Под давлением негатива

В октябре-ноябре падение на российском рынке акций усилилось в условиях неблагоприятной внешней конъюнктуры – как в Европе, так и в США. Сектор телекоммуникаций не смог избежать влияния общерыночного негативного тренда.

Анна ЗАЙЦЕВА,
аналитик,
УК «Финам Менеджмент»

Развитию минорных настроений на рынке способствовали отсутствие прогресса в урегулировании долговых проблем Греции и Испании, слабый эффект QE3 и масштабный ураган «Сэнди» в США, из-за которого торги на американских биржах были остановлены на несколько дней, – и это накануне президентских выборов, когда рынки традиционно демонстрируют растущий тренд.

Негативный внешний фон оказывал значительное давление и на российские площадки. Начало ноября отечественные биржи провели в боковом движении: ожидания развязки президентских выборов в США сдерживали инвесторов от активных действий. Однако информация о победе Обамы спровоцировала масштабные распродажи рисковых активов на американских биржах. Кроме того, инвесторы вновь заговорили об угрозе «фискального обрыва». На этой почве российские индексы продолжили падать, но ощущение перепроданности рынка удерживало участников от масштабных распродаж.

Рост в порядке исключения

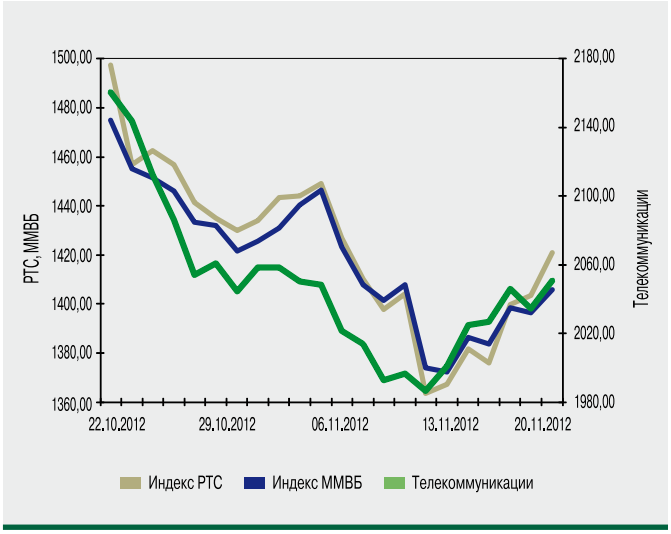
Бумаги телекоммуникационного сектора в октябре зафиксировали значительное снижение. Исключение составили только акции МТС, которым на позитивных корпоративных новостях удалось закрыть месяц ростом в 1%, до уровня 233,69 руб. В акциях оператора отмечалась высокая волатильность – инвесторы реагировали на новости о компании весьма эмоциональной торговлей: после покупок следовала немедленная фиксация. Основные новости пришли на рынок в начале ноября. Так, разрешился затяжной конфликт в Узбекистане: апелляционная коллегия Ташкентского городского суда по уголовным делам отменила постановление об обращении в доход государства имущества ООО «Уздунробита», 100%-ной «дочки» МТС. Суд определил объем финансовых претензий к «Уздунробите» в размере порядка $600 млн с возможностью выплаты этой суммы в рассрочку в течение восьми месяцев. Порадовала компания инвесторов и своим отчетом. Так, чистая прибыль группы МТС за III квартал 2012 г. по US GAAP выросла на 74% – до $630 млн, а консолидированная выручка группы, номинированная в долларах, в III квартале осталась стабильной в квартальном исчислении и составила $3,132 млрд.

Бумаги «Ростелекома» в рамках негативного общерыночного тренда потеряли 8,8%, опустившись к отметке 120,48 руб. за акцию. Корпоративные новости также не способствовали активизации покупок. Ожидаемыми для рынка оказались результаты по РСБУ за 9 месяцев 2012 г., согласно которым чистая прибыль «Ростелекома» выросла на 38% – до 32 млрд руб. Абонентская база оператора увеличилась в III квартале до 13,55 млн пользователей (12,9 млн в предыдущем квартале). Однако поводом для массовых распродаж акций «Ростелекома» стала информация о проведенных сотрудниками МВД обысках в доме главы компании Александра Провоторова, а также в доме ее крупнейшего миноритария (владеет 10,4% акций)

Справка ИКС

За месяц, с 20 октября по 20 ноября, индекс ММВБ потерял 4,36%, откатившись к отметке 1396,39 пункта. Индекс РТС снизился на 5,5%, остановившись на уровне 1403,59 пункта. Рост индекса «ММВБ телекоммуникации» за рассматриваемый период составил 4,76% – до уровня в 2034,24 пункта.

Динамика биржевых индексов
в период с 22 октября по 20 ноября 2012 г.



и основателя фонда Marshall Capital Константина Малофеева. Обыски проводились в связи с подозрением в хищении кредита на $225 млн, полученного от ВТБ (напомним, что в 2007 г. банк выдал кредит «Русагропрому» на покупку у Nutritek Group молочных заводов, принадлежащих компаниям г-на Малофеева). В свою очередь, г-н Провоторов в 2006 г. являлся одним из топ-менеджеров фонда Marshall Capital. На этой новости бумаги «Ростелекома» в моменте теряли свыше 4%, но в ходе торгов их снижение нивелировалось, и к закрытию сессии коррекция по акциям составляла порядка 2%.

Бумаги VimpelCom Ltd. снизились на 2,52%, достигнув отметки $10,81. Компания опубликовала ряд позитивных корпоративных новостей, однако преобладание коррекционных настроений на рынках не позволило котировкам акций расти. Оператор решил отказаться от активов в Африке и Азии; вместо этого VimpelCom намерен сконцентрироваться на более развитых рынках – таких как Россия и Италия, составляющих 70% его бизнеса. Компания уже приступила к переговорам с потенциальными покупателями о продаже части бизнеса в Бурунди, в Центрально-Африканской республике и в Зимбабве. Эти три актива оценены в сумму более $60 млн – они приносят около $94 млн выручки ежегодно. Помимо этого, сдвинулся с мертвой точки конфликт крупнейших акционеров группы. В конце октября Altimo Holdings & Investments Limited увеличила голосующую долю в Vimpelcom Ltd. с 41,9 до 47,85%. 26 октября Altimo Coop и кипрская Bertofan Investments Limited договорились о купле-продаже конвертируемых привилегированных акций Vimpelcom. В соответствии с договором Altimo Coop должна приобрести у Bertofan 123 млн 600 тыс. привилегированных акций на общую сумму $217,536 млн. Таким образом, Altimo станет крупнейшим акционером Vimpelcom. Через несколько дней после выхода данной новости в СМИ появилась информация о том, что Telenor может продать свою долю в холдинге Vimpelcom, однако позже данная информация не подтвердилась.

Не выбраться из тренда

Наибольшие потери за рассматриваемый период понесли акции РБК, снизившиеся в цене на 9,07%, до 13,787 руб. за бумагу. Акции медиахолдинга уже давно не могут выбраться из длительного нисходящего тренда, а прошлый месяц еще больше усилил их падение и поставил перед бумагами РБК новые уровни поддержки, вернув их значение на начало 2012 г. – к 13,8 руб. за бумагу.

Капитализация АФК «Система» снизилась на 7,58%, составив 23,289 руб. Если в октябре акции компании снижались вслед за рынком, то уже в ноябре, после нескольких новых крупных сделок, бумаги «Системы» принялись отыгрывать потери. Компания продолжила диверсифицировать бизнес, заключив еще несколько сделок. В частности, она объявила о возможной консолидации европейской нефтяной компании Argos Group Holding B.V.; кроме того, «Система» приобрела 100% голосующих акций в уставном капитале ОАО «Верофарм».

Акции IBS Group просели на 4,32%, в результате чего стоимость ценных бумаг компании составила $16,6.

Распродажа активов?

Среди российских интернет-компаний наибольшее падение зафиксировали бумаги Mail.Ru Group (на 4,81%, до $30,7). Еще в октябре акции холдинга хорошо росли на фоне публикации промежуточных неаудированных результатов за III квартал 2012 г.– совокупная сегментная выручка увеличилась на 36,5% по сравнению с аналогичным периодом 2011 г., достигнув 4,965 млрд руб. Компания сообщила об уменьшении своей доли сразу в нескольких активах. Так, был продан пакет социальной сети Facebook, и теперь доля Mail.Ru Group составляет 0,52%. Позже стало известно, что Mail.Ru Group полностью вышла из состава акционеров Groupon и Zynga. Предполагается, что вырученные средства компания направит на дивиденды или покупку российских активов – возможно, сети «ВКонтакте».

С минимальными потерями завершили прошлый месяц акции российского поисковика Yandex (снижение на 0,31%, до уровня $22,17). Хорошим поводом для роста компании послужила публикация отчетности по US GAAP: согласно представленным данным, чистая прибыль Yandex за III квартал 2012 г. достигла 2,3 млрд рублей ($74,2 млн), увеличившись на 34% по сравнению с аналогичным показателем III квартала 2011 г. Рентабельность по чистой прибыли составила 32%. Консолидированная выручка выросла по сравнению с показателем того же периода прошлого года на 41% – до 7,3 млрд руб. ($235,2 млн). Однако рост акций российского поисковика на данной новости был краткосрочным, позже бумаги компании показывали планомерное снижение. ИКС

В ИТ – незначительная облачность

Вы прочитали об облачных технологиях десятки статей, были на конференциях и презентациях, но «облачно» в вашей организации не стало? Помимо очевидных, тому есть скрытые причины, на первый взгляд не относящиеся к облачной теме, но тормозящие внедрение и развитие частных облаков.

Александр ШИБАЕВ, начальник управления эксплуатации обеспечивающих систем, МЦИ Банка России

Дело в том, что облачная революция изменяет весь уклад привычной и где-то даже размеренной айтишной жизни. Не оговорился ли автор? Модернизации, инновации, бесконечные решения и предложения, внедрения и адаптация к требованиям бизнеса – и это размеренная жизнь?! Увы! Это напряженная жизнь извозчиков начала 20-го века – сено не завезли, сбруя износилась, лошади не чищены... А автомобили уже появились. И счастливые обладатели роскошных экипажей и конюшен внезапно оказались перед дилеммой – проверенная лошадь и логистика поставок фуража либо непонятный автомобиль и трудности с техобслуживанием. Может, не надо ничего менять, подождем годик-другой, а там видно будет?

В информационных технологиях сейчас такой же революционный момент.

Идет облачная революция. Почему же не «застилают небо» частные облака? Я привел некоторые ответы гипотетических организаций на этот вопрос.

«У нас все работает»

Это не совсем так. Полгода на техническое задание, год на реализацию при непомерном (на взгляд бизнеса) бюджете – таков типичный график работ ИТ-подразделения. Плюс постоянные модернизации и устранение аварий. Бизнес-подразделения такая ситуация едва ли устраивает. Коллеги-айтишники, обратите внимание: все идет как обычно, а ваша ценность для организации снижается. Вы еще не почувствовали этого?

Бизнесу требуется надежная стабильная работа плюс быстрая адаптация к меняющимся требованиям – невозможный сплав желаний в рамках ИТ-понятий 20-го века. Но 21-й век понятия меняет.

Бизнес ищет, где полнее и оперативнее удовлетворяются потребности, меньше проблем и дешевле. Вполне житейская логика. Поэтому рано или поздно бизнес-подразделение найдет внешнего облачного провайдера, подключится к нему и решит все проблемы, например с офисным документооборотом.

Что делать? Понять, что эра уникальных ИТ-решений для каждого потребителя прошла. Информационные технологии хотят потреблять люди, не знающие, что такое «протокол» и «интерфейс». Чтобы пользоваться ИТ-услугами, как водой и электричеством. Уникальную джакузи наполняют стандартной водой, подключив к стандартному вентилю и стандартной розетке. Это пользователь делает сам и с удовольствием!

Отбросьте убеждение (ложное!), что бизнесу некуда податься и он будет вечным просителем у информатизаторов. На ваше место придет надежный, недорогой и гибкий облачный оператор и предоставит услугу, а CAPEX превратится в OPEX.

Осознайте, что 2013 г. станет переломным, и понятие «создать» приложение (или программный комплекс), т.е. создать силами ИТ-подразделения, трансформируется в понятие «скомпоновать приложение», с чем пользователь будет справляться сам. Так поступите мудро – дайте пользователю возможность самому создавать себе виртуальный компьютер и выбирать приложения.

«Все как сервис» – и вас будут любить, как любят Google и Apple!

Но не всех, а тех, кто не будет уволен.

Подразделения информатизации и информационной безопасности не без оснований видят в частном облаке угрозу своим рабочим местам. Несколько тысяч «гугловцев» обслуживают несколько десятков миллионов пользователей. В вашей организации такое же соотношение? Собственных сисадминов уже уволили сотни, может быть, тысячи средних и мелких предприятий, переключившихся на услуги облачных провайдеров.

В некоторых организациях доказательства «вредности» частного облака имеют конечной целью лишь сохранение привычного уклада и рабочих мест подразделений информатизации. Какое-то время это будет работать – до конца 2012 г. Дальше аргумент «у нас все работает» перестанет быть вашим оправданием. По моему опыту, для администрирования облака организации до 1000 человек нужны два администратора и договор на техподдержку. Задумайтесь!

«У нас уже все виртуализировано»

Это очень хорошо. Подавляющее большинство организаций в мире используют виртуализацию. Однако ответьте, вы гарантируете доступность и

работу сервиса? Готовы к резкому всплеску нагрузки? Вы в курсе того, что происходит в виртуальной среде? А старинное приложение под NT почему не на виртуальном сервере?

Виртуализация – еще не облако. Виртуализация – это в первую очередь повышение эффективности использования оборудования и радикальное ускорение развертывания систем. Это первый шаг в будущее. Она позволяет расцепить (навсегда!) приложение и «железо», т.е. выход из строя любого элемента оборудования не влияет на работу приложения – в крайнем случае, вызывает паузу в несколько секунд на миграцию виртуальной машины на другой физический сервер.

Время развертывания серверов и приложений сокращается драматически – с месяцев до часов. Экономятся электроэнергия, место в серверном помещении и деньги на приобретение серверов под отдельные задачи. Появляется возможность маневра, перераспределения ресурсов, что недостижимо в физическом мире. Может быть, вы даже планирование осуществляете на основе анализа нагрузки, а не на основе заявок пользователей, которые всегда хотят больше и сразу.

Все это так. Но кто и как использует ресурсы? Не простаивают ли виртуальные машины вследствие неправильного начального заказа ресурсов? Или по той же причине какое-то приложение работает медленно и требуется добавить мегабайт-мегафлопов, но вы об этом не знаете? А если большие ресурсы нужны только в конце месяца, а остальное время приложение не используется?

И главное – ИТ-администратор по-прежнему все делает сам. Создает, мониторит, управляет, ошибается, кстати, и не успевает.

Облако позволит избавить администратора от рутины: часть функций выполняется автоматически, часть – переходит к пользователю (в режиме самообслуживания).

В ИТ-подразделениях неотвратимо грядет дифференциация: одни будут «творить решения», другие – дежурить и менять в стойках типизированные «серверные элементы». Но и теми и другими кто-то должен управлять – ИТ-менеджмент не исчезнет!

При этом работа ИТ-подразделения серьезно трансформируется: обслуживание огромного количества пользовательских устройств, инсталляция и настройка приложений и т.д. превращаются в операторскую деятельность по управлению облаком. Для этого необходимо срочно осваивать и внедрять новые технологии – динамический, программно-определяемый центр обработки данных, программно определяемые сети (SDN). Без этого не достичь требуемых бизнесу гибкости, надежности, эластичности, абсолютной доступности.

Облачная технология позволит контролировать потребление сервиса. Это важно. Сложилось устойчивое мнение, что «администраторов много и они ничего не делают». Работы у администраторов действительно много, причем разноплановой, интересной и не очень – от творческого решения технологической задачи до рутинного поиска неисправности и профилактических работ.

Облако позволит реально измерить и «монетизировать» работу ИТ-служб в договорных единицах – бонусах, баллах, тугриках. Все в мире имеет цену... кроме заявки от бухгалтерии установить к утру новую версию программы отчетности. Но, оформляя в облачном «столе заказов» свою заявку и видя прайс-лист услуг, бухгалтер удивится самому факту наличия цены и задумается, так ли уж нужен этот заказ. Я знаю случай, когда заявка на установку приложения на нескольких десятках рабочих мест в офисах по всему городу превратилась в заявку на пять мест в соседней комнате.

Учет потребляемых ресурсов или сервисов (в облаке доступны обе модели) – важнейшая функция облака. Именно учет и тарификация позволят перейти к понятию «сервис». Высокодоступный, оптимальный по цене, гибкий по настройке сервис – эта мечта пользователя должна стать целью ИТ-подразделения. Облако позволяет этой цели достичь.

Не облачные технологии – цель ИТ-подразделений. Они лишь средство. Цель – предоставить сервис.

Для этого необходима реорганизация ИТ-деятельности. Принципы и методы изложены и описаны давно. Это стандарты и рекомендации ITSM, ITIL, COBIT и др.

Итак, от виртуальных серверов мы подошли к основам основ – организации ИТ-процесса.

«У нас уже внедрены процессы управления инцидентами...»

Этого недостаточно. Можно сказать, что облачная технология для виртуальных серверов – это полнофункциональная система автоматизации на принципах ITSM. Вообще, облако – самое комплексное, самое полное решение по построению ИТ-процессов на основе ITSM. Облако и ITSM неразлучны.

Облако помогает правильно организовать взаимодействие как внутри ИТ-службы, так и с пользователями. Сервис – деятельность, имеющая ценность для потребителя. Организуйте предоставление сервиса в облаке в соответствии с принципами и правилами ITSM, т.е. перейдите от понятия «дисковое пространство» к «услуге хранения данных», и ваша работа обретет ценность. Вы быстро научитесь учитывать требования, контролировать качество, увидите узкие места и начнете мыслить категориями сервиса. И вас начнут лучше понимать бизнес-подразделения.

Фактически облако – это ITSM-каркас, который максимально облегчит преобразование ИТ-службы.

Вас удивляет, что говоря об облаке, я не оперирую техническими терминами? Не рассуждаю о готовности вашего ЦОДа стать «динамическим»? О трудностях предоставления приложений в виде сервиса?

Уверяю вас, технические вопросы второстепенны. Переход в облако требует изменения «информационной» философии. Взрывной рост Интернета в 2010–2011 гг. был вызван не в последнюю очередь абсолютным упрощением подключения к Сети с любого

устройства. Никаких патчей, настроек каналов, конфигурирования протоколов! Пользователи стали просто людьми, пользующимися Интернетом. И вообще, в слове «пользователь» есть завуалированный намек на некую техническую неграмотность. Это нехорошо! Но облако выручает и здесь.

Сложность облачной технологии скрыта от пользователя. Он просто пользуется. А профессионалы информационных технологий выполняют свою сложную работу, не докучая ему непонятными вопросами.

И все взаимодействуют на принципах ITSM.

«Облако небезопасно»

Это серьезно. Вы хотите и даже обязаны достоверно знать, кто имеет доступ к вашей информации. И тут понятие «облако» играет против себя – раз в облаке, значит, неизвестно где и неизвестно кто читает и изменяет ваши данные. В целом мысль неверная, но на 50% правда. Парадокс? Ничуть.

Загадка: «Неизвестно, где лежит информация, и неизвестно, кто ей пользуется. Что это?» Это Интернет. Кстати, никого это не смущает, таковы правила игры. Пароли и правила доступа затрудняют работу хозяина информации, но ответа на вопрос, не обошел ли кто-то эти правила, не дают. На первый взгляд, и в облаке так же, но только на первый.

Должен признать, что информация в облаке действительно лежит неизвестно где. «Ага, попался! – воскликнут скептики, – мы так и знали, облако – ”проходной двор”». Уважаемые скептики, мы знаем, где лежит информация, только когда речь идет о собственном компьютере или флешке. Все!

Технология RAID не позволяет сказать, на каком серверном диске находится информация. SAN и NAS вычеркивают из «адреса» информации понятие «сервер», заменяя его на бесконечное понятие «сеть». Виртуализация переводит адрес хранения информации в понятие географическое – в ЦОДе на такой-то улице. Вы не ошибетесь, только если скажете, что информация находится где-то на планете. Но я уже слышал о космических веб-серверах.

Таким образом, мы должны выбрать уровень неизвестности. Но существует жесткая зависимость – чем точнее адрес, тем менее надежно хранилище. Диск вполне может выйти из строя, и информация пропадет, а выход из строя ЦОДа весьма маловероятен, к тому же серьезный ЦОД катастрофоустойчив и информацию можно хранить на нескольких ЦОДах в масштабе планеты.

Облака живут в ЦОДах. Поэтому, выбирая облако, вы выбираете высший уровень надежности хранения и вполне приемлемый ответ на вопрос «где?» – в ЦОДе.

Информационная безопасность должна знать точный ответ не на вопрос «где?», а на вопрос «кто?». Кто имеет права доступа к информации, как информация защищена от уничтожения/искажения, кто ее читал и кто пытался прочитать? Система информационной безопасности в облаке должна отвечать на эти и массу других вопросов.

Но не отвечает.

В настоящее время нет решения для частного облака от одного поставщика, в котором реализованы все требования информационной безопасности и тем более с российскими особенностями. Если на рекламных презентациях вы слышите, что «в решении нашей фирмы реализованы все требования ИБ, и мы советуем информацию при хранении шифровать», то знайте, что продавец, подстраховываясь шифрованием, скрывает прорехи в своей системе безопасности. Зашифрованную информацию, конечно, чужой не прочтет, но попытаться может.

Поэтому для обеспечения информационной безопасности необходимо использовать решения нескольких поставщиков. Это удорожает частное облако, усложняет работу администраторов, но чудесным образом закрывает большую часть возможностей нарушить и снимает большую часть ответственности с плеч пользователя. Пользователь – вечное слабое звено классической информационной безопасности. Поэтому защита персональных компьютеров, сетей, баз данных сложна, требует огромных затрат, никак не меньших, чем возможные затраты на ИБ в частном облаке. Но вредный пользователь способен не выполнять требования безопасности на своем ПК, вторгаться в работу сети, несанкционированно подключаться к базам данных и нарушать, нарушать, нарушать...

В облаке возможности нарушения сведены к минимуму – пользователь может только то, что разрешено. А возможности контроля, противодействия и упреждения всевозможных нарушений ИБ в частном облаке максимальны, практически абсолютны.

В Банке России мы создали макет облачной инфраструктуры* и проверили возможность соблюдения действующих у нас жестких правил информационной безопасности. Набор из нескольких продуктов разных поставщиков обеспечил выполнение всех правил. Получены ответы на все волнующие ИБ-службу вопросы, замечены и предотвращены все несанкционированные попытки, все санкционированные учтены. Нарушения ИБ обнаруживаются и пресекаются on-line и on-time и не требуют комиссий по расследованию инцидента.

Можно констатировать – частное облако безопасно. Про публичное так сказать нельзя.

Выше я обрисовал ряд ключевых моментов в движении к частному облаку, вам осталось только создать его. Чтобы что-то создать, надо что-то купить – частное облако требует «стройматериалов». Что купить и где?

Что нам предлагают в фантике «частное облако»?

Уважаемый читатель! Если вы успели подумать, что я – «по другую сторону баррикад», то теперь вы уж точно увидите, что мы вместе и у нас общие интересы. Все, что сказано выше, обращено внутрь организации –

*А. Шибаев. Из тумана – в облака. «ИКС» № 6’2012, с. 67; № 7-8’2012, с. 64.

потенциального создателя частного облака. А снаружи творятся интересные дела.

Маркетинговый нажим и всепроникающая реклама сделали понятие cloud флагманом, локомотивом, драйвером и все-всем-всем в ИТ-индустрии. В 2011 г. большие начальники крупных организаций оказались в ситуации, когда они знают о передовой технологии больше любого своего системного администратора. Высокие обсуждения с высоких трибун, «национальные облачные платформы», облачные операторы, масса cloud-возможностей и cloud-продуктов... Продавцы предвкушали всплеск спроса, аналогичный спросу 1999 г. в связи с «истерикой-2000».

Я пошел на этот кипящий облачный ИТ-рынок в ноябре 2011 г. Оказалось, что под маркой «частные облака» продаются совершенно разные вещи, иногда имеющие весьма отдаленную связь с понятием «облако».

Москвичи знают, что лучшие огурцы растут в Луховицах. Продавцы знают, что лучше всего продаются огурцы из Луховиц. Спросите любого продавца на любом рынке: «Откуда огурцы?» – «Из Луховиц». Только почему-то надписи на коробке по-турецки.

С продажей облаков абсолютно так же, как с огурцами из Луховиц, но с добавлением ИТ-специфики.

Например, отдел продаж ПО крупного производителя решил, что облако поможет увеличить продажи, и сформировал под маркой «частное облако» набор имеющихся в распоряжении продуктов для управления всей ИТ-инфраструктурой. У покупателя круглые глаза – оказывается, надо покупать кучу лицензий, требуется огромная работа по инсталляции, и возникают большие сомнения в возможности охвата всего имеющегося разнообразия оборудования и приложений. Покупатель озадачен.

Другой отдел этого же производителя тоже перестроился и продает нечто под лозунгом «облако – это ЦОД в одном шкафу». «Покупатель, забудьте все, что у вас есть, и купите новый спецкомплект – блейд-серверы, системы хранения, ПО управления... Высокая надежность, использование нескольких недорогих серверов повышает гибкость и облегчает ремонт...». Оказывается, для облака нужно покупать «железо», да не простое, а облачно-ориентированное! Покупатель в недоумении.

Но есть третий отдел, который решил поправить бизнес по продаже «тяжелых» серверных решений. «Берите наш суперсервер – это лучшая основа для облака». А продавец самых больших в природе серверов уже продает их как лучшее решение для размещения виртуальных машин. Правда, цена на виртуальную машину будет сопоставима с ПК из золота, украшенным кристаллами Swarovski. Странно, а как же с эластичностью, оптимизацией затрат под текущие потребности?

А вокруг снуют продавцы с лотками – «cloud-in-box, включил – и облако работает».

Предлагаются облака как способ внедрения принципов ITSM в организации...

Проспавший начало облачной эры программный гигант встрепенулся и наседает с обещаниями, что в следующей версии все будет «виртуализировано и облачно» – будете довольны. Но в 2013 г.

Крупнейший продавец гипервизоров вырастил из них «программно-определяемый ЦОД» и предлагает огромное количество продуктов по соответствующим ценам.

Гиганты локальных вычислительных сетей, на мой взгляд, своей нерасторопностью тормозят движение к облаку и только обещают в необозримом будущем облегчить конфигурирование ЛВС с помощью программно-определяемых сетей. Судите сами: мы научились быстро создавать сложные виртуальные серверные конфигурации, но, как в 20-м веке, мучаемся с сегментами, VLAN, файрволами, подсетями и т.д.

И все открывают для широкой публики свои публичные облака!

Что делает крупная организация в таком круговороте? Берет паузу. И разворачивает макет облачной инфраструктуры. Надо понять, как это работает и как может быть применено.

Аналитические агентства прогнозируют – рост облачного рынка в 2012 г. составит 19%. При этом констатируют падение продаж серверов. Предполагаю, что рост – за счет малых и средних компаний, которые подключаются к публичным облакам, а падение – за счет крупных, которых запутали продавцы.

Облачная революция касается и производителей информационно-технологических продуктов. Облака – это не еще один двигатель торговли компьютерным железом и ПО, а шаг к превращению информационных технологий в утилитарную (т.е. обыкновенную) услугу для людей. Производители понимают, что эра персональных компьютеров прошла, малый бизнес перестает покупать легкие серверы и переходит в публичные облака. Крупные организации централизуют вычисления в ЦОДах, что снижает продажи серверов уровня отделов и департаментов. На сцену выходят недорогие, сверхэнергоэффективные процессоры. Достигнутой производительности хватает для любых бизнес-задач, и фокус неумолимо перемещается в сторону разработки модульных приложений, полностью независимых от аппаратной части.

Проходит золотой век ИТ-отрасли, когда производители ПО выпускали приложения, требующие все большей производительности ПК, а пользователь годами покупал очередные полуфабрикаты версий, не работающих без сервис-паков и патчей, но требующих модернизации компьютеров.

ИТ-отрасли надо заглянуть за горизонт – может быть, там чья-то заботливая мама, «листая» TV-каналы с помощью iPhone (понятие «компьютер» ей неизвестно), заинтересовалась рекламным роликом и, не отходя от TV, оформляет «тур-ваучер» – билеты, бронь, трансфер, экскурсии и т.д. – все в два клика! – и заодно выбирает новый характер куклы-робота для ребенка, учитывающий будущую поездку на другой континент.

То, что сегодня – смелая фантазия, завтра уже повседневность, сказал, кажется, Жюль Верн. ИКС

ЭКСПЛУТАЦИЯ снова НА ПОВЕСТКЕ ДНЯ!

Окончание. Начало см. «ИКС» № 11'2012, с. 53.

Эксплуатация сетей в условиях снижения маржинальности бизнеса и роста стоимости самого процесса – проблема не для однократного обсуждения, которое состоялось за круглым столом «ИКС». Тем не менее в ходе дискуссии профи заложили кирпичи в фундамент решений, кардинально меняющих модели эксплуатации.

«ИКС»: Какова динамика цены вопроса эксплуатации? И как эксплуатировать сеть в условиях снижения маржинальности операторского бизнеса?


С. ФОМИЧЕВ

Сергей ФОМИЧЕВ, директор по развитию бизнеса, «Мастертел»: Если раньше при высокой маржинальности оператор мог позволить себе делать всё, что хочет: покупать любое, самое дорогостоящее оборудование, строить кабели любой емкости, – то сейчас для того, чтобы быть в рынке, ему приходится искать другие пути. С одной стороны, от этого может страдать эксплуатация. С другой, научиться жить с разумными ограничениями и эффективно использовать более сложные процессы – наверное, единственный вариант. Это как при приеме на работу выбирать между двумя кандидатами: между преданным, но посредственным, или талантливым, но сложно управляемым. Так вот, лучше научиться управлять талантливым человеком, чем работать с тупым.

Дмитрий УРЫВАЕВ, директор по эксплуатации сетей, заместитель технического директора, «ВымпелКом»: Рост расходов на эксплуатацию, безусловно, происходит, потому что сети и трафик передачи данных растут по экспоненте. В общем объеме затрат на эксплуатацию сегодня самая большая доля приходится на арендные платежи. Второе – это плата за частотный спектр. Третье – за электроэнергию. Четвертое – поставщикам основного оборудования за техподдержку. И только на пятом месте идут затраты на персонал, на договора с подрядными организациями и т.д. Работая с первыми четырьмя составляющими, мы можем себе позволить поддерживать рост затрат на эксплуатацию на адекватном уровне. При этом подчеркну: рост численности персонала, прямо пропорциональный росту размера сетей, не может быть обоснован!


Д. УРЫВАЕВ

Поэтому эксплуатационные расходы надо рассматривать с разных сторон. И с точки зрения инвестиций в развитие, которые позволяют в дальнейшем снизить удельные затраты на эксплуатацию. И в аспекте использования специальных мероприятий, которые дают возможность снизить затраты в пересчете на единицу оборудования (например, тендеры на укрупненные объемы или на более продолжительные сроки обслуживания). И с позиций внедрения новых технологических решений, которые в принципе за счет эволюции оборудования позволяют снизить затраты на эксплуатацию. Также оптимизации расходов на эксплуатацию способствуют общие с другими операторами контрагенты на техническое обслуживание и на аварийно-восстановительные работы. Иными словами, network sharing во всех его проявлениях.


А. ВРОНЕЦ

Александр ВРОНЕЦ, гендиректор, «ПроектСвязьТелеком»: Эксплуатация – это часть большого инвестиционного и инновационного процесса. Я бы предложил простую формулу. Если ваши затраты растут не быстрее доходов, то вы нормально развивающаяся компания. Если вы хотите улучшить ваши показатели за счет оптимизации затрат – вы занимаетесь тюнингом, это путь к продаже компании и уходу из этого бизнеса.

Сергей ПАХОМОВ, руководитель отдела телекоммуникаций и связи, «Манго Телеком»: Задача снижения стоимости эксплуатации для нас приоритетна, так как от нее в значительной степени зависит себестоимость услуг. Однако на первом месте у нас – качество сервиса, что накладывает определенные

ограничения на способы удешевления эксплуатации. В целом стоимость эксплуатации сети закладывается на этапе ее проектирования и зависит от выбранных технологий и отработанных решений. В частности, грамотное проектирование региональной сети позволяет заметно снизить эксплуатационные расходы.


С. ПАХОМОВ

Какие у нас здесь проблемы? Во-первых, отсутствие единого провайдера ЦОДов для размещения оборудования узла связи. В разных городах мы вынуждены размещаться в ЦОДах разных операторов – и на разных условиях. Во-вторых, ни у одного из операторов большой тройки мы не имеем одного общего менеджера, через которого могли бы взаимодействовать по всем нашим проектам. Это усложняет взаимодействие, увеличивает количество договоров. В третьих, зачастую приоритетный для нас провайдер не имеет точки присутствия в нужных нам сооружениях. Тогда каналы передачи данных по городу и каналы передачи данных с Москвой мы вынуждены заказывать у разных провайдеров или даже использовать составной канал через двух провайдеров внутри города. В случае аварии на таком канале восстановление сервисов может занимать довольно много времени. Поэтому мы вынуждены организовывать резервные каналы, что, естественно, сказывается на стоимости сети.


Ю. ДОМБРОВСКИЙ

Юрий ДОМБРОВСКИЙ, президент, Ассоциация региональных операторов связи: Пока мобильный бизнес был сумасшедшим по прибыльности, операторы не стремились ограничивать себя в расходах. Сегодня времена изменились. Очевидна тенденция использования аутсорсинга. В аутсорсинг попадает то, что дальше от клиента, что меньше влияет на основной бизнес, на самочувствие клиента. Маркетинг на аутсорсинг не отдашь, а многие технические вопросы – вполне. Здесь надо справляться общими усилиями с новой болезнью беспроводного телекома, обусловленной несовершенством договорной системы аренды и Гражданского кодекса и выражающейся в проблемах размещения базовых станций, башен и т.д.

Расширяется и углубляется тенденция интеграции сетей разных операторов, она распространяется и на эксплуатацию, и на владение сетями, даже на общее оптоволокно. На развивающихся рынках уже работает модель совместного использования активной инфраструктуры, при которой одна компания строит все (антенны, сеть и пр.) и предлагает оператору: «Давайте свои частоты, мы запустим сеть, и она будет работать на вас».


В. ВАЛЬКОВИЧ

Владимир ВАЛЬКОВИЧ, руководитель Департамента технического развития и эксплуатации, Orange Business Services: Мое личное мнение: для эксплуатации, для людей технических, которые создают какое-то решение или предлагают что-то оптимизировать, губительны большие бюджеты. При наличии неограниченных средств у них теряется творческое начало, вряд ли бы в таких условиях конструктор Калашников создал столь простой и надежный автомат. Это важно, потому что, помимо качества, есть соотношения цена/качество и цена/производительность. О цене не нужно забывать.

Кроме того, мы иногда слишком много внимания уделяем неким высокоуровневым вещам (активации приложений, различным системам автоконфигурации, автоматизации) и забываем про базовые принципы эксплуатации: про инженерную инфраструктуру, энергетику, климатику, про технику безопасности и охрану труда, если хотите, – это тоже часть эксплуатационного процесса.

«ИКС»: Какие нормативные правовые вопросы эксплуатации сетей связи волнуют участников рынка и регулятора?

Алексей БЕГИШЕВ, менеджер по развитию партнерской сети в России, Беларуси и Казахстане, Agilent Technologies: Наверное, все понимают, что противопоставление бизнеса и эксплуатации вынужденное: эксплуатация попадает под сокращение расходов в силу экономических причин. Может быть, надо что-то в консерватории подправить?


А. БЕГИШЕВ

Я не предлагаю однозначного решения, я о поступательном движении. Нам нужна помощь регулятора, который создаст некоторый вектор развития, позволяющий нашим компаниям вкладывать в эксплуатацию.

Давайте отстранимся от текущей концепции Минкомсвязи, которое говорит: качество – дело рынка, заказчик голосует ногами, это его выбор, мы не можем его регулировать. Давайте подумаем о создании системы, на базе которой сможем предоставить операторам, обладa-

ющим определенным уровнем качества услуг, преференции при участии в тендерах, при раздаче частот, при определении уровня оплаты и т.п. И тогда сформируется вектор движения компаний по пути не срезания, а вкладывания средств, в том числе и в эксплуатацию.


О. СВИРСКИЙ

Олег СВИРСКИЙ, технический директор, МТС: Рынок меняется очень динамично, и правовая база должна отражать эту динамику. Например, в ряде стран Европы, Америки существуют дотационные программы по «зеленым» технологиям, которые могут сильно влиять на затраты в части энергообеспечения и эксплуатации объектов связи, но благоприятны для экологии страны. Также актуален вопрос публичного сервитута – специальной системы, в соответствии с которой оператор имеет право зайти на любой объект, и держатель этого объекта обязан выдать технические условия. Они могут быть дорогими, они могут быть трудновыполнимыми, но они должны быть реальными. В данный момент у нас обсуждается только коммунальный сервитут, который не всегда соответствует потребностям пользователей в развитии сетей, покрытия.

В части регуляторики актуальна разработка реальных, действующих условий для развертывания сетей по специальным программам, имеющим большое социальное значение. Например, покрытие федеральных трасс, развитие систем оповещения и т.п.

А. ВРОНЕЦ: Мы живем в пору создания негосударственной экспертизы проектных решений. На территории страны действуют уже 150 негосударственных экспертиз. Наш тезис таков: экспертиза должна быть достаточно короткой, понятной и прозрачной. Для этого нужно регулятору серьезно поработать, чтобы выявить вопросы, подлежащие регулированию, и те, которые будут решаться заявительным порядком. Считаю, многие вопросы нужно отдать инженерному сообществу для решения, создав систему жестких нормативов, методик, последующего контроля со стороны надзорных органов.

Алексей РОКОТЯН, директор по работе с госорганами, «ВымпелКом»: Сегодняшняя нормативная база к изменениям в сфере эксплуатации, внедрению моделей аутсорсинга, совместного использования сетей не готова никак. Я так понимаю, что методики работы надзора к этому тоже, мягко говоря, не готовы. Но разговор с новой администрацией связи об этом начался.


А. РОКОТЯН

К сожалению, механизм рабочих групп участников рынка однозначной эффективности не продемонстрировал. Вопрос взаиморасчетов, например, никогда такая рабочая группа не решит. А вот вопросы технические и эксплуатационные, общие требования к эксплуатации – может, и это неплохо работает.

Нормативную базу надо готовить, в том числе путем ее решительного упрощения. У нас во всех документах обозначена достаточно спорная ситуация: есть оператор, значит, у него должна быть своя сеть, которую он сам ввел в эксплуатацию, получил кучу бумажек и т.д.и т.п. Приходит надзор и говорит: а почему у тебя вот здесь не так? Это мешает жить и развиваться даже в рамках существующих моделей, не говоря уже о таких новых, как активный sharing. Неудачная регуляторика и упрямый инспектор – два фактора, которые могут всё то красивое и перспективное, о чем мы сегодня говорили, остановить на корню. Новый регулятор обещает, что быстро поправит нормативную базу. Дай бог.

Подготовила
Наталия КИЙ

О том, что представляет собой эксплуатация 21-го века, «ИКС» продолжит разговор в новом году, в теме номера 4'2013.

Гигабит. 10, 40, 100...

Группа компаний Accton, в которую входит тайваньская компания Edge-Core Networks, разрабатывает и производит комплектующие для компаний – лидеров сетевого рынка. И пусть Edge-Core пока не вошла в пул крупных мировых вендоров – но даже небольшая компания не должна технологически отставать от гигантов, считает CK NG, руководитель технического департамента Edge-Core Networks.

– Какие тренды в развитии сетевого оборудования наблюдались за последние год-два, и как они отражаются в оборудовании компании Edge-Core Networks?

– Основным трендом, бесспорно, является увеличение полосы пропускания сетей абсолютно для всех приложений, так что, думаю, очень скоро заказчики начнут требовать от операторов соединения со скоростью до 1 Гбит/с в расчете на одного пользователя. Именно поэтому компания Edge-Core Networks неуклонно наращивает производительность и функциональные возможности своих гигабитных решений, не забывая при этом о таком их достоинстве, как цена. В последние годы активно шло развитие сетей 3G, 4G, в частности сетей LTE, а это, в свою очередь, заметно повысило интерес к широкополосным оптическим транспортным сетям Metro Ethernet, которые используются для работы базовых станций. В таких сетях очень важна точная синхронизация работы всех базовых станций по времени, поэтому в своем оборудовании, предназначенном для сетей Metro Ethernet, мы используем SyncE (Synchronized Ethernet) и протокол PTPv2 (Precision Time Protocol), что позволяет добиваться точности синхронизации менее 1 мкс.

CK NG: «Скорости будут расти и в кабельном, и в беспроводном мирах»

Еще один явный тренд последних лет – развитие облачных сервисов, для качественной реализации которых также нужны очень высокие скорости передачи данных. Чтобы обеспечить требуемую пропускную способность, необходимы коммутаторы с портами 10 и 40 Гбит/с. Таких же скоростей требуют решения для дата-центров, в которых для управления потоками данных между коммутатором, серверами и СХД обычно используется протокол OpenFlow. Его мы также поддерживаем в своем новом оборудовании, в частности в коммутаторах ECS5610-52S (48 портов с полосой пропускания 10 Гбит/с и четыре порта 40 Гбит/с) и ECS6610-16S (16 портов 40 Гбит/с).

– Практически все ведущие производители сетевого оборудования указывают на активно идущий процесс коммодитизации сетевой инфраструктуры. Как он влияет на работу вендоров? Упрощает или усложняет их жизнь?

– Коммодитизация – закономерное явление, она касается очень многих технологий: в какой-то момент создаваемые на их базе товары становятся продуктами массового спроса и производятся с использованием стандартных компонентов. Несколько лет назад это произошло с компьютерами, теперь настал черед сетевого оборудования. Оно уже достаточно хорошо стандартизовано и рассчитано на эксплуатацию широкими массами пользователей, в том числе и теми, которые не являются квалифицированными специалистами по сетевому оборудованию и компьютерным технологиям.

В таких условиях вендор должен найти способы выделить свой продукт на рынке. Здесь очень велика роль R&D-департамента и разработчиков ПО для нашего оборудования, которые в тесном взаимодействии с конечными заказчиками реализуют новые функции, повышают уровень безопасности и качество сервиса QoS, обеспечиваемое нашим оборудованием, делают его пользовательский интерфейс более удобным. Да, зачастую работа с клиентами, нацеленная на то, чтобы удовлетворить их требования, очень нелегка, но именно такая работа позволяет нам выйти на новых заказчиков и расширить свое присутствие на рынке. С одной стороны, коммодитизация усложняет нам жизнь, но с другой – способствует развитию нашего бизнеса.

– В каком сегменте сетевого оборудования можно, по вашему мнению, в ближайшее время ожидать максимального технологического прогресса?

– Наиболее активно, на наш взгляд, сейчас развивается оборудование для операторов городских сетей, и это вполне объяснимо в свете ярко выраженного тренда на увеличение полосы пропускания до 1 Гбит/с в расчете на абонента. Именно поэтому мы сейчас развиваем нашу операторскую линейку оборудования для агрегации и сетевого доступа в сторону увеличения количества гигабитных и 10-Гбит/с портов. В качестве примера можно привести агрегирующие коммутаторы, предназначенные для операторских и корпоративных Ethernet-сетей: ECS4810-12M (12 портов 1 Гбит/с), ECS4610-24F (24 порта 1 Гбит/с), ECS4660-28F (24 порта 1 Гбит/с и два порта 10 Гбит/с), ECS5510-24S (24 портов 10 Гбит/с).

Процесс построения новых широкополосных операторских сетей и модернизации имеющихся идет сейчас во всем мире. Он находит свое отражение и в стандартизации

Коммутатор ECS5610-52S

соответствующих технологий для городских сетей. Этим занимаются Международный союз электросвязи (МСЭ) и некоммерческая отраслевая ассоциация Metro Ethernet Forum (MEF), в работе которой принимает участие и компания Edge-Core Networks. Например, в соответствии с рекомендациями МСЭ ITU-T G.8032 в наших коммутаторах, предназначенных для операторских сетей, поддерживается технология ERPSv2 (Ethernet Ring Protection Switching), позволяющая в случае обрывов внутренних сетевых соединений находить резервный путь и восстанавливать нормальную работу сети в течение 50 мс. Недавно вышеупомянутый агрегирующий коммутатор ECS4660-28F прошел сертификацию на соответствие стандартам MEF-9 и MEF-14, продемонстрировав тем самым возможности обеспечения заданных параметров полосы пропускания сети, управления трафиком и создания VPN-соединений с требуемым уровнем качества сервиса (QoS). Кроме того, наше оборудование поддерживает разработанные ITU-T стандарты OAM (Operation, Administration and Maintenance) Y.1731, которые являются улучшением IEEE 802.1ag, т. е. в нем реализованы функции, позволяющие быстро обнаруживать участок сети Metro Ethernet, где произошел сбой, и восстанавливать его работу (ранее эти функции были доступны только в локальных Ethernet-сетях).

– Вот уже несколько лет все ведущие производители сетевого оборудования заявляют о поддержке протокола IPv6, но проблем с построением сетей IPv6 еще немало. Реализация каких функций в сетях IPv6 представляется сейчас наиболее актуальной?

– Еще два года назад подавляющее большинство оборудования, «украшенного» логотипом IPv6, имело только базовые функции управления IPv6-сетями, т.е. с его помощью можно было выполнить пингование соединения в сети: определить IPv6-адрес устройства, узнать, работает ли сервер и есть ли с ним связь, – а также организовать соединение по протоколу Telnet. Правда, до поры до времени операторы не очень-то беспокоились о бедном наборе функций в IPv6-сетях, поскольку им хватало запасов адресов IPv4. Но быстрый рост числа подключенных к Интернету устройств, в том числе планшетов, телевизоров, мобильных телефонов, холодильников и прочей бытовой электроники, заставило их задуматься о построении полноценных IPv6-сетей и, соответственно, о формировании конкретных требований к производителям сетевого оборудования, касающихся функциональных возможностей сетей IPv6, которые не уступали бы по своим характеристикам имеющимся сетям IPv4. В частности, во всех современных сетях IPv4 есть поддержка очень важных функций безопасности, и именно над реализацией этих функций в сетях IPv6 мы сейчас работаем. Например, в нашей программной платформе EdgeCOS, которая уже сертифицирована для использования в сетях IPv6, есть функция IPv6 Source Guard (аналог IPv4 Source Guard), которая предотвращает некоторые несанкционированные действия пользователей сети с использованием подменных IP-адресов и перехват злоумышленниками передаваемых по сети данных. Кроме того, мы реализовали поддержку функций контроля групповой передачи данных, таких как MLD snooping, MVRv6 (Multicast VLAN Registration v6), которые позволяют операторам связи использовать среду IPv6.

Коммутатор ECS5510-24S

– В каких направлениях, на ваш взгляд, пойдет развитие сетевых технологий и сетевого оборудования в ближайшие годы?

– Основное развитие будет следовать уже упомянутому тренду расширения полосы пропускания сетей. Поэтому все производители сетевого оборудования, в том числе и компания Edge-Core Networks, работают над увеличением пропускной способности каждого порта своих коммутаторов и маршрутизаторов. Динамика наращивания пропускной способности Ethernet-портов особенно ярко проявляется в коммутаторах, которые используются в дата-центрах: в 2012 г. кривые, описывающие снижение количества портов 1 Гбит/с и увеличение числа установленных портов 10 Гбит/с, пересеклись – и уже в следующем году скорость 10 Гбит/с станет в коммутаторах ЦОДов доминирующей. В этом году также начался заметный рост поставок 40-Гбит/с коммутаторов, а со следующего года в дата-центрах ожидается появление коммутаторов с портами 100 Гбит/с. Во всяком случае компания Edge-Core готовит к выпуску коммутатор с шестью такими портами, который помещается в корпусе высотой 1U, предназначенном для установки в стандартную 19-дюймовую стойку.

Еще одно направление развития – это технология Wi-Fi стандарта IEEE 802.11ac, позволяющая передавать данные со скоростью более 1 Гбит/с. Эта технология, в частности, будет использоваться для создания беспроводных транспортных сетей, связывающих базовые станции сетей 3G и 4G. В портфеле Edge-Core уже есть решения, которые позволят операторам хотя бы частично отказаться от прокладки кабельных транспортных сетей, снизив тем самым свои капитальные затраты и одновременно сэкономив на эксплуатационных расходах.

В общем, скорости будут расти и в кабельном, и в беспроводном мирах, и наша задача – обеспечивать широкую полосу во всех своих решениях, которые должны быть не только полнофункциональными, но и привлекательными по цене.

Как сократить издержки на инфраструктуру

Дилип БХАНДАРКАР

Любые облачные сервисы имеют в своей основе дата-центр, чаще всего не один. И цены на эти сервисы отражают затраты провайдера на инфраструктуру. О том, как сократить издержки, рассказывает главный архитектор Microsoft Global Foundation Services Дилип БХАНДАРКАР.

– Корпорация Microsoft заявляет, что у нее самая низкая в мире стоимость облачных сервисов. Какой вклад вносит в эту стоимость инфраструктура ЦОДов?

– Ценами на сервисы занимаются соответствующие финансовые подразделения компании, а моя основная задача состоит в том, чтобы максимально снизить издержки на инфраструктуру наших ЦОДов – инженерную, серверную, сетевую и т.д. Мы стараемся сократить любые расходы, которые, на наш взгляд, избыточны. Например, в традиционных корпоративных дата-центрах все инженерные системы обычно дублированы, и именно за счет этого их цена фактически удваивается, а мы резервируем оборудование по схеме N+1, т. е. на пять трансформаторов ставим только один резервный.

Кроме того, мы всегда тщательно выбираем место для размещения ЦОДа. Например, в нашем дата-центре в Дублине не было необходимости в создании традиционной системы кондиционирования, так как для охлаждения там достаточно нагнетания внешнего холодного воздуха с помощью вентиляторов. Правда, при строительстве первой очереди мы перестраховались и установили в качестве резерва традиционные кондиционеры, но в течение полутора лет случая их включить так и не представилось, поэтому на следующих этапах строительства они уже не применялись.

– Какова роль ИТ-оборудования в снижении затрат на создание и обслуживание ЦОДа?

– Сэкономить позволяет, например, правильный выбор серверов. В каталогах производителей часто можно видеть, что увеличение производительности сервера на 10% сопровождается повышением его цены на 40–50%. Мы же принимаем решение о покупке сервера, исходя из общей стоимости владения им (TCO) в течение трех лет, его производительности в расчете на $1 затрат и 1 Вт потребляемой энергии. В среднем начальная цена сервера составляет 50% от TCO, а стоимость потребленной им за это время электроэнергии – 20% TCO. Серверы с процессорами, имеющими сниженное энергопотребление, обходятся дороже обычных, но если они позволяют уменьшить TCO, то их использование будет оправданным. Кроме того, можно сэкономить, повысив температуру воздуха, подаваемого на сервер, до 30–35°C. На надежность работы серверов при их эксплуатации в течение 3–4 лет это никак не влияет. Снизить издержки позволяет и наше программное решение System Center 2012, с помощью которого один администратор может управлять тысячами серверов.

– Существует ли типовая конфигурация для серверов, которой вы придерживаетесь?

– В наших ЦОДах используются малые, средние и крупные веб-серверы, файловые серверы и серверы баз данных, рассчитанные на работу с накопителями разной емкости, так что получается девять разных конфигураций, которым отвечают сотни моделей серверов. Спецификации конфигураций пересматриваются каждый год, и здесь главными критериями являются производительность исполняемых на них приложений и TCO. Но замена самих серверов проводится выборочно раз в 3–4 года.

– Есть ли еще резервы для повышения энергоэффективности инфраструктуры дата-центров компании?

– Традиционные возможности мы, конечно, уже исчерпали, и дальнейшее движение в этом направлении требует внедрения очень дорогих решений, что, несомненно, скажется на цене сервисов. Но мы не почиваем на лаврах, а исследуем целый ряд альтернативных решений, направленных на снижение энергопотребления. Правда, все эти работы находятся пока в стадии экспериментов: нужно сначала разобраться, какова будет цена подобных решений и насколько они будут надежны.

– Возможно, имеет смысл строить больше ЦОДов там, где климат позволяет обходиться без принудительного охлаждения?

– Еще три года назад климат в месте будущей дислокации ЦОДа не имел большого значения, а сейчас первое, что мы учитываем при принятии решения о строительстве дата-центра, – это сводка погоды в данном месте за последние 50 лет, и уже потом рассматриваем информацию об источниках электроэнергии и ее стоимости, о доступности полосы пропускания сетей связи и наличии специалистов. Однако иногда у нас нет выбора, и довод близости к клиентам перевешивает все остальные. Например, у нас есть ЦОД в Сингапуре, где климат довольно жаркий, но даже там вместо фреоновых кондиционеров построена система водяного охлаждения.

– Планирует ли Microsoft строительство дата-центра в России?

– Климат здесь для построения энергоэффективной инфраструктуры ЦОДа подходящий, но нужны и экономические обоснования такого проекта, а их пока нет.

Беседовала **Евгения ВОЛЫНКИНА**

Мыльные пузыри, «мегафишки» и другие двигатели ИТ-рынка

Для стимуляции спроса на ИТ-решения, особенно в корпоративном секторе, массово генерируются мифы и легенды, нацеленные на создание иллюзий, «модности» той или иной технологии/псевдотехнологии и повышение ее «капитализации».

Дмитрий АВЕРЬЯНОВ

«Золотой лихорадкой» нашего времени смело можно считать ИТ-лихорадку. Тезис «Реклама – двигатель прогресса» давно стал основным в ИТ-секторе. Вендоры, консультанты и интеграторы дружно раздувают мыльные пузыри и запускают их в направлении армии заказчиков, которая с замиранием предвкушает чудодейственные технологии для скорейшей победы над всеми проблемами автоматизации. Вначале все бросаются рисовать «бизнес-квадратики», потом, забыв о CASE-панацее, прыгают в омут ITSM, далее возносятся на «облака» Cloud Computing... Поднятая в начале 2000-х волна бизнес-моделирования и оптимизации бизнес-процессов на основе «новейших» нотаций должна была за десятилетие наплодить столько референтных моделей, что не осталось бы обделенных областей. Но где эти эталонные модели?

Собрав урожай, поставщики и консультанты, готовят к запуску очередную PR-компанию. Потребители, наигравшись в популярные ИТ-игрушки и в большинстве случаев в них разочаровавшись (но при этом изрядно потратившись), все равно ждут обновления ассортимента. Кроме того, как устоять перед армией «ИТ-светил» и профессиональных коучеров, искусно соблюдающих дистанцию между PR-пузырем и откровенным одурачиванием?

Конечно, почти каждый мыльный ИТ-пузырь основан на здравой идее, но масштабы PR-шелухи, очковтирательства и профанации поражают воображение.

Автор книг по методологии ITIL Роб Ингланд, известный также как it-skeptic, констатирует на примере ITIL*, что вначале создаются удобные заблуждения, а потом сообщество вендоров-консультантов-аналитиков строит на базе этих заблуждений серьезный рынок консалтинга, обучения и программного обеспечения. Причем ИТ-специалисты компаний-заказчиков вынуждены подыгрывать коллегам-менеджерам, так как чтобы удержаться на «ИТ-олимпе», от них требуется защищать соответствующий солидный ИТ-бюджет и наращивать ИТ-подразделения. Поэтому CIO заинтересован разъяснить своим коллегам из бизнес-подразделений организации, что если они решат сохранить просто серверную, а не вложиться в «настоящий ЦОД», то именно они поставят бизнес под угрозу. (Разница между этими вариантами, вполне возможно, сведется лишь к замене штампика на технорабочем проекте или к появлению на двери в серверное помещение позолоченной таблички «Корпоративный центр обработки данных».) А если добавить упоминания об Uptime Institute, TIA 942 и мантры про «непрерывность бизнеса», то при защите бюджета проекта гарантирована немая сцена «бизнес-кролики смотрят на ИТ-удава». Но есть ли где-то ответ на элементарный вопрос: чем, собственно, серверная отличается от ЦОДа?

Что поделать, ИТ-мода беспощадна к ИТ-бюджету. Консультанты и сейлы легко объяснят, как потратить ИТ-бюджет на «экономию», «снижение ИТ-расходов», в крайнем случае на «повышение эффективности ИТ» и получение самых-самых «конкурентных преимуществ». Причем упор будет обязательно сделан на «правильную» ИТ-стратегию, инновационные решения, системный и процессный подходы, сервисные модели, некие best practice и, как ни странно, возврат инвестиций (хотя с последним советчики уже стали осторожнее).

Вокруг ИТ-нововведений, включая такие как интеграционная шина и сервис-ориентированная архитектура (SOA), корпоративное хранилище и business intelligence, unified communications и Web 2.0/Enterprise 2.0 (теперь уже Web X.0 и Enterprise X.0), BPM и ERP/КИС, SaaS, мультисервисность, создается вуаль таинственности. Шелуха общих рассуждений и размытие конкретики затрудняют использование заложенного в них рационального зерна, но помогают насаждению «удобных» заблуждений. Например, ту же «мультисервисность» рынок отыгрывал уже неоднократно: вначале при временном уплотнении (TDM как возможность передачи в таймслотах данных пользователя), потом при статистическом (приход FR/ATM стал расцветом «мультсервисности»), далее как «сети следующего поколения» NGN, включая конвергенцию, softswitch и др.

Мыльные пузыри

Два ИТ-пузыря планетарного масштаба эффектно лопнули почти одновременно и практически у нас на глазах. Вспомните панику в связи с «проблемой 2000 года», нараставшую в нашей стране с середины 90-х: сертификация на Y2K compliance, специальная правительственная комиссия, национальный план действий... По некоторым оценкам, объем мировых инвестиций в этот пузырь, лоп-

* Роб Ингланд. Овладевая ITIL. Скептическое руководство для ответственных лиц. М: «Лайвбук», 2011.

нувший в 23:59:59 31 декабря 1999 г., составил полтриллиона «зеленых». Этот миф считается наиболее результативной реализацией техники продаж FUD*.

Второй пример – пузырь dot-com. Первый «бум дот-комов» стоил не менее $5 трлн и был основан на том, что переоцененные компании «с видом на Интернет» становились публичными, выходя на IPO, и их акции – за счет волшебной добавки .com к названию – росли как на дрожжах (в том числе с применением некоторых махинаций, включая laddering – искусственный скачок цен на акции), а потом рухнули.

Но не следует думать, что теперь пузырей вокруг нас мало. Аналогично психологии фондового рынка, где «мегапузыри» давно затмили очертания реального сектора экономики, создаются спекулятивные рынки «ИТ-фишек», мегапрограмм типа «Электронная Россия». Давно уже назрела необходимость коррекции, однако «медведей» пока можно назвать единицы, включая «it-скептика» Роба Ингланда и «it-провокатора» Карра Николаса (такой ярлык приклеили автору статьи IT Doesn't Matter** за иную точку зрения на традиционное ИТ-мироздание). Сегодня мало кого волнуют реальные отечественные передовые технологии и их становление, ведь можно зарабатывать проще – на мыльных пузырях, принесенных из-за океана. Ни текущая модель отечественной рыночной экономики, ни «заботы» государства на протяжении более 20 лет не отвечают потребностям развития отрасли.

Почему ИТ-пузыри так стабильны? Выше уже назывались любовь к красоте, ИТ-мода, масштаб передовых технологий, желание приобщиться к таинствам best practice. К тому же большую поддержку оказывает ИТ-мифология, также предварительно подготовленная и популяризованная.

Популярные мифы

В ИТ-сфере существует два распространенных заблуждения: о необходимости скрывать (защищать) все знания о вашей ИТ-системе и об уникальности вашего бизнеса (и соответственно вашей ИТ-системы).

Первое базируется на идее о том, что «вокруг одни конкуренты», практически бизнес-враги, и раскрывать им сокровенные знания об ИТ-системе и ИТ-проектах – значит потерять «конкурентное преимущество». Пусть все наступают на те же грабли, что и вы, при создании и эксплуатации своих ИТ-подсистем. Никто не открывает свои технорабочие проекты по «ИТ-фишкам», не делится опытом ведения проектов: техническими заданиями, реальными цифрами возврата инвестиций и др. Параноидальная подозрительность, в большинстве случаев маскирующая дилетантские подходы заказчика и подрядчика или нездоровую заинтересованность, соглашения о неразглашении (non-disclosure agreement, NDA) в части технологий и деталей реализации ИТ-системы создают информационный голод и наносят вред ИТ-сообществу. Речь не идет о бизнес- или персональных данных, не говоря уж о том, что некоторые фрагменты данных по ИТ-блоку могут быть скрыты, включая IP-адреса.

Кроме сокрытия информации, в ИТ отлично действует принцип дезинформации (на «ИТ-фронте» как на войне). Если в ИТ все плохо, то на страницах печати будет наоборот, а провальный проект под «волшебным пером» автора станет восхитительным.

Миф об уникальности вашего бизнеса и соответственно ИТ-системы звучит так: «У вас очень много специфики, типовое решение вам не подходит (тем более что описания его, как правило, и нет), будем все перерабатывать под вас». Уникальный случай – и соответственно уникальный ценник. Аналогичная ситуация сложилась лет десять назад с унификацией ИТ-подсистем в войсках: в рамках НИР Минобороны России главные конструкторы АСУ разных видов войск, поняв, что типовые решения будут изготавливать (продавать) не они, а следовательно, они потеряют массу заказов, красочно расписали, как у них все специфично и ничего от других ОКР им никак не подойдет. Действительно, зачем нам повторное использование чужих наработок, типовые решения? Государству тоже не до стандартизации и унификации, у него и так забот хватает. А в это время различные госкомпании выбрасывают на однотипные и зачастую тривиальные проектные решения совсем не тривиальные миллионные средства. И это при том что подавляющее число ИТ-проектов в стране – поставка и внедрение типового «железа и софта» путем создания из них комплексов и небольшой адаптации. А чтобы выдать такие проекты за нечто высокотехнологичное, достаточно пары известных мировых брендов и новомодной аббревиатуры, кодирующей «ИТ-фишку»: ЦОД, BI, BPM, NGN... И hi-tech пузыри становятся дорогими и секретными, хотя никто не ведет речи об отечественной СУБД или ОС или производстве «железа» (для этого сегодня достаточно наклейки «сделано в России» на корпусе заморского устройства). Не продаются/не сдаются серверные? – назовем их ЦОД, не продаются серверы – назовем их Cloud System, вяло идет продажа аутсорсинга – назовем это облачными технологиями.

В заключение книги «Овладевая ITIL» it-skeptic приводит золотое правило заказчика в ИТ-отрасли – «подвергай все сомнению». Но, конечно, от коррупции это не спасет, и зачастую ИТ-профанации поддаются осознанно. А масштабы коррупции в ИТ у нас российские.

■ ■ ■

Почему ИТ-пузырям пока нет эффективного противодействия? Ведь с уровнем зрелости ИТ-отрасли у нас далеко не все слава богу. И если бы провальные ИТ-проекты были столь же хорошо заметны, как падения спутников, то не только неудачи «Роскосмоса» были бы на первых полосах СМИ. Не говоря уж о том, что в ИТ-отрасли трудятся лучшие умы России, включая выпускников МГУ, Бауманки, Физтеха и других ведущих вузов...

О рецептах оздоровления – в следующей статье.

---

* Fear, Uncertainty, Doubt – прием маркетинга, зародившейся предположительно в IBM и основанный на том, чтобы вызвать страх, неуверенность, сомнения в случае отказа от насаждаемого «правильного» решения.

** Nicholas G. Carr. IT Doesn't Matter. Harvard Business Review, May 2003.

ИКС pro технологии

68 Е. ВОЛЫНКИНА. Проектирование и строительство ЦОДа: уникальность с типизацией

76 М. БАЛКАРОВ. Легенды и мифы прецизионного кондиционирования-2

78 А. ПАВЛОВ, Д. КУСАКИН, Д. БАСИСТЫЙ. Типовые отказы ЦОДов и их профилактика

82 А. АННЕНКОВ. Автономное и универсальное новое устройство пожаротушения российского производства

84 С. КУЧУМАРОВ. Сети для систем безопасности: оптимальные топологии

88 А. СЕМЕНОВ. Системы интерактивного управления в малых и средних СКС

91 Новые продукты

Проектирование и строительство ЦОДа

уникальность с типизацией

Евгения ВОЛЫНКИНА

Проект каждого ЦОДа считается уникальным, но все эти «частные случаи» можно тем не менее свести к нескольким крупным типам. Рецепты выбора заготовки дата-центра для ее последующей «заточки» давали участники 7-й международной конференции «ЦОД-2012», организованной журналом «ИКС».

Процесс проектирования дата-центров за время существования этой отрасли оброс гласными и негласными правилами, но на самом начальном этапе он в принципе не отличается от процесса проектирования промышленных зданий и бизнес-центров. Заказчик должен определиться с тем, каких специалистов и какие организации он хочет и должен привлечь для проектирования и строительства данного конкретного ЦОДа, чтобы на выходе получить дата-центр, способный решать поставленные перед ним бизнес-задачи.

Кого позовем?

На рынке, как отметил генеральный директор ADM Partnership Максим Иванов, уже сложилось несколько типичных моделей организации проектирования и строительства ЦОДа. В этом увлекательном занятии участвуют заказчик, консультант, проектная компания и системный интегратор. Консультанты, о важной роли которых в создании дата-центров давно говорили эксперты этого рынка, наконец-то перестали восприниматься заказчиками как лишнее звено. Теперь их все более активно привлекают на этапах формирования технических требований к проекту, составления технического задания и заданий на проектирование. Не сомневаются теперь заказчики и в необходимости привлечения специализированной проектной компании.

Но вот проект дата-центра выполнен и принят заказчиком. Что дальше? В простых проектах, где заказчик уверен в собственных силах, вполне правомерен традиционный подход: в качестве подрядчика нанимается системный интегратор, который реализует проект, решает все связанные с этим задачи и сдает ЦОД под ключ. Но и в таком простом случае заказчику стоит оснащать свой дата-центр оборудованием, поставщики которого оказывают техническую поддержку при монтаже. При этой конфигурации все риски реализации проекта берет на себя заказчик, и можно только пожелать ему удачи.

В достаточно серьезных проектах заказчик обычно привлекает генерального подрядчика, который берет на себя все функции управления процессом (в том числе выбор субподрядчиков для выполнения тех или иных работ) и несет ответственность перед заказчиком за соблюдение сроков и сметы проекта. Более того, правильный генподрядчик может даже взять на себя финансирование части работ субподрядчиков, если заказчик по каким-то причинам не хочет раздавать крупных авансов. В этом случае заказчик передает ответственность за проект генподрядчику, что, правда, чревато определенным риском. Поэтому некоторые заказчики, особенно крупные, в последнее время стали брать на себя подбор субподрядчиков и управление строительством. По мнению М. Иванова, такая схема вполне имеет право на жизнь, но только при наличии у компании собственной сильной службы технического заказчика и производственно-технического отдела. Кроме того, заказчик должен быть готов к работе с большим количеством субподрядчиков (а их на проекте ЦОДа мощностью от 1 до 3 МВт может быть 10–15) и к финансовым рискам. Так что при реализации относительно несложных проектов заказчики все чаще обращаются к управляющим компаниям, которые выбирают подрядчиков и несут ответственность за их работу перед заказчиком, а последний сохраняет за собой функции управления финансовыми потоками. Ну а для масштабных и сложных проектов, особенно если строящийся объект будет состоять из нескольких корпусов и/или предпола-

гается поэтапный ввод мощностей в эксплуатацию, нужны и управляющая компания, и генподрядчик, причем финансово независимые друг от друга. Генподрядчик должен отвечать за качество работ и соблюдение сроков, а управляющая компания – за финансовую эффективность строительства. Но в любом случае выбор схемы реализации проекта ЦОДа остается за заказчиком.

Опыт варягов

В России уже не первый год работают международные управляющие компании и компании, выступающие в качестве генеральных подрядчиков. Именно их часто привлекают для своих проектов крупные российские заказчики, справедливо полагающие, что для создания столь серьезного объекта, как дата-центр, нужен достаточно большой опыт строительства аналогичных сооружений. Подобные компании обычно не ограничивают свои услуги функциями генерального подрядчика, они способны обеспечить полный жизненный цикл проекта – от проектирования инженерной и ИТ-инфраструктуры до запуска оборудования в эксплуатацию. Одной из таких компаний, присутствующих на российском рынке, является M+W Germany. Как отметил руководитель ее отдела развития бизнеса в области ИТ и телекоммуникаций Мальте Матиас, благодаря правильной организации работ можно сократить сроки строительства ЦОДа с 15 до 12 месяцев и даже до восьми. Кроме того, при разработке концепции действительно продвинутого ЦОДа нужно учитывать не только требования к надежности и безопасности или технологии, которые планируется в нем использовать, но и варианты поэтапного модульного строительства и развертывания всей инфраструктуры, корпоративные стандарты, географическое расположение дата-центра, климат в этой местности и даже политическую ситуацию в стране.

Принцип модульности строительства дата-центра, похоже, стал уже всеобщим. Он позволяет сократить первоначальные расходы и свести к минимуму простаивающие площади и оборудование. Хотя, по мнению М. Матиаса, главное в концепции построения ЦОДа – даже не модульность, а возможность масштабирования. Это позволяет строить гибридные решения, объединяющие достоинства классических и модульных подходов, т. е. можно к крупному дата-центру добавлять по мере необходимости новые модули, совместимые с ранее построенными системами. Например, в арсенале M+W есть и так называемый дата-контейнер площадью от 20 до 100 кв. м, и «дата-куб» размером от 100 до 1000 кв. м, и дата-модуль площадью более 1000 кв. м. Кроме финансовой эффективности не забыта и энергоэффективность. В одном из проектов в центральной Европе M+W удалось добиться PUE, равного 1,12, что потребовало использования технологии адиабатического воздушного охлаждения, отказа от водяных теплообменников и механических систем охлаждения.

PUE vs TCO

Подумать о том, какой ценой получается низкий PUE, предлагает директор проекта ЕРЦОД «Ростелекома» Александр Мартынюк: «При разработке проекта дата-центра надо найти некий баланс PUE и общей стоимости владения TCO, без которого проект может получиться либо технически совершенным, но слишком дорогим, либо очень дешевым, но ненадежным, и значит, никому не нужным». О проектах с низким PUE говорят очень много, однако среднемировой уровень PUE в реально существующих дата-центрах сейчас составляет 1,9, а в новых проектах – 1,5. Какую экономию на счетах за электричество может дать снижение PUE? Понятно, что при небольшом общем энергопотреблении ИТ-нагрузки и уменьшение затрат на электроэнергию окажется небольшим. Если же потребляемая мощность нагрузки составляет весьма внушительные 5 МВт (таких проектов в России пока очень немного), то, по подсчетам А. Мартынюка, при нынешних ценах на электричество разница в его стоимости для дата-центров с PUE, равными 2,0 и 1,5, составит 63 млн руб. в год, а за 4,5 года набежит сумма, позволяющая построить ЦОД мощностью 1 МВт.

Однако надо помнить, что снижение PUE далеко не всегда дает прямой экономический эффект, поскольку внедрение энергоэффективных решений может оказаться довольно дорогим удовольствием. Например, более эффективные системы охлаждения обычно занимают больше места, чем традиционные, что в условиях вписывания ЦОДа в существующее здание, да если оно еще находится в центре Москвы, будет означать оплату дополнительных квадратных метров, которую не покроет никакая энергоэффективность. В такой ситуации владелец дата-центра, скорее всего, предпочтет традиционные системы охлаждения, а всю свободную площадь займет серверными стойками. Если же ставится задача построения ЦОДа с рекордно низким PUE (порядка 1,1–1,17), то на это должен быть изначально нацелен весь проект, т. е. дата-центр придется строить с нуля по специальному про-

екту с выбором площадки под конкретное техническое решение, что подходит не каждому заказчику.

Пока для подавляющего большинства российских заказчиков дата-центров актуальны не инновационность и энергоэффективность, а максимально достижимое качество реализации проекта в рамках выделенного бюджета. Строительство же дата-центров со сверхнизким PUE, даже при наличии благоприятных, как в нашей стране, климатических условий, имеет чисто маркетинговый смысл.

Модульная экономия

Принцип модульности при построении дата-центров появился в свое время как способ сокращения капитальных и операционных затрат, а также непроизводительного простоя площадей и оборудования. Этот же принцип взяли на вооружение производители оборудования для инженерной инфраструктуры. Как рассказал технический специалист Emerson Network Power Андрей Вотановский, он реализован в семействе ИБП Liebert, которые позволяют наращивать мощность системы бесперебойного питания с достаточно небольшим шагом (минимум 10 кВА). Таким «квантом», в частности, является ИБП

Liebert NXc (модели мощностью 10 и 20 кВА), поддерживающий работу до четырех систем в параллельном режиме. Он отличается длительным временем работы на встроенных батареях при отключении питания (до 64 мин), что по достоинству должны оценить заказчики, которые по каким-то причинам не хотят устанавливать ДГУ или дополнительные батарейные шкафы. Средне-низкий мощностной диапазон этого семейства ИБП представлен моделью Liebert NX (от 30 до 60 кВА), которая также поддерживает соединение в параллель до четырех систем. Но ее «конек» – почти плоская нагрузочная характеристика, что означает возможность работы с высоким КПД при разных нагрузках.

ИБП Liebert APM (диапазон мощностей от 30 до 150 кВА) – это модульная система с возможностью «горячей замены» силовых и батарейных модулей, которая отличается своим пассивным шасси: в нем нет активных элементов, все можно снять и заменить. Более того, в этом ИБП можно применять внешние батареи сторонних производителей. На использование в современных системах электропитания в новых мощных ЦОДах нацелен ИБП Liebert 80NET (диапазон мощностей от 60 до 500 кВА), который поддерживает подключение в параллельной конфигурации до восьми таких систем. Наконец, самый мощный ИБП в арсенале Emerson – модульный Liebert Trinergy (мощности от 200 до 1200 кВА), что при возможности устанавливать в параллель до восьми систем позволяет строить решения мощностью 9600 кВА. Кроме мощности эта модель отличается интеллектуальным режимом отключения избыточных силовых модулей в зависимости от нагрузки.

Сделано на заводе

Еще одна тенденция, проявившаяся на рынке в последние два-три года, – ориентация вендоров на выпуск готовых комплектных модулей электропитания и кондиционирования. Однако, как предупреждает начальник отдела технического пресейла компании R-Style Александр Шапиро, при общем высоком техническом уровне подобных решений далеко не все заявленные их производителями преимущества реально нужны заказчикам, а кроме того, подобная типизация и модульность не всегда приводят к экономии.

Комплектные модульные системы для инженерной инфраструктуры дата-центров выпускают и крупные мировые вендоры, и компании второго эшелона. В каталогах уже фигурируют готовые модульные решения для кондиционирования с системами воздушного фрикулинга и традиционными промышленными системами охлаждения на случай жаркой погоды, а также модули с полным набором инженерных систем, имеющие общий сверхнизкий PUE (от 1,05 до 1,15), которые помещаются в 20- или 40-футовые контейнеры. Причем это не просто попытка впихнуть стандартное решение в стандартный же контейнер, это действительно энергоэффективные решения достаточно высокого уровня, потребовавшие серьезных научных и опытно-конструкторских разработок. Они прибывают на площадку заказчика фактически в готовом виде, собранные и протестированные на заводе с высоким качеством производства, и имеют технические характеристики, которые не сможет гарантировать даже опытный системный интегратор, собирающий подобное решение на заказ. Эти решения не требуют длительного монтажа и пусконаладочных работ, и их можно дополнять другими модулями по мере роста ЦОДа. Однако цена таких решений довольно высока и, несмотря на все заявления производителей, не позволяет снизить общую стоимость владения дата-центром.

В качестве достоинства подобных систем производители указывают возможность их перебазирования, но, как показывает жизнь, такой потребности у заказчика практически никогда не возникает. Кро-

ме того, подобное решение требует создания дополнительных интерфейсов для систем охранно-пожарной сигнализации, контроля доступа, мониторинга и видеонаблюдения. Оно также увеличивает количество зон контроля и общий периметр ЦОДа, который надо охранять. К числу недостатков следует еще добавить неизбежную привязку к одному вендору. Так что, по мнению А. Шапиро, при всей технической прогрессивности комплектных модулей использовать их следует, лишь если они соответствуют концепции ЦОДа заказчика и обеспечивают значительное улучшение количественных характеристик дата-центра (низкий PUE), если заказчик не только готов за это платить, но и уверен в долговременной поддержке производителя и сможет действительно с выгодой использовать сэкономленное на монтаже время.

Традиции в большинстве

Большинство заказчиков пока предпочитают традиционный подход к созданию дата-центра, несмотря на то что этот процесс обычно ограничен по времени. Как считает Павел Савранский, заместитель директора по развитию компании «Электронная Москва», ЦОД следует проектировать под конкретную задачу, чтобы оптимизировать и капитальные, и операционные расходы. В данном случае предстояло построить дата-центр, который должен обеспечить бесперебойную работу собственных информационных систем «Электронной Москвы», использующих облачные технологии, и информационных систем клиентов, в числе которых есть и городские ИС.

Список основных технических требований к ЦОДу был довольно серьезный: отдельно стоящее здание, допускающее реконструкцию, возможность организации широкополосных каналов связи, высокий уровень отказоустойчивости инженерных систем, большая плотность размещения серверного оборудования (что означает наличие соответствующих электрических мощностей и построение серьезной системы охлаждения), управляемость инженерных систем, поэтапное строительство и экономическая эффективность дата-центра. При выборе тех или иных технических решений проектная команда руководствовалась их качеством (поскольку от него зависит отказоустойчивость ЦОДа), стоимостью (учитывая ограниченность бюджета), экономической эффективностью при эксплуатации, возможностью масштабирования, скоростью и простотой монтажа, поскольку сроки реализации проекта были очень сжатыми. Стоит отметить, что в финансировании проекта принимает участие и владелец здания ЦОДа, которое «Электронная Москва» арендует. В итоге слаженной работы инженерной команды проектирование дата-центра было выполнено в фактически рекордные сроки – три месяца. Из-за тех же ограничений по времени на объекте одновременно находятся четыре-пять подрядчиков, что требует четкого планирования их работы, а это непросто, так что работы идут в круглосуточном режиме. Дата-центр еще не запущен в эксплуатацию, но, как сказал П. Савранский, все ключевые участники буквально живут этим проектом (и даже видят о нем сны), так что он просто обязан быть успешным.

Контейнеры с перспективами

И тем не менее модульные контейнерные решения для ЦОДов упорно пробиваются на рынок, в том числе на российский, где есть уже свои отечественные производители подобных систем. В числе первых на него вышла компания «Ситроникс», предложившая

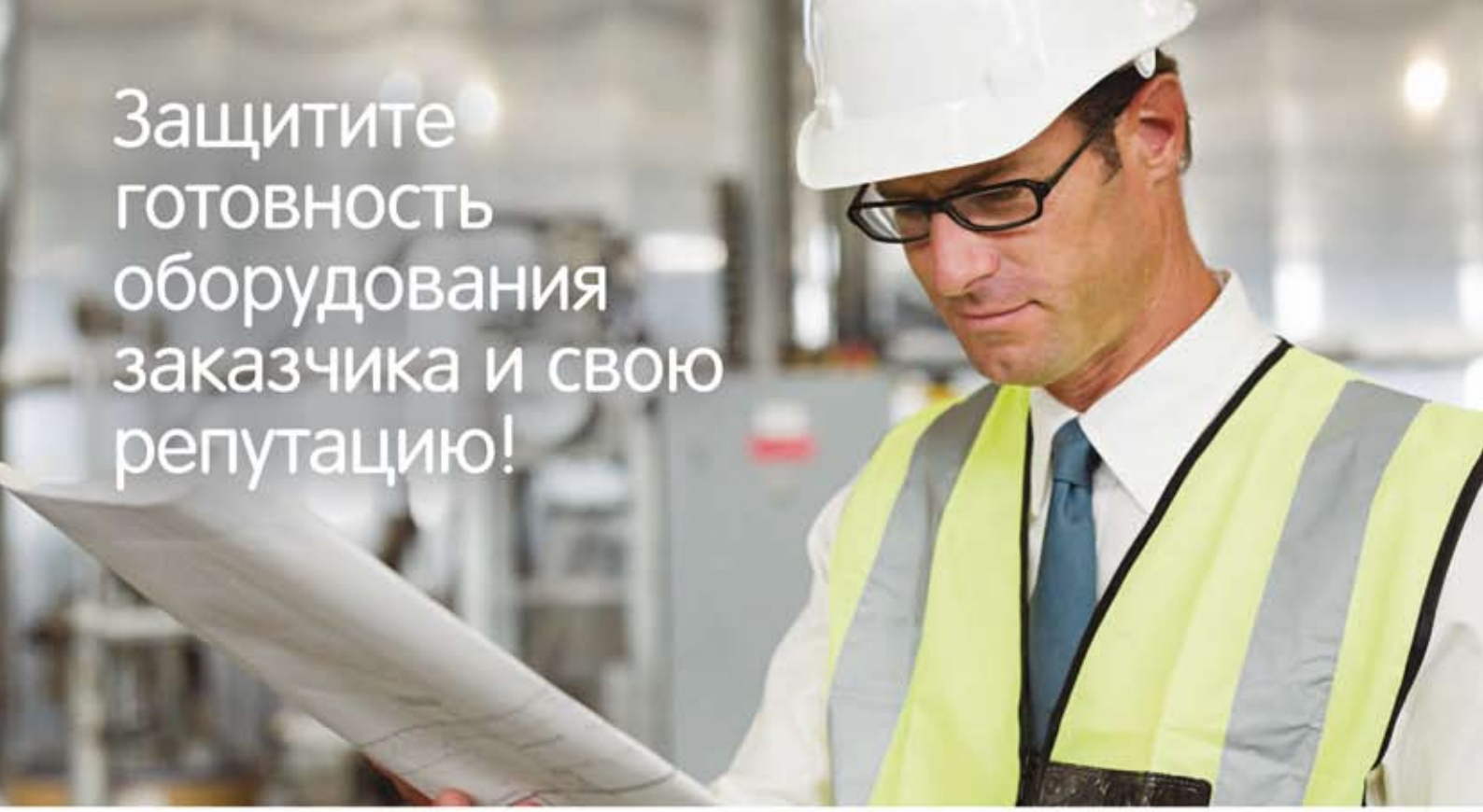
свой мобильный ЦОД еще в 2008 г. Как отметил главный архитектор бизнес-решений в области ЦОД «Ситроникса» Владимир Алеев, сейчас активно развиваются и одноконтейнерные («все в одном»), и многоконтейнерные конфигурации (со специализированными контейнерами для ИТ-оборудования и инженерных систем) модульных дата-центров. Одноконтейнерные представляют собой фактически автономный мобильный ЦОД, который для запуска в эксплуатацию нужно только подключить к источнику электроэнергии и каналам связи. Существуют даже мобильные дата-центры, предусматривающие размещение ИТ-оборудования до доставки ЦОДа на место. Но у них есть ограничения по вычислительной мощности: в 20-футовый контейнер пока не удалось вместить больше семи стоек, а в 40-футовый – больше 12. Тем не менее это направление развития ЦОДов представляется очень перспективным, особенно в свете автоматизации управления дата-центрами, которая позволяет создавать по-настоящему автономные ЦОДы и устанавливать их на удаленных площадках, где нет дефицита электричества, но есть проблемы с обслуживанием.

Сейчас «Ситроникс» предлагает несколько модификаций своих контейнерных ЦОДов «Датериум» для разных вариантов использования. Мобильный ЦОД «Датериум-2» размещается в 20-футовом контейнере, он допускает установку семи полноразмерных стоек с ИТ-оборудованием общей подводимой мощностью 40 кВт. В этом дата-центре типа «все в одном» внутри установлены системы бесперебойного электроснабжения (с резервированием по схеме N+1), прецизионного кондиционирования, газового пожаротушения, удаленного мониторинга и управления. МЦОД «Датериум-3-80» в 40-футовом контейнере позиционируется как дата-центр для мощных виртуализованных систем. Он рассчитан на установку ИТ-оборудования с энергопотреблением до 80 кВт. Правда, в нем из-за более высокого уровня резервирования ИБП (N+N) можно установить только шесть серверных стоек. Оба контейнера рассчитаны на российский климат, поэтому в них серверные помещения отделяются от входа тамбур-шлюзом. Но для сугубо суровых северных условий есть особая модификация «Датериум-3-Север», работающая в диапазоне температур от −55 до +45°С. Правда, не всегда контейнерные ЦОДы действительно стоят на улице; бывает, что заказчик, желая избежать дорогой общестроительной подготовки помещения для традиционного дата-центра, просто устанавливает контейнер с ЦОДом внутри бывшего цеха или какого-то быстровозводимого здания.

Почти одновременно с «Ситрониксом» свое первое изделие в категории мобильных дата-центров на базе 40-футового контейнера представил еще один российский производитель – компания TeleCore. Как сообщил ее коммерческий директор Виталий Кустуктуров, производство создавалось на базе оборонного предприятия, которое более 40 лет специализировалось на выпуске мобильных пунктов охраны для систем залпового огня, так что принципы автономности инженерных систем известны там давно. Поэтому решение от TeleCore является полностью автономным. Оно обеспечивает отвод до 10 кВт тепла со стойки, системы бесперебойного питания и охлаждения в нем имеют резервирование по схеме N+1, возможны использование фрикулинга и работа с ДГУ (дизель-генератор может находиться как внутри контейнера, так и за его пределами).

Первый экземпляр мобильного ЦОДа TeleCore был установлен в 2008 г. в С.-Петербурге на площадке одной из ритейлерских компаний, а всего на сегодняшний день выпущено 10 таких дата-центров, контейнеры для них изготавливались по индивидуальным проектам под конкретную конфигурацию и компоновку ЦОДа каждого заказчика. За это время было разработано три типовых решения разных размеров и вариантов компоновки, на базе которых и выполнены все проекты. В некоторых из них была использована система охлаждения на фреоновых кондиционерах производства Fujitsu, которые не требуют сертифицированного запуска и обслуживания, что снижает начальную цену и общую стоимость владения решением. По словам В. Кустуктурова, производственный цикл с изготовлением, установкой мобильного ЦОДа и пусконаладочными работами занимает три-четыре месяца, все инженерные системы тестируются и устанавливаются на заводе, так что на площадку приезжает фактически готовое изделие, которое вводится в эксплуатацию за несколько дней, а цена по сравнению с зарубежными аналогами со сходными мощностными характеристиками получается ниже. Но производитель признает и наличие недостатков у этих контейнерных ЦОДов, а именно относительно высокую удельную стоимость стойкоместа и невысокую вычислительную мощность из-за ограничений на отвод тепла из контейнера.

В принципе недостатки модульных контейнерных дата-центров известны давно, но есть много



Защитите готовность оборудования заказчика и свою репутацию!

Рекомендуйте решения Schneider Electric, обеспечивающие высочайший уровень надежности!

Выбор продуктов и решений для бизнеса — дело непростое. Необходимо, чтобы они не только работали на нужды заказчика, но и позволяли точно оценивать бизнес, его прибыльность, величины денежных потоков. Еще одно важное требование — возможность поставки в соответствии с графиком проекта.

Вперед с проверенной практикой надежностью!

Schneider Electric предлагает полный ассортимент решений защиты электропитания критичных приложений в промышленных и ИТ-средах. Наши проверенные практикой системы, в которых применяются компоненты высочайшего качества, позволяют добиваться нужного уровня производительности, безопасности и надежности для реализации проектов в соответствии с нормативными требованиями, эффективно и с опережением графика. И главное, мы предлагаем самые сжатые сроки исполнения заказов, доступные по цене услуги и запасные части, техническую поддержку по развертыванию, монтажу и эксплуатации, а также обслуживание в устраивающем заказчика режиме.

Стать доверенным консультантом: с нами — реально!

Накопленный объем знаний по отраслевой тематике, штат опытных специалистов и исследователей с именем в своей области делают компанию концептуальным лидером и новатором. Мы сыграли ведущую роль в формировании современных представлений о защищенном электропитании и управлении энергией. Наша репутация наряду с системой обучения, простыми в использовании средствами проектирования и интернет-калькуляторами, беспрерывным обслуживанием и поддержкой поможет вам стать доверенным партнером и консультантом по энергетическим вопросам. Компания Schneider Electric готова обеспечивать своих партнеров всем необходимым для развития бизнеса, поддержания лояльности заказчиков и выделения из рядов конкурентов.

Решения защищенного электропитания на выбор

- Продукты. Полный каталог решений электропитания Schneider Electric, включающий продукцию наших ведущих брендов, таких как APC by Schneider Electric и GUTOR, предлагает уникальный выбор одно- и трехфазных ИБП, выпрямителей, инверторов, активных фильтров и статических переключателей номиналом от 1 кВА до нескольких МВА.
- Решения. Верный выбор комбинации продуктов и услуг Schneider Electric позволяет получить все преимущества полного решения — системы, ПО и услуги — из единого источника.

Загружайте информационную статью, участвуйте в конкурсе и получайте призы от Scheider Electric!

Зайдите на сайт www.SEreply.com и введите код 79096v

Schneider Electric

ситуаций, когда заказчики готовы с ними мириться и считают именно такие решения выгодными. Поэтому перспективы развития у мирового рынка модульных ЦОДов довольно хорошие. По данным компании The 451 Group, которые привел В. Алеев, объем этого рынка в 2011 г. составил $460 млн, а к 2015 г. должен увеличиться до $2,5 млрд (рост более чем впятеро); кроме того, опрос, проведенный в 2012 г., показал, что 9% компаний уже используют такие ЦОДы и 8% планируют это сделать в ближайшее время. К примеру, именно модульный ЦОД решила заказать компания «Башнефть» в ситуации, когда датацентр нужен был срочно, а строительство «нормального» корпоративного ЦОДа, даже при возможности начать его немедленно, в эти сроки никак не укладывалось. Как рассказал начальник отдела развития инженерной инфраструктуры и связи АНК «Башнефть» Виталий Шункин, ни одна из технологических площадок, имевшихся у шести предприятий, которые входят в состав этой компании, не соответствовала требованиям обеспечения бесперебойной и катастрофоустойчивой работы ИТ-оборудования, предназначенного для централизации всех имеющихся информационных систем. Поэтому решено было строить новый корпоративный дата-центр. Площадку с возможностью подключения достаточных электрических мощностей и оптоволоконных линий связи искали пять месяцев, к этому моменту был подготовлен рабочий проект ЦОДа, но бизнес-критичные информационные системы не могли ждать окончания строительства, поэтому проект был разделен на временное и постоянное решение. В качестве временного был выбран мобильный ЦОД от «Ситроникса», который соответствовал климатическим условиям Уфы (от –42 до +42°C), так что через четыре месяца корпоративная ИТ-инфраструктура была запущена в эксплуатацию. По словам В. Шункина, мобильный ЦОД успешно выдержал башкирскую зиму, а технический персонал навещал его только для техобслуживания. А в это время шло строительство постоянного ЦОДа с общим энергопотреблением 930 кВт,

половина из которого приходится на ИТ-нагрузку (т. е. коэффициент PUE составил 2,0). Этот датацентр находится внутри модульного помещения физической защиты Lampertz, которое, в свою очередь, располагается в легковозводимом ангаре общей площадью около 670 кв. м.

Проект с аутсорсингом

Совсем другой подход к консолидации ИТ-инфраструктуры у Департамента информационных технологий г. Москвы. Как отметил начальник управления технической политики ДИТ Москвы Алексей Аляев, в плане организации деятельности столичное правительство похоже на очень крупную компанию с территориально распределенными подразделениями, с той только разницей, что цель обеспечения прибыльности не стоит, но экономить надо. Именно для экономии городского бюджета и был начат проект централизации ведомственных и районных ИТ-систем.

Для получения действительно гибкой ИТ-инфраструктуры, которую можно было бы быстро расширять для выполнения различных проектов и точно так же сворачивать по их завершении, решено было использовать мощности коммерческих датацентров. Работа с ними строится по нескольким моделям. Во-первых, это традиционная аренда стоек в ЦОДе для размещения собственного ИТ-оборудования, во-вторых, покупка вычислительных ресурсов по требованию (облачная модель IaaS), в-третьих, использование модели SaaS (по такой схеме, например, работает система электронного документооборота, единая почтовая система правительства Москвы и некоторые другие приложения). Таким образом, проблемы проектирования и строительства дата-центра заказчик перекладывает на плечи провайдера, который выбирается по конкурсу и качество работы которого находится под контролем. И это тоже можно считать одним из типичных вариантов создания ЦОДа.

Словом, каждый выбирает по себе... ИКС

Российский рынок коммерческих дата-центров 2012–2016

Аналитический отчет

iKS CONSULTING

- Российский рынок дата-центров – емкость, динамика, тенденции
- Структура рынка по игрокам, услугам, регионам
- Региональное развитие рынка дата-центров
- Перспективы облачных услуг
- Новые проекты на российском рынке
- Бизнес-модели российских дата-центров
- Факторы роста рынка
- Перспективы и прогнозы
- Профили основных игроков

Роль центров обработки данных в развитии ИТ и телекоммуникационной отрасли России стремительно возрастает: расширяется ИТ-инфраструктура предприятий, растут потребности крупных интернет-проектов, многократно увеличивается объем трафика, передаваемого по сетям операторов.

Какую динамику демонстрирует российский рынок? Какие площадки были запущены в 2011–2012 годах, какие будут запущены в 2013–2014 годах? В чем специфика российского рынка? Почему растет популярность услуг коммерческих дата-центров среди крупных корпоративных клиентов? Что явилось отличительными тенденциями этого года и чего ждать в ближайшем будущем?

Ответы на эти и многие другие вопросы предлагает отчет iKS-Consulting «Российский рынок коммерческих дата-центров 2012–2016»

Параметры отчета:

- Количество страниц: **115**
- Цена: **95 тыс. руб.** без НДС
- Выход: **декабрь 2012 года**

Подробная информация:
+7 (495) 505-10-50
E-mail: ef@iks-consulting.ru
iKS-Consulting

www.iks-consulting.ru

Легенды и мифы прецизионного кондиционирования – 2

Михаил БАЛКАРОВ,
технический эксперт,
Emerson Network Power,
ATD, CDCDP

Типичных ошибок в проектировании прецизионного кондиционирования для технологических целей, в частности для охлаждения компьютерного оборудования, больше, чем мы насчитали в предыдущей статье (см. «ИКС» № 9'2012, с. 77). В этот раз предмет нашего рассмотрения – заблуждения относительно систем охлаждения в целом.

Миф 1. Свободное охлаждение невозможно в теплом климате

Практика показывает, что классические системы с чиллерным фрикулингом вполне эффективны даже в Греции и Испании. Наиболее важный параметр для использования свободного охлаждения – стоимость электроэнергии, а не климат. Как это ни парадоксально, гораздо сложнее обеспечить фрикулинг в сильные морозы.

Кстати, набирающее популярность адиабатическое охлаждение, основанное на испарении воды, вообще практически не зависит от температуры наружного воздуха. Для него важны только влажность и наличие дешевой воды.

Миф 2. Концентрация гликоля подбирается для предотвращения замерзания

Этим правилом можно руководствоваться в теплом климате. Но в сильные холода, такие, как на большей части территории нашей страны, мы сразу попадаем в среду действия мифа. Проблема в том, что при снижении температуры у растворов гликоля значительно возрастает вязкость. Раствор не замерзает, но его становится практически невозможно прокачивать.

Единственное реально работающее решение – обеспечивать относительно высокую температуру теплоносителя. Поэтому все теплообменники должны работать одновременно и должна присутствовать тепловая нагрузка.

В нештатной ситуации система может замерзнуть, но без повреждения труб и теплообменников. В некоторых системах имеет смысл специально замораживать часть теплообменников для уменьшения интенсивности отдачи тепла в сильные морозы.

В справочнике ASHRAE* даются четкие рекомендации: «В периоды простоя в холодную погоду для предотвращения повреждения оборудования (например, для подготовки к зиме теплообменника в системе HVAC) достаточно 30%-ного (по объему) раствора этиленгликоля или 35%-ного (по объему же) раствора пропиленгликоля».

Миф 3. Система охлаждения подбирается только по производительности

На самом деле в первую очередь должна проверяться способность системы подать нужное количество воздуха.

Для охлаждения серверного оборудования воздуха нужно много – до 1 м^3/с на 12 кВт тепловыделения, если допустимый перепад температур задан в 10°. Перепад температур на входе и выходе сервера – величина паспортная. В современных моделях блейд-серверов он может достигать 30°. Это, с одной стороны, хорошо, поскольку воздуха требуется подавать в три раза меньше, с другой стороны, температура на выходе становится на эти же 30° выше, что может приводить к другим проблемам.

Миф 4. Производительность оборудования можно подобрать по каталогам

Изготовители кондиционеров зачастую не указывают явную производительность, поэтому нельзя просто ориентироваться на номинал, не глядя в документацию. Кроме того, производительность зависит от состояния воздуха – чем теплей и суше воздух на входе в кондиционер, тем коэффициент явной производительности ближе к 1, тем большая часть холодильной мощности расходуется с пользой, а не на ненужное осушение воздуха. Тем более что убыль воды из воздуха приходится восполнять, затрачивая на это дополнительное количество энергии и ресурс увлажнителей.

У моделей нижнего ценового диапазона производительность может заметно отличаться от заявленной, причем обычно в меньшую сторону. Даже сертификация Eurovent для продуктов высшего класса допускает отклонения ±7%.

Кроме того, номинал указывается для определенной температуры на улице, следовательно, с ростом температуры производительность падает, даже при увеличенных внешних блоках.

Оптимальный способ подбора оборудования – это специализированная программа от производителя.

Миф 5. Теплый воздух поднимается к верху стойки

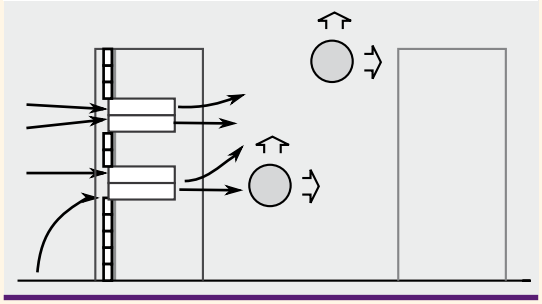
При нагреве воздуха его плотность уменьшается. В теории это приводит к тому, что более теплый воздух

*ASHRAE Handbook Fundamentals. American Society of Heating, Refrigerating и Air-Conditioning Engineers. 2009.

поднимается вверх (рис. 1). Оценим этот процесс количественно.

Пусть воздух с 18°C и 60% RH нагревается до 30°C и 25% RH. Его плотность при этом уменьшится с 1,2 кг до 1,15 кг на 1 м³. На этот кубометр из-за разности в весе (0,05 кг) действует сила Архимеда, равная 0,5 Н, что приводит к его подъему с ускорением 0,43 м/с² ($a = F/m$). То есть на высоту стойки (2 м) воздух с пола поднимется примерно за 3 с ($t = \sqrt{2s/a}$).

Рис. 1. Теплый воздух поднимается вверх



Но рассчитывать на естественную циркуляцию теплого воздуха можно только в случае низкой плотности мощности в стойке. Горизонтальные скорости воздуха, который гонят вентиляторы серверов, намного превосходят скорость конвективного подъема даже в нашем идеальном случае. Пусть стойка по горизонтали занимает 0,4 м ширины горячего коридора. Воздух будет успевать подняться до ее верха только при горизонтальной скорости не более 0,15 м/с ($v = s/t$). В этом случае стойка сечением 1,2 м² (600 мм × 2000 мм) потребляет воздуха не больше 0,16 м³/с. Если исходить из того, что на отвод 1 кВт тепла требуется 0,075 м³/с воздуха (старое оборудование), то тепловыделение стойки не должно превышать 2 кВт.

На практике же подъем горячего воздуха еще меньше. Во-первых, при мало-мальски разумной расстановке оборудования горячий воздух выбрасывается не в зону холодного воздуха, а в такой же горячий, что уменьшает разницу плотностей и соответственно подъемную силу. Во-вторых, в реальности конвективный подъем значительно замедляется из-за возникающих сил трения. Так что его скорость меньше примерно на порядок.

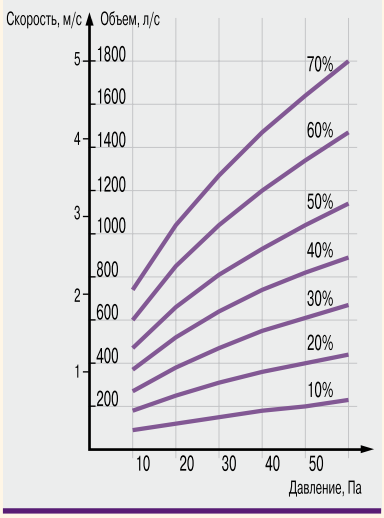
Миф 6. Сопротивление решеток фальшпола должно быть минимальным

На самом деле перфорированные плитки – эффективный механизм регулировки подачи воздуха. Характеристики плиток с разным уровнем перфорации, рассчитанные по формуле из книги И.Е. Идельчика*, приведены на рис. 2.

Сопротивление плиток при классическом варианте фальшпольного охлаждения должно выбираться таким образом, чтобы, с одной стороны, была обеспечена необходимая подача воздуха, а с другой стороны, падение давления на них было бы больше, чем остальные изменения давления, как статические, так и динамические. Ведь элемент с наибольшим сопротивлением оказывает наибольшее влияние на процесс.

В случае применения контейнеризации роль такого демпфирующего элемента переходит к замкнутому пространству контейнера, поэтому решетки действительно имеет смысл выбирать с максимально открытым (живым) сечением.

Рис. 2. Зависимость скорости воздушного потока и объема пропускаемого воздуха от его давления при разном уровне перфорации плиток фальшпола



Миф 7. Сопротивление подфальшпольного пространства вызывает проблемы

Идеи насчет важности сопротивления трения пропагандируются некоторыми производителями активных вентиляторных плиток. Разумеется, размещать лотки, трубы и кабели поперек потока воздуха – это дурная практика. Тем не менее основные проблемы возникают вовсе не из-за сопротивления трения. Сильнее всего на неравномерность подачи влияет именно динамическое падение давления, приводя к уменьшению подачи и даже подсосу воздуха в фальшпол рядом с кондиционерами. Оно же приводит к значительным колебаниям подачи при переключении между разнесенными в пространстве кондиционерами.

Миф 8. Серверная требует трехкратного воздухообмена

Серверная – это не то место, где постоянно находится персонал. Поэтому вентиляцию можно и нужно сводить к минимуму, достаточному для поддержания небольшого избыточного давления. Происхождение данного заблуждения – бессмысленные и беспощадные требования действующей Инструкции по проектированию зданий и помещений для электронно-вычислительных машин (СН 512-78). Учитывая скорость прогресса вычислительной техники, очевидно, что этот документ устарел еще в момент написания.

К счастью, в проекте можно указать следующее: «Согласно п. 1.1 инструкции, ее нормы не распространяются на здания и помещения для электронно-вычислительных машин, устанавливаемых в соответствии со специальными требованиями». Поэтому далее ее положения используются в качестве рекомендательных, а не обязательных.

*И.Е. Идельчик. Справочник по гидравлическим сопротивлениям. 3-е изд. М.: «Машиностроение», 1992.

Миф 9. Для проекта берутся параметры А или Б из СНиП по климатологии

Увы, с годами нормативные документы иногда становятся хуже. В старом СНиП был параметр В – абсолютные максимумы. Именно эта величина и должна использоваться при проектировании критических задач. Вряд ли заказчик одобрит работоспособность системы на уровне 0,98 в течение года. Замечу, что, согласно п. 5.12 СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование», в задании на проектирование допускается принимать более низкую температуру наружного воздуха в холодный период года и более высокую температуру наружного воздуха в теплый период.

■ ■ ■

Надеюсь, этот краткий анализ мифов поможет избежать типичных ошибок или пригодится при обосновании выбираемых решений. ИКС

Типовые отказы ЦОДов и их профилактика

Андрей ПАВЛОВ, генеральный директор, DataDome
Дмитрий КУСАКИН, независимый консультант
Дмитрий БАСИСТЫЙ, независимый консультант

Надежность ЦОДа, как известно, зависит не только от качества установленного в нем оборудования и правильности проектных решений. Может быть, даже в большей степени на нее влияют качество монтажных работ и исполнения процедур эксплуатации.

В данной статье мы расскажем о типовых проблемах в процессе эксплуатации ЦОДа, которые встречались в нашей практике.

Дизель-генераторные установки

Основой бесперебойной работы ЦОДа является бесперебойное энергоснабжение ИТ-оборудования и систем кондиционирования. С учетом качества и надежности отечественных внешних электрических сетей узким местом в системе энергоснабжения ЦОДа становятся ДГУ и ИБП. Причем незапуск ДГУ может принести гораздо больший ущерб, нежели выход из строя ИБП.

Очевидно, что в случае пропадания внешнего городского энергоснабжения последним оплотом бесперебойной работы ЦОДа остается дизель-генераторная установка. А значит, любой сбой в ее работе может привести к остановке всего ЦОДа. При этом сама ДГУ представляет собой сложное инженерное устройство, состоящее из множества компонентов, каждый из которых может стать причиной аварии.

В качестве примера рассмотрим проблему, возникшую в результате поломки системы вентиляции контейнера ДГУ. В одном из ЦОДов произошел следующий инцидент: в момент пропадания напряжения на городских вводах ДГУ запустилась в аварийном режиме, электроснабжение ЦОДа было восстановлено. Дежурная смена, инженеры, присутствовавшие в то время в дата-центре, занялись выяснением причин пропадания внешнего снабжения, при этом перестав уделять внимание «стабильно работающей» системе. Через короткий промежуток времени ДГУ остановилась, ЦОД был обесточен полностью. После выяснения причин аварии оказалось, что в контейнере ДГУ из-за засора всего-навсего не открылись шторки жалюзи вентиляции. Температура в контейнере существенно поднялась, и была подана автоматическая команда на отключение двигателя. А поскольку в ЦОДе отсутствовала централизованная система мониторинга, то информация об ошибке не появилась на мониторах дежурной смены. Аварию удалось устранить, лишь принудительно открыв шторки жалюзи ДГУ.

Один из способов решения данной проблемы – система мониторинга, отслеживающая максимальное количество параметров ДГУ, в том числе температуру в контейнере, и работоспособность и состояние вспомогательных систем. В случае же отсутствия такой системы (что сложно себе представить для ЦОДа) необходимы четкие инструкции дежурной смене, предписывающие личную проверку пуска ДГУ и работоспособности вспомогательных систем.

Электрощитовое оборудование и автоматика

Как показывает практика, некорректные алгоритмы работы и ошибки системы автоматики электрощитового оборудования могут вызвать не менее серьезные проблемы, чем неработоспособность ДГУ.

Например, в одном из дата-центров случился сбой, хотя и не приведший к аварийному останову инженерных систем, но ухудшивший экономические показатели бизнеса. Произошло кратковременное пропадание городского ввода, в результате чего автоматика подала сигнал на запуск ДГУ, но при дальнейшем восстановлении энергоснабжения она не перевела нагрузку обратно на внешний ввод. Дизель-генераторная установка находилась вне зоны прямой видимости дежурной смены, а система мониторинга не отслеживала работу системы автоматического ввода резерва (АВР). В результате ДГУ мощностью 1 МВт проработала не менее 4 ч и

сожгла порядка 1 куб. м дизельного топлива, что обошлось ЦОДу в сумму около $1000. Сумма, может быть, и не критичная для устойчивости экономики ЦОДа, но эти расходы были совершенно лишними и их легко было избежать. К тому же, проработай ДГУ еще какое-то время, могло закончиться дизельное топливо, а это спровоцировало бы остановку всего дата-центра.

Случаются на практике и ошибки автоматики другого рода, вызванные некорректной настройкой реле контроля фаз. При приемке вновь построенного дата-центра зачастую не уделяется должного внимания уставкам границ срабатывания АВР. Настройка может проводиться на граничное значение по умолчанию – 400 В, в то время как среднее значение входного напряжения составляет 380 В. Пока ЦОД еще недостаточно нагружен, срабатывания АВР и перехода на ДГУ не происходит, но когда дата-центр начинает приближаться к расчетной мощности, напряжение под нагрузкой проседает на 5–7 В, автоматика может воспринять это как пропадание городского ввода и дать команду на запуск ДГУ и перевод всей нагрузки на резервный источник электроснабжения. Затем городское напряжение начинает расти, происходит обратный переход на городской ввод. Такая ситуация может запустить неконтролируемую цепочку переключений с городского ввода на ДГУ и обратно, которую можно прервать только вручную.

Зачастую во время пусконаладки системы энергоснабжения подрядчик неправильно выставляет настройки селективности групповых и стоечных автоматов, что впоследствии может вызвать каскадное отключение группы потребителей от нагрузки во время короткого замыкания на одном из потребителей. Ток короткого замыкания, возникающий в стойке, при неверных настройках автоматов может пройти на групповой автомат, либо отключив его, либо пройдя еще выше по иерархии электрораспределительной системы и отключив автомат более высокого уровня, включая ГРЩ. Для ЦОДа это достаточно критично, так как ошибка всего лишь в одной стойке способна обесточить от нескольких рядов стоек до всего ЦОДа целиком.

Помимо приведенных примеров работа автоматики электроснабжения может вызвать массу других ошибок в работе дата-центра, так как логика ее работы – суть основа надежности ЦОДа. Чтобы избежать ошибок, связанных с автоматикой электроснабжения, следует обратить на нее пристальное внимание на стадии проектирования, а во время эксплуатации проводить периодические комплексные испытания логики взаимодействия инженерных систем ЦОДа, моделируя всевозможные аварийные ситуации и отслеживая поведение системы.

Источники бесперебойного питания

Продолжая тему ошибок в энергосистеме ЦОДа, нельзя обойти вниманием такой важный элемент системы энергоснабжения, как ИБП. Наиболее типичной аварийной ситуацией с ИБП можно считать короткое замыкание на его электросхемах вследствие некачественного обеспыливания устройства и уборки. В нашей практике было два прецедента, связанных с некачественной уборкой ИБП, которые привели к выгоранию его электрических схем и далее к деградации всей системы бесперебойного энергопитания ЦОДа. Нельзя сказать, что данная проблема – удел исключительно инженерии дата-центра, но с учетом важности этих компонентов для работоспособности ЦОДа и высокой вероятности события из-за больших мощностей ИБП, рекомендуем обратить на нее пристальное внимание в процессе эксплуатации.

Часто также происходят инциденты с батарейными блоками ИБП, приводящие к задымлению и даже пожару. А виной всему некачественная протяжка соединительных перемычек аккумуляторных батарей. Особенно часто это происходит, если при производстве батарей используют свинцовые клеммы. Свинец – пластичный материал, со временем он становится текучим, в буквальном смысле течет. И если периодически не протягивать соединения, то через некоторое время контакт ослабевает, в этом месте возникает локальное повышенное сопротивление, и при прохождении большого электрического тока оно начинает нагреваться. Со временем под воздействием электричества и тепла свинец плавится, что с высокой вероятностью может привести к задымлению и пожару.

Проблема касается не только контактов ИБП, но и в целом всей системы электрораспределения ЦОДа. Как часто говорят, электрика – наука о контактах, и 80% всех проблем с электрикой связаны с некачественно выполненными соединениями. Эти проблемы могут вызвать в ЦОДе пожар, не говоря уж о том, что даже минимальное локальное задымление может привести к значительному простою ЦОДа в результате срабатывания системы газового пожаротушения.

Помимо прочего необходимо уделять повышенное внимание равномерности заряда аккумуляторных батарей (АКБ). В начале эксплуатации ИБП аккумуляторные батареи часто заряжаются и разряжаются крайне неравномерно, что может негативно повлиять на их срок службы и длительность работы ИБП в автономном режиме. Эта проблема возникает вследствие различных уровней заряда батарей в начале их эксплуатации. Частично ее можно устранить, используя метод «раскачки» АКБ – так же, как мы поступаем обычно с батареями мобильных устройств. Перед началом промышленной эксплуатации ИБП желательно несколько раз провести процедуру полного разряда и затем полного заряда батарей.

Система кондиционирования

Известно, что за несколько минут простоя системы кондиционирования температура внутри машинного зала может вырасти на десятки градусов. При этом вероятна, как минимум, остановка ИТ-нагрузки по перегреву, а в худшем случае – потеря важной информации. Поэтому вторым по значимости для работы ЦОДа фактором, после непрерывности энергоснабжения, является поддержание требуемых значений влажности и температуры.

Мы постоянно пропагандируем идею, что ЦОД – это единый организм, живущий по своим правилам, в кото-

ром инженерные подсистемы неразрывно взаимодействуют между собой, растут и развиваются вместе с дата-центром. Если нет поддержки и понимания этой идеи, возникает первая проблема – отсутствие оптимизации ресурсов ЦОДа с ростом его энергопотребления. Например, во вновь построенном ЦОДе неопытная служба эксплуатации включает в работу все кондиционеры или большую их часть, не учитывая, что работает только небольшая часть ИТ-нагрузки и, соответственно, выделяется лишь малая часть номинальной тепловой нагрузки. Это провоцирует слишком частые повторения циклов включения и выключения компрессоров, что влечет за собой повышенный износ оборудования и преждевременный выход его из строя. Точно так же необходимо четко и правильно настроить периоды переключения кондиционеров в режиме ротации, чтобы снизить риск преждевременного износа оборудования. Ни в коем случае нельзя допускать частого включения кондиционеров на непродолжительное время.

Стоит обратить внимание и на такую проблему, как обмерзание вентиляторов внешних блоков системы кондиционирования в холодное время года. И хотя частое переключение кондиционеров в режиме ротации приводит к более быстрому износу оборудования, тем не менее зимой эту процедуру стоит проводить чуть чаще, чем в теплый период.

Не работающий длительное время вентилятор зимой вполне может механически заклинить после атмосферных осадков (ледяного дождя, снега) или из-за образования сосулек. При последующем запуске кондиционера это приведет к сбою и к отключению кондиционера по аварии.

Этих проблем можно избежать, просто проведя подготовку кондиционеров к наступающему холодному или теплому сезону, скорректировав количество хладагента в системе и уделив особое внимание обслуживанию внешних блоков.

Касаясь жидкостных систем холодоснабжения, нельзя не отметить проблемы с системой распределения хладагента, т. е. трубопроводами. Как ни старались мы равняться на Запад в области качества проведения монтажных работ, оно по-прежнему оставляет желать лучшего. Особенно это относится к простым, казалось бы, сантехническим работам. Причем, как известно, жидкость – один из основных врагов электрических систем ЦОДа, а жидкость, находящаяся непосредственно в ЦОДе, – это враг в квадрате. Поэтому предотвращение протечек в жидкостных системах холодоснабжения – задача номер один для службы эксплуатации любого ЦОДа. Мы неоднократно сталкивались с авариями в дата-центрах, при которых происходили утечки хладагента непосредственно в машинный зал, и в подавляющем большинстве случаев это случалось в местах подсоединения шкафных кондиционеров к системе трубопроводов. Такие соединения, как правило, выполняются с помощью гибкой подводки, поэтому на этапе строительства необходимо максимум внимания уделить качеству применяемых в данном узле материалов и квалификации персонала, выполняющего работы. Не стоит и забывать о периодической проверке и протяжке креплений этих узлов в процессе эксплуатации.

В завершение темы об ошибках системы кондиционирования расскажем еще об одной проблеме: автоматическом запуске системы фреонового кондиционирования после кратковременного пропадания энергоснабжения либо после переключения на аварийный источник энергоснабжения. Это случается с оборудованием далеко не всех производителей, но если вам не повезло и вы выбрали оборудование, для которого такая проблема существует, лучше диагностировать ее заранее. Дело в том, что некоторые модели прецизионных кондиционеров после пропадания питания или всплесков напряжения трактуют данное событие как «ошибку чередования фаз». Эта авария относится к критическим, автоматически она не снимается, сделать это можно только вручную. Каково же было удивление службы эксплуатации некоего коммерческого ЦОДа, когда после пропадания напряжения на городском вводе и запуске ДГУ все кондиционеры выдали «ошибку по фазировке» и отказались запускаться. Для диагностирования этой аварии рекомендуем провести комплексные испытания ЦОДа при его приемке и обязать подрядчика устранить проблему до начала эксплуатации. В некоторых случаях может помочь перепрограммирование контроллера, а в других придется ставить стабилизатор напряжения или принимать иные меры.

Система видеонаблюдения

Описанную ниже проблему нельзя классифицировать как аварию или отказ, но если вы учтете следующий совет, это позволит вам избежать затяжных споров с подрядчиками по эксплуатации инженерных систем. Старайтесь содержать систему видеонаблюдения в состоянии «полной боевой готовности»! Этой системе, особенно в машинных залах, многие не придают особого значения, считая, что она полностью работоспособна, а по факту нередко нужная камера оказывается не в фокусе, смотрит «в землю», или же запись просто не ведется. Но при «разборах полетов» только видеозапись позволяет однозначно определить виновных и оценить действия персонала в критических ситуациях.

Собственно, этот последний совет касается не столько технической части ЦОДа, сколько организации его службы эксплуатации в целом.

■ ■ ■

Как показывает наш опыт, большая часть аварий в дата-центре происходит из-за повышенного влияния человеческого фактора и зачастую из-за отсутствия у службы эксплуатации опыта, строго прописанных регламентов и технологических карт проведения работ. Резюмируя все сказанное выше, хочется отметить, что четко отлаженная работа службы эксплуатации, способной предотвратить большинство возникающих проблем, как известных, так и новых, – залог надежной и безотказной работы столь сложного объекта, как ЦОД. ИКС

Cloud & Mobility
CONFERENCE

издается с 1992 года
ИКС
www.iksmedia.ru

2-я международная конференция Cloud & Mobility 2013

для руководителей и сотрудников корпоративных департаментов ИТ и сервис-провайдеров

19 марта 2013 года, Москва, Центр «Digital October»

Развитие облачных вычислений и мобильности остаются основными движущими силами, оказывающими сегодня влияние на трансформацию корпоративных ИТ-архитектур. Использование частных, публичных и гибридных облаков, BYOD, кросс-платформенных мобильных приложений, управление гетерогенными ИТ и информационная безопасность являются одними из наиболее обсуждаемых сегодня тем в среде ИТ-профессионалов. На второй ежегодной конференции Cloud & Mobility 2013 мы продолжим изучение опыта первопроходцев и поиск лучших практик для минимизации рисков наблюдаемых процессов трансформации.

Цели конференции:

- Рассмотреть ключевые аспекты перехода к облачной инфраструктуре
- Профессионально обсудить вопросы применения облаков и доступа к ним
- Узнать от поставщиков и пользователей о последних отечественных примерах использования облаков и мобильных облачных решений
- Рассмотреть мобильные решения и устройства как инструмент бизнеса
- Изучить лучшие бизнес-кейсы и примеры отдачи от внедрения
- Обсудить перспективы развития облачных услуг в мире и в России

Аудитория конференции:

ИТ-директора, руководители служб поддержки ИТ-инфраструктуры и информационных систем, ведущие отраслевые эксперты и аналитики, владельцы и руководители ЦОДов, представители крупнейших сервис-провайдеров и поставщиков решений.

www.cloudmobility.ru

Регистрируйтесь и присоединяйтесь к участникам конференции!
Дополнительная информация по телефонам:
+7 (495) 785-14-90, 229-49-78, 502-50-80

Организатор – журнал «ИКС»

Автономное и универсальное

новое устройство пожаротушения российского производства

Антон АННЕНКОВ,
исполнительный директор,
Группа компаний
«Пожтехника»

Информация – один из наиболее ценных ресурсов любой современной компании. Утеря данных или сбой в ИТ-системе могут оказаться критически опасными для бизнеса. А ведь причиной такого сбоя может стать и небольшое замыкание в системе питания серверной стойки...

Для предупреждения возгораний и сведения к минимуму ущерба в случае их возникновения в коммуникационных шкафах, серверных стойках, устройствах управления производством, специальных сейфах и другом электротехническом оборудовании применяются современные автономные установки пожаротушения.

В 2012 г. на рынке средств пожарной безопасности появилось новое автономное устройство шкафного тушения российского производства – R-Line (АУШТ-NVC). Это компактное устройство предназначено для автоматического обнаружения и безопасного тушения возгораний в закрытых 19-дюймовых шкафах.

В состав решения R-Line (АУШТ-NVC) входят следующие основные компоненты:

- устройство обнаружения пожара – аспирационная камера с двумя адресно-аналоговыми дымовыми извещателями;
- устройство пожаротушения – модуль с газовым огнетушащим веществом 3M Novec™ 1230, экологически чистым и безопасным для оборудования и для персонала;
- система управления и связи с общей системой пожарной безопасности, позволяющая управлять системой удаленно;
- система электропитания (класс А), при возникновении сбоев способная работать автономно.

Эффективно и безопасно

В качестве огнетушащего вещества в устройстве R-Line (АУШТ-NVC) используется газовое огнетушащее вещество нового поколения Novec™ 1230. Оно уже зарекомендовало себя на рынке средств пожарной безопасности как наиболее эффективное решение. Novec™ 1230 является диэлектриком, что позволяет безопасно тушить электротехническое оборудование. Оно также безвредно для человека, не понижает концентрацию кислорода в помещении, нетоксично и не попадает под международные ограничения, связанные с защитой окружающей среды.

Технические подробности

Устройство R-Line (АУШТ-NVC) устанавливается в верхней части 19-дюймового шкафа. Встроенная аспирационная система обнаружения возгорания, состоящая из адресно-аналоговых дымовых извещателей, проводит непрерывный отбор проб воздуха по всему объему защищаемого шкафа. Такой контроль позволяет минимизировать время между обнаружением возгорания и запуском процесса тушения.

Устройство может функционировать независимо от внешних источников питания и систем управления, что, в свою очередь, сводит к минимуму возможность отказа или ложного срабатывания. Блок питания со встроенным источником резервного питания (аккумуляторные батареи) гарантирует непрерывную работу системы.

Новинка выпускается в исполнении как для стандартных 19-дюймовых герметичных шкафов, так и для шкафов любой нестандартной формы, с возможностью монтажа установки как внутри, так и снаружи защищаемого объема. Таким образом,

Автономное устройство шкафного тушения R-Line (АУШТ-NVC)

Огневые испытания

В ноябре 2012 г. специалисты ГК «Пожтехника» провели сравнительные демонстрационные огневые испытания установки на базе компании «Ростелеком» в Ростове-на-Дону. Установка испытывалась в условиях, максимально приближенных к рабочим: использовались реальные стойки с оборудованием, работающим под напряжением. Все пуски установки были успешными – возгорание в стойках было обнаружено на ранней стадии, тушение происходило за 5–10 секунд, при этом оборудование продолжало работать в штатном режиме! По результатам испытаний специалистами оператора было выдано положительное заключение и рекомендации для применения устройства пожаротушения R-Line (АУШТ-NVC) на объектах ОАО «Ростелеком».

R-Line (АУШТ-NVC) – это практически универсальное решение для защиты небольших объемов, оно может быть использовано для защиты различного электротехнического оборудования и в шкафах нестандартной конфигурации. Это позволяет экономить значительные средства, когда установка системы автоматического газового пожаротушения по объему всего помещения оказывается слишком дорогостоящей. При этом обеспечивается полноценная и надежная защита оборудования.

Установка чрезвычайно проста в монтаже и эксплуатации, в случае срабатывания она приводится в исходное рабочее состояние прямо на объекте.

Все это делает устройство пожаротушения R-Line (АУШТ-NVC) поистине универсальным решением для защиты шкафов с электронным оборудованием.

Оценили по достоинству

В числе основных преимуществ R-Line (АУШТ-NVC) специалисты отмечают:

- эффективность – тушение возгораний за 10 секунд;
- возможность работы в энергонезависимом режиме (без использования внешних источников питания) более 20 часов;
- универсальность – подходит для защиты любого электротехнического оборудования;
- возможность тушения электротехнического оборудования (благодаря диэлектрическим свойствам огнетушащего вещества);
- долговечность – срок эксплуатации более 10 лет;
- простоту эксплуатации –устройство не требует дополнительного обслуживания, после срабатывания его можно привести в рабочее состояние прямо на объекте.

Устройство пожаротушения R-Line (АУШТ-NVC) соответствует всем требованиям нормативных документов, применяемых к автоматическим установкам газового пожаротушения, и имеет сертификат соответствия Техническому регламенту о требованиях пожарной безопасности.

Демонстрация работы автоматической установки шкафного тушения R-Line (АУШТ NVC) с использованием модельного очага состоялась в Академии государственной противопожарной службы МЧС России

На выставке MIPS в этом году новое решение отмечено дипломом «Рекомендовано к внесению в Реестр новой техники и московский территориальный строительный каталог для применения на объектах города Москвы». По результатам совместных с компанией «Пожтехника» испытаний устройство R-Line (АУШТ-NVC) было высоко оценено специалистами Академии МЧС РФ.

Сети для систем безопасности

оптимальные топологии

Сергей КУЧУМАРОВ,
бренд-менеджер,
«АРМО-Системы»

В основе практически всех систем физической безопасности сегодня лежат цифровые решения. Но если несколько лет назад преобладающими каналами для связи и интеграции в них были RS232/422/485, то сейчас альтернативы сетям Ethernet практически нет.

Современные тенденции в развитии систем безопасности таковы, что самый стремительный рост наблюдается в сегменте IP-видеонаблюдения. Кроме того, производители, выпускающие контроллеры СКУД, пожарные панели и другое охранное оборудование, закладывают практически во все устройства возможность передачи данных по Ethernet. На этом фоне существенно выросла популярность сетевых систем безопасности по сравнению с традиционными, что обусловило и повышение спроса на активное сетевое оборудование.

Среди наиболее важных факторов, способствующих распространению сетевых систем, необходимо выделить возможность передачи в рамках одной сети сигналов и сообщений систем различного назначения с сохранением общности управления и мониторинга. К несомненным преимуществам сетевых решений относятся также универсальность средств передачи данных (медный кабель и оптоволокно), отсутствие необходимости ретрансляции и неограниченные расстояния передачи данных. Широкий ассортимент оборудования, разумная цена и хорошая информационная база делают сетевые системы еще более привлекательными для пользователя.

Специфика сетей в сфере безопасности

Создание надежной и высокопроизводительной сети для проекта комплексной системы безопасности или для автоматизации управления инженерией объекта – задача не менее важная, чем правильный выбор интеграционной платформы и оконечного оборудования. Очевидно, что плохо функционирующая сеть может свести на нет преимущества самой современной аппаратуры и средств автоматики. Кроме того, надо четко представлять специфику таких сетей по сравнению с офисными (LAN) и территориальными (WAN) коммуникационными структурами. Особенности их таковы:

- существенно отличающийся по объему и преобладающему направлению трафик (сетевая телекамера создает преимущественно однонаправленный и довольно стабильный поток) по сравнению с мультимедийным офисным или интернет-трафиком;
- эпизодический и крайне незначительный по объему трафик от контроллеров систем безопасности и средств автоматизации;
- более однородная номенклатура установленных источников данных и прикладного программного обеспечения, изолированность их от внешних сетей, а следовательно, менее жесткие требования к информационной безопасности сетей;
- гораздо более высокие требования к физической защите (противодействие саботажу);
- территориальная разбросанность подсетей по контролируемым площадкам (цеха, периметры, филиалы объекта);
- необходимость обеспечить живучесть, невосприимчивость к электромагнитным помехам и др.

Такой предварительный анализ естественным образом подводит нас к выбору между двумя возможными отказоустойчивыми топологиями сети – «дерево» (trunk) и «кольцо» (ring). По мнению автора, топология «кольцо» наиболее полно отвечает требованиям, предъявляемым к сетям в сфере систем безопасности.

Основным строительным элементом современной одноранговой (плоской) сети или подсети является коммутатор (switch), повторители (hub) сейчас практически не используются. Для объединения нескольких сетей применяются маршрутизаторы (router) и мосты (bridge), которые в рамках данной статьи мы не рассматриваем.

Ключевые моменты в работе одноранговой сети

Основные задачи, решаемые на уровне сетевого коммутатора, таковы:

- создание сети;
- авторизация (безопасность);

IP-технологии выходят вперед

В недавнем отчете компании IMS Research (2012 г.) прогнозируется, что до конца текущего года мировой рынок систем видеонаблюдения вырастет более чем на 12%, и это несмотря на неопределенность общей экономической ситуации и вялость основных трендов. По данным аналитиков, объем реализации IP-камер видеонаблюдения, составлявший в 2011 г. 40% общемирового дохода от продаж камер слежения, возрастет в 2016 г. до 60%. Таким образом, IP-технологии начинают вытеснять традиционные решения.

- проверка целостности информации;
- фильтрация трафика;
- сегментирование и качество связи;
- управление сетью;
- питание устройств;
- масштабирование.

Главная функция коммутатора – выполнение обязанностей «почтальона», т. е. передача пакета из порта-источника в порт-получатель в пределах емкости коммутатора или далее, если адрес порта-получателя не обнаружен в собственной таблице адресов. При этом доставить информацию надо без потерь и с минимальными задержками. Надежную передачу данных обеспечивает принцип store-n-forward, благодаря которому устраняются потери информации по причине перегрузки канала.

Хотелось бы отметить, что в лучших современных коммутаторах производительность внутренней коммутационной шины (switch fabric) превышает суммарную производительность всех портов в дуплексном режиме, за счет чего обеспечивается неблокирующая коммутация.

Создание сети предполагает стандартизованную реализацию физических принципов, применяемых для передачи цифровой пакетной информации на уровне порта (электрический или оптический импульс), т.е. обеспечение «стыкуемости» и «взаимоузнаваемости» активного оборудования сети при передаче цифровой информации в одноранговой сети с коммутацией пакетов.

Для контроля допустимых адресов участников сети используется **авторизация** (политика безопасности), что гарантирует предсказуемость потоков данных, например при создании виртуальных подсетей.

Проверка целостности информации гарантирует, что единичный пакет принят целиком без пропусков и без искажений. **Фильтрация** трафика и **сегментирование** сети обеспечивают оптимальный режим работы, в котором информация попадает именно туда, куда она направлена.

Наличие инструментария для **управления сетью** позволяет сконфигурировать коммутаторы и настроить оптимальные режимы их работы (CLI-интерфейс, веб-интерфейс, SNMP).

Что касается **питания устройств,** то с современными коммутаторами можно использовать оконечные устройства (камеры, точки доступа Wi-Fi, контроллеры), поддерживающие стандарт PoE (Power-over-Ethernet) и High-PoE.

Масштабирование для обеспечения необходимой емкости сети достигается за счет соединения коммутаторов через uplink-порты, с помощью агрегирования (объединения нескольких портов в один виртуальный порт более высокой пропускной способности) или стекирования через специальные разъемы устройств.

Современные коммутаторы выпускаются в нескольких исполнениях и имеют различные конструктивные особенности. В частности, так называемые промышленные устройства, которые наиболее интересны в контексте создания сетевых систем безопасности, выпускаются, как правило, в компактных корпусах для монтажа на DIN-рейку. При этом они имеют большое время наработки на отказ (не менее 200 тыс. ч), не имеют вентиляторов (fanless), способны работать в диапазоне температур от –40 до +75°C и даже имеют защиту по классу IP67 (тип исполнения M12).

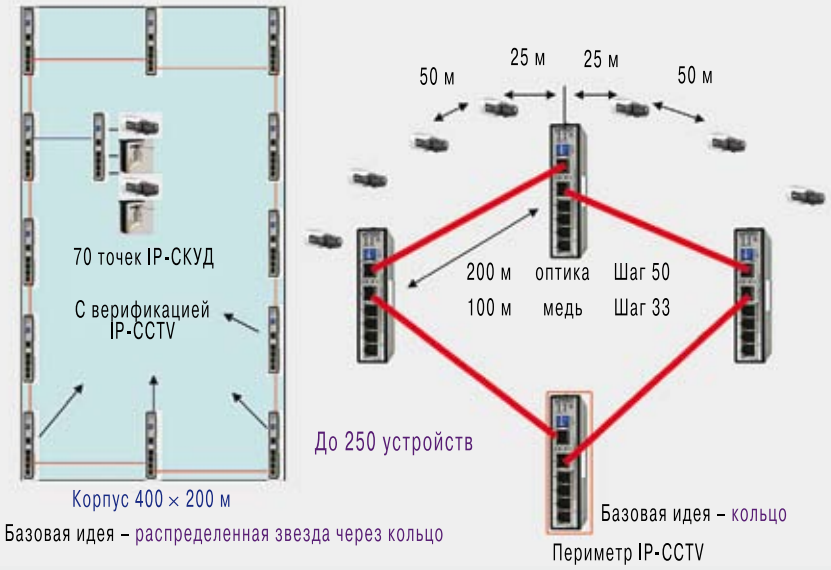
Топологии сетей

Анализируя топологии сетей с применением современных коммутаторов (рис. 1), нетрудно заметить, что применение однотипных устройств невысокой производительности как на уровне доступа (камеры), так и на уровне интеграции (видеорегистратор) имеет ряд фундаментальных ограничений. Например, восходящий трафик быстро увеличивается, и если объем его в 64 Мбит/с сам по себе для коммутатора на уровне 2 проблемы не представляет, то передать суммарный трафик 128 Мбит/с от двух узлов в кольцевую магистраль и/или на видеорегистратор уже не представляется возможным. Возможное решение очевидно – переход на уровне 0 на коммутаторы, имеющие «кольцевые» (или резервные в древовидной топологии) и дополнительные порты с пропускной способностью не менее 1 Гбит/с.

Впрочем, в некоторых прикладных системах, например в таких, где трафик генерируется ситуационно (видеодетектор движения, видео по запросу, системы видеоверификации для СКУД), возможно построение достаточно эффективных и бюджетных сетей на основе простейших коммутаторов (два примера практических инсталляций приведены на рис. 2).

Рис. 1. Примеры топологий сетей

Рис. 2. Примеры бюджетных сетей



Для построения более производительных сетей можно использовать коммутаторы с портами 1000T/SFP Combo (рис. 3). По мнению автора, такие коммутаторы наиболее перспективны, потому что в них заложен значительный ресурс развития. Например, на объекте установлена сеть с кольцевой топологией и пропускной способностью 100 Мбит/с, практически непрерывно работают 30 камер с типовым видеопотоком H.264 2,5 Мбит/с (суммарный поток 75 Мбит/с), т.е. заложенный ресурс практически исчерпан. Если понадобится добавить несколько более современных камер с разрешением HD, это потребует создания новой сети. В данном случае получается ложная экономия – в будущем все равно придется заплатить значительно больше с учетом не только замены активного оборудования, но и, возможно, части кабельной сети.

Топология и отказоустойчивость

С точки зрения живучести системы отказ сетевой камеры ведет к потере канала наблюдения, а обрыв кабеля в том или другом месте – к выходу из строя целого сегмента сети, при неблагоприятном стечении обстоятельств не исключен даже отказ всей системы (пример – отказ центрального коммутатора, к которому в результате неоптимального проектирования подключены и сервер системы, и сетевой видеорегистратор, и рабочая станция). Значит, урон даже от однократного отказа может быть катастрофическим для функционирования системы.

Именно по этой причине вряд ли можно рекомендовать топологию «звезда» для построения ответственных интегрированных систем безопасности, базирующихся исключительно на IP-решениях, поскольку при такой схеме предельно критичен даже единичный отказ. В специализированных прикладных локальных сетях, развернутых в пределах одного, пусть даже и протяженного объекта, где доступ к элементам сети гарантирован и требует приемлемого времени на восстановление, обычно вполне достаточно обеспечить защиту от однократного отказа за счет использования топологии «кольцо». В территориально распределенных сетях городского или регионального масштаба необходимо повышать защиту и кратность парируемых отказов, используя топологию «дерево» и/или полносвязную, по крайней мере для узловых коммутаторов. При этом стоимость сети может существенно вырасти. Для борьбы с возникновением в древовидных сетях замкнутых маршрутов, по которым пакеты теоретически могут циркулировать бесконечно, принимаются специальные меры.

Тем не менее есть два принципиальных возражения против использования древовидных структур в системах безопасности. Первое – это сложная, не всегда прозрачная топология сети и специфическое администрирование, что требует достаточно хорошей сетевой подготовки специалиста, который будет заниматься пусконаладкой. Второе – довольно большое время восстановления (переназначения оптимального маршрута) сети при отказе, достигающее нескольких секунд для небольших систем и нескольких минут для крупных сетей. В сфере безопасности такое длительное нарушение работоспособности систем недопустимо. Однако использование более высококлассного оборудования, поддерживающего скоростные алгоритмы или алгоритмы динамической маршрутизации, может оказаться слишком затратным. Кроме того, следует принять во внимание, что на практике чаще всего нет возможности установить каждый отдельный узловой коммутатор в отдельном шкафу (серверной) и проложить каждый магистральный кабель в отдельном кабельном канале. В результате топология, которая физически при проектировании выглядит как древовидная, на практике в смысле уязвимости вырождается в лучшем случае в кольцевую (представим себе возгора-

Рис. 3. Оптимальные топологии сети

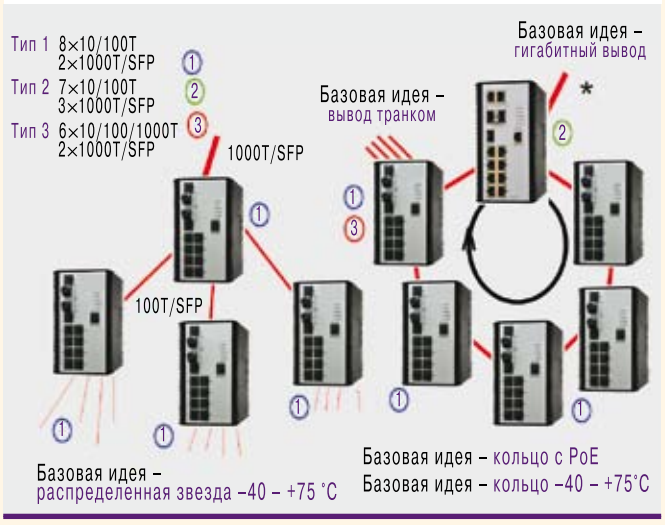
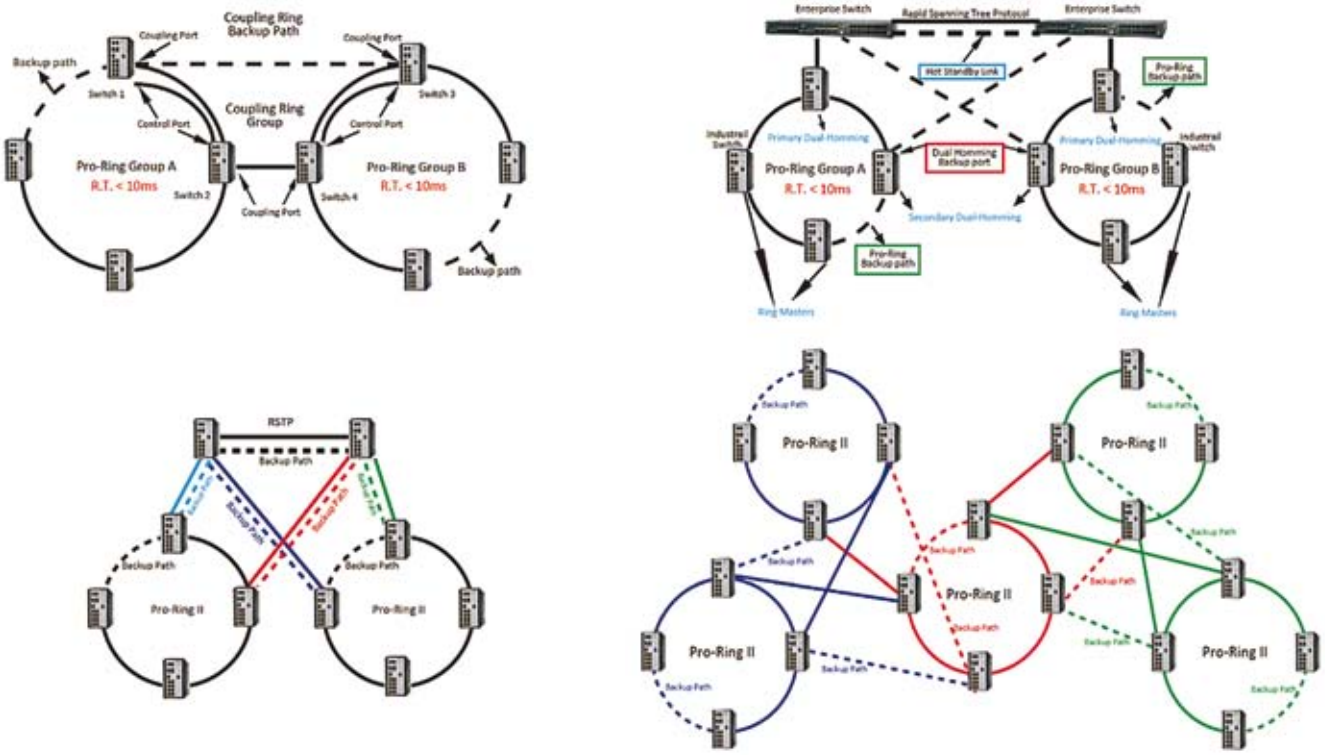


Рис. 4. Топологии отказоустойчивых сетевых систем безопасности



ние в шкафу, где установлено несколько узловых коммутаторов).

Появление высоконадежных коммутаторов с поддержкой технологии кольца, с быстрым (не более 10–30 мс) восстановлением и с пропускной способностью не менее 1 Гбит/с существенно упрощает и оптимизирует топологию сети. Такие коммутаторы, имеющие приемлемую стоимость, сейчас выпускает ряд компаний, например LanTech, Moxa, Hirschmann, GE/UTC, ComNet и др. Эти производители поставляют активное сетевое оборудование в том числе в защищенном от низких температур (Industrial) и даже во всепогодном (IP68 или M12) исполнении.

Практика сетевых систем безопасности

Из нескольких достаточно сложных топологий отказоустойчивых прикладных систем передачи цифровой пакетной информации, представленных на рис. 4, технология быстрого восстановления соединения реализуется только в пределах кольцевых структур. Дополнительные резервные маршруты настраиваются с помощью протоколов STP/RSTP. По этим причинам при проектировании рекомендуется учитывать возможные задержки при восстановлении сети.

Сетевые коммутаторы, поддерживающие топологию «кольцо», работают достаточно просто. Один из них назначается «мастером», в случае его отказа другой, наиболее близкий по сетевому адресу, берет на себя роль резервного, или субмастера. Остальные коммутаторы переключаются в режим «кольцо», как правило, с помощью DIP-переключателей на корпусе. Мастер посылает по кольцу в одном направлении служебные сигналы и, получив их по так называемому заблокированному порту, делает заключение о целостности кольца. В противном случае принимается решение о разрыве кольца, и пакеты посылаются так, как это происходит в обычной одноранговой сети, т.е. в обоих сегментах сети как к мастер-коммутатору, так и от него.

На практике время восстановления (переконфигурирования) сети настолько незначительно, что не происходит даже существенного срыва видеопотока формата H.264 от мегапиксельных камер.

Еще большая эффективность такого режима достигается за счет того, что IP-CCTV камеры используют для передачи видеопотока протокол UDP, при котором не устанавливается логическое соединение с адресатом; таким образом, вся ответственность по отслеживанию целостности сети целиком ложится на активное каналообразующее оборудование.

Порты SFP Combo позволяют сразу, без дополнительных затрат, строить сеть на основе медных соединений, используя кабель UTP/STP с максимальной длиной кабельного сегмента до 100 м. При использовании дополнительных съемных SFP-модулей имеется возможность без ретрансляции включать в топологию сети волоконно-оптические сегменты, длиной до нескольких километров при использовании мультимодового волокна и до нескольких десятков километров в случае одномодового волокна.

■ ■ ■

Индустрия безопасности – относительно небольшая отрасль, в которой развитие во многом идет вслед за

компьютерными системами, а тренды ИТ-сферы оказывают непосредственное влияние на запросы клиентов. Благодаря распространению Интернета, увеличению пропускной способности каналов, переходу с аналога на цифру и постоянному улучшению качества «цифровой картинки» сетевые технологии стали весьма востребованными в среде «безопасников». Конечно, на первый взгляд человеку неискушенному коммутаторы могут показаться очень сложным оборудованием, но в современных устройствах все необходимые настройки и процедуры могут выполняться через встроенный в них веб-сервер, а настройщику необходимы лишь базовые знания протокола TCP/IP и навыки опытного пользователя ПК. ИКС

Системы интерактивного управления в малых и средних СКС

Андрей СЕМЕНОВ,
доктор техн. наук

Способ автоматизации управления физическим уровнем информационной инфраструктуры в сетях большого масштаба известен – это использование систем интерактивного управления. Сегодня на повестку дня выходит та же задача для средних и малых СКС, но классическое оборудование в них неэффективно.

Информационная инфраструктура современного предприятия строится, как известно, в соответствии с моделью открытых систем. Одно из основных преимуществ такой модели – в немалой степени способствовавшее ее повсеместному распространению – состоит в том, что она открывает широкие возможности для реализации принципа plug & play на всех уровнях. Этот принцип сводится фактически к автоматическому изменению конфигурации и выполнению соответствующих настроек, что позволяет приступить к работе сразу же после запуска системы.

Физический уровень в этом отношении стоит особняком. Отсутствие в нем обязательного для применения источника питания означает, что для решения задач управления необходимо привлекать внешние ресурсы. В этом качестве обычно выступают мускульная сила и интеллект системного администратора.

При всех достоинствах системного администратора как непосредственного участника процесса администрирования кабельной системы ему не чужды и весьма серьезные недостатки. Как всякий представитель рода homo sapiens он более или менее часто совершает ошибки: например, в некоторых случаях пренебрегает установленными регламентами, в том числе не фиксирует изменения, проведенные в сети, забывает писать отчеты и т.д.

Зависимость нормального функционирования информационной системы от того, что называют человеческим фактором, в последнее время стала гораздо сильнее. Это вызвано следующими причинами:

- ростом масштабов информационных систем, в том числе из-за процессов глобализации;
- переходом на децентрализованную модель построения информационных систем, характерную в первую очередь для предприятий со множеством филиалов, представительств и иных структурных единиц;
- увеличением количества разнообразных сервисов, предоставляемых информационной системой;
- ростом скорости передачи информации и уменьшением помехоустойчивости каналов связи;
- повышением требований к конфиденциальности хранимых и обрабатываемых данных.

Как следствие, задача автоматизации процессов управления физическим уровнем информационной инфраструктуры предприятия по мере развития ИТ становится все более значимой. Один из эффективных способов хотя бы частичного ее решения – обращение к системам интерактивного управления (СИУ).

Новые сферы применения

Системы СИУ были разработаны и внедрены в широкую инженерную практику еще в начале 90-х гг. прошлого столетия. Об их востребованности говорит то, что положение об обязательности применения СИУ в крупных кабельных системах было включено в нормативную базу. В частности, оно введено в нормативную часть последних редакций европейских стандартов администрирования СКС.

Тем не менее до недавнего времени основной областью применения оборудования СИУ оставались сети большого масштаба, для которых, собственно, они и разрабатывались. Сейчас же все более актуальным становится внедрение СИУ в сети среднего и даже малого масштаба. Во-первых, наибольший объем портов инсталлированных информационных систем приходится на малые и средние информационные кабельные системы. Во-вторых, у средних и малых компаний есть естественная потребность в экономии на дорогих человеческих ресурсах – путем уменьшения загрузки системного администратора, увеличения общей эффективности его

работы и снижения требований к его профессиональной квалификации. В третьих, все более широкое распространение получает модель привлечения внешних специализированных компаний (аутсорсинг).

Особенности СИУ в малых и средних СКС

Классическое оборудование СИУ, рассчитанное на эксплуатацию в больших кабельных системах (СКС с несколькими тысячами портов), неэффективно в системах среднего и тем более малого масштаба. Классические СИУ слишком тяжеловесны для этой области применения, большая часть их функционала на практике оказывается невостребованной – просто в силу разного масштаба объектов. Далее, оборудование классических СИУ требует от системного администратора глубоких профессиональных знаний, в том числе из-за множества регулировок и настроечных функций. Наконец, коммутационное поле малых и средних кабельных систем из соображений экономии в большинстве случаев строится по схеме интерконнекта, которая весьма тяжело поддерживается программно-аппаратными комплексами, созданными на ранних этапах развития техники СИУ.

Попытки разрешить перечисленные проблемы предпринимались в течение последних пяти-семи лет. Наиболее очевидным способом следует считать обращение к таким СИУ, которые непосредственно взаимодействуют с системой управления современного активного сетевого оборудования. Тем не менее переделочный характер подобных решений, несмотря на оригинальность и остроумность некоторых из них (как наиболее яркий пример в этой области можно назвать разработку Pan-View iQ компании Panduit), закономерным образом не принес удовлетворительного результата. Отрасль остро нуждается в специализированных разработках, изначально учитывающих все нюансы новой области применения (мы будем обозначать их термином «малые СИУ»).

Требования к малым СИУ

Фактически выше уже сформулированы основные требования к таким СИУ: хорошие экономические характеристики, реализация базовых для данного оборудования функций, возможность эксплуатации персоналом с минимальным уровнем специальных знаний и адаптированность к работе совместно с коммутационным полем, построенным по схеме интерконнекта.

Из перечисленных требований вытекает необходимость обращения к системе сайтов. Последнее означает деление всей совокупности коммутационных панелей на отдельные области, в пределах которых работают отдельные сканеры СИУ. Недостаток подобной структуры – невозможность отслеживания соединений между панелями различных сайтов – не проявляется в небольших сетях просто из-за их малого масштаба. Кроме того, нельзя сбрасывать со счетов такое существенное преимущество, как резкое увеличение скорости работы системы и упрощение ее настройки.

Не менее логичным выглядит требование выстраивать процедуры взаимодействия с оборудованием через веб-браузер. Это дает возможность получать близкое к реальности изображение коммутационного поля и предоставляет программный интерфейс, интуитивно понятный для широкого круга пользователей.

Отдельные сканеры малой СИУ или их функциональные аналоги должны поддерживать режим автономной работы, который для этих устройств является фактически основным. Отсюда немедленно следует требование наличия в системе не только агента, но и сервера. Кроме того, для объединения контроллеров в единую систему и поддержки функции дистанционного мониторинга и управления самой аппаратурой СИУ возникает необходимость ввести в состав аппаратной части оборудования сетевой интерфейс класса не ниже 10/100 Base-T.

Идея создания полномасштабного автономного контроллера доведена до практического внедрения пока только компанией RiT Technologies – в продукте EPV, входящем в состав ее СКС серии SMART.

Решение проблемы интерконнекта

Схема интерконнекта основана на прямом соединении портов активного сетевого оборудования (как правило, его функции выполняет коммутатор ЛВС) и коммутационной панели СКС. Данное решение вполне логично с точки зрения реализации физического уровня информационной системы, но с точки зрения построения СИУ оно создает очень большие сложности. Главное направление решения проблемы заключается в искусственном преобразовании схемы интерконнекта в кросс-коннект, к которому затем применяются уже хорошо отработанные процедуры отслеживания соединения двух портов коммутационного оборудования.

На практике для внедрения СИУ в СКС с коммутационным полем на основе интерконнекта до последнего времени применялись накладки на переднюю панель активных сетевых устройств. Они содержали все необходимые элементы датчиков подключения, и сканеры работали с ними, как с обычной коммутационной панелью.

Исполнение такой накладки в виде гибкой полоски с печатными проводниками, наклеиваемой непосредственно на переднюю панель коммутатора, впервые было применено более десяти лет назад в системе iTracs одноименной компании. Общий недостаток такого подхода – способ крепления, далеко не всегда обеспечивающий нужную степень эксплуатационной надежности. Жесткие накладки (такие как ReView от RiT, системы Future Patch компании ТКМ, панели серии AMPTrac Ready от TE Connectivity) в случае их адаптации к активному сетевому оборудованию по этому параметру выглядят заметно лучше, однако они не решают главную проблему группового исполнения датчиков подключения: сложность согласования формфакторов накладки и передней панели коммутатора.

Частично проблема может быть решена с помощью системы SMART Interconnect компании RiT, основной компонент которой – выносная приставка, устанавливаемая перед коммутатором с небольшим зазором. За счет гибкости кабеля шнура она дает существенно большую свободу в выборе активного сетевого обору-

дования. Однако данное преимущество получено за счет усложнения конструкции шнура, на вилке которого предусматриваются дополнительные контакты.

Радикальный способ решения проблемы интерконнекта видится в отказе от централизованной схемы построения датчика в пользу распределенной. Для этого в каждый порт коммутатора устанавливается вставка с микросхемой, а для обмена данными с контроллером привлекается техника промышленных полевых шин или иные низкоуровневые подходы. Фактическое соответствие уникального адреса микросхемы вставки и порта коммутатора прописывается в ПО управления в процессе инициализации СИУ на этапе запуска в эксплуатацию. Такое решение требует некоторой переработки конструкции вилки, но технически это намного более простая операция, чем создание новой панели-накладки. Подобный подход используется в настоящее время в серийной продукции компании RiT Technologies. Сходная идея реализована в шнурах PanView iQ Interconnect Patch Cord. В отличие от аналога микросхема датчика подключения монтируется в вилке, а для привязки к порту коммутатора выполняется специальная процедура подключения шнура.

Ренессанс контактных схем датчиков подключения

Одним из ключевых компонентов аппаратной части СИУ является датчик подключения коммутационного шнура к порту панели, который может быть построен по контактной либо бесконтактной схеме. В первых серийных СИУ использовались исключительно контактные схемы (системы PatchView и iTracs), что объяснялось меньшей сложностью их реализации. В системах, созданных в первом десятилетии нового века, разработчики уже обращались преимущественно к бесконтактным схемам (световые затворы и различные варианты RFID-меток). В основе такого подхода лежало стремление устранить ненадежный непостоянный контакт из цепей сканирования состояния портов коммутационных панелей.

В последнее время мы наблюдаем возврат к контактным схемам построения чувствительных элементов. Этот процесс во многом инициализирован и серьезно стимулируется стремлением распространить область действия СИУ на случаи построения коммутационного поля по схеме интерконнекта, что безусловно необходимо в малых и средних СКС. Выше уже отмечалось, что наибольшая эффективность в этой области обеспечивается в случае перехода на распределенную схему построения датчика на основе вставок с микросхемами. Последние в процессе работы требуют напряжения питания, которое проще всего подать по прямой электрической цепи. Альтернативный вариант, основанный на накачке конденсатора электрической энергией по радиоканалу с последующим ее съемом на электронные компоненты (один из вариантов системы Future Patch), отличается существенно более низким КПД и потому до серийного продукта доведен только в этой разработке.

Возврат к контактной схеме из-за необходимости подачи напряжения дистанционного питания означает также переход на 10-контактное исполнение вилок коммутационных шнуров, для изготовления которых применяются 10-проводные гибкие кабели. Дополнительная пара проводов используется исключительно для технологических целей, ее наличие не влияет на основные информационные цепи передачи. Последнее положение требует дополнительного доказательства: в результате производитель СИУ вынужден проводить специальные испытания и отдельную сертификацию своих шнуровых изделий.

Дополнительные контакты могут располагаться в одном ряду с основными (система PatchView) или же выноситься на верхнюю поверхность корпуса вилки, с исполнением в форме скользящей пластинчатой детали (система MapIT компании Siemon) либо в виде гребня. В последнем случае говорят о контакте типа «зуб». Такой контакт может быть одиночным (тогда для обеспечения двухпроводной линии их требуется две штуки). Технически более сложно, хотя и заметно более эффективно, исполнение этого компонента по схеме «сэндвича», т.е. в виде двух симметричных металлических деталей, разделенных изолирующей прокладкой (система PanView iQ).

Степень эксплуатационной надежности узла подключения, которая необходима для СКС с ее многолетней гарантией, достигается за счет обращения к принципу контактной шины. Суть решения состоит в том, что в момент подключения вилки к розетке панели два контакта скользят друг по другу в плотно прижатом состоянии. Это позволяет сдвинуть частицы загрязнений (эффект самоочистки) и эффективно разрушить оксидную пленку, что необходимо для минимизации переходного сопротивления.

Прижимающее усилие, которое в обязательном порядке требуется для нормальной работы контактной шины, создается двумя основными способами. Первый – обращение к классическому нажимному контакту по схеме традиционных разъемных соединителей RJ45 (системы PatchView и Quareo от TE Connectivity). Второй способ реализован по двухсторонней схеме за счет исполнения контакта в форме V-образной щели.

Современные системы интерактивного управления – при условии некоторых технических усовершенствований – могут быть успешно внедрены в кабельные системы среднего и даже малого масштаба. Технически такое внедрение требует отказа от централизованной схемы построения, характерной для СИУ первых поколений, в пользу перехода на распределенную схему управления.

Обращение к распределенной схеме построения датчика подключения позволяет успешно решить проблему интерконнекта, что критически важно для кабельных систем среднего и малого масштабов. В целях расширения функциональных возможностей системы и достижения энергетической выгодности происходит возврат к контактным схемам построения чувствительных элементов датчиков подключения с использованием 10-проводных шнуровых кабелей и соответственно 10-контактных вилок. ИКС

Модульные ИБП

ИБП ENTEL IPS-M отличаются высокой плотностью мощности и гибкостью структуры. Конструктивно ИБП представляет собой набор системных стоек 19" с модулями статического переключения и мониторинга. Пользователь может самостоятельно «построить» необходимый ему ИБП, выбрав одну из четырех доступных системных стоек и необходимое количество силовых модулей в соответствии с мощностью защищаемой нагрузки.

Системные стойки выпускаются в двух вариантах по внешним габаритам. Шкаф размерами 2000×600×600 мм может обеспечить максимальную мощность 60 кВА. Шкаф размерами 2000×600×800 мм – мощность 60, 100, 150 и 200 кВА.

Требуемая общая мощность шкафа набирается с помощью дополнительных силовых модулей следующих мощностей: 3, 6, 10, 15 или 20 кВА.

Особенности системы:

- фазность конфигурируется в зависимости от требований: 1/1, 3/1, 1/3 или 3/3;
- имеется возможность резервирования по схеме N + X, что подразумевает возможность постепенного масштабирования и модернизации в рабочем режиме;
- все модули используют один или несколько батарейных модулей, что обеспечивает требуемое время автономии;
- общий КПД системы превышает 95%, а входной коэффициент мощности (PF) достигает 0,99;
- компактность – к примеру, один модуль 15 кВА весит 18 кг.

Общая мощность модульной системы, построенной на базе ENTEL IPS-M, может достигать 600 кВА.

«Инжиниринговая компания Гулливер»: +7 (495) 663-2172

Оптический абонентский терминал

STR-ONT – совместное предложение Группы СТР и компании PT Inovação (Португалия) для сетей GPON – основывается на рекомендации ITU G.984.x и поддерживает услуги triple play (передача данных, голоса, ТВ), предоставляя к ним доступ по интерфейсам Ethernet, Wi-Fi, FXS, RF Video Overlay и USB.

Терминал поддерживает высокоскоростные (до 2,5 Гбит/с в нисходящем потоке и до 1,24 Гбит/с в восходящем) каналы передачи данных в одном оптическом кабеле с коэффициентом деления 1:64.

STR-ONT соответствует стандарту G.984.4 (OMCI), что дает возможность интегрировать терминал в любую систему и взаимодействовать с оборудованием OLT любого производителя.

Управление терминалом производится по стандартам OMCI, TR-069 и TR-156. Это позволяет провайдерам услуг осуществлять полный контроль за оборудованием без участия пользователя.

Группа СТР: +7 (812) 612-1261

Программный комплекс для поддержки услуг M2M

PETER-SERVICE M2M – это многофункциональное решение для организации полного цикла поддержки услуг M2M (телематика и телеметрия), которое предоставляет провайдерам услуг, оказывающим M2M-сервисы на сетях операторов связи, единую точку доступа к M2M-услугам в части биллинга, тарификации и управления инфраструктурой.

В состав комплекса входит приложение «Единый центр управления и мониторинга M2M», в рамках которого реализовано гибкое управление процессами, характерными для технологии M2M. Единый центр позволяет потребителям услуг самостоятельно осуществлять управление и мониторинг, получать подробную информацию о состоянии M2M-услуг в режиме реального времени.

PETER-SERVICE M2M предусматривает защиту провайдера услуг от противоправных действий со стороны потребителей и позволит предотвратить нецелевое использование (сценарии обработки смены оборудования, блокировка и настройка уровня информирования о событиях и т.д.).

Благодаря открытому интерфейсу (API) комплекс PETER-SERVICE M2M легко интегрируется с существующей инфраструктурой операторов связи и провайдеров услуг, обеспечивая получение данных с оборудования оператора, мониторинг состояния M2M-соединений, управление пулом SIM-карт, формирование отчетности и гибкий механизм информирования.

«Петер-Сервис»: +7 (812) 326-1299

Энергоэффективные процессорные модули

Kontron CP3003 – модуль формата 3U CompactPCI на основе процессоров Intel Core 3-го поколения (Ivy Bridge). Может применяться для создания встраиваемых систем промышленного, оборонного, медицинского, транспортного назначения, а также различной испытательной и измерительной аппаратуры.

На CP3003 устанавливается двух- или четырехъядерный процессор, который может масштабироваться до Intel Core i7-3612QE с тактовой частотой 2,1 ГГц. Это позволяет в 2 раза увеличить вычислительную мощность целевой системы и в 4 раза ускорить обработку 3D-графики по сравнению с процессорными платами такой же мощности рассеивания. Для приложений, не требующих столь высокой производительности, доступны менее мощные процессоры, в том числе с низким (LV) и сверхнизким (ULV) энергопотреблением.

Графическая подсистема Intel HD4000 поддерживает технологии DirectX 11, OpenGL 3.1 и OpenCL 1.1, что помимо роста производительности обеспечивает возможность подключения трех независимых дисплеев. В двух разъемах SO-DIMM процессорного модуля CP3003 можно разместить до 16 Гбайт памяти DDR3 (1600 МГц) с поддержкой ECC. Возможна установка до 32 Гбайт флеш-памяти SLC NAND для хранения операционных систем и приложений.

Модуль CP3003 конструктивно имеет два исполнения: однослотовое – базовая плата с фронт-панелью (4HP) и двухслотовое – базовая плата плюс плата расширения и фронт-панель (8HP). Базовая плата CP3003 имеет следующие интерфейсы: 1 x VGA, 2 x USB 2.0 и 2 x Gigabit Ethernet на фронтальной панели, а остальные интерфейсы – USB 2.0, COM (RS-232) и SATA 3 Гбит/с и 6 Гбит/с – доступны на плате либо через тыльный разъем ввода-вывода. Плата расширения CP3003-HDD добавляет на фронтальную панель порты USB 3.0, Gigabit Ethernet, RS-232 и два порта DisplayPort, а также возможность установки карты CFast или до двух устройств 2,5" HDD/SSD. В качестве дополнительного расширения может быть использована плата-носитель для мезонинов XMC.

Kontron CP6004-SA – модуль формата 6U CompactPCI, предназначенный для создания приложений оборонного, медицинского и телекоммуникационного назначения. Он базируется на чипсете Intel QM77 Express и процессорах Intel 3-го поколения. Вычислительную мощность можно масштабировать посредством установки различных процессоров. Высшая производительность достигается с помощью четырехъядерного Intel Core i7-3615QE с тактовой частотой 4 x 2,3 ГГц. По сравнению с предыдущими версиями на процессорах Intel Core 2-го поколения вычислительная мощность модуля выросла в среднем на 20% наряду с ростом отношения производительности к потребляемой мощности. Благодаря встроенной графической подсистеме HD 4000 с поддержкой технологий DirectX 11, OpenGL 3.1, AVX и OpenCL 1.1 вдвое увеличилась скорость обработки медиаконтента HD-качества и 3D-графики.

Объем кэш-памяти CP6004-SA – 6 Мбайт, оперативной памяти DDR3 ECC SO-DIMM с частотой 1600 МГц – до 16 Гбайт. Поддерживается технология «горячей» замены и конфигурируемая шина PCI 64-bit/66 МГц или PCI-X.

Для адаптации к прикладным решениям CP6004-SA имеет большой набор интерфейсов: шесть слотов SATA с возможностью организации RAID-массивов 0/1/5, шесть портов USB 2.0, два порта RS-232, три независимых графических интерфейса (1 x VGA, 2 x DVI/HDMI), HDA. Для работы в высокопроизводительных телеком-приложениях служат пять портов Gigabit Ethernet, подключенных по шине PCI Express. Один SATA-порт (6 Гбит/с) предназначен для подключения устанавливаемого на модуль 2,5-дюймового SSD, HDD либо поставляемой под заказ флеш-памяти SATA объемом до 32 Гбайт для хранения операционной системы и приложений.

Модуль поддерживает интерфейс IPMI (Intelligent Platform Management Interface) и полностью подходит для использования в системах высокой готовности.

«РТСофт»: + 7 (495) 967-1505

Система ГЛОНАСС/GPS-мониторинга транспорта

Аппаратно-программный комплекс Omnicomm включает в себя три основные составляющие: бортовые регистраторы, датчики уровня топлива и ПО.

Регистраторы серии Omnicomm Profi предназначены для контроля транспорта, использующегося в самых тяжелых условиях. Возможности подключения датчиков уровня топлива и периферийных устройств к этим регистраторам сочетаются с повышенной защитой от климатических воздействий и попыток саботажа персоналом предприятия. Регистраторы серии Omnicomm Optim применяются в ситуациях, когда не требуется повышенная защита и специфическая функциональность. В модели сохранено большинство функций, необходимых для мониторинга, и обеспечивается высокая надежность работы на транспортных средствах любого возраста и состояния. Регистраторы Optim и Profi соответствуют требованиям к оборудованию ГЛОНАСС, изложенным в приказе Министерства транспорта РФ от 31.07.2012 № 285.

Программное обеспечение Omnicomm Autocheck 2.0 имеет расширенную функциональность по сравнению с предыдущими версиями – контроль геозон,

уведомления о событиях и нарушениях, доступное пользователю разграничение прав доступа. В новой версии ПО благодаря механизму предварительной обработки данных отчеты строятся быстро, вне зависимости от интервала времени и количества транспортных средств. Для ПО Autocheck 2.0 разработан новый интерфейс, который позволяет отображать произвольное количество картографических окон и отчетов.

Omnicomm: + 7 (495) 989-6220

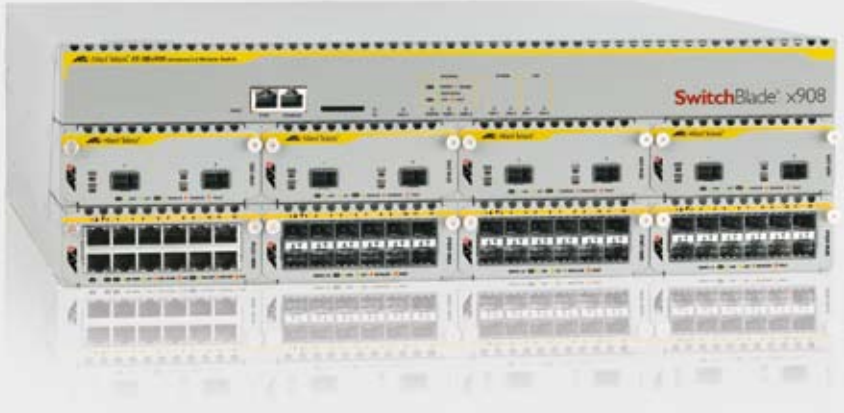
Мультипортовые гигабитные модули расширения

Модули XEM v2 предназначены для коммутаторов третьего уровня. Модель XEM-12Tv2 имеет 12 гигабитных портов с разъемами RJ-45, а XEM-12Sv2 – 12 гигабитных слотов под SFP.

Модули XEM v2 используют более современный набор микросхем, чем их предшественники, – такой, как на двухпортовых модулях 10G XEM-2X, позволяющих без замены самого шасси коммутатора SBx908 расширить его функциональность, не увеличивая стоимость. Эта возможность реализуется благодаря расширенному режиму (Extended Mode) обновленной версии ОС AlliedWare Plus, при включении которого становятся доступны:

- до 65536 MAC-адресов в таблице коммутации;
- до 128 групп агрегации портов LAG;
- до 4096 правил QoS или списков контроля доступа ACL;
- до 8196 адресов типа NextHop соседних маршрутизаторов.

Расширение списка контроля доступа (Access Control List) и увеличение количества классов QoS обеспечивают гибкость и безопасность работы сети, улучшая контроль сетевого трафика. Расширенный функционал технологии Link Aggregation, а также увеличенный размер аппаратных таблиц коммутации и маршрутизации позволяют применять SwitchBlade x908 в качестве коммутатора уровня 2 или 3 для ядра больших сетей.



В модулях XEM v2 отсутствует вентилятор охлаждения, что повышает их надежность в эксплуатации. Поддержка стандарта IEEE 802.3az (Energy Efficient Ethernet) дает возможность модулю XEM-12Tv2 экономить электроэнергию: он потребляет менее половины мощности своего предшественника.

Модули XEM-12Sv2 и XEM-12Tv2 совместимы с коммутаторами серии x900-12XT/S, x900-24X и SwitchBlade x908 под управлением ОС AlliedWare Plus начиная с версии 5.4.2–2.5.

Allied Telesis: +7 (495) 935-8585

ИКС

Блог, еще раз блог!

Антон **РАЗУМОВ**

Поисковые запросы как угроза безопасности

>>>> 6 ноября прошли самые цифровые президентские выборы за всю историю США. Перед днем голосования миллионы американцев заходили в Интернет, чтобы получить информацию о кандидатах и следить за избирательной кампанией. Однако предвыборный ажиотаж имеет и темную сторону: поисковые запросы по избирателям, кандидатам и кампаниям могут обернуться для обитателей сети кражей их персональных данных и проникновением на компьютеры вредоносного ПО.

Киберпреступники сегодня поставили себе на службу технологию, широко распространенную среди законопослушных компаний, – поисковую оптимизацию (SEO). Если цель злоумышленника – заставить пользователей перейти по определенному адресу в результатах поиска, здравый смысл подсказывает, что самым легким способом ее достижения является использование наиболее популярной новости дня. В ноябре это были президентские выборы в США.

В наши дни мошенники все больше используют в своих целях нишевые новости местного значения. Дело в том, что по менее популярным запросам выдается меньше результатов поиска с безопасных сайтов, а это увеличивает шансы перехода по вредоносной ссылке. Главными мишенями злоумышленников стали местные списки кандидатов, новости местной кампании или кандидаты, дополнительно внесенные в бюллетень.

...

Ни один надежно работающий метод поисковой оптимизации не теряет популярности. До сих пор не забыты такие традиционные методы привлечения посетителей, как оставление ссылок на форумах и в комментариях. Мошенники все так же пользуются страницами, оптимизированными под определенные поисковые запросы и предназначенными для побуждения к переходу на вредоносный сайт. Поисковые системы, например Google, стараются предотвратить действия злоумышленников, угрожая удалить сайты с такими страницами из результатов поиска. Однако ответственность за безопасность компьютера полностью лежит на пользователе.

Мой совет – относитесь настороженно к результатам поиска, URL-адреса которых вам кажутся странными или неуместными. Существуют компании, составляющие рейтинги безопасности URL-адресов. На вашем компьютере должны быть установлены как минимум антивирус и двусторонний межсетевой экран. Избежать интернет-угроз, в том числе во время выборов, можно, если всегда быть информированным и оставаться начеку.

комментировать

Рустэм **ХАЙРЕТДИНОВ**

Саботаж программистов

>>>> Одна из «закладочных» историй... Риэлторская компания переходит на электронный документооборот. Теперь агенты посылают на специальный адрес электронной почты сообщение определенной структуры: адрес, этаж, количество комнат, площадь и т.п. Специальная программа разбирает такие сообщения и раскладывает информацию по полям базы данных.

Приходит кризис осени 2008 г., продажи катастрофически падают, компания в авральном режиме сокращает персонал. «А что у нас делает вот этот программист? Поддерживает почтовый разборщик и ведет базу данных квартир? Что ее поддерживать, она уже полгода работает без сбоев». Увольнение проходит, как это рекомендуют делать инструкции по увольнению «айтишников»: программиста вызвали к высокому руководству, поблагодарили за службу, обещали поднять зарплату, объяснили, что он – самый важный сотрудник компании... После его ухода ему отключают доступ ко всему, уничтожаются все упоминания о его учетной записи в корпоративной информационной системе, охрана получает приказ не пускать его на территорию компании.

На следующее утро программист и еще дюжина сотрудников получают на проходной свои трудовые книжки и уходят восвояси. Вечером перестает работать база данных. При попытках восстановить ее обнаруживается, что базы нет и нет программы, которая ее обслуживала. Базу восстанавливают из источника резервного копирования, но самых актуальных данных в копии нет. К тому же агенты не готовы работать с базой через интерфейс командной строки, поэтому производительность оставшихся агентов падает.

При более глубоком расследовании оказалось, что в тот злополучный день на почтовый адрес, письма на который обрабатывал пресловутый «разборщик», пришло письмо, начинающееся со странной комбинации символов...

комментировать

Дмитрий **КУТЯВИН**

1 000 000 000 смартфонов

>>>> Количество используемых в мире смартфонов по итогам третьего квартала 2012 г. впервые превысило один миллиард. Об этом сообщает Bloomberg со ссылкой на исследование компании Strategy Analytics. Как отмечается в исследовании, только за последний год количество активных смартфонов увеличилось на 47% – с 706 млн до 1 млрд 38 млн устройств.

Интересно, а в России станут ли смартфоны так же популярны или мобильный телефон будет использоваться только для звонков?

комментировать

Блогеры-безопасники множатся. Инфобезопасность – та среда, которая растет и цветет на удобренной информационными угрозами почве. Риски предвыборного ажиотажа в США, безопасность в Силиконовой долине, саботаж хитроумных программистов, уязвимости в Skype... Значит, есть повод повысить свою ИБ-грамотность.

Михаил ЕМЕЛЬЯННИКОВ

Безопасность в Силиконовой долине

>>>> Страсть наших охранных служб, бюро пропусков и даже обычных рецепшн к фиксации паспортных данных при посещении вполне безобидных офисных центров раздражает давно и основательно. Обычной практикой, в Москве во всяком случае, становится сканирование, копирование паспорта даже несколько раз за время посещения – на входе в здание, на этаж, а потом и в офис конкретной компании. Зачем это делается, и что потом происходит с персональными данными, никто объяснить не может.

...

Итак, типовой вариант прохода в здание инновационной, передовой, современной компании в Силиконовой долине, где-нибудь в Купертино или Маунтин-Вью. Скрывать им, безусловно, есть что (пресловутые охраноспособные результаты интеллектуальной деятельности) – иначе бы они не стали знаменитыми «компаниями из Силиконовой долины». Но тем не менее...

Вас встречает представитель компании, который организует встречу или переговоры. Вместе с ним подходите к рецепшн и от руки вписываете свои ФИО и название компании в Соглашение о неразглашении (NDA), бланки которого тут же лежат стопочкой. Девушка за стойкой вас фотографирует, вносит в компьютер указанные вами имя и фамилию и печатает бейдж гостя. Все. Охранников на горизонте не видно. На недоуменный вопрос: «А что, с ID (паспортом) сверять данные не будут?» следует не менее недоуменный ответ: «Вас же сопровождает представитель компании, зачем еще нужен паспорт?».

Далее – передвижение по офису с сопровождающим и без видимых ограничений, хороший бесплатный обед с трудовым коллективом. Кстати, в обеденную зону, как правило, можно зайти, минуя рецепшн. Встречи, переговоры, покидание здания без каких-либо отметок на выходе и сдачи бейджа.

Людей в черном вокруг не видно. Никто не смотрит искоса, низко голову наклоня. Никто не интересуется документами. И что-то мне подсказывает, никто не страдает от несанкционированных действий посетителей, попыток кражи интеллектуальной собственности и нарушений пропускного режима.

А в целом работать в Долине, похоже, здорово. Чистый воздух, широкие зеленые улицы, огромные парковки у каждого здания. Раскованные хипстеры всех национальностей и цветов кожи. И все улыбаются. Они не думают о безопасности. Они думают о работе..

комментировать

Михаил ГОТАЛЬСКИЙ

Очередная уязвимость в Skype

>>>> дает злоумышленникам возможность получить доступ к учетной записи пользователей, зная только их e-mail. При этом количество уязвимостей в сервисе нам неизвестно, и нельзя ожидать гарантий, что они не всплывут завтра или послезавтра и что вы с ними не столкнетесь. Массовый пользователь всегда остается в группе риска, и уменьшить его он может только частой сменой логинов и паролей, а также сохраняя конфиденциальность e-mail адресов, используемых при регистрации.

Что касается госструктур, использующих Skype в работе (муниципальные власти, мэры городов), то для них единственным надежным выходом остается изоляция систем коммуникаций от Интернета....

комментировать

Александра КРЫЛОВА

Забота о качестве?

>>>> «В связи с массовым увольнением сотрудников ОПС работает по следующему графику...» – гласило объявление на двери почтового отделения на оживленной московской улице. В другом было написано, что ОПС «срочно требуются операторы почтовой связи – з/п от 16 тыс. рублей и почтальоны – з/п от 13 тыс. рублей».

А двумя неделями раньше мне довелось услышать выступление Елены Наумчик, руководителя департамента качества обслуживания ФГУП «Почта России». Она говорила о том, что руководство понимает, что плохое качество сервиса приводит к потере доходов, снижение доходов не позволяет повышать зарплату сотрудникам, что ведет к снижению их мотивации в качественном обслуживании клиентов. И рассказывала о шагах, сделанных за полтора года: о разработке процедур и правил клиентского обслуживания, об обучении и тестировании 100% (370 тыс.) операторов, о возложении ответственности за соблюдение этих стандартов на «второе лицо» в каждом филиале «Почты России»... Все эти нововведения отрабатываются сначала в экспериментальных почтовых отделениях.

Наверное, отделение почтовой связи, из которого в массовом порядке уволились почтальоны и операторы, просто не относится к числу экспериментальных.

комментировать

Реклама в номере

ИК ГУЛЛИВЕР
Тел/факс: (495) 663-2172
E-mail: info@ikgulliver.ru
www.ikgulliver.ru . . . с. 71

ПОЖТЕХНИКА
Тел.: (495) 687-6949
Факс: (495) 687-6943
E-mail: info@firepro.ru
www.firepro.ru . . с. 82–83

РТСОФТ
Тел.: (495) 967-1505
Факс: (495) 742-6829
E-mail: rtsoft@rtsoft.ru
www.rtsoft.ru . . . . . с. 23

EDGE-CORE NETWORKS
Тел.: (916) 625-8272
E-mail: russia@edge-core.com
www.edge-core.com . .с. 62–63

HP
Тел./факс: (495) 797-3900
www.hp.ru . . . . . с. 21

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

PANASONIC
Тел.: (495) 739-3443
E-mail: office@panasonic.ru
www.panasonic.ru . . . с. 11

RUSAT
Тел.: (495) 933-1614
Факс: (495) 933-1625
E-mail:sales@rusat.com
www.rusat.ru . . . 4-я обл.

SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.apc.com/ru . . . с. 73

SONY ELECTRONICS
Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu . . . с. 15

Указатель фирм

.masterhost 20
ABBYY 50
Accton 62
ACM 8
ACM-Консалтинг 15
ADM Partnership 68
Agilent Technologies 60
Allied Telesis 93
AltegroSky 16, 22
Altimo Coop 54
Altimo Holdings & Investments Limited 54
Amazon 16
Apple 23, 55
Argos Group Holding B.V. . 12, 54
ASHRAE 76
Autodesk 12
AVM 20
baza.net 27
Bertofan Investments Limited 54
Bloomberg 94
China Telecom 50
Cisco 12, 20
Citrix Systems 12
ComNet 87
C-Ring Iran 50
C-Ring Telecom 50
CSBI Group 17
DataDome 78
Delta Electronics 15
Deutsche Telekom 16
Directum 14
D-link 20
DrayTek 20
Edge-Core Networks 62
EMC 12
Emerson Network Power . 20, 76
ENOG 20
Eutelsat 16, 22, 40, 46
Facebook 23, 54
Forrester 16
GE/UTC 87
Google 23, 55, 94
Groupon 54
Hirschmann 87
HP 23
Huawei Technologies 23
IBM 16, 66
IBS Group 16, 54
IDC 16
IDS Scheer 10
IEEE Computer Society 8
iKS-Consulting 27
IMS Research 84
Intel 12, 92
Intelsat 46
InterZet 27
JetRadar 12
Kontron 92
KPMG 8
Lampertz 74
LanTech 87
Look at Media 26
M+W Germany 69
Mail.Ru Group 54
Marshall Capital 54
McKinsey & Company 6
Meraki Inc. 12
MetaSoftware 9
Metro Ethernet Forum 63
Microsoft 13, 64
MJA Association 24
Moxa 87
Mozilla Corporation 23
My-Apps 26
Neilson 24
Nokia 13
Nutritek Group 54
OCS 13
Omnicomm 93
Orange Business Services . . . 46, 47, 60
Panasonic 16
Panduit 89
PT Inovação 91
QIWI 16
Rackspace 16
RIPE NCC 20
RiT Technologies 89, 90
RSI 8
R-Style 8, 70
Samsung Electronics 23
SAP 23
Siemens Enterprise Communications 13
Siemon 90
Silver Tail Systems 12
Skylogic 22, 40
Software AG 10
SPIRIT 33
Staffware 10
Strategy Analytics 94
Swisscom 23
Synqera 16
TARP Worldwide 24
TE Connectivity 89
Technicolor 20
Tele2 15
TeleCore 72
Telekomunikacja Polska 50
Telenor 54
The 451 Group 74
TimeWeb 20
TNS 18, 26
TPV Technology 37
TrueConf 33
T-Systems 16
Uptime Institute 65
VimpelCom Ltd. 54
Visa 16
Yandex 54
Yota 16
YouScan 16
Youtube 23
Zynga 54
«Азертелеком» 50
АП КИТ 6, 42
«АРМО-Системы» 84
АРПАТ 37, 38
АРПП 42
«АС Байкал ТВ» 19
Ассоциация региональных операторов связи 60
«Афонтово» 19
АЦВИ 26
Банк России 55, 57
«Башнефть» 74
«Билайн» 24, 27
«Верофарм» 54
«Весть» 10
«Весть-МетаТехнология» . . . 10
«ВКонтакте» 54
ВТБ 54
ВЦИОМ 12
«ВымпелКом» . . . 14, 15, 23, 24, 27, 50, 51, 59, 61
«Газпром космические системы» 22
«Газпром» 22
ГК Optima 35
«ГЛОНАСС/ГНСС-Форум» . . 51
«Голден Телеком» 27
«Гринпис Россия» 26
Группа СТР 91
Гуманитарный институт телевидения и радиовещания . 8
«Енисей ТВ» 18
ИМЭПИ РАН 8
«Инжиниринговая компания Гулливер» 91
Институт системного программирования РАН 8
«Интерспутник» 14
«Инфосистемы Джет» 17
ИНЭУМ 9
ИТМ и ВТ 8
«Квантум» 27
«Клуб клиентов Почты России» 95
«Компания ТрансТелеКом» . . 12
Координационный центр национального домена сети Интернет 8
ФГУП «Космическая связь» . . 22, 33, 39, 40
«Лаборатория Касперского» . 50
«ЛГ Электроник Рус» 37
«Линкс» 43
«Линукс-инк» 34
«Логика бизнеса 2.0» . . . 9, 10
«Манго Телеком» 59
«Мастертел» 59
МГТС 12
МГУ 66
«МегаФон» 14, 25, 27, 49, 50, 51
«Медиа Альянс» 20
«МетаТехнология» 10
МИРБИС 8
МИЭМ 8, 9
МНИТИ 8, 36, 37, 38
НТЦ «Модуль» 37
МТС 12, 14, 25, 27, 50, 51, 53
МФТИ 8
«Навигатор» 27
НАТ 19
НИИР 33
«НИС ГЛОНАСС» 47
НИС 51
НСС 12
«Областное телевидение» 19
«Открытые Технологии» . . . 14
«Петер-Сервис» 91
«ПетерСтар» 27
«Пилот» 12
ГК «Пожтехника» 82, 83
«Почта России» 95
«ПроектСвязьТелеком» . . . 59
РАСПО 8, 42, 43, 44
РБК 54
РДТЕХ 34, 35
«РОСА» 8, 44
«Роскосмос» 66
«Роснано» 35
«Роснефть» 9
Российская академия народного хозяйства и государственной службы при Президенте РФ 8
«Российские космические системы» 33, 47, 48
«Ростелеком» . . . 12, 14, 15, 27, 50, 52, 53, 54, 69, 83
«РТКомм.РУ» 33, 51
РТРС 18, 38, 39
«РТСофт» 92
«Русагропром» 54
«РуСат» 8, 48, 49
РУССОФТ 42
«Самараэнерго» 14
«Самсунг Электроникс Рус» . . 37
«Связьинвест» 35
«Сетьтелеком» 22
«Синтерра» 27, 49, 50
«Синтерра-Медиа» 50
АФК «Система» 12, 54
«Ситроникс» 71, 72, 74
«Скат-7» 27
«Сколково» 16, 35
НП «Содействие развитию и использованию навигационных технологий» . . 51
«Стрим ТВ» 27
«Сумма Телеком» 51
ТВК 18
ТВКиК 12
«Техносерв» 52
ТКМ 89
«ТНТ-Телесеть» 18
«Триколор ТВ» 16
«ТТК-Самара» 12
«Уздунробита» 53
УК «Финам Менеджмент» . . 53
«Холдинг ТРЭКЕР» 17
«Хоум Кредит» 17
ЦАГИ 9
Центр верификации Linux 8, 44
«Электронная Москва» 71
«ЭР-Телеком» 15
«Яндекс» 51

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 204; тел.: (495) 981-2936, 981-2937.

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

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