Опять падение – в рамках общерыночного тренда

Прошедший месяц оказался напряженным для мировых и российских фондовых площадок. Основной поток негативных новостей шел из-за рубежа.

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

Так, ФРС США приняла программу «Твист» – вопреки ожидавшемуся запуску очередного этапа «количественного смягчения» (QE3). Однако эта программа, кратковременно улучшающая рыночную конъюнктуру, но не способная привнести на рынок мгновенную дополнительную ликвидность, разочаровала инвесторов.

Много негатива генерировалось и в Европе. С одной стороны, так и не было найдено решения греческой долговой проблемы, хотя рынок расстраивало даже не столько это обстоятельство, сколько нерешительность еврочиновников и их неспособность совместно решать возникающие проблемы. С другой стороны, добавила пессимизма информация о снижении суверенных рейтингов ряда европейских стран, также испытывающих серьезные бюджетные проблемы.

Определенное давление оказывали на российские площадки и внутренние факторы, в числе которых как ослабление курса рубля к доллару наряду с продолжением оттока иностранного капитала, так и жесткая отставка со своих постов вице-премьера и министра финансов Алексея Кудрина, что способствовало росту неопределенности на российском рынке для инвесторов.

«Ростелеком» разочаровал

Крупнейший игрок российского телекоммуникационного сектора, объединенный «Ростелеком», за месяц потерял 10,28% капитализации – цена акции упала до 148 руб. Вероятно, инвесторов разочаровали достаточно слабые результаты оператора по итогам I полугодия 2011 г. по МСФО, согласно которым выручка «Ростелекома» выросла всего на 6% – до 71,2 млрд руб., а прирост чистой прибыли составил лишь 2% (19,1 млрд руб.).

Пессимизм инвесторов не уменьшила даже позитивная информация о подаче «Ростелекомом» заявления на листинг на Лондонской фондовой бирже (LSE). Листинг 25% обыкновенных акций класса «А» в Лондоне способен выступить положительным драйвером для стоимости акций компании, так как способствует большей прозрачности финансовых показателей и росту инвестиционной привлекательности бумаг оператора.

Акции «Таттелекома» подешевели за месяц на 7,13% – до 0,197 руб. Каких-либо значимых корпоративных новостей за обозначенный период не публиковалось, динамика бумаг эмитента по преимуществу определялась негативной общеотраслевой конъюнктурой.

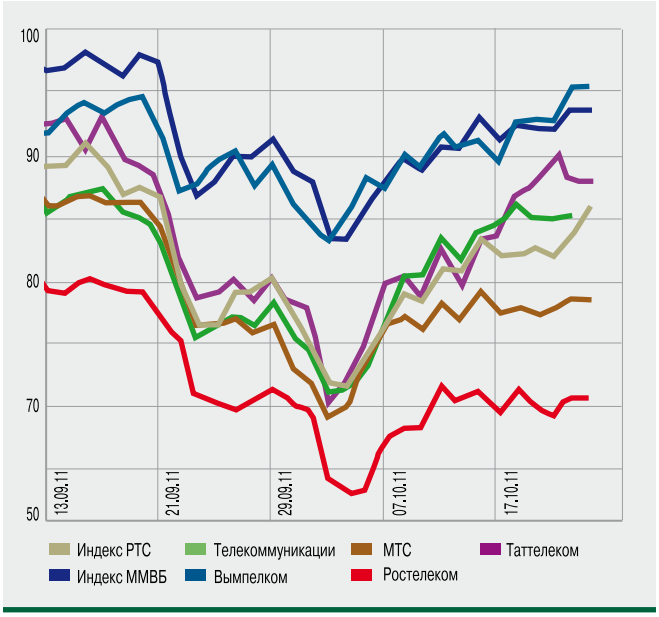
В сотовом стане неспокойно

Акции российских сотовых операторов демонстрировали снижение на уровне рынка в целом. Капитализация МТС

Справка ИКС

В условиях высокой информационной насыщенности, преимущественно негативными новостями, российский рынок акций за период с 15 сентября по 14 октября вновь демонстрировал коррекционные настроения. Индекс ММВБ за прошедший месяц потерял 6,12%, снизившись до 1431,92 пункта, в то время как долларовый индекс РТС показал небольшой прирост – на уровне 0,54%, до 1448,5 пункта. Индекс «ММВБ Телекоммуникации» в рамках общерыночного тренда ММВБ также демонстрировал снижение – до 2097,63 пункта, или на 5,71%.

Динамика биржевых индексов и индексов телекоммуникационных компаний в период с 13 сентября по 17 октября 2011 г.



снизилась на 7,79% – до 189,64 руб. за акцию. Определенное влияние на нее оказало помесячное сокращение абонентской базы оператора в августе, в то время как у ближайших конкурентов по «тройке» база, напротив, весьма ощутимо росла. Основным же негативным фактором для бумаг компании стала информация о переходе из МТС в Vimpelcom Михаила Герчука, на должность главного коммерческого директора. Переход топ-менеджера, вероятно, мог быть воспринят инвесторами как отсутствие уверенности в перспективах развития бизнеса МТС и, напротив, наличие таких перспектив у ближайшего конкурента.

В свою очередь, расписки VimpelCom на NYSE на фоне позитивных новостей, касающихся обновления топ-менеджмента, выросли на 3,61%, до $10,16. Помимо этого были опубликованы новости о том, что дочка «Вымпелкома» получила LTE-частоты в Италии, и о том, что компания осуществила прямое соединение сетей с кипрским оператором Cyta, что позитивно не только с точки зрения качества, но и с точки зрения стоимости услуг. Был и некоторый негатив для инвесторов – информация о том, что ФАС обвинила «Вымпелком» и МТС в ценовом сговоре при реализации смартфонов iPhone, что грозит операторам санкциями со стороны ведомства.

АФК «Система» потеряла около 8,9% капитализации, упав в цене до 25 руб. за акцию. Снижение происходило на фоне публикации в целом благоприятных корпоративных новостей. Компания отчиталась по US GAAP за II квартал – чистая прибыль возросла на 131,2%, до $332 млн, а выручка достигла $9 млрд, увеличившись почти на треть. Кроме того, в начале октября «Система» объявила о намерении незамедлительно начать выкуп своих обыкновенных акций и GDR, рассматривается также возможность выкупа обыкновенных акций и/или GDR ее «дочки» – МТС.

ИТ-бумаги дешевели – но не все

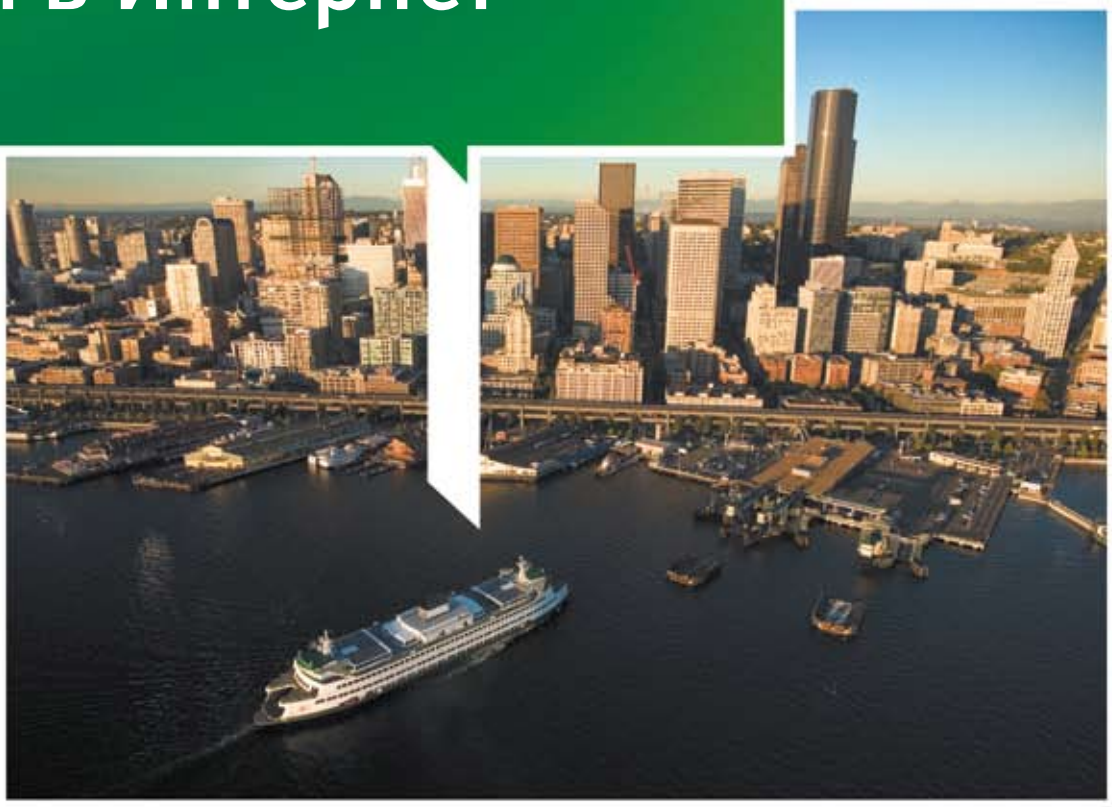
Акции «Ситроникса» демонстрировали последний месяц крайне низкую ликвидность. За этот период состоялось всего два торговых дня, последние торги на РТС по бумаге происходили 20 сентября по цене $0,011. На ММВБ акции «Ситроникса» были допущены к торгам только 30 сентября – они будут обращаться в секторе РИИ (Рынок инноваций и инвестиций). Сам факт появления такой компании в высокотехнологичном секторе примечателен для инвесторов и найдет в долгосрочной перспективе позитивное отражение в капитализации компании. Однако пока, в условиях волатильного рынка, бумаги компании на РИИ ММВБ не пользуются достаточным спросом, торгуясь на уровне 0,4 руб.

Акции «РБК-Информационные системы» потеряли за месяц более 12,6%, откатившись до 24,3 руб. Компания предложила кредиторам изменение условий кредитного соглашения, подписанного в рамках реструктуризации долга в апреле прошлого года, с тем чтобы иметь возможность использования свободных денежных средств и привлечения дополнительного финансирования. Помимо этого на состоявшемся в октябре ВОСА (внеочередном собрании акционеров) было принято решение о допэмиссии в размере 51,1 млн акций.

Бумаги российских ИТ-компаний Mail.ru Group и Yandex N.V. подешевели в прошедшем месяце сильнее акций остальных публичных участников рынка – на 15,45 и 18,73% соответственно, до $31,2 и $24,17. В течение месяца цены на акции обеих компаний опускались ниже цены размещения – такая динамика была вызвана преимущественно негативной конъюнктурой мировых финансовых рынков и вытекающей отсюда боязнью инвесторов вкладывать капитал в традиционно более рисковые ИТ-активы. В случае с Mail.ru Group дополнительное давление на бумаги компании могла оказывать ее активность в развитии новых, сомнительных с точки зрения инвесторов направлений бизнеса, в то время как держатели акций «Яндекса», вероятно, предпочли зафиксировать полученную ранее прибыль.

Бумаги IBS Group, напротив, выросли на 1,32%, достигнув отметки в $15,4 за акцию. Росту котировок, по всей видимости, способствовало существенное удешевление бумаг компании в прошлом месяце (почти на 15%), а также положительная оценка инвесторами ряда корпоративных событий. В частности, было заявлено о том, что входящая в тройку лидеров российского рынка разработчиков медицинских ИТ-систем компания «Смарт Дельта Системс» привлекла инвестиции от связанных с IBS Group структур, что позволит ей получить подряды в здравоохранении. Другой позитивной для инвесторов новостью стала информация о том, что «IBS Экспертиза» (входит в IBS Group) выиграла тендер Минобрнауки на создание общероссийской системы прогнозирования потребностей в профессиональных кадрах, что способно в долгосрочном периоде позитивно сказаться на капитализации материнской компании. ИКС

Кругосветный доступ в Интернет



Удобный роуминг от сети «МегаФон» позволит Вам всегда находиться на связи и общаться с близкими практически в любом обитаемом уголке мира.

В командировке или отпуске – «МегаФон» обеспечит Вам качественную связь для работы и отдыха. «МегаФон» является одним из лидеров в области роуминга: на сегодняшний день услуги мобильной связи доступны абонентам «МегаФона» на всей территории России, в 23 странах мира, а также на круизных лайнерах и даже в самолетах. С роумингом «МегаФона» во время отпуска и командировок Вам доступна не только голосовая связь, но и передовые услуги: мобильный Интернет, MMS и т.д.

Эти услуги активно используют наши клиенты, например Холдинг «Северсталь»:

«Компания «МегаФон» является нашим приоритетным поставщиком услуг связи на корпоративном уровне. Многие сотрудники, особенно в генеральной дирекции и управляющих компаниях, очень мобильны, и естественно, у нас потенциально большие затраты на роуминговый трафик. Причем большую часть затрат составляет не голосовой трафик, а трафик передачи данных. Сотрудники, находясь в командировке, всегда должны иметь доступ к своей корпоративной электронной почте и другим корпоративным ресурсам. К счастью, мы находим понимание у наших партнеров и нам удается оптимизировать эти затраты».

8-800-550-75-00
B2B.sales@megafon.ru

МегаФон
Связь идей и результатов

Организатор

ИКС

Партнеры

Зачем оператору услуга безопасности

Необходимые, но невостребованные. Затратные, но дешевые. Обязательные, но дополнительные. Все эти противоречивые характеристики относятся к операторским услугам информационной безопасности. «Дешифровке» их роли и места в бизнесе операторов связи был посвящен организованный «ИКС» круглый стол «Информационная безопасность как услуга оператора. Специфика внедрения и предоставления».

В дешифровке роли и места услуг ИБ в бизнесе операторов связи приняли участие:

Александр БЛОХИН, начальник отдела информационной безопасности, **МГТС**
Николай БОГОЛЮБОВ, менеджер по маркетингу, **Dr.Web**
Андрей БУГАЕНКО, директор по ИТ, **«МегаФон»**
Вадим ВАНЬКОВ, заместитель гендиректора по коммерческой деятельности, **«Комкор»**
Александр ЗОЛОТНИКОВ, руководитель департамента информационной безопасности, **Компания ТТК**
Муслим МЕДЖЛУМОВ, начальник отдела безопасности сети, **«РТКомм.Ру»**
Сергей МИШЕНКОВ, советник министра связи и массовых коммуникаций
Александр ПУШКАРЬ, менеджер сектора антивирусных услуг, **Dr.Web**
Александр СИКОРСКИЙ, начальник отдела криптографической защиты информации департамента информационной безопасности, **МТС**
Михаил СУКОННИК, региональный директор, **Radware**
Дмитрий УСТЮЖАНИН, руководитель департамента информационной безопасности, **«ВымпелКом»**
Сергей ФОМИЧЕВ, директор по развитию бизнеса, **«Мастертел»**
Дмитрий ЮФЕРОВ, консультант по продуктам безопасности, **Landata**

Вел круглый стол **Михаил ЕМЕЛЬЯННИКОВ,** консалтинговое агентство **«Емельянников, Попова и партнеры».**


М. ЕМЕЛЬЯННИКОВ

М. ЕМЕЛЬЯННИКОВ: Безопасность как услуга оператора связи – тема далеко не новая. Но для российского рынка она не нова именно в плане обсуждения: почему такая очевидная услуга продвигается с таким трудом.

Уже ясно, что значительная часть рынка, в первую очередь сегменты SOHO и SMB, не в состоянии решать проблему информационной безопасности самостоятельно – там нет ИТ- и ИБ-специалистов, нет денег, нет возможности создать инфраструктуру. Казалось бы, они должны активно откликаться на предложения услуг безопасности, самая очевидная из которых – защита от DDoS-атак. Но подвижки здесь пока невелики. Почему? Я бы на первое место среди причин поставил недостаток доверия.

М. СУКОННИК: У операторов сформировалось мнение, что со стороны корпоративных клиентов нет спроса на услуги защиты от DDoS-атак. Но корпоративные клиенты высказывают строго противоположную точку зрения: что они вынуждены покупать, например, наши решения самостоятельно, потому что операторы связи не могут предоставить им необходимый уровень защиты. «Задидосить конкурента» стало в России национальным видом спорта. Я набираю в поисковике «заказать DDoS-атаку» и получаю шесть-восемь страниц ссылок: как ее заказать, сколько она стоит, с книгами жалоб и предложений, отзывами и маркетинговыми ходами. Компании это видят и, сознавая, что «заказать» могут и их интернет-ресурс, покупают и внедряют вендорские решения защиты от DDoS-атак. Подтверждение тому – наша статистика. У Radware два основных направления деятельности –

балансировка и оптимизация трафика ЦОДов и информационная безопасность. И если по миру в среднем на безопасность у нас приходится примерно 20% оборота, то в России – 50%. Потому что здесь это актуально. Клиентам услуга нужна. Просто они не могут найти, по крайней мере у большинства операторов, тот уровень сервиса, который им требуется. Может быть, поэтому нет доверия? Наше оборудование, конечно, решает вопрос 100%-ной защиты от DDoS-атак для крупных фирм, но бизнес среднего размера, по-моему, ожидает от операторов услуги защиты в качестве элемента SLA.

А. БУГАЕНКО: Мы уже полтора года предоставляем услугу защиты от DDoS-атак и на собственном оборудовании, и на оборудовании известного вендора. Клиентов не так много, как хотелось бы. Услуга сложна для продажи клиенту, неудобна, потому что для ее оказания оператор должен «привести» клиента в свой ЦОД или как минимум на свою сеть. На чужой сети такую услугу оказывать невозможно. А корпоративный или государственный клиент, которому эта услуга нужна, вряд ли станет ради одной услуги менять оператора. И, конечно, эта услуга не окупается. Я вам ответственно заявляю: срок ее окупаемости – не при нашей жизни. Поэтому я считаю, что это не самостоятельная услуга, а часть комплексной услуги по обеспечению клиентам хорошей простой жизни с телекомом.

? → Как откликаются пользователи на предложения операторов связи по оказанию услуг защиты от DDoS-атак, есть ли реальный спрос? И, вообще, готов ли рынок эти услуги воспринимать?

М. МЕДЖЛУМОВ: Не могу сказать, что мы в «РТКомм.Ру» наблюдаем ажиотажный спрос на услугу защиты от DDoS-атак, но динамика появления клиентов все-таки положительная: за первые два квартала нынешнего года клиентов пришло столько же, сколько за весь 2010 г. В основном это клиенты, которые уже сталкивались с подобными проблемами, но немало и тех, кто осознанно подходит к вопросу защиты своих ресурсов и подключается к услуге превентивно. Думаю, что в дальнейшем эта услуга станет неотъемлемой частью подключения к Интернету.


В. ВАНЬКОВ

В. ВАНЬКОВ: У большинства крупных российских интернет-операторов услуга защиты от DDoS-атак уже внедрена и успешно предоставляется. Понятно, что решение достаточно дорогое, и не все себе могут позволить использовать именно операторское решение. Мы оказываем эту услугу корпоративным клиентам – финансовым организациям, крупнейшим электронным площадкам, а также другим операторам и их клиентам. И спрос на нее немалый. Конечно, спрос подогрет популярностью самих DDoS-атак – их скорость и мощность за три года выросли на 1000%.

А. ЗОЛОТНИКОВ: DDoS-атаки – один из наиболее распространенных сегодня видов киберпреступлений, но спрос на услуги противодействия им пока невысокий. Это говорит о том, что рынок не готов к потреблению услуг информационной безопасности. Здесь имеются в виду и предприятия госсектора, и крупные корпоративные клиенты, и сегмент SMB. Например, у ТТК есть современное оборудование и специально обученный персонал для оказания услуг по противодействию DDoS-атакам. Однако нашими клиентами являются в основном те предприятия, которые уже ощутили на себе последствия киберпреступления как в финансовом, так и в имиджевом плане.


Н. БОГОЛЮБОВ

Н. БОГОЛЮБОВ: Мы имеем большой опыт общения с массовым сектором и видим, что люди зачастую не осознают возможные риски при работе в Интернете. Поэтому операторы нередко включают антивирус в свои интернет-тарифы, чтобы его уже не требовалось оплачивать дополнительно. Таким образом пользователь получает с услугой доступа в Интернет готовую защиту, что выгодно и оператору и абоненту.

С. МИШЕНКОВ: Я буду выступать как клиент. Причем клиент, наверное, с 1992 г. Первая локальная сеть в Минсвязи была создана в НТУ, и я изначально позаботился о двух вещах. Мне совсем не хотелось, чтобы мои данные оказались у кого-то и чтобы эту сеть, так сказать, повергли. Обе задачи мы решили просто: это была локальная сеть без выхода наружу. И все! В НТУ работало 20 компьютеров, но в каждой комнате находился еще один компьютер с выходом в Интернет. Все сотрудники знали: если хоть одно письмо будет напечатано на этом компьютере – его отберут. Решение радикальное и, я считаю до сих пор, правильное. Это нас спасало, когда падали все сети, когда уродовались компьютеры по всему миру.


С. МИШЕНКОВ

С домашнего компьютера через Интернет я никаких закрытых документов, разумеется, передавать не буду, но меня бесит, что после выхода в Сеть его постоянно нужно «чистить». Хорошо, что со спамом операторы вроде научились бороться. А вот с червями, по-моему, нет. Это взгляд потребителя, и я был бы счастлив, если бы операторы меня защищали. И даже, наверное, я мог бы им за это платить. Но немного.


Д. ЮФЕРОВ

Д. ЮФЕРОВ: Действительно, информационная безопасность – это не только защита от DDoS-атак, не только антиспам, но и защита от вирусов, хакерских атак, от утечки конфиденциальных данных. На мой взгляд, сейчас на рынке эти решения практически не представлены. А заказывают не только DDoS, заказывают и хакерские атаки на ресурсы конкурентов. Я представляю решение от Palo Alto, и с большинством присутствующих здесь компаний мы не раз говорили о том, что было бы хорошо предоставлять услугу чистого канала, услугу виртуальных систем безопасности. В США, на Ближнем Востоке реализации уже есть. В России, к сожалению, работающих проектов до сих пор нет.

? → Нет спроса – нет и реализации. Давайте попытаемся понять, как операторам различных сетей связи выстраивать идеологию при предоставлении услуг информационной безопасности в разных сегментах рынка, как формировать спрос на них.


Д. УСТЮЖАНИН

Д. УСТЮЖАНИН: Сегодня все операторы просто грезят облачными сервисами. Оператору интересно стать не просто «трубой» для передачи данных, но и провайдером облачных сервисов, которые немыслимы без предоставления как бы дополнительных услуг информационной безопасности. Пока рано что-то определенное говорить про российский рынок. Но, например, коллеги из Telecom Italia говорят, что если два-три года назад первым вопросом клиентов был: «А что это за сервисы, зачем эти облака нужны?», то сейчас главный вопрос, который задает руководитель бизнеса себе и руководителю по ИТ: «А почему мы еще не сделали то-то и то-то в облаках, если это дешевле, эффективнее и, в конце концов, безопаснее?». Я считаю, что вслед за западным рынком мы через пару лет тоже придем к полному пониманию, что для бизнес-сегмента облачные сервисы очень важны. А что касается частного клиента, то ему просто необходимы операторские услуги безопасности. При подготовке к запуску услуг «Родительский контроль» и «Чистый Интернет» мы работали со специальными фокус-группами. И люди говорили, что им действительно тяжело самостоятельно справиться с вирусами, оградить детей от нежелательного контента. А первый их вопрос был: «Ну почему оператор этого не делает?».


А. БЛОХИН

А. БЛОХИН: В МГТС «Родительский контроль» уже действует, но не в полном объеме. Ранее была запущена услуга, позволяющая ограничивать время выхода в Интернет, которая первоначально продвигалась как маркетинговая, стоившая определенных денег. Но в итоге она была включена в пакет подключения к Интернету в виде бесплатного дополнительного приложения – якорной услуги. Сейчас в группе компаний МТС ведутся работы по созданию полнофункциональной конвергентной услуги «Родительский контроль» на базе сетей мобильного и фиксированного операторов, входящих в группу.

А. ПУШКАРЬ: Нашему сервису «Услуга Антивирус Dr.Web» (проект AV-Desk) уже четвертый год: услуга впервые была запущена в 2007 г. в «Корбине Телеком» для массового сектора. К настоящему времени мы внедрили сервис у более чем 350 операторов в России и за рубежом. Со стороны операторов мы видим полное понимание необходимости предоставления услуги антивирусной безопасности для массового сегмента. Для них это возможность заработать на услуге, снизить вирусную активность в своей сети и повысить лояльность абонентов.


А. ПУШКАРЬ

На корпоративном рынке, особенно это касается сегмента SMB, складывается парадоксальная ситуация. Риски информационной безопасности многие осознают, но до возникновения инцидента, ведущего к серьезным финансовым или имиджевым потерям, часто не рассматривают как критические. Я полагаю, что операторам имеет смысл более активно информировать своих клиентов об угрозах, связанных с работой в Интернете, и предлагать услуги по их нейтрализации.

А. ЗОЛОТНИКОВ: Хочу сказать несколько слов об услуге противодействия нежелательному контенту, ее важности для нашего общества и государства. Мы прекрасно понимаем ту роль, которую играет Интернет в нашей жизни. Контент во всем его многообразии, постоянно совершенствующаяся информационная надстройка Интернета, оказывает влияние на все стороны жизни государства и общества, на формирование общественного мировоззрения. В первую очередь это относится к воспитанию наших детей и молодежи. И защитить их от опасностей в Интернете – наша общая задача. Здесь и возникает такой важный аспект, как социальная ответственность оператора связи. От его позиции в этом вопросе, по нашему мнению, зависит очень многое.

Другой вопрос – использование Интернета внутри организации. Это вопрос эффективности работы сотрудников и, в конечном счете, компании в целом, ее экономики.

Что ожидает оператор от вендоров с точки зрения разработки и внедрения услуг информационной безопасности?

А. БУГАЕНКО: Оператор от любого вендора ждет конечную у с л у г у. Придите и расскажите, как на моей инфраструктуре и ваших решениях развернуть услугу, на которой я буду зарабатывать деньги. А большинство вендоров приходят и рассказывают, какое у них замечательное оборудование или софт. Но мне как оператору не нужно оборудование или софт. Мне нужно предоставить удобную и востребованную услугу клиенту. И сделать это мы можем только вместе. Потому что у меня есть сеть, а у вас – софт или железо. Если честно: знаете, почему корпоративный пользователь так прохладно относится к идее услуги антивируса, которую вендор продвигает вместе с «одним крупным оператором»? Потому что ему нужно что-то устанавливать. Если бы вы дали инструмент, который работал бы в облаке у оператора, чтобы человек просто поставил галочку и получил защиту, – услуга пошла бы.


С. ФОМИЧЕВ

С. ФОМИЧЕВ: Скажу с точки зрения оператора «второго эшелона». Только в Москве, например, работает порядка 150–200 операторов. Из них, наверное, лишь десяток могут позволить себе купить оборудование у вендора. Здесь я поддерживаю Андрея: действительно, антивирус – не самая востребованная услуга на корпоративном рынке. Но если появится модель аутсорсинга защиты от DDoS-атак и подобных услуг – оставшиеся 140 операторов станут работать в этом направлении, и проблема во многом будет решена. Речь идет не об аренде оборудования, а именно о том, чтобы было решение, которое можно использовать в аутсорсинге.

А. ПУШКАРЬ: К сожалению, не всякую услугу по обеспечению информационной безопасности можно предоставить в облаке. Обеспечить надежную антивирусную защиту персонального компьютера пользователя без установки на него агента не представляется возможным.

Наверное, оператор все же не вправе рассчитывать, что вендор создаст ему бизнес-модель. Вендор делает железо или пишет софт и продает его не только оператору связи, но и конечному пользователю, и крупному корпоративному клиенту, и в SMB. Хотелось бы услышать, по каким критериям оператор выбирает поставщика решений для реализации сервисов безопасности?

М. МЕДЖЛУМОВ: Выбирая решения по безопасности, мы стараемся тестировать продукты как зарубежных, так и российских вендоров. Например, в двух недавних проектах остановились на отечественных решениях. Почему? При более низкой стоимости их качественные характеристики не хуже. Кроме того, производители готовы доработать продукт под конкретные требования оператора, в частности выбранный нами вендор подготовил APS-пакет для интеграции с облачной платформой «РТКомм.Ру».


А. БУГАЕНКО

А. БУГАЕНКО: А у меня такой вопрос к вендорам: готовы ли они к тому, чтобы оператор инвестировал в них в обмен на создание для него эксклюзивных решений? Мне кажется, что это вполне внятная модель взаимодействия. Мы такую модель используем в течение трех лет: инвестировали в вендора, в нужное нам оборудование и ПО, получили его, и теперь на основе разделения доходов бизнес имеет и наш вендор, и мы сами.


А. СИКОРСКИЙ

А. СИКОРСКИЙ: При выборе вендора оператор должен руководствоваться следующими критериями. У разработчика программно-аппаратных средств должно быть налажено промышленное производство, он должен уметь произвести свой продукт. То есть разработчик должен быть достаточно крупной компанией. Затем вопрос доверия. Ориентироваться нужно именно на испытанные, отработанные и сертифицированные технологические решения; на компании, которые хорошо и давно зарекомендовали себя на рынке.

Все операторы – это ОАО, ЗАО, ООО. А в законах об акционерных обществах и об обществах с ограниченной ответственностью совершенно справедливо написано, что целью их деятельности является извлечение прибыли. И если безопасность – это всегда чистой воды затраты, а не возврат инвестиций, то как не превратить нужную услугу в обузу?

А. ЗОЛОТНИКОВ: Основная часть комплекса услуг информационной безопасности оператора связи, которые он предоставляет клиенту, нужна самому оператору. И мы для себя приняли так называемую модель нулевой стоимости вхождения. Это означает, что оборудование, которое мы закупаем для обслу-

живания собственных сетей, имеет определенный резерв, и исходя из него мы можем предложить нашим клиентам дополнительную услугу. Если мы видим, что услуга востребована, то начинаем работу по включению ее в продуктовый портфель компании.


А. ЗОЛОТНИКОВ

М. МЕДЖЛУМОВ: Хочу рассказать, как мы получили деньги на новую услугу, которая сейчас разрабатывается в компании, – защиту от спама. Обнаружив, что у одного из наших крупных клиентов есть серьезные проблемы со спамом как входящим, так и исходящим (к нам поступали постоянные жалобы на него), мы выбрали вендора антиспам-решений и предложили клиенту услугу защиты. Клиент согласился ее протестировать. В процессе подготовки и тестирования выбранный поставщик доработал свое решение с учетом требований «РТКомм.Ру» и полностью кастомизировал интерфейс под клиента. Пилот длится месяцев восемь, сейчас он на этапе согласования договоров. Драйвером появления и развития услуги выступает сам клиент. Приобретая услугу, он полностью окупает наши вложения в оборудование и ПО, а мы готовы масштабировать созданную услугу и предлагать ее другим клиентам.


М. МЕДЖЛУМОВ

А. СИКОРСКИЙ: Российский рынок непредсказуем не только в части услуг информационной безопасности, но и вообще новых телекоммуникационных услуг. И четко понять, насколько та или иная услуга будет востребована той или иной категорией клиентов или пользователей, весьма сложно. Для этого нужно проводить дорогостоящие исследования, опросы. У нас детальный опрос по всей стране для клиентской услуги потребует больших финансовых вложений. И если оператор затрачивает эти средства, он должен быть уверен, по крайней мере, что эта услуга пойдет. Поэтому, чтобы соблюсти баланс интересов оператора и возникающих рисков, относительно услуг безопасности необходимо проводить активную разъяснительную работу среди клиентов. От этого будет зависеть востребованность услуг оператора, который «в одном флаконе» предлагает и услуги безопасности. А для того чтобы понять, как формируется в структуре телекоммуникационной услуги элемент безопасности, нужно помнить, что у оператора – бизнес, который в принципе с безопасностью не связан, но от нее сильно зависит. Оператор крайне заинтересован в том, чтобы защитить свою сеть. А клиентам оператора, безусловно, важно, на какую сеть «садиться» – на менее или более защищенную.

М. СУКОННИК: Хочу обратить внимание сотовых операторов на еще одну важную вещь. Зайдите в общественный транспорт – и увидите там массу народа, едущего с различными гаджетами и «сидящего» в Интернете. Эти гаджеты никак не защищены. До России волна еще не докатилась, но западная практика показывает, что вопрос уже не только в вирусах и червях, которые в эти гаджеты попадают. Сотовые сети становятся источником уже упоминавшихся здесь DDoS-атак. И когда DDoS-атака с мобильных устройств пойдет через вашу сотовую сеть – атаковать будут какой-нибудь банк, – ваша сеть упадет, и вы ничего сделать не сможете. Потому что это рассредоточенная атака с незащищенных и постоянно перемещающихся, меняющих адреса мобильных устройств. Это сейчас серьезная головная боль у западных операторов, и мы помогаем с ней справиться.


М. СУКОННИК

М. ЕМЕЛЬЯННИКОВ: Итак, мы пришли к выводу, что услуги безопасности оператору связи нужны по двум основным причинам. Во-первых, ему нужна безопасная собственная сеть, во-вторых, эти услуги помогут оператору продавать другие телекоммуникационные услуги. Если сегодня покупается просто услуга доступа, то завтра будет покупаться услуга безопасного доступа.

В то же время мы выяснили, что стоимость внедрения этих услуг очень высока, а окупаемость абсолютно неочевидна. Однако когда эта услуга включается в большой пакет услуг оператора и продается комплексно, ее стоимость можно заложить в конечную цену пакета. Значит, надо искать схемы – и специалисты в области ИБ, маркетинга и продаж вынуждены учиться говорить на одном языке.

И, главное, мы поняли, что рынок, безусловно, будет развиваться, но пока резкого его подъема и очевидных путей для него в России не просматривается. Наверное, это предмет для совместной работы операторов, вендоров, интеграторов, которые должны еще тратить деньги на изучение потребностей клиентов. ИКС

Электронный офисный планктон

Редкий случай: читатели «ИКС» могут ощутить себя не только участниками рынка, но и обычными потребителями. Вашему вниманию – обзор рынка офисной электроники.

Максим САВВАТИН,
аналитик
iKS Consulting

Российский рынок офисной техники[1] существует уже почти два десятка лет. Первые официальные поставки на нем относятся к началу 90-х, когда в стране массово стал развиваться бизнес разных масштабов – от совсем небольших компаний до крупнейших предприятий общероссийского значения. Кроме того, шли поставки новых импортных устройств – вместо старой, еще советской, оргтехники – в государственные учреждения.

На новый рынок активно выходили все основные вендоры, производящие офисную технику, прежде всего Canon, Xerox, HP, Epson. Позже на нем появились и другие представители сегмента офисной техники, прежде всего нацеленные на высокопроизводительные решения.

В первом десятилетии нового века на российский рынок, как и на мировой, быстро стали проникать корейские производители электроники, в частности Samsung и LG. За достаточно короткий срок они сумели завоевать рынок в ряде категорий офисной техники. Особенно агрессивно выступала на рынке компания Samsung, которой удалось стать одним из лидеров в сегменте недорогих лазерных принтеров, потеснив в нем ведущих мировых вендоров.

В последние годы развитие российского рынка офисной техники замедлилось, в первую очередь конечно же из-за финансового кризиса, который сказался на нем крайне негативно. В 2009–2010 гг. темпы роста рынка несколько снижались, но по итогам 2010 г. – как по объему продаж в денежном выражении, так и по количеству проданных устройств – он вплотную приблизился к показателям 2008 г., на который пришелся пик продаж офисной техники.

По оценкам iKS-Consulting, объем рынка офисной техники в 2010 г. составил примерно $650 млн. Возможно, уже по итогам 2011 г. он превысит значение в $750 млн.

Одним из основных сегментов рынка офисной техники, составляющим примерно 70% от всего его объема, является рынок устройств печати – принтеров и многофункциональных устройств (МФУ), объединяющих в одном корпусе принтер, сканер и копир, а иногда еще и факс. На сканеры, факсы и проекторы приходится всего лишь 30% рынка.

Печать не кончается

По итогам 2010 г. объем российского рынка устройств печати для корпоративных пользователей превысил отметку в $455 млн. По итогам 2011 г. iKS-Consulting предполагает его увеличение на 15–20% – до $520–550 млн. Рост рынка в текущем году наблюдается во всех основных сегментах: лазерных, струйных принтеров, МФУ.

Большую часть продаж принтеров в корпоративном сегменте контролируют несколько компаний. Четверка производителей (HP, Xerox, Samsung, Canon) занимает более 80% рынка в денежном выражении. Другие игроки, в основном японские производители, сосредоточены в более узких нишах, например в сегменте высокопроизводительных напольных принтеров и МФУ, нацеленных прежде всего на крупный бизнес, где требуются большие объемы печати. В число основных игроков в данном сегменте, помимо производителей из Top-4, входят и такие сильные компании, как Konica Minolta, Toshiba, Ricoh.

Конкуренция на рынке принтеров весьма сильна, тут в ход идут и маркетин-

[1] В данной статье к категории «офисная техника» отнесены следующие устройства: лазерные и струйные принтеры (включая МФУ и высокопроизводительные напольные аппараты), офисные мультимедийные проекторы, офисные сканеры и факсы всех видов.

говые приемы (разнообразные акции по стимулированию продаж), и ставка на сервисное обслуживание, и один из самых важных факторов для корпоративных клиентов – экономия на расходных материалах для печати (картриджах, тонерах и т.п.).

Несмотря на активный рост сегмента принтеров и МФУ, производители уже задумываются о возможных последствиях внедрения электронного документооборота. Тем не менее лидеры в целом оптимистично смотрят на данное новшество и даже считают возможным увеличение рынка печати. Например, внедрение системы электронного документооборота приводит фактически к дублированию документов, которые теперь хранятся не в бумажном виде, а в некой электронной базе, так что пользователь может оперативно найти электронную копию документа и ее просмотреть либо распечатать. Соответственно, с одной стороны, количество бумажных документов уменьшается, с другой – лишь возрастает, поэтому влияние электронного документооборота на рынок устройств печати его игроки рассматривают даже с некоторым оптимизмом.

По оценкам iKS-Consulting, объем рынка офисной техники в 2010 г. составил $650 млн. Возможно, уже по итогам 2011 г. он превысит $750 млн

Офисы выбирают лазер

Российские офисы уже более десяти лет активно внедряют лазерные технологии печати, значительно снижающие расходы на печать, даже в рамках небольшого офиса. В пользу лазера говорят также скорость и качество отпечатка, особенно при черно-белой печати, которая и необходима большинству сотрудников. Доля традиционных чернильных (струйных) принтеров и МФУ, которые по-прежнему еще популярны у частных пользователей, в корпоративном сегменте крайне незначительна; их применение ограничено в основном узкими нишами, где требуется, например, распечатка цветных изображений формата А3 или фотографий. Отметим, что в Европе, в отличие от нашей страны, струйная печать в офисах распространена более широко, производители предлагают целый ряд офисных моделей. Одним из основных игроков в данном сегменте является компания HP.

Лазерные принтеры с возможностью цветной печати, напротив, постепенно завоевывают популярность у корпоративных клиентов, несмотря на более высокие стоимость владения и изначальную стоимость самого принтера. Уже сейчас цветные устройства составляют примерно 5% от всех проданных лазерных принтеров, а их доля в продажах за последние кварталы у ряда основных игроков достигает 20–30%. Рост объемов цветной лазерной печати обусловлен тем, что многим корпоративным потребителям все чаще требуется распечатывать в цвете разного рода материалы, прежде всего презентационные.

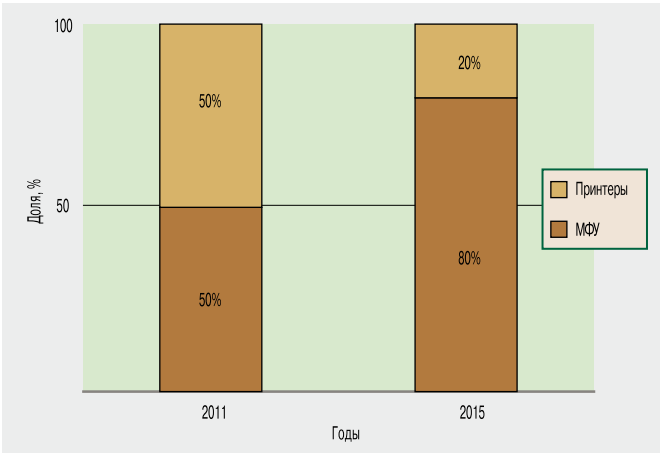
Тем не менее основные вендоры отмечают, что в ближайшее время на рынке по-прежнему будет доминировать черно-белая лазерная печать – благодаря оптимальному сочетанию стоимости таких принтеров и расходов на их эксплуатацию.

Помимо лазерных решений, на рынке предлагаются печатающие устройства на основе LED-технологии. В этих принтерах изображение вместо лазера формируется множеством светодиодов. LED-принтеры обеспечивают более низкую стоимость отпечатка, однако качество печати в этом случае не всегда соответствует качеству лазерных технологий. По прогнозам iKS-Consulting, LED-принтеры продолжат увеличивать свою долю на рынке, но серьезно не пошатнут позиции лазерных устройств.

МФУ наступают

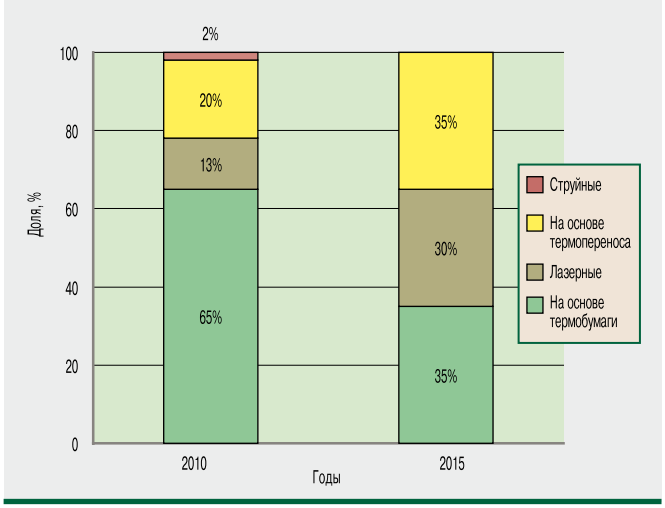
В последние 5–7 лет на рынке офисной техники сложился отчетливый

Рис. 1. Соотношение продаж принтеров и МФУ



тренд к увеличению доли многофункциональных устройств. Лишь в кризисный 2008-й темпы роста продаж МФУ несколько замедлились, потребители предпочли сэкономить на многофункциональности, выбирая более дешевые принтеры. Но с точки зрения универсальности и возможностей работы МФУ значительно выгоднее для пользователей, и потому по мере нормализации финансовой ситуации во всех сегментах (малый и средний бизнес, крупные компании) клиенты, как и до активной стадии кризиса, вновь стали покупать именно многофункциональные устройства (рис. 1).

Рис. 2. Структура продаж в сегменте факсов



По оценке iKS-Consulting, рынок МФУ сейчас наиболее динамичен среди всех сегментов офисной электроники. Как и в случае с базовыми принтерами, основной спрос у корпоративных потребителей приходится на лазерные устройства. Уже в ближайшие годы в сегменте лазерных устройств продажи МФУ сравняются с продажами принтеров, а через 3–4 года доля МФУ вырастет до 80%.

Факсы и сканеры не сдаются

Несмотря на активное восхождение, можно даже сказать триумф МФУ, традиционные устройства пока еще стараются удержать свою долю на рынке. Но рынок традиционных факсов, например, уже показывает замедление роста, а к 2015 г. iKS-Consulting прогнозирует его снижение в денежном выражении более чем на 70%.

Продажи данного типа устройств смешаются в регионы страны, где спрос на них пока сохраняется, поскольку покупка МФУ там не всегда рациональна, в том числе из-за отсутствия качественного сервисного обслуживания и ограниченных возможностей транспортировки больших аппаратов.

В России традиционно наиболее популярны факсы, использующие термобумагу, как наиболее дешевые в обслуживании – на их долю приходится почти две трети рынка (рис. 2). Постепенно набирает популярность сегмент лазерных факсов, доля которого в течение ближайших 3–4 лет, по оценкам iKS-Consulting, может достичь 30%, в том числе за счет вытеснения традиционных устройств на основе термобумаги.

Пул игроков на рынке факсов несколько иной по сравнению с рынком принтеров, в частности в данном сегменте сильны позиции компании Panasonic. Активно действует на рынке французская Sagem, продающая в России факсы под брендом Philips.

Сегменту сканеров также в значительной мере угрожает бурное развитие МФУ. Рынок хотя и продолжает рост, но уже начинает стагнировать; в особенности это заметно в сегменте недорогих бюджетных устройств, которые полностью замещаются современными МФУ. Однако более дорогие профессиональные решения для качественной работы с графикой по-прежнему пользуются спросом. Это объясняется тем, что большинство МФУ, предлагаемых в близком ценовом сегменте, не имеют функций сканирования с высоким разрешением, что необходимо для работы с графическим материалом.

Рынок факсов даже в большей степени, чем сегмент принтеров, подвержен влиянию внедрения и развития электронного документооборота, поскольку факсы во многих компаниях и госучреждениях в первую очередь используются для рассылки официальных документов.

Проекторы стремятся в 3D

Еще одной заметной составляющей рынка офисной техники становятся мультимедийные офисные проекто-

Среди основных трендов в сегменте проекторов – выпуск и расширение ассортимента продукции с поддержкой 3D

ры. Доля этого сегмента в общем объеме рынка превышает 15%, в 2010 г. его объем перешагнул отметку в $100 млн.

Рынок проекторов весьма сильно пострадал от кризиса, но тем не менее он очень быстро восстанавливается, причем растут продажи как бюджетных устройств, так и многофункционального профессионального оборудования, стоимость которого исчисляется десятками и сотнями тысяч рублей. Основные потребители проекторов – отели и конференц-залы, медицинские и образовательные учреждения, но традиционные офисы также часто приобретают проекторы для презентационных нужд.

Среди основных трендов в данном сегменте – конечно, выпуск и расширение ассортимента продукции с поддержкой 3D, но пока такие решения весьма дороги. Кроме того, производители стараются в каждой новой модели улучшить одну из основных характеристик проектора – его яркость.

Все основные вендоры в сегменте офисной техники будут расширять программные решения, направленные на интеграцию с облачными технологиями

Тренды будущего

Рынок офисной техники в России активно выходит из кризисного периода: уже по итогам 2011 г. большая часть сегментов рынка приблизится, а возможно, даже сравняется с уровнем предкризисного 2008-го.

В ближайшие 3–4 года iKS-Consulting ожидает умеренного развития рынка офисной техники. Часть сегментов, например факсы и сканеры, будут показывать снижение темпов роста, а рынок принтеров и МФУ, наоборот, продолжит расти.

Что касается объема рынка в целом, iKS-Consulting прогнозирует его увеличение до $1150 млн к концу 2015 г. (по сравнению с $750 млн в 2011 г.).

В последние годы один из основных трендов на рынке офисной электроники формируется за счет снижения себестоимости производства при одновременном улучшении качественных показателей и расширении функционала устройств. Учитывая достаточно высокую конкуренцию в каждом из сегментов рынка, основные производители офисной техники продолжат предлагать новые решения, позволяющие оптимизировать обслуживание и сделать продукт более удобным для потребителя. Принтеры и МФУ становятся все более независимы от компьютера, некоторые модели уже оснащаются разнообразными беспроводными интерфейсами, начиная от Wi-Fi и заканчивая встроенными 3G-модулями. По оценкам iKS-Consulting, будет появляться все больше продвинутых офисов, желающих избавиться от лишних проводов.

Уже сейчас виден тренд конкуренции не только на технологическом, но и на софтовом уровне. Программные решения играют особую роль в сегменте крупного бизнеса, а также в нишевых сегментах, например в полиграфии, где использование специализированного фирменного софта значительно увеличивает эффективность работы.

В ближайшем будущем все основные вендоры в сегменте офисной техники будут активно расширять программные решения, направленные на интеграцию с облачными технологиями, набирающими популярность в корпоративном сегменте. Уже сейчас многие модели принтеров ведущих поставщиков готовы к работе с облаками.

Еще одно направление, которое будет активно развиваться в ближайшие годы, – аутсорсинг печати. Данный тренд получил распространение еще до кризиса, сегодня многие вендоры предлагают подобные программы и в России. Схема аутсорсинга состоит в том, что клиент платит фактически только за конкретное количество копий, при этом оборудование остается у него на балансе, а с сервисной организацией подписывается контракт, в котором регламентируются минимальное и максимальное количество копий. Возможны и другие варианты. Такие услуги предлагают и сами производители – но они предпочитают работать с ключевыми заказчиками и крупными компаниями, а с малым и средним бизнесом взаимодействуют специальные сервисные компании, являющиеся партнерами того или иного вендора. Сейчас подобную программу на российском рынке продвигает HP, в ближайшее время ожидается и активизация ее основных конкурентов.

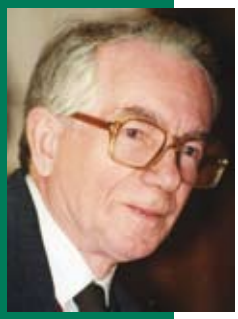
По нашим оценкам, в последующие годы аутсорсинг печати должен получить широкое распространение в России, а число компаний, постоянно использующих данную модель, будет исчисляться тысячами. ИКС

Быть ли свадьбе?
Ионосфера и DRM

Пригож телом, а хорош ли делом?

Окончание. Начало см. «ИКС» № 10, с. 53.

В полевых экспериментах на коротких волнах требуемый для устойчивого бесперебойного DRM-вещания уровень сигнала оказался намного выше, чем предполагалось по результатам лабораторных опытов. И это заставляет уделить особое внимание условиям работы КВ-каналов в цифровом режиме, уровню сигнала и помехам от других станций.



Юрий ЧЕРНОВ,
главный научный сотрудник ФГУП НИИ радио, д-р техн. наук

Вездесущие соседи

Их не зовут. Они приходят сами как незваные гости. И хорошего от них не жди. Они заселяют рабочий канал и соседние с ним. Конечно, существует процедура международного согласования сезонного расписания работы вещательных станций, но поскольку КВ-сигналы распространяются многими путями с различным затуханием, то невозможно предсказать, какие в данном месте в ближайшие полчаса-час или сегодня-завтра будут наблюдаться помехи, кроме как от станций, регулярно работающих на данную зону[1]. На практике оказалось, что их мешающее действие намного превосходит то, которое ожидалось командой разработчиков DRM после лабораторных испытаний. В аналоговом радиовещании не очень сильная помеха (на 10–15 дБ ниже сигнала) слышна, но не разрушает смысл передачи, при цифре такая же помеха, если она создает отношение С/П ниже критического, прерывает текст.

К сказанному надо добавить, что и сами ионосферные каналы, по которым движутся сигналы, привносят селективные замирания, диффузность, многолучевость, доплеровские эффекты и еще что-то неопознанное, что иногда препятствует декодированию и при высоком уровне сигнала. Основные видимые дефекты – пропадание сигнала и искажение звучания, которые при частом появлении делают речь неразборчивой, а содержание непонятным.

Подмосковные вечера и дни

Напомним, измерения цифровых КВ-сигналов в Подмосковье в марте – сентябре 2011 г. проводились с помощью приемника «Орленок» интервалами от 0,5 до 4,5 ч (для надежности работали одновременно два приемника, один с добавочной антенной в виде провода длиной ≈ 4 м). Запись параметров сигнала осуществлялась через каждые 3–5 мин в течение всего периода приема. Без сбоев (за исключением трех дней, когда были помехи) принималась только румынская радиостанция, в период 19.00–20.00 МСК работавшая на частоте 11615 кГц с модуляцией 64 QAM. Она создавала среднюю напряженность поля 61 дБ, что примерно на 31 дБ выше пороговой по Рек. BS.1615 (30 дБ для 64 QAM). Эта же станция утром (08.30–09.00) работала на частоте 7390 кГц с таким же высоким уровнем сигнала, и почти все дни хорошо. Но все же в утренних сеансах было больше случаев плохого приема, чем в вечерних. Всего с использованием штатной антенны приемника контролировалось 20 частот (данные о наиболее слышимых станциях приведены в табл. 1). За исключением румынской станции, работавшей на частоте 11615 кГц, среднее реальное превышение уровня сигнала над порогом по Рек. BS.1615 составляло 20 ± 8 дБ, однако для приема без частых сбоев на некоторых частотах требовалось увеличение уровня сигнала еще на 2–10 дБ (см. предпоследний столбец табл. 1 – цифры до и после дробной черты).

По остальным частотам картина примерно такая же. На дополнительную антенну прием на 2–5 дБ лучше, но при обнаруженном дефиците более 20–25 дБ это играет небольшую роль.

Проведенные измерения позволили выявить ряд важных особенностей. Прежде

[1]Чернов Ю.А., Хохловкин Я.Д. Экспериментальные исследования девиации пеленгов коротковолновых сигналов (обзор). Зарубежная техника связи, Минсвязи, ЦНТИ, сер. «Радиосвязь, радиовещание, телевидение», 1988, вып. 21–22, с. 1.

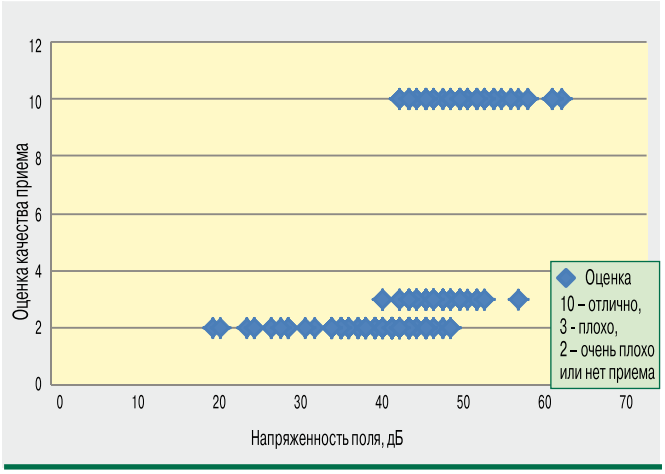
Табл. 1. Результаты измерений цифрового КВ-сигнала в Подмосковье в марте–сентябре 2011 г.

Место передачи	Частота, кГц	Периоды работы (МСК)	Сигнал за период измерений* / уровень для хорошего приема, дБ (мкВ/м)	Модуляция	Среднее / необходимое превышение над порогом для хорошего приема, дБ (мкВ/м)	Доля времени приема на штатную антенну, округленно, %
Румыния	11615	19.00-20.00	61 (47–69)	64 QAM	+ 31/17	100**
Румыния	7390	08.30-09.00	58 (48–68)/60	64 QAM	+ 28/30	75
Испания	9780	09.00-13.00	43 (20–60)/52	64 QAM	+ 13/22	30
Португалия	11995	12.30-14.00	37 (32–42)/42	16 QAM	+ 12/17	10
Индия	9950	22.00-02.30	45 (29–58)/55	16 QAM	+ 20/30	45
Краснодар	7225	18.00-20.00	51 (37–59)/56	16 QAM	+ 26/31	20

*В скобках – диапазоны средних уровней сигналов за отдельные пятиминутные интервалы.
**В течение трех дней прием был плохим из-за сильных помех от АМ-станций.

всего, непостоянность и непредсказуемость качества приема. Если в один день прием был хорошим при напряженности поля от 50 дБ, то в другой день при уровне сигнала 55 дБ или более высоком прием мог быть плохим. Такое перекрытие условий наблюдалось на всех трассах,

Рис. 4. Зависимость качества приема испанской DRM-радиостанции (9780 кГц) от уровня сигнала



оно является органическим свойством ионосферного канала. Типичный пример – прием испанской станции, работавшей на частоте 9780 кГц с модуляцией 64 QAM (рис. 4). В какие-то дни отличный прием начинался с уровня сигнала 40 дБ, а в другие дни при уровне вплоть до 52 дБ прием был плохим или его не было вовсе.

На основе подобных результатов и были получены оценки необходимого уровня полезного сигнала для табл. 1.

В одном интервале работы качество приема также не оставалось постоянным. Оно могло резко измениться в течение буквально получаса (табл. 2). Такая картина для испанской станции наблюдалась ежедневно и в разных вариантах имела место для всех станций, наблюдавшихся длительный период.

Иными словами, в реальных условиях напряженность поля выше рекомендованного в Рек. BS.1615 порога нисколько не гарантировала хорошего приема.

В целом можно сказать, что ни одна станция, кроме ранее упомянутой румынской, перекрывавшей порог в среднем на 31 дБ (см. табл. 1), не обеспечивала устойчивого радиовещания даже при уровне сигнала на 20 и более децибел выше порога.

Среди прочих причин здесь нужно назвать и АМ-помехи. Практически во всех сеансах и на всех частотах они присутствовали в основном канале (в единичных случаях) или в каналах, отстоящих от него на ± 5 или 10 кГц (наиболее частая ситуация). Было замечено, что когда в соседнем канале (± 10 кГц) уровень помех был примерно равен сигналу DRM или выше его, появлялись сбои или их число увеличивалось. Это находится в явном противоречии с Рек. BS.1615, согласно табл. 17 которой прием DRM не нарушается, если помеха в соседнем канале (± 10 кГц) превышает сигнал даже на 30 дБ и более. Видимо, в действительности внеполосные излучения АМ-сигналов значительно превышают те, для которых в лабораторных условиях формировалась эта таблица. Во многих случаях, когда уровень мешающего сигнала в соседнем канале оказывался выше

Табл. 2. Фрагмент записи 23.04.2011 прохождения сигнала с оценкой напряженности поля и качества приема испанской станции

Время, МСК	Уровень сигнала, дБ	Прием	Оценка
09.00	56	Идет	10
09.10	49	Идет	10
09.15	48	Идет	10
09.21	51	Идет	10
09.30	45	Идет с провалами	3
09.35	44	Идет с провалами	3
09.45	44	Идет плохо. Часто провалы	2
09.57	44	Идет плохо. Часто провалы	2
10.20	41	Идет плохо. Часто провалы	2
10.30	42	Идет плохо. Часто провалы	2
10.48	40	Не идет	2
11.15	36	Не идет	2
12.50	23	Не идет	2

указанного в Рек. BS.1615 значения не на 30, а 10–12 дБ, уже наблюдались короткие, по 1–3 с провалы. Они следовали часто, через 10–20 с. Иногда провалы были более длительными.

В итоге прием вроде бы есть, но уж очень много пропусков. В музыкальной передаче или рассказе о молодой писательнице, опубликовавшей несколько романов, перерывы в приеме сильно не напрягают. Но в новостях, где обсуждается, скажем, когда начинать бомбить Ливию, провалы по десять и более секунд лишают сообщение смысла. И каждый раз приходит мысль, что намного лучше иметь не самый хороший аналоговый приемник, чем такой рваный и жеваный DRM. В результате многодневного контроля стало очевидным, что в реальных условиях продолжительные периоды приема DRM без провалов – это большая редкость, подарок природы. Зачастую не помогало и повышение уровня сигнала в разы.

Анализ большого объема экспериментального материала показал следующее. Жизнь DRM на коротких волнах гораздо сложнее и замусореннее, чем это представлялось первоначально. Для минимальной гарантии хорошего приема необходимо иметь три смежных канала по 10 кГц, свободных от помех, в среднем из которых будет работать выбранная станция. На бытовом языке это означает, что надо иметь свободную жилплощадь, причем значительно большую, чем для АМ-вещания. И без спонтанных наездов дальних родственников или попыток пристроиться слева или справа. В ближайшие лет десять это вряд ли возможно. А, может быть, и вообще природа распространения КВ в ионосфере не позволит этому случиться[1].

Несколько лет назад в МСЭ-Р поднимался вопрос о выделении полос частот в КВ-диапазоне для DRM-вещания на плановой основе. Но по ряду причин, в том числе и по причине неисповедимости путей помех, эта идея не получила развития. И все-таки, на мой взгляд, это был неплохой шанс.

К сожалению, приходится отметить, что и при достаточном уровне сигнала (например, 55–60 дБ для режима 64 QAM) нет гарантии такой же зоны покрытия, как при аналоговом вещании. Вследствие пороговых свойств цифровых сигналов она неизбежно будет меньше из-за обрезания периферийных частей. Но и в самом лучшем случае мы не будем избавлены от сбоев, поскольку даже при распространении без помех, как показывают наблюдения, сигнал претерпевает некоторые внутренние структурные изменения, не всегда позволяющие его правильно декодировать.

Введение иерархической модуляции тоже не панацея. При работе станции с модуляцией 16 QAM также требуется большее превышение уровня сигнала над порогом, чем предложено МСЭ-Р (см. табл. 1).

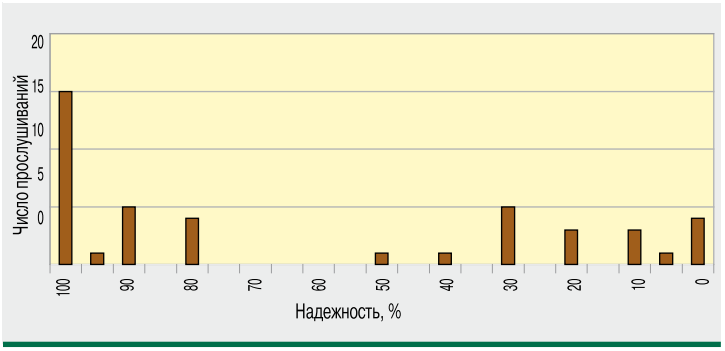
Оглядимся вокруг. А что в Интернете?

Обращает на себя внимание большой процент сообщений в Интернете о приеме DRM-станций с низкой надежностью. Например, на одном из КВ-каналов за период 2006–2011 гг. из 43 сообщений (каждое сообщение относится к определенному месту приема (стране, городу) и дате приема) 15 говорят о приеме с надежностью 100%, 18 – 50% и ниже (рис. 5).

Число сообщений от слушателей в Интернете по годам в сумме по всем каналам также весьма показательно. Пик интереса к DRM-вещанию на коротких, длинных и средних волнах наблюдался в 2007 г., а к 2010 г. он упал до нуля (рис. 6).

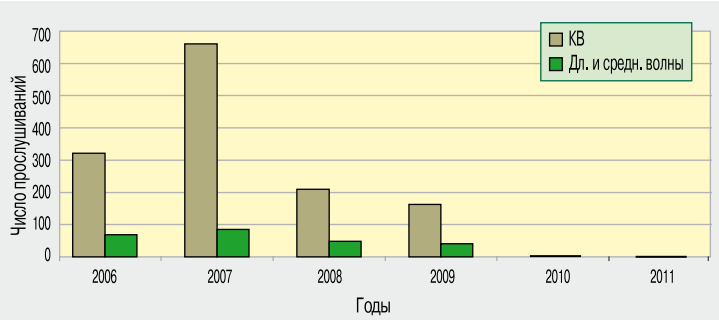
В реальных условиях продолжительные периоды приема DRM без провалов – это большая редкость, подарок природы

Рис. 5. Число прослушиваний DRM-станций с разной надежностью



[1]Чернов Ю.А., Хохловкин Я.Д. Экспериментальные исследования девиации пеленгов коротковолновых сигналов (обзор). Зарубежная техника связи, Минсвязи, ЦНТИ, сер. «Радиосвязь, радиовещание, телевидение», 1988, вып. 21–22, с. 1.

Рис. 6. Число прослушиваний DRM-станций по годам



Отметим, что и суммарное время DRM-вещания в мире неуклонно уменьшается. В прошлом году оно превышало 28 тыс. мин, к 18.04.2011 было заявлено 27 008 мин, 24.06.2011 – уже 25 493 мин. А спустя лишь три недели – 19.07.2011 – DRM-вещание сократилось до 25 313 мин[1]. Кроме того, при прослушивании по всему списку обнаруживается множество «мертвых душ». В DRM-вещании, как видим, еще не все установилось, и положительные сдвиги пока не проглядываются. Примечательно, что за все 11 лет изучения DRM, как на СВ, так и на КВ, несмотря на оглушительную рекламу первых лет, мне неизвестны сколько-нибудь обстоятельные аналитические публикации о положительных долговременных результатах работы DRM в каком-либо диапазоне в какой-либо стране. Создается впечатление, что мировому радиовещанию по этому вопросу хорошего сказать нечего, а плохого говорить почему-то нет желания. Иногда, как с магнитофона, повторяются рекламные заявления, которые были вброшены 11 лет назад.

Суммарное время DRM-вещания в мире неуклонно уменьшается

Роль ионосферы в составлении расписания DRM-вещания на КВ мы не рассматриваем. Это вопрос очень объемный, здесь отметим лишь кратко, что работа передатчиков на смежные территории на одной и той же или на соседних частотах может отягощаться наличием извивающихся, подвижных как ртуть, глухих коридоров между зонами, где никакая станция приниматься не будет (см. Чернов Ю. Как внедрять DRM будем? «ИКС» № 3'2011, с. 67). На коротких волнах, в отличие от средних, полезные зоны из космоса выглядят как «танцующие кляксы».

Жизнь молодых трудно предсказать

После всего сказанного, опираясь на житейский опыт, трудно предположить, что семейный союз ионосферы и DRM будет счастливым и сохранится на долгие времена. Характерами не сошлись. Скорее всего, под легендой радиовещания DRM продолжит жизнь как полигон для любителей радиоигры или «радиорыбалки». Но и эта его сторона вряд ли окажется интересной. При АМ-вещании каждый неожиданный прием дальней станции, когда она еле-еле слышна, приводит радиолюбителя в восторг. Но при цифровом вещании этого «еле-еле» не бывает, поэтому и восторг, вероятно, также будет отменен. Правда, может случиться нечаянная радость с другой стороны. Поймать дальнюю слабую станцию, хорошо говорящую на DRM, – тоже событие. Почти невероятное.

Что в итоге? Ничего. С многократными извинениями остается повторить набившую оскомину реплику: сделать можно, но за это, по-видимому, надо будет платить. Платить за создание высокой напряженности поля. И платить много. И как бы здесь не взлететь на новый виток мощности, какой аналог и представить не мог. А у ионосферы приданого нет. Партнер тоже не оплатит. Так что в обозримом будущем, дорогие друзья, если и можно рассчитывать на свадьбу и долгую счастливую жизнь отдельно взятой семьи, то лишь при наличии приватизированной частотной жилплощади, охраняемой Законом.

■ ■ ■

Возможно, когда-нибудь наступят другие времена, все DRM'ные семьи будут обеспечены жилплощадью, а заботливая радиополиция навсегда избавит мир от непрошеных гостей и соседей, вот тогда наступит долгожданная пора непрерывных свадеб, и радиозагсы не будут успевать записывать вновь прибывающие счастливые пары...

Но можно ли на это надеяться? ИКС

[1]http://drm.org/old/for-broadcasters/live-broadcast-schedule.

Механизмы резервирования ЦОДов: разделяй и... спи спокойно

Остановка дата-центра даже на несколько часов означает для компании серьезные убытки? Тогда ничего не остается, как принять все меры для снижения вероятности такого события. Эффективным решением станет создание резервного ЦОДа на площадке в существенном удалении от основной.

Александр ГУЛЯЕВ, руководитель отдела сетевых проектов Центра сетевых решений компании «Инфосистемы Джет»

Только такое географическое резервирование центра обработки данных может дать более или менее твердую уверенность в том, что в результате очередной техногенной катастрофы или банальной ошибки персонала ЦОДа системы, обслуживающие бизнес компании, внезапно не остановятся.

Итак, решение о необходимости создания второго ЦОДа с целью резервирования критичных бизнес-систем принято. Сразу же появляется ряд специфических требований к сетевой инфраструктуре компании и нового ЦОДа. В частности, нужно построить отказоустойчивую инфраструктуру сети, которая позволит обеспечить работу приложений и кластеров, разнесенных на разные площадки, а также автоматически отрабатывать возможные нестандартные ситуации, вплоть до полной потери одной из площадок. При этом с точки зрения пользователей или клиентов перерыв в предоставлении сервиса должен быть минимальным и практически незаметным, а процедура его восстановления до исходного состояния – по возможности автоматической.

С точки зрения сетевого архитектора требуется решить как минимум две задачи:

- организовать бесперебойный доступ пользователя к приложениям, размещенным на разных площадках, как в нормальном, так и в аварийном режиме работы одного из ЦОДов;
- гарантировать бесперебойное функционирование приложений, разнесенных на разные площадки.

Отказоустойчивость для клиентов

Когда площадка одна, способ предоставления сервиса очевиден: клиентское приложение обращается к конкретному серверу. Если серверов несколько и ПО системы не предлагает собственных средств обеспечения отказоустойчивости или распределения нагрузки, на помощь приходят балансировщики нагрузки. В настоящее время они являются неотъемлемым компонентом любого ЦОДа. Но когда площадок две и на каждой из них есть собственный набор серверов, а размещаться они могут даже на разных континентах, средства локальной балансировки уже не всегда подходят, особенно когда площадки расположены на большом расстоянии друг от друга и нельзя организовать между ними каналы Ethernet. Ведь локальный балансировщик – это часть оборудования одной из площадок, и в случае аварии он также становится недоступным и не может перенаправить входящий запрос на другую площадку.

Решить проблему позволяют механизмы глобальной балансировки (рис. 1). При использовании глобальной балансировки принятие решения о выборе сервера происходит в два этапа: сначала определяется адрес сервиса на одной из площадок, а затем локальный балансировщик выбранной площадки перенаправляет запрос на конкретный сервер.

Благодаря такой двухуровневой схеме, а также постоянной связи между локальными и глобальными балансировщиками достигается и масштабируемость решения, и его высокая отказоустойчивость. Глобальных балансировщиков, как и ЦОДов, может быть несколько, что дает возможность построения различных конфигураций ИТ-инфраструктуры.

Кроме решения задачи резервирования, применение балансировщиков позволяет минимизировать время отклика приложений, экономить пропускную способность каналов связи, обеспечить равномерную утилизацию ресурсов в ЦОДах за счет мониторинга загрузки серверов и динамического распределения запросов.

Отказоустойчивость для приложений

С сетевыми решениями, поддерживающими функционирование разнесенных в разные ЦОДы приложений, тоже не все просто. В большинстве случаев требуется единый Ethernet-сегмент, объединяющий Ethernet-сети, расположенные на двух и более относительно близких друг к другу площадках. Это обусловлено особенностью работы многих вычислительных систем, в частности – кластеров. Самый простой способ решения этой задачи – создать транковые Ethernet-соединения между коммутаторами ядра ЦОДов и направить в них трафик нужных нам подсетей. Такая схема применяется очень часто, но ее практическая реализация всегда вызывала ряд вопросов. Начнем с того, что подобная конструкция усложняет логическую структуру сети и сдерживает возможности ее масштабирования. В результате увеличиваются размеры сетевых сегментов и появляется большой объем широковещательного трафика, который занимает часть полосы пропускания в каналах и мешает полезному трафику.

Вторая задача продиктована необходимостью резервировать соединения и сетевое оборудование в ЦОДах. Она требует применения специальных протоколов для предотвращения образующихся в таком случае петель. Наилучшим вариантом преодоления этих трудностей является кластеризация сетевых коммутаторов уровня ядра/агрегации. Подобные решения предлагают сейчас несколько производителей, например, Cisco – технологии VSS и vPC в различных линейках оборудования, Brocade – технологию MCT, Juniper – Virtual Chassis и т.д.

Организация резервирования требует наличия как минимум двух Ethernet-каналов, проложенных по различным трассам, что не всегда возможно, так как для этого необходимо иметь собственное оптическое волокно либо соответствующую услугу, предоставляемую оператором. Через дешевый IP-канал такое соединение работать не будет.

Но выход все же есть. На выделенных IP-каналах можно применить достаточно надежные и хорошо себя зарекомендовавшие технологии MPLS L2VPN. Современные маршрутизаторы отлично справляются с созданием высокоскоростных MPLS-туннелей, а само решение не ограничено какой-либо одной топологией или определенным числом ЦОДов, хорошо масштабируется и обладает надежностью операторского класса. Кроме решения на базе MPLS стоит упомянуть фирменную технологию Cisco OTV (Overlay Transport Virtualization), реализованную в коммутаторах серии Nexus, которая позволяет использовать между ЦОДами каналы IP для передачи Ethernet-трафика.

Безопасность – еще один насущный вопрос, о котором не стоит забывать в современных условиях. Для шифрования трафика, передаваемого через Ethernet-каналы между ЦОДами, можно применить решение на базе стандарта MAC Security. Это позволит обезопасить сетевой трафик от возможных атак или перехвата злоумышленником, не прибегать к дополнительным устройствам шифрования и сэкономить средства при внедрении.

Построив резервный ЦОД, следует помнить о необходимости синхронизации данных приложений и организации резервного копирования. И снова на помощь приходят сетевые технологии. Работающие поверх TCP/IP протоколы, используемые для синхронизации и резервного копирования, хорошо поддаются оптимизации. Сетевая индустрия предлагает специализированные устройства оптимизации трафика для ЦОДов. Их отличительные особенности – возможность эффективно работать на каналах с высокой пропускной способностью, а также большой объем встроенного хранилища данных. В результате применения таких решений становится возможным сократить время резервного копирования, например, с десяти часов до одного часа, ведь эти устройства задействуют весь арсенал доступных средств оптимизации: оптимизацию TCP и других протоколов, дедупликацию данных, кэширование и т.д.

Очевидно, что системы резервного копирования могут взаимодействовать с серверами по каналам Fibre Channel и нагружать только инфра-

Рис. 1. Работа отказоустойчивой системы балансировки нагрузки в нормальном режиме и в случае выхода из строя одной из площадок ЦОДа

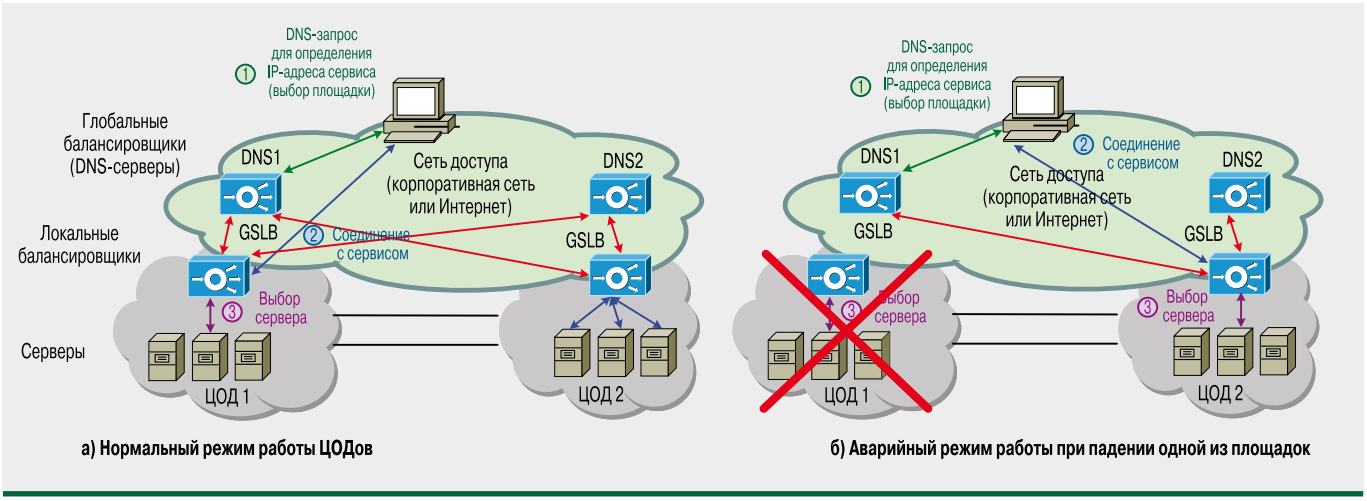
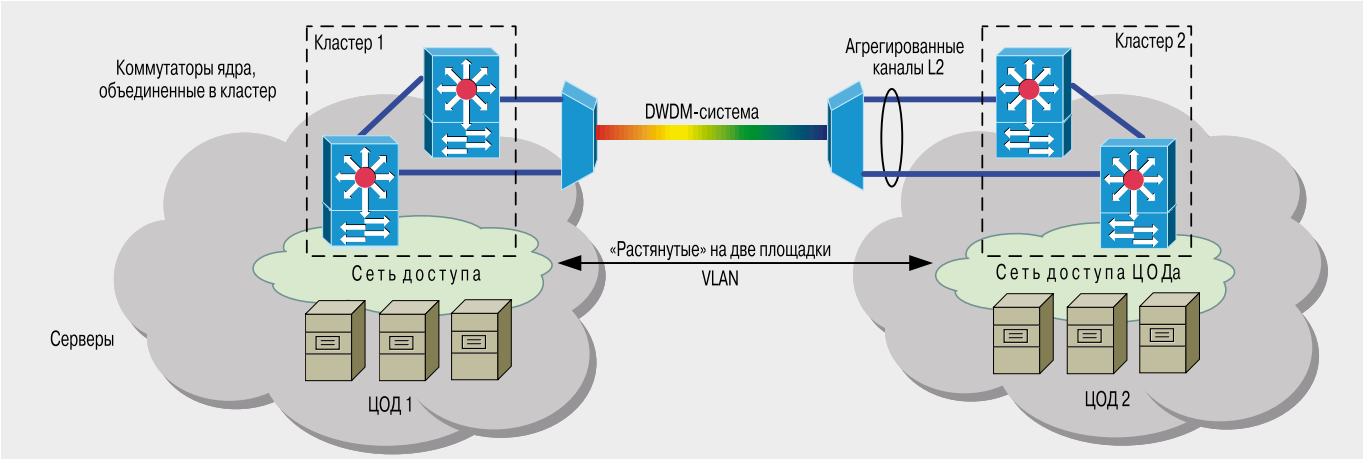


Рис. 2. Отказоустойчивая связь сетей ЦОДов на втором уровне с использованием средств кластеризации коммутаторов и агрегации каналов Ethernet



структуру СХД. С другой стороны, отдельные оптические каналы для Fibre Channel также обойдутся недешево. В случае, когда для резервного копирования или сети хранения данных требуется транспорт Fibre Channel, а возможность организации каналов через оптическую линию связи отсутствует, как правило, применяются решения на базе протокола FCIP (Fibre Channel по IP).

Но по-настоящему революционным решением для объединения ЦОДов представляется универсальный конвергентный транспорт, в частности, протокол FCoE (Fibre Chanel over Ethernet), позволяющий использовать единый Ethernet-транспорт для передачи сетевого трафика и трафика Fibre Channel. До недавнего времени дистанция для конвергентного соединения не могла превышать 300 м, что ограничивало его применение одним ЦОДом. Однако уже сегодня производителями заявлена поддержка multihop FCoE и возможность увеличения дальности конвергентного соединения до 10 км, что позволяет говорить о применимости этой технологии для объединения ЦОДов.

Через призму виртуализации

Выше мы рассмотрели типичные стандартные сценарии, которые остаются актуальными в большинстве случаев при резервировании ЦОДов. Теперь посмотрим на резервирование ЦОДов через призму виртуализации, ставящей перед сетью новые нетривиальные задачи.

Одна из серьезных сетевых проблем в эпоху виртуализации – необходимость обеспечения мобильности виртуальных машин. Настройки сетевых коммутаторов всем хороши, за исключением того, что они, как правило, статичны. Если вы переключаете сервер на другой порт коммутатора, администратор должен добавлять команды на одном или нескольких сетевых устройствах, что значительно повышает риск ошибок и соответственно нарушения работоспособности сети. Да и сами трудозатраты на осуществление нужных настроек влияют на операционные издержки компании.

Виртуализация с ее возможностями адаптироваться под задачи клиентов или растущую нагрузку требует от сети готовности приспосабливаться к динамично меняющемуся ландшафту ЦОДа. Ведь по-настоящему эффективная виртуальная инфраструктура не должна иметь архитектурных ограничений в части развития или привязки тех или иных серверов к строго определенным сетевым сегментам – в идеале сеть должна автоматически принимать нужную конфигурацию для поддержки работы сервисов, а не наоборот.

По сути, большинство производителей оборудования смирились с тем, что стандартными способами выполнить эти требования не получится, и стали предлагать собственные решения, зачастую несовместимые друг с другом. Но прослеживается одна общая тенденция: сеть все плотнее интегрируется с вычислительной инфраструктурой и средствами виртуализации. Причем интеграция идет с двух сторон: как путем организации взаимодействия между ПО сетевого управления и системами управления виртуальными ресурсами, так и за счет интеграции сетевого оборудования с серверными компонентами и драйверами. Современные сетевые решения для ЦОДов уже сейчас позволяют поддерживать миграцию виртуальных машин в пределах ЦОДа и снять нагрузку по обработке сетевого трафика с процессоров виртуализованных серверов, перенеся ее на сетевые коммутаторы. Это повышает отдачу от вычислительных ресурсов, дает возможность более эффективно внедрять сетевые политики и обеспечивать безопасность.

■ ■ ■

Несмотря на очевидное усложнение логической структуры сети, сопровождающее организацию географического резервирования ЦОДов, решения, которые позволяют эффективно построить такую архитектуру, существуют и продолжают совершенствоваться. Дополнительный импульс развитию таких решений сообщает растущая популярность облачных технологий, в особенности – публичных облаков, для которых потеря одного дата-центра наиболее критична, так как чревата простоем бизнеса не одной, а сотен или даже тысяч компаний. ИКС

От PUE – к «зеленому» дата-центру

Российские дата-центры в последние годы сильно выросли в техническом отношении, а по показателю энергоэффективности PUE новые и проектируемые ЦОДы находятся фактически на мировом уровне. Следующая ступень, на которую им предстоит подняться, – использование «зеленых» технологий.

Харкирит СИНГХ.

Об этом рассказывает председатель наблюдательного совета консорциума The Green Grid в регионе EMEA Харкирит СИНГХ.

– Сложно ли стать членом The Green Grid?

– Нет, никаких предварительных условий для вступления в консорциум нет, и никаких обязательств членство в The Green Grid не накладывает. Просто компании-участники могут делиться друг с другом опытом и лучшими практиками, и на основе этих данных консорциум разрабатывает свои документы и метрики для измерения эффективности использования ресурсов. Мы стремимся к привлечению участников из самых разных стран мира.

– Что консорциум понимает под «зелеными» технологиями?

– «Зеленые» технологии – это технологии, позволяющие минимизировать ущерб для окружающей среды от создания и эксплуатации ИТ-инфраструктуры. Такая минимизация достигается за счет повышения эффективности использования электроэнергии и воды, за счет уменьшения объема вредных выбросов в атмосферу, в том числе CO_2. То есть мы исповедуем комплексный подход к потреблению любых ресурсов.

– Известно, что консорциум The Green Grid разработал несколько метрик, определяющих эффективность работы ЦОДа. В России среди них наиболее известна PUE (Power Usage Effectiveness, коэффициент эффективности использования электроэнергии). Существует ли сегодня общепризнанная методика расчета PUE дата-центра?

– Это была одна из первых метрик, разработанных The Green Grid. Коэффициент PUE был предложен в 2007 г., и со временем его интерпретация несколько эволюционировала. В выпущенной в 2007 г. так называемой Белой книге коэффициент PUE определялся в самом общем виде. Ко второму этапу работы над этой метрикой мы собрали и проанализировали отзывы представителей отрасли, после чего выпустили второй официальный документ, где были даны детальные инструкции по расчету этого параметра. Сейчас мы вышли на третий этап определения PUE, предполагающий глобальную гармонизацию, т.е. согласование метрик энергоэффективности, использование которых закреплено в законодательствах разных стран мира. Результатом этой работы будет заключение соглашения об определении PUE в США, Европе и Японии. Ну а заключительным этапом будет принятие глобального международного определения PUE.

– Насколько полно коэффициент PUE отражает степень экологичности дата-центров?

– PUE – это лишь один показатель работы дата-центра, характеризующий его инженерную инфраструктуру. Для определения степени экологичности ЦОДа нужна модель зрелости, которая позволяет оценить эффективность работы не только инженерной, но и ИТ-составляющей дата-центра, а также объемы выбросов CO_2, эффективность использования водных ресурсов, переработки и утилизации отходов. Например, в дата-центре, соответствующем высшему, пятому уровню модели зрелости, механические системы охлаждения не должны применяться ни в какое время года.

– Какие еще метрики для дата-центров находятся в работе у The Green Grid?

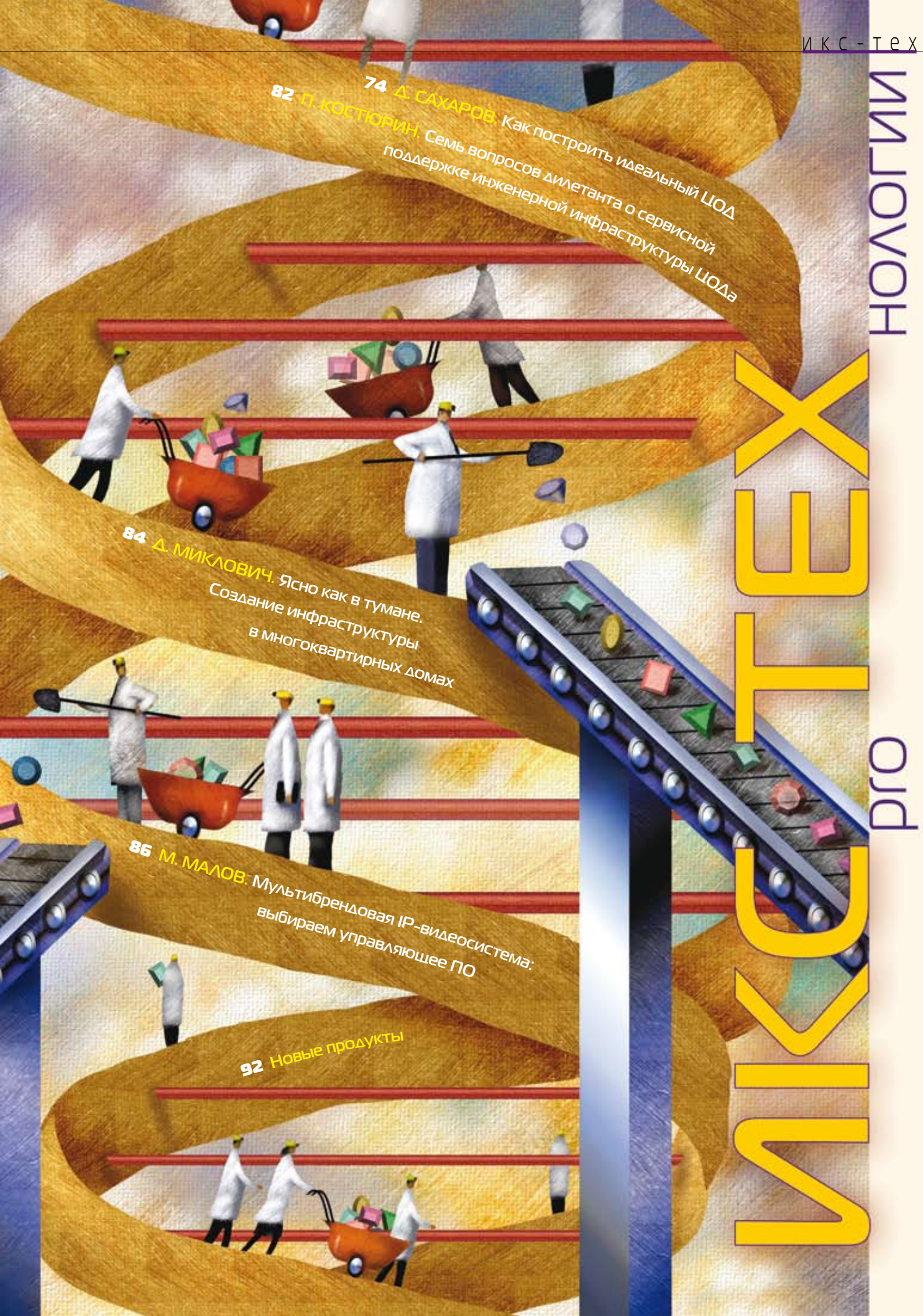
– Сейчас мы занимаемся метриками, описывающими эффективность использования водных ресурсов и повторного использования выделяемого дата-центром тепла, степень загрязнения окружающей среды, объем выбросов CO_2, эффективность функционирования компьютерной инфраструктуры. Работа над ними пока находится на самом первом этапе: сформулированы общие определения метрик и идет сбор отзывов от всех заинтересованных сторон, после чего будут выпущены следующие версии разрабатываемых метрик.

Беседовала **Евгения ВОЛЫНКИНА**

Справка ИКС

The Green Grid – это открытый некоммерческий консорциум, который объединяет различные компании, причастные к миру дата-центров, а также разработчиков стандартов и конечных пользователей. Основная цель консорциума – повышение эффективности использования всех ресурсов, потребляемых дата-центрами и компьютерными системами, т.е. развитие и популяризация применения в ЦОДах «зеленых» технологий. В настоящее время членами The Green Grid являются около 200 компаний и организаций из разных стран мира. Главным образом это компании из США, Европы и Японии, поскольку именно там начал развиваться рынок дата-центров. В отделении EMEA доминируют компании из Западной Европы, а российских компаний среди членов The Green Grid пока нет.

ИКС pro технологии



Как построить идеальный ЦОД

Дмитрий САХАРОВ

О том, какие условия и требования должны выполняться при построении современных дата-центров, чтобы обеспечить высокую надежность работы его ИТ-инфраструктуры, доступность данных и приложений, зарубежные и российские компании рассказали на 6-й Международной конференции «ЦОД-2011», организованной журналом «ИКС».

Согласно проведенному IDC анализу рынка коммерческих ЦОДов в России, в 2010 г. объем расходов на услуги дата-центров превысил $160 млн. По мнению аналитиков, этот сегмент будет развиваться быстрыми темпами, опережая средние показатели рынка ИТ в целом. При этом растет число ЦОДов, обеспечивающих высокий уровень надежности обработки информации и ее доступности.

Заказчики, создающие ЦОДы, по-прежнему стремятся использовать решения, с помощью которых можно существенно сократить как инвестиции в расширение ИТ-инфраструктуры, так и операционные затраты на ее администрирование и обслуживание. Как подчеркнул Леонид Шишлов, менеджер по развитию ЦОД компании Intel, основные пути достижения этих целей таковы: замена серверного оборудования на более современные системы, что позволяет консолидировать серверные ресурсы и одновременно снизить расходы на энергопотребление; виртуализация серверов и СХД, повышающая в несколько раз уровни загрузки серверов и ЦОДа в целом; и наконец, использование более эффективных систем энергообеспечения и охлаждения, что также помогает снизить операционные расходы ЦОДа.

Александр Мартынюк, генеральный директор компании «Ди Си Квадрат», считает, что заказчики в России преодолели базовый уровень понимания, что именно они строят в виде ЦОДа, а теперь переходят к более эффективным решениям и пытаются их оптимизировать: «Идут процессы консолидации небольших серверных систем и строительство крупных ЦОДов на больших площадках, что положительно сказывается как на операционных затратах, так и на потенциале развития дата-центров». Требования к производительности, надежности, энергоэффективности ЦОДа, подчеркивает он, теперь прописываются в техзадания заказчиков.

По мнению А. Мартынюка, появились новые тенденции в применении инженерных решений для инфраструктуры и четко обозначились приоритеты при создании ЦОДов коммерческими и корпоративными заказчиками: «Коммерсанты готовы вложить деньги в энергоэффективное решение, но такие решения должны быть обоснованы – экономия на операционных расходах должна соотноситься с грамотными расходами на капитальное строительство. Компании, создающие или трансформирующие свой корпоративный ЦОД, ставят очень высокие требования к уровню надежности, производительности и энергоэффективности, и в большинстве крупных проектов требуется сертификация Uptime Institute как гарантия того, что заказчик получает инженерное решение, соответствующее лучшим мировым практикам».

Требования заказчиков определяются бизнесом

В компании «РЖД» для решения задач управления пассажирскими перевозками, движением поездов и всей инфраструктурой отрасли еще в 2000-х гг. началось создание разветвленной ИТ-инфраструктуры, рассказал Игорь Бессонов, главный инженер Московского ИВЦ – структурного подразделения ГВЦ ОАО «РЖД». К настоящему времени она насчитывает более 250 тыс. подключенных к ней хостов и 20 тыс. управляемых узлов в сети передачи данных. Кроме ГВЦ, который существует 50 лет, в системе действовали 17 дорожных ИВЦ, каждый из которых представлял собой ЦОД.

В компании реализована вертикально интегрированная структура управления, и ИТ-инфраструктура формировалась подобным же образом. Однако в 2007 г. началось преобразование ИТ-инфраструктуры отрасли в направлении консолидации ее ресурсов – в ней будут всего три крупных ЦОДа и 14 дорожных ИВЦ, которым остаются лишь задачи линейной эксплуатации. При этом ГВЦ превращается в управляющую компанию, а обработка информации для решения основных задач отрасли возлагается на Московский ЦОД (1 МВт, более 300 стоек серверов, 5 мейнфреймов, 12 систем IBM p-серии, 8–10 блейд-систем, 3 дизельные электростанции, 2 холодильные машины, около 20 кондиционеров), Санкт-Петербургский и Екатеринбургский ЦОДы.

Важнейшими показателями трансформируемой ИТ-инфраструктуры отрасли являются обеспечение ее катастрофоустойчивости и высокой доступности. Поэтому в дополнение к существующим зданиям каждого из

трех основных ЦОДов строятся новые, в которых будут размещаться резервные ЦОДы, выполняющие синхронную репликацию данных, а между тремя ЦОДами городов будет реализована асинхронная репликация данных. «Это обеспечит переключение нагрузки в случае локальной аварии (катастрофы) ЦОДа в каждом городе, а также позволит переключать нагрузку в случае региональной аварии (катастрофы). Например, у системы «Экспресс» для продажи билетов в кассах допустимое время простоя составляет 1 час, и увеличение этого времени приводит к весьма серьезным негативным социальным последствиям», – подчеркнул И. Бессонов.

Иные требования к проектам создания ЦОДа предъявляют контент-провайдеры. Как пояснил Павел Завьялов, заместитель технического директора Mail.Ru, в ИТ-инфраструктуре компании насчитывается 9 тыс. серверов, из них 420 в собственном ЦОДе, остальные – в арендуемых центрах. При этом Mail.Ru выступает и как оператор связи, и как поставщик ресурсов Интернета, поддерживая взаимодействие со всем, что существует в российском сегменте Сети.

По мнению П. Завьялова, рынок ЦОДов в Москве для контент-провайдеров ограничен. «Если вы банк, у вас есть бизнес-задача и вам нужно десять стоек, то вы всегда найдете стойки в имеющихся ЦОДах. Но для Mail.Ru нет смысла арендовать меньше 100 стоек по причине подвода оптической связи к большому количеству точек, где они будут размещаться, а также по причинам административным. И когда я жалуюсь на то, что не могу найти нужное количество арендуемых

Avirsa Projects представила услуги проектирования и создания ЦОДов и решения для их оснащения – серверы Wexler Business Server с низким энергопотреблением

стоек, то это означает, что я не могу спланировать свою жизнь на три года вперед», – посетовал он.

При этом П. Завьялов утверждает, что владеть собственным ЦОДом экономически очень эффективно – честно пересчитанная экономистами стоимость владения стойкой в своем дата-центре существенно меньше, чем та, которую можно получить на рынке Москвы. В то же время строить ЦОД в Москве крайне дорого по причине высоких цен на недвижимость, а также проблем с энергоснабжением. «Электричества в Москве почти нет и оно очень дорогое. Как показывает практика, в Москве можно получить подключение к электроэнергии по 1-й особой категории, но та же практика показывает, что цена этого под-

Компания Powercom показала на своем стенде оборудование для корпоративных заказчиков – трехфазные ИБП VGD31, VGD33, ONL33

ключения равна нулю – обязательства, на которые готов подписаться оператор, по факту не выполняются, – сказал он. – Для Mail.Ru проблема безотказного энергоснабжения – это проблема номер один, и ее можно решить только за счет использования дизель-генераторов. Падение электричества – это огромные материальные потери, вызванные простоем, и заметные потери, связанные с тем, что, когда оборудования много, обратно включается не все. Та же проблема с кондиционированием, поскольку сбои в кондиционировании повышают износ оборудования. Это два требования, которые мы предъявляем к инфраструктуре ЦОДа».

Казалось бы, для Mail.Ru реальным выходом из ситуации, когда потребность компании в серверных мощностях быстро растет, является создание собственного ЦОДа за пределами Москвы. Но по ряду причин реализовать подобный проект в настоящее время трудно. Во-первых, придется перестраивать работу инженерных служб, что для компании представляет определенный риск. Во-вторых, логика развития Интернета в стране, в особенности в регионах, приводит к тому, что консолидировать серверные мощности поставщика контента можно только в Москве. «В любом регионе могут быть корпоративные ЦОДы, и понятно, на каких условиях можно договориться об аренде мощностей, но никто не понесет сотни стоек в регионы, потому что нести трафик обратно будет стоить дороже самих стоек в силу транзитных тарифов, – говорит П. Завьялов. – В большей части мы свой трафик должны будем направлять обратно в Москву, а гнать его по региональным тарифам, в 10 раз более высоким, экономически невыгодно. Наконец, я пока не видел предложений от региональных ЦОДов с качеством и с экономикой, которая нас устраивает».

Иной подход к развитию инфраструктуры ИТ и требования к построению собственных ЦОДов демонстрирует компания «МегаФон». Как рассказал Алексей Семеняка, руководитель группы услуг пакетных сетей ЦОД этой компании, в период 2005–2009 гг. потребности в площадях ЦОДов увеличивались в полтора раза ежегодно. В конце 2009 г. был построен – с соблюдением требований Tier III – ЦОД в Новосибирске, крупнейший за Уралом. В 2010 г. «МегаФон» купил компанию «Синтерра», ЦОДы которой вошли в состав ИТ-инфраструктуры оператора, и в октябре того же года был открыт крупнейший в России ЦОД в Самаре, впервые в стране сертифицированный по классу надежности Tier III.

«Нашей компанией запланировано создание крупнейшей в России сети ЦОДов, с тем чтобы охватить максимальную территорию и большее число абонентов. Мы подготовили программу строительства «больших ЦОДов», которые кроме Самары и Новосибирска будут созданы в Москве, Петербурге, Краснодаре и на Дальнем Востоке, – заявил А. Семеняка. – Это будут универсальные ЦОДы, которые компания будет использовать как для собственных нужд, так и предоставляя коммерческие сервисы: аренду площадей, стоек, физических и виртуальных серверов, а также сервисы инфраструктуры, платформ, ПО (*aaS)».

В то же время А. Семеняка подчеркнул, что большие инвестиции невозможны без детальной оценки и получения ответов на следующие вопросы: сколько ЦОДов требуется компании, какими должны быть параметры отдельного ЦОДа и каковы критерии выбора площадок для строительства. «Это многопараметрическая задача, включающая такие показатели: стоимость электроэнергии, возможность построения эффективного охлаждения в данном климате при заданном показателе энергоэффективности PUE, наличие поблизости магистрали ВОЛС, наличие трудовых ресурсов и др. Все эти измеримые деньгами параметры позволяют в каждом отдельном случае определять оптимальные характеристики ЦОДа», – считает он. При этом компания должна учитывать, что увеличение числа площадок проекта повышает катастрофоустойчивость, но делает невозможными мгновенную перестройку и рост существующей инфраструктуры. Сокращение числа площадок при консолидации ресурсов решает эти проблемы, но требует повышения производительности сети и перехода на новые технологии, что увеличивает стоимость проекта. И эта ситуация характерна для любого заказчика, планирующего создавать свои ЦОДы.

А. Семеняка также отметил общие подходы к построению современного ЦОДа: это универсальность, которой удается добиться за счет возможности изменения доли оборудования, выполняющего разные функции, гибкость благодаря модульной структуре ЦОДа и достижение максимально возможной энергоэффективности при значении показателя PUE = 1,3.

Почему так важна энергоэффективность?

В современном ЦОДе, как объяснил Алексей Мелешенко, директор по ИТ-инфраструктурным решениям компании «Ситроникс», не менее 50% операционных затрат приходится на стоимость потребленной электроэнергии, а удельное энергопотребление составляет не менее 2 кВт на квадратный метр полезной площади. Поэтому при среднем сроке жизни ЦОДа около 10 лет стоимость потребленной электроэнергии приближается к 50% совокупной стоимости владения (TCO), т.е. даже превышает капитальные затраты на строительство. «Если удастся сэкономить всего 10% от этого количества электроэнергии, годовая экономия может составить весьма значи-

ЦОД не должен сдерживать рост бизнеса!

Только InfraStruxure предлагает тройное преимущество постоянной готовности круглые сутки, без праздников и выходных, высокой оперативности и экономии за счет эффективности

Инженерная архитектура InfraStruxure нового поколения

Центр обработки данных должен служить компании опорой в росте — будь то удвоение продаж или численности персонала — а не становиться препятствием для ее развития. Однако слишком часто бизнес испытывает ограничения ресурсов систем инженерной инфраструктуры. Найдется ли в стойках место для дополнительных серверов? Хватит ли электрической мощности новым ИТ-системам? APC by Schneider Electric удалось решить эти проблемы с помощью проверенной практикой высокопроизводительной, масштабируемой и комплексной инженерной архитектуры ЦОДа InfraStruxure.

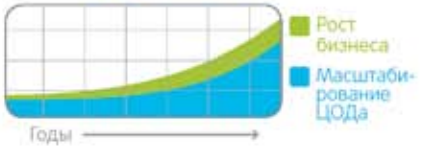
Центры обработки данных InfraStruxure — опора бизнеса!

Мы называем центры обработки данных, построенные на основе инженерной архитектуры InfraStruxure, опорой бизнеса. Что это значит? Все очень просто. ЦОД можно назвать опорой бизнеса, когда он: находится в постоянной готовности круглые сутки без праздников и выходных; постоянно работает на наивысшем уровне характеристик; поспевает за стремительным ростом бизнеса; на каждом этапе — от проектирования до эксплуатации — выходит на все более высокие уровни эффективности использования энергии и способен развиваться в гармонии с основной деятельностью компании. Более того, модульная инженерная архитектура InfraStruxure позволяет спроектировать интегрированное решение, в точности соответствующее требованиям на сегодняшний день и легко адаптируемое к их изменениям в будущем.

Тройное преимущество InfraStruxure

InfraStruxure предлагает тройное преимущество качественного превосходства: высочайший уровень готовности, простоту и оперативность адаптации к изменениям требований бизнеса и экономию за счет эффективного использования энергии. Как можно быть лучшей «опорой бизнеса», не обеспечивая качество, скорость и экономию одновременно?

InfraStruxure



Центры обработки данных InfraStruxure — опора бизнеса!

- Готовность: безостановочная работа круглые сутки без праздников и выходных благодаря лучшим в своем классе системам электропитания ответственного оборудования с модульными блоками распределения питания, системам охлаждения с теплообменниками, максимально приближенным к источникам тепла, а также ПО контроля и моделирования изменений параметров инженерных систем.
- Оперативность: простота развертывания инженерной инфраструктуры в сжатые сроки. Все компоненты системы спроектированы с учетом совместной работы, а архитектура в целом рассчитана на любые, самые высокие темпы роста бизнеса.
- Эффективность: благодаря передовым конструктивным решениям, включая трехступенчатые инверторы ИБП и вентиляторы систем кондиционирования с переменной скоростью вращения, достигается настоящая эффективность использования и экономия энергии.
- Управляемость: управляющее ПО InfraStruxure Management Software позволяет отслеживать и управлять свободными ресурсами и уровнем резервирования систем электропитания и охлаждения, а также свободным пространством в стойках для оптимального использования ресурсов инженерной инфраструктуры центра обработки данных.
- Гибкость: начиная с совместимости шкафов с ИТ-оборудованием любых производителей до полной масштабируемости по электропитанию и отводу тепла.

Загрузите БЕСПЛАТНО информационные статьи APC в течение 30 дней, ответьте правильно на вопросы и получите шанс выиграть планшетный компьютер iPad!

Зайдите на сайт www.apc.com/promo и введите код 97131t

APC by Schneider Electric

тельную величину. По данным конференции AFCOM за 2008 г., в типичном ЦОДе 50% электроэнергии тратится на оборудование ИТ, 37% потребляет система охлаждения и кондиционирования воздуха, 10% – потери в системе бесперебойного электроснабжения и энергораспределения. Так как ИБП достигли предельных показателей эффективности, то можно попытаться сократить расходы на систему охлаждения», – считает А. Мелешенко.

Если в ЦОДах предыдущих поколений обычно используют холодильники, охлаждающие воздух, то «Ситроникс» предлагает применять технологию свободного охлаждения (free cooling), считая, что для наших широт вполне естественно использовать холодный наружный воздух для охлаждения ИТ-оборудования в ЦОДе. Но А. Мелешенко отметил, что практически сделать это в существующих ЦОДах сложно – они не проектировались для подачи больших количеств наружного воздуха непосредственно к ИТ-оборудованию, а в системах охлаждения применяется охлажденная вода, которая подается в машинный зал. И ее закачка насосами вносит заметный вклад в снижение энергоэффективности ЦОДа.

«Ситроникс» представил свою линейку модульных центров обработки данных Daterium серийного производства, с контейнером уникальной конструкции

Л. Шишлов, отмечая аналогичную ситуацию в существующих ЦОДах, привел такие данные. В стандартных дата-центрах, где используемая мощность не превышает 2–4 кВт на стойку, системы кондиционирования, как правило, работают неэффективно – горячий воздух от серверов перетекает в «холодный коридор», где смешивается с холодным воздухом, что приводит к дополнительному расходу энергии и денег. Поэтому Intel предлагает перестраивать существующие ЦОДы, применяя вытяжные шкафы и системы герметизации горячего воздуха, которые могут одновременно использоваться в одном ЦОДе. Вытяжные серверные стойки делают весь ЦОД «холодным коридором», и при этом появляется возможность более глубокой консолидации оборудования в серверных стойках, которые могут потреблять более 25 кВт на стойку.

Такой конструктивный подход к трансформации ЦОДа дал возможность Л. Шишлову заявить: «Лучший ЦОД – это тот, что не надо строить!».

Стандарты, которым стоит следовать

При трансформации или строительстве ЦОДа проектировщики все чаще стремятся сертифицировать свое решение по одному из уровней (Tier), предложенных Uptime Institute.

Как рассказал Марк Эктон, директор сети Uptime Institute в регионе EMEA, в 1992 г. была разработана базовая топология инженерной инфраструктуры ЦОДа, которая завоевала признание в отрасли. Правда, он подчеркнул, что в 2009 г. Uptime пересмотрела многие документы, выпущенные ею ранее: «Сейчас мы говорим о топологии как о плане, позволяющем достичь того уровня готовности, отказоустойчивости, бесперебойности в работе ЦОДа, который требуется заказчикам. Предлагаемые нами уровни – от Tier I (базовый) до Tier IV (наивысший) – отражают соответствие независимым стандартам. На основании этих стандартов мы представляем поставщиков, говорим о надежности, о доступности данных, устойчивости, предлагаем разные показатели, позволяющие сравнивать ЦОДы с точки зрения как поставщиков, так и заказчиков. Кроме того, мы стимулируем инновационное проектирование и конструирование ЦОДов».

М. Эктон объяснил, что консультационный комитет Uptime Institute оказывает помощь операторам ЦОДов, заказчикам, пользователям. Но при этом Uptime – независимая от вендоров организация, ее консультанты не предлагают и не рекомендуют никакого конкретного оборудования клиентам, они используют объективный подход для оценки проектов ЦОДа и сертификации построенных центров. Для этого на первом этапе проверяется документация проекта, из которой делается вывод о том, какого уровня ЦОД можно построить. Затем оцениваются процессы развертывания и строительства ЦОДа, чтобы понять, насколько они соответствуют первоначальному проекту. Наконец, консультанты Uptime проверяют физическую инженерную инфраструктуру созданного ЦОДа и сертифицируют его по определенному уровню (Tier) надежности, бесперебойности, отказоустойчивости. В настоящее время консультанты Uptime работают в 40 странах мира и уже участвовали в обследовании и сертификации более 110 ЦОДов.

Естественно, что в ЦОДе, сертифицированном по уровню Tier IV, за счет резервирования всех систем и мониторинга их состояния обеспечена высокая бесперe-

бойность: если возникает отказ, ЦОД автоматически реагирует на него за считаные минуты. Хотя, как заметил М. Эктон, далеко не всем заказчикам требуется ЦОД, сертифицированный по уровням Tier III или IV: «Для них было бы достаточно ЦОДа уровня Tier II, однако в нем рано или поздно может выйти из строя участок инфраструктуры (единой сети электропитания, единой системы охлаждения и т.д.), что нарушит работу центра в целом».

Компания «МегаФон» отметила, что ЦОДы, построенные в Самаре и Новосибирске, были сертифицированы по уровню Tier III. Пример трансформации дата-центра в Москве привел Дэвид Хамнер, президент DataSpace – российской компании, которая в сотрудничестве с Uptime Institute занимается строительством и перестройкой ЦОДа уровня Tier III. В его здании в районе Таганки общей площадью 6000 кв. м создано 12 машинных залов, каждый около 230 кв. м, и заново выстроена вся инженерная инфраструктура. По рекомендации консультантов Uptime в проект в ходе строительства были внесены определенные изменения, повысившие отказоустойчивость ЦОДа: например, замена имеющихся скоростных переключателей нагрузки в разы увеличила надежность.

На стенде Conteg – готовый модуль для решения с отводом тепла через вытяжную трубу на базе шкафа RSF-42-60/120

Когда стандарты бессильны

Компания ADM Partnership, как рассказал ее генеральный директор Максим Иванов, реализовала для Сбербанка РФ проект ЦОДа, который стал одним из первых в России, сертифицированных по Tier IV. При этом М. Иванов отметил, что такие параметры, как уровни надежности и доступности по стандартам Tier или энергоэффективность PUE, должны рассматриваться с точки зрения целевого назначения ЦОДа – в корпоративном дата-центре скорее всего будет более важен уровень функциональности и надежности, а не PUE. Должна учитываться стоимость электроэнергии в регионе, где строится ЦОД, – если стоимость киловатт-часа мала, то можно затратить меньше денег на строительство, получая не только абстрактную, но и коммерческую эффективность. Наконец, необходимо обращать внимание на качество реализации решения: по проекту оно может относиться к уровню Tier III, но некачественный монтаж приведет к потерям, – а также на соблюдение опреде-

ленных условий эксплуатации ЦОДа: например, если зимой открывают двери, то тратится больше энергии на обогрев, и затраты растут.

И в этом с М. Ивановым целиком согласен М. Эктон: «Наш опыт показывает, что недостаточно построить самый лучший ЦОД, так как если его не обслуживать должным образом, ничего не выйдет. Большая часть – 73% – проблем, возникающих в ЦОДе, связана с человеческим фактором. Ведь по какому бы уровню ЦОД не был сертифицирован, главное, чтобы он эксплуатировался эффективно, чтобы его сотрудники были специалистами высочайшей квалификации, чтобы они работали ответственно, чтобы они были мотивированы. Поэтому мы пытаемся разработать стандарт операционной устойчивости, который помог бы компаниям, эксплуатирующим ЦОДы, подняться выше уровня физической инфраструктуры».

Компания «Линдекс» совместно с Huber+Suhner продемонстрировала подход к подключению оптических коммутаторов типа Brocade – при помощи оптических претерминированных кабельных сборок

От генподряда до сопровождения эксплуатации ЦОДа

Компания HP известна в России как поставщик компьютерных систем и технологических решений для построения ИТ-инфраструктуры. Но на конференции «ЦОД-2011» она предстала в новой роли – поставщика услуг полного цикла проектирования и строительства ЦОДа.

Как отметил Александр Зайцев, менеджер по развитию ЦОД подразделения CFS HP Россия, еще в 1972 г. в США была создана компания Einhorn Yaffee Prescott (EYP), которая начала предлагать услуги оптимального проектирования ЦОДов. После того как в течение 2004–2007 гг. EYP консолидировала более 87 ЦОДов и полученная заказчиками экономия оказалась весьма значительной, Hewlett-Packard решила приобрести эту компанию, создав в своей структуре подразделение по оказанию услуг HP Critical Facilities Services (CFS).

В настоящее время подразделение HP CFS предлагает заказчикам, в том числе российским, услуги, относимые к четырем группам: Critical Facilities Consulting (консультации и технологическое планирование ЦОДов), Critical Facilities Design (проектирование инженерных систем, технологической инфраструктуры, планирование и оценка стоимости), Critical Facilities Assurance (разработка стратегии функционирования, тестирование и ввод ЦОДа в эксплуатацию), Critical Facilities Implementation (проектирование и строительство ЦОДов «под ключ»). Кроме того, это подразделение HP проводит работы по анализу энергоэффективности, состояния и возможностей инфраструктур, термическому анализу, оценивает операционные риски и оказывает услуги по выбору строительной площадки (Critical Facilities Standardized Services).

Создаваемые ранее ЦОДы, отметил А. Зайцев, как правило, имели монолитную конструкцию, где в машинных залах не разделялись зоны оборудования, обрабатывающие задачи разного уровня критичности для заказчика. HP предлагает переходить к «гибридным» конструкциям, где уровень Tier в отдельных машинных залах будет адекватен задачам, что сэкономит не только деньги, но и физическую площадь. В России есть примеры реализации проектов «гибридных» ЦОДов, отвечающих уровню Tier III.

На основе «гибридной» концепции HP разработала типовой проект ЦОД «Бабочка» – сборную конструкцию из пяти модулей. Модуль для размещения ИТ-оборудования рассчитан на 160 стоек и 800 кВт энергопотребления; он обслуживается модулями охлаждения, генератора и управления параметрами питания. Все модули собираются на заводе в США (в Европе пока нет), затем привозятся на площадку и в течение шести месяцев собираются, что существенно сокращает затраты средств и времени. Но в России, признал А. Зайцев, примеров реализации подобных проектов пока нет.

Контейнерные ЦОДы – это экономия

Дополнительную возможность ускорить построение современного ЦОДа HP видит в использовании мобильных комплексов HP POD и HP EcoPOD. Фактически эти комплексы представляют собой законченные ЦОДы «в контейнере», в состав которых, кроме стоек для размещения ИТ-оборудования, входят системы энергоснабжения, охлаждения и мониторинга электропитания и состояния всех инженерных инфраструктурных систем.

А. Мелешенко, в свою очередь, представил разработанные «Ситроникс» мобильные «контейнерные» ЦОДы Daterium-2 (обеспечивает уровень доступности Tier II) и Daterium-3 (Tier III). Он подчеркнул, что такие контейнерные ЦОДы, вмещающие 6–7 стоек для установки ИТ-оборудования, позволяют достаточно легко реализовать систему охлаждения free cooling, которая оказывается на 3–4 порядка более производительной, чем система вентиляции в большинстве существующих стационарных ЦОДов, и увеличивают срок службы кондиционеров (на широте Москвы примерно в три раза). Кроме того, «контейнерные» ЦОДы Daterium можно устанавливать на неподготовленную площадку.

«В результате эксплуатации Daterium-3, работавшего с использованием системы охлаждения free cooling, мы получили среднегодовое значение показателя энергоэффективности PUE, равное 1,28, в то время как в существующих ЦОДах этот показатель достигает величины 2,0!», – заявил А. Мелешенко. ИКС

Семь вопросов дилетанта о сервисной поддержке инженерной инфраструктуры ЦОДа

Павел КОСТЮРИН,
директор департамента сервиса и аутсорсинга компании «АМДтехнологии»

Современный ЦОД – это живой организм, требующий пристального внимания. Но не всегда его инженерную инфраструктуру может полноценно обслуживать собственный отдел эксплуатации. В таких случаях целесообразно отдать сервисную поддержку на аутсорсинг в профильную инженерную компанию.

1. Мы построили ЦОД. Что дальше?

Любой ЦОД требует регламентного обслуживания. Какова бы ни была его стоимость, сколько бы стоек в нем ни было установлено, если есть инженерная инфраструктура – системы кондиционирования, бесперебойного гарантированного электроснабжения и т.д., их обязательно нужно обслуживать. Практически все инженерное оборудование имеет рекомендуемые графики проведения регламентных работ, а сложные системы вообще не подлежат гарантии без заключения заказчиком сервисного договора с авторизованной организацией.

2. Можно ли полагаться на свою службу эксплуатации?

Зачастую собственная служба эксплуатации компании – владельца ЦОДа не имеет достаточной квалификации для выполнения даже половины требуемых работ. Обеспечение функционирования среднестатистического центра обработки данных складывается из обширного перечня задач (см. таблицу). Не говоря уже о складе запасных частей, которые нужно закупать и всегда иметь под рукой для того, чтобы можно было гарантировать отказоустойчивость ЦОДа и непрерывность предоставления сервисов.

Прогресс не стоит на месте, и требования к исполнителям в области сервисной поддержки из года в год становятся все строже. Буквально несколько лет назад поддержку оборудования в режиме 24 × 7 могли предоставить только такие «монстры», как Sun, IBM, HP, APC. Сейчас же речь идет не о прибытии обслуживающей бригады на место аварии в течение четырех или двух часов после размещения заявки и даже не о способности исполнителя гарантировать устранение неисправности не более чем за четыре часа после регистрации заявки. Мы вышли на уровень, когда заказчики оперируют такими понятиями, как «процент гарантированной доступности инженерной инфраструктуры ЦОДа в год». Например, одному из наших заказчиков была нужна гарантированная доступность сервисов ЦОДа в год не менее 99,95%! И эти требования, как правило, вовсе не прихоть. Они обусловлены размером убытков от перерыва предоставления ЦОДом сервисов, ведь стоимость подобного обслуживания на порядок выше стандартного.

Сервисные задачи для поддержки среднестатистического ЦОДа

ЧТО?
Система кондиционирования
Система бесперебойного энергоснабжения (ИБП, ДГУ)
Система автоматического газового пожаротушения
Система контроля доступа и видеонаблюдения
Структурированная кабельная система
Выделенная электросеть
Система мониторинга окружающей среды и параметров энергопотребления серверных помещений
Система фальшпола серверного помещения
Система дренажа
КАК?
Обеспечение отказоустойчивости (время простоя ЦОДа не более 20 мин в год)
Время прибытия на объект в случае аварийной ситуации не более 4 часов в режиме 24 × 7
Время восстановления работоспособности обслуживаемого оборудования не более 4 часов (высокий приоритет)
Замена вышедшего из строя ЗИП
Ежемесячное регламентное обслуживание подсистем
Создание, верификация и поддержание в актуальном состоянии комплекта документов, описывающих обслуживаемую подсистему
Поддержка «горячей» линии в режиме 24 × 7
Предоставление доступа к системе регистрации запросов
Выполнение работ от замены лампочки до настройки систем мониторинга
Заправка ДГУ топливом, гарантированное время заправки – не более 4 часов с момента получения заявки, в режиме 24 × 7
Гарантия доступности ЛЮБЫХ ресурсов в любое время
Аудит эффективности инженерных систем
Превентивное решение проблем с оборудованием с помощью мониторинга основных его показателей
Уборка серверного помещения (еженедельный клининг, ежеквартальная уборка под фальшполом, вакуумная продувка стоек)
Подсобные работы

3. Как создать такую систему обслуживания?

Прежде всего нужно провести аудит всей инженерной инфраструктуры на соответствие условиям работы и проанализировать ее эффективность. В случае необходимости выдвинуть предложения по усовершенствованию систем или замене оборудования. Неразумно браться за обслуживание инженерной инфраструктуры, расчетная мощность которой ниже требуемой ИТ-оборудованием.

После выполнения этой немаловажной задачи можно подумать и об инструментах для организации собственно обслуживания. Без дежурной смены при этом не обойтись. Например, в упоминавшемся случае с обеспечением доступности ЦОДа на уровне четырех девяток было предложено создать две дежурных смены, причем одну непосредственно на объекте. В ее обязанности входило:

- с помощью систем мониторинга следить за состоянием ЦОДа и окружающей среды;
- проводить обход и осмотр всего инженерного оборудования один раз в два часа;
- при отказе оборудования не позднее чем через пять минут проверить выполнение автоматического ввода резерва или ввести в работу резервное оборудование вручную;
- не позднее 30 минут с момента регистрации выхода инженерного оборудования ЦОДа в аварийный режим работы выявить неисправное устройство и причину отказа и при необходимости вызвать вторую дежурную смену;
- документировать все свои действия и состояние оборудования в реальном времени.

Вторая дежурная смена, как вы поняли, состояла из инженеров, готовых прибыть на объект в течение часа.

Ну и конечно же под проект был закуплен ЗИП и регулярно выполнялось регламентное обслуживание оборудования.

4. Хорошо, убедили. Но какой уровень сервиса нужен для ЦОДа?

Для начала нужно определиться, насколько важна непрерывность его функционирования.

Если критичность простоя невысока либо имеется резервирование элементов инфраструктуры (N + 1, 2(N + 1)) или целых подсистем (S + S), то сервисные организации можно привлекать для проведения регламентных работ или по факту выхода оборудования из строя.

Если же критичность простоя высока, то к организации сервисной поддержки нужно подходить очень ответственно. В первую очередь требуется сервисная организация, имеющая опыт эксплуатации таких объектов. Это может быть как мультиинжиниринговая компания, так и системный интегратор, который умеет хорошо управлять сервисными проектами и у которого есть квалифицированные и надежные партнеры по инженерным системам.

5. Как же выбрать аутсорсера?

Для того чтобы не ошибиться при выборе аутсорсера, который будет осуществлять сервисную поддержку инженерной инфраструктуры ЦОДа, следует руководствоваться несколькими важными критериями.

Во-первых, аутсорсер должен гарантировать конфиденциальность информации. Не лишним будет заключить соглашение о конфиденциальности с каждым потенциальным участником конкурса. Помимо ответственности за разглашение информации исполнитель должен нести ответственность за работу, которую он выполняет. Предоставляемые им услуги должны строго соответствовать соглашению об уровне сервиса (SLA) – самому важному документу в сервисном контракте.

Во-вторых, аутсорсер обязан оказывать услуги комплексно. И желательно, чтобы он обходился своими ресурсами. Ведь в таком случае путь прохождения заявки значительно сокращается и время реакции, соответственно, тоже. С другой стороны, мы прекрасно понимаем, что редкая инженерная компания обладает всеми ресурсами, необходимыми для эксплуатационного обслуживания ЦОДа (см. таблицу), и, скорее всего, ей придется брать кого-то на субподряд. В этом случае я бы предложил организовать ознакомительную встречу, на которой присутствовали бы все исполнители по всем системам, чтобы вы могли сами оценить их компетентность и квалификацию.

И наконец, инженерный персонал аутсорсинговой компании обязательно должен пройти сертификацию на выполнение работ, предусмотренных сервисным контрактом. Требуйте прислать вам копии всех необходимых сертификатов ДО заключения договора.

6. Как научить исполнителей разговаривать со мной на одном языке?

Прежде всего необходимо дать понять сервисной организации, что для вас важно не только соблюдение регламентов и стандартов сервиса, но и интеграция сервисного проекта в структуру бизнес-процессов предприятия. Это значит, что исполнителям придется думать не только о выполнении своих работ, но и об их влиянии на ваши бизнес-процессы, придется продумывать и согласовывать с вами планы проведения работ и т.д.

7. Для чего сервисной компании соглосовывать со мной планы работ?

Давайте представим себе ситуацию: в вашем ЦОДе запланированы регламентные работы на дизель-генераторной установке, которые помимо всего остального включают в себя замену охлаждающей жидкости и сезонную смену топлива в баке. В случае пропадания внешнего электропитания ИБП смогут поддерживать работу ЦОДа не более 15 мин. А при слитых охлаждающей жидкости и топливе, чтобы привести ДГУ в состояние, когда она сможет запуститься, потребуется более получаса.

Выходит, не получи вы план проведения данных регламентных работ с временными интервалами, вы бы не увидели, какой риск грозит вашему центру обработки данных в случае пропадания городского питания. Вы дадите согласие на такие работы? А если минута простоя ЦОДа стоит миллион долларов?

■ ■ ■

Как бы то ни было, привлекать сервисных интеграторов или делать все своими силами – решать вам. ИКС

Ясно как в тумане

Создание инфраструктуры в многоквартирных домах

Дэвид МИКЛОВИЧ, директор по продуктам компании Emerson Network Power

Оптические сети подходят все ближе к абоненту, усложняя создание в многоквартирных домах инфраструктуры электропитания для телекоммуникационных систем.

Будущее передачи голоса, данных и видео – оптоволоконные линии, и это будущее уже наступает. Оптоволокно, конечно, устраняет необходимость промежуточных систем питания для усиления сигнала в медных линиях. Однако его использование не решает всех проблем с электропитанием в телекоммуникационных сетях. Наоборот, повсеместное развертывание широкополосных сетей и вызванные им ожидания пользователей являются источником новых проблем при создании инфраструктуры электропитания для сетей связи.

Не будем забывать, что электронные устройства должны преобразовывать звуки и изображения в световые импульсы для передачи по оптоволоконным линиям, а затем преобразовывать эти импульсы обратно в цифровую информацию для прослушивания и просмотра. А для работы электронных устройств требуется источник питания постоянного тока. Несмотря на то что многие сложности здесь удалось преодолеть, питание оптических сетей в многоквартирных домах остается проблемой. И вопрос здесь в том, кто будет предоставлять это электропитание и где будет располагаться соответствующее оборудование.

История вопроса

Изначально операторы связи создавали активную сеть из медных линий и подавали в них питание 48 В постоянного тока с аварийным питанием от аккумуляторных батарей. Точки подключения электропитания находились в центральном узле и в других узлах по всей сети для того, чтобы ослабить влияние сопротивления медных проводов. Между тем оптоволоконные линии потребляют небольшое количество энергии даже при передаче сигналов на большие расстояния. Компании, предоставляющие кабельные услуги, развернули оптику быстрее, чем операторы связи, и теперь конкурируют с последними в области предоставления услуг triple play (передачи голоса, данных и видео).

Медные линии, используемые в традиционных сетях, позволяют доводить сигнал с постоянной мощностью непосредственно до центрального узла. Однако при передаче сигналов на большие расстояния их пропускная способность ограничена. Кроме того, большая часть медных линий эксплуатируется уже 50–60 лет и серьезно повреждена коррозией. Поэтому, чтобы скомпенсировать потери в наземных линиях и повысить конкурентоспособность по отношению к кабельным компаниям, операторы связи расширяют использование оптоволокна, заменяя им отдельные участки своих старых сетей, архитектура которых основана на центральном узле. Это позволяет предоставлять абонентам услуги, требующие высокой пропускной способности.

По мере того как оптоволокно все глубже проникало в операторские сети (и сегодня добралось до пассивных участков от центрального узла до домов или предприятий и не требует источников питания в промежуточных точках), вопросы электропитания становились менее острыми. Какую бы сетевую архитектуру вы ни выбирали, отрасль быстро предлагала соответствующее решение по обеспечению электропитания (даже для такой трудночитаемой разновидности аббревиатуры FTTx, как FCeTTH – Fiber Close enough To The Home, т.е. оптика до максимально близкой к дому точки). Эти решения имеют различную конфигурацию, рабочее напряжение, размеры и место установки, однако все они в большинстве случаев выполняют свою главную функцию без каких-либо проблем.

Единственным раздражающим исключением был и остается вопрос с многоквартирными домами.

Неочевидные трудности

Несмотря на новейшие технологические достижения, доведение оптоволокна до абонентов в многоквартирных домах – задача по-прежнему более трудная по сравнению с той, которую приходится решать в частных домах. Само прокладывание оптического кабеля до пользователей не сложнее, чем проведение медной витой пары. Основные трудности вызывает преобразование оптических сигналов в электрические.

Есть несколько вариантов развертывания сетей, но ни один из них не является оптимальным для проведения оптоволоконных линий в многоквартирные дома. В здании можно установить главный оптический распределительный концентратор (FDH), подключенный к домовой электросети и преобразующий оптические сигналы в электрические. Оператор может разместить этот концентратор в подвале или цоколе здания и через кабель-каналы протянуть от него коаксиальный кабель или кабель категории 5 до отдельных пользова-

телей. Также оптические кабели могут быть проложены из подвала здания до индивидуальных абонентских терминалов (ONT), расположенных внутри квартир или на этажах. Доступ к сети возможен и с помощью Wi-Fi. Развертывание сети может выполняться различными способами в зависимости от структуры здания и требуемого количества подключений. Однако сложность заключается вовсе не в технологии создания сети.

Например, если в доме живет 500 человек, то при установке электронного оборудования в подвале здания простого подключения электропитания мощностью 300 Вт будет недостаточно – оператору придется установить там небольшую электростанцию постоянного тока и обслуживать ее. Это означает, что персонал оператора должен иметь в это помещение круглосуточный доступ. Однако поскольку территория здания оператору не принадлежит, это может вызвать массу споров по правам жильцов и владельцев здания, не говоря уже о проблемах безопасности. Если же электронное оборудование расположено за пределами многоквартирного дома, приходится решать вопросы по защите окружающей среды, выделению участка для размещения оборудования и обеспечить подключение к генераторам аварийного питания.

Кроме того, в одних домах есть подвалы, а в других их нет, в одних предусмотрены монтажные шкафы, в других – нет. Распределительный концентратор, может быть, нужно располагать на крыше и пробрасывать коаксиал или кабель категории 5 вниз. Очевидным решением было бы завести оптоволокно в каждую квартиру и установить резервную батарею в каждой жилой секции, но в некоторых домах размещение аккумуляторных батарей запрещено противопожарными правилами или условиями страхования. Поэтому подход в каждом случае свой – как правило, это смесь оптоволокна, меди и иногда небольших Wi-Fi-сетей.

Баталии из-за резервных батарей

Как и следовало ожидать, такая ситуация вызывает массу непрекращающихся споров о том, кто должен нести ответственность за резервное питание. Одни операторы заявляют, что их ответственность не простирается дальше обеспечения исправности оборудования и питания для оптоволоконной линии на центральном узле. Они считают, что установкой резервных аккумуляторных батарей должен заниматься владелец здания.

Другие соглашаются взять на себя часть ответственности и устанавливают средства оповещения на абонентские терминалы (ONT) или модули (ONU). Эти устройства посылают пользователям по оптической линии сообщения о том, что аккумуляторная батарея почти разрядилась и ее необходимо менять. Также и сам терминал может оснащаться индикаторами, предупреждающими пользователя о низком заряде аккумуляторной батареи. Если модули ONU или терминалы ONT установлены за пределами здания, то оператор может взять на себя ответственность за них благодаря наличию круглосуточного доступа. Если же эти устройства установлены, например, в гараже домовладельца, то установка розетки переменного тока и обслуживание аккумуляторной батареи должны выполняться самим домовладельцем. Однако кто будет нести ответственность за токсичные материалы при замене аккумуляторной батареи? Оператор сдаст батарею в службу утилизации, но обычный пользователь, скорее всего, выбросит ее на свалку.

При длительных отключениях электроэнергии система может выключить передачу видео, чтобы снизить энергопотребление и как можно дольше поддерживать передачу голоса и данных. Чаще всего в терминалах ONT используются небольшие 12-вольтовые аккумуляторные батареи, которые способны обеспечить питание электронного оборудования в течение 6–12 ч в зависимости от того, какие функции задействуются. При использовании всех функций их может хватить лишь на 4 ч, а при передаче только голоса время работы увеличится до 24 ч. Реальная продолжительность работы будет зависеть от состояния батареи, температуры окружающего воздуха и т.д.

> При переходе на VDSL и HDTV энергопотребление растет. Десять лет назад линия на протяжении большей части дня потребляла 1 Вт, а теперь – 2–3 Вт

Следует помнить, что при переходе на VDSL и HDTV энергопотребление растет. Десять лет назад линия на протяжении большей части дня потребляла 1 Вт, а теперь практически весь день потребляет 2–3 Вт. В то же время пользователи все более отрицательно относятся к аварийным отключениям при перегрузке системы и кратковременному использованию аварийных источников питания. Для операторов, которые не ограничиваются телефонной связью и предоставляют услуги кабельного телевидения и доступа в Интернет, локальные отключения электроэнергии и связанное с ними ухудшение обслуживания абонентов являются настоящей головной болью. И основания для этого веские. Вам бы хотелось, чтобы ваш VoIP-телефон замолчал? Почему бы в таком случае не воспользоваться сотовой связью? Или чтобы в то время, когда вы смотрите телепередачу, пропал сигнал HD TV только потому, что кто-то выключил не тот рубильник в электрощитовой? Поскольку услуги поставляются в комплексе, то неприятные последствия будут более серьезными, чем при отключении только доступа в Интернет, как в настоящее время.

Потому неудивительно, что потребители негативно относятся к автоматическим отключениям электроэнергии. Вы сможете смотреть передачи HD TV в случае частичного отключения электроэнергии? А видео через YouTube?

Будущее тонет в тумане

Волна развертывания широкополосных сетей заставила обратить серьезное внимание на топологию оптических сетей. Но несмотря на то что операторы по всему миру запускают крупномасштабные широкополосные проекты, нерешенные вопросы размещения оптических линий в многоквартирных домах остаются. И с ними столкнется каждый оператор независимо от того, находится ли он уже в процессе строительства оптоволоконных сетей или только приступает к нему.

На первых порах в качестве временной меры, чтобы удержать абонентов от перехода к конкурентам-кабельщикам, операторы могут подводить оптику на близкое расстояние к зданию клиента и использовать существующие медные линии там, где это возможно. Но многие специалисты считают, что подобные топологии (FTTN, FTTC) через 5–10 лет устареют и операторам придется устанавливать оптические кросс-коммутаторы и оптические разветвители, чтобы подвести оптические линии на расстояние не более 150 м к модулям ONU или терминалам ONT каждого абонента.

Взрывной рост спроса на телевидение высокой четкости и онлайн-видео создает на широкополосные службы такие нагрузки, с которыми могут справиться только оптические линии, особенно если приплюсовать сюда передачу данных и голосовую связь. Компаниям, которые занимаются строительством многоквартирных домов, также приходится учитывать этот момент.

Какую бы архитектуру не имел многоквартирный дом, потребность в системе электропитания постоянного тока не исчезает, а лишь видоизменяется. Могут отличаться требования к рабочему напряжению, размеру и способу использования систем, они могут устанавливаться на крышах зданий или на столбах, но эти системы в здании должны присутствовать обязательно. Также система обязательно должна оснащаться аккумуляторной батареей – будь то небольшого размера 12-вольтовая батарея или крупная моноблочная аккумуляторная ячейка.

Ну а кроме того, нужно решить, кто должен владеть этими системами и где они должны располагаться.

■ ■ ■

Несмотря на то что в решении описанных проблем принимают участие поставщики услуг, пользователи, владельцы зданий и земельных участков, местные администрации, торговые компании и другие стороны, до сих пор неясно, как можно упростить развертывание сетей в многоквартирных домах. ИКС

Мультибрендовая IP-видеосистема: выбираем управляющее ПО

Михаил МАЛОВ,
ведущий эксперт компании «АРМО-Системы»

Независимо от того, какую из двух задач вам предстоит решить – модернизировать существующую гибридную видеосистему или создать сетевую с нуля, в первую очередь необходимо грамотно выбрать управляющее программное обеспечение.

Сегодня на рынке свои продукты предлагают компании – производители IP-оборудования и ПО, а также платформо-независимые разработчики. Рассмотрим на конкретных примерах, что следует учитывать, выбирая ПО для управления многоканальной мультибрендовой системой видеонаблюдения.

Общий знаменатель

Сила и слабость мультибрендовой IP-видеосистемы в том, что в единой связке функционируют IP-устройства разных вендоров, которые должны не только быть идеально совместимы между собой, но и соответствовать предъявляемым к системе требованиям. Вместе с тем свои ограничения накладывают и специфика того или иного объекта, и характеристики проложенной/проектируемой сети, и, наконец, всегда непомерно узкие рамки бюджета. Поэтому и аппаратные и программные компоненты имеет смысл подбирать трезво и взвешенно.

Создание многоканальной IP-видеосистемы подразумевает наличие базового комплекта оборудования – IP-камер различных типов, видеосерверов, сетевых видеорегистраторов и т.д., а также ПО для их администрирования и работы с видео и данными. При существенных различиях профессиональные программные решения для систем видеонаблюдения и безопасности известных зарубежных производителей имеют ряд одинаковых свойств, в числе которых:

- открытая архитектура «клиент-сервер»;
- поддержка многосерверных конфигураций;

- возможность инсталляции на ПК либо аппаратные устройства регистрации (например, NVR);
- централизованное и/или локальное управление, удаленное администрирование видеосистемы;
- практически неограниченная расширяемость, позволяющая задействовать в системе сотни и тысячи IP-устройств;
- возможность выбора стационарных и мобильных клиентских приложений;
- разнообразные режимы записи аудио- и видеоинформации, поиска данных в архиве, просмотра и анализа текущего и архивного видео, экспорта видеофрагментов и др.

В теории ПО для многоканальных мультибрендовых IP-видеосистем обеспечивает все необходимые функции для охранного видеонаблюдения, а также поддержку IP-камер и сетевого оборудования многих торговых марок, присутствующих на российском рынке. А как на практике?

Комплексный подход

Главное, что выделяет современные программные продукты известных компаний, – это открытость для интеграции с новейшими IP-устройствами системы видеонаблюдения, а также системами контроля и управления доступом (СКУД), охранно-пожарной сигнализации (ОПС) и другими приложениями, которые могут использоваться в составе системы безопасности объекта. Один из удачных примеров такого комплексного подхода – ПО Video Surveillance Manager компании Cisco (CVSM).

Поскольку функционал CVSM реализован с применением стандартных сетевых протоколов, с помощью этого программного обеспечения можно управлять локальной или распределенной IP-видеосистемой на базе IP-устройств Cisco и других производителей, среди которых AXIS, Bosch, IQinVision, Panasonic, Sony и др. Полнофункциональное ПО работает под управлением ОС Linux, имеет модульную структуру и обеспечивает передачу, мониторинг, хранение и управление данными. Неоспоримое достоинство этого решения – гибкость: чтобы создать видеосистему требуемого масштаба и конфигурации, достаточно комбинировать аппаратные компоненты (камеры, видеосерверы, маршрутизаторы) и отдельные модули CVSM.

Ядром IP-видеосистемы может являться модуль Video Surveillance Media Server, предназначенный для веб-мониторинга, управления всеми видеоисточниками в системе и т.д. Он «отвечает» за сбор, маршрутизацию, непрерывную, событийную и/или экстренную запись видео и аудио с камер, контроль полосы пропускания каналов и т.д. Модуль MS поддерживает видеокодеки M-JPEG, MPEG-4 и H.264, функцию Dual Streaming и др.

Удаленное конфигурирование оборудования и его интеграцию в системные приложения обеспечивает модуль Video Surveillance Operations Manager (рис. 1), позволяю-

Обратите внимание на видеоаналитику и возможности интеграции

Григорий ИЗОТОВ, руководитель направления инженерных сетей и систем компании «Информсвязь»

В настоящее время рынок предоставляет широкий выбор программного обеспечения для IP-видеосистем. Базовый функционал таких систем (запись/воспроизведение архива, вывод «живого» видео, отработка примитивных тревог) приблизительно одинаков. Различаются же они в основном архитектурой, разнообразием дополнительного функционала (алгоритмами видеоаналитики, возможностями интеграции в комплексные системы безопасности) и поддержкой «железа» различных производителей.

Один из трендов на рынке ПО IP-видеосистем – появление аналитических алгоритмов: распознавание лиц и номеров машин, подсчет проходов, отслеживание забытых и оставленных предметов, сопровождение движущихся объектов, детектирование пересечения зон, возгораний и задымлений и других сложных событий, а также алгоритмов шумоподавления и постобработки некачественного или искаженного сигнала. Внедрение этих алгоритмов значительно повышает эффективность работы служб безопасности и эксплуатации и уменьшает влияние человеческого фактора.

Особое внимание необходимо уделить возможностям интеграции видеосистемы с другими охранными и инженерными решениями. В последнее время обособленные средства видеонаблюдения все больше уступают место единым системам безопасности, интегрированным как на уровне межсистемного взаимодействия (начиная с сопряжения на уровне «сухих» контактов и заканчивая протоколами взаимодействия OPC, LON, BACNet, EIB), так и на уровне пользовательского интерфейса (использования 2D-планов и 3D-моделей охраняемых объектов).

Комплексная интеграция средств безопасности и применение мощных аналитических алгоритмов позволяют раскрыть и полностью задействовать весь потенциал видеосистемы. Ресурсы видеоаналитики в сочетании с датчиками и контроллерами управления других систем позволяют не только минимизировать ложные срабатывания, но и предупредить развитие чрезвычайных ситуаций на самых ранних стадиях, мгновенно предоставить операторам наиболее объективную и всестороннюю оценку ситуации.

Выбирать ПО для системы IP-видеонаблюдения следует тщательно, так как в современных условиях эта система из рядового компонента превратилась в один из центральных элементов безопасности, став самым наглядным и информативным инструментом.

щий эффективно управлять всеми активами, будь то камеры, хранилища или мониторы, а также добавлять новые камеры и настраивать их параметры с одной страницы. Надо отметить, что через интерфейсы CVSM возможна настройка параметров как неподвижных камер, так и поворотных, для которых доступно управление PTZ-функциями с помощью клавиатуры, мыши и джойстика, программирование пресетов и туров автопатрулирования. Наряду с этим поддерживается создание интерактивных карт с добавлением фото, графиков, отображением размещения камер на объекте и др.; просмотр видео в режиме реального времени или в записи с ПК и мобильных устройств, включая iPhone; выбор отказоустойчивых опций записи/хранения данных для их восстановления при любых сбоях.

Отличительной особенностью программного продукта Cisco является возможность просмотра всех каналов видео на неограниченном числе мониторов и/или на видеостенах в мультиэкранном режиме, для чего применяется модуль Virtual Matrix, играющий роль виртуального матричного коммутатора. Помимо вывода на экраны текущего и архивного видео VM осуществляет автоматическое воспроизведение тревожного видео по сигналу от охранных датчиков, от системы пожарной сигнализации или СКУД.

В зависимости от масштаба и конфигурации видеосистемы в качестве ее ядра можно использовать аппаратное устройство Cisco Video Surveillance Encoding Server с предустановленным ПО. Оно предназначено для кодирования, распространения, управления и архивации видеоинформации, имеет емкий внутренний архив, возможность подключения внешних хранилищ – DAS, NAS, SAN, тревожные интерфейсы и позволяет работать с аналоговыми и IP-камерами.

Дальнейшее расширение возможностей ПО Cisco обеспечивается как за счет интеграции с приложениями других систем, например, производства компании Lenel Systems, так и путем поступательного наращивания функциональных и технических характеристик CVSM.

Современное ПО управления IP-видеосистемами открыто для интеграции с системами контроля доступа, охранно-пожарной сигнализации и другими приложениями системы безопасности объекта

Широкие возможности настройки

Жизнеспособность крупномасштабной или распределенной IP-видеосистемы во многом зависит от функциональности управляющего ПО, поэтому при создании подобных систем решающее значение имеет выбор специализированного профессионального инструментария, такого как русифицированное программное обеспечение XProtect Enterprise компании Milestone Systems (рис. 2).

В нем реализована поддержка более 1145 моделей IP-камер (в частности, мегапиксельные модели, камеры с 360° паноморфными объективами ImmerVision и др.), а также других IP-устройств 94 производителей. XProtect Enterprise имеет мультисерверную и мультиклиентскую архитектуру, GUI-меню с интуитивно понятным управлением, поддерживает неограниченное число каналов, кодеки M-JPEG, MPEG-4 и H.264, удаленную работу с текущим/архивным видео, локальное хранение данных и долгосрочное архивирование во внешних сетевых хранилищах, интеллектуальный поиск и воспроизведение архивных видеофайлов, двунаправленную передачу звука и обеспечивает скорость записи до 30 кадров в секунду на канал.

В отличие от ряда аналогов, ПО предоставляет пользователям такие возможности, как массовые

Рис. 1. Интерфейс VS Operations Manager: настройка камер, графические планы объекта, быстрый доступ к видео

настройки для всех подключенных камер и для всех пользователей; сохранение любых системных/пользовательских настроек в виде отдельного файла с последующим его экспортом/импортом в программы с такой же либо сходной конфигурацией; наличие автоматических «точек восстановления» (резервного копирования при изменениях в конфигурации) с возможностью возврата к прежним настройкам и др.

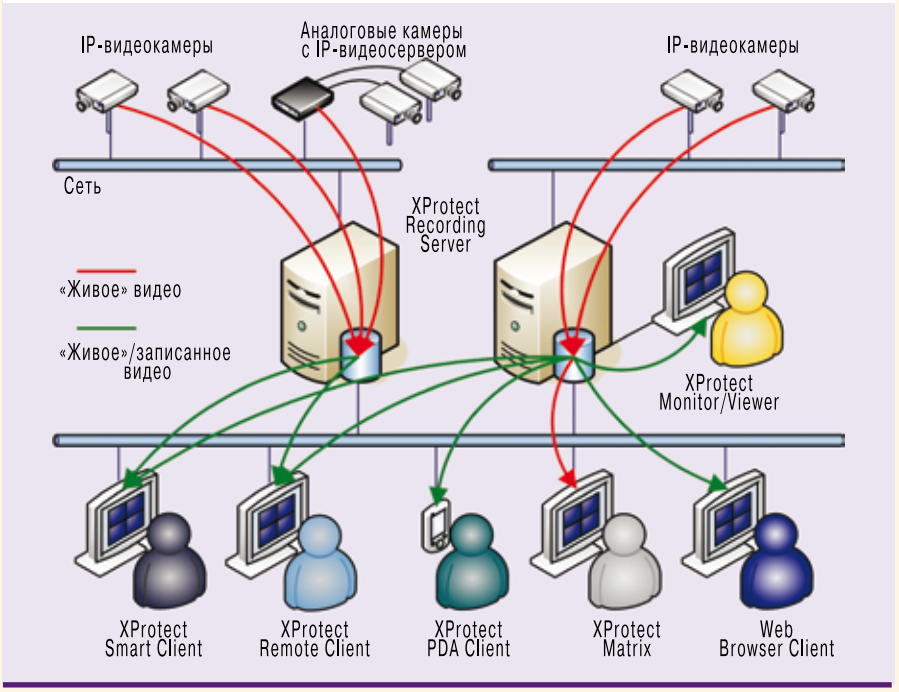
XProtect Enterprise предусматривает возможность удаленного просмотра видео через веб-браузер и допускает различные типы клиентских приложений. Базовое – Remote Client – устанавливается на сервер видеосистемы и обеспечивает удаленный просмотр текущего и/или архивного видео от нескольких камер одновременно, ведение поиска по архиву, управление PTZ-камерами через интерфейс ПО и т.п.

Приложение Smart Client инсталлируется на клиентском компьютере и открывает доступ ко всем серверам и устройствам системы, предоставляя возможность просмотра видео (с выбором до 100 IP-камер одновременно), применения алгоритмов поиска, перехода по пресетам из меню PTZ-камеры, выполнения анализа изображения и др.

Приложение для мобильных устройств PDA Client, устанавливаемое на ноутбук или КПК, позволяет организовать беспроводное интернет-соединение (WLAN, GPRS и др.) и полнофункциональное удаленное видеонаблюдение. Для вывода видеопотоков на мониторы операторов предназначено приложение Matrix Monitor. Все эти приложения не лицензируются и могут быть инсталлированы на неограниченном числе ПК.

ПО Milestone не только предоставляет оператору IP-видеосистемы полный набор функций для просмотра видео в полноэкранном и/или мультиэкранном режимах, различные алгоритмы записи, поиска и обработки данных, активации программного детектора движения и др. Оно обеспечивает возможность построения распределенных системных решений, открытых для интеграции с системами видеоаналитики, контроля и управления доступом, охранно-пожарной сигнализации, экстренного оповещения и эвакуации, инженерными и другими системами.

Рис. 2. Архитектура ПО Milestone XProtect



Экономичное решение

Для мониторинга видео- и аудиоинформации, поступающей от сетевых и/или аналоговых камер, на рынке присутствует и недорогое профессиональное ПО, например программное обеспечение Net-Station торговой марки Smartec. Оно предназначено для построения гибридных/IP-систем видеонаблюдения как небольшого, на четыре камеры, так и среднего и крупного масштаба с сотнями камер, серверов и различными клиентскими приложениями.

Несмотря на демократичную стоимость одного канала, функциональность этого ПО не выглядит урезанной. В перечне поддерживаемого оборудования IP-устройства ведущих марок: Arecont Vision, AXIS, Bosch, IQinVision, JVC, Pelco by Schneider Electric, Sony и др., а также вся линейка устройств Smartec, включая IP-камеры и IP-видеосерверы семейства NEYRO с алгоритмами видеоаналитики английской компании VCA. Net-Station имеет русифицированные интерфейсы, совместимо с VGA, HDTV и мегапиксельными камерами, предусматривает удаленный просмотр видео и воспроизведение аудиосигналов в реальном времени либо в записи, поддерживает интерактивные графические планы eMap, разнообразные алгоритмы поиска в архиве с применением графического навигатора, дистанционное управление входами и выходами тревоги, деинтерлейсинг и др.

На базе NetStation и одного сервера можно создавать гибридные видеосистемы из 32 камер (скажем, восемь аналоговых и 24 сете-

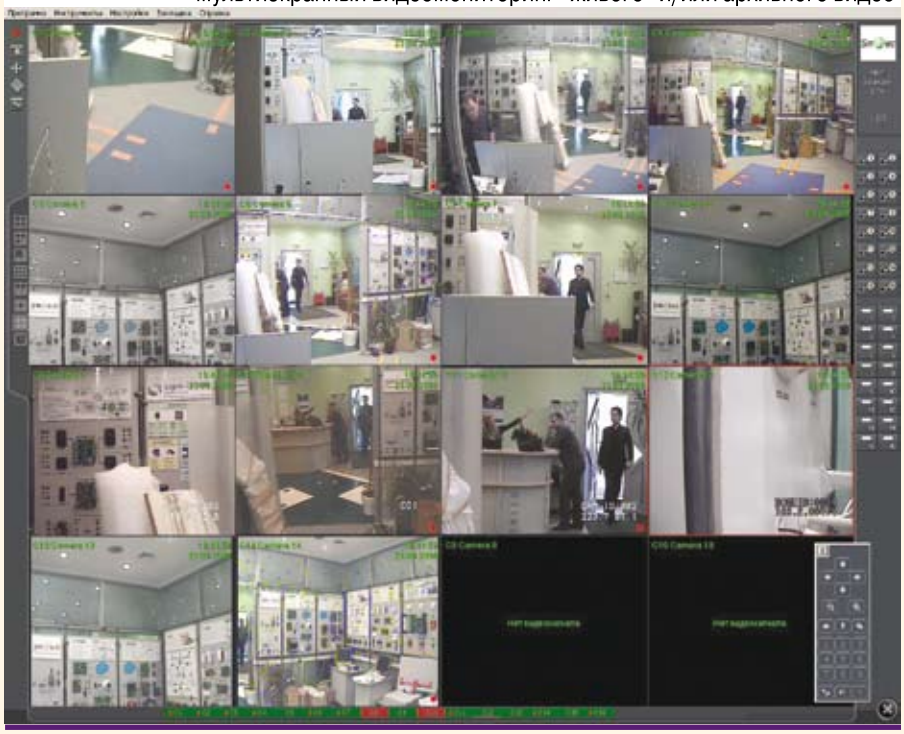
Жизнеспособность крупномасштабной IP-видеосистемы во многом зависит от функциональности управляющего ПО, поэтому при их создании решающее значение имеет выбор специализированного профессионального инструментария

вые либо 16 аналоговых и 16 сетевых), что принципиально важно при необходимости расширения системы с сохранением уже установленных на объекте камер. ПО поддерживает алгоритм дифференциальной компрессии видеосигнала Delta JPEG, а также MPEG-4 и Motion JPEG. Многоуровневый конфигуратор отражает все доступные функции конкретной камеры для настройки изображения, фреймрейта и т.п., а для мегапиксельных моделей применимы функции цифрового масштабирования и динамического разрешения.

Одна из ключевых возможностей NetStation – удаленное видеонаблюдение и синхронизированное аудиопрослушивание в режиме реального времени. Одновременно с записью видео- и аудиопотоков от камер это ПО обеспечивает возможность вывода на монитор изображения по всем каналам (рис. 3), причем предусмотрено подключение до восьми мониторов на одно АРМ оператора IP-видеосистемы.

Для работы неограниченного числа удаленных пользователей с текущим, записанным видео и функциями видеокомплекса могут использоваться клиентские приложения CMS Professional и CMS Mobile. Для КПК типа PocketPC и мобильных телефонов бесплатно предлагается Mobile Client, позволяющий осуществлять удаленный доступ к видео посредством беспроводного подключения по сетям 802.11b/g и 802.3. Mobile Client можно установить на мобильные устройства, работающие под ОС Windows Mobile 5/6, Android или Symbian, а также на iPhone, iPad и Blackberry. Приемлемое качество работы с видеоархивом обеспечивается при любом типе подключения – от модемного до GPRS- и 3G-соединений.

Рис. 3. Русифицированный интерфейс ПО NetStation – мультиэкранный видеомониторинг «живого» и/или архивного видео



Немаловажно, что NetStation поддерживает управление поворотом, наклоном и масштабированием PTZ-камер, в том числе задание для них предустановок и туров автопатрулирования с помощью клавиатуры, джойстика, мыши или через интерфейс ПО.

> Для мультибрендового ПО поддержка IP-устройств многих известных марок позволит не только создать эффективную систему видеонаблюдения сегодня, но и быстро расширить ее в будущем

Минуту внимания

Программные продукты, как представленные в настоящем обзоре, так и оставшиеся за его рамками, имеют свои конкурентные преимущества, которые при определенных условиях могут оказаться решающими. Выделить главное и второстепенное без привязки к конкретному объекту или проекту довольно трудно, поэтому имеет смысл обозначить лишь некоторые моменты, существенные при выборе ПО для многоканальной IP-видеосистемы.

Прежде всего обращайте внимание на количество каналов на один сервер, которое поддерживает то или иное программное обеспечение, – с этим напрямую связаны вопросы конфигурирования системы. Для мультибрендового ПО особенно важно наличие в списке поддерживаемого оборудования IP-устройств многих известных марок – это позволит не только создать современную и эффективную систему видеонаблюдения сегодня, но и станет гарантией ее простого и быстрого расширения в будущем.

Опять-таки, в ответ на текущие требования и в расчете на перспективу желательно, чтобы в ПО была реализована поддержка сетевых камер с мегапиксельным разрешением, имелись возможность создания подробных графических карт объекта с расположением каждой IP-камеры и прямым доступом к ее видео одним кликом мыши, мобильные клиентские приложения, например для сотрудников службы охраны, патрулирующих территорию. Желательно также, чтобы ПО было открытым для интеграции с другими приложениями в составе системы безопасности объекта. ИКС

Профессиональное оборудование для охранных IP-систем видеонаблюдения

Smartec

Весь товар сертифицирован

STC-IPM3096A

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

STC-IPM3095A

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

STC-IPM3595A

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

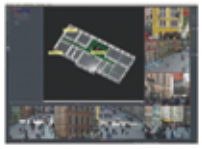
- Всегда на московском складе
- Программа развития дилеров
- Инструкции на русском языке
- Техническая поддержка
- Гарантийные/сервисные услуги

STC-IPX3062A (с видеоаналитикой VCA)

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

STC-IPX3562A (с видеоаналитикой VCA)

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



NetStation

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

армо-системы
www.armosystems.ru

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

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

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

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

Маршрутизаторы «все в одном»

Линейка мультисервисных корпоративных маршрутизаторов доступа AR G3 состоит из моделей трех серий AR1200, AR2200 и AR3200, предназначенных для мультисервисных сетей масштаба предприятия с числом пользователей от 10 до 500.

Все маршрутизаторы построены в соответствии с концепцией «все в одном» на базе универсальной платформы маршрутизации VRP третьего поколения, которую характеризуют высокая производительность, поддержка проводных и беспроводных сетей, применение технологии неблокируемой коммутации, обеспечение безопасности, использование многоядерных процессоров и резервирование основных элементов.

Многоядерный процессор позволяет одновременно обрабатывать несколько потоков трафика, в том числе голос, видео и данные при сохранении высокой производительности. Скорость коммутации трафика в маршрутизаторах AR G3 составляет в зависимости от модели от 8 до 80 Гбит/с.

При работе в беспроводных сетях поддерживаются стандарты Wi-Fi 802/11b/g/n и 3G (CDMA2000/WCDMA/TD-SCDMA) с возможностью создания VPN-сетей. Кроме того, маршрутизаторы смогут работать в сетях LTE и переключаться с сетей 3G на сети LTE.

В проводном режиме реализована поддержка интерфейсов xDSL, E1/T1, ISDN для сетей на базе медного кабеля и интерфейсов Gigabit Ethernet и GPON с пропускной способностью до 10 Гбит/с для оптоволокна. Все коммутаторы линейки AR G3 имеют встроенные средства защиты корпоративных сетей (брандмауэр, поддержка VPN и разных технологий аутентификации, модули шифрования).

Huawei Technologies: (495) 234-0686

Комплект разработчика телематических сервисов

M2M Smart Services Developer Kit – полнофункциональный инструментарий разработки телематических сервисов с использованием облачных вычислений для передачи и накопления данных на телематических серверах и шлюзах.

Продукт состоит из совместимого со стандартом COM Express встраиваемого «компьютера-на-модуле» Kontron nanoETXexpress на процессоре Intel Atom E640 (1 ГГц), объединительной платы M2M и аудиовидеоплаты для конфигураций с мониторами, помещенных в корпус габаритами 67 × 100 × 27 мм.

На внутренней флеш-карте формата MicroSD имеется 4 Гбайт памяти для M2M-приложений, связующего ПО и ОС. Встроенный акселерометр, поддержка HDMI и HD-аудио позволяют разработчикам реализовать как запись передвижений в пространстве, так и аудиовидеосервисы. Внешний USB-порт упрощает использование комплектов программных средств разработки, предлагаемых независимыми поставщиками ПО.

В M2M Smart Services Developer Kit реализована передача данных со скоростью 300 Мбит/с по стандарту 802.11b/g/n на частоте 2,4 ГГц и 802.11a на частоте 5 ГГц. Интегрированный приемопередатчик 802.15.4 (WPAN) обеспечивает гибкую поддержку широкого спектра протоколов и сетевых топологий, таких как 6LoPAN, беспроводной HART, ZigBee и других с использованием интерфейса 802.15.4 MAC.

Комплект разработчика также содержит драйверы для работы с сертифицированным модулем Ericsson 5521gw с возможностью его предустановки. Поддержка 3G WWAN либо предустановлена, либо добавляется установкой сертифицированного модуля PCI Express 3G/4G. Для разработки дополнительных телекоммуникационных возможностей могут быть добавлены другие 3G/4G-модули и драйверы.

«РТСофт»: (495) 742-6828

ИБП для серверов

Masterys Green Power 60 и 80 кВА – одиночные, с двойным преобразованием и высоким уровнем эффективности ИБП, предназначенные для питания серверов последнего поколения (представляющих собой емкостную нагрузку).

КПД ИБП Green Power составляет 96%, что подтверждено сертификатом TÜV SÜD. Коэффициент мощности на входе 0,99, на выходе – 0,9 как для емкостных, так и для опережающих нагрузок. Вход/выход – 3/3. Допуск по входному напряжению – ±20% без ухудшения характеристик, –40% при 50% $P_{ном}$. Ток короткого замыкания – до 2,7×$I_{ном}$. Входной THDI – <2,5%.

В ИБП реализован 3-й уровень технологии IGBT. Для сервисных работ предусмотрены фронтальный доступ и встроенный байпас.

Masterys GP 60 и 80 кВА имеют многоязычный цветной графический дисплей и дружественный пользователю интерфейс. ИБП допускают управление через локальную сеть и удаленный мониторинг.

Габариты (Ш×Г×В) – 600×800×1400 мм. Вес – 180 кг (модель 60 кВА), 200 кг (модель 80 кВА).

Socomec UPS: (495) 775-1985

Контейнерный ЦОД с фрикулингом

Контейнерный ЦОД HP POD 240a имеет общую площадь 930 м^2. Он состоит из двух 40-футовых модулей и горячего коридора между ними. Коридор благодаря своей ширине (2,5 м) позволяет комфортно производить обслуживание оборудования. В каждый из модулей можно установить 22 серверных стойки высотой 50U.

В отличие от предыдущих контейнерных решений HP дата-центр POD 240a оборудован системой охлаждения, и для его работы не нужен приток холодной воды извне. POD 240a рассчитан на работу без ангара при внешних температурах до –29°C. Система охлаждения с автоматизированной системой управления может в зависимости от условий окружающей среды работать в трех режимах: полный фрикулинг в диапазоне температур от +14 до +30°C (в этом случае PUE=1,05), частичное кондиционирование с подмешиванием горячего или холодного воздуха (средний PUE=1,15) и полное кондиционирование (PUE=1,3). Система охлаждения рассчитана на отвод в среднем 30 КВт тепла со стойки (в пиковом режиме до 60 КВт).

HP: (495) 797-3500

Настенные коммутационные шкафы

Шкафы Eurolan Midwall имеют сварную раму и две пары 19-дюймовых направляющих: переднюю и заднюю. Обе пары направляющих могут быть установлены по глубине шкафа на любом расстоянии друг от друга. Благодаря этому в шкафах можно размещать оборудование, крепящееся на четыре точки или на две пары 19-дюймовых рейлингов.

Спереди шкафы закрываются дверью с дымчатым безопасным стеклом в раме из двух металлических коробчатых профилей. Дверь шкафа снабжена надежным немецким замком. Боковые стенки шкафов выполнены на резьбовых соединениях и не снимаются.

Задняя панель представляет собой монтажный кронштейн, который крепится на стену, а затем на него навешивается корпус шкафа в сборе. Это позволяет точно позиционировать шкаф по горизонтали с помощью строительного уровня и обеспечить ввод кабелей из стены через заднюю панель. Дополнительные кабельные вводы имеются в крыше и днище. Эти вводы закрываются декоративной крышкой, которая снимается при необходимости.

В шкафы устанавливаются 19-дюймовые горизонтальные распределители электропитания.

Глубина шкафов – 600 мм. Несущая способность – 60 кг. Высота – 7, 9, 12, 16 и 20U.

«Линдекс»: (495) 775-2510, 223-2295

Беспроводная точка доступа для SOHO

DAP-1155 поддерживает беспроводное соединение с устройствами стандарта IEEE 802.11b/g/n (2,4 ГГц) на скорости до 150 Мбит/с. Точка доступа помещена в компактный эргономичный корпус, оснащена двумя LAN-портами 10/100BASE-TX для подключения Ethernet-устройств к беспроводной сети и кнопкой WPS для быстрой настройки безопасного соединения по Wi-Fi. Устройство также способно работать в режиме моста.

DAP-1155 поддерживает шифрование WEP/WPA/WPA2. Для предотвращения несанкционированного доступа в беспроводную сеть можно использовать фильтрацию подключаемых устройств по MAC-адресу.

Расширенный функционал DAP-1155 включает поддержку WMM для приоритетной передачи аудио, видео и голосовых приложений, функции балансировки нагрузки за счет ограничения количества пользователей, подключающихся к точке доступа, и IGMP Snooping.

Рекомендованная розничная цена – $32,3.

D-Link: (495) 744-0099

Платформа для монтажа коммутационного оборудования в ЦОДе

Платформа Mixed Media Platform обеспечивает унификацию конструктивов для оптического и «медного» коммутационного оборудования. В состав платформы входят монтажные шкафы NETpodium и серия коммутационного оборудования UCP (Universal Connectivity Platform).

Шкафы NETpodium ориентированы на монтаж пассивного и активного коммутационного оборудования. Конструкция основана на сборном каркасе и навесных панелях. Материал – алюминий.

Шкафы имеют встроенные кабельканалы, позволяющие удобно размещать большое количество кабелей, и вертикальные кабельные организаторы значительной емкости, благодаря которым можно отказаться от применения традиционных горизонтальных организаторов и сэкономить ценное монтажное пространство. Для установки оборудования вместо стандартных винтов используются специальные фиксаторы, что обеспечивает быстрый монтаж и упрощает перестановку оборудования. Шкафы можно соединять в ряд и «спина к спине».

В основе коммутационной системы UCP – использование унифицированного посадочного места, позволяющего размещать «медное» и оптическое коммутационное оборудование в одном юните монтажного пространства. Также в состав системы входят специализированные кронштейны, обеспечивающие размещение коммутационного оборудования либо над шкафами, либо под фальшполом, либо внутри монтажных шкафов, но за пределами основного монтажного пространства 19-дюймовой рамы.

В качестве посадочного места используется формат Quick-Fit, позволяющий как устанавливать претерминированные модули (кассеты), так и применять традиционные технологии монтажа. Все выпускавшееся ранее оборудование в формате Quick-Fit также поддерживается. Допускается установка большинства линеек оборудования AMP NETCONNECT, таких как претерминированные кассеты MRJ21 и MPO/MPOptimate, модули AMP-TWIST различных категорий и т.д.

Mixed Media Platform ориентирована на применение в ЦОДах, однако возможна ее инсталляция в кроссовых узлах офисной СКС, когда требуется размещение ИТ-оборудования с высокой плотностью портов.

TE Connectivity/AMP NETCONNECT: (495) 790-7902

Блог, еще раз блог!

ИКС

ПЕТР ДИДЕНКО

Сотовые операторы – зло

>>>> Они делают огромное количество денег, но не потому, что хорошо работают. Исторически так сложилось, и они так делали всегда.

Для нас придумали международный роуминг, иногда за $5/минуту при том, что давно есть Skype/etc и мы все знаем, сколько на самом деле стоит поговорить с той стороной земного шарика – нисколько. Есть даже роуминг внутри России – форменный грабеж. Внутри своей же сети, но в другом городе ты почему-то должен платить значительно дороже – с чего бы?..

А иногда они думают, что надо зарабатывать не на трафике, бегающем по их «проводам», а на сервисах, из которых тот трафик и «проистекает». Почему бы операторам не заниматься «клаудом», а? Тогда включается бюрократия, и для начала они года два-три строят гигантский дата-центр. Затем оказывается, что не очень понятно, а что же там хостить, что продавать юзерам-то?

Я понимаю, что вся эта картинка очень упрощенная, но очень хочется, чтобы сотовым товарищам действительно несколько подзакрутили трубу нетрудовых доходов. А то у неподготовленных ИТ-умов создается впечатление, что это нормально, что так можно, что так нужно, что так бывает. Это – не рынок. Так не должно быть.

комментировать

Михаил ЕМЕЛЬЯННИКОВ

Зачем министру знать Трудовой кодекс?

>>>> По сообщению радиостанции «Голос России», «министр транспорта РФ Игорь Левитин поручил Росавиации сделать доступной для всех авиакомпаний базу данных командиров воздушных судов, в которой содержится информация об их обучении, переподготовке, количестве часов налета и так далее... "И если пилот провинился в одной авиакомпании, это будет сигналом руководителям других авиакомпаний очень серьезно подумать, прежде чем его взять", – сказал Левитин».

Наверное, озвученное предложение министру кто-то подготовил. Проработал. А те, кто это делал, законов тоже не читали. А зачем? Это пусть коммерсанты заморачиваются. К ним там Роскомнадзор ходит. А не в госорганы.

Я тоже считаю, что пьяный летчик, допущенный к управлению, – преступление. Но уж если мы хотим, чтобы законы выполняли, надо начинать их выполнять в государственных органах.

Алгоритм действий законы предлагают совсем другой. СНАЧАЛА внесите изменение в закон (а право законодательной инициативы у министерства есть), а уж ПОТОМ поручайте Росавиации раскрыть базу командиров судов другим компаниям. А никак не наоборот.

Господа чиновники, читайте законы. Они не только для налогоплательщиков писаны.

комментировать

ДЖОН ЭРНХАРДТ

Офис где угодно

>>>> Долгие переезды на работу в часы пик, необходимость «как штык» к определенному часу быть в офисе – все это постепенно уходит в прошлое.

К 2013 г. мобильные сотрудники составят 35% трудоспособного населения нашей планеты. Какой регион мира станет лидером мобильности к 2013 г.?

В сугубо количественном отношении больше всего мобильных работников через год с небольшим будет в Азиатско-Тихоокеанском регионе (более 700 млн человек, или 62% от общего числа мобильных сотрудников во всем мире). По степени же распространенности такого метода работы в лидерах будут Соединенные Штаты и Япония, где возможность трудиться в мобильном режиме получат три четверти сотрудников предприятий.

Думать, что надомный работник всегда работает спустя рукава, неверно. Напротив, 45% опрошенных сказали, что в удаленном режиме они зачастую работают на 2–3 часа в день дольше, чем в офисе.

Сокращение текучести кадров и повышение производительности труда – два наиболее очевидных преимущества мобильной работы с точки зрения работодателей. Но есть и другие плюсы, затрагивающие интересы всего населения. Например, если бы 50 млн жителей США получили возможность половину недели работать на дому, ежегодно покрываемое ими расстояние при поездках на работу сократилось бы на 91 млрд (!) миль. Это, в свою очередь, существенно сократило бы количество ДТП, сохраняя жизнь и здоровье 77 тысячам человек в год.

комментировать

Реклама в номере

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

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

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

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