Выпавший из обоймы

С началом деловой активности этого года отечественные биржевые индексы показывали стремительный рост на фоне повышения аппетита инвесторов к риску. Отраслевой сектор телекоммуникаций двигался дружно, но остался без должного внимания инвесторов, уступив по темпам роста таким секторам, как финансы, машиностроение и электроэнергетика.

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

В январе биржевые индексы на российских площадках быстро росли: снизившиеся опасения наступления рецессии в Европе и улучшение макроэкономических показателей в Китае и США вновь подняли привлекательность рисковых активов. Традиционная поддержка пришла с сырьевых рынков, где цены на нефть выросли на фоне обострения ситуации вокруг Ирана. Однако в феврале главным раздражителем для рынков вновь выступила Греция, а именно затянувшиеся переговоры греческого правительства с Еврокомиссией, МВФ и ЕЦБ об условиях предоставления второй программы помощи и списания долга.

«Ростелеком»: вершина не покорена

На хороших объемах, но при высокой волатильности проходили торги акциями «Ростелекома». На протяжении января бумаги оператора торговались в коридоре 150–155 руб., пытаясь закрепиться на последней максимальной отметке; тем не менее покорить данную вершину им не удалось, и в конце января котировки откатились к декабрьским уровням в 145 руб. за акцию. Однако вскоре общий позитивный настрой рынка и ряд корпоративных новостей помогли акциям компании оттолкнуться от уровня поддержки, в результате чего цена бумаг «Ростелекома» на 15 февраля остановилась на отметке 151,01 руб., потеряв 1,52%.

Среди корпоративных новостей в первую очередь стоит отметить сообщение о том, что Министерство связи и массовых коммуникаций РФ согласовало с Минэкономразвития и Росимуществом и внесло в правительство предложение второго этапа реорганизации государственного телекоммуникационного холдинга «Связьинвест». Предполагается, что предложенная схема позволит избежать предварительного выкупа «Связьинвестом» своего блокпакета у «Ростелекома». Образовавшиеся казначейские акции «Ростелекома» после присоединения будут погашены. Сделка стала возможной благодаря тому, что «Ростелеком» выкупил 3,86% своих акций, ранее принадлежавших Сулейману Керимову. В дальнейшем «Ростелеком» планирует использовать выкупленные акции для приобретения у «Связьинвеста» сотового оператора «Скайлинк» (1,91% акций), а затем акций нескольких региональных операторов связи. В результате пакет «Связьинвеста» в «Ростелекоме» вырастет до 45,7%. Ранее также сообщалось, что из этого пакета государство передаст 2% «Ростелекома» ВЭБу, уже владеющему приблизительно 2,3% обыкновенных акций оператора, в качестве компенсации за отмену права требовать у «Связьинвеста» выкупа своего пакета акций «Ростелекома».

Есть лицензия – есть рост

Бумагам сотового оператора МТС наконец-то удалось прервать затяжной декабрьский нисходящий тренд. Начиная с января акции компании начали восстанавливать позиции, уверенно оттолкнувшись вверх от нижнего уровня поддержки в 178 руб. Благодаря своим известным «защитным свойствам» акции ОАО «МТС» неоднократно возглавляли списки лидеров роста, обгоняя широкий рынок; в результате за рассматриваемый период они выросли в цене на 8,66%, до уровня 222 руб. за акцию. Поддержку котировкам оказал и ряд корпоративных новостей. Во-первых, компания превзошла конкурентов по росту числа абонентов: по данным на конец декабря 2011 г. консолидированное число абонентов МТС составило 105,78 млн, что на 508,1 тыс. больше показателя на 30 ноября 2011 г. Во-вторых, для роста акций появился новый фундаментальный фактор – оператор получил лицензию на предоставление услуг подвижной радиотелефонной связи в сетях LTE (Long Term Evolution) на территории Москвы и Московской области.

Вокруг ГЛОНАССа

Хорошим ростом отметились бумаги АФК «Система», прибавив по итогам рассматриваемого периода 8,06% – до уровня 26,879 руб. Компания продолжила наращивать пакет активов, подтвердив верность выбранной бизнес-стратегии. Так, она увеличила свою долю в уставном капитале ОАО «НИС» с 51 до 70% путем выкупа дополнительного выпуска акций компании. В качестве оплаты АФК «Си-

Справка ИКС

За период с 15 января по 15 февраля индекс ММВБ прибавил 8,48%, достигнув уровня 1579,38 пункта. Индекс РТС вырос на 15,4%, остановившись на отметке 1661,92 пункта. Капитализация отраслевого индекса «ММВБ телекоммуникации» увеличилась на 5,13% – до отметки 2291,17 пункта.

стема» внесла в уставный капитал «НИС» принадлежащий ей пакет в 51% долей в уставном капитале «М2М телематика». Таким образом, «НИС ГЛОНАСС», федеральный сетевой оператор в сфере навигационной деятельности, стал контролирующим участником «М2М телематики».

Акции медиахолдинга ОАО «РБК» выросли в цене на 7,73%, остановившись на отметке 15,466 руб. После продолжительного декабрьского падения бумаги компании в январе устремились вверх, следуя за общей позитивной динамикой рынка. Скорее всего, на котировках акций РБК сказались технические факторы – участники рынка обратили внимание на подешевевший, но весьма перспективный актив.

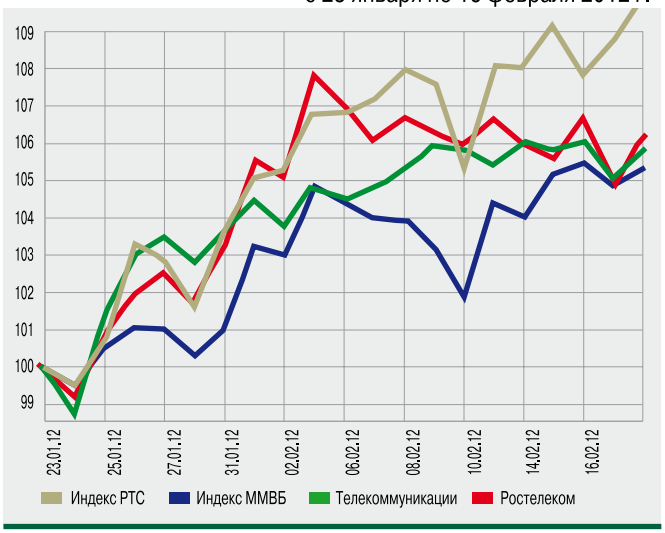
Хорошие новости «из-за бугра»

Порадовали участников рынка бумаги отечественных эмитентов, размещенные на зарубежных площадках. В частности, акции IBS Group выросли за рассматриваемый период на 17,8%, достигнув уровня $18,4.

Новость о планах IPO социальной сети Facebook подогрела интерес инвесторов к рынку интернет-индустрии. Благоприятным фоном успешно воспользовались акции российского интернет-поисковика Yandex N.V., которые за рассматриваемый период прибавили в цене 15,97%, достигнув $21,5. В бумагах же российского интернет-холдинга Mail.ru Group данная новость вызвала всплеск покупок, в результате акции компании выросли на рекордные 29,5%, до $34 за штуку (напомним, что Mail.ru Group владеет 2,38% акций этой соцсети).

Бумаги VimpelCom за рассматриваемый период выросли на 14,2%, достигнув отметки $11,98. Среди корпоративных новостей по компании стоит отметить сообщение о том, что единственный акционер ОАО «ВымпелКом», VimpelCom Ltd., одобрил реорганизацию российской компании в форме присоединения к ней нескольких «дочек». А компания Telenor увеличила голосующую долю в

Динамика биржевых индексов в период с 23 января по 16 февраля 2012 г.



VimpelCom до 36,36%, выкупив 234 млн привилегированных акций оператора у подконтрольной Нагибу Савирису Weather Investments II за $374,4 млн.

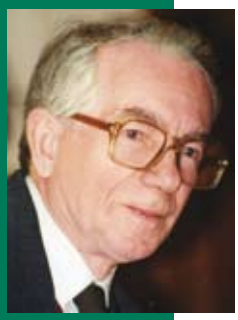
Лузер

Лишь акции компании «Ситроникс» за рассматриваемый период потеряли в стоимости, откатившись к отметке $0,53 (снижение на 11,67%). Инвесторов разочаровало сообщение агентства Fitch, подтвердившего долгосрочный рейтинг дефолта эмитента ОАО «Ситроникс» в иностранной и национальной валюте на уровне «B-» с «негативным» прогнозом. Fitch также подтвердило приоритетный необеспеченный рейтинг компании в иностранной и национальной валюте на уровне «B-», национальный долгосрочный рейтинг «BB-(rus)» с «негативным» прогнозом и национальный приоритетный необеспеченный рейтинг «BB-(rus)». ИКС

Всему свое место. DRM'у тоже

Всяк сверчок знай свой шесток.

Где, кому и зачем нужен DRM? Это наиболее неудобный вопрос, который выкристаллизовался в результате первого круга обсуждения условий применения цифровой модуляции для радиовещания до 30 МГц. В статье, которая завершает серию публикаций[1], посвященных внедрению DRM, предпринимается попытка рассмотреть проблему с разных сторон.



Юрий ЧЕРНОВ,
докт. техн. наук

Полвека назад была опробована идея сеять кукурузу повсеместно, особенно на севере. Результаты известны. Примерно то же самое мы видим сейчас в отношении DRM. Его пытаются насадить везде. И хорошо, если с наивной мыслью «а вдруг взойдет?». Так ведь на полном серьезе – «прикажу, и будет работать». Удивительно. Нельзя дразнить всесильную природу. Не пощадит.

Нельзя также отвлечься от мысли, что DRM – образование искусственное, как говорится, самой жизнью не вызванное. Хорошим парням захотелось чего-то эдакого, в частности сделать КВ-вещание в чем-то лучше. Но ведь Михайло Васильевич нам давно объяснил, что ежели в каком месте чего прибудет, то в другом обязательно столько же убудет. Чего прибудет – странники из других земель поговаривают разное и много чего диковинного... да и верно ли все это? А вот чего убудет, надо подумать – не прогадать бы.

И будет ли новое устройство, которое усиленно навязывают, лучше старого? С одной стороны, вроде немного лучше, а с других сторон? И почему за это «немного» надо платить так много? Ведь затраты и хлопоты огромные. Под грузом всех этих вопросов трудно принять решение. Но уж если вставать на путь внедрения DRM, то нужно разбираться по порядку. Начнем с длинных и средних волн.

На длинных и средних волнах

В предыдущих публикациях отмечалось, что DRM должен найти свои ниши, где он может с успехом заменить аналоговую систему. По-видимому, он может быть работоспособен в первую очередь там, где поведение радиотранспортной системы предсказуемо и не требуется одновременного охвата как можно большего числа слушателей. В силу своих пороговых свойств DRM на это не способен, это не его амплуа. Область, где этот стандарт может работать, имеет по крайней мере два измерения. Для него нужны подходящая геофизическая среда и социокультурная ниша, где он не был бы лишним и чужим в ряду собратьев по доставке информации (ведь он будет отбирать на себя часть аудитории).

Где будут слушать DRM?

В **больших городах** столько всего передается во все часы суток и с хорошим качеством, что чего-то еще не требуется. Причем из-за помех длинные и средние волны здесь слушают мало и редко. В этих условиях УКВ звучит лучше. Кого и зачем DRM будет заменять?

Если же рассматривать DRM как новую систему, то для ее работы с учетом пороговых свойств нужна очень высокая напряженность поля. По зарубежным данным[2], для столиц примерно 70–90 дБ. Помех в больших городах немерено. А прием необходимо обеспечить и во дворах-колодцах, и в квартирах с железобетонными стенами, в том числе и на первых этажах, и много еще где пожелает слушатель включить приемник с коротенькой штыревой антенной. Какие там биржевые таблицы и интерактивность! И без сложных расчетов можно уверен-

[1] Чернов Ю. Цифровое радио. Плюсы и минусы. «ИКС» № 1–2'2010, с. 55;
Чернов Ю. Где DRM'у жить хорошо. «ИКС» № 3'2010, с. 58;
Чернов Ю. Как внедрять DRM будем? «ИКС» № 3'2011, с. 67;
Чернов Ю. Ионосфера и DRM. Быть ли свадьбе? «ИКС» № 10'2011, с. 53, № 11'2011, с. 65.

[2] МСЭ-Р, Док. 6E/403, 2006 г., Мексика.

но сказать: гиблое это дело. Слишком уж большой мощностью передатчика придется заплатить за такой каприз.

Небольшие города. Жизнь спокойная и размеренная. Не бурлит. ТВ есть, радио есть. Дополнительная информация, возможно, части жителей будет интересна, но не жизненно необходима. Если найдутся лишние деньги, может быть, где-то и попробуют. И то, если будут приемники. А они откуда? – еще один вопрос.

Деревни и села, а также малозаселенные просторы. Я полагаю, хорошо известно, как живет далекое село. Премьер говорит, «там пять-восемь тысяч зарплата», дров не добьешься, а тут еще DRM. Да вы чё, издеваетесь? С этим все ясно. На много лет вперед.

К **оповещению о катастрофах** и других чрезвычайных событиях в любых населенных пунктах и на любых территориях путь DRM'у должен быть закрыт. Категорически. На нем должна быть табличка: «Осторожно, DRM! Опасно для жизни!». Это его отметина на всю жизнь. Как родимое пятно. Полагаться на него в экстремальных ситуациях действительно опасно для жизни, и не в переносном смысле, а в прямом. В самый нужный момент в самом нужном месте DRM может вдруг стать нем как рыба. Это же не аналог, который не с лучшим качеством, но и через завалы помех донесет до человека спасительное слово.

Ради чего ломаются копья

Во многих публикациях писатели-вещатели преподносят целые списки сказочных возможностей DRM. О том, как они реализуются, на основе натурного тестирования приводятся интересные детали, особенно в международных документах. При их рассмотрении видно, что почти все, что может DRM, может и аналог. Единственное, что дает именно DRM и чего ждут вещатели и радиослушатели, это **стабильность.** Действительно, уровень сигнала DRM и качество звучания на выходе приемника сегодня будут такими же, как вчера. И такими же будут завтра, в отличие от аналога, на который вдруг может напасть трескучка от соседней электропилы.

Но это при условии, что сигнал будет. И сегодня, и завтра, и потом. Каким для этого должен быть его уровень? Немало экспериментов, тестов и сопутствующих публикаций посвящено этой проблеме. Стабильность – есть или нет? От этого зависит, быть DRM'у или не быть.

Проверка на стабильность в частотных полосах ниже 30 МГц требует времени. Минимум год непрерывных измерений и прослушиваний (по крайней мере зима – лето). Известные опубликованные тесты – это дни, недели. Природные каналы непостоянны, и о стабильности на годовом отрезке по таким коротким периодам сказать ничего нельзя.

Где все-таки DRM'у будет жить хорошо?

Благоприятны условия для DRM, как уже отмечалось[1], **в странах с ровным климатом,** расположенных в широтном поясе Северной Африки, Индии, Юго-Восточной Азии. В этой зоне зиму от лета отличают специфические климатические явления, а отнюдь не смена тепла на мороз. Для стран с резкими перепадами температур перспектива неочевидна. В Рекомендациях МСЭ-Р содержатся сведения о влиянии климатических условий на работу систем радиовещания, в том числе и цифровых. В теплых регионах, упомянутых выше, минимальные значения параметров с небольшой гарантийной добавкой обеспечат длительные периоды работы без сбоев при минимальной потребляемой мощности. Поскольку прямых экспериментальных данных о долговременной стабильности работы DRM в каких-либо регионах к сегодняшнему дню нет, то можно опираться только на известные данные о поведении уровня сигнала на годовом интервале. Но это не дает стопроцентной уверенности для разных ситуаций, и конечно, не является достаточным основанием для планирования.

Важно, что в условиях умеренных помех, когда прием и в системе АМ, и в DRM идет, в DRM атмосферные разряды не будут вызывать непрерывных тресков, как то будет происходить в аналоговом вещании. Эта выигрышная сторона DRM проявится скорее всего в низких, **приэкваториаль-**

К оповещению о чрезвычайных ситуациях путь DRM'у должен быть категорически закрыт. На нем должна быть табличка: «Осторожно, DRM! Опасно для жизни!»

[1] Чернов Ю. Где DRM'у жить хорошо. «ИКС» № 3'2010, с. 58.

ных широтах, отличающихся активной грозовой деятельностью. Здесь, если интенсивность атмосферных разрядов не превысит некоторую норму, зона комфортного приема системы DRM может реально быть больше, чем у аналоговой, при той же или даже меньшей мощности передатчика. Это та возможная ниша, где геофизическая среда благоприятна. Однако результаты сравнительных наблюдений такого рода, если они и проводились, автору неизвестны.

Еще можно обратиться к Западной Европе, климат там подходящий.... Но уж очень много помех от других станций на всех частотах ниже 30 МГц.

В **средних широтах** на обширных пространствах с континентальным климатом и развитым лесным покровом о выгоде применения DRM сейчас уверенно говорить нельзя. Слишком велики будут необходимые мощности для компенсации увеличенных летних потерь (перепады до 15–20 дБ). И здесь возникают две проблемы.

1. При увеличении мощности будут увеличиваться и взаимные помехи. И если всюду поднимать мощность, то сохранятся те же взаимные претензии, но на более высоком витке. Это путь в тупик.

2. Насколько правильны предпосылки об уровне помех, относительно которых определяется минимальная необходимая напряженность поля? При подготовке к Региональной административной радиоконференции по длинным и средним волнам для Регионов 1 и 3 (Женева, 1975 г.) в качестве достаточной была принята величина напряженности поля 60 дБ на частоте 1 МГц при наличии только атмосферных и бытовых помех. В другом документе пояснялось, что отличное качество обеспечивается при отношении сигнал/шум 40 дБ, хорошее – при 30 дБ. Практически при уровне сигнала 60 дБ его качество в сельской местности средней полосы приближается к отличному. Понятно, что тогда уровень шума в полосе пропускания приемника близок к 60 – 40 = 20 дБ (мкВ/м). Может быть, несколько выше. Между тем карта атмосферных помех (исходные данные см. в рекомендации МСЭ-Р P.372-10. Радиошумы) чрезвычайно пестрая. Уровень шума зависит от частоты, времени суток, от сезона года и географического района. Для территории России карта, созданная в МСЭ-Р, не точно отражает реальность, так как во время формирования базы данных сведения о помехах нашего региона были весьма скудными. Но по этой карте можно сделать обобщенный вывод, что есть территории, где во все сезоны уровень помех значительно ниже среднего уровня, принятого МСЭ-Р для планирования. В таких районах применение DRM может быть оправданным.

Десятилетия назад обсуждался вопрос о слишком мощном излучении над СССР, фиксируемом со спутников. Надо радикально снижать общую излучаемую мощность. И думается, что там, где для работы цифры нужно будет увеличивать мощность, применять ее не следует. Экология и без того уже в критическом состоянии. Ситуация выглядит так:

Мы не можем ждать милостей от природы...
И.В. Мичурин

Она сама нуждается в милостях от нас.
Ю. А. Чернов

Все это подводит к мысли о том, что не только дешевле, но и с экологической точки зрения целесообразнее развивать DRM там, где мощности излучения для покрытия тех же зон потребуются меньшие, чем при аналоге. Желательно разработать несложную концепцию внедрения DRM, направленную на наиболее справедливое решение задач вещания, не обременяющее при этом экологию. Скорее всего, в средних широтах в регионах с большими лесными массивами организовать цифровое вещание будет проблематично. Возможно, в будущем, в малолесистых и стабильно теплых районах или на Крайнем Севере, где вечная мерзлота, а растительность в основном не выше карликовых берез, экспериментальные исследования покажут техническую целесообразность применения цифры. Нужна ли она будет для передачи информации в этих районах с их демографической и социальной спецификой, это другой вопрос.

На коротких волнах

О трудностях цифрового КВ-вещания подробно рассказано в предыдущей публикации[1]. Видимо, регулярная работа на КВ даже с аналоговой системой не может именоваться радиовещанием. Это звание ей присвоили на заре радиовещания, когда для передачи хоть чего-нибудь и как-нибудь за 2–5 тыс. км другого просто не было. Люди и этому были безмерно рады и с неподдельной гордостью называли то, что доносилось от КВ-приемников, не иначе как Его Величество Радиовещание. Прошло 90 лет. Цивилизация, в том числе техническая, шагнула так, что голова кружится. А КВ-«радиовещание» – почти столетие – в летаргическом сне. Все как во времена босоногих радиолюбителей. (Именно поэтому хорошим парням захотелось чего-то эдакого, из чего в итоге родился DRM. И не их вина, что среда обитания для DRM оказалась – я уверен, они этого не предполагали – недружественна к этому ненатуральному продукту). Но, вероятно, в память о былых заслугах, то, что передается на КВ, как престарелого почетного члена президиума на юбилейном собрании, продолжают величать радиовещанием. Приятно, но не по делу.

Где КВ-DRM может обосноваться? Сейчас для меня нет ответа. Везде его подстерегают опасности. Ему надо, например, чтобы не было больших помех от

[1] Чернов Ю. Ионосфера и DRM. Быть ли свадьбе? «ИКС» № 10'2011, с. 53, № 11'2011, с. 65.

других станций. Ни в рабочем канале, ни в соседних. Укрыться от них легче в наших северных районах. Но там постоянные возмущения в ионосфере, большие и малые магнитные бури, зимой также низкие частоты отражения, пурговые помехи, забивающие любой прием. Одним словом, из огня да в полымя. Перебивать все большой мощностью – это, очевидно, не выход. Наверное, нужно провести дополнительные изыскания подходящих мест для КВ-линий, где DRM'у было бы безопасно. Но нет гарантии, что и в такой тихой заводи, если она найдется, сегодня все будет как вчера, а завтра как сегодня. Ионосфера, подозреваю, – тайный член Ордена иезуитов, и верить ей по меньшей мере неосторожно. Нужны дальнейшие кропотливые исследования.

Рассуждения за вечерним чаем

Зачем бежим впереди паровоза? Опасно! Все еще только изучают, много неясного. Прогресс – он не мгновенен, период привыкания и адаптации в нашем деле длится годами, с оглядкой: а что у других? И если другие не кидаются в омут с головой, то, может быть, в этом есть резон, и нам надо бы погодить? Не следует думать, что все те, кто выступают за осторожный и обдуманный подход к внедрению новых систем, являются их противниками. Просто нельзя игнорировать классическое практическое соображение, что «всему свое место». Это место еще предстоит найти, и, возможно, поиск будет не так легок, как кажется. Мы еще не знаем, почем DRM нынче, а тем более почем он будет завтра. И разве не заслуживает внимания тот факт, что за 11 лет приглядываний ни одна страна не отказалась от аналогового радиовещания, заменив его цифрой, даже там, где природные условия вполне благоприятны?

Кстати, кто может быть слушателем DRM? По-видимому, прошло то время, когда в доме на видном месте стояли как часть мебели радиоприемные агрегаты типа СВД-9, СВД-М с автоматом для смены пластинок и более поздние отечественные разработки «Мир», «Ригонда» и др. с управляемой полосой пропускания, регулировкой тембра с тонкомпенсацией, а иногда и с шумоподавителем. Я и мои коллеги хорошо знакомы с такими приемниками, и кроме восхищения их работой и звучанием сказать больше нечего. Приемников с приличным, не «пластмассовым», звуком на прилавках увидеть не удается. Сейчас в массовом использовании акцент сместился ко всевозможного рода «мыльницам» разных размеров, легким в управлении, которые просто по законам физики могут только предоставить смысл текстовой передачи или показать содержание музыкальной программы. Именно показать, потому что звучание таких устройств в пластмассовом корпусе с динамичком диаметром 5–10 см без низких частот музыкальным не назовешь. В сравнении с упомянутыми выше приемниками их качество не выше «неуда». При использовании таких «мыльниц» главная забота – не качество звука, а не пропал бы сигнал. А ведь приманкой-то было качество не хуже CD-проигрывателя. Даже современные габаритные комбайны с дисками и радио в «химическом» корпусе в подавляющем большинстве обладают неприятным звучанием. У малогабаритных устройств звук будет ущербным при любой системе вещания, потому что возможности пластмассового корпуса с миниговорителями одинаковы при любом носителе программы, будь то аналог или цифра. О каких CD или ОВЧ-ЧМ с колонками может идти речь – «их тут рядом не стояло»! А ведь обладателей «мыльниц» – легион! Здесь, уважаемые коллеги, есть о чем подумать.

■ ■ ■

За 11 лет своей жизни DRM породил множество проблем. И пока не оправдал ни одной надежды. Поэтому ответ на вопрос о «шестке» для DRM (в первую очередь на ДСВ), на мой взгляд, звучит так: «шесток» там, где в годовом обозрении с DRM лучше, чем с другими системами, можно организовать высококачественное вещание и без уменьшения охвата аудитории обойтись меньшими мощностями. На таких условиях не каждая страна сможет претендовать быть приютом для DRM.

P.S. Все вышеизложенное – одно из многих возможных мнений. Мне известны и другие точки зрения. Очень по делу высказался один из моих коллег: «А не очередной ли это кусочек сыра?». Мир знает много подобных примеров. Может, не спешить, чтоб людей не насмешить?

Здесь тоже есть о чем подумать. ИКС

Закон «О персональных данных»: поправки приняты, концепция не изменилась

Новая редакция закона «О персональных данных» не только не уменьшила государственное администрирование в этой сфере, но и усилила его. По-прежнему требуется приведение закона в соответствие с духом европейского регулирования, с ФЗ «Об информации, информационных технологиях и защите информации», с Конституцией РФ.

Василий ЛЕВЧИК, руководитель рабочей группы по нормативным правовым вопросам Ассоциации региональных операторов связи

Европейское регулирование в сфере защиты персональных данных

Принятый после ратификации Россией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, Федеральный закон «О персональных данных» продолжает вызывать споры экспертов и участников рынка. Еще не получив опыта правоприменения, он уже был скорректирован в наиболее одиозных своих нормах. Однако представляется, что причина «неприменимости» закона кроется в самой его концепции, предусматривающей тотальное и неоправданно детальное государственное администрирование в данной сфере.

Базовая конвенция и последующие евродирективы обязывают стран-участниц обеспечить защиту персональных данных путем соблюдения следующих понятных и справедливых требований:

- Информация собирается и обрабатывается только для объявленных, явных и законных целей законными и добросовестными методами, с согласия ее субъектов (кроме особых, явно оговоренных случаев).
- Собирается только относящаяся к делу информация, необходимая для объявленной цели, и хранится она в форме, позволяющей идентифицировать ее субъектов, не дольше, чем это необходимо.
- Собранная информация корректно обрабатывается, при необходимости уточняется и актуализируется.
- Принимаются меры против несанкционированного раскрытия или злоупотребления информацией. Данные, оборудование и программное обеспечение предохраняются от физического повреждения.

При этом регуляторные меры страны-участницы выбирают самостоятельно. От них не требуется, например, администрировать деятельность операторов персональных данных. Предполагается, что лица, связанные с персональными данными, подчиняясь национальному регулированию, самостоятельно и добросовестно примут необходимые меры и применят соответствующие процедуры и технические средства.

Тем самым европейское регулирование не накладывает на государство обязанность вводить детальное регламентирование такой деятельности, нести ответственность за его необходимость и достаточность, а также контролировать следование ему.

Основная задача европейского регулирования – защита граждан от возможных злоупотреблений со стороны государства, особенно в случаях, когда они вынуждены предоставлять свои персональные данные в рамках установленных административных процедур. В таких случаях граждане, давая свое согласие на обработку персональных данных, действуют безальтернативно, поэтому представляется обоснованным, чтобы требования к защите персональных данных устанавливались прежде всего для государственных и иных организаций, оказывающих населению госуслуги.

Но когда потребитель вступает в отношения с коммерческими предприятиями, действующими в условиях рынка, он самостоятельно делает выбор и принимает решение о достаточности или недостаточности предлагаемой ими защиты его персональных данных. Следовательно, здесь полная регламентация действий оператора персональных данных по их защите излишня (и, как показывает анализ, она все равно не охватывает всего разнообразия двусторонних

Табл. 1. Сравнение требований к защите персональных данных в ФЗ «О персональных данных» предыдущей и действующей редакций

ФЗ «О персональных данных» от 27.07.06 № 152-ФЗ (предыдущая редакция), ст. 19	ФЗ «О персональных данных» от 25.07.11 № 261-ФЗ (действующая редакция), ст. 19
2. Правительство Российской Федерации устанавливает **требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных…**	**3.** Правительство Российской Федерации… устанавливает: 1) **уровни защищенности персональных данных** при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных; 2) **требования к защите персональных данных при их обработке в информационных системах персональных данных,** исполнение которых обеспечивает установленные уровни защищенности персональных данных; … **4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации** в соответствии с частью 3 настоящей статьи **требований к защите персональных данных для каждого из уровней защищенности**, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных **устанавливаются федеральным органом исполнительной власти**, уполномоченным в области обеспечения безопасности… **5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности,** органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых **определяют угрозы безопасности персональных данных…**

и многосторонних отношений, включая агентирование). В таких случаях целесообразнее регулировать права и ответственность сторон*.

Избыточность администрирования в ФЗ «О персональных данных»

Отечественный закон выстроен по схеме Директивы 95/46/ЕС Европарламента/Евросовета от 24.10.95 «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», однако в отличие и от нее, и от базовой конвенции вводит в своей ст. 19 детальную регламентацию в этой сфере, поручая правительству установить требования к защите персональных данных, определить состав и порядок организационных и технических мер такой защиты, причем во всех информационных системах, а не только в государственных. Этот подход принципиально расходится со ст. 16 рамочного закона «Об информации, информационных технологиях и защите информации», согласно ч. 5 которой подобные требования предъявляются только к государственным информационным системам.

Эксперты и участники рынка постоянно обращали внимание всех субъектов законодательного процесса на избыточность установленного в ст. 19 ФЗ «О персональных данных» администрирования, тем не менее в новой редакции закона оно было существенно расширено (табл. 1).

Помимо установленных законом вполне понятных в духе европейского регулирования обязательств по обеспечению безопасности персональных данных (ст. 19 ч. 1 обеих редакций), оператор теперь не волен выбирать состав принимаемых им для этого мер, а должен следовать указаниям ст. 18.1 ч. 1 и ст. 19 ч. 2 (там обращает на себя внимание обязательное применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации), а также будущих подзаконных нормативных правовых актов. Свободен же он только в том, что не регламентировано: «Оператор **самостоятельно определяет** состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, **если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами…**» (ст. 18.1 ч. 1).

В качестве своеобразной компенсации за тотальную регламентацию новая редакция закона устанавливает контроль и надзор за выполнением мер по обеспечению безопасности персональных данных только для их обработки в государственных информационных системах (ст. 19 ч. 8), а возможность введения контроля и надзора за деятельностью остальных операторов персональных данных отнесена в ч. 9 на усмотрение правительства (табл. 2).

При этом очевидно, что отсутствие контроля и надзора никоим образом не снимает обязательств по соблюдению установленных требований и выполнению предписанных мер, равно как и не освобождает от ответственности за нарушения в этой сфере.

Для приведения закона «О персональных данных» в соответствие с базовым ФЗ «Об информации, информационных технологиях и защите информации» следует скорректировать его ст. 18.1 и 19, установив, что деятельность по защите персональных данных регламентируется только для операторов государственных информационных систем, а остальным достаточно вы-

*Можно, например, предложить гипотетический закон «О безопасности жизни», поручающий правительству утвердить «Требования к поведению на территории Российской Федерации» (или, допустим, «Нормы безопасного проживания»), следуя которым граждане уменьшали бы для себя возможные риски и угрозы. Однако в реальности подобное регламентирование применяется лишь в наиболее опасных случаях, а весь остальной спектр отношений регулируется путем установления ответственности за те или иные антиобщественные деяния и поступки в УК и КоАП РФ.

Табл.2. Сравнение требований по контролю и надзору в сфере персональных данных в ФЗ «О персональных данных» предыдущей и действующей редакций

ФЗ «О персональных данных» от 27.07.06 № 152-ФЗ (предыдущая редакция)	ФЗ «О персональных данных» от 25.07.11 № 261-ФЗ (действующая редакция)
ст. 19 **3. Контроль и надзор** за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации...	**ст. 18.1** **4. Оператор обязан** представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом **подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.** **ст. 19** **8. Контроль и надзор** за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, п**ри обработке персональных данных в государственных информационных системах** персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации... **9.** Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, **решением Правительства Российской Федерации** с учетом значимости и содержания обрабатываемых персональных данных **могут быть наделены полномочиями по контролю** за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и **не являющихся государственными информационными системами** персональных данных...

полнять требования ст. 16 ч. 4 ФЗ «Об информации, информационных технологиях и о защите информации».

Неконституционность вводимой законом регламентации

Вся рассмотренная регламентация представляется необоснованной, поскольку в ее введении нет необходимости, предусмотренной ст. 55 ч. 3 Конституции РФ. Ниоткуда не следует, что права субъектов персональных данных нельзя обеспечить иначе как тотальной регламентацией мероприятий по их защите. Наглядная иллюстрация безрезультатности и бессмысленности такой регламентации, а также контрольно-надзорной деятельности в этой сфере – широкое предложение на черном рынке сведений из баз данных именно государственных органов и организаций, содержащих как персональные данные, так и коммерческую тайну.

Очевидно, что могущественные государственные структуры, включая силовые, с технической точки зрения вполне надежно защищают свои информационные системы от проникновения извне. Также очевидно, что продаваемая из них весьма объемная и вполне актуальная информация добыта отнюдь не в результате взлома этой защиты. И ситуация, конечно, не исправится от того, что принятые технические и организационные меры будут утверждены постановлениями правительства или приказами уполномоченных ведомств.

Таким образом, вводимые законом требования отнюдь не необходимы для целей ст. 55 ч. 3 Основного закона. Требуется лишь элементарное соблюдение уже существующих законов, исполнение всеми ведомствами, прежде всего правоохранительными, своих функций.

Некорректность формулировок закона

Некоторые прямые нормы Федерального закона допускают различное толкование, другие приводят к неожиданным следствиям, которых законодатели, наверняка, не имели в виду.

1. Понятие «оператор персональных данных» (ст. 3 ч. 2) формально распространяется на огромное количество лиц: на сотни тысяч российских школ, детских садов, работодателей, включая государственные организации. При этом в определении «оператор – ... юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных...» фрагмент фразы после «а также» можно толковать двояко:

– либо включая в круг операторов и лиц, которые обрабатывают персональные данные, и лиц, определяющих цели и содержание такой обработки (т.е. расширяя круг операторов);

– либо относя к числу операторов лиц, которые не только заняты непосредственно обработкой, но при этом еще и сами определяют ее цель и содержание (т.е. сужая учитываемую область).

Первое толкование представляется менее вероятным, поскольку тогда операторами персональных данных будут являться миллионы наемных работников, выполняющих такие действия по заданию своих работодателей. Очевидно, однако, что нормы закона не должны допускать такое противоположное толкование.

2. Введенное в ст. 11 ч. 1 уточнение, согласно которому биометрические персональные данные считаются теперь таковыми, если «используются оператором для установления личности их субъекта», легализовало хотя бы обработку обезличенных (толпа или случайные лица в кадре) фото-, кино- или видеоизображений – при прежнем определении возникала коллизия со ст. 152.1 ГК РФ. Однако остается формальное требование получения именно письменного разрешения на опубликование фотографий или распространение ТВ-сюжетов с участием называемых при этом лиц. Ведь, действительно, без «установления личности» изображение не может быть снабжено верной подписью или комментарием. Особенно удивительно это по отношению к публичным, широко известным лицам. И даже если однажды такое лицо дало согласие на публикацию (и соответствующий выпуск СМИ, согласно ст. 8 закона, получил статус «общедоступного источника»), то каждый следующий раз на распространение нового изображения или видеоряда требуется новое же разрешение.

3. Если при распространении персональных данных используются «средства автоматизации, и в том числе информационно-телекоммуникационные сети», то «рядовые» граждане, не являющиеся журналистами, учеными или творческими работниками, не имеют права сообщать (например, публиковать в Интернете) никакие сведения о других лицах без их согласия (ст. 6 ч. 6). Более того, давая интервью для СМИ перед телекамерой или просто в микрофон (а изображение и звук сейчас обрабатываются на компьютерах), каждый, кто сообщает какие-либо сведения о третьем лице, может быть обвинен в использовании средств автоматизации, пусть даже принадлежащих не ему, а СМИ, – закон не придает этому обстоятельству значения. При этом речь идет не о клевете, а просто о любых фактах, возможно, известных многим. Во всех таких случаях распространитель сведений должен быть готов доказывать, что делал это «исключительно для личных и семейных нужд» (ст. 1 ч. 2 п. 1) либо, наоборот, «для достижения общественно значимых целей» (ст. 6 ч. 1 п. 7) – и эти две крайности сами по себе уже выглядят парадоксально.

Законодатели, конечно, имели в виду защиту личной и семейной тайны, информации о частной жизни (ст. 23 ч. 1 и ст. 24 ч. 1 Конституции РФ), однако поскольку понятие «персональные данные» гораздо шире, то получилось зримое несоответствие свободе слова и свободе оборота информации (ст. 29 ч. 1 и 4 Конституции РФ). С другой стороны, оговорка «для личных и семейных нужд» в ст. 24 ч. 1 Конституции РФ не предусмотрена.

О соотношении понятий «персональные данные» и «личная и семейная тайна», «информация о частной жизни» – читайте в следующем номере «ИКС».

Ниоткуда не следует, что права субъектов персональных данных нельзя обеспечить иначе как тотальной регламентацией мероприятий по их защите

Безопасность и фрод-контроль в сетях NGN/IMS

Окончание. Начало см. «ИКС» № 1–2, с. 64.

Илья ЕХРИЕЛЬ, технический директор «НТЦ СевенТест», канд. техн. наук
Эдуард БАЖЕНОВ, начальник отдела разработки решений OSS/BSS, «НТЦ СевенТест»
Владислав КОЛЕСНИК, заместитель начальника отдела разработки решений OSS/BSS, «НТЦ СевенТест»

Применение протоколов IP и SIP, а также разнообразие механизмов доступа делает сети NGN/IMS уязвимыми для DoS-атак и фрода. Для противодействия этим угрозам безопасности необходимы комплексные системы с функциями кросс-анализа всех используемых протоколов и подсистем.

Примеры реализации DoS-атак в IMS

Защита от DoS/DDoS-атак – одно из требований к системе безопасности, отсутствующих в стандартах IMS. Хотя в IMS существует механизм аутентификации абонентов с помощью IPsec и SIP Digest, а также авторизация доступа абонентов к услугам через HSS, но и легитимные абоненты имеют возможность генерировать атаки на инфраструктуру IMS. Причем эти атаки могут опираться на сообщения протокола SIP, на сообщения протокола RTP или обоих сразу.

В сравнении с интернет-атаками анонимных абонентов вероятность атак на инфраструктуру IMS несколько меньше, поскольку абоненты имеют договорные отношения с поставщиком услуг и системе известны. Однако с точки зрения потери доходов оператора, оттока абонентов и даже угрозы человеческой жизни (если затронуты услуги экстренных служб) последствия успешных атак могут быть даже более тяжелыми.

Одна из услуг IMS – определение статуса присутствия (многими сейчас рассматривается как база для создания массы коммерчески интересных услуг) – позволяет информировать подписчика о том, находятся ли другие пользователи в онлайне, а также о доступных в данный момент возможностях для связи с ними. Когда пользователь заказывает такую услугу относительно интересующих его абонентов, производится обмен транзакциями SUBSCRIBE и NOTIFY с серверами услуги присутствия, которые управляют информацией о статусе каждого из абонентов.

Для уменьшения количества транзакций в процессе заказа используется специальная функция, но вместо нее злоумышленник может взять длинный список легального абонента и вызвать посылку сотен сообщений к серверу услуги присутствия. Задействуя одновременно длинные списки большой группы абонентов, можно организовать на сервер присутствия DDoS-атаку.

В IMS маршрутизация и тарификация многих услуг (присутствия, VoIP, push-to-talk) осуществляется через CSCF. В результате нарушение работы сервера присутствия по причине DDoS-атаки может вызвать задержку обработки трафика других услуг. Ведь если ответ от сервера присутствия не получен в течение определенного спецификацией протокола SIP таймера (32 с), то каждый SIP-запрос к серверу может быть повторен до 10 раз. Повторные запросы вместе с трафиком самой DDoS-атаки создадут дополнительную нагрузку на CSCF.

Повышенная нагрузка на CSCF ведет к тому, что не попавшие под атаку серверы других услуг не получают вовремя ответы от этого узла и также могут сгенерировать по 10 повторных запросов к нему в следующие 32 с, что вызовет полную перегрузку CSCF и отказ предоставления всех услуг.

Учитывая, что серверы услуг никогда не имеют десяти- или даже пятикратного запаса процессорной мощности, необходимой для выполнения логики услуг, видим, что для организации DDoS-атаки, которая способна нарушить работу IMS-сети, обслуживающей миллионы абонентов, злоумышленнику необходимо получить доступ всего к нескольким клиентским аккаунтам.

Примеры реализации фрода в IMS

Как уже отмечалось, уязвимости безопасности, затрудняющие обнаружение фрода в сетях NGN/IMS, порождаются двумя особенностями этих сетей, а именно: применением протоколов IP и SIP, а также разнообразием механизмов доступа. Как и в сетях ОКС7, в основанных на SIP сетях IMS маршруты передачи сигнальной и пользовательской информации разделены. Это также повышает вероятность нелегитимного пользования услугами.

Осуществлению многих видов фрода, например кражам и нелегитимному использованию IP-адресов, способствует открытость IP-сетей. Их децентрализованная архитектура предполагает наличие интеллектуальных пользовательских терминалов, способных напрямую контактировать с другими сетевыми элементами, что значительно увеличивает риск нелегитимного использования сетевых ресурсов.

Если терминалы пользователей подключены одновременно к сети IMS и публичному Интернету, то поль-

зователи получают возможность взаимодействовать непосредственно (peer-to-peer) с помощью прямой адресации, что может противоречить тарифной политике оператора сети IMS.

А вполне легитимная технология использования SIP-прокси-сервера в качестве учрежденческой АТС может применяться и для международного фрода путем разделения одного аккаунта между несколькими пользователями. В этом случае задействуется стандартная SIP-процедура переадресации, а группа пользователей работает с одним счетом, связанным с данным аккаунтом, что требует от оператора сети IMS, у которого зарегистрирован такой сервер, дополнительных мер контроля.

Предоставление услуг, основанных на IP-протоколе, зачастую связано с бизнес-моделью, отличной от модели ТфОП. В новой модели кроме потребителя и оператора сети участвуют и поставщик услуг, и поставщик контента, и оператор системы мобильных платежей. Любой их них может явиться целью фродстерской атаки, следовательно, для фрод-контроля необходимо собирать и сопоставлять данные от разных компаний, что намного его усложняет.

Фрод-сценарии зависят от услуг и технологий. С развитием NGN/IMS фрод продолжит эволюционировать, особенно с переходом от безлимитной «битовой трубы» к тарификации услуг на основе потребленного трафика и вида контента. Так, скорее всего, целью фродстеров станет не просто установление соединения, а скачивание дорогостоящего контента. Вместе с тем нельзя надеяться, что в эпоху NGN/IMS исчезнут традиционные, давно известные виды фрода.

Благодаря конвергентной природе сетей NGN/IMS угрозы различных видов (финансовые, исходящие из природы сети Интернет, от хакеров, от фродстеров) будут смешиваться/взаимно дополнять друг друга. Поэтому ранее самостоятельные подразделения противодействия фроду, управления рисками предприятия, гарантирования доходов и сетевой безопасности должны будут объединить свои усилия в борьбе с фродом.

Методы и системы противодействия DDoS-атакам и фроду в сетях NGN/IMS

Поскольку успешная DDoS-атака может привести к полной перегрузке серверов CSCF, механизм защиты целесообразно реализовывать в специализированном устройстве.

Идеально, если защита против подобных атак организована для каждого сетевого элемента IMS. Однако, учитывая требования к аппаратным компонентам, стоимость такого подхода может быть очень высока. Очевидный выход – акцентировать внимание на защите пограничных элементов IMS, таких как P-CSCF и A-BGF (Access Border Gateway Function), размещаемых на границе сети доступа между абонентскими терминалами и ядром сети, а также I-BCF и I-BGF (Interconnect Border gateway), находящихся на границе ядра сети с сетями других поставщиков услуг. Обычно функции системы обнаружения и предотвращения вторжений (IDPS) возлагаются на пограничный контроллер SBC (Session Border Controller), который формально не является частью инфраструктуры IMS.

Система IDPS предназначена для оперативного обнаружения начала DDoS-атаки и блокирования ее источника без прерывания предоставления услуг другим абонентам. Это требует оснащения SBC функциями мониторинга скорости сигнального потока, контроля форматов сообщений в комплексе с возможностью динамического создания «черного списка» IP-адресов источников атак.

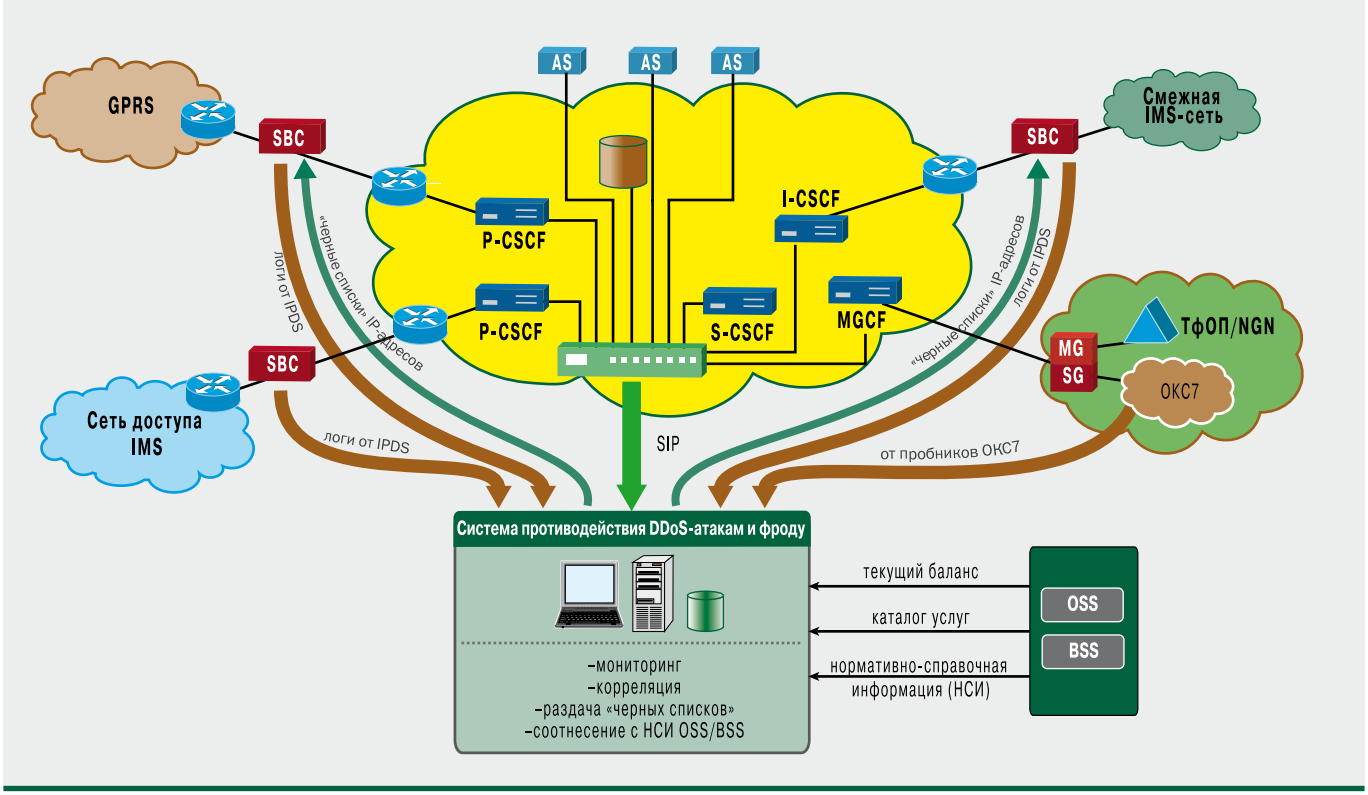
Одна из мер безопасности в IP-сетях – углубленная проверка пакетов (DPI), под которой подразумевается мониторинг и контроль пакетов на уровнях с второго по седьмой модели ISO/OSI.

Инспекция на нижних уровнях – с второго по четвертый – охватывает некоторые виды распознавания атак по типу DDoS, но не приводит к выявлению фрода.

Исследование уровней с четвертого по седьмой обычно входит в понятие «обработка контента». Именно здесь обнаруживаются многие виды угроз IMS: новейшие методы DDoS-атак с применением вредоносного ПО, спам, фишинг и нежелательный контент. Мониторинг и контроль однорангового трафика данных, в частности BitTorrent и LimeWire, также производится на этом уровне.

Системы анализа и противодействия фроду нужно оценивать не только по их способности локально анализировать характеристики сетевого трафика и противодействовать отдельным видам угроз, но и по способности сопоставлять множество факторов, влияю-

Пример организации системы противодействия атакам и фроду для IMS-сетей



щих на все аспекты безопасности процесса предоставления услуг.

В деле обеспечения безопасности мультисервисных услуг важен комплексный анализ угроз на всех участках технического обеспечения услуги. Это подразумевает выявление угроз не только на одном участке сети или для одного семейства протоколов, но и для их совокупности (SIP, ISUP, INAP, Sigtran, H.323/Megaco), поскольку в этом случае эффективность противодействия фроду значительно повышается.

Непосредственному осуществлению практически любого вида фрода предшествует DoS-атака, направленная на отказ одной из функций реализации логики услуги. Поэтому для результативной борьбы с фродом необходим совместный анализ логов от локальных систем IPDS, записей о сессиях IPDR, а также об объемах и структуре потребляемого трафика от пробов системы мониторинга.

Применение для борьбы с фродом только систем IPDS, даже оснащенных функциями DPI, не приводит к необходимому результату, поскольку они ориентированы на анализ сетевого трафика на локальном участке сети и вне контекста обеспечиваемой услуги. Контроллеры SBC не дают информации о характеристиках трафика клиента, который может косвенно влиять на IMS-услуги, и защищают на уровне протокола доставки сообщений, но не на уровне протокола, осуществляющего поддержку услуги.

С другой стороны, внедрение систем с функциями кросс-анализа и корреляции всех протоколов и подсистем, используемых для обеспечения услуги, сокращает время, необходимое для идентификации конкретного вида фрода и активации мер противодействия ему.

Система, способная обеспечить безопасность сети NGN/IMS, должна также выполнять контроль, распознавание и проверку контента на основе сигнатур с открытым набором правил. Сигнатуры позволяют классифицировать IP-трафик с помощью адресов IPv4 и IPv6, типов приложений, классов QoS и определяемых пользователем сигнатур приложений.

Кроме того, комплекс должен обладать программируемостью и дружественным интерфейсом пользователя для оперативной модификации и настройки встроенных средств исследования сложных текстовых протоколов, выявления вирусов и обнаружения вредоносных программ в полезной нагрузке.

■ ■ ■

Множество видов доступа, открытая распределенная архитектура, потенциальная одновременность DDoS-атак и фрода, широкая номенклатура новых услуг выдвигают ряд требований к системам противодействия атакам и фроду для IMS-сетей.

Некоторые уязвимости сетей IMS могут быть нивелированы на этапе проектирования сети, однако для достижения наилучшего результата безопасность должна быть обеспечена на всех уровнях архитектуры IMS специализированными системами. Основные требования к этим системам таковы: централизация контроля и сбор логов от локальных систем, возможность сопоставления информации о разных типах данных и протоколах, контроль контента, наличие встроенных шаблонов и гибкость настройки фрод-критериев. ИКС

Интегрируем оптимальную маршрутизацию трафика и взаиморасчеты

Все больший интерес сегодня вызывают ИТ-решения, позволяющие оператору связи эффективнее использовать ресурсы сети с точки зрения рентабельности. Один из подходов предполагает, что система поиска оптимальных маршрутов трафика работает совместно с системой взаиморасчетов оператора с его партнерами.

Леонид КАН,
начальник группы «Интерконнект», компания «Петер-Сервис»

Оператор должен обеспечить клиенту указанный в договоре уровень качества обслуживания, затратив при этом минимум собственных средств. Существует класс систем, с помощью которых он может соответствующим образом сконфигурировать свою сеть, – это так называемые системы маршрутизации по критерию наименьшей стоимости (Least Cost Routing, LCR).

Критерием оптимальности при расчете маршрутов служит требование обеспечить заданное качество обслуживания при минимальной стоимости. Тарифы, предоставляемые партнерами, могут существенно различаться по цене. Очевидно, что при прохождении большого объема трафика внедрение системы оптимальной маршрутизации должно привести к значительному экономическому эффекту.

По итогам оптимальной маршрутизации трафика соответствующим образом должны измениться и взаиморасчеты между операторами. Как учесть в расчетах результаты оптимизации, выстроить взаимодействие между системой взаиморасчетов и системой LCR? Такую работу мы провели после создания в компании «Петер Сервис» собственной системы LCR.

Задачи оптимальной маршрутизации

Трафик, проходящий через сеть оператора связи – эксплуатирующей организации (ЭО) в общем случае может поступать как от клиентов (потребителей услуги), так и от других операторов связи. В упрощенной схеме на рис. 1 сеть ЭО представлена четырьмя внутренними коммутаторами и четырьмя коммутаторами-шлюзами. Трафик к поставщикам услуг может проходить по разным маршрутам (возможные его пути изображены линиями и стрелками). Поставщиками услуг выступают другие операторы связи – партнеры ЭО.

Каждый поставщик услуги при передаче трафика устанавливает индивидуальные тарифы на различные направления (диапазоны номерной емкости) вызовов. Договор с поставщиком может оговаривать качество предоставляемых услуг, зависимость стоимости трафика от его объема, от времени суток и т.п. Перед ЭО стоит задача сконфигурировать свою сеть так, чтобы оказывать услугу клиентам с заданным качеством и с минимальными собственными затратами.

Под конфигурированием сети понимают создание таблиц маршрутизации для коммутационного оборудования.

Рис. 1. Прохождение вызовов через сеть ЭО

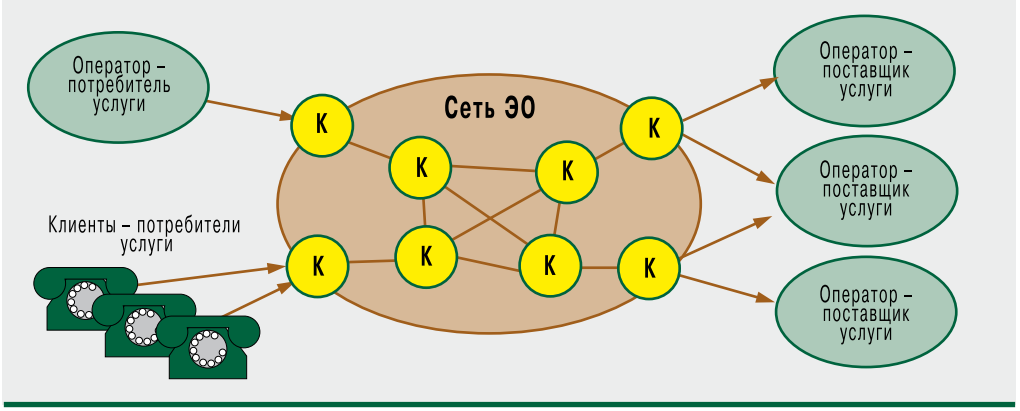


Таблица маршрутизации – это перечень соответствий между префиксами телефонных номеров и набором поставщиков услуг, через которых можно передавать вызовы. Поставщики услуг в наборе либо выбираются последовательно, один за другим, либо для каждого поставщика назначается процент общего объема трафика. Возможна комбинация этих двух подходов.

Необходимо различать маршрутизацию внешнюю и внутреннюю. Внешняя (иначе – коммерческая) маршрутизация выполняется на коммутаторах-шлюзах. В качестве критериев при ее расчете используются тарифы операторов-партнеров, предполагаемые объемы трафика, гарантированные объемы, пропускная способность каналов связи и качество каналов. При расчете внешней маршрутизации топология сети ЭО не имеет значения.

Внутренняя (или техническая) маршрутизация – это маршрутизация по сети ЭО до коммутаторов-шлюзов; именно при ее расчете учитывается топология сети ЭО. Внутренняя маршрутизация проводится после внешней и на основании ее результатов.

Далее в статье речь пойдет только о внешней маршрутизации.

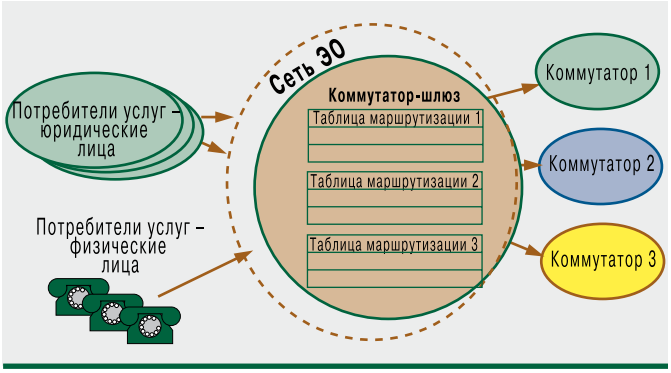
В результате расчета маршрутизации, во-первых, формируются командные файлы для загрузки таблиц маршрутизации на коммутационное оборудование, во-вторых, подготавливаются данные для актуализации нормативно-справочной информации (НСИ) для систем взаиморасчетов между операторами связи. Отметим, что такая актуализация – одно из направлений интеграции систем взаиморасчетов с системами LCR.

Поиск оптимального маршрута

В сети ЭО существует выделенный коммутатор – шлюз, в который загружаются таблицы маршрутизации (рис. 2). Для каждого вызова коммутатор в соответствии с таблицей маршрутизации выбирает возможное направление. Варианты направления вызовов выбираются последовательно – в порядке уменьшения их приоритета.

Рассматривая простейший пример таблицы маршрутизации, для наглядности будем считать, что каждый коммутатор относится к одному поставщику. Пусть эксплуатирующая организация оказывает услуги по передаче трафика на N направлений (полный набор префиксов состоит из N значений). При этом трафик M может направляться разными способами (по количеству поставщиков услуги, с которыми у эксплуатирующей организации заключены соответствующие договоры). Тогда таблица маршрутизации будет состоять из N строк и двух столбцов: в первом столбце содержатся значения префиксов, во втором – список поставщиков услуги, отсортированный в порядке понижения приоритета поставщика. В общем случае в каждом списке содержится M поставщиков.

Рис. 2. Маршрутизация вызовов



При поступлении вызова на коммутатор-шлюз путем максимального вхождения определяется префикс из таблицы маршрутизации и в соответствии с ним рассматриваются возможные пути направления вызова. Список поставщиков упорядочен по приоритетам, и коммутатор всегда пытается направить вызов по наиболее приоритетному направлению (при наличии технической возможности). Если возможности нет, то выбирается направление с меньшим приоритетом и т.д.

Приоритеты для поставщиков услуг в системе оптимальной маршрутизации устанавливаются по следующим критериям:

- тарифы операторов-партнеров;
- статистика по объемам пропущенного трафика;
- пропускная способность каналов;
- показатели качества каналов.

На каждом коммутаторе могут быть одновременно загружены несколько таблиц маршрутизации, отличающихся набором префиксов, параметрами «вид трафика» и «источник трафика». Вид трафика – это характеристика некоторой услуги по пропуску трафика; конкретное содержание такой услуги оператор определяет самостоятельно. Например, если он предоставляет услуги международной связи с двумя уровнями качества, то может определить в системе два вида трафика: «международный обычный» и «международный премиум».

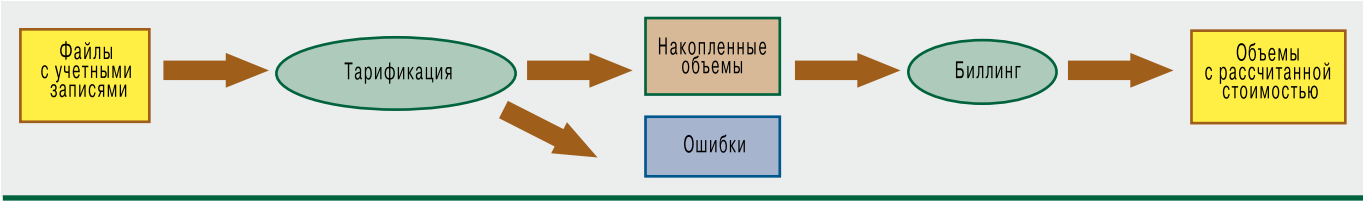
Источник трафика – это так же произвольно формируемая пользователем группировка потребителей услуги (источников, из которых поступают вызовы). Примеры таких группировок: физические лица, юридические лица, операторы.

При установке соединения для каждого вызова выбирается таблица маршрутизации в соответствии с видом и источником трафика. По таблице маршрутизации определяется дальнейшее направление вызова.

Как уже говорилось выше, конечной целью поиска оптимального маршрута является формирование командных файлов для загрузки в коммутатор таблиц маршрутизации. Исходной информацией для этого служат прайс-листы из договоров, которые ЭО заключает с операторами связи – поставщиками услуг. В прайс-листах, которые предоставляют поставщики услуг, перечислены направления (префиксы) и тарифы по данному направлению. Задача оптимизации состоит в том, чтобы для каждого префикса определить последовательность выбора поставщика при маршрутизации вызова. Для этого используются специальные алгоритмы.

Полученная таблица маршрутизации учитывает следующие критерии выбора оптимального направления

Рис. 3. Этапы обработки вызовов



трафика: тариф партнера, статистика передаваемых объемов по направлению и показатели качества.

Ранжирование партнеров по тарифам проводится с учетом статистической информации о предполагаемых объемах трафика по направлениям. Эти данные могут быть сформированы программой взаиморасчетов между операторами связи. Таким образом, необходимость ранжирования партнеров создает еще одну предпосылку для интеграции двух систем.

LCR плюс АСР

Автоматизированные системы расчетов (АСР) предназначены для информационной поддержки взаиморасчетов за оказанные услуги между компаниями-операторами (партнерами), включая операторов транзитных узлов связи и операторов, предоставляющих услуги конечным пользователям. К числу таких услуг относятся и услуги передачи трафика, для которых, собственно, и необходима маршрутизация.

Процесс обработки вызовов в АСР состоит из двух основных этапов: тарификация и биллинг (рис. 3).

Тарификация – это накопление объемов однотипных вызовов, а биллинг – расчет стоимости накопленного объема однотипных вызовов. Тарификация в АСР обеспечивает системе LCR статистические данные, необходимые в тех случаях, когда тарифы партнера зависят от пропускаемых объемов.

И тарификация и биллинг проводятся на основе введенной пользователем нормативно-справочной информации о партнерах и их тарифах. Таким образом, изменения в маршрутизации трафика требуют внесения соответствующих изменений в НСИ.

Функциональность загрузки всех CDR (Call Detail Record), поступающих с коммутаторов, обычно реализована в системе расчетов, следовательно, в случае интеграции не будет необходимости в такой функциональности в LCR.

Рис. 4. Интеграция систем оптимальной маршрутизации и взаиморасчетов
(на примере АСР Peter-Service ITC)

В интегрированной системе (рис. 4) LCR импортирует сведения о тарифах партнеров в электронном виде, а затем считывает информацию с коммутационного оборудования (текущие настройки маршрутизации, показатели качества) и получает от АСР статистическую информацию об объемах пропущенного трафика на различные направления.

На основании этой входной информации система LCR рассчитывает оптимальные маршруты для каждого направления и подготавливает предложения по изменению маршрутизации вызовов (пользователь может отредактировать эти предложения перед загрузкой в коммутационное оборудование). Кроме того, система актуализирует НСИ, автоматически загружая тарифные планы партнеров.

Что дает интеграция

Необходимость актуализации нормативно-справочной информации в системах взаиморасчетов является самой очевидной причиной для интеграции их с системами поиска оптимального маршрута. Синхронизация НСИ из разных систем разных производителей – непростая задача, но она существенно упрощается в случае единого интегрального решения, основанного на общей справочной системе.

Важным звеном в интеграции является ранжирование партнеров по тарифам с учетом пропуска предполагаемых объемов трафика. Эта задача предполагает развитие системы расчетов, появление в ней новых специализированных режимов тарификации, обеспечивающих накопление статистических данных по пропущенным объемам трафика, необходимых для работы LCR.

Кроме того, интеграция позволит избежать дублирования такой востребованной в обеих системах функциональности, как загрузка CDR и прайс-листов партнеров.

Отдельное внимание следует обратить на то, что механизм определения оптимального маршрута в значительной степени является эвристическим. Интеграция же LCR с системой расчетов позволит протестировать маршруты-кандидаты и сделать вывод о том, являются ли они на самом деле оптимальными (для этого, например, в нашей системе расчетов разрабатывается специальный режим тарификации). Анализ результатов тестирования даст полную картину того, что произойдет, если предложения по изменению маршрутизации вызовов будут загружены на коммутационное оборудование. ИКС

Медь и оптика: за мирное сосуществование

СКС – продукт консервативный по своей природе. Но при развертывании корпоративных ИС быть узким местом права не имеет. Куда направлена «кабельная эволюция»? – об этом наш разговор с Игорем СУНЧЕЛЕЕМ, директором представительства Eurolan в России.

Игорь СУНЧЕЛЕЙ

– Какие потребности, возникающие при проектировании и развертывании СКС, стремятся «закрыть» своими новыми решениями и компонентами производители?

– Прежде всего – повышение пропускной способности систем. Для решения этой задачи и появились кабели категории 6A, обеспечивающие технологию передачи 10G Ethernet по каналам до 100 м длиной. Борьба за полосу пропускания продолжается, и очень важной ее стороной является помехозащищенность: по мере роста скоростей влияние внешних электромагнитных излучений выходит на передний план. Понимая это, компания Eurolan сознательно вошла в круг поставщиков СКС, предлагающих для категории 6A экранированные решения: неэкранированных кабелей этой категории в ее продуктовом портфеле нет.

Кроме того, многие производители, и мы в том числе, активно ищут и находят способы сокращения трудоемкости монтажа и его ускорения – иными словами, создают удобства для специалистов, прокладывающих СКС.

– А насколько заказчики готовы использовать высокоскоростные решения?

– В России уже есть проекты на СКС различных производителей, в которых кабели категории 6A доводятся до каждого рабочего места. Подобный проект на 2000 портов реализован на базе наших продуктов в Московском планетарии. И все же потребности российских заказчиков в решениях категории 6A сегодня несравнимы с тем горячим спросом, которым они пользуются в Швеции, где компании целенаправленно выбирают наши решения этой категории на 5–6 тыс. рабочих мест. Я объясняю это их стремлением делать все основательно и надолго.

– Какие перспективные технологии и решения в области СКС плохо приживаются на российской почве?

– Технология пневматической прокладки волокна, Blown Fiber, по которой оптические волокна с помощью компрессора вдувают в размещенные в грунте или разведенные по зданию трубки из специального материала. Технология очень популярная в мире. По крайней мере, у Eurolan много таких проектов в Скандинавии, в том числе и для жилого сектора. В России эту технологию пока никто не использует, очевидно, из-за более высокой стоимости первой инсталляции. Между тем, инвестировав один раз, заказчик получает возможность быстро и недорого масштабировать свою СКС: новые волокна можно будет «вдувать» в нее на расстояния до 2 км за 15–20 мин.

Не находят пока должного применения в России и решения «домашних СКС».

– Какие же СКС вы считаете самыми востребованными в нашей стране?

– Наибольшим спросом по-прежнему пользуются медные системы категорий 5e и 6. Причин тому несколько: и конкурентоспособность медных решений по цене в сравнении с оптическими, и отсутствие в достаточном количестве приложений для рабочих мест, которым требуется скорость более 100 Мбит/с. Кроме того, доведение оптики до каждого рабочего места сдерживается отсутствием в ПК и ноутбуках оптического порта для подключения к сети.

– Отмечаете ли вы в последние год-два изменения структуры заказчиков СКС, с которыми работают ваши партнеры – системные интеграторы?

– По большому счету кардинальных изменений не произошло: мы по-прежнему ориентированы на корпоративный сектор. Вместе с тем не могу не отметить сегодня сдвиг продаж в область сегмента high-end. Рынок СКС продолжает выходить из кризиса. Тех, кто выбирает алюминиевые и омедненные решения, системы noname, становится все меньше.

Зато растет количество заказчиков, уделяющих внимание пожарной безопасности СКС, наличию у производителей российских сертификатов на компоненты системы, в том числе довольно редких – например, подтверждающих негорючесть кабеля в пучке.

Справедливости ради нужно отметить рост спроса на оптические решения. В 2011 г. их доля в структуре продаж Eurolan по сравнению с предыдущим годом увеличилась вдвое – с 10 до 20%.

– Вы считаете, что соотношение медных и волоконно-оптических СКС в недалеком будущем изменится? Как?

– Поскольку медь по-прежнему способна конкурировать с оптикой по цене, от нее никто не откажется. Более того, продолжатся попытки найти замену медному проводнику в целях удешевления решения.

Однако в связи с ростом потребности в скорости серверных решений и обработки данных волоконно-оптические интерфейсы, особенно 100G Ethernet, будут становиться все более популярными. Их использование оптимально именно на высоких скоростях: медные решения для такого применения будут слишком дороги.

Беседовала **Александра КРЫЛОВА**

ИКС pro

Технологии

Старая новая виртуализация в мире СХД

Надежда ПРИВЕЗЕНЦЕВА

Стимулом к развитию виртуализации СХД в большой степени послужила серверная виртуализация, особенно учитывая проникновение виртуальных машин в сегмент критически важных приложений. Но принципы виртуализации для СХД отнюдь не новы, пусть даже успехи этой технологии в мире хранения данных не так велики, как в мире серверов.

Говорим «виртуализация», подразумеваем...

Применительно к системам хранения данных (СХД) виртуализацию можно понимать двояко – как «внешнюю» или «внутреннюю». Внутренняя, т. е. виртуализация на уровне одной системы хранения, присутствует в индустрии уже давно. Она лежит в основе организации многоуровневого хранения данных, функций Thin Provisioning и многих других, в том числе классической организации RAID. Вариант внешней виртуализации предполагает объединение гетерогенных систем хранения в общий пул ресурсов. В свое время на такой вариант виртуализации хранения возлагались большие надежды, однако пока на рынке СХД не удалось достичь результатов, сопоставимых с успехами в сфере серверной виртуализации. Причина тому – отсутствие единой доминирующей архитектуры для систем хранения, проприетарность аппаратных и программных платформ СХД. «Исторически каждый производитель решал задачи виртуализации самостоятельно, в соответствии со своим видением проблемы и сложившимися традициями в R&D, к тому же некоторые технологии были защищены патентами», – отмечает Владислав Логвиненко (группа по развитию бизнеса HP Storage в России). В такой ситуации сложно было появиться специализированному вендору, подобному VMware, который мог бы продвигать единое решение для всего рынка.

Производители систем хранения предложили рынку свои технологии, направленные на полную виртуализацию всей сети хранения данных, включая СХД разных производителей. Такие решения существуют в виде контроллеров системы хранения (Hitachi USP/USP V) или в виде специализированных программно-аппаратных устройств (appliance), включаемых в тракт передачи данных между серверами и сетью SAN. Примеры таких устройств-виртуализаторов – EMC Invista, NetApp V-Series, HP StorageWorks SAN Virtualization Services Platform (SVSP), IBM SAN Volume Controller (SVC). Скажем, IBM SVC способен объединять в пул практически любые системы хранения с общим унифицированным интерфейсом управления, существенно упрощая администрирование СХД. Помимо консолидации ресурсов хранения такие решения призваны создать основу для построения распределенных инфраструктур хранения, а в последнее время – и облачных сред. «Данный подход является альтернативой технологиям удаленной репликации, а может быть, и их заменой в будущем», – убежден Дмитрий Агеев из IBM. Кроме того, внешняя виртуализация привносит новые возможности в старые системы, продлевая их жизнь в дата-центре.

Решения на базе внешних виртуализаторов – скорее прерогатива крупных компаний. Но есть и альтернативы для сегмента midrange. Например, год назад IBM выпустила дисковый массив StorwizeV7000, который основан на технологиях SVC и имеет встроенную функцию виртуализации. В отличие от виртуализатора, в StorwizeV7000 есть собственные диски для хранения данных, а по мере необходимости к массиву можно дополнительно подключать внешние системы.

Стоит также отметить, что существуют программные средства виртуализации СХД, которые устанавливаются на стандартные серверы. Например, ПО HP LeftHand P4000 Virtual SAN Appliance (VSA), развертываемое на серверах VMware ESX или Microsoft Hyper-V, превращает диски имеющихся серверов и систем хранения DAS и SAN в виртуальную кластерную систему хранения LeftHand. Доступны на рынке и такие программные продукты, как DataCore SANsymphony-V, FalconStor NSS, Virsto. Например, с помощью SANsymphony-V можно управлять любыми устройствами хранения, способными работать с Windows Server и подключаемыми по Fibre Channel, iSCSI или напрямую к серверу.

SAN, NAS или...

Наиболее широко технологии виртуализации распространены в области систем хранения с блочным доступом (SAN). Как уже упоминалось, стимулом к виртуализации СХД во многом послужила серверная виртуализация, а системы SAN лучше приспособлены для работы с гипервизорами. «Немаловажно отметить, что современные гипервизоры научились напрямую работать с такими СХД, перенося высоконагруженные операции, например миграцию виртуальных машин или их клонирование, напрямую на уровень СХД и освобождая ресурсы процессора и сети», – говорит Александр Грубин (департамент систем хранения данных HP Россия). К примеру, набор таких технологий под названием vStorage API имеется в VMware vSphere. Кроме того, по сравнению с системами с файловым доступом (NAS) системы SAN, как правило, обеспечивают лучшие быстродействие, надежность и доступность, масштабируемость и более эффективное использование дисковых ресурсов.

Но не все так однозначно. Хотя в некоторых приложениях, прежде всего при построении кластерных решений, без SAN не обойтись, сегодня уже нельзя утверждать, что решения на базе SAN являются единственно правильным выбором как для сред виртуализации, так и для других областей. «Производительность систем на основе блочного и файлового доступа практически идентична, – говорит Владимир Мешалкин (АМТ-ГРУП), – а поддержка со стороны гипервизоров всесто-

ронне развита для обоих типов систем». Поэтому вариант использования NAS стоит рассматривать, уделяя особое внимание трем основным параметрам – полосе пропускания (bandwidth), операциям ввода-вывода (IOPS) и задержке (latency). Поскольку работа виртуальной среды непосредственно связана с файлами – виртуальными машинами, системы с файловым доступом в ряде случаев могут обеспечить наилучшие показатели.

В пользу NAS, по мнению Романа Ройфмана из компании NetApp, говорит и характерная для виртуальных сред тенденция к взрывному росту числа виртуальных машин. Это влечет за собой необходимость масштабирования виртуальной инфраструктуры и усложнение управления. И вот здесь у NAS появляются преимущества – легкость управления данными, простое масштабирование с блокировками на уровне файлов или отдельных виртуальных машин. Это значительно облегчает эксплуатацию больших ферм. А благодаря использованию современных каналов 10G системы NAS не только не уступают SAN в производительности, но и в ряде случаев превосходят их.

Валерий Рыбин (компания «Открытые технологии») и вовсе считает мифом мнение о лучшей приспособленности SAN к виртуализации. Да, доступ по файловому протоколу требует больше вычислительных ресурсов, чем по блочному. Однако времена медленных одноядерных процессоров ушли в прошлое, и сегодня скорость обработки файловых протоколов на ESX-серверах почти сравнялась с производительностью блочных протоколов. К этому можно добавить, что при использовании NAS нет необходимости разворачивать дополнительную оптоволоконную сеть хранения, поскольку NFS-протокол работает поверх IP.

Конечно, никто не отрицает, что NAS не всегда превосходит SAN, что для одних задач практичнее применять одну, для других – другую архитектуру. В свете этого стоит обратить внимание на унифицированные системы хранения (Unified Storage), одновременно предоставляющие и блочный, и файловый доступ.

...Unified Storage?

Функционал блочного хранения и файлового хранения «в одной коробке» сегодня предлагают практически все производители. «Пока вряд ли можно сказать, что эта технология пользуется популярностью, но как тенденция она уже существует. С учетом активно растущих потребностей в файловом хранении в будущем такой подход должен прижиться и стать стандартом», – полагает Кирилл Янчевский из Hitachi Data Systems. Например, Oracle реализует концепцию Unified Storage во всех СХД: протоколы FC, iSCSI, CIFS, NFS поддерживаются как в SAN-системе Oracle Pillar Axiom 600, так и в NAS-системах Oracle ZFS Storage. При этом специалисты Oracle Hardware рекомендуют заказчикам, выбирая Unified Storage, обращать внимание на особенности реализации. В решении Oracle функции SAN и NAS в рамках единой СХД возложены на разные типы контроллеров. Благодаря этому массив эффективно обрабатывает любые виды нагрузок. А системы, изначально оптимизированные только под файловый доступ, вряд ли будут максимально эффективны для «тяжелых» приложений с доступом через SAN.

Старейшим «игроком высшей лиги» на рынке унифицированных систем хранения является компания NetApp. В настоящее время на нем присутствуют также

IBM с системой StorwizeV7000, EMC с продуктами серии VNX и ряд других вендоров. В ближайшее время можно ожидать увеличения числа компаний, предлагающих подобные решения.

Как отмечает Александр Зейников (компания LSI в России и СНГ), наряду с объединением существующих протоколов в одной системе границы между SAN и NAS будут еще больше размываться при использовании более сложных механизмов доступа к данным, таких как NFS 4.1 (pNFS). Этот протокол новой версии помимо традиционного файлового предлагает возможности блочного доступа, а также нового для мира СХД объектного доступа.

Унификация, несомненно, поможет сократить вложения, упростить управление и лучшим образом утилизировать возможности аппаратного и программного обеспечения СХД. «Но в большинстве случаев универсальное решение будет хуже специализированных, уж очень велики различия между блочными и файловыми СХД: в режимах работы кэша, организации резервного копирования и защиты от катастроф, в способах выделения пространства, используемых протоколах», – констатирует Сергей Платонов (компания Avroraid). Да и что греха таить, под маркой «унифицированной системы» на рынке порой появляются решения, которые на поверку оказываются блочными системами с встроенным NAS Appliance.

По мнению Александра Яковлева из Fujitsu, унифицированные решения реально востребованы в довольно ограниченном сегменте. В большинстве случаев заказчик для своих приложений использует либо файловое, либо блочное подключение, и применение специализированного хранилища NAS или SAN будет более эффективным. На недостаточность в ряде случаев «унифицированного» подхода обращает внимание и Евгений Пухов (EMC Россия и СНГ). Речь идет о задачах, где встречаются «большие данные», вычислительные кластеры, высоконагруженные СУБД, критичные к времени отклика, или же распределенные интерактивные приложения Web 2.0. «Для всего этого у EMC есть отдельные подходы, – отмечает Е. Пухов. – Унифицированные системы хранения – это базовый фундамент любой организации, но многие задачи требуют специализированных инструментов для хранения. Принцип one size fits all не везде работает».

Унифицированные системы NAS/SAN предназначаются для SMB-рынка, подчеркивает В. Логвиненко. Однако при этом они обычно работают под управлением Linux/UNIX, и для них приоритетным является NFS-протокол. А большинство малых и средних организаций работают в Windows-среде. Интеграция таких систем в Windows-инфраструктуру требует от системных администраторов особых знаний. А для работы с CIFS-протоколом необходима эмуляция, что замедляет скорость файлового доступа. Поэтому HP придерживается комбинированного подхода – предлагает как «чистые» NAS-системы (HP X1000/X5000), так и NAS-шлюзы (X3000/X9000), которые используются с СХД, предоставляя одновременно и блочный, и файловый доступ. При этом почти все NAS-системы HP работают под управлением Windows Storage Server (WSS) и хорошо совместимы с CIFS-протоколом. А поскольку WSS одновременно предоставляет и блочный доступ по протоколу iSCSI, NAS-система может использоваться и для работы серверов приложений, подключаемых через Ethernet.

По пути предложения шлюзов, позволяющих добавить функционал NAS к уже развернутой группе массивов, идет и компания Dell, которая в прошлом году анонсировала шлюз NAS Dell EqualLogic FS7500 для дисковых массивов EqualLogic PS Series.

Интересен взгляд на перспективы конвергенции SAN и NAS со стороны производителя сетевого оборудования. По мнению Николая Умнова (филиал Brocade в России и СНГ), решения SAN и NAS еще долго будут существовать независимо. Поэтому Brocade предлагает отдельно инфраструктуру Fibre Channel для SAN и отдельно Ethernet, в том числе для NAS. Конвергенцию же компания Brocade (разрабатывающая и конвергентные решения) понимает как перенос отработанных решений из мира FC в мир Ethernet – не с целью заменить технологию FC на FCoE, а чтобы упростить управление сетями Ethernet. В рамках этого направления компания предлагает перейти к Ethernet-фабрике, поддерживающей протоколы Ethernet, DCB (CEE), FCoE. Протокол FCoE предполагается использовать для подключения серверов в рамках одного шкафа, а для доступа к системам хранения рекомендуются более зрелые технологии FC, NAS и iSCSI – каждая из них имеет свою область применения, и они сильно не конкурируют.

RAID в новом качестве

Архитектура RAID – по сути не что иное как виртуализация жестких дисков для повышения отказоустойчивости и производительности массива. По выражению Е. Пухова, это «первый шаг в облако, сделанный еще на заре персональных компьютеров». Технология RAID имеет уже примерно 20-летнюю историю, но этот подход по-прежнему активно работает и развивается, хотя уже немного в другой плоскости. «Сейчас виртуализуют не столько диски, сколько целые системы хранения и даже ЦОДы целиком», – добавляет Е. Пухов, приводя в пример системы старшего класса EMC Symmetrix, в которых внутренняя виртуализация касается контроллеров и шины межконтроллерного взаимодействия. В качестве альтернативы EMC развивает направление параллельных систем хранения данных без единой точки отказа – при этом система хранения представляет собой вычислительный кластер и масштабируется горизонтально.

Классическая RAID-архитектура имеет ряд недостатков, и основной из них, пожалуй, – длительное время восстановления данных на диске массива (а с ростом емкости дисков это время еще более увеличивается). Потенциально его можно сократить путем увеличения RAID-группы, однако в этом случае узким местом становится диск четности.

Эту и другие проблемы, связанные с RAID, вендоры решают посредством проприетарных наработок. Например, Avroraid предлагает использовать RAID 6 (два диска четности на группу) в сочетании с фирменным алгоритмом Advanced Reconstruction, который повышает производительность массива и скорость рекон-

струкции данных. Это происходит за счет автоматического исключения из процесса реконструкции до двух дисков, производительность которых находится ниже заданного предела; данные с таких дисков вычисляются с использованием контрольных сумм. Производитель утверждает, что решение позволяет сократить время реконструкции массива объемом 18 Тбайт до 3,5 ч.

Другой путь решения проблемы – технологии интеллектуального размещения блоков данных. Так, в IBM XIV данные, поступающие в систему, разбиваются на разделы (partitions) размером в 1 Мбайт. Разделы распределяются по всем дискам системы по механизму псевдослучайного распределения. Для каждого раздела создается зеркальная копия, которая помещается в другом модуле хранения (система может содержать до девяти модулей хранения данных по 12 дисков в каждом). В случае сбоя система определяет пострадавшие разделы и немедленно начинает создание новых копий. В процессе восстановления участвуют все диски, за счет чего этот процесс радикально сокращается – заявлена возможность восстановления жесткого диска емкостью 1 Тбайт менее чем за 30 мин.

Технологию распределения данных по множеству дисков используют и другие производители: Panasas, EMC, Hitachi, HP. Например, в СХД HP 3PAR и EVA нет традиционных RAID-групп, дисковое пространство разбито на сегменты фиксированной емкости, из которых, как из конструктора, собираются логические тома. В один логический том могут входить сегменты из десятков дисков, таким образом, операции ввода-вывода разнесены на большее количество шпинделей, что повышает производительность массива. Резервных (spare) дисков не требуется, свободное пространство, как и занятое, равномерно распределено по всем дискам массива.

Среди прочего, такой вариант виртуализации дискового пространства упрощает реализацию функции Thin Provisioning: данные каждого логического тома можно динамически перемещать по физическим дискам, в том числе SSD, чтобы получить максимальный уровень производительности. Федерализация хранения (онлайн-миграция логических томов с одной СХД на другую) также реализуется гораздо проще.

Компании NetApp и Oracle (Sun) идут по пути тесной интеграции RAID с файловой системой (решения WAFL/RAID-DP и ZFS/RAID-Z соответственно). Эти решения позволяют снять проблему неатомарности операций записи в классической RAID-архитектуре. Неатомарность означает, что операция записи не выполняется как одно целое, запись блока данных и блока контроля четности происходит независимо. Возникает временно́е окно между двумя операциями (write hole), в течение которого возможно повреждение RAID-массива в случае сбоя. Указанные технологии позволяют исключить проблему неатомарности записи благодаря журналированию; кроме того, производительность случайного доступа можно заметно повысить за счет организации размещения блоков при записи.

Между тем, по мнению А. Яковлева, более реальной альтернативой является увеличение уровня надежности существующих уровней RAID за счет специальных аппаратных механизмов. Ряд таких механизмов, позволяющих сохранить высокий уровень надежности не в ущерб производительности системы, реализован, например, в дисковых системах ETERNUS DX S2 компании Fujitsu.

Ресурсы в кредит

Рациональное использование ресурсов хранения – задача не менее важная, чем обеспечение производительности и надежности СХД. Среди технологий, призванных решить эту задачу, – дедупликация (ряд производителей применяют ее не только для резервного копирования, но и для активных данных); сжатие данных перед размещением их на дисках массива; мгновенные снимки и копии, которые позволяют отказаться от создания полных копий данных; технология «тонкого» (или динамического) выделения ресурсов хранения – Thin Provisioning, позволяющая «выдавать в кредит» емкость для хостов.

Напомним, суть Thin Provisioning – в предоставлении хостам большего пространства, чем физически имеется на системе хранения. «Виртуально» логический том может иметь любой размер, но физическая емкость си-

стемы хранения используется лишь тогда, когда в том записываются данные. На сегодня Thin Provisioning реализована в подавляющем большинстве СХД. В некоторых системах хранения (например, Oracle) этот функционал входит в базовую поставку и не требует отдельного лицензирования. Однако технология связана со своими «накладными расходами» и несет определенные риски – как, впрочем, и любая другая технология виртуализации внутреннего пространства СХД. Основной риск, как предупреждают специалисты Huawei, это неконтролируемый рост объема данных (из-за вирусов или программных ошибок), который влияет в большинстве случаев на общий пул хранения данных, а не только на конкретный том. К тому же для большинства систем хранения использование «тонких» томов вносит дополнительные ограничения, например невозможность создания снэпшотов, расширения тома и т. п.

К. Янчевский обращает внимание на риск потери всех данных в случае единовременного выхода из строя нескольких носителей в одной RAID-группе: «При классическом подходе потеря двух дисков в зеркале или группе RAID 5 приводит к потере данных внутри этой группы, в случае же использования Thin Provisioning это будет потеря данных всех групп, так как все данные “размазаны” по разным группам». Поэтому для Thin Provisioning рекомендуется использовать массив RAID 6 как наиболее защищенный.

Существует риск перерасхода дискового пространства, например когда некое приложение или неожиданно стартовавшая операция начинают интенсивно записывать данные на «тонкий» диск, забирая все свободное пространство массива. Производители стремятся предлагать ПО, способное контролировать расход пространства. Такую функцию выполняет, например, плагин EMC VSI (Virtual Storage Integrator), предназначенный для интеграции виртуальной среды VMware с массивами EMC. Возможности подобного ПО, конечно, не безграничны, пополнять дисковую емкость все равно придется. Андрей Вересов (группа по развитию бизнеса 3PAR, HP в Центральной и Восточной Европе) настоятельно рекомендует своевременно реагировать на оповещения о том, что следует увеличить дисковую емкость, и при использовании Thin Provisioning придерживаться стратегии регулярного добавления дисков по мере необходимости. Но если пределы масштабирования СХД достигнуты, проблема перерасхода может встать особенно остро. Возможность же отменить Thin Provisioning, сделав из «тонкого» диска обычный, существует не во всех дисковых массивах.

Потерять производительность систем хранения данных – риск, пожалуй, еще более существенный. В первую очередь Thin Provisioning влияет на производительность задач, связанных с интенсивной записью (линейный монтаж видео, резервное копирование и пр.), поскольку выделение пространства по требованию приложения накладывает дополнительную нагрузку на контроллер СХД. Компания EMC рекомендует там, где нужна производительность, использовать традиционные тома, «тонкие» же применять там, где более важны эффективность

Проблемы RAID-архитектуры и перспективные альтернативы

Сергей ПЛАТОНОВ,
product manager,
компания AVRORAID

Технология RAID существует уже 20 лет. За эти годы в индустрии хранения данных произошли существенные перемены, резко выросли объемы системных носителей и хранимых данных. Именно это в первую очередь привело к поиску альтернатив классическим архитектурам RAID.

Какие же особенности RAID требуют от разработчиков новых решений?

Время реконструкции данных на диске массива. При выходе из строя жесткого диска объемом 3 Тбайт его полная реконструкция займет не менее 8 ч при условии высокой производительности контроллера массива; на практике большинству современных контроллеров для этого требуется двое-трое суток. Однако сейчас на рынке появляются системы без такого недостатка: в частности, решения AVRORAID сокращают время реконструкции массива объемом 18 Тбайт до 3,5 ч.

Неатомарность операций записи. В подавляющем большинстве имплементаций классических архитектур RAID запись блока данных и контрольных сумм на диски выполняется параллельно и независимо. В случае сбоя при записи можно получить несоответствие данных страйпа и рассчитанных контрольных сумм. Эта проблема (называемая RAID write hole) решается путем тесной интеграции RAID с файловой системой или использования специальных журналов в энергонезависимой памяти. Решения WAFL/RAID-DP компании NetApp и ZFS/RAIDZ от Oracle (Sun) позволяют избежать неатомарности записи за счет журналирования; кроме того, организация размещения блоков при записи значительно повышает производительность случайного доступа.

Производительность записи на массив. Необходимость хранения избыточных данных и расчета контрольных сумм не может не сказаться на производительности записи. Особенно остра эта проблема для случайной записи. Производительность заметно падает и при выходе из строя дисков в массиве и их реконструкции. В классе СХД для потоковых данных есть решения, полностью реализующие возможности СХД даже в RAID 6, который исторически считался медленным. Например, СХД на платформе AVRORA на 48 дисках SAS обеспечивает в RAID 6 скорость чтения и записи до 4 Гбайт/с, при этом выход одного или двух дисков из строя не приводит к «проседанию» производительности. Существуют также технологии интеллектуального размещения блоков данных, значительно снижающие риск потери информации и уменьшающие время реконструкции массива, как это сделано в IBM XIV.

и совокупная стоимость владения, – для архивов и файлового хранения. А компания HP предлагает бороться с потерей производительности путем аппаратной реализации функционала Thin Provisioning: в массивах HP 3PAR это сделано с помощью специальных микросхем ASIC.

Но наиболее сложной задачей при реализации Thin Provisioning остается возвращение блоков LUN, освободившихся после удаления данных, в общий пул ресурсов (Space Reclamation или Thin Reclamation). Если не использовать Thin Reclamation, система хранения продолжает воспринимать освободившиеся блоки как содержащие данные, процент заполнения LUN не снижается, и «тонкий» том постепенно становится все более и более «толстым». Проблема эта лежит не на стороне СХД, а на стороне сервера, а именно файловой системы и приложений. Некоторые файловые системы и приложения не адаптированы для Thin Provisioning – они занимают сразу все доступное физическое пространство, что в конечном счете может привести к нехватке места и остановке сервисов.

Каждый производитель решает задачу по-своему. «К сожалению, сейчас нет единого для всех производителей механизма возврата освобожденных файловой системой блоков, – сетует Р. Ройфман. – Хотя отдельные файловые системы со встроенными механизмами возврата блоков уже представлены на рынке и в последние годы мы видим значительные усилия индустрии по стандартизации таких механизмов, но пока можно говорить лишь об отрывочных решениях». Для примера возьмем реализацию Thin Reclamation в массивах HP 3PAR. В упоминавшуюся выше микросхему HP 3PAR ASIC встроена функция Thin Persistence, которая ищет на дисках блоки, состоящие из нулей, и возвращает их в пул свободной емкости. Кроме того, функция позволяет анализировать данные перед записью на «тонкий» том, обнаруживать и не записывать на СХД данные, которые были удалены приложениями, но физически остались на диске сервера.

■ ■ ■

С использованием принципов виртуализации связаны не только упомянутые в статье, но и ряд других технологий, например автоматизированное распределение данных по уровням хранения (storage tiering). Каждая из них несет потребителю свои преимущества, но при этом порождает определенные риски. Взвешивая «за» и «против», всегда нужно иметь в виду конечную цель. Чему заказчик отдаст предпочтение – эффективности (защите инвестиций) или надежности и отказоустойчивости? Применительно к СХД есть основания полагать, что отказоустойчивость, независимость от аппаратных и программных сбоев, все-таки важнее. ИКС

Экономичные режимы работы систем охлаждения ЦОДов

Часть 3. Максимум времени – в экономичном режиме

Окончание. Начало см. «ИКС» №12'2011, с. 76; №1-2'2012, с. 80.

Джон НИМАНН, менеджер Schneider Electric по продуктовой линейке внутрирядных и малых систем охлаждения
Джон БИН-мл., директор APC by Schneider Electric по инновациям в области систем охлаждения уровня стойки
Виктор АВЕЛАР, старший исследователь-аналитик научно-исследовательского центра APC by Schneider Electric Data Center Science Center

Продолжаем сравнительный анализ экономичных режимов. Как добиться, чтобы система охлаждения как можно дольше работала в экономичном режиме и меньше – в неэкономичном?

Сравнение количественных характеристик

Напомним, что во 2-й части статьи мы выбрали из 15 возможных типов экономичных режимов те, для которых выполняются два условия: возможна работа в смешанном режиме, с пониженной нагрузкой на компрессор, и поддерживается испарительное охлаждение. Для шести выбранных режимов мы провели сравнительный анализ с учетом качественных характеристик. Теперь сравним те же режимы по ряду количественных характеристик (табл. 2); лучший по каждому показателю режим выделен цветным фоном.

Годовое потребление воды

Использование градирни предполагает значительный расход воды на испарение, происходящее круглогодично, в любой сезон (около 150 л воды на 1000 т холодопроизводительности[1]). В случае экономичных режимов, не использующих градирни, потребление

[1] Arthur A. Bell, Jr., HVAC Equations, Data, and Rules of Thumb. New York: McGraw-Hill, 2000, с. 243.

Экономика испарительного охлаждения

При выборе системы охлаждения ЦОДа с применением испарительного охлаждения необходимо учитывать стоимость испарительного охладителя с обвязкой, собственно воды и водоподготовки.

Применение испарительного охлаждения наиболее эффективно в сухом климате, например в Лас-Вегасе или Дубае. В более влажном климате есть опасность, что полученная экономия не покроет стоимости испарительного охладителя и расходов на его эксплуатацию.

воды значительно меньше, так как испарительное охлаждение применяется только при жаркой погоде.

Капитальные затраты на систему охлаждения

В эти затраты включаются расходы на проектирование, стоимость всех материалов и работ по установке, все накладные расходы по проекту, связанные с системой охлаждения в целом, исчисляемые в долларах на ватт ИТ-нагрузки. Например, для режима обхода чиллера на базе теплообменника учитывается стоимость чиллера. Этот вариант характеризуется наивысшими среди всех рассматриваемых капитальными затратами – из-за стоимости градирни, трубопроводов, насосов и разрабатываемой на заказ системы управления. Проектирование и реализация системы управления влекут за собой существенные затраты, поскольку большинство компонентов (если не все) приобретаются у разных производителей, а значит, для надежного функционирования системы и получения ожидаемой экономии потребуются разработка заказного ПО, его тестирование, верификация и настройка. Затраты на настройку такой системы обычно распределяются на год или более продолжительный срок. В настоящем анализе эти затраты отнесены к капитальным, но можно рассматривать их и как эксплуатационные.

Таблица 2. Экономичные режимы: количественные характеристики

Характеристика	Режимы с использованием воздуха			Режимы с использованием воды		
	Обход кондиционера с непосредственным использованием наружного воздуха*	Обход кондиционера на базе воздушного теплообменника*	Обход кондиционера на базе вращающегося теплообменника*	Обход чиллера на базе теплообменника**	Обход моноблочного чиллера на базе орошаемого теплообменника**	Обход компрессора периметрального кондиционера с использованием второго змеевика*
Годовое потребление воды, л	379	4 777 000	973 000	26 000 000***	485 000	485 000
Капитальные затраты на систему охлаждения в целом, $/Вт	2,2	2,4	2,8	3,0	2,3	2,0
Годовые затраты на обслуживание системы охлаждения в целом[4*], %	75	75	83	100	100	92
Полные затраты энергии на охлаждение	737 506	340 365	377 625	589 221	736 954	960 974
Общее время работы в экономичном режиме, часов в год	5723	7074	5990	4705	5301	4918
Общее время работы в смешанном режиме, часов в год	0	1686	2770	3604	1773	3800
Оценка среднегодового значения PUE	1,34	1,25	1,26	1,31	1,34	1,39

* С испарительным охлаждением

** Предполагается, что экономайзер включен в контур чиллерной воды последовательно с чиллером (возможна работа в смешанном режиме).

*** Потребление воды градирней складывается из испарения, просачивания и сдува (см. http://www.cheresources.com/ctowerszz.shtml).

[4*] В процентах от показателя базовой традиционной системы, включающей чиллер и градирню.

В таблице приведены данные для ЦОДа мощностью 1 МВт, расположенного в Сент-Луисе (шт. Миссури, США) и работающего под нагрузкой 50%. Предполагается, что в ЦОДе реализованы внутрирядная система охлаждения (экономичный режим с использованием воды), подвесной потолок (экономичный режим с использованием воздуха) и изоляция горячих воздушных потоков (все режимы). Вентиляторы переменной производительности установлены в блоках подготовки воздуха уровня помещения.

Использованы следующие допущения:

- максимальная нагрузка в ЦОДе – 1 МВт (без резервирования);
- ИТ-нагрузка – 500 кВт;
- среднее увеличение температуры воздуха после использования – 13,9°С;
- средняя температура воздуха у передней стенки шкафа – 24°С;
- максимальная относительная влажность воздуха на воздухозаборнике сервера – 55%;
- максимальная точка росы – –10°С;
- отношение объемов кондиционированного воздуха и фактически использованного для охлаждения ИТ-оборудования – 1,2;
- проектный перепад температуры чиллерной воды – 6,7°С;
- произведение коэффициента производительности чиллера (COP) на интегральный показатель эффективности при частичной нагрузке (IPLV) равно 9;
- минимальная температура воды в бассейне градирни – 4,4°С (за счет подогрева от размерзания);
- проектный диапазон температур градирни – 5,6°С.

Система охлаждения с режимом обхода моноблочного чиллера на базе орошаемого теплообменника обходится примерно на 23% дешевле благодаря тому, что в подсистему обмена теплом с окружающей средой входит не так много компонентов и меньше потребность в настройке. С другой стороны, для такой системы характерен более высокий показатель PUE ЦОДа (меньшая эффективность).

Годовые затраты на обслуживание системы охлаждения

Система из чиллера и градирни широко применяется в ЦОДах и хорошо подходит на роль эталона для сравнительного анализа эксплуатационных расходов. В табл. 2 годовые расходы на эксплуатацию приведены в процентах по отношению к такой системе. В расчет годовых эксплуатационных расходов включаются все компоненты системы охлаждения во всех режимах работы, в том числе в экономичных. Например, для режима обхода чиллера на базе теплообменника в расчетах учитывается чиллер. Системы охлаждения с экономичными режимами, в которых применяется воздух, характеризуются меньшими эксплуатационными расходами, но большим числом компонентов и повышенным уровнем сложности.

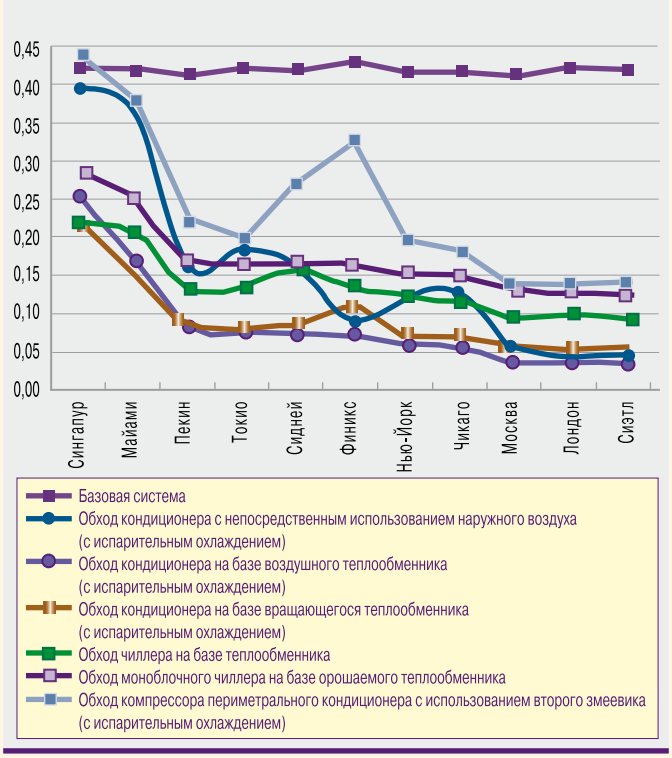
Полные затраты энергии на охлаждение

Эта характеристика представляет собой годовое потребление энергии всей системой охлаждения. Хуже других по данному показателю выглядит экономичный режим с обходом компрессора фреонового кондиционера с использованием второго змеевика в корпусе периметрального кондиционера. Основная причина этого – в низкой энергоэффективности распределенных систем охлаждения. А наилучший показатель – у режима обхода кондиционера на базе воздушного теплообменника; второе место с минимальным отрывом занимает режим с обходом кондиционера на базе вращающегося теплообменника.

Полезно также сравнить энергопотребление в экономичном режиме с традиционной системой из чиллера и градирни, используемой в большинстве ЦОДов мощностью от 1 МВт. Эта базовая система предполагает применение периметрального охлаждения без разделения разнотемпературных воздушных потоков и без экономичных режимов, с температурой чиллерной воды 7,2°C[1] и вентиляторами постоянной производительности в фанкойлах. Сравнение различных экономичных режимов с этим базовым уровнем по коэффициенту эффективности энергопотребления системы охлаждения (CLF)[2] проводилось для 11 городов (рис. 8), где имеется значительное количество ЦОДов. CLF представляет собой составляющую PUE, относящуюся к системе охлаждения ЦОДа.

Если не брать нетипичные климатические условия, такие как в Сингапуре, любой из рассматриваемых режимов обеспечивает экономию энергии в сравнении с базовой системой. Режим с обходом кондиционера на базе воздушного теплообменника характеризуется наименьшим расходом энергии на охлаждение практически во всех рассматриваемых климатических зонах: 381 385 кВт·ч в среднем в год. Это соответствует экономии в 79% в сравнении с базовой системой, в среднем расходующей 1 834 403 кВт·ч в год. Хорошие результаты показывает и режим с обходом кондиционера на базе вращающегося теплообменника.

Рис. 8. Коэффициент эффективности энергопотребления системы охлаждения в различных экономичных режимах



Общее время работы в экономичном режиме

Этот показатель говорит о том, сколько часов в год в среднем система охлаждения работает в полностью экономичном режиме. Напомним, что в статье анализ базируется на характеристиках ЦОДа, расположенного в Сент-Луисе (шт. Миссури, США), – данный показатель сильно зависит от географического положения. Режим обхода кондиционера с непосредственным использованием наружного воздуха характеризуется наименьшим общим временем работы в экономичном режиме – из-за ограничений по влажности в помещениях ЦОДа. В рассматриваемом примере он может работать без вспомогательного охлаждения в течение 7074 ч в год.

Общее время работы в смешанном режиме

Когда погодные условия недостаточно благоприятны и экономичный режим не обеспечивает нужной

[1] В системе на чиллерной воде экономичный режим позволяет повысить рабочую температуру. А повышение температуры чиллерной воды до 10–15°C значительно увеличивает общее время работы в экономичном режиме.

[2] Коэффициент CLF определяется как отношение общего энергопотребления системы охлаждения к энергопотреблению ИТ-нагрузки (последнее в рассматриваемом примере равно 500 кВт × 8760 ч/год).

температуры в ЦОДе, приходится прибегать к дополнительному компрессорному охлаждению. Это очень важный элемент, поскольку в мире не так уж много климатических зон, где возможна круглогодичная работа систем охлаждения в экономичном режиме. Очень часто система работает в смешанном режиме гораздо дольше, чем в экономичном, что позволяет добиться заметно более существенной экономии от смешанного режима. Режим обхода кондиционера с непосредственным использованием наружного воздуха характеризуется наименьшим общим временем работы в смешанном режиме – из-за ограничений по влажности в помещениях ЦОДа.

Оценка среднегодового значения PUE

Показатель эффективности использования энергии (Power Usage Effectiveness, PUE) рассчитывается как отношение общего энергопотребления ЦОДа к энергопотреблению ИТ-оборудования (предполагается типовая инфраструктура электропитания). Режим обхода компрессора периметрального кондиционера, установленного в ЦОДе, с использованием второго змеевика внутри корпуса кондиционера дает наивысшее (т.е. наихудшее) среднегодовое значение PUE – 1,39. Самое же низкое значение PUE, 1,25, – у режима обхода кондиционера на базе воздушного теплообменника, что соответствует примерно 26%-ной экономии на счетах за электроэнергию в сравнении с базовой системой (PUE 1,68).

От чего зависит время работы в экономичном режиме

Сколько часов в год система охлаждения сможет работать в том или ином экономичном режиме, зависит от ряда факторов. Наиболее важный из них – географическое положение ЦОДа. Весьма существенно также влияют конструкция системы охлаждения и ее уставки.

Географическое положение

Допустимость работы в экономичном режиме полностью зависит от географического положения ЦОДа. В определенные сезоны погодные условия могут делать ее вообще невозможной. Информацию об общем времени работы в экономичном режиме публикуют ASHRAE (American Society of Heating, Refrigerating and AirConditioning Engineers – Американское общество инженеров по системам отопления, охлаждения и кондиционирования воздуха), NREL (National Renewal Energy Lab – Национальная лаборатория возобновляемых источников энергии), NOAA (National Oceanic and Atmospheric Administration – Национальное управление по изучению и освоению океана и атмосферы) и ряд других организаций. Эти показатели рассчитываются по данным метеонаблюдений для конкретной местности.

Уставки системы охлаждения

Существует два основных способа увеличения общего времени работы в экономичном режиме: 1) выбор места с более благоприятными климатическими условиями и 2) повышение температуры на воздухозаборниках серверов. Очевидно, что для действующих ЦОДов первый способ нереален. Зато второй вполне реален и в настоящее время применяется и в новых, и в существующих дата-центрах. В версии ASHRAE Standard TC9.9 от 2008 г. максимально допустимая температура на воздухозаборнике сервера (по показаниям сухого термометра) была повышена с прежних 25 до 27°C. Однако уставка температуры кондиционированного воздуха зависит не только от этой величины, но и от качества разделения горячих и холодных воздушных потоков.

Разделение воздушных потоков

В типичном ЦОДе горячий и холодный воздух в значительной мере смешиваются – из-за неоптимального размещения шкафов с оборудованием и плохого управления воздушными потоками. В таком сценарии при уставке температуры кондиционированного воздуха 27°C температура на воздухозаборнике сервера может доходить до 32°C. Это означает, что данную уставку приходится значительно снижать.

Чтобы повысить уставку температуры кондиционированного воздуха и, как следствие, общее время работы в экономичном режиме, необходимо разделить горячие и холодные воздушные потоки. Здесь возможны два варианта: с изоляцией «горячих» либо «холодных» коридоров. В новом строительстве всегда используется первый, поскольку он обеспечивает значительно большее общее время работы в экономичном режиме. Разделение разнотемпературных воздушных потоков позволяет получить значительную прибавку в эффективности в любом ЦОДе, использующем экономичный режим. В целом считается, что нет смысла вкладывать средства во внедрение экономичного режима, пока ЦОД не оснащен той или иной системой разделения разнотемпературных воздушных потоков.

Как уменьшить использование неэкономичных режимов

До недавнего времени экономичные режимы работы системы охлаждения рассматривались как вспомогательные, дополняющие основную систему. В большинстве ЦОДов охлаждение проектировалось таким образом, чтобы проектная холодопроизводительность достигалась в базовом режиме, при отключенном экономайзере. Однако по мере оптимизации ЦОДов с точки зрения энергоэффективности экономичные режимы становятся основными, в результате чего открывается ряд новых возможностей повышения экономической эффективности дата-центра.

1. Если конструкция рассчитана на работу в смешанном режиме даже в самых неблагоприятных условиях, так что на компрессорную систему охлаждения никогда не возлагается полная нагрузка ЦОДа, можно установить компрессорную систему меньшей мощности – с соответствующим сокраще-

нием капитальных затрат и повышением эффективности.

2. Если конструкция рассчитана на работу только в экономичном режиме даже в самых неблагоприятных условиях, можно вообще отказаться от компрессорного охлаждения.

3. Если конструкция рассчитана на работу в экономичном режиме почти в любых условиях, кроме самых неблагоприятных, можно отказаться от компрессорного охлаждения, внедрив систему управления потребляемой мощностью ИТ-систем или перераспределения ИТ-нагрузки между несколькими ЦОДами.

Внедрение конструктивных решений, позволяющих сократить либо исключить использование компрессорного охлаждения, сделает возможным создание высокоэффективных систем охлаждения ЦОДов. Этот новый подход к построению системы охлаждения позволяет снизить ее энергопотребление примерно наполовину в сравнении с традиционными подходами и в то же время повышает масштабируемость и готовность, упрощает техническое обслуживание.

Подведем итоги

В прошлом экономичные режимы работы систем охлаждения в большинстве дата-центров всерьез даже не рассматривались. С тех пор многое переменилось: значительно выросли энерготарифы, необходимая температура охлаждающего воздуха повысилась, появились требования ограничить углеродные выбросы. Новые стандарты и нормативы, такие как ANSI/ASHRAE Standard 90.1-2010 и UK Carbon Reduction Commitment, заставляют руководителей ЦОДов задумываться над снижением энергопотребления. Ряд экономичных режимов работы систем охлаждения применим в широком диапазоне климатических условий. А во многих местностях такие режимы могут выступать в качестве основных – с переводом компрессорных систем охлаждения на роль дополнительных или резервных.

В определенных климатических зонах экономичные режимы позволяют экономить более 70% расходов на годовое энергопотребление системы охлаждения, что соответствует снижению среднегодового показателя PUE ЦОДа более чем на 15%. Однако экономичных режимов, существует по крайней мере 15 типов, и для них нет четких определений. Поэтому прежде всего необходимо выработать единую терминологию, без которой невозможно сравнение, выбор или составление спецификаций систем охлаждения с экономичными режимами. Предлагаемые в настоящей статье терминология и определения, наряду со сравнением экономичных режимов по количественным и качественным характеристикам, призваны помочь проектировщикам ЦОДов принимать правильные решения. ИКС

Климат региона и микроклимат ЦОДа

Учет климатических зон при анализе эффективности системы холодоснабжения

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

Тимур ТОЛОКОННИКОВ,
ведущий инженер отдела
исследований и развития
United Elements

Из общего энергопотребления оборудования ЦОДа до 30% может приходиться на систему поддержания микроклимата. При оценке эффективности этой системы необходимо рассматривать различные факторы, в том числе и климатические условия территории, где находится ЦОД.

Помещение ЦОДа – сложный с точки зрения инженерных сетей объект, и обеспечение его круглогодичной работоспособности ложится на владельца серьезной финансовой нагрузкой. Одним из основных потребителей энергоресурсов в инженерной инфраструктуре ЦОДа, обеспечивающей его бесперебойную работу, является система поддержания микроклимата. К тому же помимо эксплуатационных затрат это и значительные капитальные расходы. Поэтому крайне важна правильная оценка проектного решения, чтобы, с одной стороны, эксплуатационные расходы не превышали запланированных значений, а с другой – чтобы мощность оборудования не была завышенной. Именно баланс капитальных и эксплуатационных расходов обеспечивает владельцу приемлемый срок окупаемости ЦОДа.

Коэффициенты энергетической эффективности

На данный момент подавляющее большинство систем поддержания микроклимата построено на основе парокомпрессионной фреоновой холодильной машины (чиллеры, фреоновые прецизионные кондиционеры). Для оценки энергетической эффективности чиллеров, работающих в режиме охлаждения, принято пользоваться тремя базовыми коэффициентами, разработанными международной сертификационной организацией Eurovent.

COP (Coefficient of Performance) – холодильный коэффициент. Это отношение холодопроизводительности компрессора к его потребляемой мощности. Значение COP не учитывает влияние на энергоэффективность других компонентов чиллера, в частности вентиляторов конденсатора. Для большей достоверности оценки в дополнение к COP был предложен коэффициент EER.

EER (Energy Efficient Ratio) – это коэффициент энергетической эффективности, рассчитываемый как отношение холодопроизводительности холодильной машины к ее потребляемой мощности, включая мощность вентиляторов. Таким образом, он более точно оценивает энергопотребление холодильной машины при номинальных условиях работы. Однако оценка энергоэффективности по коэффициенту EER при длительной эксплуатации системы холодоснабжения дает значительную погрешность, поскольку чиллер большую часть года работает в условиях, отличных от номинальных. Чтобы учесть этот фактор, Eurovent разработала дополнительный коэффициент ESEER.

ESEER (European Seasonal Energy Efficient Ratio) – коэффициент сезонной энергоэффективности. Как показали европейские исследования, в среднем в течение годового периода эксплуатации чиллер 3% времени работает в условиях 100%-ной нагрузки, 33% времени – при 75%-ной нагрузке, 41% – при 50%-ной нагрузке и 23% времени – при 25%-ной нагрузке. Коэффициент EER чиллера при разных нагрузках ($EER_{n\%}$, где n – процент нагрузки) принимает разные значения.

Таким образом, значение ESEER рассчитывается по следующей формуле:

$$ESEER = 0{,}03 \times EER_{100\%} + 0{,}33 \times EER_{75\%} + 0{,}41 \times EER_{50\%} + 0{,}23 \times EER_{25\%}. \quad (1)$$

Для аналогичных целей в США разработан еще один коэффициент – интегральный показатель при частичной нагрузке (Integral Part Load Values, IPLV). Этот показатель определяется в соответствии со стандартом Института кондиционирования воздуха, систем отопления и холодоснабжения AHRI.

Значение IPLV рассчитывается аналогично ESEER, но с другими коэффициентами в уравнении. Так, считается, что при 100%-ной нагрузке чиллер работает только 1% времени, при 75%-ной нагрузке – 42% времени, при 50%-ной – 45% времени и при 25%-ной нагрузке – 12% времени. Тогда:

$$IPLV = 0{,}01 \times EER_{100\%} + 0{,}42 \times EER_{75\%} + 0{,}45 \times EER_{50\%} + 0{,}12 \times EER_{25\%}. \quad (2)$$

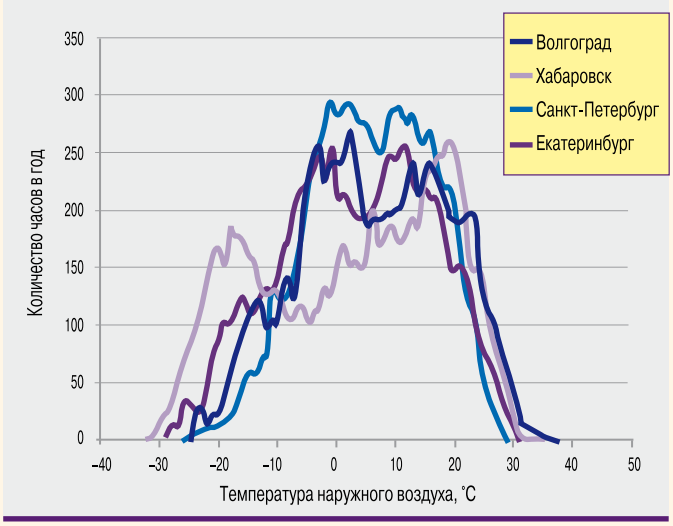
Особенность интегрального показателя при частичной нагрузке состоит в том, что длительность работы в условиях 100%-ной нагрузки принята равной 1%. Предполагается также, что при проектировании системы холодоснабжения закладывается запас в 20–30% по холодопроизводительности.

Необходимо отметить, что коэффициенты ESEER и IPLV ориентированы на территории, где они были раз-

работаны (на страны Европы и США соответственно). Коэффициенты, входящие в расчетные уравнения, не отражают таких факторов, как различные амплитуды температуры для разных климатических зон.

Различия в климатических параметрах для регионов России хорошо иллюстрируют кривые годового распределения температур для четырех городов (см. рисунок). Пики на кривых соответствуют наиболее распространенным температурам за год. Например, для Северо-Запада характерны температуры в диапазоне от –2 до +12°С (см. график для Санкт-Петербурга), на Дальнем Востоке этот диапазон смещен к значениям от +7 до +20°С (график для Хабаровска). Таким образом, территория России включает различные климатические зоны, и применять один и тот же коэффициент ESEER для всех районов страны будет некорректно.

Годовое распределение температур в разных регионах России



Климатические базы данных

При определении годового энергопотребления наиболее целесообразно использовать климатические данные для каждого отдельного региона. Климатическая информация представлена в специальных базах данных в виде массива из 365-дневного ряда почасовых значений следующих параметров: температура, влажность, солнечная радиация, направление и скорость ветра и др. Причем эти параметры должны быть наиболее близки к средним многолетним значениям.

За последние 30 лет было предложено несколько вариантов наборов таких данных — reference year (что можно перевести как «эталонный год» или «справочный год»). В литературе подробно описаны типы справочных годов и методики их расчета*. В нашей работе использованы данные для так называемого типичного метеорологического года (Typical Meteorologic Year,

* См. Вишневский Е.П., Салин М.Ю., Чепурин А.В. Расчет теплофизических характеристик атмосферного воздуха. // СОК (Сантехника, отопление и кондиционирование), № 11' 2009, с. 86.

Каждому климату – свое решение, а Крайнему Северу особенно

Егор БУРАКОВ, руководитель отдела технического сопровождения продаж компании HTS

При решении вопроса о том, необходимо ли устанавливать на объекте ту или иную систему охлаждения, одним из главных критериев является климатическая зона, в которой расположен дата-центр. Разделяя оборудование по типу охлаждения с учетом климатических условий, можно сказать, что классическая газокомпрессионная машина подходит для любых климатических зон; холодильные машины, использующие «свободное» охлаждение (фрикулинг), скорее применимы для умеренного климата, а экстремальные климатические параметры Крайнего Севера требуют специальных решений.

Используемая сегодня в климатике технология газокомпрессионного цикла хорошо зарекомендовала себя в самых разных условиях. Но, к сожалению, данные системы слабо реагируют на изменение параметров окружающей среды, в частности температуры.

Линейка прецизионных кондиционеров немецкого производителя STULZ, решения которого мы предлагаем, включает модели типа GE, обеспечивающие свободное охлаждение посредством промежуточного теплоносителя. Данная схема позволяет утилизовать естественный холод, не подавая в помещение наружный воздух даже при выключенном компрессоре холодильной машины. Система совмещает надежность газокомпрессионного цикла и энергосбережение, характерное для фрикулинга. Холодильная машина оснащена инвертором, который снижает потребляемую мощность пропорционально нагрузке в помещении ЦОДа, сохраняя номинальное значение холодильного коэффициента, что повышает экономичность использования оборудования. Наша компания предлагает в проектах не только кондиционеры, использующие такую схему, но и чиллеры внутреннего исполнения со встроенными теплообменниками свободного охлаждения.

И наконец, когда речь идет об оборудовании для охлаждения ЦОДов в России, нельзя забывать о том, что в северных районах нашей страны наружная температура воздуха может опускаться до –60°С. Для таких условий требуются не только специальные материалы, но и схемы холодильной машины, способные выдержать включение при температурах ниже –40°С. Специалисты нашей компании разработали уникальный зимний комплект, позволяющий эксплуатировать оборудование в условиях Крайнего Севера. Низкотемпературные комплекты зарекомендовали себя как надежное оборудование на объектах оператора связи «СахаТелеком» в Якутске, РАО «ЕЭС России» в Салехарде и в других проектах.

HTS® HOSSER TELECOM SOLUTIONS

Энергопотребление системы холодоснабжения ЦОДа в течение года в разных климатических зонах

Холодопроизводительность		Потребляемая мощность, кВт	Санкт-Петербург			Волгоград			Екатеринбург			Хабаровск		
			Время работы		Энергопотребление, кВт	Время работы		Энергопотребление, кВт	Время работы		Энергопотребление, кВт	Время работы		Энергопотребление, кВт
кВт	%		%	ч		%	ч		%	ч		%	ч	
1640	100	586	25	2179	1 276 894	8	716	419 576	19	1700	996 200	14	1250	732 500
1230	75	366	43	3760	1 376 160	51	4499	1 646 634	45	3928	1 437 648	48	4181	1 530 246
820	50	210	32	2821	592 410	41	3545	744 450	36	3132	657 720	38	3329	699 090
410	25	87	0	0	0	0	0	0	0	0	0	0	0	0
Итого					**3 245 464**			**2 810 660**			**3 091 568**			**2 961 836**
«Условный» ESEER					3,39			3,53			3,48			3,49

TMY), распространяемые компанией Meteonorm. В базах Meteonorm содержатся данные за период с 1961 по 1990 гг. с 7400 метеостанций по всему миру, из которых более 500 станций находятся в России.

«Типичный метеорологический год» состоит из двенадцати «типичных метеорологических месяцев» (typical meteorological months, TMM), выбранных из многолетней базы данных. Отбор TMM основан на статистическом анализе и оценке четырех климатических параметров: общей солнечной радиации (GSR), температуры по сухому термометру (DBT), температуры точки росы (DPT) и скорости ветра (WS). Месяцы отбирались по сложной методике с использованием статистической величины Finkelstein-Schafer (FS). В результате были отобраны месяцы, наиболее близкие к средневзвешенному значению по данным многолетних наблюдений. Таким образом, в набор данных TMY включены месяцы из нескольких разных годов.

Энергоэффективность системы холодоснабжения для разных регионов

В качестве примера рассмотрим систему холодоснабжения ЦОДа на базе винтового чиллера с асимметричным регулированием производительности** мощно-

** Этот подход обсуждался в статье авторов «Резервирование и оптимизация систем холодоснабжения ЦОДов», «ИКС» №12'2010, с. 89.

Главный фактор в расчетах – загрузка серверов

Виктор ГАВРИЛОВ, технический директор компании «АМДтехнологии»

Раздел, посвященный мероприятиям по обеспечению энергосбережения, становится неотъемлемой частью любого проекта ЦОДа. Расчетные данные по затратам на электроэнергию необходимы, в числе прочего, для выбора концепции построения системы кондиционирования и для сравнения различных подходов к отводу тепла.

Системы кондиционирования основных типов делятся на два класса. В одних для ассимиляции теплопритоков в течение всего года используются холодильные машины или фреоновые кондиционеры; в системах другого класса работоспособность ЦОДа большую часть года обеспечивается за счет разности температур воздуха снаружи и в обслуживаемом помещении, а холодильные машины подключаются только при пиковых нагрузках или не подключаются вовсе. Для корректного сравнения вариантов важно привести рассматриваемые системы к общему знаменателю, т. е. сравнивать их в одинаковых условиях. Здесь важны все основные показатели работы оборудования: температура воздуха в холодном коридоре, температура нагретого воздуха, забираемого системой кондиционирования, суммарный расход воздуха, потребление энергии в различных режимах работы.

Иногда в ходе сравнения проектировщики допускают ошибку при оценке коэффициента энергетической эффективности холодильных машин (EER), подменяя его коэффициентом ESEER – сезонной энергетической эффективности (он учитывает изменение нагрузки на холодильную машину в зависимости от температуры наружного воздуха в течение года). Это правомерно для систем комфортного кондиционирования и вентиляции, так как при уменьшении наружной температуры уменьшаются и теплопритоки в помещениях, соответственно, снижается нагрузка на холодильные машины. Но для ЦОДа нет прямой зависимости между нагрузкой на систему холодоснабжения и изменением температуры наружного воздуха, загрузка чиллеров в любое время года связана только с загрузкой серверов. Безусловно, чиллеры не работают все время со 100%-ной загрузкой, безусловно, при снижении температуры наружного воздуха потребляемая мощность холодильной машины несколько уменьшается (за счет снижения температуры конденсации), но, чтобы оценить разгрузку холодильных машин, необходимо прежде всего знать, как меняется в течение года нагрузка на серверное оборудование.

стью 1640 кВт. Анализ энергоэффективности проводили двумя способами: рассчитывая стандартные коэффициенты энергоэффективности (ESEER и IPLV) и на основании данных климатической базы Meteonorm.

В первом случае коэффициент энергоэффективности ESEER, рассчитанный по формуле (1), составил:

$$ESEER = 0{,}03\times(1640/586) + 0{,}33\times(1230/366) + 0{,}41\times(820/210) + 0{,}23\times(410/87) = 3{,}87.$$

Коэффициент энергоэффективности IPLV, рассчитанный по формуле (2), составил:

$$IPLV = 0{,}01\times(1640/586) + 0{,}42\times(1230/366) + 0{,}45\times(820/210) + 0{,}12\times(410/87) = 4{,}28.$$

При расчете энергоэффективности на основании базы данных Meteonorm вычисления проводились для четырех городов России, находящихся в разных климатических зонах: Санкт-Петербург, Волгоград, Екатеринбург и Хабаровск (результаты расчета представлены в таблице).

В расчете также учитывалось неравномерное распределение в течение суток нагрузок на холодильное оборудование от потребителей, основная доля которых – это нагрузки от работающих вычислительных средств. Общая же расчетная холодопроизводительность (1640 кВт) оставалась в каждом случае одной и той же.

Сравнение показало, что разброс в значениях энергопотребления для рассматриваемых городов достигает 13,4%. В то же время, как видно из расчета, коэффициент сезонного энергопотребления ESEER и показатель IPLV завышены по сравнению с «условными» ESEER, рассчитанными на основе отдельных коэффициентов для каждого города.

Такие результаты объясняются тем, что большую часть времени чиллер работает при высоких нагрузках (от 50 до 100% от максимальной), а в режиме 25%-ной нагрузки (с максимальным EER) практически не работает. Дело в том, что климатическая составляющая в нагрузке на чиллер составляет меньшую часть, а основная нагрузка приходится на работающие вычислительные устройства.

Отметим, что более серьезное влияние на энергоэффективность системы холодоснабжения ЦОДа оказывает тип системы охлаждения. В зависимости от внешних климатических условий и стоимости необходимых энергоресурсов в разных регионах страны в ЦОДах применяются следующие системы холодоснабжения:

- на базе чиллеров с центробежными компрессорами на магнитных подшипниках;
- на базе чиллеров с фрикулингом;
- система тригенерации на базе абсорбционных чиллеров;
- система адиабатического охлаждения.

Более подробное сравнение различных схем холодоснабжения в зависимости от климатических условий и тарифов на энергоресурсы в том регионе, где расположен дата-центр, мы проведем в следующей статье.

Некоторые выводы

Использование в расчетах климатической информации по регионам России, отражающей особенности разных климатических зон, позволяет точнее определить действительное энергопотребление систем поддержки микроклимата в ЦОДе, чем с помощью стандартных коэффициентов энергоэффективности (ESEER и IPLV).

В то же время в нагрузке ЦОДа основная часть приходится на электронное оборудование (серверы), а не на климатическую составляющую. Поэтому различия в энергопотреблении в зависимости от региона при прочих равных условиях невелики (по результатам нашего исследования – не более 13,5%).

В связи с этим представляет значительный интерес анализ схем микроклиматического обеспечения ЦОДа в зависимости не только от климатических параметров, но и от стоимости энергоресурсов в различных регионах нашей страны. ИКС

Бессменный часовой

Организация системы физической безопасности в здании ЦОДа

В списке систем, необходимых для функционирования ЦОДа, обязательно присутствует комплекс, обеспечивающий его физическую защиту. Функции и состав этого комплекса стоит продумать еще на стадии составления технического задания на инженерную инфраструктуру дата-центра.

Елена КУРГАШЕВА,
ведущий инженер
по ТСБ компании
«АРМО-Системы»

Архитектурно ЦОД может быть выполнен как выделенная часть внутри здания или как отдельно стоящее строение. Мы будем рассматривать второй вариант как более общий. В качестве начальных условий также примем, что все помещения вычислительного центра являются отапливаемыми и в них отсутствует агрессивная и взрывоопасная среда.

Физическую безопасность ЦОДа обеспечивают два комплекса инженерных систем: технические системы безопасности (ТСБ) и автоматические проти-

вопожарные системы. Комплекс ТСБ состоит из следующих подсистем:

- охранно-тревожной сигнализации (СОТС);
- видеонаблюдения (СВН);
- контроля и управления доступом (СКУД).

Поскольку речь идет об отдельно стоящем здании, особое внимание необходимо уделить защите периметра.

В целях повышения безопасности объекта, а также для взаимного усиления подсистем рекомендуется их интегрировать, что даст возможность проводить их общий мониторинг и настройку из единого интерфейса. Такие решения есть у компаний Bosch Security Systems, Honeywell Security Group, Siemens и Lenel International, причем они способны обеспечить не только интеграцию систем ТСБ, но и их взаимодействие с противопожарным комплексом.

Оборона по периметру

Периметр здания является первым рубежом защиты при доступе в ЦОД. Для его охраны можно применить датчики, в которых используются различные технологии: вибрационные, емкостные, проводоволновые, радиолучевые или инфракрасные. Задача этих устройств – создать контур безопасности, препятствующий несанкционированному проникновению людей на территорию вычислительного центра.

В обязательном порядке внешний периметр ЦОДа должен контролироваться системой видеонаблюдения, способной фиксировать несанкционированные действия и попытки проникновения на территорию с таким качеством изображения, чтобы злоумышленника можно было идентифицировать. Следовательно, в зоне внешнего периметра необходимо обеспечить освещенность, достаточную для надежной круглосуточной работы видеонаблюдения.

Для доступа на внутреннюю территорию в периметре устраивают КПП, оборудованные кнопками тревожной сигнализации с выводом на центральный пост службы безопасности. Как правило, КПП состоит из комнаты охраны и тамбура-шлюза, через который проходят сотрудники и посетители. Все помещения при этом контролируются СКУД. Для проезда автотранспорта пропускные пункты оборудуют автоматическими воротами с управлением с пульта/брелока и с возможностью открыть их в ручном режиме при отсутствии электропитания. Датчики безопасности, установленные на створках ворот, помогут предотвратить повреждение автомобиля, находящегося в их створе. В дополнение к воротам регулировать проезд автотранспорта через КПП помогают шлагбаумы, управляемые СКУД или вручную.

Необходимо учесть, что видеонаблюдение в зоне контрольно-пропускного пункта должно охватывать внешние и внутренние зоны объекта, прилегающие к КПП, а также его внутренние помещения. В идеале въезжающий на территорию ЦОДа автотранспорт должен контролироваться не менее чем тремя камерами СВН, фиксирующими передний номер въезжающего автомобиля, лицо водителя и диагональный вид на автомобиль с задней стороны. И конечно, на КПП необходимо установить светильники, обеспечивающие работу видеокамер в ночное время.

Средства сигнализации

Охранно-тревожная сигнализация – необходимая часть комплекса ТСБ. Как правило, она состоит из средств обнаружения несанкционированного проникновения на охраняемую территорию и приемно-контрольных приборов, которые интегрируются в общую систему безопасности ЦОДа. Помимо рассмотренной ранее периметральной защиты, СОТС выполняет задачу охраны всего комплекса дата-центра. Все значимые двери (например, аварийные и запасные входы на этажах) в обязательном порядке оснащаются магнитоконтактными извещателями (герконами), а также ИК-датчиками. На оконные конструкции, как минимум во всех помещениях первого этажа, устанавливаются извещатели «на открывание» и датчики разбития стекла.

Особое внимание следует уделить защите машинных залов и серверных. Здесь, помимо герконов и ИК-датчиков, на дверях (первый рубеж) необходимо смонтировать объемные извещатели (или комбинированные ИК + СВЧ – второй рубеж), которые будут сигнализировать на контрольную панель о несанкционированном доступе в помещения. Чтобы сделать охрану машинных залов более надежной, их стены по периметру рекомендуется оснастить датчиками «на пролом». Также не стоит забывать о необходимости установки герконов на дверях, ведущих в технические помещения: венткамеры, электрощитовые и т.п.

Дополнительно отметим, что возможны внештатные ситуации, которые фиксируются визуально сотрудниками службы безопасности дата-центра, например несанкционированное проникновение или угроза жизни людей. Для оповещения о таких ситуациях дежурные службы стоит обеспечить тревожными радиокнопками с радиусом действия, соответствующим размерам объекта. С этой же целью используются проводные тревожные кнопки скрытой установки.

Желательно, чтобы постановка (снятие) помещений на охрану могла выполняться как дистанционно, с рабочего места оператора, так и локально с помощью клавиатуры, при этом большое значение имеет интеграция охранной сигнализации с системой контроля доступа.

СКУД: контроль и учет

Эта система призвана обеспечить только санкционированный проход через двери, оборудованные элементами СКУД. Поскольку в ЦОДах есть помещения разного назначения, требующие разного уровня защиты, то логично преду-

смотреть при организации СКУД возможность разграничения прав доступа для сотрудников.

Как правило, точки доступа располагаются в следующих зонах объекта: внешние входные двери, двери машинных залов и помещений кроссовых и кабельных вводов, вход на склад и т.п. Для корректной работы СКУД все двери, попадающие под защиту этой системы, необходимо оснастить электромагнитными или электромеханическими замками, доводчиками и конечно же считывателями.

В зависимости от важности защищаемого СКУД помещения можно рекомендовать различные технологии идентификации сотрудников и посетителей. Так, если это обычная входная группа, то достаточно будет установки бесконтактных считывателей карт, а вот доступ к особо важным помещениям, таким как серверные и машинные залы, желательно ограничить с помощью более надежной биометрической системы контроля доступа.

Грамотно организованная СКУД поможет организовать на объекте учет рабочего времени персонала. Для этого необходимо установить в требуемых зонах считыватели как на вход, так и на выход, а в систему при создании заложить возможность формирования отчетов о времени прохода сотрудников. Дополнительно можно предусмотреть фотоверификацию персонала при проходе через точку доступа: после считывания карты или отпечатка пальца на монитор охранника будет автоматически выводиться фотография и дополнительные данные о сотруднике.

Всевидящее око СВН

Основное требование, предъявляемое к любой системе видеонаблюдения, – это обзор всех охраняемых зон и трансляция «картинки» в режиме реального времени. Поскольку необходима интеграция видеонаблюдения с другими составляющими комплекса ТСБ, видеосистему однозначно следует ставить сетевую. К тому же в дата-центре уже есть все необходимые коммуникации и инфраструктура для IP-камер, а сетевое видео легко настроить с помощью удаленного доступа (разумеется, доступ должен быть защищен системой паролей). Учитывая специфику ЦОДа, для обеспечения высокого уровня безопасности мы бы рекомендовали использовать СВН с возможностью идентификации лиц и отслеживания перемещений людей по объекту.

Еще один важный момент – обеспечение непрерывной мультиплексированной записи видеоинформации на жесткие диски. Исходя из нашего опыта, желательно иметь дисковую память с емкостью, достаточной для хранения видеоархива за 30-дневный период. Возможность копирования фрагментов видео на внешние носители в виде «роликов» или фотоизображений на фоне текущего режима записи обеспечит дополнительные удобства при эксплуатации СВН.

Здесь же следует отметить, что при организации периметрального видеонаблюдения, будь то внешний периметр территории или периметр здания дата-центра, контроль охраняемых участков должен вестись с обязательным «перехлестом» зон наблюдения соседних телекамер и с использованием ИК-прожекторов. Лучший вид оборудования для данных целей – это фиксированные видеокамеры, заключенные в термокожухи.

Еще раз об интеграции

Самый увлекательный момент в создании комплексной системы безопасности любого объекта – это сведение всех подсистем в целостный интегрированный организм (см. рисунок), отдельные «органы» которого должны чутко реагировать на изменения, происходящие в любой части целостной системы. Интеграция подразумевает также наличие единого интерфейса для мониторинга и настройки всех подсистем ТСБ. Продолжая аналогию с живым организмом, можно сравнить рефлексы, на уровне которых все живое борется с внешними и внутренними неблагоприятными факторами, с пользовательскими сценариями, которые мы можем задать в рамках интегрированной системы безопасности. Эти сценарии определят способы реагирования комплексной системы на различные события и станут своего рода ее рефлексами.

Интегрированная система обладает также интеллектуальной

Структура интегрированной системы безопасности

составляющей: она использует алгоритмы, позволяющие выявить потенциально опасные ситуации и привлечь к ним внимание оператора. Тем самым повышается эффективность защиты и минимизируется влияние человеческого фактора.

Чтобы реализовать интеграцию такого уровня, все крупные производители комплексных систем безопасности предоставляют специализированное программное обеспечение. Например, у Lenel это платформа OnGuard, у Bosch – BIS, у Honeywell – Winmag. Каждая из этих систем поддерживает взаимодействие в режиме реального времени подсистем охранной сигнализации, контроля доступа и видеонаблюдения. Таким образом, событие, зафиксированное одной подсистемой, будет тут же передано в другую, что в комплексе обеспечит правильную и своевременную реакцию оператора и позволит полностью контролировать ситуацию на объекте.

■ ■ ■

Средства физической безопасности вносят свой – и немалый – вклад в надежность и бесперебойность работы ЦОДов. Стоимость же комплекса ТСБ выглядит весьма скромно на фоне общих затрат на оборудование дата-центра. Есть ли смысл ими пренебрегать при организации подобных объектов? ИКС

Оптические разъемы LC при высокой плотности монтажа

Денис МОРГУНОВ, менеджер по развитию бизнеса, департамент оптических компонентов и систем HUBER + SUHNER AG

Рост числа эксплуатируемых портов, скоростей и дальности передачи информации требует новых подходов к организации подключения портов оборудования и СКС. Один из подходов – использование разъемов типа LC, которые выпускаются в разнообразных конструктивных исполнениях. Однако не все они эффективны в условиях высокой плотности монтажа пассивных и активных портов.

Разъем LC

Оптический интерфейс типа LC (Lucent Connector) – один из самых широко используемых сегодня типов разъемных соединителей. Разъем был представлен рынку в 1996 г. компанией Lucent Technologies и получил признание специалистов благодаря ряду преимуществ, которые получает пользователь в реальных условиях эксплуатации конечного пассивного и активного оборудования наряду с использованием SFP-трансиверов. По оценкам аналитиков, на сегодня по всему миру установлено более 60 млн коннекторов LC. В настоящее время около 30 компаний официально обладают лицензией на производство данного типа интерфейса.

Среди главных преимуществ оптического соединителя LC – возможность разместить дуплексный оптический порт на той же площади, что и медный порт RJ45 (рис. 1), к тому же в соединителе LC используется схожий механизм фиксации защелкой.

В первоначальном варианте исполнения оптическая розетка LC имела посадочные размеры, равные размерам отверстия под медную розетку, что допускало «повторное использование» существующих медных коммутационных панелей и их комбинирование.

До недавнего прошлого удельный вес оптической проводки в общем объеме кабельной системы составлял менее 10%, поскольку основные задачи подключения активного оборудования эффективно решались с помощью традиционных медножильных СКС различных категорий. Ситуация начала меняться с появлением приложений 10G Ethernet и развитием инфраструктуры сетей хранения данных, работающих по протоколу Fibre Channel, который требует более низкого уровня потерь в канале.

Ограниченность доступных площадей в машинных залах ЦОДов и общий рост числа единиц активного оборудования на единицу площади зала привели к появлению более эффективного – с точки зрения размеров, энергопотребления и охлаждения – активного оборудования. В свою очередь это заставило производителей структурированных кабельных систем адаптировать свои решения для размещения большего количества пассивных оптических портов за счет внедрения новой малогабаритной дуплексной розетки LC (так называемый тип SC foot print), посадочные размеры которой совпадают с размерами стандартной симплексной розетки SC (рис. 2).

Рис. 1. Интерфейс LC: двукратное увеличение плотности монтажа в сравнении с оптическим интерфейсом SC

Рис. 2. Розетка LC (SC foot print) в сравнении с розеткой SC (справа)

Плотность или удобство

Появление малогабаритной дуплексной розетки LC позволило повысить плотность монтажа за счет более тесного расположения портов на коммутационной оптической панели. Сегодня на одном стандартном юните высоты можно разместить до 48 дуплексных розеток LC. С точки зрения инфраструктуры ЦОДа это означает, например, возможность существенно сократить количество используемых юнитов в стойке с активным оборудованием, сделать коммутационное поле компактнее. Однако с эксплуатационной точки зрения остается нерешенным вопрос удобства обслуживания подключаемых оптических разъемов LC. Именно здесь большинству производителей СКС так и не удалось существенно продвинуться в технологическом плане.

Удобство эксплуатации любого разъемного соединения в общем случае подразумевает, что можно получить свободный доступ к оптическому разъему, не затрагивая соседние, уже подключенные соединители. Эта проблема особенно критична в условиях высокой плотности монтажа, которая сегодня характерна для центральных коммутационных оптических кроссов, а также при подключении целого ряда типов сетевых коммутаторов или маршрутизаторов.

Не секрет, что еще несколько лет назад специалисты отделов эксплуатации крайне негативно воспринимали интерфейс LC, ссылаясь на то, что он имеет крайне малые размеры в сравнении с привычным соединителем SC, что его сложно извлечь из розетки (часто производители СКС предлагали даже использовать специальный инструмент, облегчающий эту операцию), что образуется «борода» из перепутанных патч-кордов, так как защелки разъемов все время цепляются за кабель, усложняя процесс извлечения оптического шнура.

Поскольку плотность подключений в случае LC выше в два и более раза по сравнению с другими соединителями (например, SC), а конструктивное исполнение защелки разъема LC и медного разъема RJ45 реализовано сходным образом, то в условиях подключенных шнуров доступ к защелкам существенно ограничен (рис. 3, а). Думаю, большинство специалистов хорошо помнят лучший инструмент для обслуживания дуплексных подключений LC – обычный пинцет.

Разработчики и производители оптических разъемов LC, приняв во внимание это ограничение, внесли конструктивные изменения в форму защелки (рис. 3, б). Разнообразные варианты исполнения, предлагаемые разными производителями, предполагают, например, создание дополнительной площадки для нажатия на защелку разъема (площадка является частью либо корпуса разъема, либо дуплексной клипсы), увеличение полезной рабочей площади защелки либо усложнение геометрии ее поверхности, чтобы нажатие на защелку разъема срабатывало более эффективно.

Рис. 3. Ограниченный доступ к защелкам на разъеме LC (а) и изменения в конструктиве защелки (б)

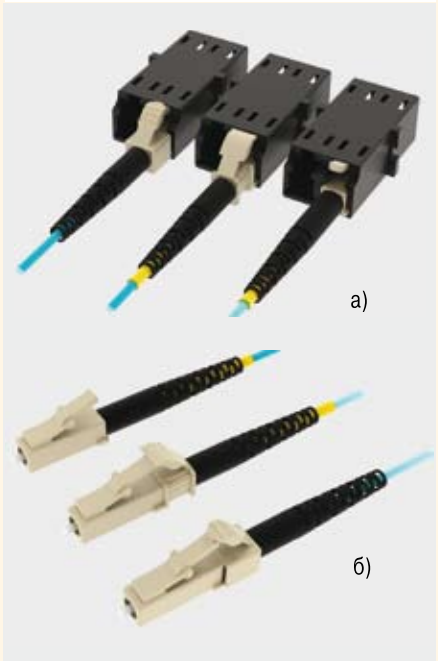
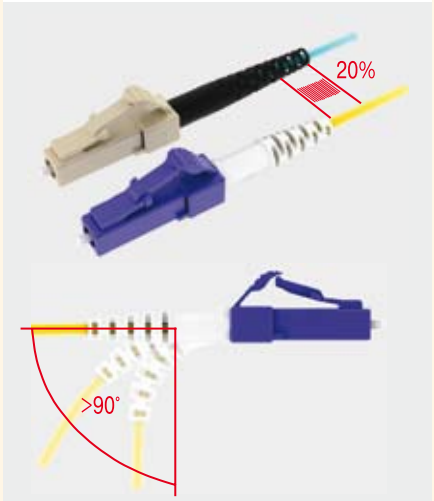


Рис. 4. Оптический разъем LC с обращенной конструкцией защелки

Наличие дополнительной площадки упрощает доступ к защелкам разъема и уменьшает перепутывание оптических шнуров. С другой стороны, в силу особенностей деформации полимерного материала и малых размеров защелки невозможно обеспечить равномерный нажим на защелки в дуплексном варианте исполнения соединителя LC. Обычно это вызывает залипание дуплексного разъема при отключении, когда одна защелка сработала, а вторая нет. Наряду с дополнительными затратами времени и сил это может привести к разрушению корпуса разъема из-за несимметричной боковой нагрузки.

Среди интересных, нестандартных решений, имеющихся на рынке, следует отметить конструктивное исполнение разъема LC с так называемой обращенной защелкой (рис. 4). Сохраняя полную совместимость с розетками стандартного исполнения, такая конструкция разъема обеспечивает хороший доступ к защелкам за счет увеличенной площадки, снижает вероятность перепутывания оптических шнуров из-за того, что кабель оптического шнура зацепится за защелку. Кроме того, в дуплексном исполнении благодаря конструкции используемой клипсы прикладываемое усилие равномерно распределяется на обе защелки.

Рис. 5. Использование укороченных гибких хвостовиков с разъемами LC



Гибкие хвостовики

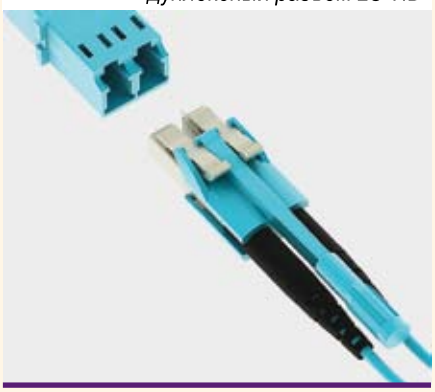
Один из альтернативных подходов, повышающих удобство обслуживания разъемных соединений LC в условиях высокой плотности монтажа, – использование укороченных гибких хвостовиков (рис. 5). Производители, предлагающие такие решения, сообщают о том, что реализуется удобный доступ к оптическим портам и что возможна безопасная выкладка коммутационных шнуров даже в условиях ограниченного пространства между плоскостью установки оборудования и дверью шкафа.

Отметим, однако, что использование укороченного тела разъема и/или гибкого хвостовика тем не менее не решает вопрос удобства доступа к защелкам самого разъема.

Конструкция LC-HD

С точки зрения эксплуатации разъемных соединений представляет особый интерес возможность комбинировать высокую плотность подключений, свойственную интерфейсу LC, с вариантом фиксации push-pull интерфейса SC. В этом случае доступ к защелкам разъемов, особенно в дуплексном исполнении, вообще не требуется. На рынке сегодня представлена такая конструкция (рис. 6) под торговой маркой LC-HD (предмет действующего патента), где аббревиатура HD означает High Density.

Рис. 6. Оптический *дуплексный разъем LC-HD*



Производитель, сохранив полную совместимость со стандартными розетками LC и трансиверами SFP/SFP+, создал решение для организации высокой плотности подключений как на коммутационных панелях, так и на картах/лезвиях активного оборудования. Главная его особенность – использование специальной клипсы, благодаря которой вообще нет необходимости в доступе к защелкам разъемов.

Предлагаемое конструктивное решение одинаково эффективно работает в случаях горизонтальной и вертикальной ориентации розеток LC или оптических трансиверов, например на лезвиях тяжелого многопортового коммутатора (рис. 7).

Прикладывая к защелкам разъемов равномерное и симметричное усилие, пользователь может подключить или отключить дуплексный разъем от порта коммутатора практически вслепую – это типичная ситуация, например, при использовании лезвий с сверхплотным монтажом трансиверов.

Немного о перспективах

И в заключение хочется обратить внимание на особый вид оптического дуплексного интерфейса – mini-LC. Это решение возникло как следствие попытки увеличить плотность монтажа трансиверов на лезвии коммутатора. Характерной его особенностью является уменьшенное расстояние между геометрическими центрами разъемов – 5,25 мм вместо 6,25 мм для стандартного исполнения. Соответствующие изменения были внесены и в конструкцию трансиверов, которые получили название mini-SFP.

По-видимому, практическое будущее такого решения пока неочевидно, хотя целый ряд производителей оптических разъемов заявил о доступности для заказа разъемов mini-LC и коммутационных шнуров на их основе. В любом случае данное решение не может быть адаптировано в рамках законченной кабельной системы, так как не выполняется требование совместимости и универсальности кабельной проводки по отношению к активному оборудованию различных вендоров в машинном зале ЦОДа.

Рис. 7. Вариант организации подключений портов коммутатора

В целом же разработчики и производители пассивных компонентов находятся только в самом начале пути, и безусловно, новые интересные инженерные решения еще будут представлены вниманию рынка. ИКС

ЦОД·2012

7-я ежегодная международная конференция

издается с 1992 года
ИКС
www.iksmedia.ru

для профессионалов в области строительства и эксплуатации дата-центров
6 сентября 2012 года, гостиница Holiday Inn Sokolniki, Москва

Цели конференции:

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

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

Основные темы конференции

ЦОД - управление
- Проектирование и строительство
- Оптимизация затрат
- Стандарты и сертификация
- Управление зданием и эксплуатация
- Модернизация
- Business Continuity
- Восстановление после инцидентов
- Энергосбережение

ЦОД - сервисы
- Облачные услуги
- ИТ-аутсорсинг
- SLA

ЦОД - системы и технологии
- Системы электроснабжения
- Климатическое оборудование
- Системы управления и мониторинга
- Виртуализация и консолидация
- Серверы, системы хранения
- Сетевая инфраструктура, СКС
- Системы физической безопасности
- Информационная безопасность

ЦОД - инновации
- Модульные ЦОДы
- Новые инженерные и климатические решения

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

Более подробная информация на сайте http://dcforum.ru

Организатор – журнал «ИКС»

Системы видеоконференцсвязи высокой четкости

Устройства KX-VC600CX и KX-VC300CX создают эффект присутствия за счет передачи стереозвука и изображения FullHD с помощью видеокодека высокого разрешения H.264. Также они поддерживают работу по протоколу SIP.

KX-VC600CX позволяет проводить четырехсторонние конференции в формате FullHD. KX-VC300CX в базовой комплектации представляет собой более экономичный вариант для двусторонних совещаний с качеством изображения до 720p.

Стабильная связь по сетям общего пользования обеспечивается технологией Panasonic AV-QoS. Воспроизведение речи без помех и прерываний достигается за счет полнодуплексной передачи звука и функции эхокомпенсации, подавляющей эхо и микрофонный эффект. При этом звук не теряет четкости даже при наложении голосов или одновременном разговоре нескольких участников. Кроме того, к KX-VC600CX можно подключить до четырех цифровых микрофонов с функцией распознавания направления звука.

Обе модели дают возможность дополнительно использовать в качестве источника видеосигнала ПК или FullHD-видеокамеру. Они могут интегрироваться в уже имеющиеся системы и применяться совместно с системами других производителей.

Для систем ВКС, реализованных только на оборудовании Panasonic, имеется облачный сервис NAT Traversal на базе удаленных серверов. Он устраняет необходимость арендовать выделенный IP-адрес и производить сложные настройки маршрутизатора.

Подключение специальной камеры, очков, дисплея/проектора позволяет проводить видеоконференции в формате 3D.

Panasonic: (495) 661-3213

Дисковая система хранения
для динамических инфраструктур

Модульная архитектура ETERNUS DX8700 S2 позволяет начать строить корпоративную СХД на базе небольшой системы и наращивать емкость хранения вплоть до 4608 Тбайт, добавляя отдельные диски или целые дисковые модули. В максимальной конфигурации в ETERNUS DX8700 S2 устанавливается 1536 дисков 3,5” или 3072 диска 2,5”, работой которых управляют восемь контроллерных модулей (поддерживается также возможность установки твердотельных жестких дисков SSD).

Для одновременной работы в сетях разных типов система оснащена интерфейсами Fibre Channel (до 8 Гбит/с), FCoE (10 Гбит/с) и iSCSI (1 или 10 Гбит/с), общее число внешних портов может достигать 128. Все модули системы ETERNUS DX8700 S2 предназначены для размещения в стандартной 19” стойке, дисковые модули имеют высоту 2U, а контроллерные модули – 19U. Энергопотребление ETERNUS DX8700 S2 в максимальной конфигурации – около 76,5 КВт.

Для управления системой хранения предназначено унифицированное ПО ETERNUS SF, использующее технологии виртуализации, «тонкого» выделения ресурсов (thin provisioning) и защиты данных («самошифрующиеся» жесткие диски), функции репликации, резервного копирования и автоматического восстановления данных. Это ПО обеспечивает дифференцированное распределение системных ресурсов в соответствии с приоритетами производительности разных приложений.

Fujitsu: (495) 730-6220

Преобразователь
постоянного тока для телекома

Устройства CPS 1500B предназначены для обеспечения электропитания телекоммуникационного оборудования в диапазоне напряжения +24 В/-48 В и -48 В/+24 В.

КПД CPS 1500B достигает 95%. Благодаря компактным размерам (высота 1U) и расширенному диапазону рабочих температур преобразователи пригодны как для наружной, так и для внутренней установки, освобождая до 83% полезной площади в стойке для основного оборудования. Вентилятор охлаждения с регулируемой скоростью вращения обеспечивает практически бесшумную работу. Наличие задних разъемов и возможность подключения под напряжением упрощают монтаж.

Начало продаж CPS 1500B в России планируется с марта 2012 г.

Delta Electronics: (495) 644-3240

Прецизионные кондиционеры

Климатические агрегаты STULZ CyberAir3 предназначены для охлаждения дата-центров и серверных помещений. Они оснащены электронными терморасширительными вентилями (ЭТРВ) Carel, поддерживают оптимальный уровень производительности и обеспечивают эффективность работы кондиционера. Прирост производительности может достигать 37% в сравнении с обычными ТРВ.

Эффективность эксплуатации увеличивают также установленные в CyberAir3 модернизированные EC-вентиляторы с крыльчаткой из армированного стекловолокна и улучшенные аэродинамические характеристики корпуса кондиционера, полученные в результате CFD-моделирования.

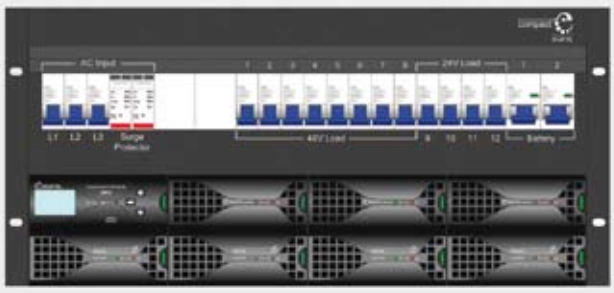
Наличие в CyberAir3 инверторного компрессора Mitsubishi с бесщеточным двигателем постоянного тока позволяет регулировать холодопроизводительность, изменяя число оборотов ротора в зависимости от фактической тепловой нагрузки.

Установки обладают холодопроизводительностью от 18 до 212 кВт и могут работать как на конденсорной или холодной воде, так и на трех различных хладагентах (R407C, R410A, R134a). Линейка CyberAir3 охватывает восемь различных типов систем кондиционирования, представленных в пяти типоразмерах.

HTS: (812) 363-1193, (495) 661-7574

Система электропитания постоянного тока

Оборудование PSC140705 входит в линейку продукции Enatel 5U Maxi Compact на 48 В мощностью до 14 кВт и использует в работе до семи выпрямительных модулей RM2048XE (2000 Вт, 48 В) с возможностью «горячей» замены, а также русифицированный модуль контроля и управления серии SM32. КПД выпрямителей RM2048XE достигает 94%, удельная мощность – 1,44 Вт/см^3. Системный контроллер SM32 способен одновременно контролировать и управлять выпрямителями, конверторами и инверторами (общим числом до 126 модулей), являясь при этом единым коммуникационным узлом аварийных сигналов и данных как системы электропитания, так и прочего подключенного оборудования (массивов резервных АКБ, систем кондиционирования, безопасности, противопожарной сигнализации и пр.). Контроллер оснащен ЖК-дисплеем, кнопками для оперативной настройки, встроенными RS232-, RS485- и mini-USB-портами и SNMP-адаптером.



Система выполнена в виде законченного металлического 19" рэка и имеет в своем составе: 15 нагрузочных и четыре батарейных автомата, защиту АКБ от глубокого разряда LVD, варисторную высоковольтную защиту по входу SPD, температурный датчик и кабель симметрии батареи и т.п.

Входные характеристики: подключение одной или трех фаз, рабочий диапазон переменного напряжения 85–300 В с частотой 45–65 Гц. Выходные характеристики: напряжение в диапазоне 43–58 В мощностью до 14 кВт, максимальный ток до 291 А.

ЗАО «Позитив» (ГК ЛПМ): (495) 979-9901

Монтажный конструктив
с встроенным жидкостным охлаждением

Мощность охлаждения 19-дюймового конструктива VARISTAR LHX 80 достигает 80 кВт. В универсальную платформу VARISTAR интегрированы два охладительных регистра (на фото) мощностью по 40 кВт, ориентированные встречно. Охлаждающий агент – вода или гликолевый раствор. Каждый из регистров содержит семь регулируемых вентиляторов hot-swap. Управление режимом охлаждения осуществляют встроенные в регистры контроллеры, также подключаемые к системе.

Производительность вентиляторов составляет 8000 м^3/ч. Температура воздуха на выходе охлаждающих регистров – 18–30°C с шагом 0,1°C. Точность поддержания режима – ± 2°C. Температура воды на входе регистров должна находиться в диапазоне 6–15°C, при выходе за диапазон указанная точность регулировки не обеспечивается.

Стандартная поставка осуществляется под напряжение 230 В (50/60 Гц), по запросу возможно исполнение под трехфазное напряжение 380 В или 48 В постоянного тока. Нормальное/максимальное энергопотребление – 2240/3220 ВА (1840/2304 Вт).

Schroff: (495) 730-5253

Блог, еще раз блог!

Владимир ЛИТВИНОВ

Думал ли я двадцать лет назад...

>>>> ...что с моим другом Левой, с которым на курортных пляжах «раздевал» в преферанс мужичков с пивными животиками, буду общаться регулярно по скайпу, находясь по разные стороны океана.

Думал ли я, что один мой знакомый Алексей, простой (а может, и нет) советский молодой человек, который успешно «втюхивал» в 90-е годы МПС и«междугородкам» секонд-хэнд компьютеры IBM, станет миллиардером и войдет в пятьдесят крупнейших олигархов России, а тысячи ветеранов-связистов, выйдя на заслуженный отдых, будут барражировать на уровне прожиточного минимума.

Кстати, зарплата президента крупнейшей телекоммуникационной компании двадцать лет назад превышала пенсию максимум в пять раз, а теперь в 250 раз!

За прошедшее двадцатилетие российская телефонная сеть осуществила полноценный кругооборот: от единого пространства до полной децентрализации компаний связи, и в итоге восстановление в единую телекоммуникационную сеть с консолидацией активов в рамках большого «Ростелекома».

Должен сказать, что несмотря на частые реорганизации акционерных компаний связи, доля пропорциональных затрат на телефонию, в отличие от большинства социально значимых услуг (ЖКХ, продукты питания, лекарства и т.д.), практически не изменилась. А при пользовании телефонной связью через Инет затраты практически обнуляются.

Уходит в безвозвратное прошлое уникальный советский социум. Общество меняется на глазах, и с этим надо жить. Инфокоммуникации развиваются фантастическими темпами, двадцать лет назад представить это было невозможно, так же как трудно представить, что будет с этой сферой еще через двадцать лет (киберпространство, «умные» дома, тотальные видеонаблюдение и электронные услуги, видеоблоги, цифровое ТВ, ликвидация текстового общения и т.д.). Жизнь интересная все-таки штука, хотя и бежит очень быстро. Главное – рассчитать свои силы на этой дистанции, берегите себя.

комментировать

Дмитрий КУТЯВИН

Символичный Возняк

>>>> Одна из самых интересных моделей смартфонов, выпущенных недавно, – Galaxy Nexus. Мое внимание привлекло обсуждение того, кто первым получил этот смартфон в США. Этим человеком оказался Стив Возняк. Возняк вместе со Стивом Джобсом в 1976 г. основал Apple. Он придумал первый персональный компьютер, с которого началось развитие компании Apple. А сейчас он будет пользоваться продукцией Google и Samsung.

Достаточно символично.

комментировать

Алексей МИШУШИН

Роскомнадзор и районный суд

>>>> Роскомнадзор на своем сайте разместил сообщение о том, что ведущим операторам, оказывающим телематические услуги связи, направлены письма о необходимости выполнения решения Никулинского районного суда г. Москвы от 12.09.2011 об ограничении доступа к признанному экстремистским интернет-сайту ******.com, а также его зеркалам.

Данное требование, признаюсь честно, удивляет. И дело не в том, что есть какие-то возражения идеологического или правозащитного характера. Напротив, я убежден, что легально определив термин «экстремистская деятельность» и порядок признания поведения экстремистским, правоохранительные органы обязаны последовательно искоренять данное явление.

Озадачило другое. Правовое основание приостанавливать доступ к тем или иным ресурсам в сети Интернет у операторов связи в настоящее время отсутствует. Да-да, отсутствует!

Но есть же решение Никулинского районного суда г. Москвы! Можно ли игнорировать его? Вправе ли мы не обращать внимание, что вышеуказанный сайт и его зеркала отдельным пунктом занесены в федеральный список экстремистских материалов, который ведет Министерство юстиции РФ?

С правовой точки зрения названные обстоятельства не имеют значения.

Операторов не уличишь в распространении экстремистских материалов, запрещенном ст. 13 закона «О противодействии экстремистской деятельности», поскольку согласно ст. 2 закона от 27.07.2006 № 149-ФЗ термин «распространение информации» означает действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. Именно действия, т.е. активное поведение...

Между тем, как предписано в п. 4 раздела XVI «Перечня лицензионных условий осуществления деятельности...», предусмотренного постановлением Правительства РФ от 18.02.2005 № 87, оператор связи обеспечивает абоненту и (или) пользователю доступ к информационным системам инфокоммуникационных сетей, в том числе к сети Интернет. При этом под доступом к информации понимается возможность получения и использования информации.

Подметили разницу? «Распространение» предполагает активность поведения распространителя, а «доступ» – это только возможность, предоставляемая абоненту.

Таким образом, на мой взгляд, операторам связи ДЕЙСТВУЮЩИМ СЕГОДНЯ ЗАКОНОДАТЕЛЬСТВОМ не установлены запреты в организации доступа к ресурсам Интернета. Операторы не могут нести ответственность за неисполнение вышеуказанного требования.

комментировать

Лева со скайпом, Алексей-миллиардер с секонд-хэндом, три фирмы и один цех, надзор и экстремистские сайты, Apple и его создатели, солнечные бури… В блогосфере IKSMEDIA.RU, как в жизни, есть все! Итак, блог, еще раз блог!

Наталия КОРОТКОВА

«Хоботов, это мелко»

>>>> Коллега-журналист поделился, что писал в одно отраслевое издание статью о провинциальном предпринимателе, наладившем бизнес с нуля и теперь владеющем тремя фирмами, одна из которых занимается производством, вторая – реализацией, а третья – учетом спроса и стратегическим планированием. Узнав о том, что «три фирмы» представляют собой крошечный цех с одним работником и пару точек реализации продукта, журналист презрительно сказал: «Как этот человек может пафосно напутствовать молодежь, как добиться успеха, ведь у него такой мелкий масштаб деятельности?».

Я незнакома с деятельностью этого предпринимателя, но позиция «маленький не может быть успешным» показалась мне знаковой для эпохи глобализации.

Недавно я предложила своим студентам кейс-стади по инновационному менеджменту, в котором рассказывалось, как один-единственный предприниматель из США самостоятельно разработал и наладил производство миниатюрных водонагревателей для походов и в первую неделю после открытия онлайн-бронирования на сайте любителей пеших прогулок на природе продал сто штук. Сто маленьких водонагревателей – это много или мало? Можно ли это считать успехом?

Я твердо убеждена, что да, потому что по соотношению затраты – выпуск это прибыльный проект, востребованный в масштабах своей рыночной ниши. Хотя доходы от этого проекта не позволят изобретателю поехать в Куршавель или приобрести недвижимость в Лондоне. Если руководствоваться количественным понятием успеха, то нужно брать интервью у Березовского и Абрамовича. Вроде бы это успех, но, простите, на чем он основан? По мне так лучше один рабочий, маленький цех и сто водонагревателей, проданных через сайт.

комментировать

Александра КРЫЛОВА

Банки продолжают мобилизацию клиентов

>>>> Для мобилизации пользователей они все чаще используют специальные мобильные приложения, обеспечивающие владельцам смартфонов комфортный быстрый доступ к разнообразным финансовым услугам с их карманных устройств.

На днях сразу два банка заявили о предоставлении таких возможностей для новых категорий своих клиентов. Сбербанк РФ выпустил бесплатное приложение «Сбербанк Он@Лайн» для iPhone в дополнение к уже имеющемуся одноименному приложению для iPad. С помощью этих программных продуктов клиенты банка, пользователи устройств на платформе iOS, могут проверять информацию по своим вкладам и картам, совершать переводы между ними, а также в счет погашения кредитов, осуществлять мгновенные платежи в адрес операторов сотовой связи, интернет-провайдеров и других поставщиков услуг.

В настоящее время мобильным приложением «Сбербанк Он@Лайн» для iPhone могут воспользоваться клиенты 11 из его 17 территориальных банков. Для доступа к мобильному приложению для iPhone используется идентификатор пользователя и пароль «Сбербанк Он@Лайн», получить который можно либо в одном из 55 тыс. терминалов самообслуживания, либо в контакт-центре Сбербанка.

комментировать

Стивен ЛЮ

Переживет ли Интернет космическую бурю?

>>>> В середине января мы стали свидетелями самой сильной солнечной бури за последние десять лет. Возникший при этом поток космических лучей вызвал мощное полярное сияние, но этим дело не ограничилось.

Помимо полярных сияний потоки космических лучей вызывают исключительно мощные электромагнитные бури. Они, в свою очередь, порождают скачки напряжения, способные повредить системы распределения электроэнергии, сбросить спутники с расчетных орбит и исказить данные электронных приборов. Вспомним, к примеру, отключение энергосистемы, оставившее без электричества канадскую провинцию Квебек.

Чем выше быстродействие электронных систем и чем выше плотность транзисторов на чипе, тем выше вероятность того, что внешний поток энергии сможет отрицательно повлиять на производительность маршрутизатора или коммутатора. Солнечные бури – явление редкое, но с точки зрения оператора, эксплуатирующего критически важную сеть, недопустимы даже редкие сбои и отказы.

комментировать

Реклама в номере

АМДТЕХНОЛОГИИ
Тел.: (495) 963-9211
Факс: (495) 225-7431
E-mail: info@amd-tech.ru
www.amd-tech.ru . . . с. 84

КОМПАНИЯ КОМПЛИТ
Тел.: (812) 740-3010
Факс: (812) 740-30-11
E-mail: info@complete.ru
www.complete.ru . . . с. 73

ГК ЛПМ
Тел.: (495) 979-9901
Факс: (495) 739-0566
E-mail: market@lpm.su
www.lpm.su . . . . . с. 13

AVRORAID
Тел.: (812) 622-1680
Факс: (812) 346-5834
E-mail: info@avroraid.com
www.avroraid.ru . . . . с. 76

HOSSER TELECOM SOLUTIONS
Тел.: (812) 363-1193
Факс: (812) 363-1194
E-mail: spb@h-ts.ru
www.h-ts.ru . . . . . с. 83

HUAWEI ENTERPRISE
Тел.: (495) 234-0686
Факс: (495) 234-0683
E-mail: enterprise.ru@huawei.com
www.huawei.com/ru/enterprise . . . . . 2-я обл.

INTEL
Тел.: (495) 641-4500
Факс: (495) 641-4510
www.intel.ru . . . . . с. 53

NETGEAR
Тел./факс: (495) 799-5610
www.netgear.ru . . . . с. 75

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

POWERCOM
Тел.: (495) 651-6281
Факс: (495) 651-6282
www.pcm.ru . . . . . с. 81

SAP
Тел.: (495) 755-9800
Факс: (495) 755-9801
www.sap.com . . . . 4-я обл.

SIEMENS ENTERPRISE COMMUNICATIONS
Тел.: (495) 737-1215
Факс: (495) 737-1432
www.siemens-enterprise.ru . . . с. 16–17

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

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

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

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

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