ИТ-отделу МОЭК еще предстоит экономически обосновать эти требования перед руководством компании, и это, скорее всего, будет нелегко. Как констатировал А. Ласый, несмотря на глубокие изменения на рынке услуг ЦОДов, произошедшие за последние три-четыре года, оценка рисков при строительстве дата-центров остается серьезной проблемой, и российский принцип «гром не грянет, мужик не перекрестится» по-прежнему незыблем.

А В. Дубинин напоминает, что помимо «правильных» параметров, прописанных в ТЗ, необходима еще и правильная эксплуатация: системы кондиционирования и охлаждения должны работать на уровне 0,6–0,7 максимальной мощности, а кроме того, их надо периодически тестировать при максимальной нагрузке, чтобы можно было спрогнозировать их возможный выход из строя и заранее подготовиться к этому событию.

О пользе озеленения

Еще одна модная тема мира ЦОДов – «зеленые» технологии охлаждения, т.е. различные варианты фрикулинга, охлаждение «воздух–воздух», роторные теплообменники и др. Долго мы считали их прихотью богатых иностранцев, но вот наконец эти технологии (правда, не без дополнительного стимула со стороны растущих цен на электричество) начали активно прокладывать себе дорогу в России. В числе первых ласточек оказались, в частности, те дата-центры, у которых были крупные проблемы из-за перегрева серверов прошлым летом. По мнению А. Мартынюка, целый ряд московских ЦОДов выдержал летние испытания именно благодаря «зеленым» технологиям.

Что же касается решений с фрикулингом, то проектировщики предлагают их российским заказчикам уже несколько лет, и эти попытки приобщения к новым технологиям становятся все более успешными. Их использование несколько удорожает проект, но повышение цены теперь нормально воспринимается заказчиками, которых убеждают цифры времени работы системы в режимах с использованием компрессоров, с частичным и полным фрикулингом, а также расчеты соответствующих последствий для энергопотребления и предстоящих операционных расходов.

Алексей СОЛОДОВНИКОВ: «Следует помнить, что рекордных значений PUE можно достичь лишь в мультимегаваттных ЦОДах»

Реализованы в России и первые решения с системой охлаждения типа «воздух–воздух» (одно из них, как и следовало ожидать, установлено в довольно прохладном месте, в Нижневартовске). Правда, А. Ласый, подтверждая высокую энергоэффективность подобных систем охлаждения, предупреждает, что для гарантии высокой надежности функционирования ЦОДа заказчик должен предусмотреть возможность резкого увеличения энергопотребления при пиковых нагрузках в случае высоких забортных температур, ведь в этой ситуации придется задействовать всю резервирующую систему охлаждения с чиллерами и фреоновыми кондиционерами, а для этого понадобятся автономные источники энергоснабжения соответствующей мощности.

Но в принципе для повышения эффективности систем охлаждения дата-центров есть совсем простые и очень недорогие решения, которые можно отнести к «зеленым» технологиям хотя бы по причине отсутствия вредного воздействия на окружающую среду. Например, Альфа-банк летняя жара подвигла на покраску крыши дата-центра в белый цвет, что привело к снижению температуры воздуха на входе установленных там внешних блоков кондиционеров на 20°С (!). Кроме того, выносные блоки чиллеров были закрыты от прямых солнечных лучей решетками, подобными тем, что в течение столетий устанавливают на окнах в жарких странах.

В общем, вековые «лучшие практики» сохраняют свою актуальность и сегодня. Вывод из всего этого напрашивается один: для повышения эффективности работы дата-центров требуются прежде всего умственные усилия.

Евгения ВОЛЫНКИНА

Найти и больше не терять

Илья ЕХРИЕЛЬ, технический директор НТЦ «СевенТест», канд. техн. наук
Инна РОЗЕНЦВАЙГ, руководитель отдела информации и маркетинга НТЦ «СевенТест»

Некорректное приземление трафика, незаконное предоставление конечным абонентам услуг МГ/МН-связи, взлом VoIP-узла – вот неполный список угроз потоку доходов оператора связи. Для борьбы с любыми видами мошенничества наиболее эффективны проактивные системы гарантирования доходов.

Украсть или сэкономить?

В соответствии с действующей трехуровневой структурой сетей связи терминация междугородного и международного трафика осуществляется последовательно через три уровня: МГ/МН-сеть – зоновая сеть – местная сеть. Если в регионе на зоновом уровне работают несколько операторов, то порядок прохождения трафика определяется договорами между ними. Обычно такие договоры предусматривают более высокие тарифы на терминацию трафика на зоновом уровне по сравнению с местным. Существенная разница в тарифах и желание сэкономить провоцируют присоединенных операторов, работающих одновременно на местном и зоновом уровнях, хотя бы частично терминировать МГ/МН-трафик других операторов под видом местного, нарушая условия договора.

Потери от таких действий партнеров несут в основном МРК «Связьинвеста», которые работают в регионах как на местном, так и на зоновом уровне и имеют многомиллионную абонентскую базу. Одновременно в тех же регионах существуют альтернативные операторы, взаимодействующие с МРК на местном уровне, которые чаще всего и «грешат» непредусмотренной договорами взаимодействия терминацией на местном уровне межзонового трафика других операторов (вызовов от абонентов сотовой связи, МГ/МН-вызовов). Так, по сообщению пресс-службы «Северо-Западного Телекома», «корректное приземление МН/МГ-трафика на сеть СЗТ может дать компании дополнительный доход в объеме от пятидесяти до нескольких сотен миллионов рублей в год».

Однако некорректный пропуск трафика может наносить ущерб и другим операторам связи с обширной абонентской базой и вызывать конфликты между участниками рынка. Причем судебные решения по этим конфликтам зачастую весьма противоречивы. Например, один оператор прекратил прием вызовов от сети сотовой связи, пропускаемых местной сетью. Россвязьнадзор, рассмотрев этот конфликт, признал действия оператора обоснованными, так как в договоре о пропуске трафика на местном уровне между ним и местной сетью был оговорен диапазон номеров, чей трафик может пропускаться через данное присоединение. Ресурсы нумерации, принадлежащие сетям сотовой связи, а также фиксированным сетям, относящимся к другим географическим зонам, в этот диапазон не входили.

В другом случае одна из МРК ограничила пропуск к своим абонентам трафика от абонентов сотовой сети, терминируемого через узел местной связи альтернативного оператора. При этом в договоре, заключенном между ними, отсутствовали положения, запрещающие альтернативному оператору оказывать другим операторам, в том числе сотовым, услуги по пропуску трафика на сеть местной телефонии. В этой ситуации УФАС признало МРК нарушившей антимонопольное законодательство.

Как мы видим, операторам следует, с одной стороны, внимательно относиться к заключению договоров межоператорского взаимодействия, а с другой – контролировать соблюдение порядка пропуска трафика, а при необходимости обладать вескими доказательствами его нарушения.

Требуются сложные критерии поиска

В бизнес-структуре оператора связи функции контроля за порядком пропуска трафика, как правило, делятся между подразделением безопасности (которое обычно осуществляет и фрод-контроль) и отделом межоператорских отношений.

Основная задача очевидна – выявить точки потенциальной утечки доходов и зафиксировать факт нелегитимного использования сетевого ресурса и/или неверную тарификацию такого использования. Большой объем данных и необходимость постоянного контроля в реальном времени подразумевает применение автоматизированных систем. Эти системы, относящиеся к классу фрод-менеджмента (Fraud Management System, FMS), могут опираться на информацию из файлов CDR (Call Detail Record) двух типов:

- от систем пассивного мониторинга, формирующих CDR на основе сигнальной информации;
- от коммутаторов, систем предбиллинга или биллинга.

Системы, использующие информацию первого типа, способны обнаружить любые потери, так как от системы пассивного мониторинга никакие вызовы скрыть невозможно. В то же время АТС вследствие определенных настроек конфигурационных параметров или изменения информации в самих записях CDR могут при формировании CDR-файлов – главного источника данных для биллинга – исключать некоторые записи и/или выдавать ошибочные и сбойные записи. В этом случае никакие дальнейшие усилия по их обработке точного результата не дадут.

CDR, получаемые от системы пассивного мониторинга, отличаются от станционных как по количеству, так и

по информативности. Расхождение между количеством станционных CDR (т.е. учтенных в предбиллинге и биллинге) и CDR, зафиксированных пробниками, может достигать 15–20%. CDR, сформированные в АТС, обычно имеют меньшее число полей по сравнению с CDR от пробников, которые могут содержать не только информационные поля, но и сами сигнальные сообщения для последующего побитового декодирования.

Еще одно достоинство решений первого класса – доступ к любой записи CDR в реальном времени, вне зависимости от завершенности или незавершенности вызова, в то время как большинство АТС формируют CDR только по завершении вызова. Обработка CDR в реальном времени позволяет оперативно рассчитывать показатели эффективности бизнеса оператора, например, зарегистрировать резкое уменьшение числа вызовов от определенного направления, падение доходов по заданному региону или недостаточный возврат инвестиций по определенному проекту.

Описанные системы выполняют мониторинг различных параметров вызова – A- и B-номеров (вызывающего и вызываемого абонентов), длительности, даты/времени, транк-группы, коммутатора, кодов OPC и DPC и т.д. – с целью обнаружения фрода и утечек, вызванных непреднамеренными ошибками, а также потерями/искажением данных при их формировании и передаче между подсистемами обработки CDR. На основе этой информации, дополнительных данных из абонентских баз, а также предустановленных фильтров, критериев и профилей производится анализ и выявление подозрительных фактов.

Кроме несанкционированного трафика, системы FMS обнаруживают и другие, актуальные сегодня виды фрода, например:

- Незаконное оказание услуг МГ/МН-связи конечным абонентам путем создания неоговоренных договором узлов услуг, например модемных пулов. Смежный оператор получает предоплату с абонентов оператора за предоставление услуг с добавленной стоимостью, а затем выставляет счет оператору, к которому подключен абонент, за услугу завершения вызова на этот модемный пул. В результате оператор несет прямые финансовые потери, поскольку вместо получения средств от смежного оператора за инициацию вызова к узлу услуг оператор платит ему как за завершение местного вызова.
- Мошенничество, связанное с предоставлением абоненту услуг интеллектуальной сети (коды 800, 803, 809).
- Взлом УПАТС клиента. В этом случае ущерб напрямую несет не оператор, но он рискует потерять важного клиента вследствие негарантированной безопасности связи. Зачастую клиент предъявляет доказательства того, что эти вызовы – результат взлома, и обоснованно отказывается оплачивать счета.
- Взлом VoIP-узла – ситуация, аналогичная предыдущей, только пострадать могут и узлы самого оператора.

Мошенничество может выявляться по явным критериям, например незаконное приземление трафика – путем обнаружения вызовов с нелегитимных для данного направления A-номеров. Такая работа выполняется системами фрод-менеджмента с помощью алгоритмов поиска на основе настраиваемых правил.

Однако операторы могут маскировать нелегальный трафик, как полностью убирая из него информацию об источнике, так и заменяя истинные A-номера номерами из своего диапазона. В таких случаях необходимы системы фрод-менеджмента, способные реализовывать более сложные, многоступенчатые аналитические методы поиска (см. таблицу), выявляющие трафик, который соответствует одному или нескольким статистическим признакам.

Контрольные вызовы – не панацея

Для обнаружения нелегальной терминации трафика давно применяется и метод прямого тестирования. Он заключается в непосредственном отслеживании маршрута, которым приходят в сеть оператора тесто-

Критерии выявления мошенничества

Вид фрода	Признаки
Приземление трафика	1. Аномально большое число вызовов с одного A-номера или без информации о вызывающем абоненте. 2. Аномальное соотношение входящего и исходящего трафика (минимальное количество входящего трафика) в целом для оператора и/или для групп A-номеров, выявленных по первому признаку. 3. Вызовы с нелегальными для данного направления A-номерами или без информации об A-номере
Подмена номера	1. Вызовы на B-номера вида $7x_1x_2...x_n$, которые выходят из сети с модифицированными B-номерами вида $x_1x_2...x_n$ (т.е. уже без 7). 2. Вызовы на B-номера вида (код страны)$x_1x_2...x_n$ длиной от 10 до 14 знаков, которые возвращаются обратно в сеть оператора с другим A-номером. 3. Вызовы на B-номера вида (код страны)$x_1x_2...x_n$ длиной от 10 до 14 знаков, которые возвращаются в сеть с модифицированными B-номерами (код страны изменен на префикс кода города РФ)
Взлом УПАТС	1. Аномальный объем исходящего МГ/МН-трафика с одного A-номера за сутки. 2. Аномальный объем входящего трафика на номера клиента за сутки. 3. Разрешенные/запрещенные направления (коды стран, МГ-префиксы) вызовов или B-номера. 4. Аномальный профиль клиента (например, вечерние и ночные МГ/МН-вызовы для бизнес-клиента)
Незаконный узел услуг	1. Аномальное количество вызовов на B-номера смежного оператора или аномальное количество длительных вызовов. 2. Минимальное количество различных номеров или префиксов вызывающей стороны (A), с которых осуществлялись вызовы на зафиксированный номер(а) B (такой критерий необходим для исключения ложного срабатывания в тех случаях, когда большое число вызовов на номера B не связано с предоставлением массовой услуги, например, входящих вызовов на групповой номер в крупной организации). 3. Несоответствие номера «белому» списку номеров (задаваемому для исключения ложных срабатываний, связанных с легальными узлами услуг)

вые МГ/МН-звонки. В процессе тестирования собирается детальная информация о совершенных звонках (CDR) как в исходной точке звонка (зарубежная сеть), так и в конечной точке (сеть тестируемого оператора).

Аргумент в пользу контрольных вызовов – дешевизна одной проверки. Однако поскольку такие проверки должны проводиться с определенной периодичностью, то общая стоимость этого метода не столь уж мала.

Говорить о высокой эффективности метода контрольных вызовов не приходится, так как по сути своей он – разовая мера, способная обнаружить лишь незначительное число точек нелегальной терминации трафика. Причина низкой эффективности еще и в том, что необходимым условием проведения контрольных вызовов является согласие на такое взаимодействие операторов, в том числе зарубежных. То есть метод требует предварительных согласований и неких технических подготовительных мероприятий. Очевидно, что быстро организовать такую проверку и сохранить ее в тайне невозможно, так как велик риск утечки инсайдерской информации. Следовательно, большинство злоумышленников на время проверки прекратят свою деятельность, а по ее окончании спокойно возобновят – до следующего раза.

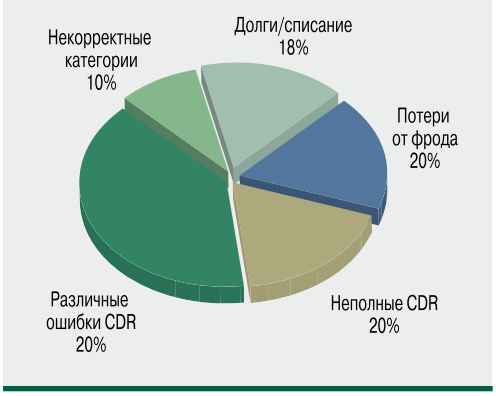
Существуют комбинированные методы, в которых тестовые вызовы регулярно генерируются автоматически и отслеживаются системами FMS. При этом преимущества автоматического контроля и прямого тестирования сохраняются и эффективность выявления фрода возрастает. Подобные методы могут выявлять не только уже свершившийся факт незаконного пропуска трафика, но и ситуации, когда такие махинации возможны, например, вызовы с неполной информацией об А-абоненте.

Другие виды потерь

Многофункциональность и гибкость новых видов услуг предполагают задание большого числа конфигурационных параметров при настройке оборудования. Давление рынка заставляет ускорять внедрение и модификацию услуг и производить их почти постоянно. Избежать ошибок при этом практически невозможно. А посему потери происходят на всех этапах предоставления услуги (рис. 1).

Потери могут вызываться ошибками (как умышленными, так и нет) при задании/модификации параметров услуг:

Рис. 1. Потери в течение цикла предоставления услуги связи



- неверными конфигурационными параметрами (прав абонентов, свойств транк-групп), приводящими к непопаданию информации о совершенных вызовах в станционный АМА-файл (файл автоматического учета сообщений) или ее искажению;
- неверными параметрами настройки систем предбиллинга и тарификации, что влечет за собой отсев вызовов без А-номеров или с А-номерами, которые не должны проходить по данной транк-группе;
- неверными параметрами конфигурации направлений, из-за чего могут проходить вызовы по транк-группам, которые по данным системы техучета отмечены как находящиеся в состоянии техобслуживания;
- вводом информации о новом клиенте в биллинговую систему с опозданием или сбоем при деактивации услуги и удалении записи о клиенте из биллинговой системы.

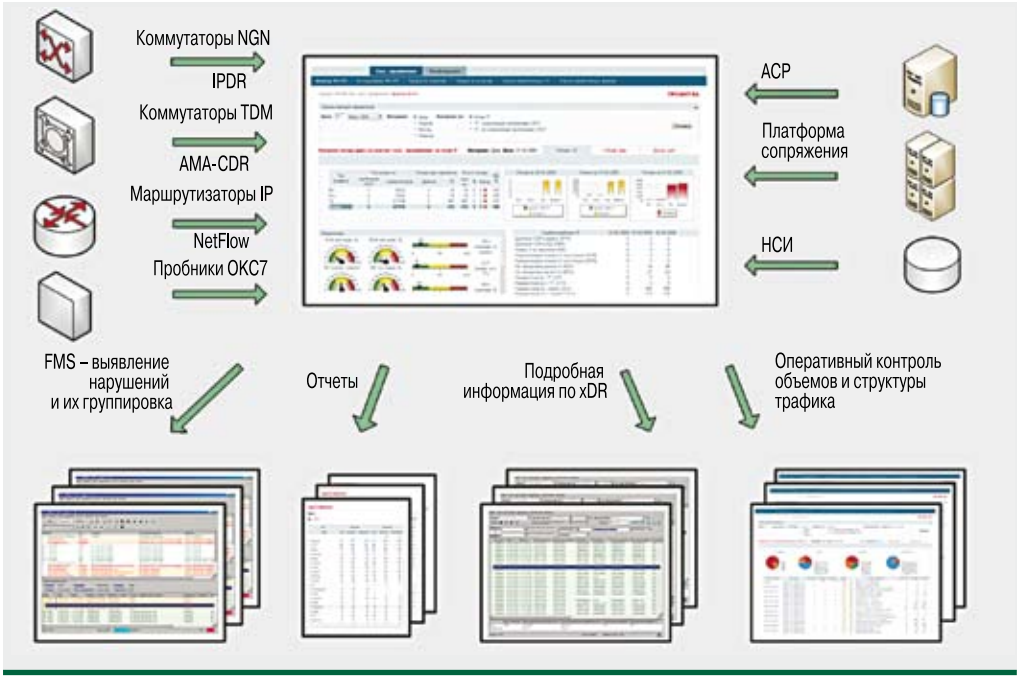
Наиболее эффективно выявлять такие потери и в ряде случаев предотвращать их позволяют системы автоматизированной сверки, которые с помощью проб независимо собирают записи CDR с сигнальной информацией и далее используют их в качестве эталонного источника при сравнении с данными АМА-файлов от коммутаторов. Сверку данных целесообразно проводить не только по выставляемым счетам (по исходящим вызовам), но и по счетам, получаемым от смежных операторов (по входящим вызовам), где случайно может быть указан объем услуг больший, чем реально оказанный.

Доходы можно гарантировать

Даже простое перечисление точек финансовых потерь оператора связи показывает, что для эффективного предот-

Операторам следует внимательно относиться к заключению договоров межоператорского взаимодействия и контролировать соблюдение порядка пропуска трафика, а при необходимости обладать вескими доказательствами его нарушения

Рис. 2. Вариант внедрения системы RA/FMS в инфраструктуру оператора



Сверку данных целесообразно проводить не только по выставляемым счетам, но и по счетам, получаемым от смежных операторов, где случайно может быть указан объем услуг больший, чем реально оказанный

вращения таких потерь необходим комплексный подход, подразумевающий не только обязательное внедрение единой программно-аппаратной системы, но и координацию действий различных подразделений для работы с этой системой.

Обеспечение полноты получения дохода требует соответствующей организации бизнеса, основанной на методах гарантирования доходов (Revenue Assurance, RA). Как и в других вопросах управления телекоммуникационным бизнесом, «законодателем мод» в этой области является Telecom Management Forum, который назвал RA новым перспективным элементом NGOSS.

По определению TMF, под RA понимают деятельность телекоммуникационной компании, направленную на то, чтобы рабочие процессы и технические системы, которые поддерживают бизнес оператора связи, всегда обеспечивали полноту, точность и правильность начисления платы за предоставленные услуги и ее сбор. При этом выделяют три подхода:

1. Реактивный:
- потери доходов обнаруживаются в результате периодических проверок;
- проблемы устраняются после их обнаружения;
- возможно повторное появление проблем.

2. Активный:
- места потери доходов обнаруживаются сразу после их возникновения;
- повторение в будущем единожды обнаруженных проблем не допускается;
- не допускается уменьшение доходов, но ничего не предпринимается для их увеличения.

3. Проактивный (упреждающий):
- предугадывается, где могут возникнуть потери доходов;
- предотвращается их возникновение;
- выявляются косвенные потери доходов.

Акцент на полноте собираемости доходов вызвал появление специализированных систем класса RA/FMS, обеспечивающих интеграцию функций автоматизации контроля прохождения данных по цепочке заказ – деньги (RA) и выявления злоумышленных действий со стороны недобросовестных операторов, жуликов и сотрудников компании (FMS).

Такие системы выполняют сбор и анализ эталонных CDR для сравнения с данными от коммутационного и биллингового оборудования, а также аналитические функции FMS для контроля поведения абонентов посредством статистических профилей. Для повышения оперативности системы формируют отчеты и тревожные сообщения подразделениям оператора, задействованным в реализации концепции RA (рис. 2).

■ ■ ■

Внедрение системы RA/FMS – лишь первый шаг к построению бизнеса оператора в соответствии с методологией RA. В дальнейшем необходима планомерная модификация бизнес-процессов для предотвращения потерь и обеспечения полноты сбора доходов. ИКС

Системы ERP: заменять, модернизировать или?..

Что делать компании, если действующая система управления ресурсами перестала удовлетворять потребностям бизнеса? Заменить отдельные компоненты или систему целиком? А может, «уйти в облака»?

Дмитрий МАРТЫНОВ,
региональный менеджер Infor в России и СНГ

История вопроса

Первые системы управления ресурсами предприятия (Enterprise Resource Planning, ERP) появились в 90-х годах XX века, когда они применялись для планирования потребностей в материалах (MRP) и в автоматизированных системах управления производством (АСУП). С тех пор набор функций систем ERP значительно расширился и охватил все аспекты деятельности предприятия. Основная цель, которую преследуют эти системы, – дать головному офису возможность эффективно управлять всеми подразделениями.

Поначалу системы ERP с их множеством модулей для различных бизнес-процессов хорошо справлялись со своей задачей. Но в эпоху глобализации, когда даже малые и средние компании нередко имеют бизнес, распределенный по всему миру, системы ERP достигли предела своих возможностей и потребовали дальнейшего усложнения. Кроме того, вследствие интенсивных слияний и поглощений компании оказались владельцами многочисленных разнородных платформ, зачастую подвергшихся серьезной адаптации под индивидуальные нужды предприятия или разработанных собственными силами.

Попытки организовать централизованное управление столкнулись с тем, что ни один отдельно взятый разработчик и ни одна система ERP не могли решить все задачи компании. Ситуация еще больше усугубилась необходимостью подключения систем предприятия к системам партнеров по бизнесу – клиентов, поставщиков и пр. Поэтому усилился интерес к небольшим разработчикам, предлагающим «навесные» компоненты для ERP, например системы управления снабжением, складскими запасами и финансами, которые позволяют расширять возможности ERP и, по сути, соединять внутренние системы с внешним миром.

В результате практически все компании сегодня оперируют разнородными средами с хаотичными наборами приложений, специализированными интерфейсами и разрозненными платформами.

Внедрение «больших» систем ERP, разработанных специально для глобальных корпораций и не рассчитанных на малый бизнес и отдельные подразделения крупных компаний, в целом ряде случаев было неудачным. Поставщики таких систем втайне надеялись, что их продукты окажутся универсальными, однако в действительности получилось ровным счетом наоборот: они не подходили ни одной компании.

Часть проектов ERP закончилась провалом из-за недостатка внутренних ресурсов или поддержки со стороны высшего руководства. В других случаях поставщики пытались вынудить клиентов модернизировать или заменить свои системы только для преодоления заранее ожидавшегося морального устаревания работающих систем, притом что новые системы не давали реальных преимуществ.

Недаром, по оценкам аналитической компании Panorama Group, 21% компаний получил только половину ожидаемых преимуществ от внедрения системы ERP, и лишь 13% клиентов были полностью удовлетворены его результатами. Нет ничего удивительного, что многие компании сохранили свои старые системы ERP, зачастую сильно адаптированные, которые исправно служили им на протяжении долгих лет, и ничего не модернизировали.

Для большинства таких компаний, пользующихся старым программным обеспечением, рационализация платформ может привести к значительной экономии и оптимизации бизнес-процессов. Однако риски, связанные с внедрением очередной масштабной системы ERP, зачастую оказываются весомее потенциальных преимуществ.

Перед такими компаниями открываются сегодня несколько путей.

Полная замена ERP

Полная замена ERP имеет смысл прежде всего в тех случаях, когда существующее решение ERP не приносит пользы бизнесу и сдерживает его рост. Некоторые особо старые системы ERP даже не поддерживаются разработчиками. По данным аналитической компании AMR, многие компании вынужденно работают со старыми бизнес-системами, не отвечающими их потребностям. Но аналитики AMR отмечают, что пассивное ожидание финансирования и ресурсов на внедрение новых систем ERP может подорвать дух персонала.

В этих довольно редких случаях необходимо принять волевое решение о замене ERP-системы. Однако для получения максимальных преимуществ и минимизации рисков необходимо выбрать поставщика, обладающего опытом внедрения подобных систем в конкретной отрасли и способного продемонстрировать успешные проекты, которые принесли прибыль его клиентам. Об универсальности в данном случае говорить не приходится.

Очень важно проверить надежность поставщика ERP-решения. Сотрудничество с ним будет длиться десятилетия, поэтому разумно выбирать ПО, не только подходящее для конкретной организации, но и предлагаемое стабильным и жизнеспособным вендором.

Помните, что для эффективного внедрения ERP требуется достаточное количество ресурсов на всех уровнях компании. Не следует ждать от поставщика, что он предоставит всех руководителей проектов и технический персонал. Успешный проект – результат командной работы с вовлечением людей, знающих ваш бизнес. Также подумайте о том, какое влияние внедрение окажет на существующие и планируемые внутренние проекты.

Практически все компании сегодня оперируют разнородными средами с хаотичными наборами приложений, специализированными интерфейсами и разрозненными платформами

Расширение возможностей

После тщательного анализа существующей инфраструктуры ERP может выясниться, что полная ее замена нецелесообразна, поскольку значительная часть компонентов системы по-прежнему отлично подходит для бизнеса. В таких ситуациях имеет смысл сохранить текущую систему, расширив ее функции за счет модернизации или замены ряда компонентов.

Однако вплоть до сегодняшнего дня многие разработчики программного обеспечения не очень помогали клиентам модернизировать системы ERP и их компоненты. Эту ситуацию можно сравнить с покупкой новой кухни. Вместо того чтобы заменить старые приборы и шкафы, типичный поставщик ПО говорит: «Давайте-ка лучше снесем ваш дом, поставим новую кухню, а затем построим дом заново! Мы не знаем точно, сколько времени это займет, но, наверное, несколько месяцев». А заказчикам было бы желательно поставить новую кухню рядом с домом, чтобы экспериментировать с ней до тех пор, пока она их полностью не устроит, а затем договориться о конкретной дате и за одну ночь установить новую кухню вместо старой.

Переход от прикладных архитектур к сервисным (SOA) делает такой путь возможным.

В прикладных архитектурах используется подход, при котором разработчик регулярно выпускает обновления для используемого клиентом ПО. Иногда выходят масштабные обновления, но чаще речь идет об исправлении ошибок и добавлении незначительных функций. Слабое место этого подхода в том, что нельзя обновить финансовый модуль (кухню), не оказывая воздействия на остальные подразделения, в которых используется система ERP (оставшаяся часть дома).

Сервисные архитектуры (SOA) помогают решить эту проблему. В модели SOA расширение набора функций осуществляется не за счет обновления основного продукта, а за счет выпуска тесно интегрированных модулей, которые дополняют или расширяют базовую систему ERP. Они могут быть как тесно связаны с ERP-системой, заменяя собой некоторые из ее базовых функций, так и работать независимо от нее, поддерживая совершенно новый набор бизнес-процессов. Эта модель дает клиентам гораздо больше гибкости с точки зрения графика и способа развертывания новых функций.

Через некоторое время традиционные системы ERP в том виде, к которому мы привыкли, могут стать достоянием истории. Этот процесс в какой-то мере уже начался, но многие разработчики по-прежнему держатся за старую модель централизованного управления, в основном потому, что они до сих пор мыслят категориями 90-х годов. На практике же предприятия работают как централизованно, так и распределенно, и поэтому их бизнес-системы должны поддерживать

обе модели ведения дел. В этом и заключается красота сервисных архитектур – клиенты получают возможность сохранить динамичность и при этом адаптироваться к любым изменениям в будущем.

На площадке или по требованию

Третий вариант – распределение программного обеспечения: часть приложений может работать на площадке клиента, а часть – в «облаке». Облачные вычисления и модель SaaS (ПО как услуга) пользуются огромной популярностью, и аналитики предсказывают ее дальнейший рост благодаря гибкости и возможности сокращения капиталовложений за счет перехода на контракты с установленным уровнем сервиса (SLA) и ежемесячной оплатой.

На первый взгляд, модель SaaS очень привлекательна: она не требует больших инвестиций в лицензии и инфраструктуру поддержки и благодаря этому быстро окупается. Однако, по оценкам аналитиков, к третьему году эксплуатации системы, внедренные на площадке заказчика, могут стать дешевле с бухгалтерской точки зрения, поскольку в игру вступает амортизация активов. Поэтому в данном случае важен хорошо продуманный долгосрочный финансовый план.

На деле только немногие компании решили полностью перенести свои системы ERP в «облако». Основная масса считает перенос данных, а также сложных специализированных приложений и процессов в облачную среду чрезмерно рискованным.

Аналитики также выражают беспокойство относительно защищенности данных, недостаточной гибкости и больших затрат на услуги интеграторов и консультантов, помогающих с адаптацией, настройкой и интеграцией приложений SaaS с решениями, развернутыми на площадках заказчиков. Такие решения можно состыковать с SaaS средствами пакетной синхронизации или с помощью веб-служб, обеспечивающих интеграцию различного уровня сложности в реальном времени.

Некоторые утверждают, что модель SaaS якобы подходит только для решения простых задач. Это не так. Несмотря на ряд ограничений, SaaS-приложения отличаются высокой гибкостью (на уровне метаданных), и значительная их часть имеет широкие возможности настройки. С другой стороны, реализация сложных сквозных моделей с развитыми средствами управления бизнес-процессами и потоками операций действительно сопряжена с определенными трудностями.

Поэтому модель SaaS лучше всего подходит для стратегического расширения (а не замены) существующих систем ERP, установленных на площадке заказчика.

Однако помните, что поставщиков надо выбирать осмотрительно. В сферу SaaS в последнее время устремились многие. Во второй половине 2009 г. увеличилось число неудачных проектов среди поставщиков приложений SaaS и облачных систем второго и третьего эшелонов. В 2010 г. эта тенденция сохранится, поскольку инвесторы не будут вкладывать средства в проекты, которые не смогли продемонстрировать свою окупаемость. Выживут только сильные компании с достаточными источниками финансирования. Поэтому выбирая поставщика облачных систем, проанализируйте его показатель ежемесячного дохода от текущих контрактов как признак ликвидности и исходите из потребностей своей организации.

Следует обязательно договориться о конкретном уровне обслуживания (SLA) в дополнение к требованию общей доступности системы. Сегодня в состав SLA часто включают гарантии производительности системы, безопасности, принадлежности данных и времени устранения неполадок. Рекомендуется даже настоять на гарантиях возврата денег, привязанных к SLA.

Вне всяких сомнений, в 2010 г. число гибридных проектов внедрения SaaS-приложений увеличится. Ведь несмотря на все преимущества модели SaaS и рост ее популярности в 2010 г., зависимость от приложений на площадках пользователей никуда не денется. По сей день используется множество приложений для больших ЭВМ, а кроме того, законы запрещают хранение определенных видов данных за пределами организации. В результате гибридные среды скоро могут стать нормой для компаний, заинтересованных в расширении возможностей своих систем с помощью облачных приложений.

■ ■ ■

Сегодня замена ERP – не единственная возможность. Сервисные архитектуры и модель SaaS уже обрели необходимую гибкость и доказали свою эффективность. Они представляют собой вполне разумные альтернативы для движения в будущее. ИКС

SaaS лучше всего подходит для стратегического расширения (а не замены) существующих систем ERP, установленных на площадке заказчика

Повышаем эффективность корпоративной мультисервисной сети

Одна из проблем региональных корпоративных мультисервисных сетей – недостаточность канальных ресурсов. Повысить эффективность функционирования такой сети можно путем комплексной оптимизации параметров сетевых протоколов. Этот подход – экономически выгодная альтернатива замене сетевого оборудования, требующей немалых затрат.

Игорь УСПЕНСКИЙ, «Информсвязь Холдинг»

Значительная часть каналов связи в регионах – это средне- и низкоскоростные каналы невысокого качества. Их реальная пропускная способность, как правило, не превышает 30–50% максимально возможной.

В качестве критерия эффективности функционирования мультисервисной сети целесообразно выбрать информационную скорость передачи в канале связи. Этот параметр характеризует количество передаваемой через канал полезной информации в единицу времени. Очевидно, что даже на «идеальных» каналах без потерь информационная скорость будет меньше пропускной способности из-за присутствия в блоках передаваемых данных служебной информации протоколов (ее объем – от 2 до 75% в зависимости от технологии передачи и конкретных настроек).

Опыт работы с региональными мультисервисными сетями связи показывает, что при традиционных методах построения сетей информационная скорость не превышает 25–30% теоретически возможного максимума. Такие низкие значения обусловлены потерями в каналах связи при передаче данных и высокой избыточностью, вносимой служебной информацией инкапсулируемых протоколов.

Повысить эффективность функционирования мультисервисной сети можно путем физического увеличения доступных ресурсов: замены существующих каналов связи на более качественные с более высокой пропускной способностью, увеличения их количества, установки более производительного и высокотехнологичного телекоммуникационного оборудования. Такой способ очень затратен и рассчитан на долгосрочную перспективу. Другой путь – настройка используемых в сети протоколов путем подбора их параметров. Здесь затраты значительно ниже, однако трудность заключается в том, что для повышения эффективности нормально функционирующей мультисервисной сети связи требуется не изменение одного-двух параметров какого-нибудь одного протокола, а нахождение оптимального сочетания значений большого количества параметров всех работающих в сети протоколов. Этот процесс часто называют «тонкой настройкой», и именно он наилучшим образом решает поставленную задачу.

Уточнение архитектуры мультисервисной сети

Наиболее распространенная топология региональных корпоративных мультисервисных сетей – простая или многоуровневая «звезда». Выбор такой топологии зачастую обусловлен стремлением разместить филиалы в областном и районных центрах. При этом узлы сети в районных центрах обычно соединены с областным узлом, а рокадные связи, соединяющие районные узлы между собой, практически отсутствуют.

В качестве примера возьмем типовую архитектуру региональной мультисервисной банковской сети, в которой мультиплексирование потоков данных на канальном уровне и их приоритизация выполняются протоколом Frame Relay; система телефонии функционирует на базе технологии Voice over Frame Relay, для кодирования голосовой информации используется протокол G.729; платежная система опирается на протокол X.25, а информационная система – на протокол TCP на транспортном уровне и протокол IP на сетевом.

Модульная модель канала связи мультисервисной сети

Для минимизации времени доставки трафика данных реального времени – голоса и видео – крупные блоки данных от протоколов X.25 и TCP/IP подвергаются фрагментации. Это позволяет уменьшить вре-

Рис. 1. Логическая схема мультиплексирования данных

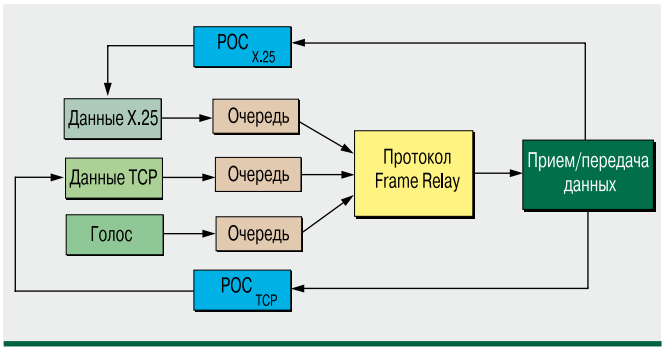
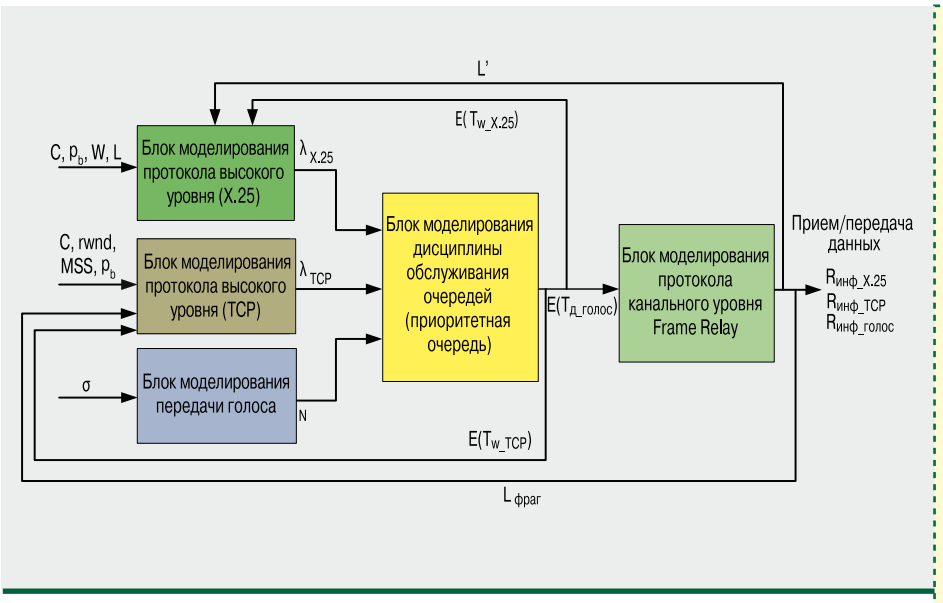


Рис. 2. Модульная модель канала связи для архитектуры протоколов Frame Relay



C – пропускная способность канала связи;
p_b – вероятность битовой ошибки в канале;
W – размер окна X.25;
L – длина информационного поля (полезной нагрузки) в кадре X.25;
t_p – время распространения сигнала по каналу;
$E(T_{w\_X.25})$ – среднее время ожидания в очереди, вносимое блоком моделирования дисциплины обслуживания очередей;
L' – длина служебных полей кадра X.25;
rwnd – размер окна передачи TCP;
MSS – размер сегмента данных TCP;
σ – джиттер голоса;
$E(T_{д\_голос})$ – среднее время доставки голосовых пакетов;
N – количество голосовых соединений;
$\lambda_{X.25}$, λ_{TCP} – интенсивности нагрузок, создаваемые трафиками X.25 и TCP соответственно;
$E(T_{w\_X.25})$, $E(T_{w\_TCP})$ – среднее время ожидания в очереди блоков данных X.25 и TCP соответственно;
$L_{фраг}$ – размер фрагмента канального уровня;
$R_{инф\_X.25}$, $R_{инф\_TCP}$, $R_{инф\_голос}$ – информационная скорость потоков X.25, TCP и голоса соответственно.

мя ожидания в очереди на передачу через канал связи по протоколу Frame Relay. Для протоколов, обеспечивающих гарантированную доставку информации через сеть, применяется процедура решающей обратной связи (на рис. 1 – $РОС_{X.25}$ и $РОС_{TCP}$ соответственно). При такой схеме мультиплексирования информационная скорость передачи для отдельно взятого канала будет складываться из информационных скоростей для каждого типа трафика – X.25, TCP и голоса.

При передаче данных в мультисервисной сети осуществляется многоуровневая инкапсуляция, т.е. протоколы верхних уровней используют для передачи данных услуги протоколов нижележащих уровней. Поэтому для изучения работы канала связи обратимся к модульной модели сети, созданной с помощью декомпозиции на уровни. Причем множество (или подмножество) выходных параметров модели нижележащего протокола будет являться множеством (или подмножеством) входных параметров для модели протокола верхнего уровня. Такой подход позволяет:

- моделировать стек протоколов любой глубины. Независимо от количества протоколов и их сложности возможность анализировать функционирование каждого протокола значительно упрощает моделирование работы канала связи;
- использовать в качестве блоков моделирования модели любой природы – математические, имитационные или экспериментальные.

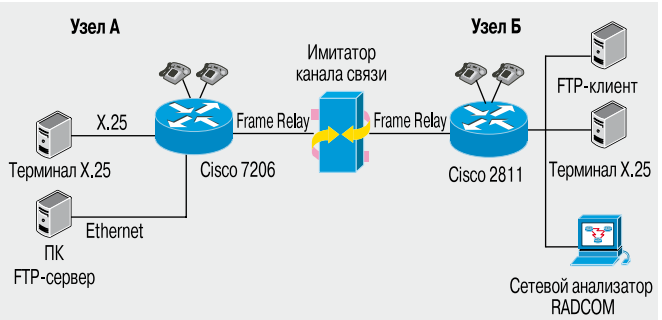
Для проведения оптимизации необходимо выделить параметры протоколов, в наибольшей степени влияющих на эффективность функционирования сети. Такими параметрами являются длины блоков данных, размеры фрагментов, тип дисциплины обслуживания очередей, величины таймеров переповтора и др. (рис. 2). Варьируя с некоторым шагом значения этих параметров, найдем такое их сочетание, при котором эффективность функционирования сети связи будет наибольшей.

Очевидно, что в случае, когда сеть имеет топологию «звезда», оптимизация работы каналов связи по каждому из направлений обеспечит оптимальность функционирования сети в целом. Таким образом, данное модульное представление канала связи позволяет проводить комплексную оптимизацию параметров протоколов мультисервисной сети.

Экспериментальная проверка результатов моделирования

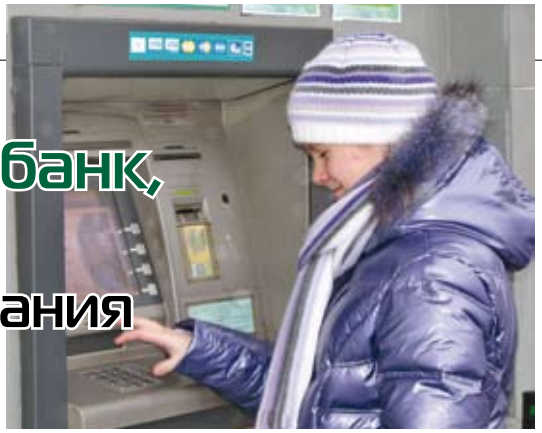
Адекватность модели проверялась на имитационном стенде ИТКС-РБ (рис. 3), который позволяет организовывать передачу голосового трафика (одно–три телефонных

Рис. 3. Имитационный стенд ИТКС-РБ



соединения), трафика TCP (передачу данных по протоколу FTP) и трафика X.25. В качестве мультисервисного протокола канального уровня используется Frame Relay. Имитация канала связи осуществляется программными средствами, что дает возможность варьировать параметры линии связи (пропускную способность, вероятность битовой ошибки, время задержки при передаче по каналу).

Эксперименты показали, что комплексная оптимизация параметров обеспечивает повышение информационных скоростей на 7–30% в зависимости от набора используемых протоколов, установленного оборудования и характеристик каналов связи. ИКС



«Всегда рядом» – говорит банк, уводя клиентов из «сберкасс» в удаленные каналы обслуживания

Банкоматы, информационно-платежные терминалы, интернет-платежи, мобильный банк – это и будни Сбербанка, и одновременно новая парадигма услуг, предъявляющая новые требования к корпоративной сети связи банка. И в первую очередь к основе сети – телекоммуникационным каналам.

Модернизация оптических артерий

Даже имея сложившуюся телекоммуникационную инфраструктуру, банки постоянно вкладывают средства в ее модернизацию. По оценкам экспертов, до 2009 г. такие затраты ежегодно росли на 15–20%. Кризис внес свои коррективы, однако необходимость затрат на постоянную модернизацию очевидна для игроков рынка. Сбербанк России, ранее заявивший о планах к 2014 г. вывести 70% платежей из операционных касс в удаленные каналы самообслуживания, в текущем году не снизил темпов модернизации телекоммуникационных каналов своей филиальной сети. Корпоративная телекоммуникационная сеть Сбербанка в Москве, объединившая около 800 структурных подразделений, была построена еще в 2002 г. на базе волоконно-оптических каналов «АКАДО Телеком».

В дальнейшем на сеть банка «спроецировалась» и модернизация сети самого оператора, который в 2006 г. внедрил на всей субмагистральной сети технологии 10G Ethernet и DWDM, а в 2009 г. модернизировал ядро сети, установив маршрутизаторы Cisco CRS-1. Это позволило перевести сеть IP/MPLS на новый уровень производительности. Модернизация сети также обеспечила интегрированную передачу данных, видео и голоса на скоростях до 1 Гбит/с, с поддержкой четырех классов качества обслуживания трафика (CoS).

Сеть банкоматов Сбербанка выросла в крупнейшую в России буквально за последние пять лет. Если в 2004 г. она насчитывала 350 терминалов на всю страну, то сейчас их количество увеличилось почти в 70 раз – до 23 тыс. Из них 1950 установлено в Москве. По сообщению Московского банка Сбербанка России, в III квартале этого года доля финансовых операций, проведенных через удаленные каналы обслуживания, составила 46,7%.

Участники рынка телекоммуникационных услуг также осознают необходимость постоянных вложений в новые разработки для банковского сектора. Так, по сообщениям «АКАДО Телеком», оператор за последние три года внедрил ряд комплексных решений для банков: это и защищенные мультисервисные сети VPN, и возможность работы в реальном времени с системами приема и обработки электронных платежей Банка России, и многое другое.

Банкоматы на связи

При выборе способов связи между терминалами и оборудованием процессингового центра банк традиционно руководствуется тремя основными критериями: надежность, цена, доступность. Выделенные каналы, созданные на основе волоконно-оптических сетей, гарантируют высокий уровень надежности, поскольку транзакции в них совершаются по защищенным протоколам. Однако на «последней миле» нередко возникают сложности, когда к месту установки терминала требуется дополнительно прокладывать кабель. Чтобы избежать этих проблем, в марте 2010 г. Сбербанк запустил в Москве проект подключения своих банкоматов посредством радиодоступа с использованием ресурсов операторов мобильной связи «Скай Линк» и «МегаФон». Терминалы соединяются по радиоканалам мобильных операторов со шлюзами на сети «АКАДО Телеком», а затем по волоконно-оптическим кабелям этой сети – с процессинговым центром Сбербанка. Такой подход обеспечил оперативность организации услуг, минимальные капитальные затраты, автоматическое резервирование каналов мобильных операторов в случае пропадания связи, возможность (при необходимости) оперативного перемещения банкоматов.

Как отмечает Леонид Гуштуров, генеральный директор ОАО «КОМКОР» («АКАДО Телеком»), проект потребовал выработки и согласования особого четырехстороннего «Регламента взаимодействия при подключении и обслуживании банкоматов». В соответствии с этим регламентом в случае возникновения аварийной ситуации единой «точкой входа» для Сбербанка является служба технической поддержки «АКАДО Телеком», которая координирует и контролирует действия всех компаний – участников проекта.

С марта по сентябрь 2010 г. в Москве было установлено 150 новых банкоматов Сбербанка, и 122 из них подключены посредством радиодоступа. Банкоматы установлены в основном в сетевых магазинах, торговых центрах, государственных учреждениях. До конца текущего года Сбербанк планирует довести количество банкоматов в столице до 2050 – и большинство новых подключений планирует также организовать с использованием зарезервированного радиодоступа.

Лилия ПАВЛОВА

ИКС pro технологии

ИТ-инфраструктура ЦОДа устремляется в «облака»

Дмитрий САХАРОВ

О том, как в условиях жесткой экономии средств и ресурсов будет трансформироваться ИТ-инфраструктура дата-центров и какие подходы и технологические решения при этом оказываются наиболее перспективными, зарубежные и российские компании рассказали на 5-й Международной конференции «ЦОД-2010», организованной журналом «ИКС».

Глобальный экономический кризис вынудил заказчиков серьезно пересмотреть взгляды на развитие собственных ЦОДов и начать использовать новые технологические решения, которые требуют существенно меньших инвестиций в расширение ИТ-инфраструктуры ЦОДов и снижают операционные расходы на ее администрирование и обслуживание. На первый план выходит общий подход: ИТ как основа для предоставления услуг обработки, передачи и хранения информации, используемой в бизнес-процессах заказчиков. Подобная перестройка потребует изменить и ИТ-инфраструктуру ЦОДа. При этом следует выбирать такие технологические решения, которые обеспечат более простое управление всей инфраструктурой, эффективное использование ее ресурсов, улучшенную защиту данных и оптимальное управление изменениями в будущем.

Задачи построения новой ИТ-инфраструктуры ЦОДа становятся все более неотложными из-за постоянного роста объемов обрабатываемой и хранимой информации, что требует повышения эффективности ИТ и использования инновационных технологий. К числу последних относят автоматизацию процессов обработки и хранения данных, консолидацию средств ИТ и обеспечение их энергетической эффективности, а также формирование в рамках ИТ-инфраструктуры виртуальных сред. Практически все вендоры считают, что для решения большинства задач заказчиков и значительного сокращения расходов на ИТ им необходимо консолидировать ресурсы обработки, хранения и передачи информации в ИТ-инфраструктуре ЦОДа и виртуализовать сосредоточенные в ней серверы, сети и системы хранения данных (СХД). Виртуализация этих основных компонентов позволит перейти к модели облачных вычислений, где ИТ-инфраструктура ЦОДа предоставляет все необходимые услуги по обработке информации «по запросу» со стороны клиентов.

Виртуализация – путь к «облакам»

Компания VMware как лидер рынка средств виртуализации представляет разработанный ею программный пакет виртуализации vSphere, на основе которого реализуются облачные вычисления, как средство превращения ЦОДа в мощную платформу для предоставления услуг. Как сказал Родион Тульский, консультант по решениям VMware в России, концепция облачных вычислений – и виртуализация как ее основа – формируют новый подход к ИТ как к некоей, зачастую внешней услуге, а трансформируемая ИТ-инфраструктура становится способна масштабироваться по требованию при высокой степени абстракции управления ее ресурсами.

В настоящее время именно на основе виртуализации и кластеризации корпорация Oracle выстраивает свою стратегию перехода к облачным вычислениям, которая должна усовершенствовать функционирование ЦОДа при обеспечении непрерывности бизнес-процессов. Владимир Алексеев, директор программы Oracle Insight&Architecture в России и СНГ, уточняет: «Облачные вычисления – это новая модель архитектуры ИТ для удобного, надежного и быстрого (по первому требованию) доступа к общему пулу гибко конфигурируемых вычислительных ресурсов (сетей, серверов, СХД, приложений, сервисов), которые могут быть назначены пользователю и быстро освобождены с минимальными усилиями обслуживающего технического персонала ЦОДа или сервис-провайдера».

Вендоры выделяют несколько моделей формирования облачных вычислений: это частные, внутренние (private) «облака», когда компании создают облачную ИТ-инфраструктуру ЦОДа для собственного использования; публичные (public) «облака», создаваемые сервис-провайдерами и предназначенные для предоставления услуг и сервисов через Интернет для многих сторонних заказчиков; гибридные «облака», представляющие собой два или более совместимых облака и позволяющие клиентам выбирать оптимальные по производительности и экономически выгодные условия размещения данных и обработки приложений.

Для клиентов создаваемое в рамках ИТ-инфраструктуры дата-центра «облако» представляет собой разделяемый набор ресурсов обработки, хранения и передачи информации, к которому обеспечен сетевой доступ (через браузер и сетевое устройство) и который предоставляет клиентам измеряемые сервисы, что позволяет им платить за ИТ-услуги по факту их использования. Любой пользователь получает требуемые услуги и сервисы в режиме самообслуживания, а гибкость выделения ресурсов в соответствии с поступающими запросами обеспечивает высокую скорость реакции облачной ИТ-инфраструктуры.

С технологической точки зрения такое «облако» должно обеспечить качество сервисов, сопоставимое с тем, которое достигается на сконфигурированных

вручную средах для обработки отдельных приложений в ЦОДе. При этом в облачной инфраструктуре виртуализованные ресурсы должны автоматически перемещаться в изменяемой в соответствии с потоком запросов вычислительной среде.

Как отметил Родион Тульский, новые решения VMware vCloud Director и vShield позволяют реализовать управляемую и безопасную обработку приложений в «облаке». Так, решение vCloud Director (на базе программного комплекса vSphere) дает возможность создавать виртуальные ЦОДы с легко доступными для пользователей пулами вычислительных ресурсов, СХД, сетей и каталогами стандартных сервисов, а за счет интегрированного модуля биллинга обеспечивает экономическую прозрачность расчетов с клиентами.

Программный пакет VMware vShield обеспечивает защиту облачных инфраструктур, используя более совершенный, адаптивный подход к безопасности за счет интеграции с существующими системами защиты. При этом vShield упрощает процессы контроля за безопасностью, увязывая в единое целое все компоненты виртуальных инфраструктур и «облаков». Кроме того, для защиты от катастроф в «облаке» VMware предлагает использовать решение vCenter Site Recovery Manager.

Выступая партнером VMware, компания EMC обеспечила интеграцию своих программно-аппаратных средств с виртуальной средой комплекса VMware vSphere и дополнила ее собственными разработками, повысив степень безопасности облачных вычислений. В частности, EMC предложила применять ее технологию VPLEX, которая позволяет многократно (до 17 раз) ускорить перемещение приложений, данных и виртуальных машин между двумя облачными ЦОДами заказчика (основным и резервным).

Корпорация Microsoft, которая довольно долго не принимала активного участия в разработке продуктов виртуализации, за последние два года решила ликвидировать отставание в этой области, выпустив две версии бесплатного гипервизора Hyper-V для ПК и три релиза серверной ОС Windows Server 2008, которые позволяют создавать пулы виртуализованных серверов и десктопов, трансформируя ИТ-инфраструктуру. Кроме того, как рассказал Василий Маланин, специалист Microsoft по решениям для ЦОД, комплекс System Center Service Manager обеспечивает управление виртуальными машинами и физическими серверами, их конфигурирование, мониторинг всех компонентов ИТ-инфраструктуры и резервное копирование данных в «динамическом» ЦОДе, созданном на базе продуктов Microsoft и ее партнеров. Так, совместное использование средств System Center и пакета Opalis позволяет автоматизировать работу инструментов управления ИТ-инфраструктурой ЦОДа с помощью схем процессов.

Стремясь перейти от отдельных продуктов к поставке законченных решений, Microsoft интегрировала свои продукты для виртуализации в объявленную в этом году компанией HP «конвергентную инфраструктуру». В результате создается полностью интегрированный, виртуализованный стек аппаратных средств HP (серверов, СХД, сетей), с единым управлением ИТ-инфраструктурой и сервисами от HP, Microsoft и партнеров. Дальнейший путь заказчиков к облачной ИТ-инфраструктуре ЦОДа Microsoft видит в использовании ими любой из трех моделей – SaaS, PaaS и IaaS на базе предлагаемых ею продуктов. Это могут быть вызываемые по сетям приложения (SaaS); использование системы Microsoft Azure, которую компания сама применяет, выступая в качестве сервис-провайдера, предоставляющего услуги своих мощных ЦОДов как внешних «облаков» по отношению к пользователям (PaaS); и комплексы ПО System Center и Dynamic Infrastructure Toolkit, обеспечивающие управление виртуализованной ИТ-инфраструктурой (IaaS). Для защиты данных Microsoft предложила свою систему Forefront Client Security с простым управлением.

О том, насколько ценной для заказчиков может оказаться трансформация ИТ-инфраструктуры ЦОДа в «облако», говорят результаты исследования, проведенного Symantec в 2009 г.: за счет виртуализации и консолидации серверов, СХД, сетевого оборудования (в инвестициях компаний в ИТ они составляют около 45%) заказчикам удается сократить на 30–60% затраты на закупку оборудования и снизить операционные расходы на управление и администрирование на 10–15%.

Аналитики отмечают и ряд проблем, которые более половины заказчиков считают весьма важными при внедрении «облаков»: обеспечение защиты данных, производительность и доступность ресурсов, сложность настройки, конфигурирования и интеграции «облаков» в существующую ИТ-инфраструктуру. Кроме того, определенные сложности при использовании ресурсов «облаков» могут быть связаны с требованиями регулирующих органов, запрещающими передачу информации вовне.

Выявленные проблемы заказчиков позволили аналитикам IDC и Forrester прогнозировать, что к 2012 г. в корпоративных ИТ-бюджетах расходы на услуги публичных «облаков» вырастут лишь на 9%, а 91% прироста расходов будет направлен внутрь компании, на трансформацию собственных ЦОДов, причем 44% больших компаний заинтересованы в создании своих внутренних «облаков».

Аппаратный инструментарий виртуализации

Обретя после покупки компании Sun возможность предлагать не только свои программные продукты, но и аппаратные решения, Oracle провозгласила «комплексный подход к проектированию и эксплуатации ИТ-инфраструктуры ЦОДа» в рамках инициативы Next Generation Data Center (NGDC). Этот подход опирается на технологии серверной виртуализации и кластеризации и гипервизоры, используемые как в системах SPARC на базе многопоточных процессоров Sun для среды ОС Solaris, так и в серверах архитектуры x86/x64, работающих в среде ОС Linux, Windows, Solaris. Как заявил В. Алексеев (Oracle), «это единственное ПО виртуализации, для которого сертифицированы ВСЕ продукты Oracle, начиная от баз данных и кончая приложениями».

Еще одно решение для виртуализованных ЦОДов нового поколения – платформа Cisco Unified Computing System (UCS). По словам Александра Скороходова, системного инженера-консультанта представительства Cisco в России, эта платформа, основанная на стандартной архитектуре x86, обеспечивает виртуализацию вычислительных ресурсов при консолидированном вводе-выводе и единое подключение к сетям хранения SAN и сетевым хранилищам NAS через виртуализованный адаптер.

Cisco предлагает в составе UCS три модели блейд-серверов на базе процессоров Intel Xeon нового поколения. Встроенная система управления UCS Manager позволяет динамически выделять ресурсы «по запросу», обеспечивает масштабируемость создаваемых на основе этой платформы решений (управление блейд-серверами в количестве до 320 как одной системой) без увеличения сложности и интеграцию с партнерскими решениями. За счет виртуализации платформы сокращается число серверов, коммутаторов, адаптеров, кабелей, снижаются требования к питанию и охлаждению, что в целом приводит к уменьшению затрат клиентов. Опыт внедрения UCS в ИТ-инфраструктуру Cisco показал, что можно добиться снижения энергопотребления на 33%, получить 40%-ную экономию на кабельной системе, сократить расходы на серверы и СХД, уменьшить время ввода сервисов в эксплуатацию и простои системы.

Хранение – компактное и экономичное

Помимо вычислительных систем, при трансформации ИТ-инфраструктуры ЦОДа в «облако» необходимо создавать эффективные хранилища информации. Такие СХД предлагает компания EMC, опираясь на технологию формирования автоматизированных многоуровневых хранилищ FAST (Fully Automated Storage Tiering). Эта технология подразумевает, что в дисковый массив СХД, наряду с традиционными жесткими дисками Fibre Channel и SATA, встраивается небольшое количество (до 4% емкости) твердотельных дисков. На них средства управления информацией FAST перемещают часто используемые данные, а редко используемая информация размещается на дисках Fibre Channel. По словам технического консультанта EMC Россия Федора Павлова, применение технологии FAST в виртуальной среде способно улучшить на величину до 80% использование дискового пространства в СХД Symmetrix VMAX, в 2,5 раза снизить время отклика системы и на 60% увеличить ее производительность. При этом в СХД можно установить на 30% меньше дисков, достигая тем самым 17%-ной экономии питания и охлаждения.

Кроме того, EMC предложила использовать в хранилищах, создаваемых в «облачной» виртуализованной среде ЦОДа, свою систему резервного копирования с блочной дедупликацией EMC Avamar, которая многократно сокращает объемы хранимой в СХД информации.

На уменьшение объемов архивов неструктурированной информации в виртуализованной среде нацелено и решение Symantec Enterprise Vault. Максим Цветаев, системный инженер российского офиса Symantec, отметил, что при неуклонном росте объемов информации и желании пользователей «хранить все и вечно» возрастает количество дубликатов данных, а время на резервное копирование сокращается. Кроме того, затрудняется поиск и обработка архивируемых данных. В решении Enterprise Vault, предусматривающем архивирование с резервным копированием и предотвращением потери данных, для уменьшения объемов архивов применены технологии дедупликации (устраняющие избыточность), удаление ненужных данных в соответствии с предписаниями, а также индексирование, обеспечивающее эффективный поиск. Symantec Enterprise Vault дает возможность уменьшить затраты на хранение более чем на 65%, в два раза сократить время резервного копирования и восстановления, снизить расходы на поиск и обработку информации на величину до 87%. При этом, как отметил М. Цветаев, решение демонстрирует высокую производительность: с его помощью заказчики архивируют более 5 млн сообщений в день.

Комплексные решения для ИТ-инфраструктуры

Два года назад компании Cisco, EMC и VMware создали альянс с целью объединения своих продуктов и технологий – виртуализации, вычислительных и сетевых систем, СХД. Результатом сотрудничества участников альянса стало интегрированное решение VBLOCK, которое, как сказал Ф. Павлов (EMC), предложено как строительный элемент для ЦОДов нового поколения в виде трех моделей. Во всех компонентах каждой модели VBLOCK (серверах, сетях и СХД) используются технологии виртуализации, что позволит заказчикам, внедряющим это решение, перейти к формированию унифицированной ИТ-инфраструктуры в своих ЦОДах в виде внутренних «облаков» при минимальных рисках интеграции.

В свою очередь, Oracle объявила о реализации «комплексного подхода к проектированию и эксплуатации ИТ-инфраструктуры ЦОДа», в рамках которого вендор обеспечивает заказчикам доступность своих технологий облачных вычислений для всех клиентских ИТ-

сервисов, давая возможность использовать технологии Oracle как для частных «облаков», так и для публичных. Примером эффективного внедрения разработок Oracle в области виртуализации и совершенствования на ее основе процессов ИТ служит ИТ-инфраструктура самой компании: если в 1998 г. в 40 дата-центрах Oracle во всем мире использовалось 52 вида приложений, обрабатывающих фрагментированные массивы данных для несвязанных бизнес-процессов, то в настоящее время в трех ЦОДах компании используется единое приложение Oracle E-Business Suite на основе глобально стандартизованных процессов, с однородной базой данных и глобально управляемыми бизнес-процессами.

Другой пример, приведенный В. Алексеевым (Oracle), показал эффективность использования технологии виртуализации Oracle VM в компании LCRA, в инфраструктуре которой насчитывалось более 100 физических и виртуальных серверов. За счет внедрения Oracle VM и Oracle Enterprise Linux Architecture при формировании четырех кластеров стандартных серверов Dell за 5 лет заказчик сэкономил более $1,5 млн, значительно повысив к тому же производительность обработки баз данных Oracle.

Не только серверы, но и десктопы

Одна из задач современного ЦОДа – обеспечить безопасный и эффективный доступ сотрудников компаний к корпоративным ресурсам. В последние годы эта задача становится все сложнее из-за того, что удаленные сотрудники все шире используют ноутбуки и разнообразные мобильные устройства. Решение проблемы предложила Citrix Systems, разработав технологию виртуализации десктопов.

Как пояснил Сергей Халяпин, руководитель отдела системных инженеров российского офиса Citrix, раньше, когда настольные ПК сотрудников были жестко связаны через сети с основными ресурсами ЦОДа, их администрирование и управление доступом были весьма сложными и дорогостоящими. При том что необходимо было контролировать и управлять ПО и ОС на каждом ПК, их обновление могло потребовать многих дней при ограниченных возможностях восстановления данных и безопасности. К тому же эти проблемы возрастали многократно при замене клиентского оборудования. Поэтому Citrix предложила технологию виртуализации десктопов Citrix XenDesktop, которая подразумевает использование виртуализованных и изолированных компонентов клиентского устройства: профиля пользователя и приложений и ОС, с которыми он работает. Они могут храниться централизованно в ЦОДе компании и доставляться на ПК пользователя по запросу. Для этого на конечном устройстве пользователя инсталлируются компоненты решения Citrix – гипервизор XenClient и App Receiver, обеспечивающие его виртуализацию, а на серверах ЦОД работают компоненты XenDesktop, XenApp, XenServer и Essentials для Microsoft HyperV. В сети доставки применяются компоненты NetScaler и Branch Repeater, обеспечивающие независимость и защищенность создаваемого соединения «устройство пользователя – серверы ЦОДа».

Решение Citrix XenDesktop использует две модели доставки по технологии FlexCast: потоково доставляемый десктоп (в режиме online) и обработка виртуальных приложений в физических десктопах (online и offline). По расчетам Citrix, в режиме доставляемых десктопов (профиля, ОС и ПО) один сервер в ЦОДе может обслуживать до 400–500 пользователей. Если сервер осуществляет поддержку разделяемых десктопов, то на нем может быть создано до 50–60 виртуальных машин, выполняющих обработку информации и приложений.

Виртуализация десктопов позволяет, по утверждению Citrix, минимизировать затраты на управление ими и достичь гибкости и эффективности облачных решений при обеспечении безопасности информации, хранимой в ЦОДе. Пользователь может обращаться как к корпоративному ЦОДу, который с помощью ПО Xen Cloud Platform трансформируется в «облачную среду», так и к публичным «облакам» сервис-провайдеров, оказывающих услуги по модели SaaS. Причем Citrix Systems и Microsoft в настоящее время вошли в пятерку крупнейших поставщиков услуг SaaS в мире. В то же время Citrix своим решением XenDesktop обеспечила пользователям доступ к приложениям с любых видов настольных и мобильных ПК и устройств: ПК под управлением Windows и Linux, Mac, тонких клиентов и смартфонов, планшетов, мобильных телефонов, подключаемых к самым разным сетям передачи данных. Как сказал С. Халяпин, в 2009 г. 100 млн пользователей по всему миру ежедневно работали с виртуальными приложениями и десктопами при помощи решений Citrix.

В свою очередь, VMware предложила решение VMware View для виртуализации рабочих мест сотрудников, которые также могут в качестве виртуального десктопа использовать различные мобильные устройства, настольные ПК, работающие под управлением Windows и Mac OS, тонкие клиенты. По словам Р. Тульского (VMware), в новой версии VMware View 4.5 обеспечена полная поддержка Windows 7 и возможность работать в режиме offline, а также интеграция с различным ПО других разработчиков и поддержка современных аппаратных компонентов ПК – портов USB, смарт-карт для PCoIP.

Обеспечить непрерывность бизнеса

Еще одна важная задача, которую должна решить ИТ-инфраструктура ЦОДов нового поколения, – обеспечение непрерывности бизнес-процессов, что подразумевает защиту данных и приложений от любых сбоев аппаратных средств. Традиционно отказоустойчивость достигается за счет резервирования и избыточности компонентов ИТ-инфраструктуры, специального ПО, контролирующего состояние данных (Oracle DataGuard и его аналоги), кластеризации серверов и СХД, резервного копирования на ленты.

Дмитрий Дощаный, директор центра решений департамента вычислительных систем КРОК, отметил, что технология виртуализации позволяет по-новому подойти к этой проблеме в пределах ЦОДа. Средства

управления и контроля за виртуальными машинами, предлагаемые поставщиками средств виртуализации, уже обеспечивают отказоустойчивость и высокую доступность данных и приложений. При этом устанавливаемая система виртуализации настраивается один раз, защищает все виртуальные машины, а лицензию необходимо приобретать только на одну копию ОС и приложения, что снижает стоимость решения.

Однако ограничиваться только инструментами, встроенными в системы виртуализации, не стоит, так как они не отслеживают состояния ОС и приложений, не защищают от сбоя СХД и от логической порчи данных. Чтобы достичь более высокого уровня отказоустойчивости, КРОК предложила использовать решение для непрерывной защиты данных EMC RecoverPoint CDP, которое обеспечивает быстрое, единообразное восстановление после отказа на нужную точку для разных приложений и может применяться с аппаратными средствами разных поставщиков. Хотя и это решение обладает определенными ограничениями: работает только в сетях Fibre Channel и не полностью интегрируется с приложениями.

Как полагают в КРОК, если заказчику необходимы очень высокие уровни отказоустойчивости и доступности данных и приложений для поддержания непрерывности бизнес-процессов, то ему нужно строить распределенную ИТ-инфраструктуру в виде основного и резервного ЦОДов. В такой распределенной ИТ-системе можно применять решения виртуализации, предлагаемые VMware (ПО Site Recovery Manager) и обеспечивающие катастрофоустойчивость инфраструктуры, решение EMC RecoverPoint CRR для непрерывной защиты данных, решения Double-Take, EMC RepliStor, IBM Replify для интеллектуальной репликации на уровне ОС, а также средства дедупликации для повышения отказоустойчивости. Как заявил Д. Дощаный, с помощью таких решений можно создать в ИТ-инфраструктуре ЦОДа систему защиты данных и приложений от максимального количества сбоев, которая будет простой в эксплуатации и иметь разумную стоимость.

Управлять развитием ЦОДа

Изменение ситуации на рынке и конкурентная борьба требуют от заказчиков постоянного развития бизнеса, что, в свою очередь, приводит к необходимости внедрять новые приложения и расширять ИТ-инфраструктуру ЦОДа в условиях ограниченного бюджета. Поэтому заказчикам будут весьма полезны решения для оптимизации работы бизнес-приложений в ЦОДе и планирования развития его инфраструктуры, предлагаемые Radware и Avocent.

Компания Radware решила задачу уменьшения количества серверов и лицензий ПО (вместе с соответствующими расходами) с одновременным улучшением качества работы при росте числа приложений и пользователей, обеспечив равномерность загрузки приложений на серверах (физических/виртуальных) и снизив число реализуемых ими дополнительных функций, с тем чтобы высвободить процессорную мощность для обработки основных приложений. Применяя решения Radware, заказчики могут сократить затраты на приобретение оборудования и операционные расходы – на обслуживание ИТ-инфраструктуры, электричество, охлаждение, помещения и персонал.

Центральным компонентом предложенной Radware системы управления и контроля приложений стали программно-аппаратные платформы AppDirector/Alteon, которые в рамках ЦОДа ведут постоянный анализ состояния серверов и приложений, обеспечивают балансировку, модификацию и перенаправление трафика для оптимизации работы приложений, акселерацию приложений за счет компрессии, кэширования, мультиплексирования TCP. Эти же платформы способны выполнять глобальную балансировку приложений между несколькими ЦОДами, управлять пропускной способностью сетей и формировать оптимальный трафик.

Использование платформ AppDirector/Alteon, как утверждает Михаил Суконник, региональный менеджер Radware по продажам в России и СНГ, значительно увеличивает производительность серверных систем при обработке приложений и обеспечивает более высокое качество услуг с точки зрения пользователя. Так, по данным вендора, при работе Microsoft SharePoint Server 2007 втрое сокращается время загрузки страниц удаленными пользователями, на 65% уменьшается требуемая пропускная способность сетей передачи данных при снижении загрузки процессоров в серверах на 40%. Высокие эксплуатационные показатели достигнуты при работе Oracle E-Business Suite 12 – благодаря компрессии требуемая пропускная способность сетей снижается на 60%, а использование в AppDirector/Alteon кэширования сокращает количество запросов, поступающих на серверы, на 80%.

В то же время новые приложения и увеличение числа пользователей требуют внедрения в ИТ-инфраструктуру ЦОДа новых сервисов, новых серверов и пересмотра приоритетов в обработке приложений. Решение Bandwidth Management от Radware позволит не только избежать высоких начальных инвестиций в решение для контроля доставки приложений и проектов модернизации и замены оборудования (а также связанных с этим расходов и остановок сервиса), но и инвестировать в ИТ-инфраструктуру по мере роста запросов.

Компания Avocent, вошедшая в декабре 2009 г. в состав корпорации Emerson, предложила ряд решений для оптимизации ИТ-инфраструктуры ЦОДа и управления ее ресурсами, в том числе для ЦОДа нового поколения, реализуемого в виде «облака». Для этого, по утверждению Юрия Колесова, регионального менеджера Avocent в СНГ (Emerson Network Power), заказчики должны иметь централизованно хранимую документацию, что позволит им управлять изменениями в ИТ-инфраструктуре ЦОДа, используя надежные сервисы и ведя мониторинг систем и контроль потребления энергии. Со своей стороны Avocent предложила широкий набор встраиваемых в ИТ-инфраструктуру аппа-

ратных средств для мониторинга подключенных к сети серверов, СХД, сетевых устройств и ПО управления DSView 3, которое обеспечивает доступ ко всем физическим и виртуализованным устройствам, контролируя их состояние и управляя потреблением электроэнергии. Эти продукты Avocent позволят заказчикам эффективно отслеживать возникающие в ИТ-инфраструктуре незапланированные инциденты и на величину до 70% сократить простои оборудования, предупредить его перегрузку и подсчитать реальную стоимость используемой электроэнергии с помощью системы отчетов.

Кроме того, Avocent разработала систему Avocent MergePoint Infrastructure Explorer (AMIE) для планирования ресурсов ЦОДа, которая дает возможность оценивать наличие ресурсов – свободного места, электропитания, охлаждения, сетевых портов и веса – и принимать обоснованные решения, касающиеся изменений в ИТ-инфраструктуре ЦОДа в будущем. AMIE упрощает процесс планирования, предлагая заказчикам календарь проектов, с помощью которого они могут сравнивать сценарии и выявлять возникающие проблемы, а также оценивать прогнозируемый эффект от реализации проектов изменений.

Эффективность решений Avocent подтверждают такие показатели: во всемирной системе банков при инсталляции в среднем до 3 тыс. серверов в год время проработки проектов сокращается с 60 до 10 дней, в торговых предприятиях, где внедряется 75–100 серверов в месяц, сокращение затрат времени на проекты составляет 30%, что обеспечивает экономию до $157 тыс. в год. Сейчас решения Avocent используют более 85% компаний, входящих в список Fortune 1000, а компании Apple, Acer, Dell, Fujitsu Siemens, HP, IBM, Intel, Lenovo, Microsoft, NEC применяют их в своих продуктах. В России с использованием решений Avocent выполнено более 50 крупных проектов в банках, телекоме, промышленности, финансовых и страховых компаниях, в госсекторе.

■ ■ ■

Как отмечает Зеус Керравала, аналитик Yankee Group, на рынке нет вендоров, которые имели бы все необходимые для построения «облаков» технологии и решения – серверы, сетевые средства, сети хранения, СХД, платформы виртуализации. Поэтому заказчикам при переходе на «облачную» ИТ-инфраструктуру своих ЦОДов приходится делать выбор между технологиями нескольких вендоров, оценивая их сильные и слабые стороны, чтобы избежать значительных проблем в будущем. ИКС

Миграция к сетям стандарта 802.11n

Стандарт 802.11n рассматривается специалистами как первый технологический прорыв в области беспроводных локальных сетей после принятия 802.11a/g. Какие особенности новой технологии нужно учесть, чтобы ее внедрение в корпоративную сеть было успешным?

Александр ГОРНАК, технический директор компании «Новые Системы Телеком»

В настоящее время со стандартом IEEE 802.11n для беспроводных локальных вычислительных сетей (БЛВС), принятым в сентябре 2009 г., связывают большие надежды на повышение эффективности работы как существующих, так и новых приложений. Действительно, 802.11n позволяет значительно поднять производительность Wi-Fi-сетей (пропускную способность в среднем в 5 раз, дальность связи – в 2 раза). Интерес к новому стандарту проявился еще до его официальной ратификации: большинство производителей Wi-Fi-оборудования первые решения для предприятий, основанные на черновых версиях 802.11n, начали выпускать в 2008 г. И сегодня поставщики продолжают направлять своих заказчиков к новой Wi-Fi-технологии. Более того, продукты, поддерживающие только 802.11a/b/g, постепенно «вымываются» с рынка: производители чипсетов для БЛВС уже полностью переориентировались на поддержку 802.11n и прекращают выпуск старых чипов 802.11a/b/g. Поэтому переход к 802.11n в корпоративных сетях – дело времени, а расширенные возможности стандарта стимулируют ускорение этого процесса и строительство новых сетей 802.11n.

Однако проектирование и развертывание БЛВС 802.11n приносит и новые проблемы.

Особенности технологии

Часть проблем, встающих при внедрении технологии 802.11n, обусловлены ее особенностями и сделанными в ней усовершенствованиями.

MIMO

Один из ключевых компонентов 802.11n – радиотехнология MIMO (Multiple Input Multiple Output), которая дает возможность оборудованию обрабатывать несколько входящих и исходящих потоков данных.

Каждая система MIMO определяется количеством передатчиков и приемников, работающих в ее радиоцепях. В обозначении параметров системы MIMO

первое число указывает количество передатчиков, второе – количество приемников. Например, система MIMO 3x4 состоит из четырех радиоцепей с тремя передатчиками и четырьмя приемниками. В настоящее время большинство производителей корпоративных WLAN выпускают радиосистемы MIMO 2x3 или 3x3. Поскольку каждая радиоцепь требует питания, то система с MIMO будет потреблять большую мощность, чем обычная станция 802.11a/b/g.

При передаче радиосигнала может наблюдаться многолучевость – распространение сигнала по двум или более траекториям вследствие отражения. В результате копии одного и того же сигнала прибывают на приемную антенну с интервалом в несколько наносекунд. Для традиционной БЛВС эта разница во времени может привести к повреждению данных и необходимости повторной передачи на втором уровне, что отрицательно сказывается на производительности системы.

А радиосистема MIMO, передавая несколько радиосигналов одновременно, извлекает из многолучевости выгоду. Фактически каждый отдельный радиосигнал передается своей радиоцепью и антенной системы MIMO. Он содержит поток уникальных данных, отличных от данных других потоков, передаваемых по другим радиоцепям. Все независимые потоки данных распространяются по различным путям, поскольку разнесение передающих антенн составляет по крайней мере половину длины волны (пространственное мультиплексирование). Когда клиентская станция 802.11n с MIMO 2 x 3 отправляет два уникальных потока данных к точке доступа 802.11n, та получает оба потока, и эффективная пропускная способность удваивается.

Кроме того, использование в системах MIMO нескольких разнесенных антенн при приеме сигнала позволяет увеличить дальность связи.

Опционально в 802.11n предусмотрена поддержка технологии формирования луча (beamforming), когда с помощью интеллектуального антенного массива передаваемые сигналы синфазно фокусируются на приемнике. Это весьма перспективный подход, но, к сожалению, в настоящее время он практически не представлен на рынке.

Защитный интервал

Данные модулируются поверх несущего сигнала в последовательности битов (символов). В условиях многолучевого распространения символ может прибыть на приемник до завершения приема предыдущего символа. Этот эффект, называемый межсимвольной интерференцией, приводит к разрушению данных. Временная разница между различными путями распространения одного и того же сигнала (задержка распространения) обычно составляет 50–100 нс (максимум около 200 нс). Для устранения межсимвольной интерференции в стандартах семейства 802.11 символы следуют друг за другом с временным защитным интервалом (guard interval), который в 2–4 раза превышает задержку распространения.

В системах 802.11a/g защитный интервал между OFDM-символами составляет 800 нс. В стандарте 802.11n есть возможность установить защитный интервал равным 400 нс, что позволяет приблизительно на 10% повысить пропускную способность. Однако это увеличивает риск потери данных из-за межсимвольной интерференции, поэтому опциональный интервал 400 нс должен применяться только при наличии хороших радиочастотных условий.

Каналы 20 МГц и 40 МГц

В системах 802.11a/g передача ведется на радиоканале шириной 20 МГц. Оборудование стандарта 802.11n также может работать на 20 МГц-каналах, но для передачи данных использует 52 OFDM-поднесущие (вместо 48 в 802.11a/b/g), что позволяет несколько увеличить объем данных, передаваемых в той же частотной полосе. Однако в 802.11n можно вести прием и передачу и на OFDM-каналах шириной 40 МГц, что удваивает частотную полосу, доступную для пропуска данных. В этом случае задействуется 114 OFDM-поднесущих, из которых 108 транспортируют данные. Канал 40 МГц реализуется через связывание двух смежных 20 МГц OFDM-каналов (первичного и вторичного).

В диапазоне 2,4 ГГц имеются три непересекающихся канала шириной 20 МГц. Из них можно сформировать только один канал 40 МГц, что не позволяет строить беспроводную сеть без частотного перекрытия. Поэтому для работы в этом режиме Wi-Fi Alliance рекомендует перейти в полосу 5 ГГц, где можно создать несколько неперекрывающихся 40 ГГц-каналов.

К сожалению, в России диапазон 5 ГГц является лицензируемым и, как правило, не используется в корпоративных БЛВС. В диапазоне 2,4 ГГц технология 802.11n должна работать с каналами 20 МГц. Существуют, однако, исключения из правил. Некоторые производители предлагают собственные одноканальные решения, позволяющие на частоте 2,4 ГГц развернуть один канал 40 МГц с несколькими точками доступа.

Усовершенствования на уровне 2

Для обеспечения больших скоростей передачи в технологии 802.11n также улучшен MAC-подуровень канального уровня. В числе улучшений – механизмы агрегации кадров и подтверждения приема для блока кадров. Благодаря им рост пропускной способности по сравнению с 802.11a/g может достигать 100% (в зависимости от типа трафика).

Агрегация кадров – механизм, позволяющий объединять несколько кадров 802.11 в один для последующей передачи.

Подтверждение приема блока подразумевает передачу только одного кадра подтверждения (так называемого Block ACK-кадра) после приема группы кадров вместо передачи множества ACK-кадров подтверждения после приема каждого отдельного кадра из группы.

Оба механизма снижают заголовочную избыточность на MAC-уровне и конкуренцию за доступ к среде

передачи, что повышает пропускную способность и надежность системы.

Проектирование и интеграция

Специфика 802.11n проявляется и при интеграции сети этого стандарта в существующую беспроводную и проводную инфраструктуры предприятия, и при обеспечении производительности и сетевой безопасности.

Обратная совместимость

В соответствии со стандартом радиостанции 802.11n должны быть обратно совместимы с радиостанциями 802.11a, 802.11b и 802.11g. Поправка 802.11n определяет четыре различных механизма защиты для реализации обратной совместимости. Однако все они создают чрезмерные накладные расходы на MAC-уровне.

Стандарт 802.11n также определяет формат кадра, не связанный с унаследованными технологиями (greenfield-формат) и, следовательно, не совместимый с 802.11a/b/g. Сеть, состоящая только из точек доступа и клиентских устройств стандарта 802.11n, не нуждается в защитных механизмах и имеет максимальную производительность. Но на практике развертывание такой «чистой» сети 802.11n затруднительно в силу того, что в большинстве организаций имеется множество 802.11a/b/g-клиентов, и обратная совместимость с большой вероятностью будет востребована. Следует понимать, что платой за нее будет снижение производительности БЛВС.

PoE

Поскольку точки доступа (ТД) обычно устанавливаются под фальшпотолком и в других труднодоступных местах, то большинство из них получают питание через систему электропитания PoE (Power over Ethernet). PoE устраняет необходимость подвода электрических кабелей и установки розеток для каждой точки доступа. К ТД достаточно протянуть один низковольтный Ethernet-кабель. Это значительно снижает стоимость развертывания сети и обеспечивает большую гибкость в выборе мест размещения ТД.

Стандарт 802.3af PoE определяет возможность подведения к точке доступа через Ethernet-кабель максимум 15,4 Вт с максимальным энергопотреблением 12,95 Вт.

Как правило, точки доступа 802.11n для предприятий используют MIMO 3x3 и способны работать в двух диапазонах частот. В большинстве случаев для питания таких точек доступа 15,4 Вт будет недостаточно. Когда будут широко распространены ТД MIMO 4x4, проблемы с электропитанием станут еще острее.

IEEE недавно ратифицировал поправку 802.3at, которая увеличивает возможности PoE до 25 Вт. Технологию 802.3at PoE иногда называют PoE Plus.

Производители оборудования, помимо оснащения точек доступа 802.11n портами Ethernet с поддержкой PoE Plus, предлагают и другие варианты. В том числе – оснащение ТД двумя портами 802.3af, снижение возможностей MIMO (за счет уменьшения активных передатчиков при питании от стандартного PoE) и, конечно, питание через обычную электрическую розетку. Отметим также, что некоторые производители выпускают точки доступа 802.11n с оптимизированными схемами электропитания, для которых хватает возможностей стандарта 802.3af.

При выборе поставщика оборудования 802.11n особое внимание следует уделить методу питания точек доступа. Следует понимать, что использоваие ТД 802.11n приведет к значительному увеличению потребляемой мощности. Поэтому при развертывании этих точек доступа необходимо тщательно планировать бюджет PoE с учетом других устройств, таких как VoIP-телефоны и видеокамеры, которые также требуют PoE.

Существующая инфраструктура

Точки доступа 802.11n способны передавать данные со скоростью, которая превышает пропускную способность портов Fast Ethernet (100 Мбит/с), обычно предоставляемых беспроводной сети. Если в сети несколько точек доступа 802.11n, то в проводной инфраструктуре могут возникнуть узкие места. По этой причине проводная сеть должны быть обновлена для обеспечения большей пропускной способности.

Так, скорее всего, коммутаторы уровня доступа, предоставляющие свои порты множеству точек доступа 802.11n, должны будут иметь несколько Gigabit Ethernet-каналов в сторону ядра сети.

Большинство Ethernet-коммутаторов, установленных на уровне доступа, поддерживают только порты доступа 10/100 Мбит/с, и теоретически потока данных от одной ТД 802.11n с несколькими радиоцепями достаточно для перегрузки Ethernet-соединения 10/100 Мбит/с. На практике же приложения, работающие сегодня поверх корпоративных беспроводных сетей 802.11n, не перегружают проводную сеть. Однако по мере роста популярности технологии 802.11n приложения, требующие большей полосы пропускания, включая видео, будут становиться обычным явлением для Wi-Fi.

Как правило, точки доступа 802.11n уже имеют восходящие порты Gigabit Ethernet, и потому в предвосхищении таких приложений рекомендуется провести модернизацию кабельной инфраструктуры. Конечно, Gigabit Ethernet может быть реализован в кабельных системах категории 5e, тем не менее следует рассмотреть возможность обновления кабелей до категории 6.

Архитектура БЛВС

Одной из наиболее популярных и признанных архитектур БЛВС для предприятия является архитектура, в которой центральное место отведено контроллеру (или специализированному коммутатору) беспроводной сети. Контроллер управляет доступом абонентов, качеством обслуживания и параметрами трафика на уровне абонентов, обеспечивает безопасный доступ к защищаемым сетевым ресурсам и приложениям, поддерживает многие другие функции. Точки доступа ра-

ботают в связке с контроллером, получая от него все необходимые настройки.

В рамках этой архитектуры точки доступа передают кадры 802.11 через IP-инкапсулированный туннель к центральному контроллеру, откуда данные затем направляются к сетевым ресурсам. Однако при наличии в сети значительно более производительных точек доступа 802.11n контроллер может стать узким местом. Поэтому необходимо учитывать, что при миграции к новой сети может понадобиться покупка более производительного контроллера или модернизация существующего.

Альтернативой этому подходу может быть переход к архитектуре распределенной передачи данных, предлагаемой в последнее время некоторыми производителями БЛВС. Суть этого подхода состоит в том, что контроллер обрабатывает только данные управления, а интеллектуальные точки доступа 802.11n поддерживают аутентификацию пользователей и принимают решения о продвижении трафика на границе сети. Продвижение трафика данных в обход контроллера напрямую в проводную сеть освобождает большие ресурсы в контроллере, позволяя значительно увеличить масштабируемость БЛВС.

Безопасность

При развертывании сети 802.11n возникают новые проблемы, связанные с безопасностью. Традиционные беспроводные системы предотвращения вторжений (wireless intrusion prevention systems, WIPS) обнаруживают радиопередатчики 802.11n в случае, если они работают на первичном или вторичном 20 МГц-канале и используют формат кадра, понятный сенсорам унаследованной системы безопасности. Однако сенсор на базе стандарта 802.11a/g не сможет расшифровать передачи на 40 МГц-каналах и с кадрами в формате, не совместимом с 802.11a/g. Если злоумышленник установит ТД 802.11n, работающую в таком формате, то WIPS с датчиками устаревшего стандарта 802.11a/g ее не обнаружит. Решение этой проблемы заключается в оснащении WIPS новыми сенсорами, поддерживающими радиоинтерфейсы 802.11n.

В сети 802.11n удваивается количество каналов, которое нужно проверять для обнаружения несанкционированных устройств и действий. Система WIPS должна прослушивать на предмет возможных атак оба OFDM-канала – и 20 МГц, и 40 МГц.

Некоторые производители оборудования БЛВС выпускают интегрированные решения WIPS, в которых точки доступа функционируют и как сенсоры. Часть времени такие ТД заняты прослушиванием других каналов, и это может привносить задержку и джиттер в работу приложений, подобных VoWi-Fi. С другой стороны, необходимость прослушивания большего количества каналов и слишком малое время, отводимое под сканирование, увеличивают вероятность того, что атаки не будут обнаружены. Поэтому при установке интегрированного решения WIPS рекомендуется часть точек доступа полностью перевести в режим сенсоров, которые будут постоянно сканировать все каналы.

Следует также отметить, что появление новых технологий всегда сопровождается новыми видами атак. Например, уже известна атака типа «отказ в обслуживании» (DoS), использующая функцию подтверждения принятия блока кадров (Block ACK) в системах 802.11n. В будущем вероятно появление новых DoS-атак на MAC-уровне против 802.11n. Чтобы WIPS могли обнаружить эти новые нападения, необходимо регулярно обновлять файлы WIPS-сигнатур.

Обследование объекта

При обследовании сайта для развертывания сети 802.11n нужно обратить внимание на тип клиентских устройств, имеющихся на предприятии. Если все клиенты являются устройствами 802.11n, то все точки доступа должны быть развернуты с учетом получения максимальных выгод от эффекта многолучевости. Однако эффект многолучевости будет негативно влиять на клиентов 802.11a/b/g, и если такие унаследованные клиенты преобладают, то по-прежнему рекомендуется использовать узконаправленные антенны для уменьшения отражений.

Другой момент – расстояние между точками доступа. В случае только 802.11n MIMO-клиентов точки доступа могут быть размещены дальше друг от друга, так как технология MIMO обеспечивает большую область покрытия. Однако если в системе будет много унаследованных клиентов, точки доступа должны быть ближе друг к другу.

Программные и аппаратные инструменты для обследования объектов нужно обновить для поддержки технологии 802.11n.

В ходе обследования необходимо определить зоны покрытия. При пассивном обследовании клиентское устройство замеряет только силу сигнала (дБм) и отношение сигнал/шум. При активном способе обследования клиентское устройство ассоциируется с точкой доступа, и помимо радиохарактеристик, измеряются потери пакетов и процент переповторов на втором уровне. Для развертывания сети 802.11n важнее провести активное обследование, поскольку многолучевая обстановка в направлении от точки доступа к клиенту отличается от обстановки в направлении от клиента к ТД.

В обследовании любого типа должен быть выполнен спектральный анализ по выявлению потенциальных источников помех, таких как микроволновые печи или беспроводные телефоны.

■ ■ ■

Итак, мы видим, что миграция к технологии 802.11n в корпоративной беспроводной сети предполагает комплексный подход, включающий решение ряда задач, таких как выбор подходящего поставщика оборудования, аудит и модернизация проводной сетевой инфраструктуры, выбор или модернизация программных средств и инструментов обеспечения безопасности, мониторинга и обследования сети. Игнорирование этих шагов может привести к проблемам с производительностью и безопасностью сети при ее дальнейшей эксплуатации. ИКС

Эффективное командообразование в проекте ЦОДа

О том, насколько значимы в проектах создания/модернизации ЦОДов вопросы правильного проектирования и подбора технических решений, на страницах «ИКС» сказано немало. Не осталась без внимания и тема грамотной эксплуатации. Пришло время поговорить о кадрах – о человеческом факторе, который был, есть и всегда будет определяющим фактором успеха любого технологического проекта.

Александр МАРТЫНЮК,
генеральный директор,
«Ди Си квадрат»

Есть смысл начать разговор с повторения азбучных истин: дата-центр – многогранная сфера приложения специализированных знаний, в которой нет места мелочам. Энергетика, климатика, информационная и техническая безопасность, противопожарное обеспечение, ИКТ-системы и оборудование, слаботочные системы, СКС, строительство – каждая из этих предметных областей имеет свои «границы компетентности», свои подходы и специфику, свой профессиональный сленг, наконец. Неудивительно, что, оказавшись в одной проектной команде, представители каждой из этих профессиональных групп порой с трудом понимают друг друга, что, естественно, затрудняет принятие согласованных решений.

В чем суть проблемы?

Думаю, любой читатель этой статьи может в подробностях представить себе диалог между, скажем, главным энергетиком компании и представителем службы безопасности. Абсолютно разные аргументы, терминология, регламенты и документы – и каждый по-своему прав. Как в такой ситуации не уподобиться героям известной басни Крылова? Как в оптимально короткие сроки выработать единое видение проектной задачи, подготовить качественное ТЗ и обеспечить квалифицированный подбор исполнителей проекта?

Давайте рассмотрим цепочку, типичную для проекта создания нового дата-центра корпоративного заказчика. Причем не в версии «как всегда», а в варианте «как должно быть» – будем оптимистами.

Поэтапное командообразование

Этап первый

Итак, все начинается на этапе формирования бизнес-стратегии. Компания определяет свои цели и задачи, оговаривает планы развития и выдает ИТ-службе ключевые ориентиры (сроки, системы, точки регионального присутствия, требования к отказоустойчивости и т. д.), на основании которых разрабатывается ИТ-составляющая бизнес-стратегии. Как правило, эта работа поручается представителям заказчика и/или приглашенным консультантам (иногда – специалистам системного интегратора), хорошо разбирающимся как в вопросах бизнеса, так и в вопросах ИТ. Момент принятия решения о составе этой команды – первая точка отсчета для успеха проекта, на 50% (а то и больше) зависящая от пресловутого человеческого фактора. Какими бы современными ни были технологические средства и анализ развития бизнеса заказчика, определяющим фактором остается компетентность конкретных людей, сформулировавших проектную задачу и ключевые параметры проекта: сроки, бюджеты, критерии оценки качества.

Этап второй

В дальнейшем эти параметры будут преобразованы в набор из нескольких ТЗ (подобно тому как луч света, проходя через призму, разлагается в спектр) – по числу разделов проекта, к исполнению которых будут привлекаться подрядчики. Те, кто берет на себя работу по «спектральному преобразованию» исходной стратегии, – второе ответственное звено упомянутой цепочки. Для этой команды очень важно хорошее взаимопонимание. Во-первых, для того, чтобы в проекте не осталось «ничьих» задач. Во-вторых, чтобы задачи, приходящиеся на область, где пересекаются две и более профессиональные сферы, одинаково понимались и воспринимались всеми, кто вовлечен в данный процесс.

Разработка проектных ТЗ, как в консолидированной редакции, так и по отдельным разделам проекта – один из наиболее ответственных моментов. Именно исходя из ТЗ будет подбираться площадка под ЦОД. Именно на основе ТЗ будет формироваться проектное решение, будут уточняться бюджет и согласовываться сроки поставки. Поэтому так важно, чтобы на данном этапе в проект были вовлечены максимально компетентные специалисты. В идеале именно эта команда должна контролировать развитие проекта. Но даже если заказчик примет иное решение, экономить на кадровом вопросе тут весьма рискованно, ведь на кон поставлен успех проекта.

Этап третий

Третьим в цепочке проектных шагов является выбор куратора проекта (как ни крути, этот момент полностью зависит от человеческого фактора). Здесь очень важно, чтобы кандидатуры на такую ответственную позицию рассматривались не столько по принципу кумовства и близости к руководству (хотя это, безусловно, тоже надо принимать во внимание), сколько из соображений компетентности в вопросах управления проектом и способности обеспечить руководству компании и инвесторам необходимую и достаточную для них прозрачность развития проекта. В противном случае топ-менеджерам постоянно придется погружаться в оперативные вопросы. А это значит, что либо непосредственное управление бизнесом на это время будет пущено на самотек, либо топ-менеджер на протяжении всего проекта будет нести двойную нагрузку.

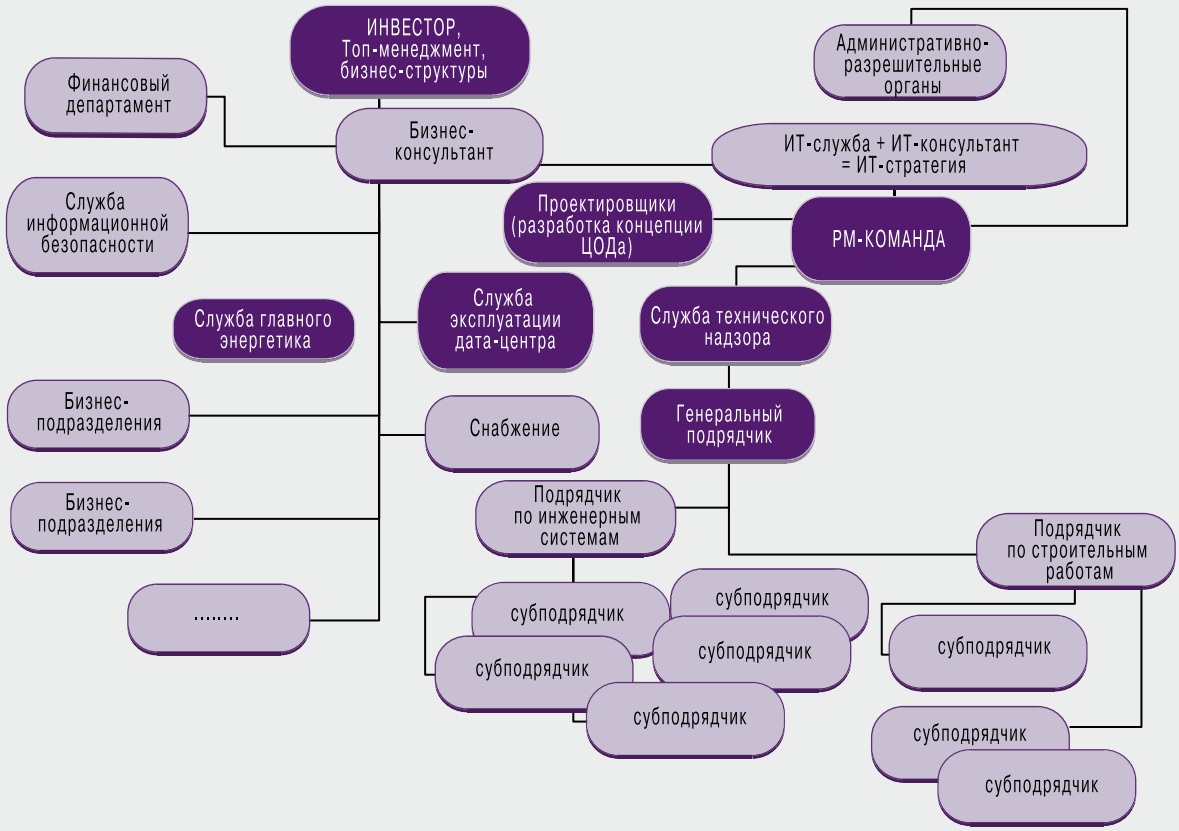
То же самое относится к подбору остальных представителей команды управления проектом, которая должна:

- иметь постоянный контакт со всеми ключевыми подразделениями заказчика (заинтересованные бизнес-подразделения, ИТ-служба, безопасность, энергетики, пожарные, климатики и т.д.);
- нести ответственность за выбор оптимальной технологической площадки и организацию тендеров по выбору генподрядчика и подрядчиков;
- обладать полномочиями для технического надзора;
- знать, когда, где и кому делегировать решение административных вопросов (например, оперативное согласование проектных решений в государственных инстанциях, организацию приемки работ и сдаточных испытаний);
- курировать вопросы своевременного заказа и поставок инженерного оборудования;
- обеспечивать соблюдение сроков и бюджетов без ущерба для оговоренного в ТЗ качества проекта.

Кто будет входить в состав этой команды – решать заказчику. Вариантов не так уж много: представители генподрядчика (как это по старинке еще любят делать в России); собственные сотрудники (пока наиболее популярная форма проектного управления); профессиональная управляющая компания (которой отдают предпочтение на Западе). Давайте рассмотрим плюсы и минусы каждого варианта с позиции эффективности конечного результата.

Но прежде – определим основные роли участников проекта (см. рисунок).

Основные роли в проекте



Кто у руля?

Генподрядчик

Такой подход – дань традициям советского времени, когда в отсутствие рынка в стране довольно успешно работала модель единого генподрядчика. В те времена в этой роли выступала большая организация, в которой действовала четко встроенная проектная иерархия. Эта организация и проектировала, и строила, и определяла исполнителей субподрядных работ на местах. В составе этой организации было также подразделение, отвечающее за координацию разделов проекта и взаимодействие исполнителей. Именно это подразделение, по сути, и осуществляло то, что мы теперь называем проектным менеджментом (PM). Для тех условий такая модель была логичной и оправданной, учитывая, что все работы выполнялись, как правило, в пределах одной структуры и в соответствии с общегосударственными стандартами. Даже если в интересах проекта требовалось взаимодействие с другими компаниями, этих компаний было отнюдь не так много, как теперь. Это, кстати, одна из причин, почему в современных реалиях описанный подход уже не может претендовать на статус единственно правильного. К тому же, как известно, многие отечественные стандарты морально устарели и каждая организация пытается разрешить ситуацию по своему.

Есть еще один аргумент, исключающий передачу функций управления проектом генподрядчику (он наглядно прослеживается на приведенной схеме): если все бразды управления проектом отданы генподрядчику, сразу возникают сомнения в объективности технического надзора. А эта роль по умолчанию не должна входить в сферу полномочий генерального заказчика: она может входить в компетенцию либо куратора, назначенного заказчиком, либо внешней управляющей команды.

Штатные сотрудники заказчика

Это, пожалуй, наиболее популярная сегодня в России модель управления проектом ЦОДа для крупных корпоративных клиентов. И объясняется это не столько эффективностью данного подхода, сколько отсутствием на рынке альтернативных предложений, обеспечивающих гарантию качества. К тому же не каждый заказчик знает, как определить благонадежность потенциальной управляющей компании, – цена ошибки слишком велика, а работа консультантов стоит дорого.

Те, кто посчитали все эти доводы определяющими, формируют проектную команду своими силами. В этом случае в более выигрышной ситуации оказываются крупные промышленные структуры, у которых в штате есть квалифицированные специалисты, по роду службы хорошо разбирающиеся в предметных областях, имеющих отношение к ЦОДам. Дополнительным плюсом могут стать полезные связи в административно-разрешительных органах, способные помочь в оформлении нужной площадки и прилегающих к ней территорий, в оперативном получении мощностей, согласовании документов в СРО и т.д. В итоге получается, что высококвалифицированный штатный персонал,

Виртуализация –
это только половина битвы за эффективность

InfraStruXure™
DATA CENTERS ON DEMAND

Принципы архитектуры InfraStruXure® для сред с высокой плотностью монтажа

1. Стойки для оборудования с высокой плотностью монтажа
2. Блоки распределения электропитания с контролем параметров на уровне стоек
3. Контроль температуры на уровне стоек
4. Программное обеспечение централизованного контроля (не показано)
5. Эксплуатационное программное обеспечение с возможностями прогнозирования и управления мощностью (не показано)
6. Эффективные системы охлаждения InRow®
7. Гибкие и масштабируемые системы электропитания с ИБП

Вы можете развернуть стойки с высокой плотностью выделяемой тепловой мощности прямо сейчас

InfraStruXure можно развернуть как основу всей архитектуры центра обработки данных или серверного зала либо встроить в крупный существующий центр обработки данных.

Виртуализация останется надолго

И это неудивительно — она позволяет экономить место и энергию, в то же время максимально использовать ИТ-ресурсы. Однако за компактность иногда приходится платить. Виртуализированные серверы — даже при загрузке на 50% мощности — требуют особого внимания к охлаждению независимо от их размера или расположения.

1. Повышение тепловыделения. Объединение серверов увеличивает плотность интеграции и тепловыделения в стойке, что создает риск простоев и сбоев.

2. Снижение эффективности. Периферийное охлаждение не позволяет справиться с перегревом в глубине стоек, а чрезмерная мощность охлаждения ведет к увеличению затрат и снижению эффективности.

3. Сбой электропитания. Виртуальные нагрузки постоянно меняются, что затрудняет прогнозирование доступной мощности электропитания и охлаждения, создавая риск повреждения сети.

Правильный подход к виртуализации

Новая архитектура InfraStruXure для сред с высокой плотностью монтажа помогает справиться с ростом тепловыделения благодаря охлаждению рядов стоек с виртуализированными серверами, управлению электропитанием на уровне стоек и мощному программному обеспечению для управления и моделирования систем. Виртуализация позволяет экономить энергию, однако реальная эффективность среды зависит также от относительной эффективности систем электропитания, охлаждения и серверов. Только оптимально подобранная мощность всей системы позволяет получить экономию за счет повышения эффективности. Чтобы построить оптимальную конфигурацию, положитесь на эффективную модульную архитектуру InfraStruXure для сред с высокой плотностью выделяемой тепловой мощности и нейтрализуйте тепло у его источника. Ваше оборудование будет работать более безопасно и эффективно, приближаясь к использованию мощности на 100%.

Виртуализация — и нет проблем

Что вы ожидаете? Архитектура InfraStruXure для сред с высокой плотностью выделяемой тепловой мощности открывает возможности виртуализации для всех, в любое время и в любом месте. Просто разверните ее и приступайте к работе.

Эффективность и виртуализация

Ваши серверы используются эффективно, но можно ли сказать то же о системах электропитания и охлаждения?

Использование мощности охлаждения | Серверы | Использование мощности электропитания

ДО ВИРТУАЛИЗАЦИИ СЕРВЕРОВ

Возможна большая экономия на серверах и системах электропитания и охлаждения.

- ☐ Оптимальное использование серверов
- ☐ Оптимальная мощность электропитания
- ☐ Оптимальная мощность охлаждения

Эффективность 29%

ПОСЛЕ ВИРТУАЛИЗАЦИИ СЕРВЕРОВ

Чрезмерно завышенная мощность электропитания и охлаждения гасит потенциальный выигрыш от виртуализации.

- ☑ Оптимальное использование серверов
- ☐ Оптимальная мощность электропитания
- ☐ Оптимальная мощность охлаждения

Эффективность 16%

ВИРТУАЛИЗАЦИИ СЕРВЕРОВ С СИСТЕМАМИ ЭЛЕКТРОПИТАНИЯ И ОХЛАЖДЕНИЯ

Оптимальная мощность электропитания и охлаждения смещает баланс в вашу пользу.

- ☑ Оптимальное использование серверов
- ☑ Оптимальная мощность электропитания
- ☑ Оптимальная мощность охлаждения

Эффективность 63%

t.a.c by Schneider Electric | PELCO by Schneider Electric | SQUARE D by Schneider Electric | Cisco Partner Technology Developer | Microsoft | IBM Alliance Partner | DELL | EMC² Select

Загрузите **БЕСПЛАТНО** любые информационные статьи в течение 30 дней и **станьте участником розыгрыша* — выиграйте планшетный компьютер iPad.**

Зайдите на сайт **www.apc.com/promo** и введите код **82854t**

APC® by Schneider Electric

APC by Schneider Electric в Москве: 119334, Москва, 5-й Донской проезд, д. 21-Б, стр. 10. Тел.: +7 495 916-7166, факс: +7 495 620-9180. Центр поддержки клиентов: 8 800 200-2722, E-mail: apcrustech@apc.com

«прикомандированный» к проекту, на несколько месяцев (возможно, год-полтора) оказывается полностью выведенным из привычного ритма и участия в бизнес-процессах.

В результате, как бы хорошо все ни складывалось поначалу, компания-заказчик вскоре оказывается перед дилеммой. Либо нужно полностью переключать этих специалистов на управление проектом и искать им замену для выполнения прямых должностных функций (тогда к моменту окончания проекта придется или кого-то увольнять, или открывать новый аналогичный проект), либо, наоборот, стоит вернуть ценных сотрудников на их рабочие места, дав им время на вхождение в курс упущенных дел, а к выполнению проектных задач все же привлечь внешнюю команду (т.е. опять настает момент выбора надежного партнера).

Совет в данной ситуации может быть лишь один – определитесь, есть ли у вас время и деньги на подобные эксперименты. Что важнее: не упустить бизнес-возможности (от которых может отвлечь проект) или не пустить в бизнес «посторонних», пусть даже у них есть необходимый вам опыт, знания и гарантии сохранения конфиденциальности полученной информации. Исходя из принятого решения, начинайте заниматься кадровым вопросом, потому что на сегодняшний день в России репутацию любой проектной команде и самому проекту делают не компании, а конкретные специалисты.

Внешняя компания

Модель, давно и успешно практикуемая в США и Европе, в России пока еще приживается с трудом. Некоторые причины такой осторожности приведены выше, и надо признать, логика в ней есть. Однако время идет. В нашей стране появляются профессиональные команды, знакомые с лучшими зарубежными практиками и методологиями, обладающие необходимой экспертизой и репутацией, подтвержденной в ходе реализации сложных инженерных проектов в России. Поэтому, если сместить акценты с абстрактных опасений и рисков возможной неудачи на конкретные требования к конечному результату проектных работ и их возможное развитие в перспективе, то принять верное решение куда легче. Переведите те же риски и опасения в параметры «профиля управляющего проектом». Дополните этот профиль важными для вас деталями. Сформулируйте критерии, отражающие уровень ответственности PM-команды, необходимые гарантии, степень компетентности в важных областях и т.д.

К примеру, убедитесь в том, что PM-команда имеет опыт разработки проектной документации с учетом отраслевых регламентов по комплексной защите объектов заказчика, и в соответствующий момент проекта (а не когда уже все построено) службы ИТ-безопасности, противопожарной безопасности, технической безопасности и главного энергетика не предъявят претензии в связи с несоблюдением важного, с их точки зрения, параграфа инструкции/корпоративной политики/отраслевого регламента. Обижаться на этих людей бессмысленно: они просто делают свою работу и, как правило, делают ее хорошо.

Если для инвестора проекта или владельца будущей площадки так важно, чтобы штатный персонал накапливал собственную экспертизу, обеспечьте его вовлеченность в проект в рамках разумного. Зачем учиться на своих ошибках – порой непоправимых, когда их можно избежать? В конце концов те, кто готов подтвердить свою компетенцию, в свое время точно так же набирались мастерства у западных компаний.

Персональный отбор исполнителей

То, что тендеры по выбору генподрядчика и подрядчиков ИТ-проекта в России, бывает, напоминают хорошо срежиссированный спектакль со своими главными героями, массовкой и «темными личностями», – тема отдельной статьи. В данном случае хотелось бы сделать акцент на Личностях, имеющих вес в профессио-

нальном смысле. Именно на них, а не на имя компании, следует ориентироваться, рассматривая конкурсные предложения. Как известно, охота за хорошими специалистами на ИТ-рынке идет непрерывно. И тот, кто еще вчера обеспечил успех (или неуспех) своей компании в проекте, может сегодня оказаться в штате ее конкурента. Из собственной практики могу припомнить несколько примеров, когда смена одного или нескольких представителей подрядчиков в проектной команде коренным образом меняла ход событий. Поэтому очень важно, чтобы на этапе выбора подрядчика в состав конкурсной комиссии входили люди, владеющие информацией о кадровых миграциях на рынке ИТ-специалистов.

Кадры решают все...

Именно этой крылатой фразой уместно завершить статью. В любом проекте – и особенно в проекте создания/модернизации дата-центра – человеческий фактор имеет огромное значение. И определяющую роль здесь играет Персона куратора проекта. От того, насколько правильно он распределит роли, насколько правильно выберет партнеров, зависит очень многое. В том числе и его собственная репутация. ИКС

Резервирование и оптимизация систем холодоснабжения ЦОДов

Надежность и резервирование жизненно необходимы для ЦОДов, сбои в работе которых обходятся чрезвычайно дорого. Для систем холодоснабжения, поддерживающих микроклимат в дата-центре, резервирование не только уменьшает риск отказа системы, но и позволяет оптимизировать потребление энергии.

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

Тимур ТОЛОКОННИКОВ,
ведущий инженер отдела
исследований и развития
United Elements

В процессе эксплуатации ЦОДа в нем необходимо постоянно поддерживать микроклиматические параметры, в частности температуру и влажность воздуха в кондиционируемых помещениях. Стандарт США для ЦОДов ANSI/EIA/TIA-942 рекомендует поддерживать температуру воздуха в пределах 20–25°C при относительной влажности 40–50%. Выход за пределы рекомендованного диапазона параметров микроклимата отрицательно влияет на работу оборудования центра и его надежность, может привести к потерям данных и остановке или отказу системы. К примеру, это может вызвать температурные деформации чувствительных компонентов серверов, что приведет к выходу их из строя или сбоям в работе. При пониженной относительной влажности существует угроза самопроизвольного электростатического разряда, который может повредить электронные компоненты или обрабатываемые данные и программное обеспечение. С другой стороны, высокая относительная влажность вызывает конденсацию влаги с сопутствующими короткими замыканиями, коррозией и повышенным износом оборудования. Для повышения надежности системы микроклимата предусматривается ее резервирование.

Табл. 1. Характеристики ЦОДов различных уровней

Параметр	Tier 1	Tier 2	Tier 3	Tier 4
Стоимость сооружения, $/кв.м	4850	6450	9700	11850+
Тип здания	С соседними		Отдельно стоящее	
Схема резервирования компонентов	N	N+1	N+1	2 (N+1) или S+S
Первоначальная мощность, Вт/кв.м	215–323	430–537	430–645	537–860
Максимальная мощность, Вт/кв.м	215–323	430–537	1075–1615	1615+
Бесперебойное кондиционирование	Нет	Нет	Возможно	Есть
Доля фальшполов, %	20	30	80–90	100
Нормативная нагрузка на фальшпол, кг/кв.м	415	488	732	732+
Общая длительность отказов за год, ч	28,8	22	1,6	0,4
Коэффициент эксплуатационной готовности ЦОДа, %	99,6712	99,7488	99,9817	99,9954

Схемы резервирования в ЦОДах

В соответствии со стандартом США ANSI/EIA/TIA-942 ЦОДы делятся на четыре класса (табл. 1). Каждый класс характеризуется минимальным коэффициентом эксплуатационной готовности: этот показатель определяет вероятность безотказной работы оборудования ЦОДа в заданный период времени. Для обеспечения необходимого коэффициента эксплуатационной готовности с целью повышения надежности системы в каждом классе ЦОДов предусмотрены определенные схемы резервирования оборудования.

В ЦОДах класса Tier 1 реализуется схема с N элементами, т.е. резервирование как таковое отсутствует. В данном случае надежность системы зависит от надежности каждого элемента и общего количества элементов, обеспечивающих работоспособность системы.

Для ЦОДов класса Tier 2 и Tier 3 предусмотрена схема резервирования N+1. В данной схеме N элементов обеспечивают работоспособность системы при максимальной производительности и один элемент выступает в качестве резервного. Подключение элементов осуществляется таким образом, чтобы при выходе из строя одного из них суммарная нагрузка равномерно распределялась между оставшимися.

ЦОДы класса Tier 4 имеют схемы резервирования 2(N+1) или S+S. Схемы 2(N+1) или 2N означают организацию параллельного резервирования. В обозначении схемы параллельного резервирования символ S (systems) может иметь, в частности, значение (N+1).

Регулирование производительности чиллеров

Перечисленные выше схемы резервирования применяются и для климатического оборудования, в том числе систем холодоснабжения. В этой связи возникает вопрос распределения мощностей чиллеров как наиболее энергоемких элементов системы холодоснабжения.

Поскольку большинство ЦОДов требуют крупных холодильных мощностей, в них, как правило, применяются чиллеры на базе винтовых компрессоров. Чтобы обеспечить необходимую производительность, в большинстве таких компрессоров используется конструкция, состоящая из осевого подвижного элемента (золотника) и уплотняющего компонента ротора компрессора. Золотник, поступательно перемещаясь вдоль оси ротора, приоткрывает отверстие байпаса, тем самым регулируя производительность. В большинстве одновинтовых чиллеров с двумя золотниками производительность регулируется одновременным (симметричным) перемещением обоих золотников вдоль ротора компрессора (рис. 1).

В асимметричном одновинтовом компрессоре нужная производительность создается за счет полной разгрузки одной стороны ротора компрессора, в то время как другая сторона остается полностью загруженной. Благодаря специальной конструкции одновинтового компрессора обеспечивается эффективный процесс разгрузки. На разгруженной стороне отсутствует компрессия и фактически нет потерь.

Как выбрать оптимальную схему холодоснабжения ЦОДа?

Виктор ГАВРИЛОВ, технический директор компании «АМДтехнологии»

Да еще повысить при этом энергетическую эффективность используемого климатического оборудования? Выбор, удовлетворяющий требованиям конкретного заказчика, в каждом случае зависит от множества факторов. Для построения оптимальной концепции системы кондиционирования необходимо не просто знать, но и уметь применять и сочетать инновационные решения, предлагаемые различными производителями климатического оборудования.

Говоря об использовании чиллеров для оптимизации холодоснабжения, отметим интересные новинки, имеющиеся на рынке. Например, компания RC group разработала чиллеры с системой Free Cooling Optimizer, которая сокращает энергозатраты на 30–40% по сравнению с традиционными системами фрикулинга. Работа системы основана на переменном расходе жидкости вместо постоянного, используемого в стандартных холодильных машинах. В результате переход в режим фрикулинга происходит при температуре наружного воздуха на 4°С выше, чем у традиционных систем.

Заслуживает внимания функциональная схема, поднимающая эффективность совместной работы систем фрикулинга и компрессионного охлаждения для моноблочных чиллеров. Известно, что у подобных холодильных машин этот режим работы самый нестабильный. Так, для высокой производительности чиллера в режиме свободного охлаждения расход воздуха должен быть максимальным, поэтому необходимо включать вентиляторы на наибольшую скорость. Но это приводит к снижению давления конденсации, и для стабильности холодильного цикла нужно, наоборот, снижать расход воздуха в ущерб эффективности. Компания Aermec выпускает чиллеры с отсечением частей теплообменной поверхности конденсатора (четыре ступени), что позволяет поддерживать оптимальное давление конденсации и при этом добиваться максимально возможного теплосъема с теплообменников свободного охлаждения.

Безусловно, заказчику трудно оценить, насколько то или иное решение отвечает его потребностям. Отобрать оптимальные решения, предлагаемые различными производителями, скомпоновать их, адаптировать к реальному объекту, разработать концепцию, отвечающую всем современным требованиям к надежности и эффективности использования климатического оборудования, – дело инжиниринговой компании, проектной организации.

Рис 1. Схема одновинтового компрессора с двумя золотниками (регуляторами производительности)

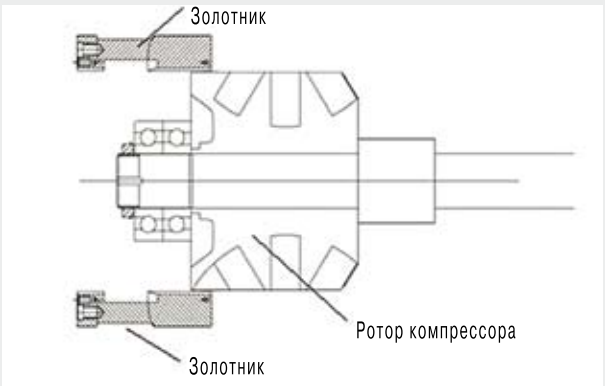
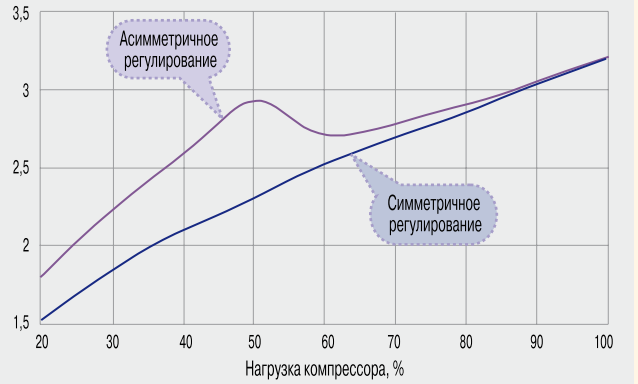


Рис 2. Качественное сравнение одновинтовых компрессоров, работающих со стандартным и асимметричным регулированием производительности



При параметрах нагрузки от 12 до 50% одна сторона винтового компрессора остается в полностью разгруженном состоянии, в то время как золотник на второй стороне перемещается в положение, соответствующее требованиям нагрузки. Для нагрузок в пределах 62–100% верхняя часть полностью загружена, а нижняя часть отрегулирована таким образом, чтобы обеспечивать точное соответствие параметрам загрузки.

В результате эффективность одновинтового компрессора с ассиметричным регулированием производительности в режиме частичной нагрузки будет выше, чем при стандартном регулировании (с симметричным перемещением золотников). Как видно из рис. 2, при ассиметричном регулировании с уменьшением нагрузки коэффициент энергетической эффективности (COP) компрессора увеличивается по сравнению с симметричным регулированием, и наибольшее значение достигается при 50%-ной загрузке компрессора. Этот режим соответствует положению золотников компрессора, когда один золотник полностью разгружен, а второй полностью нагружен.

Таким образом, работа при частичной нагрузке в диапазоне от 50 до 25% представляет интерес с точки зрения оптимизации работы чиллеров при различных схемах резервирования.

Табл. 2. Распределение потребляемой мощности и энергопотребления чиллеров в течение года

Общая хол. нагрузка		Описание работы чиллеров	Время работы		Потребляемая мощность, кВт					Электропотребление, кВт.ч
кВт	%		%	ч	Чиллер 1	Чиллер 2	Чиллер 3	Чиллер 4	Общ	
Схема N										
1800	100	1x100% + 1x100%	9	788	571	571			1142	900 353
1350	75	1x100% + 1x50%	75	6570	571	220			791	5 196 870
900	50	1x50% + 1x50%	16	1402	220	220			440	616 704
Итого				**8760**						**6 713 927**
Схема N+1										
1800	100	1x100% + 1x50% + 1x50%	9	788	571	220	220		1011	797 073
1350	75	1x50% + 1x50% + 1x50%	75	6570	220	220	220		660	4 336 200
900	50	1x50% + 1x25% + 1x25%	16	1402	220	86	86		392	549 427
Итого				**8760**						**5 682 700**
Схема 2N										
1800	100	1x50% + 1x50% + 1x50% + 1x50%	9	788	220	220	220	220	880	693 792
1350	75	1x50% + 1x50% + 1x25% + 1x25%	75	6570	220	220	86	86	612	4 020 840
900	50	1x25% + 1x25% + 1x25% + 1x25%	16	1402	86	86	86	86	344	482 150
Итого				**8760**						**5 196 782**

Оптимизация энергопотребления

В процессе эксплуатации ЦОДа нагрузка на систему холодоснабжения изменяется в течение года и зависит от различных параметров: температуры наружного воздуха, внутреннего тепловыделения и т.п. Резервирование этой системы позволяет включить в работу резервные агрегаты, снизив нагрузку на основные и тем самым повысив эффективность работы.

Рассмотрим систему холодоснабжения ЦОДа, расположенного в Московском регионе, холодильной мощностью 3600 кВт. Для расчета энергопотребления чиллеров в течение года были использованы климатические данные для Москвы, полученные с помощью системы компьютерного моделирования EnergyPlus в формате IWEC (International Weather Year for Energy Calculations – Международный климатический год для энергетических расчетов). Данные отражают почасовой ход параметров воздуха в течение так называемого справочного года, рассчитываемого по данным 30-летних метеорологических наблюдений.

В расчете также учитывалось неравномерное распределение нагрузок на холодильное оборудование от потребителей в течение суток (основная доля приходится на нагрузки от работающих вычислительных средств).

В итоге было определено, что система работает с полной нагрузкой (>90%) только 9% времени. Основной же период времени (75%) система работает с 75%-ной нагрузкой и еще 16% времени – с 50%-ной нагрузкой.

Рассматривалось резервирование чиллеров по трем схемам: N (без резервирования), N+1 и 2N при N = 2. Алгоритм работы схемы с двумя чиллерами по 1800 кВт каждый состоит в следующем. При максимальной нагрузке работают оба чиллера при 100%-ной мощности. При снижении нагрузки до 75% один чиллер продолжает работать на 100%, а второй снижает производительность до 50%. При снижении общей нагрузки до 50% в работе задействованы оба чиллера с 50%-ной нагрузкой каждый (вместо работы одного чиллера на 100%).

Алгоритм работы по схеме резервирования N+1 и 2N аналогичен предыдущей схеме с тем отличием, что нагрузка распределяется с учетом резервных чиллеров.

Данные о годовом энергопотреблении системы при схемах резервирования N, N+1 и 2N представлены в табл. 2. В результате применения резервных чиллеров (так называемое нагруженное резервирование) удалось снизить потребление электроэнергии. В случае применения одного резервного чиллера (схема N+1) потребление электроэнергии снизилось на 1 031 227 кВт·ч, что составляет 15% от энергопотребления по схеме без резервирования. При двойном резервировании (схема 2N) экономия составит 1 517 145 кВт·ч в год, или 22,5% относительно схемы без резервирования.

Резервирование системы холодоснабжения способствует повышению надежности, ремонтопригодности, гибкости и общей энергоэффективности ЦОДа. Существуют различные способы повышения степени резервирования системы. Однако каждый из них следует оценить с позиции способности системы противостоять отказам.

Во всех случаях предпочтительно применение в системах холодоснабжения чиллеров с ассиметричным регулированием производительности. Это позволяет в ходе эксплуатации системы задействовать резервное оборудование для уменьшения нагрузки на основное, реализуя при этом режим горячего резервирования и повышая общую энергоэффективность системы. За счет такого подхода удается наиболее существенно сократить энергопотребление системы холодоснабжения в системах резервирования с относительно небольшим количеством единиц используемого оборудования. ИКС

Навигаторы на платформе SiRFatlasV

Lexand Si-530, Lexand Si-535, Lexand Si-512+ (plus) A5 и Lexand Si-515+ (plus) A5 работают приблизительно на 20% быстрее своих предшественников – навигаторов на основе платформы SiRFatlasIV.

Платформа SiRFatlasV объединяет на одном чипе процессор с тактовой частотой 500 или 667 МГц, автономное DSP-ядро диапазона GPS/Galileo с поддержкой технологии SiRFAlwaysFix, контроллеры памяти DDR2-400, Mobile DDR, SD/MMC/MMC+ и NAND, аудио DAC, контроллер сенсорной панели LCD-дисплея, акселератор постобработки видео, интерфейс USB 2.0 и другие интерфейсы обмена данными. По сравнению с SiRFatlasIV чипсет SiRFatlasV экономичнее – в спящем режиме экономия заряда батареи достигает 10%. Точность определения местоположения увеличилась с 15 до 8 м.

Повышение скорости работы касается как операционной системы Windows CE 6.0, так и фирменного интерфейса, и отображения навигационных карт, и плавности воспроизведения видео (640×480 точек, MPEG4). Поддержка технологии Instant Fix II обеспечивает кэширование данных эфемерид спутников и их прогнозирование на срок до трех дней. В результате навигаторы могут стартовать в «теплом» режиме в течение трех дней с момента последнего включения.

Объем оперативной памяти навигаторов – 128 Мбайт, флеш-накопителя – 2 Гбайт; расширить массив можно с помощью флеш-карт формата MicroSD/MicroSDHC емкостью до 16 Гбайт. Сенсорные дисплеи всех моделей имеют разрешение 272×480 точек, автоматическую регулировку яркости подсветки и антибликовое покрытие.

Каждое из устройств может комплектоваться одним из трех навигационных пакетов, устанавливаемых

во встроенную память: «Навител Навигатор 3.5», «Прогород» или «Сити-ГИД 3.8». Модели Lexand Si-512+ (plus) A5 и Lexand Si-515+ (plus) A5 снабжены модулем Bluetooth, который позволяет загружать информацию о пробках на дорогах с помощью мобильного телефона, выступающего в качестве модема. Благодаря наличию в составе Windows CE 6.0 браузера Internet Explorer навигаторы можно использовать как интернет-планшет.

Лаборатория «Лександ»: (495) 792-5395

Принтер для САПР- и ГИС-приложений

imagePROGRAF iPF755 – 36-дюймовый принтер с возможностью печати изображений формата A0, предназначенный для установки в среде автоматизированного проектирования и геоинформационных систем. Встроенный жесткий диск на 80 Гбайт для хранения заданий пользователя упрощает обработку больших векторных файлов и обеспечивает работу аппарата в многопользовательской среде. Поддерживаются технология обработки изображений L-COA и интерфейс Gigabit Ethernet.

Принтер снабжен панелью управления с ЖК-дисплеем и графической анимацией. Таймер отображает время, необходимое для печати. Корзина большого объема с функцией сортировки предотвращает повреждение отпечатков.

Если при отправке задания на печать тип бумаги, загруженной в лоток, не совпадает с типом материала, заданным в настройках, на рабочей панели появляется соответствующее сообщение, и пользователь может выбрать один из трех вариантов: отменить, продолжить или заменить материал. Параллельно будет выполняться печать следующих заданий в очереди.

Пятицветная система реактивных чернил на основе красителя и пигмента дает насыщенные цвета и четкие тонкие линии (минимальная толщина 0,02 мм, точность ±0,1%). Допускается «горячая» замена чернильниц непосредственно в процессе печати.

Печатающая головка имеет 15 360 сопел, благодаря чему разрешение изображений составляет 2400x1200 точек на дюйм. Лист формата A0 в черновом режиме печатается за 48 с.

iPF755 поддерживает стандарт HP-GL/2 и HP-RTL, включая настройки палитры и пера. Помимо драйвера HDI для пользователей AutoCAD и Microsoft Office в комплект поставки входит специальный модуль, позволяющий печатать документы Word, Excel и PowerPoint, не выходя из соответствующего приложения. Также в комплект включены модуль Microsoft Office и драйвер HDI для Windows.

Для экономии пространства в офисе принтер можно встраивать в стену.

Canon: (495) 258-5600

Моноблок для бизнеса

DEPO Neos 440AIO22 может комплектоваться двухъядерными процессорами Intel Celeron Dual Core, Intel Pentium Dual Core или Intel Core 2 Duo. Он поддерживает до 4 Гбайт оперативной памяти (DDR3-1066) и жесткие диски с интерфейсом SATA II емкостью от 250 до 500 Гбайт. Интегрированный графический адаптер Intel GMA X4500 позволяет выводить изображение 16:9 с максимальным разрешением 1920×1080 точек (стандарт Full HD). В конфигурацию ПК входят накопитель DVD±RW и устройство для карт памяти SD/MMC/MS/MS Pro.

Интерфейсные возможности представлены интегрированным гигабитным сетевым контроллером, модулями беспроводной связи Wi-Fi (802.11 b/g/n) и Bluetooth, шестью портами USB 2.0, разъемами для подключения дополнительного монитора, наушников, микрофона и динамиков.

Моноблок оснащен сенсорным экраном 21,5" с поддержкой технологии MultiTouch. Размеры – 550×380×48 мм (Ш×В×Г). Имеется возможность настенного монтажа и регулировки угла наклона при установке на столе.

Дополнительное оборудование – TV-тюнер с пультом ДУ, динамики мощностью 5 Вт на передней панели и веб-камера.

На DEPO Neos 440AIO22 устанавливаются операционные системы семейства Windows 7.

DEPO Computers: (495) 969-2222

ПО для мониторинга инфраструктуры ЦОДа

Новая версия APC InfraStruxure Management Software осуществляет активное управление всей инфраструктурой ЦОДа: системами энергоснабжения, охлаждения, распределения электропитания на уровне стойки, а также системой безопасности.

Модуль InfraStruxure Efficiency 1.1 обеспечивает генерацию отчетов о месячном энергопотреблении подсистем ЦОДа, а также о выбросах CO_2, эффективности энергопотребления (PUE) и эффективности инфраструктуры ЦОДа (DCIE). Расчет стоимости потребляемой энергии и количества выбросов CO_2 может настраиваться пользователем или производится автоматически с учетом информации о выбросах CO_2 в местных системах генерации электроэнергии.

Обновленное решение InfraStruxure Capacity предоставляет возможность оповещения специалистов в случае повышения температуры или выявления других факторов среды, которые могут повлиять на работу компьютерного оборудования. Функции InfraStruxure Operations 6.1 Capacity Manager позволяют задавать пороги, формировать специализированные отчеты и автоматически готовить рекомендации по решению критических проблем, в том числе при переносе виртуальных машин. Новая утилита управления сетью в составе InfraStruxure Capacity помогает определить зависимость между различными устройствами, рассмотреть построение карт волоконно-оптических и проводных сетей от серверов через патч-панели к маршрутизаторам и коммутаторам.

APC by Schneider Electric: (495) 620-9095

Powerline-адаптер с беспроводной точкой доступа

Адаптер DHP-W306AV позволяет использовать существующую электропроводку для создания домашней или офисной сети передачи данных, подключать пользователей к беспроводной сети, а также увеличивать радиус ее действия.

Адаптер поддерживает беспроводной интерфейс IEEE 802.11b/g/n и обеспечивает скорость передачи данных до 300 Мбит/с при работе с устройствами 802.11n. Он оснащен портом 10/100BASE-TX Fast Ethernet для подключения цифровых медиаустройств, компьютеров, игровых консолей и сетевых хранилищ.

DHP-W306AV совместим с устройствами стандарта HomePlug AV и способен осуществлять передачу аудио/видеоконтента в условиях помех, создаваемых бытовыми приборами в электросети. Он включается непосредственно в электрическую розетку; скорость передачи данных по электропроводке может достигать 200 Мбит/с.

Схема организации беспроводной сети на основе DHP-W306AV

Сетевой адаптер поддерживает функцию приоритизации трафика, обеспечивая работу чувствительных к задержкам приложений. Для защиты данных, передаваемых по проводной и беспроводной сети, в адаптере реализована поддержка шифрования AES с длиной ключа 128 бит, а также протоколов WEP, WPA/WPA2 и технологии WPS.

DHP-W306AV поддерживает режим экономии питания. Если в течение определенного времени не выполняются передача или прием данных, адаптер автоматически переходит в режим ожидания для сохранения энергии.

D-Link: (495) 744-0099

Блог, еще раз блог!

Владимир ЛИТВИНОВ

Шесть директоров за 10 лет

>>>> На заочном собрании «Ростелекома», которое состоится 10 ноября, предлагается «выплатить дивиденды по результатам девяти месяцев 2010 финансового года в следующем размере:

– 0,000000411722654% чистой прибыли на одну привилегированную акцию;

– 0,000000274519684% чистой прибыли Общества на одну обыкновенную акцию».

Вот за такое решение предлагается проголосовать. Естественно, прежде чем голосовать, адекватному акционеру хотелось бы понять, что реально скрывается за этими цифрами с многочисленными нулями (1 руб., а может, 0,1 руб.). Но по неведомым для акционеров причинам сообщить реальные цифры дивидендов совет директоров «Ростелекома» отказывается. Я предпринял попытки понять суть вопроса, но лишь в одном случае получил вразумительный ответ: на момент назначения даты собрания еще не были известны результаты работы компании за 9 месяцев. Но позвольте, почему тогда созывается собрание и многотысячным тиражом рассылаются письма акционерам с закамуфлированными формулировками размера дивидендов. Должен сказать, что, на мой взгляд, в последнее время наш лексикон грешит малопонятной для широкого круга образованных людей терминологией (нанотехнологии и т.п.).

Кстати, символично, что количество нулей (шесть) после запятой в размере дивидендов соответствует числу гендиректоров «Ростелекома» после отставки основоположника компании – первого гендиректора Олега Белова. Сохраним для истории их имена: Николай Королев, Сергей Кузнецов, Дмитрий Ерохин, Константин Солодухин, Антон Колпаков, Александр Провоторов. И это за рекордно короткий срок – порядка десяти лет. То есть на одного топ-менеджера в среднем приходилось 1,5 года работы. Едва очередной гендиректор успевал создать новую команду, разработать и озвучить в СМИ очередную стратегию диверсификации бизнеса оператора, следовала отставка… Призванный в пожарном порядке последний гендиректор не имеет питерских корней, впрочем, его миссия временная – он должен произвести «зачистку» на местности консолидируемой компании. А в новоиспеченный «Ростелеком» должен заступить и, похоже, на длительный срок однокурсник президента Вадим Семенов. При этом просто не понимаю, на какие обещания в отношении главной должности в «Ростелекоме» рассчитывал уже бывший гендиректор «Связьинвеста» Евгений Юрченко.

комментировать

Наталья КОРОТКОВА

Негритянки в кокошниках

>>>> В субботу меня пригласили на прямую трансляцию премьеры оперы «Борис Годунов» в «Метрополитан Опера». Проект называется The Met – Live in HD и представляет собой 12 спектаклей ежегодно, транслируемых в прямом режиме. Он организован при поддержке The Neubauer Family Foundation и информационном участии агентства Bloomberg.

Интересно было наблюдать, как технологии меняют восприятие события. Я, например, сразу задумалась, что надеть. Ведь, с одной стороны, я иду на премьеру оперы в крупнейший оперный театр. С другой стороны – просто в кинотеатр. Видимо, не одна я задумалась об этом, потому что в зале я заметила как любителей оперного искусства в джинсах, так и дам с бриллиантами и в декольте!

Также интересно было думать о глобализации. Вот одна из известнейших русских опер. Ее ставят при участии русских артистов в Нью-Йорке. Транслируют по всему миру. В итоге я, москвичка, находясь во Франции, смогла посмотреть практически «вживую» оперу Мусоргского, поставленную в Нью-Йорке.

Пять часов в кинозале – это нелегко, но негритянки в кокошниках, немецкий исполнитель партии Бориса Годунова, старательно выговаривающий русские слова, прямые интервью с Гергиевым, Нетребко и другими оперными знаменитостями того стоят. Я думаю, что в дальнейшем число таких проектов будет расти. Конечно, это нишевый формат, и оперы не будут транслироваться в спортбарах. Но кинотеатры вполне могут использовать прямые трансляции из оперных театров как возможность привлечь еще один сегмент зрителей. Предложить им шампанское «Вдова Клико» взамен попкорна.

комментировать

Михаил ЕЛАШКИН

Я против кириллических доменов

>>>> Как вы, наверно, знаете, я всегда был против кириллических доменов как глупого и бессмысленного занятия. Но… я и против локализации «винды» всегда был – как глупого занятия. Однако против природы не попрешь – стада леммингов не хотят говорить на иностранных языках, чему порукой 300 тыс. доменов в первый день. Для сравнения: в .SU – 89 тыс., а всего в .RU чуть больше 3 млн доменов.

В общем, лед тронулся. Как русские имена файлов и меню «Файл» пробились под солнцем, так и национальные алфавиты попрут теперь. Мы с китайцами… А ведь были времена, когда ASCII был семибитным…

комментировать

Реклама в номере

АЛЮДЕКО-К
Тел./факс: (4942) 31-1733
E-mail: sales5@aludeko.ru
www.aludeko.ru . . . . . с. 13

АМДТЕХНОЛОГИИ
Тел.: (495) 963-9211
Факс: (495) 225-7431
E-mail: info@amd-tech.ru
www.amd-tech.ru . . . . . с. 90

АРМО-СИСТЕМЫ
Тел.: (495) 937-9057
Факс: (495) 937-9055
E-mail: armosystems@armo.ru
www.armosystems.ru . . . с. 37

ПИК НТЦ
Тел.: (8332) 37-6137
Факс: (8332) 37-6138
E-mail:pik@pik.kirovcity.ru
www.pik.kirovcity.ru . . . . с. 43

APC BY SCHNEIDER ELECTRIC
Тел.: (495) 916-7166
Факс: (495) 620-9180
E-mail: apcrus@apc.com
www.apc.ru . . . . . с. 87

DATADOME
Тел.: (495) 580-7348
Факс: (495) 665-6200
E-mail: info@datadome.ru
www.datadome.ru . . . с. 75, 84

EATON
Тел.: (495) 981-3770
Факс: (495) 981-3771
E-mail: UPSRussia@eaton.com
www.eaton.ru . . . . . с. 91

EDGE-CORE NETWORKS
Тел.: (916) 625-8272
E-mail: russia@edge-core.com
www.edge-core.com. . . . с. 23

HUBER+SUHNER
Тел.: (495) 775-6653
Факс: (495) 775-7794
E-mail: info.ru@hubersuhner.com
www.hubersuhner.ru . . . с. 88

LANDATA-EATON
Тел.: (495) 925-7620
Факс: (495) 925-7621
E-mail: info@landata.ru
www.landata.ru . . . . . с. 85

LENOVO
Тел.: (495) 663-8260
Факс: (495) 663-8261
www.lenovo.com/ru . . . . . с. 3

MOTOROLA
Тел.: (495) 785-0150
Факс: (495) 785-0160
E-mail: info@motorola.ru
www.motorola.ru . . . . . с. 49

QNAP
Тел.: (495) 772-9909
www.qnap.ru . . . . . с. 35

RADWARE
Тел.: +972 (3) 768 9643
E-mail: info_cis@radware.com
www.radware-rus.ru . . с. 58,59

UNITED ELEMENTS
Тел./факс: (495) 790-7434
E-mail: center@uelements.com
www.uel.ru . . . . . с. 83

VERYSELL
Тел.: (495) 777-2626
Факс: (495) 777-2629
E-mail: pr@verysell.ru
www.verysell.ru . . . . . с. 25

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.