Под грузом общерыночного негатива

Российские площадки в июле – первой половине августа несколько укрепили свои позиции, однако развитию восходящего тренда помешали негативные новости этого лета.

Анна ЗАЙЦЕВА,
аналитик УК «Финам Менеджмент»

Очередное понижение кредитного рейтинга Греции и последовавшие за ним опасения, связанные с реструктуризацией греческого долга, прибавили инвесторам нервозности. Лишь ближе к концу июля лидеры ЕС смогли найти общее решение греческой проблемы, выделив стране дополнительный транш в размере 159 млрд евро. Однако в последних числах июля обострение на рынке вызвали новости из США: страна находилась на грани «технического дефолта», республиканцы и демократы на протяжении недели, вплоть до 2 августа – окончательной даты объявления решения о повышении лимита госдолга – не могли прийти к согласию. Только за день до «часа икс» конгрессмены США достигли компромисса, в рамках которого допустимая планка госдолга может быть постепенно повышена минимум на $2,1 трлн при условии, что на протяжении ближайших 10 лет государство сэкономит более $2,4 трлн.

Однако основной шок ждал инвесторов 5 августа, когда рейтинговое агентство S&P впервые в истории понизило долгосрочный кредитный рейтинг США с наивысшего значения «AAA» до «AA+» с «негативным» прогнозом. Масла в огонь подлили новости из Европы, а именно слухи о снижении кредитного рейтинга Франции и о возможном банкротстве французского банка Societe Generale. Мировые рынки устанавливали новые рекорды падения, и лишь в середине августа, благодаря слаженным действиям президента Франции Николя Саркози, главы Центробанка и министра финансов страны, удалось стабилизировать ситуацию. На фоне этих событий несколько потерялось подтверждение международным рейтинговым агентством Fitch кредитного рейтинга США на уровне «AAA» со стабильным прогнозом.

«Ростелеком» остается ньюсмейкером

Акции «Ростелекома» демонстрировали высокую волатильность: бумаги холдинга в «дни распродаж» нередко выступали как защитный актив, но в то же время под воздействием технических и корпоративных новостей довольно долго могли находиться под давлением. В итоге за рассматриваемый период обыкновенные акции «Ростелекома» потеряли 14,25%, опустившись к уровню 162,1 руб. Следует отметить, что 10 августа завершилось объединение основного и дополнительного выпусков обыкновенных акций «Ростелекома» – теперь на фондовой бирже ММВБ все обыкновенные акции ОАО «Ростелеком» торгуются под тикером RTKM, а привилегированные – под тикером RTKMP. Интерес инвесторов к бумагам оператора подогревало ожидаемое на этом фоне включение обыкновенных акций «Ростелекома» в индекс MSCI Russia. Сразу отметим, что 17 августа MSCI Inc. ввела в состав Russia Standard Index обыкновенные акции «Ростелекома». Вес бумаги в индексе составит 3%, а изменения в индексе вступят в силу осенью – 1 сентября 2011 г.

Низкая ликвидность не позволила бумагам «Таттелекома» противостоять негативному внешнему фону. В итоге за рассматриваемый период акции компании просели на 14%, остановив-

Справка ИКС

На фоне многочисленных, преимущественно негативных новостей, за период с 1 июля по 15 августа индекс ММВБ снизился на 9,35% – до уровня 1510,69 пункта, а индекс РТС потерял 13,19%, опустившись до 1655,03 пункта. Отраслевой индекс «ММВБ телекоммуникации» уменьшился на 8,49% – до значения 2258,82 пункта.

шись на отметке 0,2156 руб. Компания опубликовала отчетность по РСБУ за I полугодие 2011 г., согласно которой чистая прибыль ОАО «Таттелеком» выросла на 17% – до 353,3 млн руб. по сравнению с 301,8 млн руб. в I полугодии 2010 г. Выручка увеличилась на 12,2% и составила 3,192 млрд руб. по сравнению с 2,845 млрд руб. за аналогичный период предыдущего года.

МТС потерял на объединении акций

Бумаги МТС на протяжении рассматриваемого периода в целом вели себя довольно спокойно, однако после сообщения об объединении по итогам торгов 10 августа акции сотового оператора потеряли 5,22%, откатившись к отметке 209 руб. Напомним, что с 11 августа обыкновенные акции МТС торгуются на ММВБ под торговым кодом MTSI – это следствие объединения дополнительного и основного выпусков акций. Дополнительная эмиссия бумаг оператора была проведена ранее для целей конвертации акций ОАО «Комстар-ОТС». Всего же за полтора месяца капитализация МТС сократилась на 5,05% – до 218,6 руб. за акцию.

Среди корпоративных новостей стоит отметить публикацию статистики за II квартал 2011 г. по РСБУ, согласно которой чистая прибыль ОАО «МТС» составила 22,9 млрд руб., что на 74% больше чистой прибыли, полученной компанией за I квартал текущего года (13,2 млрд руб.). При этом во II квартале прошлого года чистая прибыль МТС составила 12,6 млрд руб.

ИТ-компании накрыло коррекционной волной

Бумаги российских ИТ-компаний в условиях общего снижения не смогли показать защитных свойств. Коррекционная волна не обошла стороной бумаги АФК «Система», которые за рассматриваемый период потеряли 12,3%, опустившись до уровня 27,7 руб. за акцию. Компания продолжила реструктуризацию, сообщив о завершении сделки по продаже ОАО «РТИ» 63,074% акций ОАО «Ситроникс» в соответствии с ранее объявленными условиями. Напомним, что в феврале АФК «Система» и ОАО «Банк Москвы» создали ОАО «РТИ». Банк Москвы выступил инвестором новой компании, внеся в уставный капитал ОАО «РТИ» денежные средства в размере 3 млрд руб. «Система» внесла в уставный капитал принадлежащие ей 96,9% акций ОАО «Концерн «РТИ Системы», а также денежные средства в размере 2,88 млрд руб. В итоге доля АФК «Система» составила 84,6% уставного капитала ОАО «РТИ», доля Банка Москвы – 15,4%.

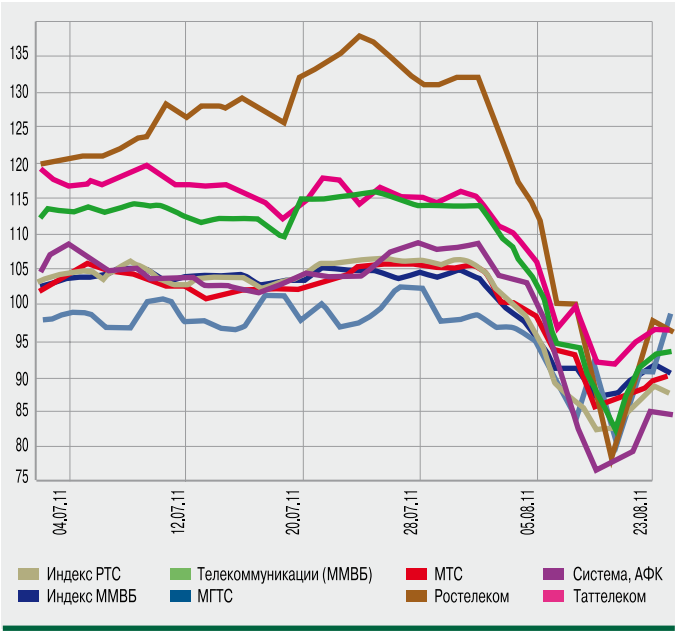
> Давление на бумаги «Яндекса» оказали случившиеся в августе технические проблемы с серверами и с индексацией поисковиком конфиденциальных данных

Рекордное падение – на 33%, до уровня 24,82 руб. – зафиксировали акции ОАО «РБК», а также бумаги IBS Group, которые за рассматриваемый период потеряли 21,38%, снизившись в цене до $17,8. Капитализация «Ситроникса» сократилась на 4,35% – до $0,66.

Капитализация Mail.ru Group снизилась: на LSE бумаги компании потеряли в цене 6,53%, до $31,05 за акцию. В июле акции эмитента активно росли – на 7,44% – на информации об увеличении доли Mail.ru Group в социальной сети «ВКонтакте», в какой-то момент их цена превысила отметку в $37, но разразившийся биржевой кризис нивелировал все завоевания.

Обыкновенные акции класса «А» компании Yandex N.V. («Яндекс»), обращающиеся на NASDAQ, за полтора месяца подешевели на 12% – до отметки $30,59. Основная причина уменьшения капитализации российского поисковика – резкая коррекция американской биржи NASDAQ, индекс которой снизился почти на 8%; падение американских площадок потянуло за собой бумаги высокотехнологичных компаний. Корпоративные новости «Яндекса» также оставляли желать лучшего. Так, 27 июля компания представила финансовые показатели за I полугодие и II квартал 2011 г., первые после IPO в мае этого года: чистая прибыль поисковика по неаудированным данным в соответствии с US GAAP в первом полугодии составила 1,945 млрд руб. (на 27,6% больше, чем за аналогичный период 2010 г.), выручка увеличилась на 61% – до 8,435 млрд руб. Давление на бумаги «Яндекса» оказали и случившиеся в августе технические проблемы с серверами и с индексацией поисковиком конфиденциальных данных, что повлекло за собой риски перетока рекламодателей к конкуренту – американской Google. ИКС

Динамика биржевых индексов и телекоммуникационных компаний в период с 4 июля 2011 г. по 23 августа 2011 г.



И machine с machine говорит...

Рынок услуг межмашинного взаимодействия обладает огромным потенциалом, раскрыв который мобильные операторы получат новый источник дохода.

Сергей БАЛАШОВ, менеджер по продуктам телематических решений и сервисов компании «ВымпелКом»

Сегодня становится важен эффективный обмен информацией не только между людьми, но и между различными устройствами (machine-to-machine, M2M), которые собирают результаты измерений, требуют наблюдения или установки определенных параметров и т.д. M2M-коммуникации – это целый пласт современных услуг. Они задействованы во всех ключевых отраслях мировой экономики – в финансах, энергетике, на транспорте и в логистике, вендинге, здравоохранении, телемониторинге промышленного оборудования, системах безопасности...

Триада M2M...

Любое M2M-решение включает в себя три основных элемента.

1. **Оборудование.** То «железо» (датчики, сенсоры, модули и т.п.), которое устанавливается в автомобиле, банкомате, на трубопроводе или любых других объектах мониторинга и которое осуществляет сбор/получение той или иной информации.

2. **Система мониторинга оборудования.** Система, позволяющая получать/отправлять, обрабатывать и представлять в необходимом формате те или иные данные и команды. Например, видеть текущее местоположение автомобиля с информацией о параметрах его движения, получать данные о давлении в трубопроводе и др.

3. **SIM-карта,** являющаяся «представителем» мобильной сети оператора, благодаря которой и осуществляется передача данных между первыми двумя элементами. Один из самых распространенных и перспективных каналов связи в M2M-коммуникациях – сети GSM/GPRS/EDGE/3G.

...и ее освоение сотовыми операторами

Сети GSM разных поколений охватывают огромные территории, поддерживая связь как между людьми, так и между устройствами, и этот факт обусловливает усиливающийся интерес операторов сотовой связи к направлению M2M. К тому же рынок голосового трафика в России, как и во всем мире, близок к насыщению. Поэтому с целью дальнейшего роста бизнеса сотовые операторы увеличивают свое присутствие на рынке передачи данных, включая сегмент межмашинного взаимодействия.

С конца прошлого века до недавнего времени операторы на рынке M2M выступали только в качестве «трубы», т.е. отвечали исключительно за передачу данных. Первый и второй элементы M2M-систем являлись зоной ответственности системных интеграторов и производителей/поставщиков оборудования. Сегодня ситуация меняется, и операторы связи все больше тяготеют к разработке комплексных M2M-решений.

Благодаря очевидным преимуществам M2M-решений на основе мобильной связи (обеспечение информационного обмена с удаленным оборудованием в труднодоступных местах или при принципиальной невозможности проводного соединения, оперативное подключение новых абонентских устройств к корпоративной сети без затрат на организацию проводных каналов, оптимизация издержек и др.), а также благодаря развитию мобильных сетей рынок начал стремительно расти. Все больше SIM-карт стало устанавливаться не в телефонах, а в других устройствах, и операторы отреагировали на это, запустив специальные тарифные планы для передачи данных в рамках межмашинного взаимодействия.

На сцену выходит четвертый элемент

Однако M2M-решения на основе мобильной связи не только дают серьезные преимущества, но и порождают ряд проблем. Одна из самых распространенных – нецелевое использование SIM-карт. Другие типичные проблемы – отсутствие какой-либо информации о работе SIM-карт и их текущем статусе, ограниченные возможности управления ими, перерасход средств и т.п.

Неудивительно, что рынку потребовался удобный инструмент управления и мониторинга SIM-карт, устанавливаемых в устройствах, который позволил бы компаниям-пользователям избежать вышеперечисленных трудностей. Компания должна иметь возможность своевременно определить, что SIM-карта используется не для мониторинга объектов, а, скажем, для выхода в Интернет с мобильного телефона недобросовестного сотрудника. В более общем виде эта задача превращается в задачу контроля над трафиком и расходами на обеспечение коммуникаций между объектами. В таком ключе система мониторинга SIM-карт должна предоставлять информацию в режиме реального времени, чтобы клиент получал онлайн-уведомления о несанкционированных действиях с SIM-карты или о резком росте трафика, нехарактерном для данного устройства. Еще одно важное требование – возможность интеграции решения с уже имеющимися ERP- и CRM-системами.

Стремясь осуществить пожелания существующих клиентов и привлечь новых, крупнейшие операторы мира начали разрабатывать и выводить на рынок специальные системы и платформы для управления SIM-картами в устройствах. Такие системы стали четвертым элементом M2M-решения. Ряд операторов – Vodafone, Telenor, Orange, T-Mobile,– затратив десятки миллионов долларов и несколько лет работы, создали собственные платформы. Другие, в числе которых AT&T, Telefonica, KPN, Rogers, O2, в рамках партнерских соглашений используют решения ведущих поставщиков M2M-платформ и MVNO-операторов (Jasper Wireless, MainGate, ASPider и др.).

И хотя оба варианта запуска M2M-платформ имеют свои плюсы и минусы, само наличие такого компонента в составе M2M-решения оказало серьезное влияние на рынок и рост количества M2M-пользователей в абонентской базе операторов. Так, если с I по III квартал 2009 г. компания AT&T подключала ежеквартально в среднем 300 тыс. абонентов, то после запуска платформы в том же году ее продажи в сегменте M2M за IV квартал 2009-го и I квартал 2010 г. составили 1,4 и 1,2 млн SIM-карт соответственно. Безусловно, здесь свою роль сыграли и другие факторы, в числе которых была сама стратегия развития M2M-бизнеса оператора, но важно то, что сейчас в Европе и США подобные платформы перешли из разряда «неплохо бы иметь» в разряд «необходимо иметь».

Такие решения постепенно появляются и у нас в стране. Пионером на российском рынке в этой области стал «Билайн Бизнес», предложивший в конце 2010 г. решение «Центр управления M2M». Оно реализовано на базе глобальной платформы Jasper Wireless, которую, как уже упоминалось, используют операторы AT&T, KPN, Rogers, O2, TelCel и др. Платформа позволяет клиентам самостоятельно управлять своими SIM-картами. Планы по запуску подобной платформы есть и у МТС.

Системы с возможностью детализированного мониторинга SIM-карт и их соединений полезны как маленькой фирме, у которой буквально каждая копейка на счету, так и большой корпорации, управляющей сотнями и тысячами SIM-карт в M2M-системах. И если в оптимизации бизнес-процессов в большей степени заинтересован крупный бизнес, то сокращение затрат необходимо и тем и другим.

Что дальше?

«Большая тройка» первые шаги в направлении M2M сделала достаточно давно. В 2008 г. «ВымпелКом» и МТС запустили решения по мониторингу транспорта в рамках партнерских программ. Чуть позже их примеру последовал и «МегаФон». Однако отметим, что данные продукты предоставляли лишь часть тех возможностей, которые может обеспечить функционал M2M. Кроме того, они не являлись законченным M2M-решением от оператора, а представляли собой решения системных интеграторов (например, «Эшелон Геолайф», РНТ, «Кобра», «M2M Телематика» и др.), которые операторы продавали своим клиентам, выступая в качестве агента.

Сегодня в России уже сформировался спрос на все элементы M2M-решения в комплекте. Следующий шаг со стороны операторов – создание комплексных M2M-решений, которые учитывают все потребности клиента в M2M. Таким образом, клиент сможет получить оборудование, услуги мониторинга, включая услуги передачи данных, услуги по установке решения в одной «точке входа» – у оператора.

Правда, возникают некоторые сомнения в возможностях операторов реализовать такие продукты. И причины этих сомнений кроются в следующем. У операторов никогда не было компетенций по разработке и инсталляции законченных M2M-решений. Это всегда было бизнесом системных интеграторов: как уже отмечалось выше, когда «большая тройка» начинала предлагать первые решения по мониторингу транспорта, клиент «передавался» партнерам и заработок операторов сводился к плате за трафик и проценту от выручки. В новой же парадигме получается, что операторы могут стать конкурентами системных интеграторов.

Однако на деле все обстоит иначе. Даже самые крупные системные интеграторы не обладают той силой бренда и той клиентской базой, которая есть у мобильных операторов. К тому же практика показывает, что некоторые корпоративные клиенты «большой тройки» не знают о существовании даже самых крупных поставщиков M2M-решений, и первое место, куда они обращаются, – это опять же поставщик услуг связи. С другой стороны, системные интеграторы сами не против выступить в роли подрядчиков и поставщиков решений для оператора, так как в этом случае для них открывается мощный канал сбыта при незначительном уменьшении маржинальности. Для рынка это также определенная выгода, особенно для крупных компаний, для которых «завести» ново-

В Европе и США M2M-платформы перешли из разряда «неплохо бы иметь» в разряд «необходимо иметь»

го поставщика – это целый бюрократический процесс, который может растянуться на полгода-год. А операторы «большой тройки» зачастую уже входят в число официальных поставщиков, и приобретение у них дополнительных услуг особых сложностей не вызывает. Уровень затрат при покупке M2M-решений у операторов прогнозируется приемлемым, поскольку операторы, не являясь «законодателями мод», ориентируются на рыночные цены.

«ВымпелКом», стремясь расширить свою линейку продуктов M2M комплексными решениями, недавно объявил о сотрудничестве с ГК «Эшелон» в рамках собственного продукта «Комплексные M2M-решения», запуск которого состоялся в апреле 2011 г. Теперь «Билайн Бизнес» продает «коробочные решения» со стандартным набором услуг для каждого сегмента M2M. Пример таких решений – продукт «Автомониторинг» с большим набором функций. При этом, если специфика бизнеса корпоративного клиента требует расширенного функционала и возможностей мониторинга удаленных объектов, дополнительной информации и данных в определенном формате, установки специального оборудования, кастомизации услуги и др., «Билайн Бизнес» готов разработать комплексные M2M-решения индивидуально для каждого клиента. Скажем, помимо определения местонахождения и других параметров движения клиенту может понадобиться тревожная кнопка, датчик топлива, вывод дополнительной информации, детализация объектов на карте и т.д.

Каким путем пойдут другие операторы связи и какой вариант окажется самым успешным – покажет время. Сейчас можно сказать только одно – российский рынок M2M растет стремительно и, несмотря на то что его объемы пока несопоставимы с рынками США и Европы (так, у AT&T уже подключено более 10 млн SIM-карт), по прогнозам аналитиков и самих операторов, в течение ближайших лет количество M2M-абонентов в России достигнет нескольких миллионов. ИКС

Три чашки капучино, *или* Как увеличить продажи интернет-провайдера

– Ничего нового, мы все это уже давно знаем!
– А почему не делаете?
Из интервью с клиентом

Не существует одного волшебного способа, удваивающего продажи, но есть 100 способов, которые увеличивают их на один-два-три процента. В этой статье вы найдете набор простых приемов, позволяющих интернет-провайдеру быстро получить отдачу.

Сергей **БОРИСКИН,**
независимый эксперт

Формула продаж

Чтобы отчетливо понимать основные параметры, которыми нужно оперировать для увеличения продаж и, соответственно, прибыли, рассмотрим общую формулу продаж.

Объем продаж есть произведение количества потенциальных клиентов (в мировой практике принято слово leads – «лиды») на коэффициент конверсии Cv, на среднюю сумму чека каждого клиента $, на количество покупок #, сделанное этим клиентом, и на маржу:

объем продаж = leads × Cv × $ × # × маржа.

Эти сомножители и есть пять основных параметров, над которыми нужно работать, чтобы увеличить продажи в любом бизнесе. Но работа над ними сильно разнится по затратам.

Проще всего работать с маржой (ценой). Чтобы изменить цену, не требуется никаких усилий, кроме волевого решения, и не нужно никаких дополнительных затрат.

Далее идут средняя сумма чека – среднее количество денег, которые оставляет у вас один абонент, и коэффициент конверсии, т.е. доля потенциальных клиентов, ставших реальными.

Самое затратное – увеличение числа потенциальных клиентов, поскольку любая реклама подразумевает те или иные вложения.

Эффективная товарная матрица

Элементы товарной матрицы – это то, что мы предлагаем абонентам. У интернет-провайдеров первым элементом матрицы являются тарифы.

Общий совет всем провайдерам: **сокращайте число тарифов**. Абонентам сложно разобраться в большом объеме информации. А непонимание тарифной сетки самими менеджерами продаж может стать губительным.

Как правило, у лидеров рынка – и российского («Акадо», QWERTY и др.), и зарубежного – имеется три-четыре тарифа. Это норма, пришедшая из других видов бизнеса. Возьмем, к примеру, кофейню. Она предлагает капучино в разных чашках: в маленькой, стандартной и большой. Нет выбора из десяти чашек разного размера. Если в наличии один вариант (только маленькая чашка) – это плохо (снижает продажи). Две – уже лучше, три – оптимальное число. При этом в основном покупается средняя порция. Традиционно официант предлагает сначала большую чашку капучино. И нередко клиент ее покупает. Почему? Потому что мы ему п р е д л о ж и л и.

Для увеличения среднего чека из меню убирается чашка, первоначально считавшаяся маленькой. Маленькой становится та, что была средней, и добавляется еще одна, теперь уже – очень большая.

Инструменты увеличения продаж

Для быстрого увеличения продаж хорошо работают приемы **up-sell** (дополнительная продажа) и **cross-sell** (продажа чего-то «соседнего»).

В соответствии с методом up-sell мы можем предлагать абонентам более дорогой тариф, двойную скорость ночью, аренду оборудования (беспроводные роутеры, СТВ и т.д.), пакет ТВ и телефонии.

В качестве cross-sell может выступать продажа антивирусов (в пакете, в отдельной коробке или в подписке на сайте), программного обеспечения (офисных пакетов и пр.), возможностей обучения (книг, курсов, обучающих дисков, миниклассов из двух-трех компьютеров для вечерних семинаров, вебинаров).

Когда абонент дал согласие купить, он с большой вероятностью купит что-то еще. Потому что он уже согласился купить. Ваша задача только предложить.

Более сложный, но также хорошо работающий прием, – использование **продукта front-end**. Это очень дешевый или вообще бесплатный продукт, который вы можете предложить абонентам. Задача – привлечь абонента в компанию, отработав на этом продукте в ноль или даже в минус. Не обязательно таким продуктом должен быть какой-то дешевый или бесплатный тариф. Отличным frontend-продуктом может послужить каталог ресурсов, где указано, как клиент может использовать Интернет. Большое заблуждение считать, что все ваши клиенты умные и сами все поймут. Надо ориентироваться на то, что абонент – Гомер Симпсон. Абоненту нужно «разжевывать», что именно он может делать в Интернете.

Еще один прием, который позволяет повысить лояльность потенциальных клиентов, – **гарантия**. К сожалению, немногие интернет-провайдеры используют гарантию возврата денег как элемент эффективной товарной матрицы. Когда абонент приходит и говорит, что он недоволен, вы обязаны вернуть ему деньги без лишних разговоров. Но для того чтобы противостоять недобросовестным абонентам, на сайте эта «фишка» должна быть представлена так: «Мы вернем деньги, но впоследствии работать с вами не сможем». В таком случае в черный список вносятся либо паспортные данные абонента, либо его адрес (если он там прописан).

Наличие временно́го ограничения существенно усиливает отдачу от рекламы

Эффективное рекламное предложение

Создавая рекламные материалы – макеты, баннеры на сайт, не забывайте о **принципе ОДП**: оффер – дедлайн – призыв к действию.

Оффер – специальное предложение, изложенное четко и ясно для абонента: акция, «цеплялка» на листовках, баннерах, модулях в Интернете и т.д.

Дедлайн – временно́е ограничение. Наличие такого ограничения существенно усиливает отдачу от рекламы. Скажем, рекламное предложение «подключись бесплатно до 15 мартобря» будет работать лучше, чем объявление «у нас бесплатное подключение». Не видя ограничения по времени, клиент не будет действовать быстро.

Призыв к действию – указание, что именно абонент должен сделать. К примеру, «звони, приходи, подключайся». Призыв должен быть выражен в глаголах, означающих реальное физическое действие: позвонить, прийти.

Принцип ОДП увеличивает отдачу от рекламного обращения на 30–40%.

Абонентский отдел и отдел продаж

Мы привыкли, что менеджеры отдела продаж – это профессионалы, которые немыслимыми движениями добывают нам абонентов, самостоятельно их находят и продают им все, что нужно.

Но таких героев найти сложно. И даже когда это удается сделать, супермены быстро уходят от нас к конкурентам, польстившись на более высокую зарплату.

Для того чтобы отдел продаж работал сплоченно и долго, разделите его на подотделы в соответствии с параметрами в формуле продаж.

Вынесите в отдельный блок создание потока потенциальных абонентов (обычно это одна из функций отдела маркетинга). Тем самым вы снимете с профессиональных продавцов (людей, которые умеют закрывать сделки) самую нудную и одновременно самую стрессовую часть работы – «холодные» звонки, визиты, обходы. Для нее берется отдельный человек (к примеру, студент). Ему прописывается скрипт (свод готовых фраз), и дальше его просто нужно контролировать.

Выявленные «теплые» абоненты передаются подотделу по работе с потенциальными клиентами, который занимается непосредственными продажами: up-sell и cross-sell, закрытие сделки. Итогом его деятельности будет заявка на подключение.

Третья часть отдела продаж – подотдел по работе с существующими абонентами. Это те сотрудники, которые занимаются увеличением суммы среднего чека, информированием абонентов о новых тарифах, дополнительных услугах и акциях.

■ ■ ■

Если вы внедрите хотя бы десяток из сотни различных простых методов увеличения продаж, то получите 20–30% прироста.

Главное, помните первое правило электромонтера: в один момент времени крутим одну ручку – иначе трудно выяснить, что именно сработало. ИКС

ИТ-специалисты учатся – качество бизнес-процессов растет

Окончание. Начало см. «ИКС» №7-8, с. 66.

Чтобы повышение квалификации сотрудников принесло пользу и им самим, и компании, важно заранее спланировать весь процесс корпоративного обучения, найти способ оценить его результаты. Но по итогам такого обучения работодателю нужно готовиться не только к повышению эффективности бизнеса, но и к росту ожиданий сотрудников.

Михаил КУМСКОВ,
эксперт Учебного центра Luxoft, д-р физ.-мат. наук, профессор МГУ

Обучение и мотивация

Само по себе обучение в компании – довольно привлекательная перспектива для сотрудника. Но эффективным мотиватором обучение становится только там, где вся система работы с персоналом сбалансирована. Если организация предлагает сотрудникам конкурентную зарплату, всевозможные бонусы, широкий соцпакет, перспективы движения по карьерной лестнице и т.д., то и обучение воспринимается в контексте корпоративных привилегий. Однако при отсутствии должных мер для поддержания лояльности сотрудников компания после обучения рискует потерять своих специалистов.

С другой стороны, компаниям с хорошо поставленным корпоративным обучением легче привлечь квалифицированных сотрудников. Они в большей степени мотивируются возможностями самореализации, саморазвития, работой в интересной команде. В результате работодатель получает очень сильную команду профессионалов.

При этом обучение не должно превратиться из привилегии в тягостную «обязаловку», поэтому подходить к организации обучения нужно системно. Тренинги следует планировать не только с прицелом на повышение качества бизнес-процессов, но и с целью заинтересовать специалистов, продемонстрировать им актуальность выбранной темы. Нельзя допускать, чтобы сотрудник потерял интерес к обучению или пресытился им. Поэтому при организации обучения особенное внимание следует уделять тому, кого компания приглашает в качестве тренера. Именно от него в конечном счете зависит эффективность всего процесса обучения.

Планирование обучения

Какие же шаги нужно предпринять, чтобы повысить квалификацию персонала? Прежде всего следует оценить масштаб проблемы, диктующей необходимость в обучении. Важно понять, с какими задачами сотрудники справляются лучше, а с какими хуже, на каких участках бизнес-процессов возникает больше всего трудностей, каких знаний и навыков не хватает специалистам. Определившись с направлением обучения, необходимо поставить перед сотрудниками конкретную цель, на достижение которой будут направлены тренинги. Это поможет в ходе обучения непрерывно фокусироваться на актуальных задачах. И наконец, при выборе учебной программы ориентироваться следует в большей степени не на название учебного центра, а на имена самих тренеров, их сферу компетенции, опыт и квалификацию.

Впрочем, обучение, как и любая инициатива, есть палка о двух концах. Поэтому работодателю, организующему для персонала тренинги, нельзя забывать и об оборотной стороне медали. Готовиться нужно не только к повышению эффективности бизнеса, но и к росту ожиданий сотрудников. В первую очередь это касается зарплаты: повышение квалификации неизменно провоцирует недовольство сотрудника своей нынешней позицией. Он начинает претендовать на повышение оклада, продвижение в должности и расширение полномочий, угрожая сменой места работы. Особенно актуальными эти амбиции становятся после получения вендорских сертификатов. Поэтому в некоторых компаниях, где специалистам оплачивают тренин-

ги и сертификацию, им предлагается подписать особое соглашение о компенсации стоимости обучения в том случае, если сотрудник сменит место работы. Такой шаг со стороны работодателя вполне понятен: высокоэффективных специалистов, прошедших обучение и поднявших уровень своей квалификации, нужно удерживать. Как уже было сказано, большую роль в этом играет сбалансированная система мотивации в компании. В противном случае единственным – и, увы, не самым надежным – способом защиты от утечки специалистов остается лишь зарплата и прочие схемы материального поощрения.

Оценка эффективности обучения

В каких случаях компании прибегают к корпоративному обучению? Когда нужно освоить новую предметную область, наладить работу нового отдела, повысить квалификацию сотрудников или же когда необходим выход на качественно новый уровень работы команды, переход на новую технологию, в том числе технологию управления и т.д. Одним словом, главный мотив организации корпоративных тренингов – это повышение эффективности бизнеса, поэтому обучение следует рассматривать как часть процессов улучшения деятельности организации. За счет повышения качества бизнес-процессов, лежащих в основе производства конечных товаров и услуг, достигается и повышение качества самих этих товаров и услуг. Поэтому главным показателем эффективности корпоративного обучения можно считать именно качество конечного продукта предприятия и качество его деятельности в целом.

По сути, корпоративное обучение есть передача специалистам лучшей практики (англ. best practice), или так называемого передового опыта. Тренер не просто рассказывает сотрудникам о новых технологиях разработки ПО, визуального моделирования или управления ИТ-проектами, но и на примере конкретной организации демонстрирует, как эти технологии воплощаются в конкретных проектах. Параллельно он акцентирует внимание слушателей на оптимальных способах достижения проектных целей и решения задач бизнеса. Чтобы проект был успешным, нужно, чтобы он правильно выполнялся и правильно управлялся. Раскрыть секреты «правильности» для конкретной организации – это и есть основная задача экспертов, проводящих корпоративные тренинги.

Управление проектами – это сфера, в которой ИТ-специалистам особенно остро нужна дополнительная подготовка. Дело в том, что сотрудники ИТ-отделов, как и многие специалисты из других областей, в массе своей привыкли к традиционному «задачному» управлению. Начальник, как правило, ставит перед сотрудником задачу и сроки ее выполнения, сотрудник соответственно отчитывается перед руководством. Современный же бизнес все чаще требует перехода к новой философии управления, которую теперь принято называть «процессным менеджментом» или «управлением, ориентированным на качество».

Ключевое различие между «задачным» и «процессным» управлением состоит в критериях успеха работы. «Задачное» управление исходит из того, что успех проекта связан с качественным и своевременным выполнением задач, порученных каждому из сотрудников. «Процессное» управление предполагает, что оценивается результат работы команды в целом. В этом случае сотрудники мотивированы помогать друг другу и делиться знаниями «на рабочих местах», ведь отставание одного приведет к отставанию всех. Другими словами, при процессном управлении проектная команда становится самоорганизованной. В этом случае сотрудники вовремя, правильно и качественно выполняют задачи, которые им формально никто не поручал. Такая схема требует качественной перестройки управленческого мышления. Но результат работы такой команды, как правило, оказывается намного лучше, чем у команд, управляемых в соответствии с традиционными «задачными» представлениями о менеджменте.

Наряду с лучшими практиками корпоративное обучение призвано внедрять в ИТ-команды идеи процессного управления. Успешность проектов в дальнейшем будет зависеть от того, как прошедшие обучение специалисты применят полученные на тренингах знания и лучшие практики. Важно здесь и то, сумеют ли менеджеры перестроить управление проектами с задачной на процессную модель.

Другими словами, корпоративное обучение обеспечивает компаниям оптимальное соотношение объема полученных знаний, бюджета и времени. При этом оно будет по-настоящему эффективно, если его результатом станет успешная работа самоорганизованной команды.

■ ■ ■

Подводя итоги, еще раз отметим, что в системе российского технического образования выпускник высшего учебного заведения готов к тому, чтобы стать хорошим ученым или исследователем. Но для командной работы в проекте ему может не хватить практических навыков и умений. Компаниям же требуются эффективные ИТ-специалисты, готовые решать конкретные бизнес-задачи, постоянно повышающие уровень своих знаний и умений, идущие в ногу с активно развивающейся ИТ-индустрией. Сама специфика отрасли предполагает постоянное обучение и повышение уровня профессиональной подготовки сотрудников. А значит, послевузовское обучение специалистов – одна из важных задач компании.

Наиболее удобным и эффективным сегодня является корпоративное обучение. Оно позволяет не только экономить время и деньги; важные его достоинства – практичность, наглядность, гибкость, а также «живой» экспертный опыт. В конечном счете обучение должно быть полезным не только для специалиста, но и для самой организации, которая таким образом инвестирует в развитие своей структуры в целом. ИКС

«Карточка горожанина» платит и идентифицирует

Объединение на одной пластиковой карте платежных и идентификационных функций повысит эффективность использования бюджетных средств, выделяемых на социальные программы, и облегчит гражданам взаимодействие с муниципальными организациями.

Игорь БУДЬКО,
главный специалист группы поддержки продаж ДРПО компании «Петер-Сервис»

Сегодня и горожане, и муниципальные власти сталкиваются с множеством проблем и неудобств, обусловленных несовершенством организационно-технического сопровождения социальных программ и процедур массового учета и регистрации документов. Муниципалитетам приходится нести большие расходы на поддержание огромной («бюрократической») инфраструктуры, обеспечивающей бумажный документооборот, при невозможности эффективного адресного оказания социальной помощи и неизбежных потерях неизрасходованных адресатами средств. К примеру, на проезд в общественном транспорте гражданину устанавливается льгота в размере 60 поездок в месяц, а фактически совершается только 10 поездок. Оставшиеся 50 поездок – это потери, вызванные отсутствием адресного учета социальной помощи. А население вынуждено терять много времени (зачастую рабочего) в очередях и в дороге при перевозке различных документов из одной инстанции в другую, скажем, при прописке по месту жительства или регистрации автотранспорта.

Ввиду большого количества и разнообразия документов, удостоверяющих льготы, и их слабой защищенности от подделок, у организаций, которые занимаются оказанием услуг льготным категориям населения, существует проблема однозначной идентификации льготника и проверки подлинности его прав на пользование льготами в запрашиваемом размере. Нередко защита таких документов сводится к подписи ответственного лица и печати, ставящихся на обычной бумаге.

Что даст и кого заинтересует «карточка горожанина»

Если рассматривать какой-либо крупный российский город, например Санкт-Петербург (более 4 млн физических и более 1 млн юридических лиц), как единое предприятие по оказанию услуг массового спроса населению с общим объемом доходов около 75 млрд руб., то в свете описанных проблем целесообразно разработать решение, которое улучшит как качество обслуживания потребителей услуг, так и финансовые показатели бюджета города.

Таким решением может стать платежно-идентификационная система на основе электронных пластиковых карт, обеспечивающая целевой учет социальной помощи населению. Электронная пластиковая карта («карточка горожанина») будет служить и платежным инструментом, и удостоверением личности, содержащим социальную и дополнительную информацию о владельце. Сочетание платежной и идентификационной функциональности в одной карте сделает возможным точный адресный контроль объема использованных социальных льгот.

Преимущества платежно-идентификационной системы для общества:

1) Прозрачная платежная и кредитная история как физических, так и юридических лиц.
2) Улучшение криминогенной обстановки за счет сокращения оборота наличных средств и адресного учета платежей.
3) Уменьшение количества налоговых нарушений и преступлений.
4) Снижение расходов на поддержание бумажного документооборота и содержание бюрократического аппарата.
5) Уменьшение расходов на поддержание оборота наличных денег (служба инкассации, кассы пересчета и т.п.).
6) Возможность адресного оказания социальной помощи и ее учета.
7) Отсутствие возможности злоупотребления социальными льготами.
8) Повышение эффективности использования бюджетных средств за счет их адресного учета.

Подобные системы уже действуют в некоторых крупных городах за рубежом и даже в трех округах Москвы. Но, в отличие от предлагаемого решения, они имеют узкую область применения, являясь лишь средством количественного контроля потребляемых льгот, что само по себе, конечно, полезно для муниципальных властей, но не слишком важно для граждан.

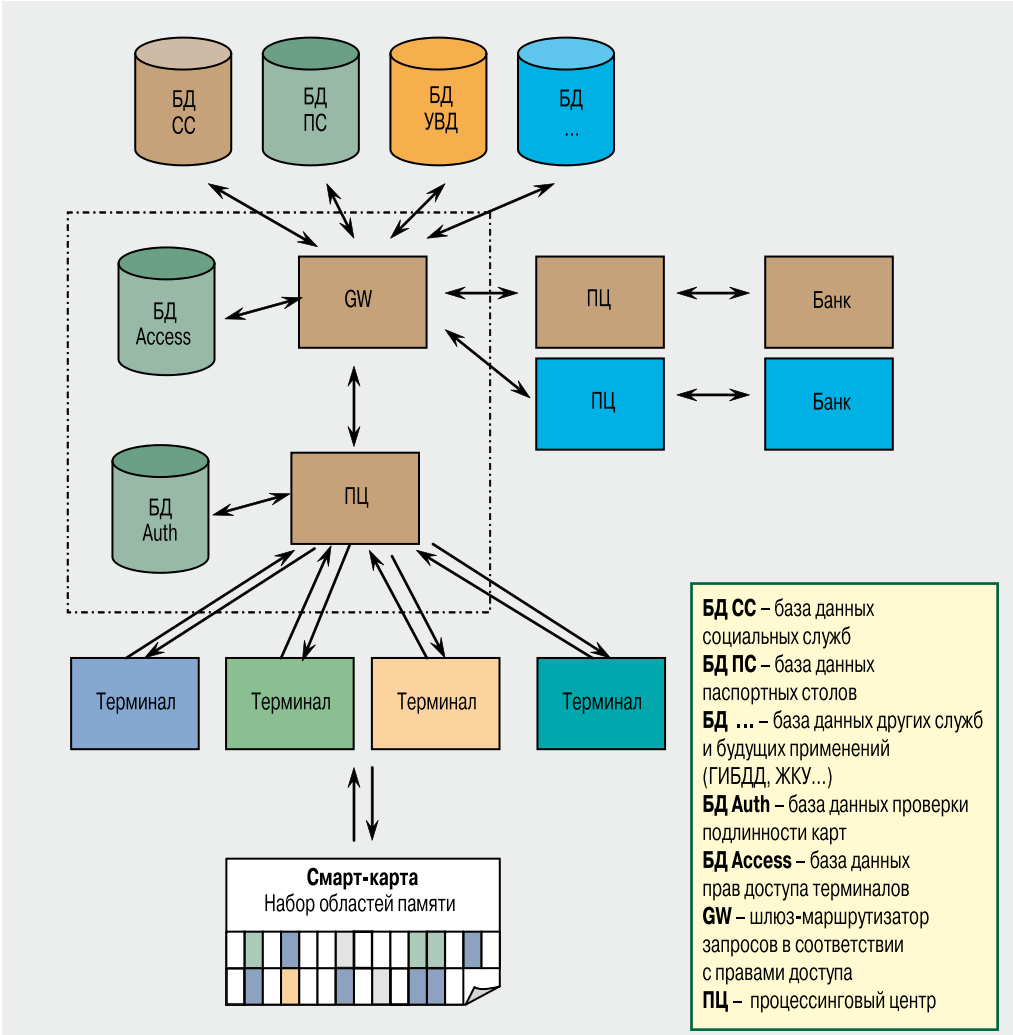
Рассматриваемая «карточка горожанина» будет иметь более широкую функциональность, чтобы своим удобством привлечь жителей, в том числе и тех, кто льготами не пользуется. Если она заинтересует широкие слои платежеспособного населения, то выручка от продажи таких карт нельготным категориям граждан поможет окупить проект частично или полностью.

Для того чтобы карта действительно стала интересной широкому кругу потребителей, она должна упрощать и ускорять выполнение официальных учетно-регистрационных процедур и позволять совершать любые платежи, как с социального счета, так и со счета коммерческого банка. Кроме того, система должна отличаться технологической простотой и удобством использования, а также обладать функциональной гибкостью с прицелом на дальнейшие применения, чтобы в будущем «карточку горожанина» можно было использовать как универсальный электронный документ для доступа к единым информационным ресурсам (вплоть до таких приложений, как медицинская карта).

Поддержать проект могут и банки, и предприятия, оказывающие услуги населению. Последним проект предоставит новое средство более полного и точного контроля движения их денежных потоков. Банки «карточка горожанина» может заинтересовать как инструмент аутсорсинговой организации карточных счетов и привлечения большой массы денежных средств населения, не говоря уже об увеличении объема безналичных платежей.

Сочетание платежной и идентификационной функций в одной карте сделает возможным точный адресный контроль использования социальных льгот

Структура платежно-идентификационной системы



Карточка горожанина. Краткий глоссарий

Смарт-карта – электронное устройство, реализующее функцию электронного удостоверения горожанина. Состоит из набора разделенных областей памяти, которые могут содержать различную информацию. Каждая запись на смарт-карте соответствует определенному полю в конкретной базе данных. Благодаря разграничению областей памяти на карте информация, относящаяся к одной БД, не может быть изменена при обращении к «соседней» БД.

База данных – хранилище информации, которая должна быть отражена в электронном удостоверении горожанина. В систему могут входить базы данных социальной службы, паспортных столов, УВД, а также любая другая информация, которую необходимо будет интегрировать в электронном удостоверении.

GW (gateway) – шлюз, предназначенный для соединения БД с процессинговым центром. Используется для создания интерфейса, обеспечивающего безопасную передачу данных, содержащих конфиденциальную информацию. Помимо этого, GW позволит масштабировать систему и подключать новые элементы через свои интерфейсы. Осуществляет проверку прав терминала, производящего операцию, на изменение запрашиваемой БД. Права терминалов запрашиваются из БД Access.

Процессинговый центр – центр обработки данных, который используется для авторизации банковских операций, а также для авторизации действий терминалов смарт-карт. Авторизует смарт-карту с помощью ПИН-кода и контрольной суммы (CRC) через БД Auth. При авторизации могут применяться алгоритмы шифрования с открытым ключом.

Терминал – устройство, производящее считывание информации, хранящейся на смарт-карте, и передачу ее для обработки в ПЦ. Также имеет возможность производить запись информации на смарт-карту.

Как потекут денежные потоки

При создании системы может быть выбрана одна из трех схем распределения социальных средств.

1. «Карточка горожанина» лица, пользующегося той или иной льготой, только регистрирует факт оказания услуги предприятием массового обслуживания, а сами денежные средства по-прежнему перечисляются непосредственно на счет предприятия (такой вариант наиболее выгоден самим предприятиям).

2. На «карточку горожанина» в раздел социальных платежей переводятся реальные деньги, но при этом отсутствует целевой контроль их использования, и гражданин имеет возможность потратить полученные средства по своему усмотрению (в этом случае проще сделать надбавку к пенсии и пособиям и отменить льготы).

3. Управление средствами по какому-либо социальному направлению поручается доверенному банку. Средства перечисляются банку на основании статистики потребления услуг, получаемой муниципалитетом из процессингового центра единой платежной системы. Банк перечисляет деньги предприятиям массового обслуживания по мере предоставления услуг и следит за их объемом. Так, если человек не потребил за месяц установленную норму услуг, то неизрасходованные средства возвращаются в актив банка, и в следующем месяце муниципалитет перечисляет банку сумму, учитывающую образовавшуюся экономию.

Какая бы из указанных альтернатив ни была выбрана, потребуется создавать такие дополнительные, но абсолютно необходимые системы, как телефонные и локальные центры поддержки клиентов, которые будут вести претензионную работу. Также эти центры могут служить еще одним каналом взаимодействия горожан с единой информационно-платежной системой города. Например, на начальном этапе, пока «карточки горожанина» не станут привычными, центры могут играть роль «единого окна» для доступа ко всем информационно-регистрационным ресурсам и для взаимодействия со всеми локальными ведомственными и муниципальными органами (паспортными столами, жилищно-коммунальными управлениями, МРЭО и т.п.). Помимо этого, телефонные центры могут выполнять справочные функции по всем вопросам, возникающим у муниципальных учреждений относительно баз данных, к которым будет иметь доступ единая платежно-идентификационная система.

Как должна быть устроена платежно-идентификационная система

Архитектурная идея, лежащая в основе проекта «карточки горожанина» (см. рисунок), заключается в том, что информационный центр системы строится не как единая база данных, содержащая копии всех имеющихся баз данных

> И архитектура системы, и структура карточки позволяют подключать информационные системы учреждений и банков гибко, по мере готовности

Преимущества платежно-идентификационной системы для граждан:

1) Удобство совершения платежей.
2) Удобство идентификации личности и подтверждения своих прав.
3) Удобство оформления официальных документов, уменьшение времени, затрачиваемого на бюрократические процедуры.
4) Минимизация количества носимых с собой идентификационных, справочных и платежных документов и снижение связанных с этим рисков (потери, порчи, износа и т.д.).
5) Минимизация криминальных рисков.
6) Прозрачность и облегчение управления собственным бизнесом (контроль работы транспорта, служащих, финансовых операций).
7) Повышение благосостояния нуждающихся граждан за счет более эффективной социальной политики.
8) Удобство получения и использования социальной информации.

учреждений и ведомств, а как синхронизирующий центр доступа со стандартизированными интерфейсами к информационным ресурсам участников проекта. Это позволит быстро запустить систему в эксплуатацию в уже существующем информационном пространстве и откроет возможность эволюционного развития и наращивания функциональности системы.

Основное достоинство системы – ее расширяемость. В ней выделены два свободно расширяемых направления – платежное и информационное (на рисунке информационные БД расположены вверху, а платежные – справа от центра). И архитектура системы, и структура самой карточки позволяют гибко, по мере готовности подключать информационные системы учреждений и банков, пожелавших присоединиться к единому информационному пространству. Тем самым обеспечивается возможность поэтапного внедрения проекта и, что немаловажно, долговечность системы, а именно возможность подключения к ней в будущем таких приложений, о которых сейчас мы даже не догадываемся. Это касается в первую очередь информационного направления.

На платежном направлении благодаря тому, что гибкость системы позволяет подключать любые новые банки, в ее платежном пространстве среди банков может возникнуть конкуренция. А поскольку банки создают собственные платежные системы лишь для того, чтобы привлечь оборотные средства на свои счета, им может оказаться выгоднее участвовать на конкурентной основе в единой городской карточке, чем нести расходы на поддержание своих процессинговых центров и на эмиссию «пластика». Поэтому можно предположить, что в будущем банки откажутся от собственных платежных систем и будут подключаться к платежно-идентификационной системе напрямую, а их процессинговые центры исчезнут из структуры системы за ненадобностью. Правда, произойдет это, скорее всего, далеко не сразу. Так как в банковской практике обработка транзакций в процессинговом центре осуществляется на платной основе, то при использовании единого процессингового центра системы банки будут платить за транзакции именно ему, что, собственно, и станет основной доходной статьей для финансирования дальнейшего развития проекта.

■ ■ ■

Подобные социально ориентированные решения сегодня не выглядят утопичными или чрезмерно сложными. С технической точки зрения такие системы абсолютно реальны. Более того, они уже давно существуют, причем во многих вариантах, так как любая электронная платежная система (например, та же Visa) включает в себя механизм однозначной идентификации клиента. Основная трудность создания подобных систем заключается в организации единого защищенного информационного пространства, охватывающего все сферы жизнедеятельности общества в целом и каждого индивидуума в отдельности, чего на данный момент в полной мере не удалось осуществить никому.

Тем не менее платежно-идентификационные системы давно рассматриваются во всем мире как наиболее логичное и перспективное продолжение эволюции электронных платежных систем. Действительно, в условиях развитой инфраструктуры безналичных платежей объединение платежного документа и документа идентификации личности открывает широкие возможности как для каждого индивидуума, так и для всего общества, использующего такие решения. ИКС

Основная трудность создания платежно-информационных систем заключается в организации единого защищенного информационного пространства

Регулирование 2.0
С персональной точки зрения

Прохожий спросил Ходжу Насреддина,
зачем он накопал в степи столько ям.
– Да зарыл в этой степи деньги, – отвечал Насреддин, –
но, как ни бьюсь, не могу найти.
– А ты не оставил каких-нибудь примет? – спросил прохожий.
– А как же! – ответил Насреддин. –
Когда я зарывал деньги, в том месте была тень
от облака, но теперь ни облака нет, ни тени.

Ключом ко всем фрагментам пазла под названием «информационное общество» – электронным госуслугам, социальным сетям, таргетированной рекламе и пр. – являются персональные данные. И чтобы пазл сложился, нужно устранить противоречия между глобальным характером информационного мира и локальным регулированием персональных данных.

Александр ГОЛЫШКО,
канд. техн. наук

Несколько лет назад на фоне слияния коммуникационных и информационных технологий, развития интернет-сервисов, превращения операторов в «битовую трубу» и т.п. возникла точка зрения, что обслуживание «длинного хвоста» каждого клиента (т.е. помимо оплаты услуг связи – вездесущая реклама, всевозможный шопинг, банкинг, «билетинг», «отелебронинг», «налогинг», «ЖКХинг» и пр. и пр.) есть основное условие благополучия будущего отраслевого бизнеса. И вот уже абонента на веб-сайте каждого оператора ожидает «личный кабинет». Но это было лишь начало.

Появились и стремительно разрослись социальные сети, в которых пользователям доступны различные сервисы для общения друг с другом. При помощи инструментов социальной сети каждый пользователь может создать свой виртуальный портрет – сформировать профиль, указав в нем подробно данные о себе: опыт работы, увлечения, интересы и цели. С развитием социальных сетей предоставляются все новые и новые привлекательные сервисы, в результате чего соцсети уже являются местом общения сотен миллионов пользователей по всему миру.

Невиданными темпами стала расти таргетированная интернет-реклама в поисковых системах, интернет-приложениях и социальных сетях – по последним данным TBG Digital, реклама на Facebook подорожала на 74%. Стоимость графической рекламы, оплата которой рассчитывается исходя из 1000 показов, по итогам II квартала 2011 г. для пользователей из США, Великобритании и Германии увеличилась на 45%. Компания Efficient Frontier (использующая свою методику) сообщила, что за год стоимость «клика» в Facebook выросла как минимум на 22%. Кстати, в 2010 г. выручка Google от рекламных бизнес-моделей составила $28 млрд против $2 млрд у Facebook. Крупнейшие корпорации забирают деньги с телевидения и перераспределяют медийные бюджеты в пользу Интернета. И спрос превышает предложение.

«Белогривые лошадки»

Известная детская песенка ставила серьезный вопрос – «что вы мчитесь без оглядки?». Теперь основной драйвер роста ИКТ-рынка – облачные технологии, которые дают любой сервис и даже инфраструктуру для любого «длинного хвоста». В рамках модели облачных услуг сервис-провайдер свободен в выборе способов и путей оптимизации инфраструктуры и снижения издержек. Клиент не владеет, не контролирует и не вступает во взаимодействие с технологиями и методами, которые используются сервис-провайдером для создания,

предоставления и поддержки функционирования облачных услуг. В обмен за отказ от «излишеств» клиент теперь имеет все – и личное хранилище разного рода данных, и набор всевозможных сервисов, и много такого, о чем даже не подозревает.

Вопросы и задачи, которые необходимо решать для успешного предоставления и получения сервисов из «облака», начинают обсуждаться в сфере здравоохранения и безопасности, логистики, транспорта, розничной торговли и многих других. Везде и всюду хотят превратить свои продукты в сервисы.

В частности, в МСЭ рассматривается модель архитектуры ресурсов. Схема такова: клиент – брокер (где определяются потребности, баланс нагрузок, QoS и пр.) – ресурс. Фактически всё (сети, компьютеры, ПО, платформы и т.д.) может быть предложено клиенту в виде «сервиса». Основной набор выглядит так: Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, Web-as-a-service.

На первый взгляд после подключения клиента к ШПД «традиционному» телекому здесь делать попросту нечего – голосовые и видеосервисы, доставляемые с различных облачных платформ, заменят телефонию и телевидение, да и вообще все коммуникации будут осуществляться через облачные серверы. Ну а разнообразные ИТ-сервисы уже давно поставляются кем угодно вне зависимости от операторских владений. Другое дело, что на практике не все так гладко, как на бумаге, – все эти «облака» еще нужно эффективно организовать и связать с клиентами и друг с другом. Но когда это, наконец, произойдет, многим придется «сушить весла» на своих телекоммуникационных «галерах». Если, конечно, «галеры» не были предусмотрительно направлены куда-нибудь в «облака».

Информация в обмен на риски

Со временем все перечисленные и неперечисленные инфокоммуникационные сервисы объединятся под брендом «информационного общества», вхождение в которое началось с активного продвижения так называемых электронных госуслуг. По сути, серверы электронного правительства – это те же «облака». Причем с точки зрения телекоммуникаций никаких особых проблем здесь нет, но во множестве появляются проблемы с персональными данными.

Ведь именно персональные данные являются ключом и к электронным госуслугам, и к социальным сетям, и к таргетированной рекламе, и к «длинному хвосту» каждого клиента. И к киберпреступности, кстати, тоже. Вкратце – на них зарабатывают или имеют иную выгоду абсолютно все, кто присутствует в Сети. Так что за проблемы?

Во-первых, в общем случае вы не знаете, где (даже в какой стране) расположен виртуальный сервер, на котором обрабатываются ваши персональные данные. И это уже риск. А согласно отечественному закону «О персональных данных» необходимо, чтобы все данные обрабатывались на территории РФ (собственно, а почему бы и нет?). В результате услуги, связанные с персональными данными, предоставляются провайдерами на мощностях (ЦОДах), расположенных «там, где надо». Поэтому «настоящая облачная модель», оптимально распределяющая всемирные вычислительные ресурсы – пока лишь мечта.

Во-вторых, работа с персональными данными чревата дополнительными расходами. Выполнение норм закона «О персональных данных» в принятой недавно редакции, как заключила Комиссия РСПП по телекоммуникациям и информационным технологиям, потребует со стороны бизнеса и предприятий бюджетного сектора экономики неоправданно больших затрат, которые серьезно затруднят их работу и отразятся на конечной стоимости услуг для потребителей. По сути, ко всем системам предъявляются завышенные унифицированные требования вне зависимости от того, какого рода персональные данные они хранят и обрабатывают. А по мнению Ассоциации региональных операторов связи, указанный закон не соответствует букве и духу европейского регулирования, предусматривающего регламентацию, прежде всего для государственных информационных систем, поскольку предоставление персональных данных является обязательным в рамках установленных административных процедур. При этом за рубежом негосударственные операторы персональных данных самостоятельно определяют необходимые меры защиты и применяют соответствующие процедуры и технические средства на свой выбор. Однако обычная реакция чиновников на самые разные законотворческие ситуации – «лучше перебдеть». Только в итоге «волны гасят-таки ветер», т.е. расходы операторов и пользователей увеличиваются, а ожидаемый эффект куда-то рассасывается.

В-третьих, в последнее время конфиденциальность персональных данных регулярно получает удары с разных сторон. Не успели улечься страсти по поводу появления в открытом доступе тысяч SMS пользователей мобильной связи, как выснилось, что доступны имена покупателей секс-шопов и их заказы. Специалисты отмечают, что любая информация, которая находится в общем доступе, может быть индексирована и найдена любым поисковиком. В частности, и в Google, и в «Яндексе» можно обнаружить заполненные бланки электронных билетов РЖД. В середине июля все пользователи соцсети Facebook могли свободно просматривать названия, описания и эскизы видео своих друзей, даже если те установили некие ограничения на доступ. Впрочем, с конфиденциальностью персональных данных у Facebook давно не все ладно. В конце прошлого года выяснилось, что соцсеть передает уникальные номера (ID) своих пользователей более чем двум десяткам сторонних организаций. Делается это даже в том случае, если пользователь установил максимальный уровень защиты. Еще один случай нарушения конфиденциальности был зафиксирован в феврале 2010 г., когда сервис по ошибке отправлял

личные сообщения пользователей не тем людям.

С другой стороны, сетевой бизнес требует все более точных персональных данных. В конце июля многие пользователи Google+ пожаловались на то, что их аккаунты стали недоступны. Выяснилось, что администрация соцсети начала применять пункт правил, о котором многие знали, но мало кто принимал всерьез. Он гласит, что пользователь должен указывать свои настоящие имя и фамилию. Один из сотрудников Google объяснил, что смысл сервиса Google Profiles – найти других людей и позволить им найти себя. Следовательно, нужно указывать то имя, под которым пользователь известен в реальной жизни. Отныне это не может быть какой-то произвольный псевдоним или случайный набор букв. Все это, конечно, так, но мы-то с вами понимаем, что кому-то хочется больше зарабатывать на таргетированной рекламе и т.п.

Персональный тупик

И, наконец, само международное сообщество, грезящее общепланетным информационным обществом, оказалось попросту не готово к глобальной работе с персональными данными. Совсем недавно члены Европарламента потребовали от юристов и членов Европейской комиссии разрешить конфликт интересов между США и Европой. Речь идет о Директиве Евросоюза о защите пользовательских данных, с одной стороны, и о так называемом Патриотическом законе США (US Patriot Act) – с другой. Впервые о существовании правовой коллизии заговорила компания Microsoft, которая сообщила своим европейским клиентам, что в случае если американские власти затребуют у нее как у американской компании данные об ее европейских пользователях облачных сервисов, то в соответствии с Патриотическим законом США Microsoft должна будет передать запрашиваемые сведения в Вашингтон, причем она даже не обязана уведомлять об этом европейскую сторону. Это прямо противоречит европейской директиве, которая требует, чтобы перед отправкой персональных данных владельцы этих данных ставились в известность. И тут на пути информационного общества возникает целый куст вопросов. Может ли Патриотический закон США отменять Директиву ЕС о защите данных? Что будет делать Еврокомиссия для разрешения этой ситуации и как обеспечивать защиту собственной информации? Имеют ли законодательства третьих стран преимущества перед законодательством ЕС? Как вообще строить глобальное информационное общество, не имея единого отношения к исходной информации для генерации практически любых сервисов – персональным данным?

Не так давно еврокомиссар Вивиан Рединг, курирующая вопросы защиты цифровых данных, заявила о том, что США и Европа должны создать «полностью совместимые» законы, касающиеся информационного общества. За это же ратует сенатор от Аризоны и экс-кандидат в президенты США Джон Маккейн. Ранее между ЕС и США уже было достигнуто соглашение Safe Harbor, по которому компании, в частности Microsoft, могут передавать европейские данные в США, но лишь в том случае, если будет обеспечен «приемлемый уровень» их безопасности. Однако для США Safe Harbor имеет более низкий приоритет по сравнению с Патриотическим законом.

Сегодня многие американские компании предлагают европейцам хранить данные в их «облаках». Однако все они тактично умалчивают об опасностях, подстерегающих европейских пользователей. Независимые эксперты указывают, что за этой юридической коллизией пристально следят не только в Microsoft, но и в Apple, Google, IBM, Facebook и Twitter, так как все эти американские компании работают и с европейскими данными. И с российскими тоже.

В результате клиентам уже начинают предлагать географический выбор мест хранения данных. Многие компании даже оформляют свои европейские ЦОДы на независимых операторов, дабы успокоить местных клиентов и избежать запросов по US Patriot Act. Мало кто сомневается, что если бы возникла обратная ситуация, когда американской стороне пришлось бы хранить свои данные в Европе, то Вашингтон использовал бы все рычаги давления для того, чтобы избежать раскрытия информации. Ведь у каждого своя правда.

Международное сообщество, грезящее общепланетным информационным обществом, оказалось не готово к глобальной работе с персональными данными

Поскольку информационное общество претендует на глобальный характер, российские нормативные правовые акты также должны предусматривать преодоление подобных коллизий. Однако в отсутствие международного права каждый так и останется при своем мнении. А в целом это – глобальный информационный тупик.

Получается, что для выхода из «персонального тупика» либо ИТ-сфера должна стать независимой от регуляторов и правительств (что крайне маловероятно в ближайшие 25 лет), либо необходимо на государственном уровне сменить модель работы с персональными данными.

Капитализм forever

Как уже отмечалось, именно персональные данные граждан являются основой множества бизнес-моделей и сервисов в сфере ИКТ. И вот что удивительно – их берут, их крадут, на них зарабатывают миллиарды (вспомним хотя бы капитализацию Facebook), ими крутят как хотят – и все совершенно бесплатно. То есть истинные владельцы этих данных, граждане, ничего с этого не имеют. Разумеется, кого-то это устраивает.

Кому-то может показаться, что истинным владельцем персональных данных следует считать государство. Ведь это государство выдает свидетельство о рождении и прочие бумажки (хоть и в электронном виде), назначает ИНН и пр. К тому же граждане порой так безответственны и беспечны и выкладывают в соцсетях такое...

Но здесь можно и возразить. Во-первых, данные называются-таки персональными, а не государственными. Во-вторых, основной ущерб от утечек этих данных наносится отнюдь не государству. Ну скажите, есть ли государству разница, узнал весь дом или нет, какой товар покупали их соседи в секс-шопе? Зато самим соседям, вероятнее всего, разница есть. Кстати, еще больше интересного таится в вашей медицинской карте, вашей кредитной истории, структуре вашей собственности (эффективное государство это и так знает). В-третьих, материальные потери от кражи персональных данных (к примеру, вместе с деньгами со счета) в первую очередь несут опять же граждане. В общем, государство здесь не собственник, а скорее нанятый охранник, обладающий соответствующим законодательством и различными инструментами его соблюдения в лице спецслужб, прокуратуры, судов и пр.

Одно из решений – превращение персональных данных каждого пользователя в его постоянную и неотчуждаемую собственность (ее нельзя продать или отнять), доступ к которой определяется владельцем и должен быть платным. Короче – за пользование чьими-либо персональными данными надо платить. Платить, причем обязательно, должны все к ним обращающиеся, если это не «свои» госструктуры (т.е. магазины, поисковые системы, рекламные площадки и пр.) – такой может быть новая государственная политика. Регулятор установит предельные цены за доступ к персональным данным (это могут быть сущие копейки, но суть в том, что они есть, как есть и основа для иска), перечень мероприятий по пресечению их несанкционированного использования, а также правила их страхования. И те, кто не платит, будут попадать в тесные объятия государственной машины.

Вот, к примеру, поисковик не удаляет страницы из результата поиска, пока владельцы сайта не примут мер, чтобы их содержимое не было доступно поисковой системе. И он тут в своем праве. Затем Роскомнадзор просит поисковиков рассмотреть техническую возможность блокировать запрос, который позволяет получить в ответ персональные данные. Прокуратура пытается защитить персональные данные покупателей интернет-магазинов. Давайте облегчим ей задачу и разрешим всем пользователям, которым не заплатили за использование их персональных данных, подать в суд на тех, кто не обеспечил защиту таковых. И тогда даже трудно себе представить, насколько быстро владельцы веб-сайтов озаботятся защитой персональных данных. И не надо разрабатывать никаких общих технических условий и помещать их в законы – рыночные игроки «со свистом» будут поспевать за ИТ-прогрессом и хакерами. Тут, глядишь, исчезнут претензии к назойливой интернет-рекламе – если вам заплатили за ее просмотр, то и возмущаться незачем, если нет – сразу же есть чем заняться прокуратуре.

Да, это новый подход к взаимоотношениям субъектов в информационном обществе. Да, это сформирует новые отношения и новые рыночные площадки. Да, это нанесет серьезный удар халяве и безответственности при использовании персональных данных. Но это и позволит обеспечить защищенность электронного гражданина будущего электронного государства. Потому что стоимость доступа к электронному гражданину будет твердой валютой того самого государства, которую не измерить в бумажках. И заодно будет легче претворить в жизнь Доктрину информационной безопасности.

Кстати, возможность сохранения номера мобильного телефона (или Mobile Number Portability, MNP) – это один из способов использования наших персональных данных. У каждого гражданина должен быть один уникальный номер (выданный ему государством), с которым он должен иметь право «гулять» по сетям (и который нельзя у него отнять). Вот для этих персональных номеров и нужно обеспечить MNP. Для остальных же телефонных номеров MNP не нужна. Пусть одни сэкономят, другие – заработают, да еще и конкуренция вокруг обслуживания граждан усилится.

Поставщики сервисов привыкли жить при капитализме и извлекать прибыль из оборота персональных данных? Получите капитализм в лице полноценного рыночного партнера/абонента/гражданина, у которого вы что-то заняли, чтобы вести свой бизнес. Ведь мы партнеры, не правда ли? ИКС

Спецзащита для облачных сред

Для руководства компаний первым барьером на пути внедрения облачных сред становится поддержание надлежащего уровня безопасности. Но многие технологии защиты в облачной инфраструктуре становятся помехой и не позволяют реализовать необходимую для бизнеса функциональность.

Рик ФЕРГЮСОН, руководитель департамента аналитики и коммуникаций, Trend Micro EMEA

Михаил КОНДРАШИН, генеральный директор компании АПЛ

ИТ и ИБ-руководители убеждены, что предоставление корпоративных данных и серверов стороннему ЦОДу неотвратимо приведет к нарушению нормального функционирования системы безопасности их компании, потере контроля над ней и доступа к информации регистрации и аудита.

Основная причина негативного отношения профессионалов к облачным вычислениям описывается одним словом: «депериметризация». Но, возможно, термин «репериметризация» будет более точным. Ведь периметр безопасности не исчезает в виртуализованной среде, где виртуальные машины с различным уровнем доверия используют один и тот же гипервизор, он не исчезает и в облачной среде с большим количеством владельцев. Разумеется, термин «периметр» все еще присутствует, но в него уже не вкладывается такой сакральный смысл, и его использование должно быть пересмотрено.

Кардинальное различие в подходах к безопасности виртуализованных сред лучше всего иллюстрирует подход к конфигурированию межсетевого экрана, традиционного средства обеспечения сетевой безопасности ЦОДа. Поставщики облачных услуг вынуждены при его настройке следовать принципу «наименьшего общего знаменателя», т. е. устанавливать наименее жесткую политику с целью избежать неполадок у некоего гипотетического клиента. Очевидно, что ни для одного реального клиента такая настройка не будет оптимальной по уровню безопасности. Кроме того, кабели, коммутаторы, полосу пропускания, платформы виртуализации и сети хранения данных в облачной инфраструктуре следует рассматривать как ресурсы, находящиеся в совместном пользовании, и поэтому они не могут считаться доверенными. Некоторые аспекты традиционной инфраструктуры объединены в гипервизоре или на уровне абстракции виртуализованной сети хранения данных; многие технологии обеспечения безопасности в новой инфраструктуре становятся помехой и не позволяют реализовать необходимую для бизнеса функциональность.

Разумеется, описанная выше ситуация не может не подорвать доверие потенциальных заказчиков к облачным технологиям.

Безопасность инфраструктуры или безопасная инфраструктура

Переход на облачные среды влечет за собой не только изменения технической архитектуры; он требует и существенных перемен в работе корпоративных команд ИТ-специалистов. Зачастую на крупных предприятиях и даже у системных интеграторов разные команды инженеров работают над проектами обособленно. В таких условиях сначала завершается одна

Словарь ИКС

Депериметризация

Этот термин впервые был предложен еще в 2004 г. при создании международного форума «Иерихон» (Jericho Forum), объединившего множество организаций, заинтересованных в совместном решении проблем, связанных с облачными вычислениями. Депериметризация означает выход за традиционные рамки корпоративных сетей и приводит к необходимости использовать многоуровневые технологии непосредственно на уровне данных, протоколов и цифровых ресурсов.

из составляющих проекта информатизации, например, монтаж физической сети или размещение серверов, и лишь затем к проекту подключаются специалисты по безопасности, обеспечивающие защиту построенной инфраструктуры.

Изоляция команд специалистов порождает принципиальные трудности. В мае прошлого года даже технологический гигант HP поднял тревогу по этому поводу. Говоря о развертывании проектов интеллектуальных grid-сетей, Ян Миттон, директор подразделения по работе с промышленностью компании HP, пояснил: «Наши наблюдения показали, что безопасность должна быть обеспечена заранее, но на практике несколько запаздывает. Это не может не вызывать определенного беспокойства. Складывается ситуация, когда разработчики проектов, словно бы спохватываясь, восклицают: “О Боже мой! А как же безопасность?”».

В виртуализованной среде появляется новая мишень для злоумышленников и вирусов – сама платформа виртуализации

Почему же недостаточное взаимодействие между командами так принципиально? Виртуализация серверов и рабочих станций (VDI) в ЦОДе, услуги IaaS, PaaS и SaaS изменили архитектуру корпоративных информационных систем больше, чем любое другое нововведение за последние 15 лет. Вместе с тем с переходом к новым технологиям ни одна из базовых проблем безопасности не исчезла. Наоборот, возникли новые угрозы, не имеющие аналогов среди своих физических предшественников, например на уровне виртуальной архитектуры. Ключевая причина указанных сложностей – периметризация, так как во многих аспектах исчезло традиционное разделение ИТ-инфраструктуры на сеть, платформу, приложения и т. д. Сейчас недостаточно быть экспертом в области только инфраструктуры или информационной безопасности. Необходимо концентрировать усилия не на обеспечении безопасности существующей, а на создании безопасной инфраструктуры.

Специфически облачные угрозы

Размещение виртуальных серверов и данных в облачной среде, т. е. совместно с серверами и данными других пользователей, конкурентов, возможно, даже злоумышленников (вспомним криминальную деятельность в облаке Amazon EC2*), вызывает множество новых проблем. Невозможность установить обновления на временно выключенную виртуальную машину приводит к тому, что в течение некоторого времени после загрузки она оказывается совершенно не защищенной от самых популярных атак – на широко известные уязвимости. С другой стороны, даже если виртуальный сервер постоянно включен и обновления регулярно загружаются, их установка может потребовать перезагрузки сервера, а облачная инфраструктура никак не помогает минимизировать подобный вынужденный простой. Поток данных, передаваемый от машины к машине одного и того же гипервизора, не затрагивает физическую сеть, поэтому традиционные технологии обеспечения сетевой безопасности не способны распознать угрозу. В виртуализованной среде появляется новая мишень для злоумышленников и вирусов – сама платформа виртуализации, но опять же никаким традиционным средством защиты невозможно предотвратить эту угрозу. Непростым вопросом является разграничение доступа к данным, так как они, несомненно, доступны техническому персоналу поставщика облачных услуг.

Для обеспечения безопасности облачных сред средства защиты должны функционировать, реконфигурироваться и контролироваться на уровне самой виртуальной машины. Ключевыми технологиями здесь являются программные межсетевые экраны с глубоким анализом пакетов и предотвращение проникновения на уровне приложений.

Уязвимый уровень приложений

Согласно докладу IBM X-Force о тенденциях и угрозах за первое полугодие 2010 г., более половины (55%) всех обнаруженных уязвимостей были выявлены в веб-приложениях.

* InfoWorld, 10 декабря 2009 г. Hackers find a home in Amazon’s EC2 cloud.

В целом количество новых обнаруженных уязвимостей оказалось самым высоким, а максимальное число уязвимостей пришлось на межсайтовый скриптинг и SQL-инъекции. Подобные атаки в облачных средах открывают возможность масштабных утечек конфиденциальной информации, а при неблагоприятном стечении обстоятельств завершаются внедрением вредоносного кода. Брандмауэры должны действовать на уровне веб-приложений и блокировать любой аномальный трафик до того, как данным или серверам будет нанесен вред.

Даже если для обнаруженной уязвимости уже выпущена заплата, ее зачастую непросто оперативно применить на серверах, где простои могут быть крайне нежелательны. Во многих случаях виртуальные машины функционируют в средах, где окна для обновления программ минимальны или вовсе отсутствуют. Это делает виртуальную машину уязвимой для атак и взлома как изнутри, так и снаружи. Необходимо обеспечить неуязвимость системы, даже если исправления еще не были применены. Здесь могут помочь средства предотвращения проникновения на уровне хоста и технология «виртуальных заплат».

Нетрадиционные средства

Обеспечение безопасности виртуальных сред осложняется тем, что многие виды традиционных средств защиты неэффективны в новых условиях, хотя виртуальный компьютер специально создается так, чтобы работать аналогично физическому. Типичный пример: антивирусы создают недопустимо большую нагрузку на систему виртуализации, особенно во время запланированной проверки всей системы. Традиционные средства антивирусной защиты не способны сканировать и обновлять выключенные виртуальные машины. В результате при включении этих машин файлы вирусных сигнатур также оказываются устаревшими, что означает повышение риска заражения сразу после старта. Обнаружение в 2010 г. уязвимости в системе VMware, когда проникновение вредоносной программы на виртуальную машину позволило исполнить код на физическом компьютере, существенно подняло ставки (и дало исследователям вредоносного ПО массу пищи для размышлений).

Но не все так плохо. Виртуальная среда дает новые возможности для защиты, хотя это требует разработки новых антивирусных продуктов. Обычно программное обеспечение системы безопасности функционирует в той же среде, что и угроза, и должно присутствовать на той же машине, которая может быть взломана. В физических сетях просто нет иных вариантов. Анонсированная компанией VMware технология VMsafe позволяет создавать системы безопасности в виртуальных средах, даже более надежные, чем их физические аналоги. В последних версиях VMware механизмы обеспечения безопасности можно помещать в виртуальное устройство, логически отделенное от защищаемых машин. Эта технология обеспечит безопасность, включая систему предотвращения вторжений (IPS) и, что важно, защиту от вредоносного ПО, в реальном времени без установки антивирусного пакета на каждой машине, нуждающейся в защите. Таким образом, даже если машина все-таки будет взломана, злоумышленники не смогут отключить сам механизм защиты.

Многие виды традиционных средств защиты, например антивирусы, неэффективны в виртуализованных средах

■ ■ ■

Индустрия обеспечения безопасности должна способствовать продвижению облачных сред – более дешевых, динамичных и экологичных. Необходимо убедиться в том, что мы создаем технологию, тесно интегрирующуюся в новую бизнес-среду, готовую к использованию в виртуальных и физических средах с единым набором средств управления и, разумеется, способную обеспечить корректную политику безопасности вне зависимости от физического расположения находящегося под защитой сервера. В противном случае в погоне за снижением текущих расходов и увеличением гибкости бизнеса в первую очередь пострадает эффективность средств обеспечения безопасности. ИКС

Борьба с мошенничеством – этично или неэтично?

О мошенничестве в финансовых и телекоммуникационных компаниях пишут часто, а историями успеха борьбы с ним делятся редко. Почему?

Андрей СТЕПАНЕНКО, директор по развитию бизнеса компании «Информзащита»

Проблема внутри

В начале нынешнего года компания Ernst &Young опубликовала примечательный отчет European Fraud Survey 2011, в котором сравнила текущее положение дел с мошенничеством в 25 странах (включая Россию) с результатами исследования 2009 г. Общий вывод экспертов – в условиях экономического кризиса количество компаний, борющихся с мошенничеством, уменьшилось примерно на четверть.

В это же время вышел отчет Cutting costs and cutting fraud. Economic crime in the public sector компании PricewaterhouseCoopers, в котором отмечалось, что за тот же период в условиях сокращения расходов на борьбу с мошенничеством доля компаний, пострадавших от него, увеличилась на 15%, а доля внутреннего мошенничества выросла более чем на треть.

Причины терпимости к мошенничеству

Конечно, в условиях кризиса многие компании были вынуждены перенаправить ресурсы на решение более приоритетных для защиты бизнеса задач. Но есть и общие причины столь вялой борьбы с мошенничеством.

С одной стороны, на растущих рынках прибыльность деятельности сохраняется на приемлемом уровне, поэтому владельцы бизнеса мирятся с потерями от мошенничества.

С другой стороны, всегда есть сотрудники, которые не заинтересованы в пресечении мошенничества. По данным исследования Profile of a Fraudster Survey компании KPMG большинство внутренних мошенников – менеджеры высшего (60%) и среднего (26%) звена.

Поэтому понятно, что успешной борьба с мошенничеством может быть при соблюдении как минимум двух условий:

- компания работает на высококонкурентном рынке, переходящем или уже вступившем в стадию зрелости, что приводит к снижению доходности бизнеса, которое не устраивает владельцев компании;
- владельцы компании способны «продавить» внедрение системы борьбы с мошенничеством, несмотря на возможное сопротивление менеджмента.

Есть ли свет в конце тоннеля?

К задаче борьбы с мошенничеством рекомендуют подходить так же, как и к управлению рисками. Это означает, что мы должны смириться с тем, что полностью защититься от мошенничества мы не сможем.

Тогда в самом общем виде задачу борьбы с мошенничеством можно сформулировать следующим образом: «Уменьшить потери от мошенничества на величину, превышающую затраты на достижение этого результата».

Вспомните принцип Парето: 20% усилий дают 80% результата, а остальные 80% усилий – лишь 20% результата. В контексте этого принципа оптимальное решение задачи борьбы с мошенничеством сводится к выявлению таких мер, внедрение которых приведет к максимальному снижению потерь.

Умеют ли компании выбирать «правильные» меры?

В отчете международной Ассоциации сертифицированных специалистов по расследованию мошенничеств The 2010 Report on Occupational Fraud and Abuse перечислены 15 направлений борьбы с мошенничеством, наиболее часто реализуемых в компаниях. Самые распространенные среди них – реактивные методы: внешний (76%) и внутренний (66%) аудит. Наименее популярная мера – выплата вознаграждений за информацию о мошенничестве (7%), хотя специальная «горячая линия» для анонимного извещения о мошенничестве используется значительно чаще (48%).

Что же из этих мер помогает ловить мошенников? Парадоксальный ответ содержится в этом же отчете. Внешний аудит помог выявить менее 5% случаев, внутренний аудит – около 14%. Абсолютным же лидером – более 40% – являются сообщения сотрудников, клиентов и иных лиц, которым стало известно о мошенничестве.

Так бороться или не бороться?

Затраты на проведение аудита существенно превышают расходы на пропаганду нетерпимости к мошенничеству, обработку полученных сигналов и возможную плату за них. То есть по принципу Парето нужно внедрять именно эти меры, и в результате задача приобретает новый этический окрас.

Возможно ли, что самые успешные проекты по борьбе с мошенничеством насаждали атмосферу слежки сотрудников друг за другом? Если да, то неудивительно, что об этих проектах не любят рассказывать.

Так появляется третье условие, необходимое для успешного внедрения системы борьбы с мошенничеством, – готовность компании решать сложную этическую проблему, затрагивающую корпоративную культуру. ИКС

ИКТЭХнологии pro

Поддержание микроклимата на базовых станциях сотовой связи

Какая система эффективнее?

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

Егор БУРАКОВ,
ведущий инженер отдела исследований и развития United Elements

Энергопотребление базовых станций – существенная часть издержек операторов сотовой связи, особенно в условиях роста объема пропускаемого сетями трафика и количества БС. Экономия на поддержании микроклимата в помещениях базовых станций может внести серьезный вклад в снижение операционных затрат.

Основной параметр микроклимата, который нужно поддерживать на базовых станциях, – температура воздуха. Отметим, что обеспечивать должный уровень температуры необходимо главным образом для систем гарантированного энергоснабжения. Например, для устойчивой работы ИБП производства Enel, по заявлению компании, требуется температура 20±5°C, а телекоммуникационное оборудование Ericsson, по данным производителя, может работать при температурах в диапазоне от +5 до +40°C.

Для правильной оценки энергозатрат системы микроклимата БС недостаточно учитывать только обобщенные данные по температурам наружного воздуха, указанные в СНиП 23-01-99 «Строительная климатология». При моделировании, результаты которого приведены в статье, использовалась информация о почасовом распределении температуры в течение года, полученная путем длительного наблюдения на метеорологических станциях аэропортов и аэродромов. При этом взят не какой-то определенный год, а так называемый типичный метеорологический год. То есть данные, представленные на каждый час в году, были усреднены, исходя из наблюдений с 1948 по 2005 гг. Это означает, что вероятность повторения выбранных параметров очень высока. Существенна также их почасовая разбивка.

Анализ энергопотребления проведен для базовой станции, расположенной в Санкт-Петербурге. Суммарное тепловыделение БС – 2 кВт, размеры – 3200 × 2300 × 2500 мм (Д × Ш × В), температура, которую требуется поддерживать, – +25°C. Для создания моделей использован дополнительный теплофизический параметр – тепловой баланс при поддержании требуемой температуры внутри помещения. Тепловой баланс представляет собой сумму всех теплопритоков и теплопотерь:

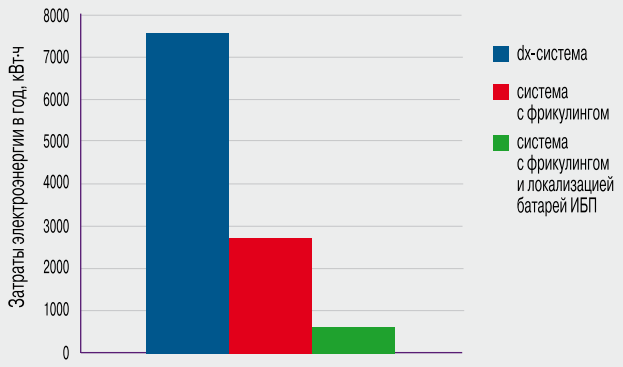
$$Q_{пом} = Q_{обр} + Q_{огр} + Q_{инф} + Q_{слрд},$$

где $Q_{пом}$ – тепловой баланс помещения;
$Q_{обр}$ – теплота, поступающая в помещение от оборудования;
$Q_{огр}$ – теплота, поступающая от ограждений;
$Q_{инф}$ – теплота, поступающая при инфильтрации;
$Q_{слрд}$ – теплота, поступающая от солнечной радиации.

Очевидно, что в значения слагаемых $Q_{пом}$ помимо теплоты, выделяемой оборудованием, свой вклад вносят внешние условия (солнечная радиация, скорость ветра), температура внутри помещения и его конструктивные особенности, влияющие на теплообмен внутреннего воздуха с окружающей средой

Рис. 1. Пример dx-решения

Рис. 2. Годовое энергопотребление различных систем микроклимата БС



(размеры, материал и негерметичность ограждающих конструкций). Поэтому если тепловой баланс помещения при заданной внутренней температуре положителен, то теплоизбытки надо компенсировать, иначе температура внутри помещения будет расти. Если же баланс отрицателен, то без компенсации теплопотерь температура будет падать. Знак теплового баланса и значение наружной температуры принимались в модели как условия выбора режимов работы.

Сплит-системы

В настоящее время на базовых станциях чаще всего устанавливаются бытовые сплит-системы, имеющие режим нагрева воздуха или дополняемые отдельным нагревателем. Для резервирования используется вторая такая же сплит-система (direct expansion, dx, см. рис. 1).

Когда температура воздуха в помещении поднимается выше установленной, включаются вентилятор и компрессор, воздух начинает охлаждаться и циркулировать до того момента, пока температура не упадет ниже заданного значения. Схема достаточно проста, но имеет ряд недостатков. Во-первых, не у всех производителей сплит-системы обеспечивают циркуляцию воздуха в помещении при выключенном холодильном контуре, в результате чего может возникнуть локальный перегрев в «горячих» точках; во-вторых, работа сплит-системы может понадобиться в холодное время года, а пуск кондиционера при температуре ниже –10°С даже при наличии таких опций, как стандартный «зимний» комплект, чреват аварийной остановкой по низкому давлению или поломкой. В российской практике используемый «зимний» комплект обеспечивает работоспособность при температурах до –30... 40°С. Однако в этом варианте при неработающем кондиционере необходим постоянный подогрев картера, на что расходуется дополнительная электрическая мощность.

Но главное, что dx-система весьма неоптимально использует условия окружающей среды. Даже если температура наружного воздуха намного ниже уровня, который нужно поддерживать внутри БС, но тепловой баланс в помещении положителен, то сплит-система будет работать на охлаждение. Для Санкт-Петербурга, например, такие условия наблюдаются практически круглый год, что приводит к высокому энергопотреблению (рис. 2).

Естественное охлаждение

Наряду с dx-решениями для поддержания микроклимата в помещениях базовых станций сегодня начинают внедряться системы, использующие для охлаждения телекоммуникационного оборудования наружный воздух (фрикулинг, рис. 3).

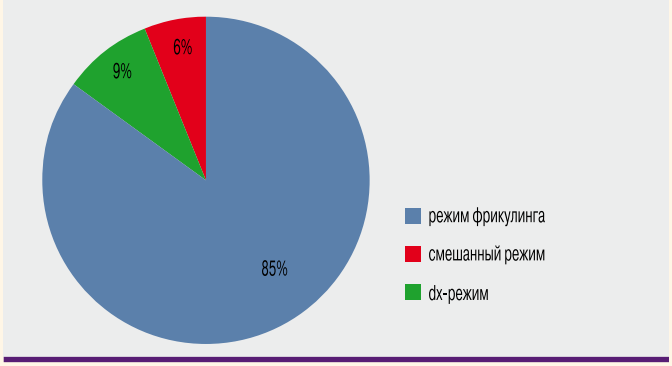
Такие системы, как правило, включают в себя вентилятор, фильтр, два воздушных клапана, систему управления и бытовую сплит-систему. Сплит-система необходима не только для работы в условиях, когда температура наружного воздуха выше уставки в помещении, но и для резервирования микроклиматической системы.

Основными параметрами выбора режима работы являются температура воздуха внутри помещения и температура наружного воздуха. Ориентируясь на них, система управления принимает решение об использовании приточного вентилятора или сплит-системы. Важную роль при этом играет расход воздуха, обеспечиваемый приточным вентилятором: чем он больше, тем больше тепла можно снять, не прибегая к включению сплит-системы. Зависимость мощ-

По сравнению с dx-решением годовая экономия энергопотребления микроклиматической системы на основе фрикулинга составит примерно 72%, а применение смешанного режима позволит дополнительно сэкономить еще 3%

Рис. 3. Система на основе фрикулинга

Рис. 4. Годовое распределение времени работы по режимам



ности системы фрикулинга от расхода наружного воздуха имеет следующий вид:

$$Q_x = \frac{L \cdot \rho}{3600} \cdot \Delta t \cdot C_\rho,$$

где Q_x – тепло, которое может быть компенсировано системой фрикулинга, кВт;
L – расход воздуха, м^3/ч;
ρ – плотность воздуха, кг/м^3;
Δt – разница между температурой наружного воздуха и температурой воздуха внутри помещения, °С;
C_p – теплоемкость воздуха, кДж/(кг·К).

При температуре наружного воздуха ниже требуемой в помещении система работает, используя холод наружного воздуха. Когда температура в помещении начинает расти, а вентилятор системы фрикулинга работает на 100% своей мощности, система переходит на циркуляцию внутреннего воздуха через сплит-систему. Как правило, оборудование допускает возможность организации смешанного режима с использованием как наружного воздуха, так и сплит-системы. Целесообразность такого режима основана на том, что в определенном диапазоне температур наружного воздуха, когда мощности фрикулинга уже недостаточно для компенсации теплопритоков ($Q_x < Q_{пом}$), энергетически выгодно задействовать на 100% мощности вентилятор фрикулинга и не на полную мощность – сплит-систему. На упомянутой базовой станции, для которой проводился энергетический анализ, смешанный режим целесообразен при температурах наружного воздуха в диапазоне от 17,2 до 19,2°С.

По сравнению с dx-решением годовая экономия энергопотребления микроклиматической системы на основе фрикулинга составит примерно 72%, а применение смешанного режима позволит дополнительно сэкономить еще 3% (рис. 2). Для рассматриваемых условий львиную долю времени система работала в режиме фрикулинга (рис. 4).

Естественное охлаждение и локализация зоны поддержания параметров

Напомним, что самым чувствительным к перепаду температур блоком БС является батарея ИБП, тогда как само телекоммуникационное оборудование способно работать при температурах от +5 до +40°С. Соответственно, ограничив размерами самих батарей ИБП зону, в которой обеспечивается требуемая для них температура, можно практически на всей территории России отказаться от парокомпрессионных систем и осуществлять охлаждение только за счет наружного воздуха. Для поддержания температуры в таком небольшом объеме производители выпускают изолированные корпуса со сборками на основе термобатарей, использующих эффект Пельтье (рис. 5, 6).

Рис. 5. Локализация батарей ИБП

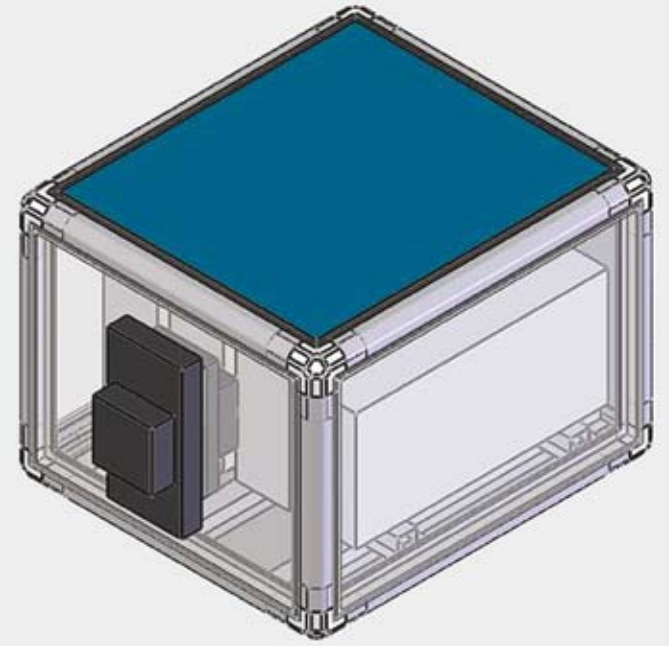


Рис. 6. Принцип работы сборки на термобатареях

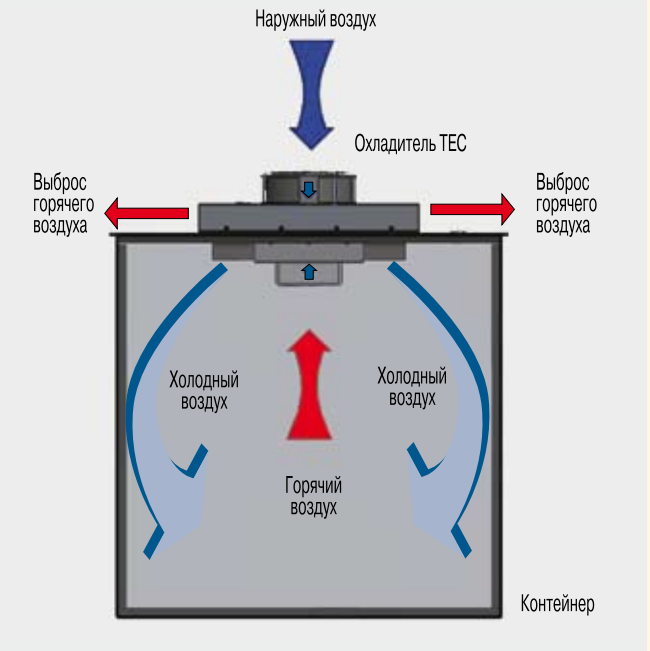
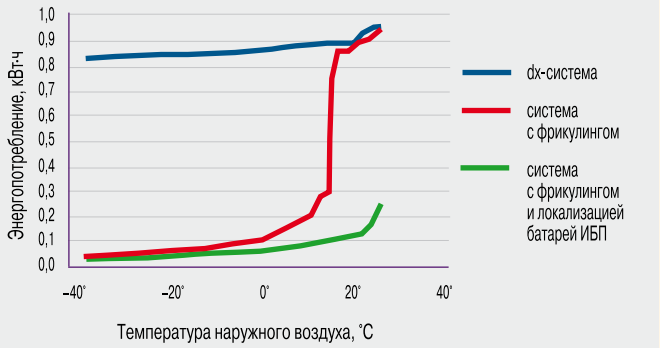


Рис. 7. Энергопотребление микроклиматической системы в зависимости от температуры наружного воздуха



Это позволяет при необходимости не только охлаждать, но и нагревать воздух внутри изолированного корпуса с батареями.

При положительном тепловом балансе приточный вентилятор поддерживает температуру в помещении в пределах от +5 до +40°C, а сборка на основе термобатарей – требуемую температуру внутри изолированного корпуса с батареями ИБП.

Для расчета экономии электроэнергии, достигаемой в предложенном варианте, использовались данные по энергопотреблению термобатарей в зависимости от перепада температур внутри и снаружи корпуса для батарей ИБП. Для рассматриваемой базовой станции годовая сумма электроэнергии, потребленной системой микроклимата с фрикулингом и локализацией батарей ИБП оказалась в 15 раз (!) меньше, чем для dx-решения (см. рис. 1). Таким образом, наиболее экономично в плане потребления электроэнергии охлаждение с помощью наружного воздуха при локализованных зонах для батарей ИБП.

Также весьма важно, что, когда температуры наружного воздуха близки к температуре внутри базовой станции, единственным решением, обеспечивающим энергосбережение, является повышение уставки температуры внутри БС при наличии системы локализации батарей ИБП (рис. 7).

■ ■ ■

Уменьшение размеров оборудования и увеличение плотности теплового потока приводят к тому, что третья из рассмотренных микроклиматических систем и ее различные модификации имеют наибольшие перспективы дальнейшего применения. Достигаемое с их помощью уменьшение расхода электроэнергии однозначно указывает на экономическую выгоду сочетания локализации зоны поддержания микроклимата с расширением диапазона уставки температуры в помещениях базовых станций. ИКС

Резервы повышения энергоэффективности ЦОДа

Александр ЛАСЫЙ,
технический директор департамента интеллектуальных зданий компании КРОК

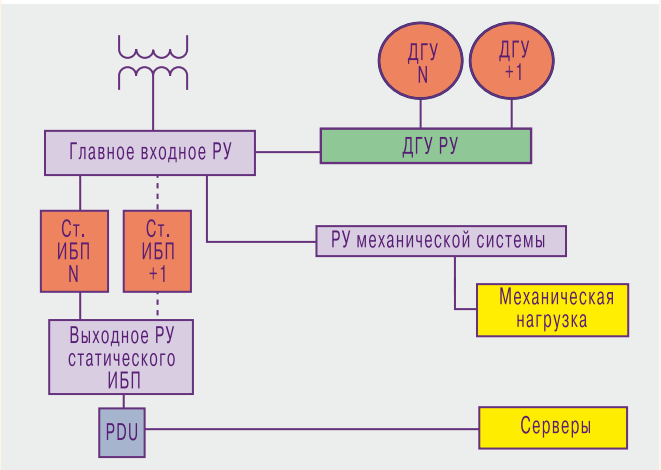
Энергоэффективность ЦОДов определяется в основном системой холодоснабжения и кондиционирования и системой электроснабжения. Остальные системы влияют на энергоэффективность незначительно, но при больших мощностях ЦОДов и несколько процентов могут дать существенную экономию.

Системы холодоснабжения и кондиционирования

Наибольший потенциал энергосбережения имеют системы кондиционирования и холодоснабжения. Большую часть года на территории России температура воздуха не превышает 20–22°C, поэтому, следуя рекомендациям ASHRAE и поддерживая температуру на входе в ЦОД в пределах 22–28°C, можно применять фрикулинг 80–85% времени в году. Значительную экономию электроэнергии дают системы воздушно-воздушного охлаждения – KyotoCooling, EcoBreese (APC), а также системы адиабатного охлаждения, разработанные в России компанией «Аякс». При их использовании среднегодовое значение PUE может достигать 1,20–1,25. Однако не следует забывать, что в тот короткий период времени, когда фрикулинг не работает, пиковое энергопотребление этих систем практически равно полезному энергопотреблению. И энергию на эти пиковые нагрузки нужно где-то брать.

Сейчас для охлаждения воды, работающей в прецизионных кондиционерах крупных ЦОДов, можно применять чиллеры с компрессорами на базе технологии Turbocore. Такие компрессоры позволяют плавно изменять энергопотребление в зависимости от необходимого количества холода. Показатель их эффективности (COP) в среднем составляет 4–5, а при оптимальных условиях – 6–8. Если наряду с этими компрессорами задействовать системы фрикулинга, то среднегодовой PUE может достигать примерно тех же значений, что и в системах с воздушно-воздушным охлаждением, а пик потребления энергии будет значительно ниже. Традиционные многокомпрессорные системы с фрикулингом могут обеспечить хорошие результаты, причем первоначальные капитальные вложения не слишком отличаются от затрат на обычные системы с воздушным охлаждением. Но при установлении оптимального температурного режима внутри ЦОДа можно добиться среднегодовых значений PUE 1,4–1,7, что в общем-то неплохо, особенно для средних ЦОДов мощностью 1–2 МВт.

Рис. 1. Система электропитания Tier II



Надежное и эффективное электроснабжение ЦОДа

Согласно классификации Uptime Institute существуют четыре уровня организации электропитания ЦОДа: Tier I, Tier II, Tier III и Tier IV.

В большинстве случаев строятся системы электропитания, соответствующие уровню Tier II или Tier III (рис. 1 и 2). Сервисное обслуживание частей системы Tier II связано с повышенным риском остановки системы в случае работ на ДГУ или ИБП и требует ее остановки, например, для обслуживания коммутирующего оборудования.

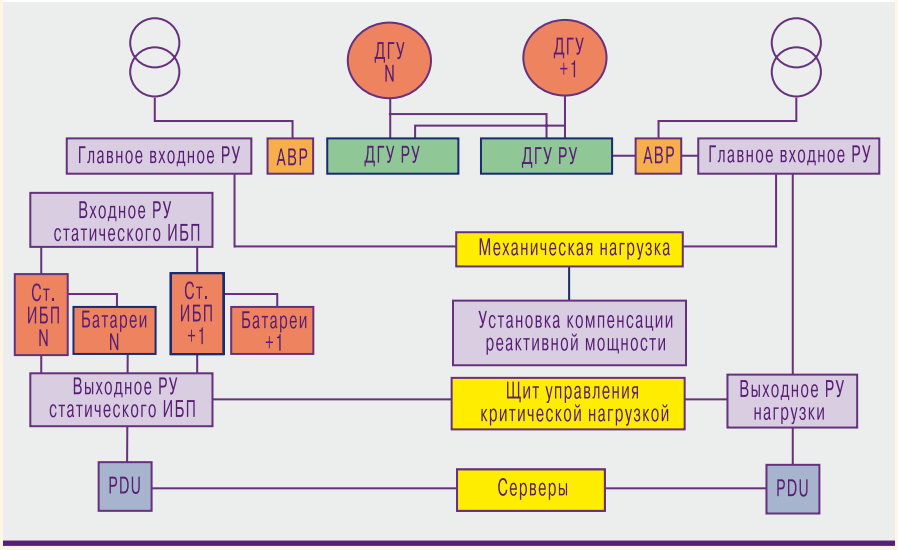
В системах Tier III активные и пассивные компоненты инфраструктуры должны быть зарезервированы, что означает наличие как основных, так и резервных систем распределения электропитания, охлаждения и т.д.

Tier IV предполагает полное резервирование всех систем, так что в системе нет единой точки отказа. При отказе любого единичного устройства система остается работоспособной. Любые эксплуатационно-ремонтные работы можно проводить без остановки серверов. В мире всего несколько систем имеют такой уровень отказоустойчивости.

Используя в крупных ЦОДах мощностью более 1–2 МВт дизельные динамические ИБП, можно существенно упростить и удешевить систему электропитания (рис. 3) и перейти от «базового» уровня готовности системы электропитания к отказоустойчивому.

Поскольку система бесперебойного питания нечувствительна к характеру подключаемой нагрузки, применение ДДИБП позволяет перевести на бесперебойное питание системы, которые обычно необходимо питать только от гарантированного источника. Благодаря этому существенно снижаются риски невосстановления систем после отключения питания, упрощаются системы коммута-

Рис. 2. Система электропитания Tier III

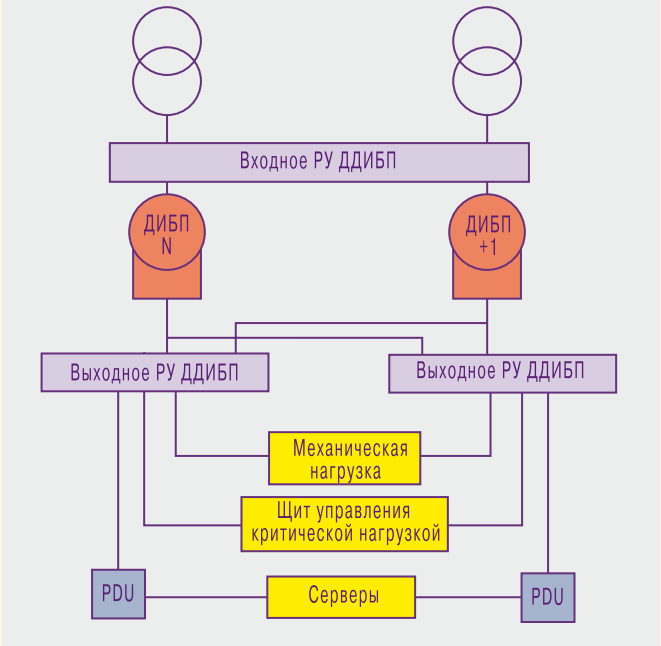


ции, становится возможным отказ от систем плавного ввода нагрузки. Кроме того, ДДИБП, обеспечивая бесперебойное питание системы кондиционирования, значительно упрощают и удешевляют ее резервирование.

Один из примеров использования ДДИБП в ЦОДе – проект компании КРОК на основе технологий HITEC Power Protection. В проекте была реализована полностью автономная по лучам схема подключения конечной нагрузки (см. рис. 3). Такая схема дает возможность выполнять любые эксплуатационно-ремонтные работы без отключения нагрузки.

Применение ДДИБП позволило максимально эффективно использовать пространство, выделенное под ЦОД, – почти на 40% уменьшилась площадь, занимаемая системой электроснабжения, благодаря чему удалось разместить дополнительные серверные стойки. ДДИБП

Рис. 3. Система электроснабжения с использованием ДДИБП уровня Tier III



компании HITEC Power Protection имеют ряд конструктивных особенностей, которые значительно повышают отказоустойчивость системы. Это резервирование системы запуска дизелей, максимально простая система подачи горючего (самотеком) и запуск дизелей на «холостом ходу» с подключением к генератору только после его выхода на рабочие обороты.

Система электропитания с ДДИБП намного энергоэффективнее комплекса «статический ИБП + ДГУ». Реальный КПД ДДИБП в данном проекте при 50%-ной нагрузке составляет 93%, что практически недостижимо для традиционного комплекса «статический ИБП + ДГУ». При более высоких мощностях агрегатов КПД может достигать 98%. Кроме того, ДДИБП не нуждаются в системе кондиционирования, требуемой для ИБП с аккумуляторными батареями, как и в системе подогрева дизелей, необходимой для ДГУ: обогрев происходит за счет естественного нагрева обмоток, т.е. «потерь» генератора, который работает постоянно. Все идет в дело, снижая энергозатраты «на собственные нужды».

Следует отметить, что системы электропитания на основе ДДИБП экономически выгодно использовать при мощностях от 1 МВт и выше. При мощностях 0,5–1 МВт ДДИБП целесообразно устанавливать только при необходимости обеспечить высокую готовность систем электропитания. При мощностях ниже 0,5 МВт начальные капитальные вложения неоправданно высоки и практически не окупаются в процессе эксплуатации.

Оптимизация систем сигнализации, мониторинга, СКС и телекоммуникации

Системы сигнализации, мониторинга, СКС и телекоммуникации на энергопотребление ЦОДов влияют незначительно, но при их оптимизации можно снизить энергопотребление на 1–3% и тем сэкономить на эксплуатации мощных ЦОДов миллионы рублей.

Например, переход в ЦОДах с одномодовых оптоволоконных систем на многомодовые при оптимальном проектировании позволяет намного уменьшить количество электроэнергии, потребляемое активным телекоммуникационным оборудованием. Если учесть, что, например, многомодовые кабели SYSTIMAX компании Commscope, соответствующие стандарту OM-4, несущественно отличаются в цене от кабелей стандарта OM-3, то в крупных ЦОДах суммарная экономия капитальных затрат по сравнению с применением одномодовых систем может достигать 15–20%.

Использование высоконадежных систем мониторинга и управления физическими параметрами производства компании Siemens может значительно уменьшить риски серьезных убытков при возникновении аварийных ситуаций, что сильно снижает затраты на эксплуатацию ЦОДов и ставки страховых премий.

Еще об установках пожаротушения для ЦОДов

Павел ИВАНОВ,
ведущий инженер
ООО «Пожтехника»

В продолжение темы газового пожаротушения – преимущества и недостатки разных видов установок и систем сигнализации.

Централизованная или модульная?

В обсуждении установок газового пожаротушения для ЦОДов, начатом в предыдущей статье*, мы остановились на том, что эти установки подразделяются на централизованные и модульные – по способу хранения газового огнетушащего вещества (см. п. 8.2.1 нового свода правил по системам противопожарной защиты СП 5.13130.2009). Разберем эти понятия более подробно.

В централизованных установках газового пожаротушения баллоны с газом размещены в отдельном помещении станции пожаротушения, они тушат сразу несколько помещений или одно из помещений. Модульные установки пожаротушения состоят из одного или нескольких модулей, объединенных общей системой обнаружения пожара и приведения их в действие. Модули способны самостоятельно выполнять функцию пожаротушения и размещаются в защищаемом помещении или рядом с ним.

Централизованные установки. Теоретически из определения можно сделать вывод, что централизованные установки экономически выгоднее. Если мы выбираем вариант тушения одного из помещений, то алгоритм будет таков: рассчитываем количество огнетушащего газа по большему помещению и подбираем типы модулей так, чтобы одновременно было возможно потушить только одно помещение. При пожаре система пожарной сигнализации определяет, в каком именно помещении произошло возгорание. После этого прибор управления подает сигнал на открытие нужного распределительного устройства и на выпуск нужного количества модулей газового пожаротушения.

В принципе этот вариант должен быть более экономичным, потому что используется меньшее количество газа и соответственно меньше модулей. Но на практике все иначе. Во-первых, потребуется выделить помещение под станцию пожаротушения, которое должно удовлетворять требованиям п. 8.12 свода правил 5.13130.2009. Это определенная высота помещения, расположение, уровни освещенности, телефонная связь с дежурным персоналом, влажность воздуха и т.д. По опыту можно сказать, что найти такое помещение очень трудно. Во-вторых, централизованные установки характеризуются сложной и протяженной системой распределительных трубопроводов. Прокладка такой системы трубопроводов обойдется дороже из-за высокой стоимости монтажа, а в некоторых случаях она вообще невозможна. В-третьих, для централизованных установок пожаротушения придется реализовать сложные алгоритмы управления пожаротушением. Нужно определить, в каком помещении произошло возгорание, запустить соответствующее количество модулей газового пожаротушения, а также открыть определенное распределительное устройство, чтобы газ вышел именно в то помещение, где произошло возгорание. Такой алгоритм можно реализовать только на базе адресно-аналоговой системы пожарной сигнализации, которая в десятки раз дороже обычной безадресной системы. Ну и в четвертых, централизованная установка пожаротушения не сможет потушить одновременно все помещения в случае быстрого распространения огня, если возгорание перейдет на соседние защищаемые помещения.

Из вышесказанного ясно, что централизованные установки пожаротушения из-за сложной системы управления и монтажа не всегда экономически выгодны, а в некоторых случаях (два-три направления тушения) даже дороже модульных. При этом они могут единовременно потушить только одно из защищаемых помещений, что не обеспечит пожарную безопасность объекта в полной мере.

Модульные установки. Эти установки, так называемый классический вариант, рассчитываются под конкретное защищаемое помещение. В каждом помещении или рядом с ним устанавливаются модули с газовым огнетушащим веществом. В модульных установках пожаротушения используются простые алгоритмы работы: нужно определить сигнал «ПОЖАР» и выдать сигнал на запуск модуля с ГОТВ. Эти алгоритмы легко реализуются на отечественных недорогих приборах. А самое главное: каждое помещение, оснащаемое пожаротушением, находится под защитой своей отдельной установки газового пожаротушения, что повышает уровень безопасности объекта.

Компактные установки

Для герметичных шкафов, когда стационарная установка газового пожаротушения не сможет доставить ГОТВ во внутреннее пространство шкафа, существуют компактные установки для пожаротушения стоек. Они полностью автономны и состоят из системы

* См. «Установки пожаротушения для ЦОДов», «ИКС» №6'2011, с. 85.

Масштабируемая адресно-аналоговая пожарная сигнализация ESSER

ESSER

Сетевая система пожарной сигнализации ESSER для защиты магазинов, офисных зданий и промышленных предприятий

ТОВАР СЕРТИФИЦИРОВАН

Серия пожарных панелей IQ8Control C

Особенности системы пожарной сигнализации ESSER:

- Семейство ПКП разной емкости для применения на небольших, средних и крупных объектах;
- Модульная архитектура сигнализации позволяет легко и быстро нарастить систему;
- Возможность объединения до 31 панели в единую сеть essernet;
- Организация интегрированной системы безопасности с помощью ПО WINMAG;
- Максимальная длина кольцевых шлейфов до 3,5 км;
- Интеграция панелей пожаротушения 8010 в кольцевой шлейф esserbus.

Технические характеристики ПКП ESSER:

- К одному ПКП может быть подключено до 40 кольцевых шлейфов esserbus;
- Широкий выбор лицевых панелей управления с отображением информации на русском языке;
- Поддержка беспроводных устройств IQWireless;
- В одном колцевом шлейфе можно объединить:
  - 127 адресных устройств / групп извещателей;
  - 32 транспондера / адресных устройства оповещения серии IQ8Alarm;
  - 48 автоматических извещателей серии IQ8Quad со встроенными устройствами оповещения.

Автоматические извещатели:

- Встроенный изолятор короткого замыкания в каждом извещателе серии IQ8Quad;
- Широкий ассортимент автоматических извещателей (дымовые, термомаксимальные, термодифференциальные, мультисенсорные, со встроенными устройствами оповещения);
- Извещатели для специальных применений (линейные дымовые, линейные тепловые, извещатели открытого пламени, извещатели для взрывоопасных применений, аспирационные извещатели и т.д.)

Транспондеры для подключения периферийных устройств

- Гибкое программирование отдельных входов и выходов транспондеров;
- Большой выбор транспондеров (12 реле, 4 входа/2 реле, 1 вход, коммуника-ционный транспондер, транспондеры для подключения сторонних извещателей и т.д.)

www.armosystems.ru

армо-системы
105066 г. Москва, ул. Спартаковская, д. 11,
Бизнес-центр "Немецкая Слобода", под.2.
Тел.: (495) 787-3342, 937-9057
Факс: (495) 937-9055
e-mail: armosystems@armo.ru
http://www.armosystems.ru

армо-петербург
196084 г. Санкт-Петербург,
ул. М. Митрофаньевская, д. 1, лит.А
Тел.: (812) 303-5353
Факс: (812) 303-5352
e-mail: armo-peterburg@armo.ru
http://www.armospb.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
http://www.armoural.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
http://www.armoural.ru

обнаружения (аспирационный извещатель либо точечные извещатели) и системы тушения – отдельного бокса, монтируемого в 19-дюймовую стойку, или маленького баллона (1–2 л) с огнетушащим веществом. Такие установки эффективны для небольших помещений, когда необходимо защитить лишь несколько стоек, либо для абсолютно герметичных стоек.

Системы сигнализации

В предыдущей статье мы немного коснулись электротехнической части установки газового пожаротушения, в частности аспирационных извещателей. Здесь мы более подробно рассмотрим системы сигнализации, которые используются для управления пожаротушением.

Безадресные системы. Это самые простые, дешевые и наиболее распространенные устройства. Они применяются в основном для управления одним направлением модульного газового пожаротушения (обычно это небольшая серверная или маленький ЦОД).

В пределах одного помещения не столь важно знать адрес сработавшего извещателя. Чаще всего задача оснащения пожаротушением одного или нескольких помещений возникает уже после сдачи в эксплуатацию всего здания (например, компания взяла один этаж в аренду и решила устроить там серверную или архив). В этом случае безадресная система будет оптимальным решением. Учитывая многообразие безадресных извещателей и приборов управления пожаротушением, выбрать такое оборудование совсем нетрудно.

Недостатки систем этого типа:

- низкая информативность (в том числе отсутствие информации о неисправности извещателя);
- необходимость установки двух извещателей на помещение;
- высокая вероятность ложных срабатываний;
- дорогостоящий монтаж и техническое обслуживание;
- ограниченные возможности управления оборудованием пожарной автоматики и т.д.

Адресные системы. Это более совершенные устройства, они позволяют определить не только зону, но и точный адрес сработавшего извещателя. При активации извещатель передает по шлейфу код адреса, который отображается на дисплее приемно-контрольного прибора (ПКП). Однако алгоритмы формирования сигнала «ПОЖАР» в безадресном (пороговом) и простейшем адресном пороговом извещателе одинаковы, что определяет столь же высокую вероятность ложных срабатываний в адресных пороговых системах пожарной сигнализации, как и в традиционных пороговых.

Адресно-аналоговые системы. Такие решения для пожарной сигнализации отличаются хорошо развитыми функциональными возможностями, надежностью и гибкостью. Основное отличие адресно-аналоговых систем от остальных в том, что извещатель сам не принимает решение о пожаре, а только передает информацию о своем состоянии на ПКП.

Принцип работы адресно-аналоговых систем заключается в непрерывном динамическом опросе всех адресных устройств, отслеживающих изменения параметров задымленности, температуры, состояния устройств пожарной автоматики и т.д. ПКП обрабатывает полученные из разных помещений данные, усредняя несколько последовательных результатов, проводит оперативный анализ контролируемых параметров в каждом помещении. Располагая совокупностью результатов измерений, ПКП анализирует их изменения во времени, например, вычисляет производную изменения температуры и таким образом определяет скорость ее роста.

Методы обработки информации, используемые в адресно-аналоговых системах, обеспечивают раннее обнаружение возгорания при отсутствии ложных срабатываний. Все эти преимущества позволяют применять адресно-аналоговые системы для реализации самых сложных алгоритмов управления пожаротушением.

Одно из важнейших преимуществ адресно-аналоговых систем – возможность защиты больших площадей. В зависимости от производителя системы и протокола обмена данными шлейфы могут поддерживать от 99 до 250 адресных устройств. Кроме того, приборы можно объединять в сеть – в большинстве случаев до 99 приборов в одной сети. Итого получаем $99 \times 99 = 9801$ адресное устройство. Такое количество устройств на шлейфе должно обладать высокой живучестью. Этим и объясняется то, что в адресно-аналоговых системах используются кольцевые шлейфы с изоляторами короткого замыкания.

Кроме живучести шлейфов, необходима и живучесть сети приборов. Приборы обмениваются информацией по сети, используя специальный протокол. Неисправность одного или нескольких устройств не окажет воздействия на работу всей системы. Во время короткого замыкания или обрыва между приборами неисправный участок автоматически изолируется, сеть переконфигурируется и передача данных продолжается по другому маршруту.

Возможности адресно-аналоговых систем позволяют эффективно обнаружить возгорание и вовремя среагировать на него. Возвращаясь же к аспирационным извещателям, следует отметить, что на сегодняшний день в адресно-аналоговых системах большинства производителей аспирационные извещатели можно интегрировать в адресно-аналоговый шлейф, без каких-либо дополнительных устройств.

Герметичность помещения

Параметр негерметичности чрезвычайно важен для проектирования эффективной установки газового пожаротушения, тем более для такого помещения, как ЦОД. Однако в настоящее время проектировщики вынуждены применять неточные данные либо выдавать заказчику задание на обеспечение допустимой степени негерметичности защищаемого помещения. В лучшем случае удается измерить крупные отверстия, но это не дает представления о реальной степени негерметичности, что, в свою очередь, приводит к ошиб-

кам при выборе клапанов сброса избыточного давления, а также к ошибкам при расчетах времени удержания необходимой огнетушащей концентрации в защищаемом помещении.

На сегодняшний день существуют установки, позволяющие с высокой точностью определить параметр негерметичности и время, в течение которого будет сохраняться заданная огнетушащая концентрация. Такие установки состоят из калиброванного вентилятора, блока питания, блока обработки данных, комплекта высокоточных датчиков давления и программного обеспечения. С помощью этого оборудования проводятся тесты по нагнетанию и разрежению воздуха в тестируемом помещении. Исходя из проведенных тестов программа вычисляет площадь открытых проемов в помещении с высокой точностью, а также рассчитывает время сохранения огнетушащей концентрации. Калиброванный вентилятор легко монтируется в дверной проем с помощью раздвижных стоек и не требует дополнительных монтажных работ в помещении.

Эта технология уже несколько лет успешно применяется в Европе и США и рекомендована ведущими международными органами по сертификации. С 2011 г. она доступна и в России.

■ ■ ■

В рамках двух статей мы рассмотрели основные принципы построения установок газового пожаротушения для ЦОДов. Как стало ясно, существует несколько видов огнетушащих веществ с разными механизмами тушения, разные типы самих установок, множество систем сигнализации. Можно только призвать читателей быть внимательными при выборе установки газового пожаротушения, ведь из всего многообразия выбора для конкретного ЦОДа всегда найдется оптимальный вариант. ИКС

Как LTE повлияет на инфраструктуру сети и энергопотребление базовых станций

Пол МИСАР, директор по управлению продуктами отдела энергетических систем компании Emerson Network Power

К 2013 г. сети LTE во всем мире, по оценкам Ericsson, будут обслуживать 32,6 млн абонентов. Внедрение этой технологии повлечет за собой переход к сетевой инфраструктуре, включающей большее количество сайтов меньшей площади и с меньшим энергопотреблением, что, в свою очередь, снизит потребности в охлаждении.

Требования к инфраструктуре беспроводной связи непрерывно растут: пользователи хотят передавать и передают по мобильным сетям все увеличивающиеся объемы данных со все более высокой скоростью. Одним из ответов отрасли на эти запросы стала технология Long Term Evolution (LTE), которая обещает обеспечить:

- сетевую архитектуру All-IP;
- эффективное использование спектра в диапазонах частот от 1,4 до 20 МГц;
- возможность дальнейшего использования существующей радиоинфраструктуры и 2G/3G-устройств;
- высокую сетевую безопасность;
- пропускную способность 100 Мбит/с в восходящем потоке и 300 Мбит/с – в нисходящем.

Однако появление LTE заставляет операторов переосмыслить свои стратегии развертывания сетей.

Транспортная сеть отстает от беспроводной

В США в транспортном сегменте беспроводных сетей ранее применялся в основном стандарт T1 (скорость передачи данных 1544 кбит/с. – *Прим. ред.*), и зачастую линии T1 становились самым слабым звеном

сотового узла из-за их низкой надежности. А высокая эффективность LTE в отношении передачи данных означает дальнейшее увеличение нагрузки на транспортную сеть и соответственно требует ее умощнения. Поэтому операторам проводных сетей следует обратить внимание на три аспекта.

- **Стоимость:** Традиционные медные системы T1 не смогут справиться с большими объемами данных, если только не увеличить количество линий на каждом сайте втрое. Вместо того чтобы полагаться на местного проводного оператора, для создания транспортной системы LTE эффективнее будет перейти на оптоволоконные Ethernet-линии или высокоскоростные радиорелейные системы. Это позволит беспроводному оператору обеспечить связь с проводной сетью, повысив надежность и сократив затраты на инфраструктуру.
- **Гибкость:** Сегодняшнее решение для транспортной сети должно быть достаточно гибким, чтобы одновременно поддерживать работу существующей инфраструктуры второго и третьего поколений (GSM, UMTS и CDMA) и справляться с будущими потребностями в транспорте для LTE. Таким решением может стать Ethernet на базе оптоволокна.
- **Надежность:** Транспорт традиционно является самым слабым звеном в сети. И повышение надежности транспортной сети потребует дополнительных расходов. Это заставит владельцев широкополосных сетей объединяться до тех пор, пока не возникнут один-два управляющих сетями крупных игрока и присоединенные к ним более мелкие операторы, продающие современные высокоскоростные услуги. В течение трех-пяти лет возникнет совершенно новая топология, и в недалеком будущем на рынке произойдет революция, которая окажет влияние в том числе и на инфраструктуру сайта.

Изменения в структуре сайта

По мере развития стандарта LTE переход к использованию только сетей передачи данных будет все более полным, голос будет передаваться в формате VoIP. Подход к развертыванию сотовой сети станет более унифицированным в соответствии с принципом «делай больше за меньшие деньги» в отношении линейных сооружений, энергопотребления и планировки площадок. Поставщики инфраструктуры должны будут предложить решения, способные делать это «больше» как на создаваемых вновь сайтах, так и на уже существующих. Сами сайты станут меньше за счет перехода на электронику повышенной плотности, потребляющую меньше энергии.

При развертывании площадок возможны два подхода.

Распределенные антенные системы

Поскольку по мере удаления от антенны скорость передачи данных падает, то чтобы обеспечивать возможность предоставления высокоскоростных услуг, расстояние от узлов беспроводной сети до потребителя должно уменьшаться. Применение распределенных антенных систем (Distributed Antenna System, DAS) подразумевает установку в окрестностях сайта множества антенн, которые поддерживаются подключенным к сети «отелем» (узлом) DAS и создают обширное покрытие. В состав «отеля» DAS входят подвод электроэнергии, выпрямители переменного тока, радиосистемы, волоконный разветвитель и устройство управления, узловые разветвители, электроника и резервное батарейное питание. Такой

Как строить LTE? Есть разные пути

«Большая тройка» американских операторов способна развернуть LTE-сети за счет собственных средств. Менее крупные операторы благодаря действующей в США программе Broadband Initiative имеют доступ к займам под низкие проценты. Это позволит им предоставлять услуги высокоскоростного доступа в Интернет в районах с ограниченным покрытием или полным его отсутствием. Средние региональные операторы второго и третьего эшелона с ограниченными оборотом наличных средств и рентабельностью, для которых доступ к государственному финансированию закрыт, могут сопротивляться решению о модернизации сети до уровня LTE. Такие операторы могут дожидаться, пока не окупятся полностью их вложения в сети 3G, оставив освоение новой технологии и борьбу с высокими ценами более богатым организациям и внимательно следя при этом за развитием ситуации и нарастанием давления со стороны потребителей. Такая стратегия выжидания довольно рискованная. Модернизация на более позднем этапе будет возможна, если конкуренция окажется не слишком острой.

Рис. 1. Использование распределенных антенных систем

«отель» может размещаться в отдельном корпусе или в нескольких небольших наружных шкафах.

Функции традиционных секторных антенн распределяются между несколькими антеннами, запитанными от оптоволоконных линий, которые протягиваются, как правило, вдоль существующих линий коммунальных сетей (рис. 1). Электропитание на каждый антенный узел подается предприятием коммунального хозяйства через точку разграничения ответственности. Для питания электроники узла требуется около 200 Вт постоянного тока, резервные аккумуляторы постоянного тока обычно не нужны.

Сайты с DAS в общем случае способны обеспечить покрытие втрое большее, чем традиционные сайты с тем же количеством несущих. Сайтам с «отелями» DAS не нужны мощные силовые установки постоянного тока и резервные аккумуляторы. Для передачи сигнала по оптоволоконным сетям требуется небольшое усиление или же оно не требуется совсем. В результате энергопотребление и необходимый батарейный резерв таких сайтов вполовину меньше, чем у существующих площадок. Кроме того, они занимают меньшую площадь.

Хотя узловым сайтам с антеннами нужны электропитание постоянного тока, точки разграничения при подаче переменного тока и наружные шкафы, эти потребности меркнут в сравнении с потребностями традиционных сайтов, имеющих аналогичные характеристики. Во многих случаях узел подключается к коммунальным сетям без обеспечения резервного питания постоянного тока (такие конфигурации могут появиться при не слишком высокой значимости передаваемых данных или типов обслуживаемых пользователей).

Выносной радиоблок

Операторы первоначально будут разворачивать системы LTE в рамках существующей инфраструктуры, особенно при наличии радиочастот. Учитывая необходимость масштабируемости и межсетевого взаимодействия, наиболее рентабельным решением является добавление радиосистемы LTE в существующий сайт сотовой сети с использованием уже действующей радиоинфраструктуры (рис. 2).

На практике это можно обеспечить за счет:

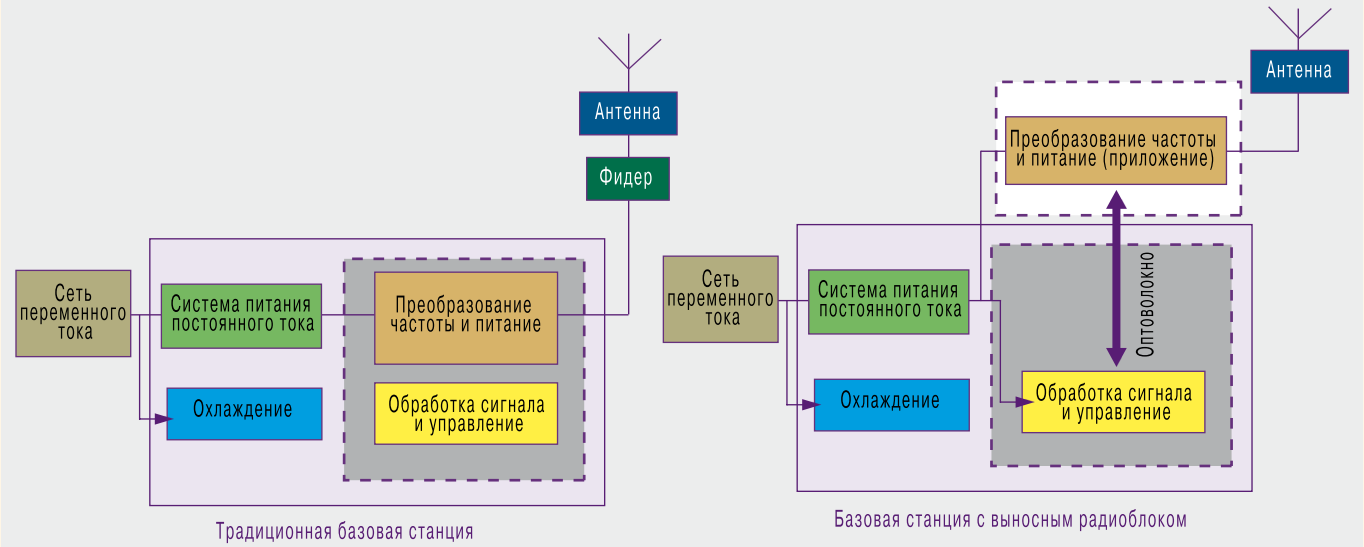
- развертывания радиоблока LTE;
- установки оборудования RXIAT;
- использования существующего электропитания и батарейного резерва постоянного тока (обычно имеются на действующих площадках в избытке).

Добиться на действующих сайтах скоростей, необходимых для поддержки функционирования «цифрового дома», никогда не удастся, если не разместить антенны вблизи абонентов. В конечном счете узловые сайты могут стать решением для эффективного распространения сигнала по сети.

Энергетический фактор

Решающее значение для операторов имеет сокращение затрат на электропитание беспроводных сетей. По

Рис. 2. Выносной радиоблок



некоторым оценкам, на телекоммуникационные сети приходится примерно 1% мирового энергопотребления. С учетом того, что по всему миру установлено более 4 млн сайтов сотовой связи, эффект от сбережения энергии окажется значительным.

Оптимизация сайтов жизненно необходима. До сих пор основное внимание уделялось радиоподсистеме и количеству энергии, уходящей на общее усиление сигнала на каждом сайте. Во многих новых проектах на основных сайтах используются удаленные радиоблоки (Node B). В них антенна и усилитель находятся на верхушке вышки, а у основания размещают радиоблок, источник питания постоянного тока и резервное питание. Благодаря эффективности распространения радиосигнала общая экономия на требуемой мощности постоянного тока, переменного тока и наружном оборудовании может достигать 50% на каждом сайте. Кроме того, оборудование LTE занимает меньшую площадь, что вносит дополнительный вклад в снижение энергопотребления сайта.

Поскольку расход электроэнергии на площадке снижается, то преимущества альтернативных и гибридных источников энергии становятся более привлекательными с финансовой точки зрения. Гибридная система управления позволит использовать возобновляемые источники энергии. Наряду с питанием от электросетей, генераторов или аккумуляторов постоянного тока в качестве стандартного резерва на каждом LTE-сайте могут устанавливаться солнечные, ветряные или топливные элементы электропитания.

Гибридная архитектура позволит снизить потребление сетевой энергии сайтом на 25–30%. Умножив на общее число сайтов, результат получим весьма внушительный. Примечательно, что на территории США сайты, использующие возобновляемые источники энергии, подпадают под 30%-ную льготу по федеральному налогу на электроэнергию, а в нескольких штатах даже предусмотрены налоговые стимулы. Возобновляемые источники энергии, кроме всего прочего, дают операторам преимущества в сфере экологии, которые способствуют их устойчивому развитию.

Сниженное энергопотребление сайта, более широкое использование возобновляемых и гибридных источников энергии делает возможным пакетное комплектование систем для быстрого развертывания, что обеспечивает суммарную экономию за счет масштаба и гибкость. При действующих тарифах на электроэнергию период окупаемости должен составить от трех до пяти лет.

Глобальные изменения

Традиционные сайты сотовых сетей не исчезнут, однако стандарт LTE заставляет операторов переключаться на инновационные методы, расширяя сети и приближая их к абоненту.

Пользователи мобильной связи сегодня все чаще выбирают беспроводные устройства даже там, где доступна проводная сеть. В результате стационарно используемая мобильная широкополосная связь растет стремительными темпами и по мере повышения скорости и эффективности все больше отнимает хлеб у проводных решений. По мнению экспертов отрасли, LTE станет мощным драйвером этого процесса, что подтверждает рост общего числа интеллектуальных мобильных устройств и типов применения данных. Все шире распространяются «интеллектуальные» дома, прибегающие к услугам беспроводных сетей для передачи данных о показаниях счетчиков воды/газа/электричества, для телевидения в формате full HD и предоставления высокоскоростного доступа в Интернет. Для них нужны более высокие скорости и сети, способные их поддерживать. Подобные сценарии использования потребуют более широкого использования распределенных антенных решений и соответственно снижения цены на каждый из компонентов вплоть до уровня ширпотреба.

Возможно, что дни высоких цен на высокие технологии сочтены, и поставщики инфраструктурного оборудования беспроводной связи будут ранжироваться в зависимости от их способности предлагать рентабельные, энергосберегающие, гибкие рыночные решения для сотовых сетей. ИКС

Пора интегрировать СКУД и видеонаблюдение для ЦОДов

Ценность информации, хранимой в ЦОДах, зачастую очень высока, поэтому важное место в их инженерной инфраструктуре отводится системам безопасности – видеонаблюдению и контролю и управлению доступом. Интеграция этих систем служит их взаимному усилению и повышению общего уровня безопасности дата-центра.

Вячеслав ПЕТИН, ведущий эксперт компании «АРМО-Системы»

Михаил МАЛОВ, ведущий эксперт компании «АРМО-Системы»

В чем же основной смысл интеграции? В первую очередь это объединение отдельных подсистем с помощью единого интерфейса, который позволяет пользователю выполнять и мониторинг, и настройку системы в целом из «одного окна». Ведь если компоненты системы автономны, то приходится для каждого из них запускать отдельное приложение, чтобы выполнить настройку, а затем, используя специфический инструментарий (который не факт что найдется!), пытаться «подружить» эти подсистемы между собой.

Достоинство интеграции также в том, что во взаимосвязанных подсистемах в ответ на событие в одной из них происходит соответствующее действие в другой. При этом можно задать любые пользовательские сценарии реагирования на различные события. Кроме того, интегрированные системы безопасности (ИСБ) обладают своего рода интеллектом, который позволяет выявить потенциально опасные ситуации и привлечь к ним внимание оператора, повышая тем самым эффективность защиты и минимизируя влияние человеческого фактора. Одним словом, интеграция – качественный скачок в построении систем безопасности.

По своему назначению дата-центры делятся на корпоративные и коммерческие. В первом случае ЦОД, как правило, не является самостоятельным объектом, а существует в окружении офисных, складских и других помещений, а возможно, и в рамках территориально распределенной корпорации. Здесь при выборе систем защиты дата-центра логично учитывать нужды компании в целом и планировать ИСБ в едином ключе. Во втором случае необходимо предусмотреть потенциальный рост дата-центра и еще на этапе проектирования заложить возможность масштабирования системы безопасности.

Сегодня на рынке интегрированных систем безопасности работает много производителей и представлен широкий спектр решений. Наиболее популярные решения разработаны компаниями Cisco, Lenel Systems International и Bosch Security Systems.

Как интегрирует Cisco

Комплексное решение Cisco для обеспечения безопасности ЦОДов (рис. 1) привлекательно, как минимум, по трем причинам. Во-первых, под этим брендом выпускается широкий ассортимент оборудования, в том числе для оснащения дата-центра и служебных помещений «под ключ». Во-вторых, решение соответствует специфическим требованиям этого ответственного объекта, где данные, по сути, дороже, чем оборудование, на котором они

Рис. 1. Концепция комплексной системы Cisco для обеспечения безопасности ЦОДов

хранятся. В-третьих, производитель оказывает всестороннюю сервисную поддержку.

При объединении в единый комплекс систем видеонаблюдения и контроля доступа на базе устройств и ПО компании Cisco создается масштабируемая, настраиваемая и простая в управлении система, обеспечивающая контроль состояния всех компонентов дата-центра в реальном времени (в состав системы войдут камеры наблюдения разных типов, видеосерверы, коммутаторы, маршрутизаторы, серверное и периферийное оборудование контроля доступа, в частности биометрические и RFID-считыватели, замки и т.д., а также соответствующие программные модули Cisco).

Система безопасности может базироваться на системе контроля и управления доступом (СКУД) Cisco – масштабируемом программно-аппаратном комплексе, не имеющем ограничений по числу владельцев карт доступа, пользователей и операторов системы и способном обращаться в процессе работы к базам данных различных служб. Для управления СКУД используется ПО Physical Access Manager (PAM), средствами которого выполняется конфигурирование контроллеров, мониторинг системы и ее интеграция с другими ИТ-приложениями.

Основные компоненты системы контроля и управления доступом Cisco – это контроллеры, модули считывателей (снабженные Wiegand-портом для подключения до двух считывателей), модули входов для подсоединения к системе кнопок выхода, охранных датчиков и т.п., модули выходов для управления исполнительными устройствами (замками, воротами, шлагбаумами и др.). Все модули СКУД подключаются к контроллеру Physical Access Gateway по локальной сети контроллеров (Controller Area Network, CAN), а повышенная сохранность информации достигается за счет того, что база данных дублируется на контроллере (в случае обрыва сетевого соединения он сохраняет все изменения и после восстановления связи передает их на основной сервер с PAM).

Другая составляющая интегрированного решения Cisco – охранная видеосистема под управлением ПО Video Surveillance Manager, в состав которой могут входить IP-камеры и различные IP-устройства Cisco и других производителей. Комбинируя программные модули VSM, можно построить масштабируемую систему с возможностями просмотра многопотокового видео, управления PTZ-функциями (перемещение, наклон, зум) поворотных камер, хранения, поиска и управления видеоинформацией. Система работает под управлением ОС Linux, которая мало подвержена зависаниям и вирусным атакам.

Через интерфейс VSM возможна индивидуальная настройка параметров каждой из камер наблюдения, создание интерактивных графических планов объекта с добавлением фотографий и графиков, отображением расположения камер и др., доступ к видео в режиме реального времени или в записи с ПК, КПК и мобильных устройств, включая iPhone. Кроме того, система позволяет применять различные отказоустойчивые опции записи и хранения данных с целью их восстановления в случае любых сбоев.

Следует отметить, что путем выбора базовых и дополнительных компонентов VSM функционал видеосистемы может наращиваться практически неограниченно. В качестве ядра ПО Cisco используется модуль Media Server, обеспечивающий сбор и хранение видеоданных, а для удаленного конфигурирования оборудования и интеграции в системные приложения предусмотрен модуль Operations Manager. Программные модули могут поставляться как автономное ПО или интегрированными в один из аппаратных компонентов решения Cisco, например в VS Encoding Server, предназначенный для кодирования, распространения, управления и архивации видеоинформации, в том числе во внешних хранилищах – DAS, NAS, SAN.

Функционал фирменного ПО реализован с применением стандартных сетевых протоколов, поэтому в состав интегрированной системы Cisco может входить оборудование сторонних производителей: как для видеонаблюдения, например камеры AXIS, Bosch, Sanyo, Sony, Panasonic, так и для контроля доступа, в частности периферийные устройства марок HID, Gianni, Smartec, ZK Software и др.

Потенциал системы Cisco может быть существенно расширен за счет интеграции с приложениями других систем, например, производства Lenel. Уже сегодня ПО Lenel для управления системой контроля доступа поддерживает IP-камеры Cisco, а в ближайшей перспективе ПО VSM будет поддерживать устройства СКУД Lenel.

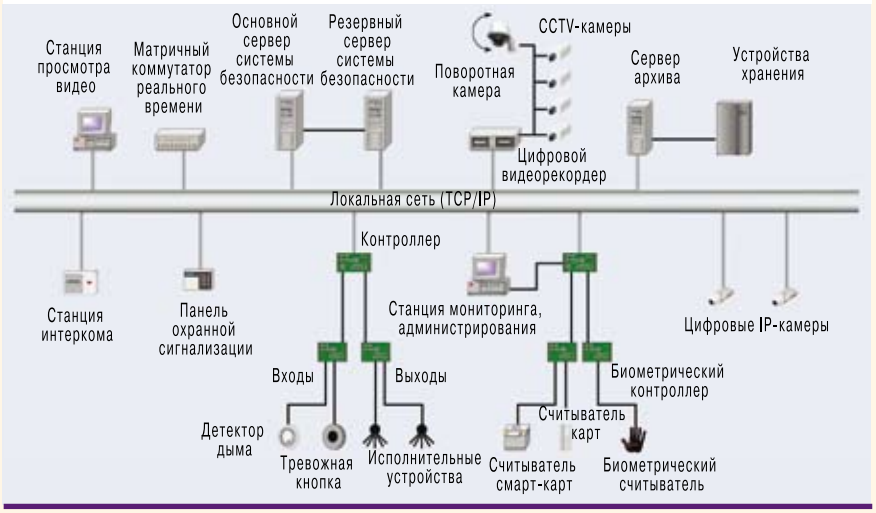
ИСБ для ЦОДа, версия Lenel

Главная особенность системы безопасности Lenel (рис. 2) – то, что она изначально формировалась как интегрированная, т.е. под фирменные контроллеры и устройства создавалась программная оболочка. С точки зрения интеграции она является наиболее проработанной из всех существующих на рынке, так как обладает широчайшим инструментарием в виде программных интерфейсов (API, OPC, SNMP и др.).

Платформа Lenel OnGuard модульная, и заказчик может сам решать, какие из системных модулей ему необходимы в данный момент, какие можно докупить позже, а от чего можно вообще отказаться. При создании ИСБ Lenel был использован иерархический принцип с возможностью выделения уровня интеграции (серверы, рабочие станции), уровня сетевых мастер-контроллеров и уровня исполнительных (полевых) контроллеров и устройств.

Модуль OnGuard Access предназначен для контроля и управления доступом в помещения или здания любого размера. Эта система может работать как в небольшом офисе всего с двумя считывателями, так и на крупных предприятиях с тысячами считывателей и с многочисленными офисами, распределенными по всему миру, что становится актуальным, когда ЦОД является частью глобальной корпорации. При этом расширение системы происходит без замены уже установленного оборудования и без переустановки программного обеспечения. Необходи-

Рис. 2. Принципиальная схема ИСБ Lenel



мо лишь докупить лицензии на вспомогательные опции и приобрести дополнительные контроллеры, модули и серверы.

Кроме того, СКУД Lenel лишена такого недостатка, как увеличение времени обработки транзакций при росте масштаба системы. Она может обслуживать неограниченное число считывателей, точек прохода (дверей, турникетов, шлагбаумов), карт доступа и стабильно функционирует при одновременной обработке большого числа транзакций.

В случае интеграции системы видеонаблюдения и СКУД, выполненной с использованием оборудования и ПО Lenel, оператор имеет возможность в одном окне мониторинга наблюдать состояние устройств контроля доступа и просматривать видео, поступающее с разных камер. Как и другие ИСБ, систему Lenel можно настроить так, что при возникновении тревожного события в СКУД на операторском экране будут всплывать окна, транслирующие изображение с конкретных видеокамер.

В этом плане платформа Lenel предоставляет интересную возможность: во всплывающем окне можно выводить сразу два потока изображений с одной и той же камеры, причем на одном из них будет отображаться «живое» видео, а на другом – события, которые происходили за некоторое время до возникновения тревоги. Таким образом, оператор сможет объективно оценить ситуацию, увидеть, как в действительности развивались события, и выбрать соответствующий способ реагирования.

До недавнего времени в ИСБ Lenel использовалась исключительно система видеонаблюдения

Интеграция видеонаблюдения и СКУД – чем теснее, тем лучше

Олег СУХОВ,
ведущий специалист по системам технической безопасности компании «Информсвязь»

Интеграция систем безопасности в центрах обработки данных, как, впрочем, и на других ответственных объектах, призвана повысить эффективность мониторинга с помощью запрограммированной реакции одной системы на событие, произошедшее в смежной. Таким образом, часть функций, ранее требовавших непременного участия оператора или администратора системы, начинает выполняться автоматически.

Системы видеонаблюдения (в том числе аналогового) уже давно способны с помощью реле и сухих контактов, которыми оборудуется большинство камер, принимать тревожные сигналы и передавать управляющие сигналы в другие системы. Например, при взломе двери контроллер СКУД генерирует сигнал, поступающий на тревожный вход камеры, изображение с ближайшей к месту события камеры принудительно выводится на монитор оператора, включается архивация видеоизображения и т.д.

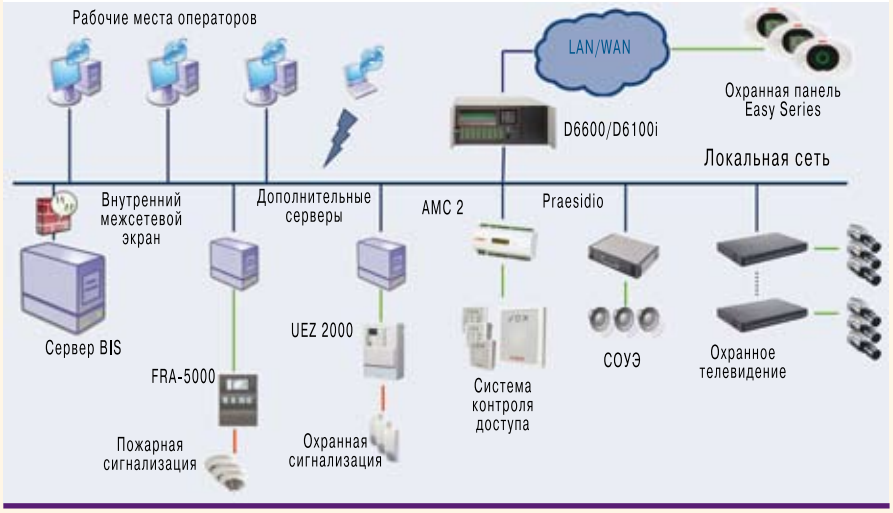
В современных системах широко используется интеграция на программном уровне, когда вся информация от периферийных устройств поступает в центральное оборудование, где она обрабатывается и формируется та или иная реакция на событие. Такие решения позволяют сделать взаимодействие интегрируемых подсистем более тесным и создавать более развернутые сценарии их совместной работы.

На сложных высокотехнологичных объектах, к коим относятся и ЦОДы, возникает необходимость интеграции не только систем видеонаблюдения и контроля и управления доступом, но и систем пожарной безопасности и других систем жизнеобеспечения. Системы видеонаблюдения, как самые информативные, должны обеспечивать оперативный контроль за любой нештатной ситуацией, а система контроля доступа, например, при пожаре должна разблокировать все выходы для беспрепятственной эвакуации персонала.

Важный аспект интеграции – наличие единого эргономичного интерфейса мониторинга безопасности объекта, который должен быть удобен прежде всего для оператора и служб реагирования.

Одно из самых современных решений в области интеграции – SCADA-система, объединяющая на верхнем уровне в единый контур функционирования все инженерные системы и системы безопасности. С ее помощью дежурный оператор на автоматизированном рабочем месте в зависимости от полномочий может проводить мониторинг и посылать управляющие команды, обеспечивая жизнедеятельность ЦОДа в целом. Внедрением таких систем сегодня занимаются крупнейшие инжиниринговые компании и системные интеграторы.

Рис. 3. Структура ИСБ Bosch



LNVR этой же марки. На данный момент в платформу OnGuard интегрирована также видеосистема SkyPoint, имеющая хорошо развитое ядро от компании Milestone и «продвинутый» интерфейс, который создан с учетом человеческой психологии специалистами фирмы OnSSI. Помимо обычного варианта работы с компьютерной мышью, существует модификация данного интерфейса для устройств с сенсорными экранами. Использование в качестве ядра в видеосистеме Lenel продукта Milestone позволяет ей поддерживать работу камер, видеоэнкодеров и IP-устройств практически всех известных производителей.

Интеграция с точки зрения Bosch

Еще одним примером интеграции систем безопасности является Building Integration System (BIS) компании Bosch Security Systems (рис. 3). Так же, как ИСБ Lenel, BIS имеет иерархическую структуру и модульный характер, что позволяет добавлять или удалять отдельные элементы системы, создавая различные их комбинации. Однако, в отличие от платформы Lenel, BIS создавались для интеграции нескольких решений одного производителя, которые вполне могут функционировать и вне рамок интегрирующей среды, и сделано это для придания комплексности и связанности системам, исторически появившимся в разное время.

Поскольку BIS имеет модульную архитектуру, то заказчик всегда платит лишь за те функции, которые ему нужны в данный момент. Ядром системы является базовый пакет BIS, который должен приобретаться для каждого нового проекта. В комплекте с базовым пакетом поставляется USB-ключ защиты и файл с основной лицензией, где содержатся уникальные данные для конкретного проекта, одна лицензия оператора и одна лицензия на OPC-интеграцию.

Базовый пакет обеспечивает центральное управление и мониторинг всех подключаемых систем. Также он содержит инструментарий конфигурирования с большой библиотекой готовых значков и шаблонов и осуществляет централизованное протоколирование всех поступающих тревог и событий от подсистем. Рассмотрим возможности модулей BIS для видеонаблюдения и контроля доступа.

Подсистема видеонаблюдения (Video Engine) поддерживает различное оборудование IP-CCTV производства Bosch, а также IP-камеры сторонних производителей. Основной пакет этой подсистемы изначально содержит по одной лицензии на подключение регистратора DiBos или Divar и кодера серий Videojet или VIP. При необходимости возможно наращивание количества регистраторов, кодеров или IP-камер с шагом единица с помощью соответствующих лицензий. Также существует отдельная лицензия для управления поворотными камерами с помощью USB-клавиатуры.

Подсистема контроля доступа (Access Engine) добавляет в BIS все необходимые функции для контроля и управления доступом. Данный модуль включает в себя большое количество предварительно сконфигурированных шаблонов моделей дверей (стандартная односторонняя/двухсторонняя дверь, лифт, турникет и т.д.), что значительно упрощает конфигурирование новой системы. Модуль Access Engine может работать с контроллерами СКУД серии AMC. Основной пакет контроля доступа (Access Engine) позволяет организовать систему контроля доступа, состоящую из 32 точек прохода и рассчитанную на 100 пользователей и 50 посетителей. При необходимости система может быть расширена дополнительными опциями, включая управление парковкой, видеоверификацию и др. Наращивание числа точек прохода можно производить опционально с шагом 32, владельцев карт – с шагом 100 или 1000, посетителей – с шагом 50 или 100.

■ ■ ■

Все рассмотренные примеры ИСБ имеют необходимый набор функций для надежной защиты ЦОДов, и на базе каждой из них можно создать гибкое масштабируемое решение. Основные различия между этими системами начинаются тогда, когда мы выходим за рамки датацентра. Если ИСБ Cisco хороша и самодостаточна именно для ЦОДа, то решение Lenel способно удовлетворить нужды крупных корпораций, где центр обработки данных является лишь одним из подразделений компании. Установка интегрированной системы Bosch будет отличным решением в случаях, когда на объекте уже имеются некоторые подсистемы этого производителя. Таким образом, окончательный выбор марки ИСБ зависит от конкретных условий на оснащаемом объекте и от необходимости вписаться в существующий контекст уже установленных систем безопасности. ИКС

Испытания оптической проводки в ЦОДах

Стандартные методики и воспроизводимость измерений

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

В волоконно-оптических сетях передачи данных оценка величины бюджета потерь в линии требует итоговых сертификационных испытаний. Точность и воспроизводимость таких измерений особенно важны для случаев, когда протяженность спроектированной СКС приближается к предельным значениям для выбранной производительности системы и соответствующей технологии передачи данных.

Подразумевается, что необходимость проведения сертификационных испытаний стационарных линий (а в некоторых случаях и каналов) и те преимущества, которые получает от этого пользователь, очевидны для профессионального сообщества, поэтому мы не будем их рассматривать. Основная цель данной публикации – обзор существующих методик испытаний и рекомендаций стандартов для оптических СКС, а также особенностей и ограничений, накладываемых волноводной структурой волокна, пассивными оптическими компонентами, источниками и приемниками излучения в составе применяемого измерительного оборудования.

В первой статье серии мы кратко обсудим состав сертификационных испытаний согласно рекомендациям стандартов и рассмотрим особенности ввода, возбуждения и распространения излучения по многомодовому волокну.

Рекомендации стандартов

Состав и периодичность испытаний оптической проводки указаны в стандарте ISO/IEC 14763-3, который определяет способы подтверждения соответствия параметров сертифицируемой СКС требованиям стандарта ISO/IEC 11801. В общем случае любая оптическая линия должна быть протестирована согласно принятому плану испытаний при помощи измерителя мощности с соответствующим типом источника излучения или рефлектометрическими методами на соответствующей центральной длине волны. Второй метод выступает как дополнительный, и его рекомендуется использовать для идентификации, локализации и поиска способа устранения неисправности в оптической линии.

Для сертификационных испытаний может быть принята одно- или двухуровневая модель (рассматриваемая в данной статье), которая определяет обязательные и дополнительные виды испытаний (табл. 1).

Таким образом, основным и обязательным способом подтверждения работоспособности оптической проводки и ее соответствия требованиям является измерение затухания в терминах либо стационарной линии, либо канала.

Здесь уместен вопрос о том, насколько получаемые результаты измерения достоверны и воспроизводимы в реальных условиях. Не секрет, что при использовании одного и того же измерителя мощности при испытании линии получают разные результаты, порой отличающиеся на 0,5 дБ и более. В чем причина?

Современные измерители мощности ведущих мировых производителей представляют собой автоматизированные комплексные системы, выполняющие измерение и обработку результатов по единому алгоритму. Причина расхождений результатов кроется в непостоянстве условий, при которых проводятся последовательные измерения. В первую очередь необходимо учитывать особенности волноводной структуры волокна, особенности ввода и распространения света.

Оптическое волокно

На практике в большинстве случаев в составе оптической СКС используются многомодовые волокна различных категорий с градиентным профилем показате-

Табл. 1. Виды испытаний оптической проводки

Испытания	Статус*	Прибор **
Основные		
Затухание излучения в оптическом тракте	N	С одной стороны
Целостность оптического волокна	N	С одной стороны
Соблюдение полярности	N	С одной стороны
Дополнительные		
Затухание излучения в оптическом тракте	N	С двух сторон
Оптическая длина волокна	I	С двух сторон
Целостность оптического волокна	N	С двух сторон
Обратные потери	I	С двух сторон

* N (normative) – обязательные испытания; I (informative) – дополнительные испытания.
** Измеритель мощности для основных испытаний, рефлектометр – для дополнительных

ля преломления. Анализ распространения света в сердцевине волокна подразумевает сложный математический аппарат и в большинстве случаев основан на приближенных решениях волновых уравнений, не всегда имеющих аналитические решения в явном виде. Чтобы упростить обсуждение, заменим реальные пространственные конфигурации полей лучевыми траекториями и введем следующие допущения:

- лучи образуют малые углы с продольной осью волокна (параксиальное приближение);
- волокна являются слабонаправляющими волноводами (малая разница между максимальным значением показателя преломления на оси сердцевины и значением показателя оптической оболочки волокна).

В общем случае в многомодовом волокне распространяется множество направляемых (удерживаемых сердцевиной) лучей, каждый из которых представляет собой дискретное решение дисперсионного уравнения и называется модой. Количество таких мод (модовый объем) зависит от конструктивных особенностей сердцевины волокна, профиля показателя преломления в сердцевине и длины волны излучения. Важно, что каждая мода (луч) распространяется под своим углом относительно продольной оси световода (рис. 1) и с различными постоянными распространения вдоль волокна. Группы мод, которые распространяются вблизи центра сердцевины (малые углы), называются модами низших порядков, а группы мод с большими углами относятся к модам высших порядков.

Очевидно, что распределение мощности излучения, переносимой каждой модой, будет определяться условиями ввода излучения от источника в сердцевину волокна. Возбужденные моды высших порядков, которые распространяются в непосредственной близости от границы раздела сердцевина – оболочка или даже частично в оптической оболочке, будут испытывать большее затухание на неоднородностях (оптические соединители, изгибы) в тракте, что приведет к высокому значению потерь в линии по результатам испытаний. Таким образом, условия ввода излучения в сердцевину волокна оказывают непосредственное влияние на результаты испытаний.

Рис. 1. Кусочно-линейная аппроксимация траектории луча в многомодовом волокне с градиентным профилем преломления

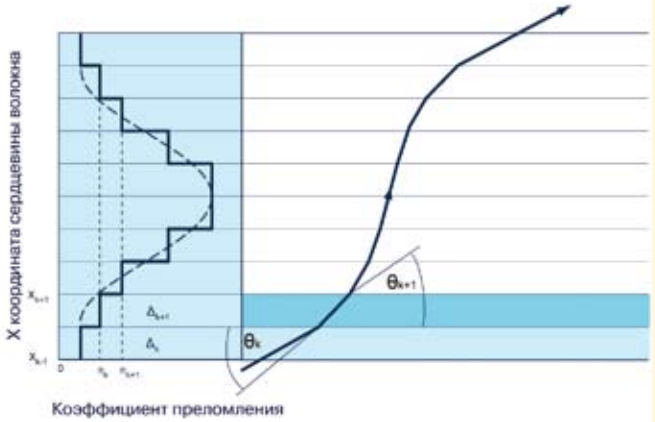
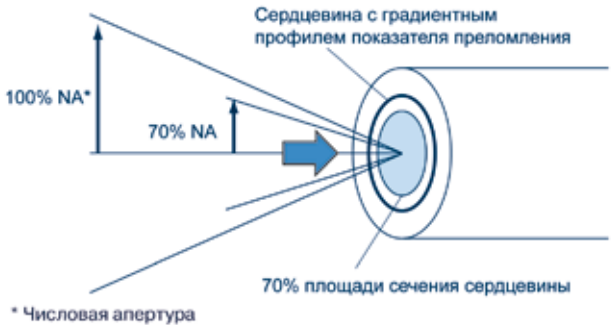


Рис. 2. Определение числовой апертуры и диаметра пучка



Условия ввода излучения

При падении электромагнитной волны на торец волокна не все направляемые моды сердцевины возбуждаются одинаково. Поэтому условия ввода определяют, как и в какой степени будут возбуждены группы мод низшего и высшего порядков. На практике для описания условий ввода используют два параметра: диаметр пятна и числовую апертуру (NA) светового пучка*. Если условия ввода таковы, что диаметр пучка превосходит соответствующее значение диаметра пятна моды сердцевины и (или) значение числовой апертуры, то можно говорить об условии ввода с переполнением сердцевины. В том случае, когда диаметр пучка и (или) числовая апертура равны 70% или менее соответствующих значений для самого волокна, принято говорить об ограниченном условии ввода (рис. 2).

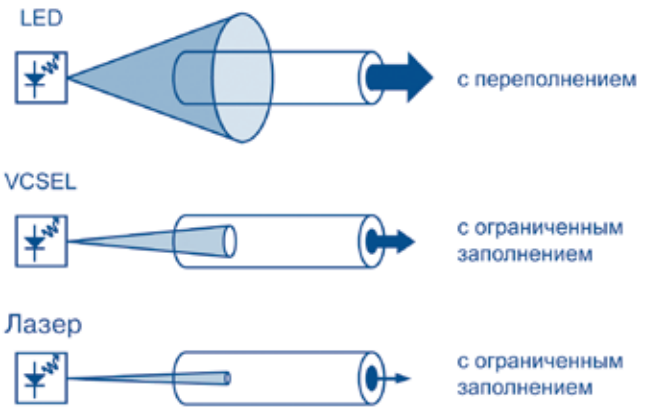
Очевидно, что тип используемого источника в общем случае будет определять и условия ввода излучения в сердцевину волокна. Для полупроводникового лазерного источника ожидаемое условие ввода будет ограниченным из-за малых значений пространственной ширины пучка и угла расхождения. В противном случае использование светодиода в качестве источника приведет к переполнению сердцевины, так как ширина пучка может на несколько порядков превосходить значение диаметра пятна моды сердцевины волокна.

Как видно из рис. 3, при использовании светодиода (LED) вся торцевая поверхность сердцевины волокна равномерно засвечивается, и значительный объем вводимой мощности будет переноситься группами мод высших порядков. В этом случае результаты измерения затухания в тракте будут завышенными.

Особый интерес представляет полупроводниковый источник VCSEL, который сегодня используется в большинстве оптических трансиверов для передачи данных на короткие расстояния. Имея достаточно малую ширину пучка излучения, такой источник засвечивает лишь небольшую часть торцевой поверхности волокна, поэтому лишь часть из возможных модовых групп будет возбуждена в сердцевине. Здесь необходимо от-

* Определения указанных понятий и соответствующие методики оценки приводятся в целом ряде стандартов, например IEC 60793-1-45, IEC 60793-1-43.

Рис. 3. Сравнение ширины светового пучка с диаметром пятна сердцевины волокна определяет условие ввода



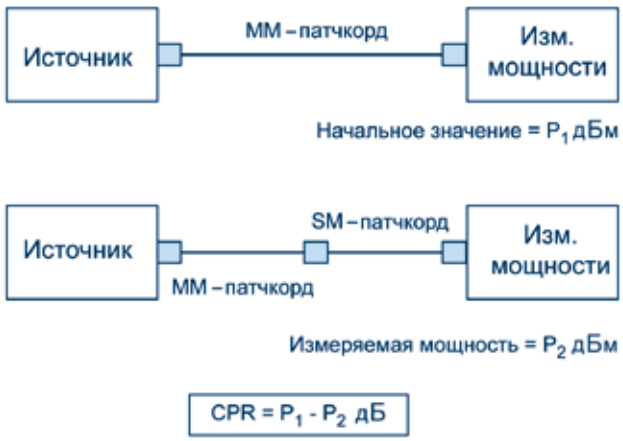
метить, что вероятность возбуждения мод низших или высших порядков зависит от места на торце волокна, на которое падает пучок. Принимая во внимание малые, в общем случае, значения осевого смещения пучка относительно центра сердцевины, можно говорить о том, что большая часть мощности излучения будет переноситься модами низших порядков вблизи оси сердцевины. Таким образом, результаты измерений затухания в тракте при ограниченном условии ввода излучения могут оказаться излишне оптимистичными и не отражать реального положения вещей.

Из сказанного выше следует важный вывод: требования по контролю условий ввода излучения в процессе измерений должны быть неотъемлемой частью регламента проведения сертификационных испытаний.

Контроль условий ввода

На первый взгляд, критерий 70/70 (рис. 2), о котором шла речь выше, представляет собой удобное мнемоническое правило определения условий ограниченного ввода излучения или ввода с переполнением. Однако вне лаборатории обеспечить точность измерения геометрических параметров волокна и светового пучка практически невозможно. Поэтому указанный способ не вошел в существующие редакции стандартов методик тестирования СКС.

Рис. 4. Схема измерения коэффициента CPR



Коэффициент CPR. Второй способ определения условий ввода излучения основан на параметре CPR (coupled-power ratio), который позволяет оценить распределение мощности по сечению сердцевины волокна и, соответственно, между различными группами направляемых мод (рис. 4). Методика измерения детально описана в стандарте IEC 61300-3-31.

Очевидно, что большие значения CPR говорят о том, что основная часть мощности переносится модами высших порядков (значительное переполнение сердцевины), поскольку на стыке многомодового и одномодового волокон будут зафиксированы большие потери. Данная методика является удобным и доступным способом контроля ввода при проведении измерений затухания в оптическом тракте. Рекомендуемые значения CPR определены, например, в стандарте TIA/EIA-526-14A (для справки они приведены в табл. 2).

Табл. 2. Рекомендуемые значения CPR

Тип волокна	CPR@850нм (дБ), кат. источника 1-3	CPR@850нм (дБ), кат. источника 4-5
Многомодовое 50/125 с градиентным профилем	11–24	0–10,9 дБ
Многомодовое 62,5/125 с градиентным профилем	14–29	0–13,9 дБ

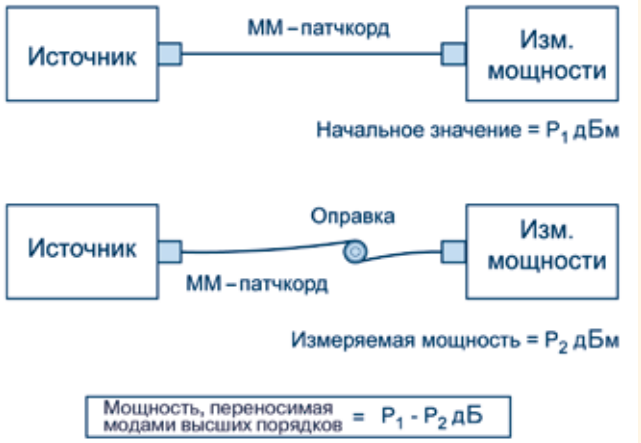
Модовый фильтр. В дополнение к измерению параметра CPR рекомендуется провести измерения, используя модовый фильтр – оправку с несколькими витками измерительного патчкорда. Очевидно, что слабосвязанные направляемые моды высших порядков становятся излучаемыми, как только возникает многократный макроизгиб волокна и нарушается условие полного внутреннего отражения на границе раздела сердцевина – оболочка. Таким образом, проведение последовательных измерений без модового фильтра и с ним позволяет оценить долю мощности, которая переносится слабосвязанными модами (рис. 5).

Для лазерного полупроводникового источника использование модового фильтра несущественно скажется на итоговых результатах измерений. Однако для светодиода наблюдаемые малые изменения могут означать низкое качество источника категорий 1–3 или плохую юстировку источника относительно волокна.

Использование оправки в общем случае позволяет снизить влияние «переходных» потерь, т.е. дополнительного прироста затухания в неустановившемся режиме. В этом случае прирост затухания на рассматриваемом составном оптическом тракте (в реальных условиях) может достигать 0,5–1,0 дБ в сравнении с затуханием на каждом отдельно взятом участке тракта, который тестируется в условиях ввода излучения с переполнением сердцевины.

Диаметр оправки и количество полных витков влияет на количество модовых групп, которые успешно излучаются за пределы сердцевины (переход от высших порядков в сторону низших порядков). Практика показывает,

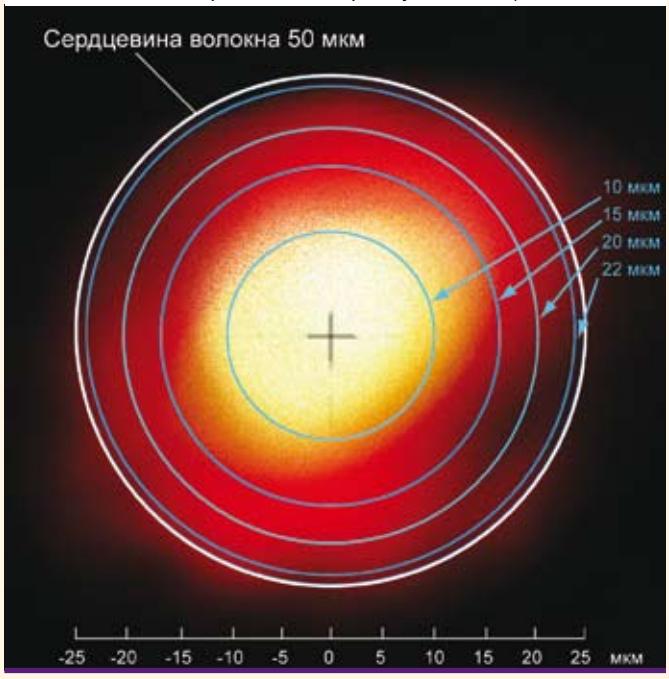
Рис. 5. Схема измерения (оценки) доли мощности, переносимой модами высших порядков



что при числе полных витков свыше 3–5 дополнительный прирост потерь незначителен. С физической точки зрения диаметр оправки влияет на силу преобразования направляемых мод в излучаемые из общего модового объема сердцевины. Кроме того, необходимо отметить, что эффективность фильтрации мод имеет спектральную зависимость, что обусловливает разные значения диаметра оправки для разных рабочих длин волн. Так, для многомодового волокна 50/125 с градиентным профилем диаметр оправки (волокно в первичной оболочке, @850 нм) составляет 25 мм, для многомодового волокна 62,5/125 с градиентным профилем – 20 мм. Дополнительная информация представлена в стандарте TIA/EIA-455-34.

При проведении испытаний на объекте обычно используют измерительные шнуры, поэтому необходимо вычесть диаметр наружной оболочки патчкорда, чтобы определить необходимый диаметр оправки.

Рис. 6. Ограничение нормированного потока мощности для четырех значений радиуса, ММ 50/125 @850 нм



Унификация условий измерения

Из приведенных выше рассуждений становится понятно, что ни один способ контроля условий возбуждения световода не гарантирует воспроизводимости результатов измерений. Здесь стоит заметить, что при достаточном запасе бюджета потерь в линии вариация результатов не играет заметной роли. Однако в случае высокоскоростных систем передачи с малым допустимым бюджетом потерь (например, 16G Fibre Channel) расхождение в результатах измерений, например в 30%, может стать принципиально важным.

В 2009 г. был утвержден стандарт IEC 61280-4-1, в котором вводится новый параметр Encircled Flux (EF), определяющий распределение интенсивности излучения по поперечному сечению сердцевины волокна. С математической точки зрения он представляет собой относительную величину, поскольку рассчитывается как отношение потока мощности через элемент сечения сердцевины, ограниченный цилиндрической поверхностью с определенным радиусом, к общему потоку мощности через сердцевину. Таким образом, можно говорить о нормированной величине потока.

Табл. 3. Значения параметра EF, задаваемые стандартом IEC 61280-4-1

Волокно 50/125, @ 850 нм		Волокно 62,5/125, @ 850 нм	
Радиус, мкм	EF, номинальное значение	Радиус, мкм	EF, номинальное значение
10	0,3350	10	0,2109
15	0,6550	15	0,4390
20	0,9193	20	0,6923
22	0,9751	22	-
	-	26	0,9350
	-	28	0,9783

Основная цель введения нового критерия, унифицирующего условия возбуждения мод, состояла в том, чтобы исключить необходимость контроля излучения конкретного источника в процессе испытаний линии и определить требования к функции распределения интенсивности излучения на выходе из соединительного шнура от порта источника. Залогом достоверности и воспроизводимости результатов измерений при использовании различных источников является установка референсных точек функции распределения в окрестности границы раздела сердцевина – оболочка (большие значения радиуса сердцевины).

Стандарт определяет четыре референсных значения радиуса, для которых задается значение нормированного потока (табл. 3) через площадь сечения, ограниченного окружностью с этим радиусом (рис. 6).

Таким образом, ограничивая кривую распределения интенсивности, мы повышаем воспроизводимость результатов, так как исключаем или снижаем влияние «переходных» потерь, которые зависят от конкретного типа источника или условий возбуждения.

Продолжение – в следующем номере «ИКС».

Fast Ethernet-коммутатор с поддержкой IPv6

ES3510MA-DC – 8-портовый управляемый Fast Ethernet-коммутатор уровня 2/4 с 2-гигабитными комбо-портами, обладающий энергосберегающими возможностями и функциями управления IPv6.

Коммутационная матрица имеет производительность 5,6 Гбит/с. Два оптических SFP-порта 100BASE-X/1GBASE предназначены для подключения к скоростным серверам или магистралям. Функция IP Clustering дает возможность администраторам использовать единый IP-адрес для управления виртуальным стеком до 36 коммутаторов.

Управление ES3510MA-DC включает поддержку DHCP Option 82, что позволяет присваивать IP-адреса абонентам в зависимости от места подключения к сети. Через CLI (Industry standard Command Line Interface), используя консольный порт или Telnet с единым пользовательским интерфейсом и набором команд, можно управлять коммутатором напрямую.

Функции управления ES3510MA-DC поддерживают как IPv4, так и IPv6. Благодаря технологиям IPv4/IPv6 Dual Protocol, SNMP over IPv6, HTTP over IPv6 и Remote IPv6 Ping коммутатор ES3510MA-DC обеспечивает плавный переход от IPv4 к IPv6.

Интеллектуальные функции QoS помогают оптимизировать сеть и повысить устойчивость передачи данных при нестабильной связи. В ES3510MA-DC реализованы функции L2 и функции безопасности, включая 802.1X аутентификацию, MAC-фильтрацию, Private VLAN, Guest VLAN и Voice VLAN.

Компактные размеры дают возможность устанавливать ES3510MA-DC в условиях ограниченного пространства, например в труднодоступных чердачных или подвальных помещениях.

Безвентиляторное исполнение обеспечивает бесшумную работу, постоянный ток позволяет шире использовать резервирование питания в сети любого размера. Два порта Gigabit Combo поддерживают технологию Green Saving, которая автоматически определяет статус линка и расстояние с целью снижения энергопотребления.

Edge-core Networks:
(916) 625-8272

Уличный оптический кросс

ШРУД-ОВ предназначен для коммутации и сращивания оптических кабелей в условиях улицы для организации сетей FTTx. Кросс позволяет коммутировать 320 или производить сварку 480 оптических волокон. Шкаф устанавливают на чугунную опору высотой 100 мм, которая на месте эксплуатации при помощи анкерных болтов крепится к бетонному основанию (перекрытию колодца). Особенность конструкции кросса – двойной металлический шкаф, выдерживающий различные механические нагрузки. Кроме того, конструкция кросса позволяет монтажнику извлечь круглую сплайс-кассету с модулем из оптического кабеля, расположить ее на расстоянии до 2 м от кросса и сваривать оптоволокно в комфортных условиях. Запас оптического кабеля выкладывается в тумбе шкафа.

При разработке этой модели кросса были учтены рекомендации специалистов «Ростелекома».

НТЦ «ПИК»: 8 (8332) 37-6140

ИБП для малого бизнеса

Компактные ИБП VX600 служат для защиты подключенного оборудования от скачков и перепадов напряжения, а также производят его безопасное выключение во время продолжительного отсутствия электроэнергии. Надежность функционирования обеспечивает встроенный микропроцессорный контроллер. Индикаторы отображают в реальном времени состояние ИБП и потребляемую мощность. Автоматическая регулировка напряжения (AVR) поддерживает безопасное стабилизированное питание подключенного оборудования. Для своевременной замены батареи предусмотрена функция автоматического самотестирования, а интеллектуальное зарядное устройство сокращает время ее заряда.

Delta Electronics: (495) 644-3240

Коммутатор приложений

Alteon 10000 отвечает потребностям передачи постоянно растущего трафика приложений доступа к Интернету, видео, мобильных приложений, сетевых сервисов (включая DNS, Diameter, DHCP и LDAP), трафика SIP и VoLTE по IMS. Коммутатор основан на аппаратной платформе Radware OnDemand Switch 4 и поддерживает пропускную способность до 80 Гбит/с.

Шасси устройства соответствует ATCA и требованиям телекоммуникационной отрасли. Платы на шасси Alteon 10000 допускают «горячую» замену, что обеспечивает непрерывность бизнес-процессов и работы критически важных приложений. Надежность операторского класса достигается за счет наличия двух распределяющих блоков и трех источников питания с балансировкой нагрузки.

Продуктовая линейка Alteon была приобретена компанией Radware у Nortel Networks и дополнена новой функциональностью. Обновлены аппаратные платформы и ПО для Alteon Series 2 и 3.

«Телеинком-ПК»: (495) 231-2120

Малогабаритная укороченная муфта

Муфта МТОК-Л7 предназначена для прямого и разветвительного сращивания оптоволоконного кабеля (ОК) различных конструкций без фиксации брони в патрубках. Броня из гофрированной стальной ленты и экраны алюмополиэтиленовых оболочек внутри муфты соединяются с помощью перемычек.

Муфта позволяет вводить ОК стандартных диаметров 14–20 мм, тонкие кабели диаметром 5–10 мм, а также малогабаритные плоские кабели. При этом специальные комплекты для ввода ОК не требуются.

МТОК-Л7 используется для установки в стесненных условиях – заполненных колодцах, шкафах, в технических помещениях и на опорах. Муфта обеспечивает монтаж городских и подвесных оптических кабелей с одной оболочкой, а также кабелей оригинальных конструкций – плоских ОК, микрокабелей емкостью до 48 оптических волокон.

Способ герметизации кожуха с оголовником механический, с применением пластмассового хомута. Муфта оснащена ступенчатыми патрубками, тонкие участки которых предназначены специально для ввода кабелей диаметром до 10 мм. Конструкция

внутренних элементов муфты позволяет крепить центральный и периферийные силовые элементы сращиваемых ОК.

Муфта имеет два круглых патрубка с внутренним диаметром 20 мм, два круглых патрубка диаметром 16 мм и один овальный патрубок. Муфта оснащается пластмассовым кронштейном, на котором можно установить три кассеты типа КС.

«Связьстройдеталь»: (495) 786-3436

Дисковая система
для высокопроизводительных приложений

Система хранения IBM System Storage DCS3700 обеспечивает размещение до 60 жестких дисков SAS в корпусе высотой 4U. Кроме того, возможно подключение двух дополнительных модулей расширения – в целом до 180 3,5-дюймовых дисков в объеме 12U. Благодаря поддержке оптимизированных с точки зрения емкости жестких дисков Nearline SAS емкостью 2 Тбайт система позволяет начать с небольшой конфигурации и довести доступный объем памяти до 360 Тбайт. DCS3700 имеет два интеллектуальных контроллера, поддерживающих RAID-уровни 0, 1, 3, 5, 6 и 10 и работающих в режиме Active/Active.

Для подключения к серверам или сетям хранения данных в системе предусмотрено два хост-порта SAS 6 Гбит/с на контроллер в стандартной комплектации с возможностью добавления дочерней карты с дополнительными портами (два порта SAS 6 Гбит/с или четыре порта Fibre Channel 8 Гбит/с на карту).

Обладая постоянной скоростью чтения с диска (4000 Мбайт/с), система DCS3700 подходит как для задач обработки больших объемов данных, так и для приложений с большим числом операций ввода-вывода, характерным для СУБД, систем электронной почты и т.д.

Для обеспечения бесперебойной работы пользователей и приложений система DCS3700 поддерживает резервирование компонентов, автоматический обход сбоев и возможности интерактивного администрирования.

В сочетании с файловой системой IBM GPFS система хранения DCS3700 становится целостным решением для управления файлами с общим доступом к дискам на основе политик.

IBM: (495) 775-8800

Михаил ЕМЕЛЬЯННИКОВ

И это все о ФЗ-152

С днем рождения, крошка!

>>>> Сегодня нашему любимчику, нашему enfant terrible, нашей надежде и нашему разочарованию исполнилось 5 лет. Он уже очень большой и взрослый для того мира, в котором должен жить. Но никак таковым стать не может.

А ведь как на крошку надеялись! Родители обещали, что он, как подрастет, станет опорой и защитой всем нашим согражданам, особенно тем, про которых нехорошие дяди и тети как чего узнают, так другим сразу и рассказывают. А вот крошка пошлет к нехорошим своих подчиненных (а младенцу их пообещали, аж трех сразу), и они этих самых нехороших крепко отшлепают. Да еще потом отведут к строгим дядям и тетям, которые знают страшные заклинания КоАП и УК, так они нехорошим еще и добавят.

И вот к пятому дню рождения и родители, и Самый Главный наказали имениннику новый костюмчик сшить. Известный модельер к тому времени как раз свой фасончик модельный предложил. И вправду весь такой европейский, либеральный, к тому же в носке дешевый и нетребовательный. Но модельер – это креативщик, а шить-то портным. Портные долго спорили, старались как могли, но лекала у всех разные были. Получился костюмчик хотя и новый, с прибамбасами, но из материальчика почему-то старого, за пять лет местами изрядно потертого. И ходить в нем к обиженным сплетнями гражданам совсем неудобно.

С днем рождения, крошка! С новым костюмчиком!

А вас всех с пятилетием ФЗ-152 «О персональных данных».

Засучим рукава, подтянем животы, выдохнем… и пойдем работать. Малыш строгий, а вдруг лютовать начнет?

Персданные владельца животных

>>>> Мне кажется, в связи с многострадальным ФЗ-152 потихоньку съехала крыша у значительного количества причастных к теме.

«Обращение с информацией, содержащей персональные данные владельца животных, осуществляется в соответствии с федеральным законодательством о персональных данных.

Основным документом, удостоверяющим факт регистрации животного, является регистрационное удостоверение. Форма регистрационного удостоверения и порядок его выдачи устанавливается федеральным органом государственной власти.

По желанию владельца животного при регистрации животного ему вводится электронный носитель информации (микрочип) с записанными на него персональными данными владельца животного и описанием индивидуальных характеристик животного.

Перечень данных, записываемых на электронные носители информации, вводимые в животное, а также порядок учета таких данных определяется уполномоченным федеральным органом государственной власти».

Это не стеб. Это – из принятого в первом чтении законопроекта «Об ответственном обращении с животными».

Может быть, пока второе чтение не началось, внести поправки и пойти дальше. Поскольку в ФЗ-152 нигде не написано, что субъект – человек, можно узаконить и персданные домашнего животного. А что, «описание индивидуальных характеристик животного» – ведь это и есть биометрические персональные данные, используемые для установления его личности. И не надо лишней бумаги тратить!

О бедном субъекте замолвите слово

>>>> Каким образом закон позволяет субъекту оценить, соответствует ли содержание и объем обрабатываемых персональных данных заявленным целям обработки и не являются ли запрашиваемые данные избыточными по отношению к заявленным целям их обработки? А никак. Можно, конечно, «накапать» в Роскомнадзор – но бесполезно. Жалоба субъекта основанием для проверки не является (об этом ниже).

В ст. 6 значительно расширены основания для обработки персданных без согласия субъекта. Расширены совершенно справедливо и в целом правильно, но никакого повышения защищенности субъекта это не предполагает. Появилось новое основание для обработки данных без согласия субъекта – «достижение общественно значимых целей», пусть и при обязательном условии, что при этом не нарушаются права и свободы субъекта. Такое основание дает возможность, например, обзванивать доноров сайта «Распил.Ру». А что – цель еще какая значимая! Общественно. Нарушены ли права тех, кому звонили? Идите в суд и доказывайте, что они нарушены, если сможете.

И в заключение. Из нового закона № ФЗ-242 «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам осуществления государственного контроля (надзора) и муниципального контроля» в подписанной президентом редакции исчез раздел о внесении изменений в ФЗ-152 в части оснований для внеплановых проверок. По-прежнему жалобы субъектов, обращения органов власти и СМИ не могут быть основанием внеплановой проверки оператора, что бы не писал Роскомнадзор в своем административном регламенте.

Так что субъект может жаловаться, может не жаловаться – результат один. Проверку его жалобы ПО ЗАКОНУ провести нельзя. По-прежнему при появлении в продаже базы данных с моими данными я, как субъект, ничего сделать не могу. И ФЗ-152 мне не помощник.

комментировать

Этим летом еще долго «аукался» пресловутый ФЗ-152. Большинство же блогеров предпочитали заглядывать в будущее – социальную сеть 2.0, облачную демократию…

Геннадий ФОКИН

Мыльный пузырь софтверного бизнеса

>>>> Болевые точки отечественного софтверного бизнеса – отсутствие или недостатки оформления нематериальных активов, неразрешенные проблемы с авторами и первичными правообладателями программ для ЭВМ (работниками) и, как следствие, торговля «воздухом», введение в заблуждение и нарушение налогового законодательства.

Последние годы софтверные компании главным своим документом называют лицензионную политику, которая при внимательном рассмотрении является не более чем системой скидок и наценок на «авторское сопровождение» эксплуатации проданных программных продуктов. Наличие интеллектуальной собственности и ее использование без нарушения интеллектуальных прав подтвердить ничем не могут, однако все скидки и наценки объясняют своим «исключительным интеллектуальным правом».

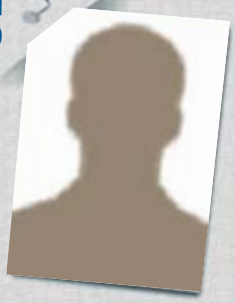
Автоматизация прочно вошла в экономику и управление – «интернет-коммерция», «облачные технологии и коммуникации», «порталы госуслуг», «цифровые деньги», «электронное правительство», «электронные кадастры» и т.д. И подо все это подведена мина замедленного действия – признание, паспортизация, легальное использование интеллектуальной собственности и соблюдение интеллектуальных прав.

Пока этот вопрос еще не задается первым, даже по госзаказу. В первую очередь спрашивают – сколько стоит? Проблемы с авторами и правообладателями средств автоматизации, вытекающие из статьи 1228.3 ГК РФ, заказчикам и покупателям даже в голову не приходят; большинство заказчиков не имеют идеологии, методологии и практики менеджмента интеллектуальной собственности… однако критическая масса рисков софтверного бизнеса накапливается и проблемы не заставят себя ждать – если болезнь запущена, то летальный исход неизбежен.

комментировать

Сушант САХАНИ

Социальная сеть 2.0



>>>> Резкий рост популярности социальных сетей в потребительской и корпоративной средах уже диктует новую динамику в бизнесе.

Допустим, мой друг разместил в сети Facebook или Google+ фотографии, сделанные во время отпуска на курорте. Найдя эти снимки и увидев, в каком замечательном месте отдохнул мой приятель, принимаю решение тоже поехать туда. Что в таком случае мне позволит сделать социальная сеть? Разве что нажать кнопку «Нравится» и добавить свой комментарий к сообщению друга. В эпоху же социальных сетей 2.0, наведя курсор на фотографии моего друга, я смогу узнать стоимость билетов и гостиниц на этом курорте. Сеть также предложит другие места, похожие на запечатленные приятелем. Наконец, социальная сеть 2.0 позволит мне забронировать авиабилеты и гостиницу, не выходя из социальной сети.

Сегодняшние социальные сети представляют собой море информации, в которой легко утонуть, и я надеюсь, что социальная сеть 2.0 будет значительно более полезной и необременительной для пользователя. Ориентируясь на социограмму пользователя, она должна будет выбирать в лавине информации лишь то, что представляет для него интерес. Кроме того, платформы социальных сетей 2.0 будут сами строить социограммы на основе действий пользователя и предоставлять актуальную для него информацию, не заставляя отвлекаться на ненужное.

комментировать

Петр ДИДЕНКО

Облачная демократия

>>>> Что представляет собой «облачная демократия» с технологической точки зрения? Это три базовых принципа: раскрытие информации, делегирование голоса с возможностью его отзыва и живая обратная связь избирателей и их представителей. Принципиально – это не что иное, как модель коллаборативного принятия решений для значительной группы людей, общающихся через Интернет. Мы предполагаем, что эта группа людей может достигать численности целого государства, и благодаря гибкости системы ее участники смогут взаимодействовать между собой и принимать решения демократичным образом.

В окружающем нас мире есть немало других групп людей, которым надо принимать решения путем голосования! ТСЖ, садовый и гаражный кооперативы, волонтерские, профессиональные организации, профсоюзы, общественные организации инвалидов, ветеранов локальных войн и конфликтов, клубы по интересам и т.д.

Голосование – это правильно, а принятие решений можно сделать эффективным. При этом пересмотр устоявшихся процедур коллаборативного принятия решений логичнее начать не с Российской Федерации, а с «Ручейка». Проектируемая нами система облачной демократии и будет технологической платформой, на которую сможет прийти любая группа людей, имеющая потребность в обсуждении, выработке и принятии решений с помощью демократических процедур. Такая группа сможет у нас получить бесплатно в свое распоряжение инструменты для обсуждения и формирования проектов решений, а также инструменты для голосования и подведения итогов.

комментировать

Реклама в номере

АЛЮДЕКО-К
Тел./факс: (4942) 31-1733
E-mail: sales5@aludeko.ru
www.aludeko.ru . . . . с. 11

АМТ-ГРУП
Тел.: (495) 725-7660
Факс: (495) 725-7663
E-mail: info@amt.ru
www.amt.ru . . . . с. 44, 45

АРМО-СИСТЕМЫ
Тел.: (495) 937-9057
Факс: (495) 937-9055
E-mail: armosystems@armo.ru
www.armosystems.ru . с. 77

ИНФОРМЗАЩИТА
Тел./факс: (495) 980-2345
E-mail: market@infosec.ru
www.infosec.ru . . . . с. 39

ИНФОРМСВЯЗЬ
Тел.: (495) 797-8899
Факс: (495) 437-5298
E-mail: root@informsviaz.ru
www.informsviaz.ru . . с. 85

КРОК
Тел.: (495) 974-2274
Факс: (495) 974-2277
E-mail: croc@croc.ru
www.croc.ru . . . . с. 74, 75

ПИК НТЦ
Тел.: (8332) 37-6137
Факс: (8332) 37-6138
E-mail:pik@pik.kirovcity.ru
www.pik.kirovcity.ru . . с. 79

РТКОММ
Тел.: (495) 988-7778
Факс: (495) 988-7776
E-mail: info@rtcomm.ru
www.rtcomm.ru . . . 4-я обл.

EDGE-CORE NETWORKS
Тел.: (916) 625-8272
E-mail: russia@edge-core.com
www.edge-core.com. . с. 91

HUBER+SUHNER
Тел.: (495) 775-6653
Факс: (495) 775-7794
E-mail:
info.ru@hubersuhner.com
www.hubersuhner.ru . с. 14

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

RITTAL
Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru . . . . 1-я обл.

SOCOMEC UPS
Тел: (495) 775-1985
www.socomec.com . . с. 73

SONY ELECTRONICS
Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu . . . с. 13

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.