

Негатив на фондовом рынке уронил акции телекома



Главным событием весны на финансовых рынках стал банковский кризис на Кипре во второй половине марта, вызвавший панику не только на острове, но и за его пределами. Упали цены на нефть и золото. Неблагоприятная конъюнктура оказала давление и на бумаги телекоммуникационных компаний.



**Анна
ЗАЙЦЕВА,**
аналитик,
УК «Финам
Менеджмент»

Меры, принятые правительством Кипра для решения проблем банков и включающие «стрижку» депозитов, оказались беспрецедентными. Они означают, что теперь за неспособность банкиров расплатиться со своими долгами могут отвечать вкладчики кредитного учреждения.

Товарные рынки продолжали находиться под давлением продавцов, в частности, из-за приближения крайнего срока, после которого инвестиционные банки США не смогут торговать сырьевыми контрактами на собственные денежные сред-

ства (закон Додда – Франка). Цены на нефть опустились ниже \$105 (–9,2%) за баррель марки Brent, а золото подешевело до \$1370 (–14,6%) за унцию.

Где конец интриги?

Капитализация телекоммуникационного холдинга «Ростелеком» за рассматриваемый период сократилась на 4,35% – до отметки 113,2 руб. за акцию. Во второй половине марта акции торговались в восходящем тренде. Напомним, что за объявлением о выходе из капитала оператора компании Marshall Capital последовали кардинальные перестановки в топ-менеджменте: в конце марта совет директоров «Ростелекома» прекратил полномочия Александра Провоторова, назначив президентом компании Сергея Калугина, ранее возглавлявшего «Национальные кабельные сети». Рынок положительно интерпретировал эти события, ожидая завершения корпоративного противостояния и устранения нефинансовых рисков на фоне появления лояльного акционера.

Дополнительным позитивным фактором для «Ростелекома» стала публикация ожидаемо неплохой отчетности за 2012 г. и утверждение высокой цены обратного выкупа ценных бумаг у миноритарных акционеров, несогласных с планом реорганизации (на уровне 136,05 руб. за обыкновенную акцию и 95,24 руб.

за привилегированную, что подразумевает солидную премию). Конечно, потенциально очень сильным драйвером было объявление о покупке банком ВТБ бизнеса четвертого крупнейшего в стране оператора сотовой связи – российского подразделения группы Tele2, так как сделка, по мнению большинства экспертов, проведена в интересах «Ростелекома». В СМИ и в профессиональном сообществе широко обсуждаются перспективы и механизмы возможной интеграции этого актива в бизнес традиционного оператора, что, несомненно, позитивно отразится на позициях последнего в сегменте голосовой связи и в перспективе, соответственно, очень сильно повлияет на акционерную стоимость.

Однако в первой половине апреля тренд развернулся и стоимость бумаг довольно серьезно скорректировалась. Можно полагать, что помимо общей неблагоприятной конъюнктуры (формировавшейся в том числе под влиянием кипрских событий), давление которой на рынок было весьма ощутимым, сыграла свою роль расстроившаяся сделка между структурами Аркадия Ротенберга и фондом Marshall Capital. Возвращение неопределенности в отношении крупнейшего миноритарного акционера и риски очередного затягивания сделки со «Связьинвестом» были негативно восприняты инвестиционным сообществом. Вероятно, второстепенным неблагоприятным фоном стало решение арбитражного суда, вставшего на сторону «Скартел» в судебном споре с «Ростелекомом» по поводу условий предоставления инфраструктуры сетей четвертого поколения, что может негативно отразиться на сроках запуска корпорацией услуг 4G.

Смешанная динамика...

Бумаги МТС, после неплохого отрезка торгов в восходящем тренде во второй половине марта, с начала апреля также оказались под давлением кризиса на Кип-

Справка ИКС



С 15 марта по 15 апреля индекс ММВБ потерял 9,1%, составив на конец периода 1359,69 пункта, а капитализация индекса РТС сократилась на 11,51% – до 1 360,8 пункта. Отраслевой индекс «ММВБ телекоммуникации» потерял за месяц 11,64%, снизившись до 2 016,40 пункта.

ре и общего ухудшения рыночных настроений. В итоге за отчетный период бумаги потеряли почти 7% (до 261,85 руб.). Из событий в индустрии на динамику торгов бумагами оператора могло повлиять прежде всего сообщение о покупке Tele2, что с высокой долей вероятности предполагает усиление в сегменте сотовой связи позиций «Ростелекома» и существенное ужесточение конкурентной среды в целом. Учитывая вступление в силу в конце 2013 г. правил MNP, такой сценарий сейчас скорее не в пользу МТС, но в целом это, конечно, в большей степени долгосрочный фактор.

Позитивным моментом определенно стала довольно сильная отчетность компании по итогам 2012 г. и объявление положений новой дивидендной политики. Результаты в целом совпали с рыночными ожиданиями, а по отдельным показателям оказались и заметно выше. Несмотря на снижение доходов на 30% (преимущественно на фоне потери подразделения в Узбекистане), чистая прибыль оказалась лучше ожиданий и составила около \$1 млрд. Выручка также превысила консенсус-прогноз, увеличившись на 0,9% – до \$12,4 млрд. Показатель рентабельности EBITDA вырос выше предварительных ориентиров – на 0,8 п.п., до 42,6%. Долговая нагрузка осталась на комфортном уровне – \$7,6 млрд. Дивидендная доходность акций оператора составит около 7% – это, несомненно, довольно привлекательный уровень. Хорошая отчетность и щедрые дивиденды поддержали котировки, однако этого позитива не хватило, чтобы нивелировать предыдущую коррекцию.

Смешанную динамику под влиянием ключевых событий рынка и индустрии демонстрировали и бумаги «ВымпелКома». При этом оператор завершил период в положительной зоне, по итогам его акции подорожали почти на 2% (до \$12 за шт.). Характерное для бумаг сектора снижение в начале апреля было компенсировано довольно сильным восходящим движением ближе к концу отчетного периода. Одним из наиболее сильных корпоративных факторов стало сообщение о готовящейся продаже группой ряда активов – алжирского оператора Djezzy и канадского Globalive Wireless. Вероятность национализации Orascom Telecom Algeria обсуждалась давно, речь в последнее время преимущественно шла об условиях сделки. По предварительным данным, цена продажи довольно высока, поэтому реакция инвестиционного сообщества была позитивной – сделка позволит нивелировать политические риски и существенно сократить долговую нагрузку за счет средств, полученных от продажи контрольного пакета ОТА. Канадское подразделение генерирует незначительную часть совокупной выручки корпорации, и продажа подразделения по большому счету нейтральна для консолидированных результатов; одновременно доход от сделки также может послужить цели снижения долга. В целом отказ корпорации от работы в ряде регионов скорее можно считать оправданным решением. Продажа низкомаржинальных или рискованных активов позволит сократить издержки (в том числе за счет

оптимизации географии бизнеса) и сконцентрироваться на наиболее перспективных локальных рынках.

«Мегафон» за рассматриваемый период потерял 5,4% своей капитализации, акции оператора откатились к отметке в 900,1 руб. в условиях ненасыщенного новостного фона. Среди значимой корпоративной информации следует выделить выпуск «Мегафоном» собственного брендированного ультрабюджетного Android-смартфона Login. Вывод на рынок такого устройства в перспективе способен позитивно повлиять на розничные продажи оператора, однако, учитывая высокую степень насыщенности рынка, вряд ли окажет существенную поддержку котировкам «Мегафона».

И корректировка вниз

Акции российских ИТ-компаний в прошедшем месяце значительно скорректировались. Наибольшее снижение было зафиксировано в случае РБК – капитализация компании снизилась более чем на 30%, до 8,08 руб. за бумагу. Столь значительная просадка, очевидно, объясняется низкой ликвидностью бумаг компании. Кроме того, инвесторы, по всей видимости, настороженно смотрят на перспективы повышения финансовой эффективности компании новым топ-менеджментом.

Капитализация АФК «Система» снизилась на 6,6%, до \$25,2 за бумагу. В апреле компания опубликовала финансовые результаты по US GAAP за 2012 г.: консолидированная выручка выросла на 3,9% (до \$34,2 млрд), чистая прибыль без учета корректировок достигла \$1,8 млрд (прирост по сравнению с предыдущим годом на 80%), показатель OIBDA без учета корректировок увеличился на 3,3% – до \$8,5 млрд. Коммерческие, административные и управленческие издержки компании снизились на 1,5%, до \$3855,8 млн, а расходы на износ и амортизацию – на 3,4%, до \$3159,4 млн.

Важнейшим событием прошедшего месяца для АФК «Система» стала победа ее индийской «дочки», Sistema Shyam TeleServices Limited (SSTL), в конкурсе на частоты в девяти округах Индии. Стоимость лицензий составила \$665 млн. Следует отметить, что параллельно SSTL отказалась от работы еще в трех округах и 10 районах, что говорит о стремлении компании сконцентрироваться на развитии бизнеса в наиболее перспективных для себя регионах. Позитивное влияние на капитализацию АФК «Система» в среднесрочной перспективе может оказать информация о возможном участии компании в приватизации крупнейшего сербского телекоммуникационного оператора Telekom Srbija, что позволит АФК серьезно нарастить абонентскую базу и укрепить позиции на глобальном рынке.

Снижение наблюдалось и в бумагах других ИТ-компаний. Так, котировки IBS Group упали на 6,52% (до \$17,2), Yandex N.V. – на 14,43% (до \$20,4), а холдинг Mail.Ru Group потерял 18,9% (до \$27,9 за бумагу) на фоне отсутствия значимой корпоративной информации. Вероятно, динамика бумаг этих компаний в прошедшем месяце была обусловлена техническими факторами. ИКС

MULTI-NETWORK REVENUE SECURITY

Реклама

Verimatrix является ведущим вендором для защиты доходов ТВ операторов, использующих мульти сети и мульти экраны по всему миру. Неоднократно отмеченный призами и независимыми аудитами экономически выгодное решение Verimatrix Video Content Authority System (VCAS™) и ViewRight® позволяет кабельным, спутниковым, эфирным, IPTV и OTT операторам расширять их ТВ сервисы и защищать бизнес модель.

www.verimatrix.com


verimatrix®
Beyond Content Protection to Revenue Security™

Александр КРУПЧИК:

«Мы намерены формировать этот рынок»

Стремление предоставить своим постоянным клиентам полный спектр услуг информационной безопасности привело системного интегратора «Радиус Групп»

к освоению новых компетенций – аудита на соответствие требованиям PCI DSS и ASV-сканирования.

Компания выходит в новый сегмент рынка инфобезопасности, причем, как отмечает Александр КРУПЧИК, директор центра информационной безопасности «Радиус Групп», не только российских, – и своих амбиций на нем не скрывает.

– В 2013 г. в структуре вашей компании был выделен департамент информационной безопасности. Чем обусловлено это решение?

– Одно из основных направлений деятельности «Радиус Групп», системного интегратора широкого профиля, – построение ЦОДов, в том числе обеспечение информационной безопасности их ИТ-инфраструктуры. Соответственно, определенные компетенции в компании имеются изначально. Кроме того, у нас есть давние клиенты, которым мы можем и хотим предоставлять дополнительные услуги информационной безопасности. Ассортимент этих услуг сформировался на основе спроса и уже реализованных сотрудниками компании проектов: так, для Global Payments Group были проведены подготовка к сертификации и сертификационный аудит (United Card Service, UCS); для МТТ – оценка соответствия ISO 27001, анализ рисков ИБ. Несколько проектов было выполнено для «ТрансКредитКарт» – комплексное проектирование системы защиты информации, анализ рисков ИБ, внедрение СТО БР ИББС (с учетом требований 152-ФЗ), разработка стратегии и планов восстановления после сбоев, подготовка к сертификационному аудиту по PCI DSS, разработка организационно-распорядительных документов, регламентирующих ИБ, проектирование и внедрение средств защиты информации, анализ уязвимостей и тестирование на проникновение.

Если со стороны наших заказчиков есть спрос на услуги информационной безопасности, почему бы его не удовлетворить? Руководствуясь этой логикой, мы расширили спектр своих компетенций в области информационной безопасности и для развития этого направления выделили отдельный департамент. Сейчас его штатная численность – пять сотрудников, в течение этого года планируется расширение штата до восьми человек с дополнительными компетенциями. И это без учета подразделения, которое специализируется на сетевой

инфраструктуре ЦОДов. Там есть специалисты, которые занимаются информационной безопасностью на сетевом уровне.

– С открытием департамента компания выходит на рынок услуг информационной безопасности. Какие это будут услуги и на каких направлениях планируете фокусироваться?

– Что касается ассортимента услуг в целом, то это комплексный аудит информационной безопасности с разработкой долгосрочных планов развития; создание системы защиты персональных данных в соответствии с 152-ФЗ; обеспечение соответствия требованиям по информационной безопасности Национальной платежной системы; консалтинг и аудит по стандарту Банка России СТО БР ИББС (стандарт носит рекомендательный характер, но многие банки ориентируются на него и стремятся выполнить его требования); внедрение стандарта Payment Card Industry Data Security Standard (PCI DSS) и сертификационный аудит; создание системы управления информационной безопасностью, подготовка к сертификации по стандарту ISO 27001; тестирование на проникновение; ASV-сканирование, внутреннее сканирование уязвимостей; внедрение системы управления непрерывностью бизнеса (BCP/DRP); разработка стратегий и планов восстановления после сбоев; проектирование и внедрение систем защиты информации с последующим сопровождением и поддержкой. Все эти работы проводят наши специалисты, имеющие сертификаты CISSP, CISA, CISM, PCI QSA, PCI ASV. Особое внимание мы уделяем вопросам аудита процессинговых центров банков, именно здесь у нас есть очень глубокие компетенции и большой опыт работы.

– Очевидно, что ставка делается на новую компетенцию вашей компании – сертификационный аудит на соответствие PCI DSS. Чем обусловлено ее освоение, насколько услуга актуальна для рынка?

– В мире стандарт PCI DSS актуален с 2006 г., в России – примерно с 2010 г. Он обязателен для любой организации, клиенты которой оплачивают товары и услуги картами в международных платежных системах. Это не только банки и процессинговые центры, но и небольшие компании, предоставляющие, например, сервисы бронирования гостиниц или билетов, интернет-магазины и пр. Но для работы с международными платежными системами информационные системы, в которых хранятся, передаются или обрабатываются данные платежных карт, должны соответствовать требованиям стандарта PCI DSS. Для поставщиков карточных сервисов соответствие PCI DSS означает, что в международных платежных системах данные держателей их карт защищены на организационном и техническом уровнях, и подтверждать это соответствие надо ежегодно.

В России много интеграторов и специализированных компаний, которые занимаются аттестацией систем информационной безопасности, но мы делаем упор на работу со своими постоянными клиентами, которым дополнительно можем предоставить этот сервис. И в нынешнем году наша компания была аккредитована Payment Card Industry Security Standards Council (PCI SSC), получив статус Payment Card Industry Qualified Security Assessor (PCI QSA) с правом работы в регионе CEMEA. QSA-компании предоставляют услуги по сертифицированному аудиту на соответствие требованиям стандарта PCI DSS, что позволяет подтвердить соответствие информационной системы требуемому уровню безопасности. Наши услуги включают в себя не только подтверждение соответствия стандарту PCI DSS, но и консалтинг. В случае выявления недостатков наши сертифицированные специалисты помогут привести информационную систему заказчика в необходимое для получения сертификата состояние. Для этого проводим консультации с заказчиком, обучение персонала, оказываем помощь в проектировании систем защиты информации, разработке и доработке организационно-распорядительной документации.

– Еще одна услуга из разряда новых – ASV-сканирование. Причем, похоже, не только для вашей компании, но и для рынка информационной безопасности в целом?

– Да, это достаточно редкая для российского рынка услуга. В России ее предоставляют, насколько мне известно, лишь три компании. А для нас освоение этой компетенции стало логическим продолжением работ по выполнению сертификационных аудитов на соответствие требованиям стандарта PCI DSS. Одно из требований международных платежных систем Visa и MasterCard состоит в том, что в информационных системах, в которых хранятся, передаются и обрабатываются данные платежных карт, необходимо ежеквартально проводить сканирование уязвимостей специализированной компанией – Approved Scanning Vendor (ASV). Если организация хочет работать с Visa и MasterCard, она должна выполнять эти требования. Поэтому в марте нынешнего года наша компания подтвердила свою компетенцию в области проведения ASV-сканирований, пройдя аккредитацию и получив соответствующий статус с правом предоставлять

услуги внешнего ASV-сканирования уязвимостей ИС по всему миру.

– Как осуществляется сканирование и кто эту услугу запрашивает?

– Сканирование проводится с помощью специализированных продуктов и позволяет проанализировать уровень защищенности информационной системы, определить уязвимости межсетевых экранов и маршрутизаторов, операционных систем, баз данных, веб-серверов, почтовых серверов, DNS-серверов, серверов приложений и др. По итогам сканирования мы не только предоставляем владельцу ИС отчет, но и оказываем консалтинговую поддержку, чтобы помочь клиентам достичь необходимого уровня соответствия системы требованиям стандарта PCI DSS. Эта услуга оказалась очень востребованной банками, интернет-магазинами, операторами мобильной связи – всеми, кто активно работает с международными платежными системами.

– Вы получили право оказывать услуги ASV-сканирования по всему миру. Действительно заманиваете на зарубежные рынки?

– Почему нет? Наличие аккредитации подтверждает высокий уровень компетенции наших сотрудников, которые могут выполнять работы на международном уровне. На английском языке мы составляем отчетные документы и направляем их в международные системы Visa и MasterCard, которые подтверждают, что они приняли наши документы. Не каждая организация имеет в своем штате сотрудников, имеющих такие компетенции и хорошо владеющих английским языком.

– Существуют ли «фирменные» технологии и подходы, которые использует ваша компания в этой работе?

– Как один из вариантов мы предлагаем использовать средства защиты с открытым кодом – они, как правило, бесплатны. Это позволяет существенно снизить стоимость и сократить сроки внедрения стандарта PCI DSS. Такой подход вряд ли интересен крупным организациям, но для небольших компаний вполне приемлем. Без ложной скромности, в этом смысле мы уникальны: в России больше никто таких продуктов не предлагает. А мы к тому же имеем все необходимые компетенции для их внедрения и сопровождения.

– Насколько ощутима конкуренция в этом сегменте рынка, какую его долю и за счет чего рассчитываете занять в ближайшие годы?

– Конкуренция, конечно, есть. Наши преимущества в этой конкурентной среде – компетенции, опыт работы, невысокие цены и хорошее качество. Важный момент: мы не только строим ЦОДы (в том числе для себя), но и будем их готовить к стандартизации по ISO 27001, по PCI DSS, будем выполнять требования по защите персональных данных в соответствии с 152-ФЗ. Что касается перспектив расширения перечня услуг, то они связаны с получением партнерских статусов. Мы не просто рассчитываем на значительную долю рынка аудита на соответствие PCI DSS и ASV-сканирования, но и намерены формировать этот рынок. И не только в России, но и в странах СНГ.

Беседовала **Лилия ПАВЛОВА**

Великий поход за качеством



Так они и живут в заблуждении, полагая, что достаточно быть добрым католиком, чтобы не оказаться в застенках инквизиции.
Хуан Антонио Льоренте. История испанской инквизиции

Что должен предпринять регулятор, чтобы качество услуг в современных мультисервисных сетях повысилось? Положиться на «невидимую руку» рынка? Контролировать все и вся? Или же создать соответствующие условия?..



Александр ГОЛЫШКО,
начальник
аналитического
отдела,
«РТ Лабс»,
канд. техн. наук

И это все о нем

Трудно найти человека, который бы не «проехался» в последнее время по качеству связи, прежде всего мобильной. И не где-то на окраинах, а прямо в столице нашей родины. Только за последний год в этом были замечены и премьер-министр, и мэр со своими чиновниками, и профильный министр со своими замами, и, разумеется, Роскомнадзор, не говоря уже о простых гражданах-пользователях. Знакомым и даже незнакомым людям в Московском регионе есть о чем поговорить: на даче рядом с Москвой «связь плохая, а то и отсутствует», там же, «чтобы словить сигнал на модеме, надо держать ноутбук над головой», «интернета таки нет, а денег на счету почему-то тоже нет», «пока разговаривал с шефом, связь пять раз обрывалась», «сменил оператора – думал, поможет»... Согласитесь, последняя фраза – самая страшная.

Всему этому можно верить или не верить, но трудности мобильной связи объективны и имеют место быть во всем мире. Во-первых, против всех нас «играет» физика, потому как у радиостов среда передачи – одна на всех, радиочастоты в дефиците, а эффективность их использования вплотную подошла к физическим пределам, очерченным еще Клодом Шенноном. Во-вторых, армия смартфонов увеличивается в год почти на 40%, «аппетит» к потреблению трафика приходит по мере роста ШПД, видео (т.е. «тяжелого» трафика) становится все больше, а свободных ресурсов сети – все меньше. Народу в Москве «толчется» тоже в прогрессии, а точки, где это удобно делать (от мегамаркетов и бизнес-центров до автопробок), растут как грибы. Сети нужно оперативно

модернизировать, и помимо денежных в больших городах есть дополнительные трудности как с кабельной канализацией, так и с размещением оборудования на крышах и чердаках. А тут еще наша специфика – не успели толком развить сети 3G, как занялись 4G, что в принципе верно и соответствует мировым трендам.

По оценкам зарубежных экспертов, в 2012 г. использование беспроводных телефонов впервые превзошло использование стационарных, свыше 35% домохозяйств полностью отказались от подключенных стационарных телефонов, в 16% они сохранились, но по большей части в качестве пресс-папье или милого сердцу антиквариата.

Вполне логично, что именно Роскомнадзор отправился сегодня в поход за качеством услуг связи, поскольку в РФ нет каких-либо утвержденных норм в данной сфере, что мешает борьбе за это самое качество. Вот, скажем, регулятор мог бы потребовать от операторов соблюдения тех или иных условий лицензии на предоставление услуг мобильной связи, а за что ухватиться? Что написано в лицензиях? Где критерии? Где методики? Для этого, собственно, в Роскомнадзоре разрабатывался проект Концепции создания системы контроля качества предоставления услуг связи в Российской Федерации, а НИИРу было поручено предложить методики контроля (оценки) показателей качества.

За что бороться?

От проекта концепции до конкретных НПА путь неблизкий, и у всех есть время подумать, как лучше это качество «ухватить». Настораживает, конечно, что объявлено о концепции системы контроля,

а не о концепции контроля систем. Эта игра слов может дорого стоить.

Исследователи утверждают, что в мобильной сети 5% пользователей могут сгенерировать более 80% трафика, способного привести к снижению скоростей и вызвать коммуникационные проблемы у остальных абонентов. Посему борьба за качество мобильной связи – явный тренд современности, и мы находимся на верном пути. Теоретически этот путь включает в себя целый набор различных мероприятий по улучшению качества (от аппаратных до регуляторных), которые должны «играть в ансамбле», и каждое из них важно по-своему.

Но встречающиеся нередко рассуждения о том, что качество связи контролировать вообще не надо и борющийся за лояльность клиентов рынок сам во всем разберется, не выдерживают никакой критики в обрисованной выше ситуации, когда у всех операторов с качеством одинаково плохо. Любой финансовый стратег тут же скажет: «Зачем деньги в сеть вкладывать, если абоненты все равно никуда не денутся? Зачем ухудшать нашу ебитду?». Мы, собственно, уже имеем общепризнанные проблемы с качеством, и что? Где оно?

Точно также вряд ли стоит надеяться, что, создав какую-то универсальную глобальную систему контроля качества предоставления услуг связи, мы сразу же решим все наши проблемы. И вот почему.

Нет сомнения, что в части качества покрытия, обрывов соединений и излишнего уплотнения каналов дальней связи (т.е. для чисто инфраструктурных услуг) все более или менее получится и над этим стоит работать. Вопросы типа «а где у вас тут покрытие и почему рвется соединение?» логичны, понятны и для специалистов в принципе решаемы. И на этом уровне нужно «пинать» операторов, дабы они улучшали указанное выше. Но для «настоящего современного качества» этого все равно будет недостаточно. Автор собственными ушами слышал, как один из действующих замминистров предлагал по сигналам снизу создавать так называемые карты качества и публиковать их везде, вплоть до салонов сотовой связи. Не только он подметил, что висающие повсюду карты покрытия порой неадекватны нашим ощущениям в тех же самых местах. И даже просто публикация реальной информации уже внесет беспокойство в ряды операторов, и им захочется что-то изменить в своих сетях.

В эпоху мультисервисных сетей (т.е. IP-трубы, в которую превратятся сети LTE-A/V) и стремительно растущей армии смартфонов клиент может потреблять из «общей трубы» одновременно несколько сервисов, имея свой индивидуальный профиль и свои особенности. Потребляемые им услуги и сопутствующие им проблемы (к примеру, время загрузки конкретной веб-страницы) могут не принадлежать ни данному оператору, ни его сети. А могут и принадлежать. При этом клиента не волнует технология, а только качество и тарифы. То есть клиент не понимает (и не должен понимать) разницу между инфраструктурными услугами и дополнительными сервисами. У него нет Скайпа, а

причиной этого отсутствия может быть что угодно, и даже не в РФ. Поэтому качество, за которое нужно бороться, принято сегодня обозначать словом «восприятие» и термином CE (Customer Experience).

Оператор, в свою очередь, может менять условия предоставления доступа конкретному клиенту – и по такой банальной причине, как «определенное качество в зависимости от тарифа» (или же для сохранения работоспособности сети при локальной перегрузке), и по вполне небанальной: куда-то приехало высокое начальство и в этой зоне на пару часов надо обеспечить суперкачество (да, остальные будут жаловаться, но «лосенок-то маленький» – на всех не хватит). Что интересно, клиент может быть удовлетворен и неважным качеством, если, к примеру, в момент деградации последнего у него будут облегченные тарифы. Тут действует схема, предложенная в свое время Кристианом Диором: если у вас кривые ноги – носите глубокое деколье.

Потенциал и риски

Измерить динамически меняющиеся параметры качества всех сервисов пытаться можно, но есть ли в этом смысл, если они у всех клиентов в каждый момент могут быть разные и это не свидетельствует однозначно о плохой или хорошей сети? Показателей качества, требующих измерения, наберется несколько десятков, и их будет необходимо контролировать во всех сетях связи во всех регионах страны (не исключая международные каналы, ведущие к зарубежным серверам). Дальнейшее развитие ИКТ еще больше усложняет какой-либо контроль «качества вообще». В частности, сегодня быстро развиваются облачные технологии и программно конфигурируемые сети, которые позволяют строить сеть поверх любой (своей, чужой) IP-инфраструктуры и дополнительно размыывают понятие «качество в конкретной сети». А с учетом трендов развития ИКТ-услуг у крупных операторов уже в ближайшем будущем не останется каких-либо пакетных продуктов, а будут предложения, которые годятся для всех клиентов, но имеют индивидуальные настройки. Это сделает бессмысленным общий контроль текущих технических характеристик в попытке оценить качество восприятия.

Кроме того, взаимодействие российских операторов с иностранными (международными) партнерами опирается на международные нормы, которые не требуют установления обязательного минимального уровня качества.

Допустим, все приведенные выше доводы несерьезны, и систему контроля будут-таки внедрять. Возникнут простые вопросы: сколько это займет времени, сколько будет стоить и кто за все это заплатит? Неужели на это есть бюджет? Или, может, стоит организовать еще и «фонд качества», куда все будут скидываться?

Кстати, большинство параметров качества услуг связи носят статистический характер, и «экспертный» метод их оценки не может не привести к большим и дорогостоящим ошибкам с точки зрения как «системы кон-

троля качества», так и неэффективных инвестиций операторов в реализацию необоснованно завышенных требований. Часто результат измерения напрямую зависит от применяемой методики. Да и вроде бы нигде за рубежом не применяют таких глобальных систем (видимо, по причине нецелесообразности), а существующие на предмет качества услуг документы МСЭ и ETSI носят лишь рекомендательный характер. Зато административный контроль показателей качества в отдельных странах есть, но он больше напоминает круглый стол (саморегулируемую организацию, СРО) регулятора и операторов, где собираются джентльмены и договариваются, как не обманывать своего потребителя (от рекламы и до реальных услуг). А то ведь последний по судам затаскает.

Заставить операторов сделать ресурс сетевой пропускной способности столь избыточным, чтобы хватило на любые скопления потенциальных пользователей с высоким качеством для всех услуг, также невозможно. Во-первых, никаких денег не хватит, во-вторых, никакой капиталист на это не пойдет, и в-третьих, не будем забывать и о радиочастотном дефиците, который удорожает инфраструктуру и который в мире никто не может отменить.

Что же касается качества восприятия, то, как уже говорилось, за него и следует бороться. Вот только чисто административные методы здесь не годятся. Потому что быть удовлетворенным «в среднем» принципиально многомерным сервисом индивидуальный клиент не может. Здесь нужен другой регуляторный подход, провоцирующий оператора на внутренний мониторинг качества его сервисов и одновременно выгодный ему (вообще «всем выгодно» – единственный реально работающий принцип, не накапливающий антагонизм между субъектами рынка), потому что у него появляется надежная обратная связь с потребителем. А это сегодня важно.

На что опереться?

До недавнего времени данная проблема «повисала в воздухе» (хотя впервые идея мониторинга качества обслуживания была сформулирована более 10 лет назад), однако за последние пару лет, когда разработчики научились переводить восприятие абонента в кон-

кретные интегральные технические характеристики сети связи, в этой области произошел ощутимый сдвиг. Сейчас у многих поставщиков имеются системы комплексного контроля качества, работающие сразу на трех уровнях: NPM (Network Performance Management – то, что использует каждый оператор для мониторинга сети), SQM (Service Quality Management – то, что позволяет судить о качестве какой-либо услуги «в среднем по палате») и CEM (Customer Experience Management – то самое вожделенное восприятие конкретной услуги конкретным абонентом, ключевые показатели которого исследуются и моделируются оператором). Кстати, результаты моделирования являются его интеллектуальной собственностью и не могут применяться «в среднем по палате».

В целом подобные системы могут осуществлять комплексный анализ сетевой информации для служб эксплуатации, маркетинга и развития, а также для страховых компаний. Оператор получает информацию о том, где на сети начинается деградация установленных его абонентами (именно для этого проводятся исследования и моделирование CE) норм качества и по какой причине. Он даже может начинать работать с жалобами еще до их реального появления. Он может понимать, как работают в его сети терминалы разных производителей и как нагружают сеть используемые приложения. И пр. и пр. Есть даже подозрение, что в обозримом будущем именно такие системы будут иметь двойное назначение, включив в себя функции COPM. Ведь принципы и результаты работы систем весьма похожи, а возможности велики. В общем, тут есть о чем подумать регулятору.

Необходимо также заметить, что внедрение указанных выше комплексных систем мониторинга качества обусловлено тем, что никакой инструментальный контроль показателей работоспособности сети или ее технических характеристик на уровнях NPM/SQM не дает комплексного представления об удовлетворенности клиента полученным сервисом или, что часто бывает, целой группой сервисов. Типичная ситуация – сеть работает хорошо, но клиенты все равно недовольны. К примеру, увеличилось время загрузки веб-страницы, что может быть вызвано сочетанием факторов или проблемами в сетях

Сделать
плохое качество
неконкуренто-
способным –
и есть наша
основная задача.
Это будет выгодно
и потребителям,
и операторам,
и регуляторам.

(серверах), находящихся даже в других странах и недоступных для отечественных надзорных органов. В этом случае конкретный оператор фактически не виноват (но формально будет привлечен к ответственности, несмотря на то что он «добрый католик»).

Еще в текущем регулировании ИКТ-отрасли наблюдается тренд постепенного отхода от технологий, сокращения количества лицензий на предоставление услуг (вплоть до единой мультисервисной) и регулирования исключительно инфраструктурного слоя, а не сервисного уровня, к которому во многом относятся обсуждаемые вопросы качества.

Так что же делать?

Целью всего действия, очевидно, должно быть повышение качества в ИКТ-отрасли на территории РФ, для чего нужно декларировать две подцели:

- повышение качества восприятия клиентом сервиса, поступающего из сети (сюда относятся все организационно-технические мероприятия по обеспечению качества в сети);
- улучшение восприятия клиентом качества обслуживания различными службами оператора при такой политике регулятора, которая позволяет гражданам получать сервисные предложения на конкурсной основе (как минимум, абоненту не должны хамить в контакт-центре, а мастер должен приходить не тогда, когда ему удобно, а когда это нужно клиенту).

В отношении технических характеристик качества услуг регулятор в первую очередь должен добиваться, чтобы операторская ИКТ-инфраструктура, на базе которой формируются ИКТ-сервисы, удовлетворяла обязательным требованиям, уже регламентированным в действующих НПА. Причем упомянутая в Концепции система хорошо впишется в слой инфраструктуры, используемой для контроля важнейших параметров сети сотовой связи, без поддержания которых говорить о качестве каких-либо дополнительных сервисов попросту бессмысленно. Это как раз на тот случай, когда «у всех плохо». Вот все и будут получать «на орехи» от надзора, пока хоть какое-то покрытие не появится (ведь про него в условиях лицензии должно быть что-то написано).

Что до использования систем комплексного мониторинга качества NPM/SQM/CEM, то регулятор может спровоцировать операторов на их установку, внося соответствующий пункт в лицензию или даже в будущую версию закона «О связи». Пусть операторы выдают в Роскомнадзор «картинку» из своего центра мониторинга с текущей ситуацией на сети – там все будет видно, всем будет удобно и меньше лишних вопросов. Можно и дальше пойти – стимулировать наличие у сервис-провайдеров систем управления информационной безопасностью. Ведь проблемы инфобезопасности с каждым днем становятся все актуальнее.

Кстати, наш регулятор уже заложил простую и одновременно эффективную регуляторную «бомбу» под неудовлетворительное качество связи с помощью планируемой к вводу услуги переносимости мобильного но-

мера (MNP). Теперь нелояльный клиент может легко «перепорхнуть» к другому оператору, где ему предоставят качество получше. И тогда за качество придется дополнительно бороться.

Как было объявлено, регулятор упростит создание ИКТ-инфраструктуры, и это тоже «шар в лузу» качества. Быть может, регулятор поразмышляет еще над одной «бомбой» – введением внутреннего межсетевого роуминга для того, чтобы «выпавшие» из сети (по причине отсутствия покрытия) клиенты могли воспользоваться услугами той сети, чей сигнал в данном месте лучше. За это на широких просторах нашей родины ему скажут спасибо миллионы граждан РФ – от автомобилистов, геологов и рыболовов до медиков, полицейских и сотрудников МЧС. Вообще любые действия регулятора, направленные на усиление конкуренции, провоцируют операторов на борьбу за лояльность клиентов, что означает и качество, и его более тщательный мониторинг, и дальнейшее развитие сети.

Создание СРО по качеству, составление «карт качества» по сигналам от потребителя – тоже хороший инструмент. Публиковать объективные данные о качестве оказываемых операторами услуг, получаемые как от операторов связи, так и от независимых организаций, можно, например, на веб-сайте Роскомнадзора. А те, кто добровольно подтверждает соответствие установленным СРО стандартам, могут снизить свои репутационные риски. Впрочем, механизм добровольной сертификации качества у нас уже существует, и его можно подкорректировать улучшением диалога участников рынка и Роскомнадзора.

Также регулятор должен контролировать своевременность информирования пользователей о существующих проблемах с оказанием услуг. Это укрепит доверие потребителя.

Основной идеей на пути повышения качества сервиса должно быть создание регулятором стимулов к этому самому повышению, но без установления каких-либо дополнительных барьеров для осуществления поставщиками услуг своей деятельности. Логика должна быть следующей: на действующих ИКТ-сетях поставщики услуг (не обязательно являющиеся операторами сетей) могут предоставлять сервис любого качества, но оно мониторится и широко освещается. Хорошее качество поощряется закономерными рыночными успехами, а плохое постепенно уходит с рынка, прежде всего из-за своей неконкурентоспособности. Собственно, сделать его неконкурентоспособным – и есть наша основная задача. Это будет выгодно и потребителям, и операторам, и регуляторам.



Вот такой ансамбль получился. Вкратце алгоритм его работы можно выразить народной мудростью: глупая женщина пытается перевоспитать мужчину, умная стремится его научить и только мудрая совершает почти невозможное – она оставляет его в покое, но создает ему определенную обстановку... ИКС

Академия совместимости



Созданное на стыке двух отраслей, оборонной и связной, ЗАО «Национальное РадиоТехническое Бюро» (НРТБ) за 13 лет стало крупнейшим экспертом в области исследований электромагнитной совместимости радиоэлектронных средств операторов связи и средств ВВС. С созданием сетей LTE НРТБ принимает новые вызовы, отмечает Виктор ПРИХОДЬКО, генеральный директор компании.

– НРТБ последовательно работало над вопросами ЭМС со стандартами GSM-900, GSM-1800, IMT-2000/UMTS (3G). Теперь очередь LTE. Насколько усложнилось обеспечение ЭМС РЭС для этих сетей?

– Мы имеем дело с принципиально новыми типами сигналов, влияние которых на РЭС как гражданского, так и военного назначения никто не проверял. Столь широкополосный сигнал – 5 МГц в диапазоне 800–900 МГц – не излучало ни одно средство. Были достаточно узкополосные сигналы 200 кГц, и их влияние – это одно, но на широкополосный сигнал приемник реагирует совершенно по-другому. Без необходимых исследований никто не сможет сказать точно, как сети LTE будут воздействовать на приемные устройства сетей ближней навигации и посадки, средства управления воздушным движением. НРТБ к таким исследованиям уже приступило.

– Речь идет о совершенно новом проекте?

– Да, это проект нынешнего года. Специалисты НРТБ с начала года активно включились в работу по исследованию влияния абонентских и базовых станций LTE на работу средств межсамолетной, а также ближней навигации и посадки. Для исследований задействовали как специальные имитаторы сигналов, так и реальные средства LTE, включая базовую станцию, размещенную на автомобиле КамАЗ. Исследованы характеристики излучений, построены математические модели трактов всех исследуемых приемных устройств. Определены защит-

ные отношения для достижения беспомеховой работы РЭС, рассмотрены все возможные варианты обеспечения условий совместного использования РЭС в отведенных полосах радиочастот. Сейчас мы готовимся представить первые результаты работы Союзу LTE.

Мы планируем в этом году в интересах Союза LTE провести комплекс исследований возможного влияния перспективных сетей LTE на все типы РЭС, работающие в полосах 800 МГц и 2,5–2,7 ГГц. Это прежде всего средства радиолокации, радиосвязи, ближней навигации и посадки, управления воздушным движением и другие. По результатам исследований могут быть разработаны конкретные рекомендации по условиям беспомеховой работы РЭС, путем доработок либо модернизации отдельных узлов, определяющих параметры излучения РЭС. Кроме того, мы готовим для операторов новинку – информационно-аналитические модели ЭМО для каждого субъекта федерации, что позволит им с высокой вероятностью планировать сети на перспективу до 2019 г.

– Но ведь работа с новым стандартом началась раньше, когда в 2012 г. по контрактам с «Ростелекомом» и «МегаФон» НРТБ обследовало электромагнитную обстановку для развертывания LTE в Краснодарском крае. Какие были получены результаты?

– Специалисты НРТБ провели комплекс натурных исследований в диапазонах 800–900 МГц и 2,5–2,7 ГГц в целях оценки возможности разверты-

вания сетей UMTS-900 и LTE в Краснодарском крае в интересах компаний, которые будут предоставлять услуги связи на Олимпиаде-2014. Мы определили и оценили тот частотный ресурс, который не был занят развернутыми РЭС различного назначения. На мой взгляд, этого недостаточно. Сети будут расти, и конечно, частотного ресурса скоро не будет хватать. Целесообразно продолжить работы, включая ряд организационно-технических мероприятий, что в значительной мере обеспечит потребности операторов в предоставлении высококачественных услуг связи.

– Если на одной и той же территории радиоэлектронные средства работают в совпадающих или близких полосах частот – взаимные помехи неизбежны?

– Их можно избежать. К слову, наши исследования показали, что в ряде случаев вполне возможно за счет проведения организационно-технических мероприятий (ОТМ) добиться того, чтобы даже радиоэлектронные средства LTE работали в одних полосах частот с другими РЭС, не создавая помех друг другу. Определить такую возможность позволяет разработанная и используемая в НРТБ комплексная взаимоувязанная система теоретических и экспериментальных натурных исследований.

Начинается все с детальных исследований и математического описания технических характеристик и особенностей РЭС рецепторов и источников помех. Далее проводится анализ и выбор моделей распространения радио-

сигналов, в том числе с учетом рекомендаций МСЭ. С использованием географических информационных систем строят цифровые модели рельефа местности и городской застройки исследуемой территории. Все это становится частью программно реализованных высокопроизводительных комплексов расчета условий ЭМС РЭС, созданных на основе современных информационных технологий. В дальнейшем математические модели калибруют по результатам экспериментальных натурных исследований. Программные комплексы сертифицируют, на них получают Свидетельства о государственной регистрации программ на ЭВМ.

Таким образом, по результатам теоретических исследований принимается решение о целесообразности проведения ОТМ (пример: оборудование базовых станций устройствами, изменяющими «Х» поляризацию на «V») и о способе проведения натурных экспериментальных исследований (с использованием летных или мобильных лабораторий) для подтверждения или достижения возможности совместной работы исследуемых РЭС.

– В натурных испытаниях НРТБ опирается на летные и мобильные лаборатории, оснащенные различным оборудованием. Какое программное обеспечение используется для совместной работы всех этих приборов?

– Специалистами НРТБ были разработаны и оборудованы летающая лаборатория на базе самолета ЯК-40, беспилотный комплекс измерения параметров электромагнитной обстановки на высотах до 600 м, три наземные подвижные лаборатории. НРТБ использует самые совершенные на сегодняшний день измерительные приборы, анализаторы спектра, генераторы сигналов, анализаторы сетей GSM, IMT-2000/UMTS, LTE, с помощью которых мы проводим натурные и лабораторные исследования.

Мы используем программное обеспечение собственной разработки, которое позволяет добиться требуемых нам функциональных возможностей и удобства работы. Оно обеспечивает управление измерительным оборудованием летных и мобильных лабора-

торий, сохранение результатов изменений параметров электромагнитной обстановки в базе данных для последующего анализа и отображения на электронной карте местности, а также оценку качества работы средств навигации посадки аэродрома и их подверженности помехам.

Мы не останавливаемся только на оценке работы действующих средств посадки, а создаем собственные. Нашими специалистами разработан современный маяк для ближней навигации посадки, который, надеемся, придет на смену действующим на аэродромах маякам, работающим в международном диапазоне частот.

Наш маяк не только передает самолету сигнал как ориентировочную ситуацию, но дает полную информацию о состоянии аэродрома, его координатах, о погоде, атмосферном давлении, ветре. Действующие сегодня маяки сравнимы по массе с автомобильным прицепом, а наша разработка – переносной ящик весом 16 кг, у которого и мощность больше, и эффективность выше. Недавно он прошел испытания на аэродроме в Мигалово, и представители нескольких военных заводов очень заинтересовались этой разработкой.

– Военные заводы хотят ее купить?

– К сожалению, есть проблема с передачей Минобороны права серийно выпускать наше оборудование. По закону «О госзаказе» ставить на вооружение можно только те средства, которые разработаны в рамках гособоронзаказа и финансировались из бюджета. Мы готовы сотрудничать и передать эту технологию, как и целый ряд других инновационных разработок, но сегодня даже просто отдать их не имеем возможности, нет такого инструментария.

Вообще, у НРТБ 86 патентов РФ на изобретения. Поэтому мы надеемся, что в законодательство будут внесены изменения, будет принят закон «О частно-государственном партнерстве», а наши продукты будут приносить пользу государству.

– Не планируете выпускать свои продукты на собственных производственных мощностях или продавать разработки невоенным заводам?

– Мы не в состоянии выпускать продукцию серийно, у нас нет производственных площадей. Но до уровня макетирования доводим продукты самостоятельно. Естественно, макет собирается из стандартных компонентов, которые мы закупаем, поскольку нет возможности разработать всю номенклатуру составляющих элементов, да это и не нужно. Изобретения и интеллектуальная собственность – в ноу-хау, а не в компонентах. Когда макет собран, формируется рабочая конструкторская документация и проводятся испытания. А если к нам обращается завод, который хочет серийно производить наш продукт, для него конструкторская документация разрабатывается отдельно.

– Таким количеством патентов может гордиться любой R&D-центр, а НРТБ – сравнительно небольшая компания, к тому же с несколько иным профилем бизнеса. Чем объяснить столь высокую исследовательскую активность?

– Конечно, патенты не самоцель. Но в НРТБ уникальный высокопрофессиональный коллектив, пять докторов наук, 14 кандидатов технических наук. У нас собраны специалисты высокого уровня подготовки, инженерные кадры, математики-программисты, специалисты по сигналам. Среди менеджеров – выходцы из Министерства обороны, Вооруженных сил (разных родов войск – ПВО, управление радиоэлектронной борьбы, космические войска, ракетно-космическая оборона).

Что касается патентов, то, к сожалению, чтобы защитить одну идею, приходится оформлять пять-семь патентов. Если на Западе при патентовании элемент сходства рассматривается очень внимательно и широко, то система патентования в нашей стране позволяет присвоить чужую идею, вписав в заявку три новых слова. Поэтому нужно предусмотреть все варианты таких «трех слов» и обеспечить идею круговую защиту. Так что, честно говоря, собственно идей у нас меньше, но мы их защищаем – и с этими идеями пытаемся «достучаться до небес».



www.nrtb.ru
+7 (495) 748-3187

От интернета людей – к интернету вещей



**Михаил
САМСОНОВ,**
вице-президент,
ГК «Старт»



**Александр
РОСЛЯКОВ,**
заместитель
директора
филиала
по перспективным
разработкам,
ГК «Старт»



**Сергей
ВАНЯШИН,**
ведущий
инженер-
проектировщик,
ГК «Старт»

Число подключенных к интернету технических устройств уже несколько лет назад превысило число людей. А к 2015 г., по прогнозам, на каждого жителя Земли будет приходиться больше двух таких устройств. «Интернет вещей» – новый этап эволюционного развития Сети, способный заметно изменить нашу жизнь.

Идея «интернета вещей» сама по себе очень проста. Представьте себе, что все предметы (домашние приборы и утварь, одежда, продукты, автомобили, промышленное оборудование и т.п.) снабжены миниатюрными идентификационными устройствами. Очевидно, что вся наша повседневная жизнь тогда преобразится. Уйдут в прошлое кражи, дефициты товаров, их перепроизводство, поскольку будет точно известно, что, в каком месте и в каком количестве производится и потребляется. Если все объекты повседневной жизни будут снабжены миниатюрными радиометками, то их можно будет дистанционно идентифицировать, а при наличии определенного «интеллекта» – и управлять ими.

И вот если задачи адресации всех радиометок-объектов и передачи информации между ними возложить на протокол IP версии 6 (IPv6), то и получится новый интернет – интернет вещей.

Как возник интернет вещей

В начале нового тысячелетия в связи с бурным развитием пакетных сетей и прежде всего интернета мировое телекоммуникационное сообщество предложило новую парадигму реализации коммуникаций на базе пакетных способов передачи информации – сети следующего поколения NGN (Next Generation Networks). Технологии NGN прошли определенный эволюционный путь от гибких коммутаторов

(Softswitch) до подсистем мультимедийной связи IMS (IP Multimedia Subsystem) и мобильных сетей долговременной эволюции LTE (Long Term Evolution). При этом всегда предполагалось, что основными пользователями таких сетей будут люди, следовательно, максимальное число абонентов в них будет ограничено численностью населения планеты Земля.

Однако в последнее время получили развитие методы радиочастотной идентификации RFID (Radio Frequency Identification), беспроводные сенсорные сети WSN (Wireless Sensor Network), коммуникации ближнего поля NFC (Near Field Communication) и межмашинные коммуникации M2M (Machine-to-Machine), совместно с интернетом обеспечивающие простую связь различных технических устройств («вещей»), число которых может быть огромным. По данным экспертов, в промежутке между 2008 и 2009 гг. количество подключенных к интернету предметов превысило количество людей. А уже к 2015 г., как прогнозируют эксперты, на каждого человека будет приходиться более двух таких устройств. Таким образом, в настоящее время происходит эволюционный переход от «интернета людей» к «интернету вещей».

Концепция сетей NGN предполагала возможность коммуникаций людей (непосредственно или через компьютеры) в любое время и в любой точке пространства. Концепция интернета вещей

Интернет вещей: договоримся о терминах

Официальное определение приведено в Рекомендации МСЭ-T Y.2060, Overview of the Internet of Things, согласно которой интернет вещей (Internet of Things, IoT) – это глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий.

Под «вещами» здесь понимается физический объект (физическая вещь) или объект виртуального (информационного) мира (виртуальная вещь, например мультимедийный контент или прикладная программа), которые могут быть идентифицированы и объединены через коммуникационные сети. Таким образом, интернет вещей в долгосрочной перспективе может рассматриваться как направление технологического и социального развития человеческого общества.

Рис. 1. Новое направление коммуникаций, реализуемое интернетом вещей



включает еще одно направление – коммуникация любых устройств, или вещей (рис. 1).

Базовые технологии

Интернет вещей – это технологическая революция, которая представляет собой будущее вычислений и коммуникаций, и ее развитие зависит от технических инноваций в нескольких важных областях.

Во-первых, для того, чтобы подсоединить вещи к интернету, необходима простая и эффективная по затратам система передачи информации и идентификации вещей. Такую возможность и необходимый функционал предоставляют различные пассивные и активные беспроводные технологии: RFID, NFC, Wi-Fi и др.

Во-вторых, польза от собранных данных о вещах проявится, только если есть возможность отслеживать изменения в физическом статусе вещей (в пространстве и во времени). Для этого используются различные сенсорные технологии.

В-третьих, чип в любой продукт будет встраиваться уже на этапе производства, и встроенный в вещи «интеллект» («умные» вещи) позволит принимать сложные и даже независимые решения.

И наконец, миниатюризация и нанотехнологии обеспечивают все более и более мелким вещам возможность экономичной коммуникации и взаимодействия между собой. Например, для приложений автоматизации дома, офиса и производства, которым достаточно беспроводного подключения к интернету с низкой скоростью передачи данных для устройств с ограниченными возможностями производительности и мощности, может использоваться технология 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), которая обеспечивает взаимодействие по протоколу IPv6 поверх маломощных беспроводных персональных сетей стандарта IEEE 802.15.4.

Комбинация всех этих технологий и приведет к созданию интернета вещей, который соединит объекты окружающего нас физического и виртуального миров.

Стандартизация

В рамках МСЭ с 2006 г. действует Глобальная инициатива по стандартизации интернета вещей, которая со-

действует унифицированному подходу к разработке технических стандартов в этой области. В рамках серии Рекомендаций Y.2xxx, относящейся к сетям следующего поколения NGN, уже утверждены рекомендации, посвященные специально интернету вещей: ITU-T Y.2060, Overview of the Internet of Things («Обзор интернета вещей»); ITU-T Y.2063, Framework of Web of Things («Основа Web-сети вещей»); ITU-T Y.2069, Terms and definitions of the Internet of Things («Термины и определения интернета вещей»). В последние годы принят также ряд рекомендаций МСЭ-Т в смежных областях, которые применимы к интернету вещей (Y.2061, Y.2062, серия H.642.x, F.747.1 и др.).

В рамках Всемирного консорциума по стандартизации в области информационных технологий создан глобальный Партнерский проект oneM2M, который занимается разработкой систем межмашинных коммуникаций.

Группа из 25 ведущих поставщиков и пользователей новых технологий (Bosch, Cisco, Ericsson, Fujitsu, Oracle, SAP, Sun и др.) сформировала в 2008 г. альянс IPSO (IP for Smart Objects), который прорабатывает вопросы использования протокола IP для подключения «умных» объектов (сенсоров и активаторов, датчиков и исполнительных устройств) и передачи информации, собранной этими устройствами.

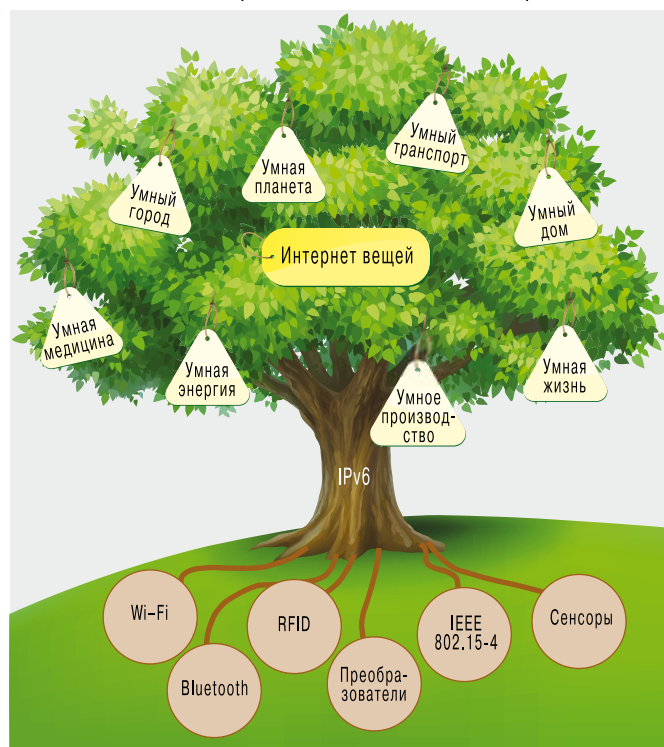
Европейский интеграционный проект IoT-A (Internet-of-Things Architecture) направлен на создание архитектуры эталонной модели интернета вещей и ее ключевых компонентов.

Умные приложения

На основе интернета вещей могут быть реализованы всевозможные умные приложения в различных сферах деятельности и жизни человека (рис. 2).

- «Умная планета» – человек сможет буквально «держатъ руку на пульсе» планеты: своевременно реагировать на упущения в планировании хозяйств, загрязнения и другие экологические проблемы, а значит, эффективно распоряжаться невозобновляемыми ресурсами.
- «Умный город» – городская инфраструктура и сопутствующие муниципальные услуги, такие как образование, здравоохранение, общественная безопасность, ЖКХ, станут более связанными и эффективными.
- «Умный дом» – система будет распознавать конкретные ситуации, происходящие в доме, и реагировать на них соответствующим образом, что обеспечит жильцам безопасность, комфорт и ресурсосбережение.
- «Умная энергетика» – будет обеспечена надежная и качественная передача электрической энергии от источника к приемнику в нужное время и в необходимом количестве.
- «Умный транспорт» – перемещение пассажиров из одной точки пространства в другую станет удобнее, быстрее и безопаснее.
- «Умная медицина» – врачи и пациенты смогут получить удаленный доступ к дорогостоящему меди-

Рис. 2. «Умные приложения» на основе Интернета вещей



цинскому оборудованию или к электронной истории болезни в любом месте, будет реализована система удаленного мониторинга состояния здоровья, автоматизирована выдача лекарственных препаратов больным и многое другое.

Сегодня и завтра: планы внедрения

Возможности интернета вещей в области генерирования, сбора, передачи, анализа и распределения огромного объема данных в мировом масштабе позволят человечеству в конечном счете получить новые знания, которые необходимы ему не только лишь для выживания, но и для настоящего процветания на протяжении многих веков. Подтверждение этому – включение интернета вещей в перечень прорывных технологий в США и в число семи формирующихся национальных стратегических отраслей промышленности в Китае.

Единые стандарты только зарождаются, но масштабные проекты в данном направлении – своего рода «интранеты вещей» – энергично развиваются уже сейчас. Так, американское агентство NASA при поддержке компании Cisco создает систему глобального сбора данных о Земле «Кожа планеты» (Planetary skin). Про умные дома наверняка многие слышали, в Японии уже не редкость умные заводы, а в США в рамках национальной инициативы оцифровки мегаполисов Connected Urban Development «умнеют» и города.

В разных странах существуют конкретные программы и планы практического внедрения интернета вещей. Так, Евросоюз развивает интернет вещей по специальной программе, включающей 14 направлений. Согласно китайской государственной программе до 2015 г. планируется реализовать 149 проектов, от иссле-

дований и проектирования оригинальных RFID-чипов, смарт-карт и беспроводных устройств до масштабных систем интеллектуальной логистики и транспорта. Не менее активно ведутся разработки в Великобритании, Австралии, Японии, Южной Корее и других странах.

Что мешает развитию?

Широкому внедрению интернета вещей препятствуют сложные технические и организационные проблемы, в частности, связанные со стандартизацией. Единых стандартов для интернета вещей пока нет. Сильнее всего глобальному внедрению препятствует расплывчатость формулировок концепции интернета вещей и большое число регуляторов и их нормативных актов.

К факторам, замедляющим развитие интернета вещей, следует отнести сложности перехода существующего интернета к новой, 6-й версии сетевого протокола IP, прежде всего необходимость больших финансовых затрат со стороны телекоммуникационных операторов и провайдеров услуг на модернизацию своего сетевого оборудования.

Существует серьезная проблема, связанная с вторжением интернета вещей в частную жизнь. Возможность отслеживать местонахождение людей и их собственности ставит вопрос о том, в чьем распоряжении окажутся эти сведения. Кто будет нести ответственность за хранение информации, собранной «умными вещами»? Кому и на каких условиях будет предоставляться эта информация? Можно ли ее собирать без согласия человека? Все эти вопросы пока остаются открытыми.

Кроме того, с появлением интернета вещей возникнет необходимость изменения общепринятых и проверенных бизнес-процессов и стратегий, что может привести к значительным финансовым затратам и рискам.

С чего начать?

Интернет вещей – это новый этап эволюционного развития интернета, характеризующийся тем, что разнородным сетям и множеству датчиков предстоит объединиться для взаимодействия под управлением единых стандартов. Эта задача требует от научно-исследовательских институтов, органов стандартизации, коммерческих организаций, государственных учреждений и учебных заведений общих усилий, направленных на достижение единой цели. Чтобы интернет вещей обрел популярность у пользователей, операторы связи, контент-провайдеры и другие участники рынка должны прежде всего разработать приложения, повышающие качество жизни простых граждан. Наиболее перспективными направлениями для внедрения интернета вещей являются энергоэффективность (Smart Grid и Smart Home), сферы логистики и торговли, персональная безопасность, получение услуг в сфере образования, здравоохранения, ЖКХ и взаимодействие с местными властями.

Интернет вещей не должен стать технологией ради технологии. Задача инфокоммуникационной отрасли – продемонстрировать его ценность для каждого человека. И тогда с интернетом вещей в нашу жизнь – в который уже раз – войдет много нового и интересного. ИКС

Фемтосоты forever

Регуляторные изменения, позволившие использовать маломощные РЭС без получения дополнительного разрешения, наконец сделали более открытым рынок фемтосот. Результат не заставил себя ждать: на рынке появляются новые игроки. Подробности – от Владимира АЛФЕРЬЕВА, заместителя директора по продукции ZyXEL Россия.



Владимир
АЛФЕРЬЕВ

– Как вы оцениваете состояние российского рынка фемтосот, в частности для сетей 3G?

– Рынок фемтосот 3G остается в статусе перспективного направления в России. Несмотря на то что уже много лет эта тема в поле зрения операторов и фемтосоты находятся в коммерческой доступности, за все предыдущие годы на стороне пользователей было установлено

всего несколько тысяч фемтосот. Это капля в море по сравнению с несколькими миллионами инсталляций по миру (по данным Small Cell Forum и Infonetics Research). Тем не менее текущая ситуация в России остается оптимистичной для развертывания малых сот: много зон, где базовые станции операторов перегружены трафиком 3G, и фемтосоты могли бы разгрузить их. Кроме того, в офисах и квартирах, где сигнал неустойчив, фемтосота способна обеспечить качественную мобильную связь сразу для нескольких абонентов. Недавно процесс регистрации фемтосот был упрощен. Теперь многое зависит от того, насколько агрессивен оператор будет предлагать услугу установки фемтосот. От абонента требуется только наличие подключения к интернету.

– Какова мотивация решения вашей компании выйти на рынок фемтосот?

– Исторически ZyXEL разрабатывал абонентские устройства для доступа в интернет, а фемтосоты как раз из этого класса. На разработку и производство фемтосот нас подвигли операторы, с которыми мы сотрудничаем. Причем фемтосоты, в которых они заинтересованы, не ограничиваются одной моделью: поставщики телеком-услуг проявляют интерес и к интегрированным устройствам – чтобы одна коробочка совмещала бы в себе и фемтосоту, и шлюз для подключения к проводному оператору со встроенным коммутатором и точкой доступа Wi-Fi.

– Какие актуальные потребительские ниши видите для оборудования фемтосот?

– Спрос на фемтосоты в России ожидаем со стороны домашних пользователей – жителей квартир и загородных домов, а также небольших офисов с неуверенным приемом сигнала связи, для которых главными критериями являются минимальная цена и простота установки. Для оператора преимущество такой услуги заключается в сокращении затрат на улучшение покрытия проб-

лемных зон, включая общественные места, и в получении дополнительного дохода от абонента, скажем, в результате увеличения трафика данных. Модель продаж подразумевает предложение этой услуги и продажу фемтосоты со стороны оператора – именно он является ключевым звеном в привлечении абонента.

– Какова роль партнерства в индустрии оборудования фемтосот?

– Работоспособность фемтосоты требует установки инфраструктурного оборудования на стороне оператора. Этим обстоятельством и обусловлено партнерство производителя сетевого оборудования и компании, специализирующейся на решениях доступа, с целью предоставить оператору объединенное решение. Пример такого партнерства в сфере разработки и производства оборудования фемтосот демонстрируют ZyXEL и ALU – наши компетенции дополняют друг друга. Другими словами, каждый производитель занимается тем, что исторически умеет хорошо делать, и такой подход является эффективным и результативным.

– Куда направлен вектор технологического развития фемтосот?

– Фемтосоты являются готовым законченным решением, которым пользуются миллионы абонентов в мире. Рост абонентской базы в ближайшие годы продолжится. Фемтосота не требует от пользователя администрирования, управление происходит удаленно, со стороны оператора. Победителями среди производителей будут компании, которые смогут предложить устройства с набором интерфейсов и функций, наиболее востребованным заказчиком. А у каждого из них своя специфика. Возьмем, к примеру, российских операторов. «Билайн» предоставляет проводной доступ в Сеть по технологии Ethernet, и ему интересен шлюз и фемтосота с интерфейсом Ethernet. «Ростелеком» в одних регионах предоставляет доступ по xDSL, а в других – по Ethernet, поэтому шлюз доступа и фемтосота должны иметь соответствующий интерфейс.

– Каковы перспективы фемтосот в применении к сетям 4G?

– Несомненно, фемтосоты будут востребованы в сетях LTE и LTE Advanced. В России операторы устанавливают базовые станции LTE на тех же площадках, где расположены БС 2G и 3G. Помимо того, что есть зоны с неустойчивой связью в силу неполного покрытия LTE, в таких сетях нередки перегрузки, и фемтосоты помогут разгрузить сеть и обеспечить качественную услугу абонентам. Взрывной рост передачи данных в сетях 3G и 4G является еще одним драйвером продвижения фемтосот, мы сейчас активно разрабатываем фемтосоты для сетей LTE в дополнение к уже предлагаемым моделям 3G.

Вопросы задавала **Наталья КИЙ**

Спутниковый мониторинг на транспорте. Как выбрать?

Растущую популярность систем мониторинга транспорта и контроля расхода топлива нетрудно объяснить: они позволяют оптимизировать затраты и повысить эффективность работы транспорта. Но чтобы выбрать подходящее для конкретной компании решение, нужно понимать, что предлагает рынок.



Станислав
ЕМЕЛЬЯНОВ,
заместитель
генерального
директора,
Omnicomm

Спутниковые системы мониторинга в их современном виде впервые появились у нас в начале 2000-х, а с 2005 г. они стали использоваться как инструмент оптимизации бизнеса, но внедрялись в небольших объемах. Можно сказать, что с этого момента началось формирование рынка систем мониторинга транспорта в странах СНГ. На сегодняшний день он насчитывает более 200 игроков, совокупное число их дилеров – более 1000. И 89% этих компаний полагают, что рынок будет расти и

впредь. Эксперты отрасли, в свою очередь, предсказывают ему бурный рост еще как минимум пять лет.

На базе спутниковых систем создается все больше продуктов и сервисов для автопарков как крупных, так и небольших компаний. Есть и поддержка со стороны правительства в виде государственных программ («ЭРА-ГЛОНАСС», проект системы сбора платежей за проезд 12-тонных автомобилей по федеральным трассам с использованием ГЛОНАСС).

Главные факторы роста популярности спутникового мониторинга – оптимизация бизнеса, снижение издержек, повышение эффективности работы транспорта. Кроме того, спутниковый мониторинг помогает предотвратить воровство (например, топлива), а это, к сожалению, традиционная российская проблема. Если учесть, что расходы на топливо в себестоимости пробега автомобиля достигают 40% и более, введение контроля этих расходов дает возможность увеличить прибыль перевозчика как минимум на 15–20%.

Мониторинг транспорта повышает прозрачность бизнес-процессов компании. Ведь на эффективность использования автопарка влияют не только водители: это и механики, которые следят за состоянием машины и должны вовремя проводить профилактику и ТО, и экспедиторы, которые дают водителям задание на работу. Объективные показатели по местоположению и маршруту, пробегу и расходу горючего служат базой для анализа работы всех звеньев компании, повышают

дисциплину, позволяют эффективно мотивировать сотрудников.

Стоимость системы по отношению к получаемой эффективности для всего автопарка зависит в первую очередь от объема потребления топлива. Также очень важно качество управления парком транспортных средств. В среднем установка системы мониторинга транспорта окупается за два–четыре месяца.

Немного о рынке

По оценке аналитического центра Omnicomm, объем мирового рынка М2М-оборудования на коммерческом транспорте составляет около \$2,7 млрд, а объем рынка оборудования для мониторинга транспорта в РФ в 2012 г. достиг \$150 млн. Таким образом, доля российского рынка – около 6% мирового. Лидеры отечественного рынка оборудования для мониторинга транспорта – компании «Техноком» и Omnicomm, которые произвели примерно по 300 тыс. штук бортовых терминалов и датчиков уровня, – работают и на европейском рынке, равно как и группа компаний НИС М2М, занимающая по обороту около 30% российского рынка мониторинга.

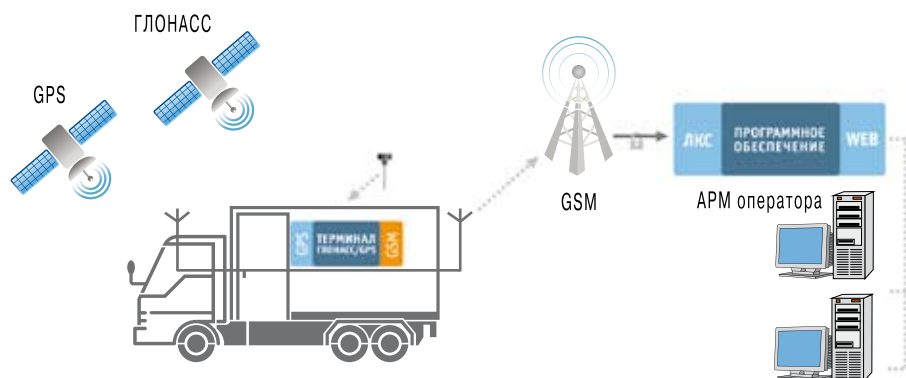
Емкость российского рынка датчиков уровня топлива оценивается в 200 тыс. штук, а систем мониторинга транспорта – 400 тыс. терминалов. Спутниковый мониторинг востребован во всех сегментах транспортной отрасли, а топливные датчики – в промышленном, транспортном и гражданском строительстве, нефтегазовой и горнодобывающей промышленности, т.е. в тех отраслях, которые потребляют много топлива. Сравнивать это направ-

Посчитаем



Допустим, компания решила оснастить системой мониторинга и контроля расхода топлива 98 единиц транспортных средств и спецтехники предприятия нефтегазовой промышленности: 18 трубоукладчиков, 13 бульдозеров, 10 экскаваторов, 14 агрегатов для сварки трубопроводов, 35 единиц различной колесной техники, 8 автотопливозаправщиков. На их оснащение потратили 3,283 млн руб. Экономия на ГСМ, а также совокупная стоимость несанкционированно расходуемого топлива за первый месяц эксплуатации системы составит 1,014 млн руб. Таким образом, срок окупаемости системы только за счет сокращения расходов на ГСМ – чуть больше трех месяцев. При этом снижаются простои техники и, как правило, выявляются случаи недолива топлива на АЗС (последнее особенно важно: зачастую в низкой эффективности транспорта стремятся обвинить водителей, а потом обнаруживаются случаи хищения топлива – недобросовестная работа автозаправщиков).

Рис. 1. Схема работы при повышенных требованиях к безопасности



ление деятельности с другими сегментами ИТ/телекома и по объемам, и по темпам роста не совсем корректно, поскольку, во-первых, это не массовый потребительский рынок, а во-вторых, сами системы не являются коробочным продуктом, они представляют собой решение, внедряемое на предприятиях проектным методом.

Как работает мониторинг

Спутниковых систем мониторинга и управления транспортом существует множество разновидностей. И на первый взгляд все они используют один принцип и имеют практически одинаковые функции.

Система мониторинга транспорта представляет собой программно-аппаратный комплекс, состоящий из двух частей – навигационной и коммуникационной. Навигационная часть – это все, что отвечает за позиционирование, определение координат транспортного средства, скорости, пройденного пути и прочих параметров движения. Аппаратная составляющая навигационной части – спутниковый приемник GPS или ГЛОНАСС/GPS. Помимо навигационных данных, системы позволяют собирать с автомобиля значения эксплуатационных параметров, такие как расход топлива, сведения о работе различных узлов и агрегатов авто-

мобиля, об их техническом состоянии. Для сбора данных об эксплуатационных параметрах обычно требуется подключить к автомобильному терминалу различные датчики и устройства.

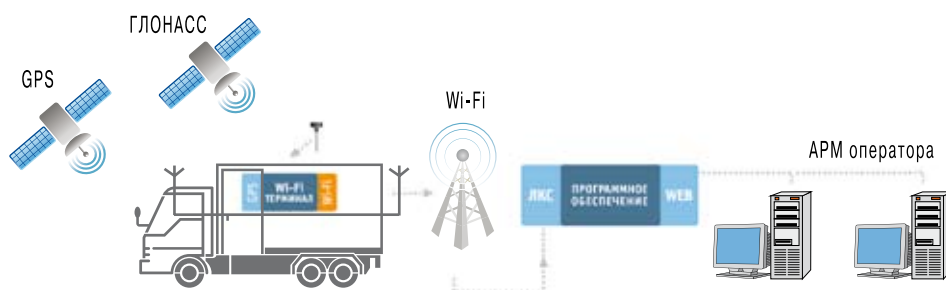
Существует несколько схем работы системы.

Схема 1 – базовая. Установленные на транспортные средства терминалы передают данные на коммуникационный сервер через интернет с использованием GSM или Wi-Fi. Диспетчерский сервер клиента загружает данные с коммуникационного сервера.

Схема 2 – если высоки требования к безопасности. Применяется, если клиенту из соображений безопасности требуется разместить все компоненты системы в контролируемой сети (рис. 1). При этом для передачи данных не используется интернет (за исключением передачи через VPN-канал). Терминалы передают данные на локальный коммуникационный сервер с использованием предоставляемого оператором сотовой связи VPN-туннеля или физического выделенного канала. Диспетчерский сервер клиента загружает данные с локального коммуникационного сервера.

Схема 3 – если нет GSM-покрытия. Применяется, если в районах использования транспортных средств отсутствует покрытие GSM-сетей, но предполагает-

Рис. 2. Схема работы в отсутствие покрытия сотовой сети



Участники рынка М2М-терминалов и спутникового мониторинга (Россия и СНГ)

Компании и решения перечислены в порядке уменьшения рыночной доли в количественном выражении (по числу установленных бортовых терминалов) по итогам 2012 г.

Производители терминалов М2М

- ✓ «Техноком» (Челябинск)
- ✓ «М2М телематика» (Москва)
- ✓ «Русские навигационные технологии» (Москва)
- ✓ Teltonika (Вильнюс)
- ✓ «ГалилеоСкай» (Пермь)
- ✓ «Скаут» (Санкт-Петербург)
- ✓ Omnicomm (Москва)

Производители датчиков уровня топлива

- ✓ Omnicomm (Москва)
- ✓ «Технотон» (Минск)
- ✓ «Сапсан» (Челябинск)
- ✓ «Русские навигационные технологии» (Москва)
- ✓ РКС (Киев)

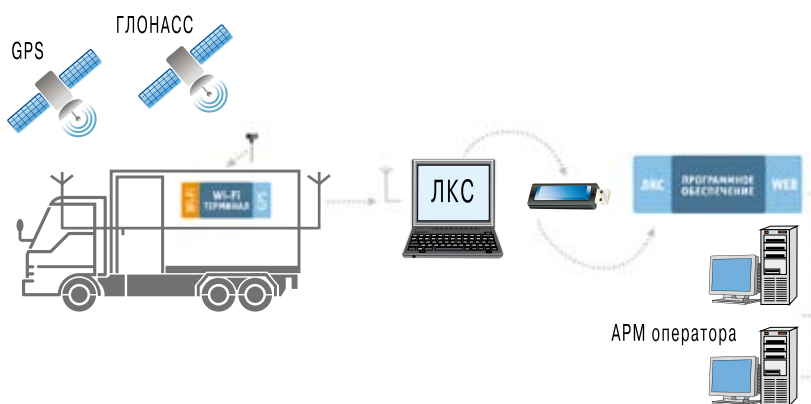
Российские системы мониторинга транспорта

- ✓ «Автограф» («Техноком», Челябинск)
- ✓ Система компании «М2М телематика» (Москва)
- ✓ «Автотрекер» («Русские навигационные технологии», Москва)
- ✓ «Скаут» («Скаут», Санкт-Петербург)
- ✓ Omnicomm (Omnicomm, Москва)

Российские датчики уровня топлива

- ✓ Omnicomm LLS (Omnicomm, Москва)
- ✓ «Стрела» («Сапсан», Челябинск)
- ✓ AT-FLM («Русские навигационные технологии», Москва)

Источник:
аналитический центр Omnicomm.

Рис. 3. Схема работы в удаленных районах в отсутствие инфраструктуры

ся наличие локальной сети или интернета и возможность стационарной установки считывающего оборудования (рис. 2). Установленные на транспортные средства терминалы во время работы собирают и накапливают данные. При входе в зону действия сети Wi-Fi (при въезде в гараж, проезде через ворота базы и т.д.) терминалы передают накопленный архив на коммуникационный сервер или локальный коммуникационный сервер через интернет либо локальную сеть. Диспетчерский сервер клиента загружает данные с коммуникационного сервера.

Схема 4 – если нет инфраструктуры. Применяется в случае отсутствия в районе работы техники как покрытия сотовых сетей, так и любых других каналов передачи данных (рис. 3). Терминалы во время работы собирают и накапливают данные. Периодически накопленные данные передаются через Wi-Fi-канал на локальный коммуникационный сервер, установленный на ноутбуке. Затем данные любым способом (через внешний USB-носитель, компакт-диск или вместе с ноутбуком) передаются в офис клиента, где переносятся на коммуникационный сервер или сразу на диспетчерский сервер клиента.

Что важно знать при выборе

Будущему пользователю систем изначально необходимо решить, какие параметры работы машин для него критично важно контролировать. Для спецтехники, к примеру, актуальнее всего контроль заправок и сливов, а также отслеживание времени работы и простоя. Для

компаний-перевозчиков хищения топлива несколько менее важны, зато необходим контроль пробега единицы техники и отслеживание маршрута ее перемещений для оптимизации логистических схем.

В российских условиях для развертывания эффективной системы контроля техники критичны следующие параметры:

- точность показаний;
- адекватное ПО, выводящее информацию в пригодном для анализа виде;
- вандалоустойчивость;
- устойчивость к термическим и вибрационным воздействиям (для карьерной техники).

Как показывает практика, решающим фактором при выборе системы контроля является итоговая эффективность ее внедрения. К примеру, на рынке существует множество сходных систем мониторинга, однако при большой вариации стоимости далеко не все из них оказываются эффективными. Низкая цена не может служить основным критерием эффективности: как правило, это показатель недоработанности системы, некачественной технической поддержки и сервиса. Именно поэтому только тестирование различных систем в реальных условиях, на технике предприятия может дать ответ на вопрос, на какой из них остановить выбор.

К примеру, существуют системы, обеспечивающие полный контроль за сливами и заправками, скоростью и пробегом, маршрутом и местоположением, временем работы или простоя техники. Подавляющую часть строительных, добывающих и

нефтегазовых компаний полностью устраивает такой функционал.

Отечественные реалии таковы, что зачастую прямые пользователи систем – обслуживающий персонал, водители – выступают против инновационных технологий. Нередко их активность принимает весьма разрушительные формы, вплоть до вывода оборудования из строя. Но и это учтено в последних отечественных разработках, которые имеют надежную защищенность от вандалов. Есть терминалы в металлическом корпусе, защищенные от всех видов помех, есть оборудование, устойчивое к пожарам и взрывам. Любые попытки нарушения связи компонентов однозначно фиксируются в системе.

И о перспективах

Количество техники, подлежащей оснащению навигационными системами, исчисляется миллионами. В настоящий момент в России системами мониторинга оснащено порядка 800 тыс. единиц транспорта, и динамика роста приближается к 100% в год. Для сравнения: в странах ЕС, по оценке Berg Insight, в 2010 г. системами мониторинга оснащено более 1 млн машин; прогноз на 2014 г. – более 16 млн оснащений.

Потребители телематических систем с каждым годом становятся все более требовательными к качеству и функционалу, поэтому одним из главных направлений развития отечественного рынка систем мониторинга транспорта является создание максимально универсальных и простых в использовании решений, удовлетворяющих быстрорастущие запросы рынка транспорта.

Основными сферами развития и использования систем спутникового мониторинга в ближайшие три-четыре года станут безопасность при перевозках и на транспорте, страхование и налогообложение, где системы мониторинга могут и должны быть задействованы в обязательном порядке. Их развитие неразрывно связано и с господдержкой отечественной системы ГЛОНАСС. Инновационные и технологические достижения в области спутникового мониторинга транспорта уже невозможно игнорировать. ИКС

70 Е. ВОЛЫНКИНА. Облака, мобильность и лично-корпоративный диссонанс
75 В. ШЕПЕЛЕВ. Liebert PCW: точное охлаждение для облачных сред, обеспечивающее максимальную экономию энергии

76 Революция в построении ЦОДов
77 Телекоммуникационное оборудование «Энергомера» – качественно, надежно, перспективно

80 Э. АЛЕХИН. Квалифицированный персонал – основа операционной устойчивости ЦОДа
85 П. КАНЕВ. Формализуем работу ИТ-подразделений

88 М. БАЛКАРОВ. Некоторые особенности проектирования чиллерных систем
91 П. КОСТЮРИН. Аудит инженерной инфраструктуры ЦОДа: зачем и как?

94 Новые продукты

Облака, мобильность и лично-корпоративный ДИССОНАНС



Евгения ВОЛЫНКИНА

рынке мобильных приложений заметно превосходит спрос, причем разрыв максимален в самом интересном для «продавцов» секторе крупных корпоративных клиентов. Заказчик, уже имеющий серьезную аппаратную и программную инфраструктуру, устоявшиеся бизнес-процессы и свою политику информационной безопасности, не склонен делать резких движений даже в очень модных направлениях. Как показала 2-я международная конференция Cloud&Mobility, организованная журналом «ИКС», вендоры уже готовы к компромиссам и к конструктивной работе в интересах клиента.

Облака для тяжеловесов и не очень

Даже такой крупный производитель, как HP, имеющий в своем арсенале комплексное облачное решение HP CloudSystem и множество других продуктов для построения облачных сред, берется приспособить к создаваемой у заказчика облачной системе уже имеющееся оборудование сторонних поставщиков. Как отметил руководитель направления облачных вычислений HP Андрей Соснихин, среди компаний, начинающих сейчас облачные проекты, нет ни одной, у которой не было бы накопленного за много лет ИТ-багажа, и это надо учитывать. Единственное ограничение по использованию имеющегося «железа» касается серверов – они должны быть построены на базе процессоров i386. Что касается сетевого оборудования и систем хранения данных, то тут ограничений нет, в частности, решение CloudSystem поддерживает сетевое оборудование Cisco и системы хранения от EMC и NetApp, т.е. компаний, которые опережают HP в соответствующих секторах рынка. Кроме того, заказчик может выбрать любую платформу виртуализации. Так, собственное облако HP, на базе которого компания в качестве провайдера предоставляет облачные сервисы, построено на платформе OpenStack с открытым исходным кодом.

Список «пряников», заманивающих в облако, дополняет возможность лизинга оборудования, а для крупных заказчиков, которые сами собираются быть провайдерами облачных сервисов на базе инфраструктуры HP, есть программа привлечения клиентов, предусматривающая выкуп их ИТ-оборудования, чтобы полученные деньги они потратили на переход в облако, и специальная система лицензирования ПО по схеме SaaS.

Облачные и мобильные приложения в качестве объектов личного пользования уже не вызывают отторжения. С корпоративными применениями ситуация иная, клиенты хотят безопасности, удобства и экономической эффективности – вендорам и провайдерам приходится проявлять гибкость.

Облачный провайдер ИТ-ГРАД подстраивается под нужды заказчиков достаточно гибким набором оборудования платформы FlexPod, в состав которой входят СХД NetApp, серверы Cisco UCS и коммутаторы Cisco Nexus, причем все это можно покупать по частям. На базе той же платформы ИТ-ГРАД построил свое собственное публичное облако и теперь старается тиражировать полученный опыт, строя частные и публичные облака для своих заказчиков. По словам руководителя проекта ИТ-ГРАД Артема Гимадиева, именно использование платформы FlexPod существенно упрощает и сокращает по времени процесс создания облачной инфраструктуры, который в «обычной жизни» предусматривает довольно длительные этапы проектирования, поставки оборудования, монтажа, тестирования и т.д., так что между формулированием запроса бизнеса на новый сервис и запуском этого сервиса в эксплуатацию часто проходят недели и месяцы. Основное преимущество FlexPod – в том, что эта платформа представляет собой протестированную инфраструктуру: ее можно построить по уже готовым спецификациям, для нее разработаны решения часто встречающихся задач (типа внедрения почтового сервера или системы виртуализации), подготовлены подробные руководства для развертывания (вплоть до настроек коммутаторов, которые должен вручную ввести системный администратор) и тесты построенного решения. Платформа масштабируется в довольно широких пределах, так что цена готовой системы может варьироваться от \$30 тыс. (ExpressPod) до \$1 млн и даже больше.

Решения компании Radware обладателями системы ExpressPod в начальной конфигурации вряд ли будут





востребованы, а вот остальные наверняка заинтересуются предлагаемыми ею средствами аппаратной балансировки и защиты приложений. Как отметил региональный менеджер Radware по продажам в СНГ Алекс Кушнир, в первую очередь они ориентированы на тех заказчиков, которые сами хотят быть провайдерами облачных сервисов, т. е. для них актуальны вопросы эффективной доставки приложений (балансировка), защиты веб-приложений и отражения атак как на приложения, так и на весь дата-центр целиком. Для этого предназначена линейка аппаратных балансировщиков Alteon производительностью от 1 до 80 Гбит/с и устройство для отражения атак DefencePro, способное отбивать атаки мощностью до 25 млн пакетов в секунду. Причем эти функции можно получить не только в «железном» виде, но и в виде облачного сервиса. В этом случае производительность балансировщика можно настроить довольно тонко (минимум составляет 10 Мбит/с, чего достаточно для большинства приложений), не тратя лишних денег. Что же касается защитника от атак DefencePro, то в договоре с заказчиком имеется интересный пункт: если в течение 18 секунд устройство не остановило атаку на систему клиента, то это в течение 20 мин в ручном режиме делает служба поддержки Radware.

Правда, нынешним облачным провайдерам придется привлекать клиентов не только средствами защиты их приложений и сайтов, но и готовностью построить заказчику всю необходимую инфраструктуру для потребления облачных сервисов. Именно так произошло с провайдером Cloud4Y, который в числе прочего подготовил к погружению в облако сеть московских частных клиник «Чайка». Как рассказал представитель Cloud4Y Заур Абуталимов, заказчик принципиально не хотел заниматься ИТ-инфраструктурой и отдал на аутсорсинг провайдеру разработку ТЗ, подготовку эксплуатационной документации, поставку оборудования, интеграцию построенной ИТ-инфраструктуры с облаком провайдера, базирующегося в двух ЦОДах в Москве, эксплуатацию рабочих мест, периферийного оборудования, сетевой инфраструктуры, каналов связи и бизнес-приложений. Работу по проекту облегчало то, что заказчик не имел унаследованной ИТ-

инфраструктуры, но скорость все равно впечатляет: на запуск первой клиники с полной установкой оборудования на местах и в дата-центре провайдера и с включением облачных сервисов ушло три недели.

Клиенты учатся считать

Но есть, конечно, заказчики, «обремененные» и богатой инфраструктурой, и многочисленным персоналом ИТ-подразделений, достаточно квалифицированным, чтобы построить собственное облако, как это сделали в компании МТС. Долгое время об экономической эффективности перехода на облачные сервисы рассказывали исключительно поставщики облачных решений, что воспринималось, в общем-то, как реклама. Но теперь об экономии стали говорить заказчики – на собственном опыте, и это большой прогресс. В данном случае при реализации проекта по созданию инфраструктуры виртуальных рабочих мест VDI ИТ-подразделение защищало бизнес-кейс перед финансовым отделом. Как рассказал системный архитектор МТС Константин Яковлев, в проекте участвует 28 тыс. рабочих мест, которые планируется в течение 10 лет полностью перевести на более дешевые тонкие клиенты в процессе естественного выхода техники из строя (по статистике в год ломаются 10% компьютеров). Но построение инфраструктуры VDI по плану займет четыре года, и к этому времени проект должен окупиться за счет того, что снизятся затраты на закупку оборудования для рабочих мест, на электроэнергию и эксплуатацию и экономия перевесит расходные статьи проекта – закупку серверов и дисковых массивов, установку их в ЦОДе, приобретение программных лицензий (по счастью, большая часть лицензий на ПО Citrix у МТС уже есть, иначе бизнес-кейс не сошелся бы).

Еще более внушительное количество сотрудников – у «Холдинга МРСК», который реализовал, правда, не VDI-проект, а проект цодотелефонии. Сделать это пришлось из-за колоссальных затрат на междугородную телефонную связь, которой пользуется половина из 190 тыс. работников этой компании, распределенной по всей стране. Как отметил главный эксперт отдела внедрения бизнес-технологий МРСК Алексей Вексин, проект позволил сократить затраты на эксплуатацию столь разветвленной инфраструктуры, оптимизировать услуги, приобретаемые у операторов связи, и расширить набор коммуникационных функций, доступных сотрудникам компании (разные виды ВКС, совместная работа с документами, мобильные приложения). Больше не требуется устанавливать АТС в каждом офисе, за все сервисы унифицированных коммуникаций отвечают несколько серверов, занимающих половину стойки в корпоративном дата-центре. Все услуги связи развертываются в качестве приложений в ЦОДе, пользователи могут свободно перемещаться по сети, централизованное управление сетью заметно упростилось, а отказоустойчивость повысилась. По словам А. Вексина, мощности разворачиваемой системы хватит на 100 тыс. пользователей, но при необходимости можно будет развернуть вторую такую же. Окупить свои инвестиции при постепенном пе-

переходе на новую систему и плановой замене устаревшего оборудования МРСК планирует за три года.

Тормоз не в технологиях

Воблачной организации работы ИТ-инфраструктуры видит перспективу и Банк России, но его случай особый: здесь во главу угла поставлены непрерывность сервиса и информационная безопасность. Четыре года назад в банке были внедрены системы виртуальных серверов и терминального доступа, а облако пока существует в виде испытательного стенда, на котором, как рассказал начальник управления эксплуатации обеспечивающих систем МЦИ Банка России Александр Шибяев, проверены несколько технических решений для частного облака по предоставлению и контролю сервисов, информационной безопасности и организации доступа к ресурсам. Эти испытания показали, что технических проблем в переходе к облачной модели предоставления ИТ-сервисов фактически не осталось, но банку придется менять организацию работы службы ИБ – она должна стать активным участником бизнес-процессов. Кроме того, внедрение облаков противоречит действующим нормативным документам для банков. Рано или поздно их скорректируют (или найдут способы обхода), но к этому моменту надо подготовить и технические и организационные решения.



Аналогичные «нетехнологичные» тормоза есть и у концепции корпоративной мобильности BYOD (bring your own device). Те компании, для которых проблемы ИБ при подключении к корпоративной сети личных мобильных устройств сотрудников не критичны (или которые уже научились их решать), не чинят препятствий BYOD, и доля таковых в России составляет уже 45%. Проще всего, как и с внедрением облачных сервисов, небольшим компаниям, но и у крупных практический подход начинает превалировать над политикой запретов. По словам руководителя департамента серверных продуктов Microsoft Светланы Лихаревой, в самой компании Microsoft проблема решена так: при подключении к корпоративной сети любого клиентского устройства проводится автоматическая проверка уста-

новленного на нем ПО на «благонадежность», и если таковая подтверждается, то доступ в сеть открывается.

Поддерживает коллег и компания Citrix Systems, уже не первый год заявляющая о том, что мобильный стиль должен позволять человеку работать из любого места с любыми приложениями и любыми данными и не задумываться о проблемах и простоях при переходе на новое место работы и на новое устройство. Но соответствие этой декларации, заявленной еще до эры BYOD, требует от бизнеса определенной гибкости. «Нужно найти решение, которое, с одной стороны, даст пользователю чувство свободы выбора (и устройства, и места работы), а с другой – обеспечит безопасность и соблюдение корпоративных политик», – считает системный инженер Citrix Леонид Майзенберг. Мировая практика показывает, что пользователь выбирает устройство, а компания обеспечивает безопасность своей ИС всеми доступными способами.

BYOD не личное дело

Оседлать волну BYOD или хотя бы постараться направить ее в конструктивное русло намерен сотовый оператор «ВымпелКом». По словам его руководителя департамента по продуктам мобильной связи бизнес-сегмента Евгении Григорьевой, каждый пятый абонент компании пользуется мобильным интернетом, несмотря на небольшой экран телефона, да и собственные сотрудники оператора хотят использовать личные устройства для решения рабочих задач в любое время и в любом месте. Поэтому в компании запущена программа Enterprise Mobility, цели которой – поддержка новых требований бизнеса по мобилизации приложений и сервисов, обеспечение финансовой эффективности внедряемых мобильных решений, смягчение рисков безопасности и других угроз при реализации концепции BYOD. После испытаний на себе планируется предложить соответствующее решение и клиентам.

Рисков мобилизации пользователей в корпоративной среде немало, но бизнес видит в ней мощный драйвер развития, для реализации которого ИТ-подразделение должно правильно организовать виртуальное корпоративное пользовательское пространство. На мировом рынке есть для этого даже коробочные решения, но, наверное, очень сложно найти компанию, которой они подходили бы на 100%. Руководитель направления мобильных технологий компании САПРАН Олег Бачурин полагает, что если решение охватывает хотя бы 80% функциональных требований компании, внедрять его надо. Во всяком случае, это сэкономит время и поможет собственным пользователям сформулировать осознанные требования к подобным решениям. Особо стоит обратить внимание на то, что интерфейс мобильного приложения должен быть интуитивно понятным, иначе даже по служебной необходимости пользователь работать с ним не будет. Кроме того, не надо пытаться втиснуть в мобильную систему все функции настольной – только необходимый набор, и очень важна поддержка и онлайн-ового, и автономного режима работы (связь может пропадать даже

в обычном лифте, и это не должно нарушать работу корпоративного приложения).

Важную роль в реализации концепции BYOD играют средства управления мобильными устройствами в корпоративной среде MDM (Mobile Device Management) и средства управления приложениями и данными MAM (Mobile Application Management). Как отметил Антон Карасев, ведущий эксперт по облачным вычислениям IBS, рынка MDM- и MAM-решений в России фактически пока не существует, наши компании только начинают проявлять к ним интерес, но в мировом масштабе он развивается около четырех лет, так что кое-какие продукты – в том числе вендоров, давно присутствующих в нашей стране, – на отечественном рынке уже есть (это, например, MDM-решения Symantec Mobile Management и SAP Afaria).

К трехбуквенным словечкам MDM и MAM уже добавились и MIM (системы управления мобильными данными), и EMM (Enterprise Mobility Management). Последнее характеризует комплексный подход к управлению мобильными устройствами и приложениями, обеспечению безопасности данных и предоставлению доступа к корпоративным ресурсам, охватывающий и MDM, и MAM, и MIM. EMM-системы объединяют управленче-

ские функции и функции ИБ. Они должны обеспечивать программную и аппаратную инвентаризацию устройств, их удаленную настройку и мониторинг, геолокацию, настройку сетевых подключений, автоматическую конфигурацию и защиту приложений, парольные полити-

ки, защищенный доступ к внутренним ИТ-ресурсам, частичную или полную очистку данных при компрометации устройства и т.д. Как рассказал руководитель практики прикладных решений КРОК Константин Астахов, такие проекты уже есть на российском рынке (например, в ОАО «Авиадвигатель»), и расчеты показывают, что экономический смысл их внедрения появляется при наличии в организации хотя бы 50 мобильных устройств.

Компания DataLine предлагает решать проблемы концепции BYOD с помощью технологии VDI. Как подчеркнул ее директор по производству Григорий Атрепьев, VDI-реализация концепции BYOD позволяет преодолеть

большую часть сложностей и рисков последней: с VDI можно использовать в корпоративной сети любое клиентское устройство без ограничений по производительности и операционной системе; эта технология гарантирует безопасность данных и возможность быстро возобновить работу даже в случае выхода из строя



Облака и доходы: что осталось за слайдом?



Алексей БЕССАРАБСКИЙ,
руководитель
отдела маркетинга,
«Манго Телеком»

На конференции Cloud&Mobility-2013 в докладах, посвященных бизнес-применению облачных и мобильных технологий, акцент делался на снижении CAPEX и OPEX, экономии на МГ/МН и т.д. А про рост доходов не упоминалось либо утверждалось, что его нет. Устраивает ли это пользователей?

Сегодня покупатель стал информированнее, данные о продуктах – доступнее. Все больше циклов продаж не заканчивается принятием решения. Растет потребность бизнеса в развитии методологий продаж, непрерывном обучении, адаптации продаж к разным типам покупателей. И все это так или иначе сводится к бизнес-процессам.

Облачные коммуникации отличает расширенная поддержка бизнес-процессов и возможность интеграции коммуникаций с бизнес-приложениями. Речь о виртуальных АТС и колл-центрах, облачных CRM, Click2Call. Информационно-аналитические сервисы облачных приложений позволяют измерить эффективность работы компании, найти слабые места в бизнес-процессах, ликвидировать их и увидеть, что изменилось – с финансовой точки зрения.

Тесная интеграция облачных АТС и колл-центров с сетями общего пользования, возможность задавать правила обработки звонков позволяют эффективнее выстраивать продажи и оптимально распределять ресурсы. Использование облачных приложений, поддерживающих бизнес-процессы и интегрированных с коммуникациями (CRM), позволяет ускорить циклы транзакций и повысить их продуктивность. А это приводит к росту лояльности клиентов и доходов.

Данные Aberdeen Group (2012–2013 гг.) показывают: в облачных колл-центрах на 80% чаще традиционных используют статистику звонков для совершенствования бизнес-процессов; на 30% чаще – централизованную запись активности с целью анализа и обучения; чаще применяется интеграция телефонии с бизнес-приложениями. Что это дает?

На американском рынке колл-центров использование облачных технологий обеспечивает рост доходов за счет уменьшения потерь клиентов на 27%; увеличивает частоту решения проблем «за один звонок» на 70%, способствует росту доходов на 13,1% в год. На российском рынке, по данным «Манго Телеком», их применение уменьшает число пропущенных вызовов почти до нуля; расширяет «воронку продаж» на 25–40%; снижает отток клиентов вдвое; повышает продуктивность специалистов до 35%. А рост доходов российских компаний составляет 50%. И это – главный итог для бизнеса.

или потери клиентского устройства. Однако реализация подобных проектов требует высокого качества связи и резервирования каналов и вычислительных ресурсов: для приемлемой работы офисных приложений нужно иметь канал шириной 0,5 Мбит/с в расчете на одного пользователя, а если необходимо поддерживать работу видео- или тяжелых графических приложений, то пропускную способность канала надо будет увеличить до 2 Мбит/с. Подобные проекты в портфеле DataLine уже есть, в том числе и свой собственный (проверять все на себе стало правилом хорошего тона), а вот клиенты, к сожалению, настаивают на анонимности.

Жизнь без офиса

К счастью, среди заказчиков есть и такие, кто готов похвастаться своими достижениями на ниве мобилизации и облаков перед широкой публикой. Вот, например, компания «Био-Витрум», дистрибьютор медикаментов, медицинского и лабораторного оборудования: как заявил ее директор по ИТ Эдуард Шишмарев, в текущем году в офисе он находился только два дня, а вся работа происходит фактически в мобильном режиме. Такие продвинутые заказчики сами выработали свои требования к инструментам мобильной коллективной работы: простота, масштабируемость, экономичность (минимум начальных инвестиций, оплата только реально потребленных сервисов), взаимосвязанность друг с другом, доступность сервисов, производительность, безопасность, управляемость из единого центра управления конфигурациями и функциональность (мобильность, гарантированная доставка почты, средства совместной работы и быстрого принятия решений). Все эти возможности обеспечивают решение на базе смартфонов BlackBerry, предлагаемых сотовым оператором «Билайн», и дата-центр компании DEAC в Риге, где распола-

гается виртуальное частное облако, в котором работают все корпоративные приложения для совместной работы и виртуальные десктопы сотрудников. Как подчеркнул Э. Шишмарев, компания занимается медициной, а все остальное, в том числе ИТ-сервисы, покупает.

Еще более примечательно появление в рядах «белых» заказчиков банка «Хоум Кредит», поскольку такого рода организации, как правило, секретят всю свою ИТ-деятельность под предлогом соблюдения жестких правил безопасности. Виктор Ковалев из «Хоум Кредит», руководитель направления по стратегическому планированию департамента управления сервисов ИТ, считает, что мобилизация банка должна быть комплексной и охватывать не только сотрудников, но и клиентов. Последние должны получать доступ к банковским услугам не столько в офисах, сколько в любых других местах, т.е. все функции должны быть им доступны со смартфонов. Под размер экрана смартфонов заточены теперь и ассортимент услуг (сведенный к минимуму), и договоры об обслуживании (максимально краткий текст, никакого мелкого шрифта под звездочками).



Правда, стремление охватить мобильными услугами все 24 млн клиентов чревато для банка массой проблем, потому что банковские сервисы должны поддерживаться всеми существующими на рынке мобильными устройствами, а реализовать эту поддержку приходится собственными силами. Кроме того, банк использует мобильные технологии для ежедневного обслуживания всех 16 тыс. точек своего присутствия по всей стране, и занимается этим 1000 сотрудников, вооруженных планшетами, причем их местонахождение центральная служба поддержки отслеживает с помощью GPS и в соответствии с полученными данными загружает на планшет необходимый набор документов. В дальнейших планах банка – внедрение технологии, позволяющей превратить в POS-терминал любой мобильный телефон, и NFC-технологии бесконтактной оплаты покупок. Перспективы инцидентов ИБ, связанных с распространением новых мобильных технологий, В. Ковалева не смущают – просто к отражению новых угроз надо готовиться.



Как мы уже отмечали (см. ИКС №4'2013, с. 18), среди докладчиков конференции Cloud & Mobility соотношение между конечными пользователями и поставщиками мобильных и облачных решений составило примерно 1:3. Однако тон на рынке задает именно меньшинство: оно не боится трудностей, в том числе в деле укрощения проблем безопасности, хочет идти в облачности и мобильности «до самой сути» и в конце концов добивается своего. Пожелаем ему побыстрее уравнивать популярность личных и корпоративных облачно-мобильных приложений – и стать наконец большинством. **ИКС**



Liebert PCW: точное охлаждение для облачных сред, обеспечивающее максимальную экономию энергии

Компания Emerson Network Power кардинально расширила функциональные возможности своей системы охлаждения Liebert PCW.

Фальшпольная система прецизионного охлаждения Liebert PCW, работающая на захоложенной воде, предназначена для средних и крупных центров обработки данных, а также небольших ЦОДов и компьютерных залов. Liebert PCW идеально подходит для дата-центров, ориентированных на облачные вычисления. Система прекрасно адаптируется к динамической среде ЦОДа и изменениям тепловой нагрузки, характерным для облачных вычислений.

МАКСИМАЛЬНАЯ ЭФФЕКТИВНОСТЬ ПРИ МИНИМАЛЬНОМ ЭНЕРГОПОТРЕБЛЕНИИ

Ключевое отличие Liebert PCW – оптимизированная внутренняя аэродинамика. Инженеры Emerson Network Power изучили характеристики воздушного потока внутри устройства и полностью переработали внутренние компоненты Liebert PCW. Благодаря новой аэродинамической конструкции Liebert PCW сопротивление воздуха внутри установки минимально. Это обеспечивает максимальную эффективность охлаждения, снижает энергопотребление вентилятора и, как следствие, сокращает расходы на эксплуатацию системы охлаждения и дата-центра в целом.

Liebert PCW объединяет в себе специально разработанные ЕС-вентиляторы нового поколения (Liebert EC Fan 2.0), высокоэффективные фильтры тонкой очистки, способствующие сни-

жению уровня шума, ультразвуковой увлажнитель и систему управления Liebert iCOM, которая реализует интеллектуальный алгоритм управления, разработанный для решений SmartAisle (холодные коридоры). Она позволяет осуществлять точное управление температурой и наиболее эффективно подводить охлаждающий воздушный поток к серверам, не допуская при этом потери ни одного ватта.

Система Liebert PCW проста в установке и отличается гибкими настройками. Она динамически реагирует на потребности дата-центра в любой момент времени, поддерживает максимальную доступность и оптимальную энергоэффективность.

КОНТРОЛЬ ЗА PUE

Оптимизировать энергоэффективность ЦОДа помогает и новое бесплатное приложение под названием Liebert PCW, доступное для скачивания на iPad в онлайн-магазине AppStore. Приложение предоставляет управляющему персоналу ЦОДа возможность отслеживать его PUE, что будет способствовать принятию более точных решений о том, как и где можно экономить энергию. Приложение включает в себя два отдельных калькулятора: калькулятор PUE для расчета энергоэффективности ЦОДа и калькулятор общих эксплуатационных расходов, позволяющий рассчитать, сколько именно средств можно сэкономить, установив более эффективное оборудование, например такое, как Liebert PCW.

Приложение также предоставляет обзор компонентов Liebert PCW, давая возможность изучить технические особенности данного решения и понять, как та или иная технология может помочь экономить энергию в ЦОДе.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ДЛЯ ЕМЕА

В странах региона ЕМЕА доступен дополнительный набор опций для Liebert PCW, нацеленный на повышение энергоэффективности и защиту окружающей среды. В их числе:

- Новая модель Liebert PCW с двойным контуром. Эта конфигурация обеспечивает избыточное охлаждение для заказчиков, которые не имеют возможности установить два блока без ущерба для энергоэффективности. На сегодняшний день Liebert PCW обеспечивает самую высокую в отрасли энергоэффективность (до 65%), и при установке ее в качестве дополнительной системы к Liebert HPC Freecooling Chiller PUE может достигать значения 1,11.
- Новый размер – теперь система поставляется в корпусе 3350 мм, позволяя увеличить мощность охлаждения до 240 кВт. Это дает возможность довести установленную мощность ИТ-оборудования до 7,5 МВт без изменения контура управления.
- Возможен заказ на выбор – инфракрасный увлажнитель, ультразвуковой увлажнитель и измеритель уровня. Это способствует улучшению рабочих характеристик Liebert PCW в установках, где предусмотрен мониторинг температуры и влажности.



Владимир ШЕПЕЛЕВ,
бренд-менеджер
Emerson Network
Power Cooling



Конструкция Liebert® PCW обеспечивает минимальное сопротивление воздуха.

Революция в построении ЦОДов

В решении RiMatrix S компания Rittal впервые в мире воплотила концепцию стандартизированного оборудования ЦОДа. Если до сих пор дата-центры проектировались индивидуально для каждого заказчика, с соответствующими затратами времени и средств, то модуль RiMatrix S от Rittal открывает новые горизонты. Готовые, сконфигурированные и совместимые друг с другом модули ЦОДов позволяют быстро и просто создавать новые дата-центры или расширять имеющиеся. Тем самым Rittal стала первой в мире компанией, предлагающей стандартизированное оборудование ЦОДа.

Индивидуальное проектирование и подбор конфигурации ЦОДа до недавнего времени представляли собой сложную задачу и требовали много времени. Различные требования в отношении готовности и безопасности, конструктивные условия и рамки бюджета неизбежно затягивали этапы проектирования и строительства на многие месяцы. «Выпуск RiMatrix S компанией Rittal ведет к смене парадигмы в мире информационных технологий, так как этот модуль впервые позволяет создать весь ЦОД из оборудования под единым артикульным номером, – объясняет Бернд Ханштайн, руководитель отдела продаж-менеджмента по ИТ-решениям Rittal. – RiMatrix S – это ответ на такие требования к ИТ-решениям, как быстрота, эффективность, надежность и гибкость». В будущем клиентам не потребуется учитывать в своих планах длительные сроки проектирования и поставки.

Благодаря концентрации внимания на стандартизации модулей ЦОДов и идеальному согласованию компонентов друг с другом система RiMatrix S обеспечивает очень низкий коэффициент PUE (эффективности использования энергии) – он составляет всего 1,15.

Комплексные серверные модули

RiMatrix S представляет собой готовый центр обработки данных, включающий следующие стандартизированные компоненты: определенное количество серверных и сетевых стоек TS IT, системы контроля микроклимата, энергоснабжения и защиты от перенапряжений, а также средства мониторинга. Вместе они составляют комплексный серверный модуль.

Чтобы повысить плотность монтажа серверных и сетевых компонентов, компания Rittal разработала для



Реклама

Rittal – The System.

Faster – better – worldwide.

ИТ-инфраструктура от элемента до системы.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

RiMatrix S новую систему контроля микроклимата, которая полностью размещается в фальшполе (система охлаждения по принципу Zero-U-Space Cooling-System, ZUCS). Воздухо-водяные теплообменники располагаются непосредственно под серверными стойками. Их вентиляторы подают холодный воздух через перфорированную нижнюю панель прямо на уровень сервера. Так как двери и боковые стенки серверных шкафов затруднили бы воздухообмен, в системе RiMatrix S применяются только стойки. Перегородка между стойкой и потолком, а также 19-дюймовой полкой разделяет зоны холодного и горячего воздуха. Резервирование системы контроля микроклимата по схеме N+1 обеспечивает высокую готовность.

Все для удобства клиента

Большое внимание компания Rittal уделяет и бесперебойному энергоснабжению сетей. Ввод питания и вторичное распределение в системе RiMatrix S предварительно сконфигурированы таким образом, чтобы без проблем использовать имеющиеся ИБП или установить новые. Электрораспределение в модулях RiMatrix S также реализовано с резервированием при помощи фидеров А и В, причем ветвь В подключена к ИБП. ИБП представляет собой вставной модуль и резервируется по схеме N+1. При установке модуля распределения питания Rittal PDU managed возможно измерение расхода электроэнергии вплоть до розетки.

Комплексный контроль осуществляется при помощи системы мониторинга Rittal CMC III (Computer Multi Control). Эта система, в которую входят процессорный блок и до 32 взаимодействующих датчиков, регистрирует все физические параметры, такие как температура, влажность или задымление. Данные измерений отображаются в программе RiZone, через которую администратор может также осуществлять управляющее воздей-

ствие. Дополнительно можно оборудовать серверный модуль системой пожаротушения.

Комбинирование для создания крупных систем

Самый маленький вариант RiMatrix S, Single 6, состоит из шести серверных стоек и дополнительной стойки для сетевого оборудования. Более крупный вариант Single 9 включает восемь серверных стоек и одну – для сетевого оборудования. Важной особенностью системы является возможность комбинирования серверных модулей для создания крупных ЦОДов: можно быстро и без проблем как составить зеркальную конструкцию с общими зонами холодного и горячего воздуха, так и выстроить модули в ряд. Модули RiMatrix S одинаково хорошо подходят для сооружения нового дата-центра в здании с дополнительным отделением коридоров или для установки вне здания в высоком контейнере. Наконец, эта мировая новинка от Rittal позволяет легко расширить существующий ЦОД и может использоваться в помещении повышенной безопасности.

Расширение и дополнение

Создав концепцию стандартизированного ЦОДа, Rittal расширяет свой ассортимент компонентов ИТ-инфраструктуры. «Конечно, возможность проектирования и постройки дата-центра по индивидуальному проекту клиента из отдельных компонентов RiMatrix будет по-прежнему доступна, – подчеркивает Бернд Ханштайн. – Только так мы сможем предложить каждому клиенту ЦОД, который будет оптимально соответствовать его конкретным требованиям».

ООО «Риттал»

125252, Москва, ул. Авиаконструктора

Микояна, 12, БЦ "Линкор", 4 этаж

тел. (495) 775-0230, факс (495) 775-0239

info@rittal.ru, www.rittal.ru



IT INFRASTRUCTURE

SOFTWARE & SERVICES

www.rittal.ru



Телекоммуникационное оборудование «Энергомера» –

качественно, надежно, перспективно

Ставропольский электротехнический завод «Энергомера» является крупнейшим производителем телекоммуникационного монтажного и электротехнического оборудования.

Опыт – залог успеха

Наша компания обладает инновационными конструкторскими и производственными мощностями и большим опытом разработки и серийного производства телекоммуникационных монтажных конструктивов и электрораспределительного оборудования, в число которых входят:

- ▶ 19" телекоммуникационные шкафы INDOOR в различных исполнениях (напольные, навесные, эконом-класса и т.п.);
- ▶ антивандальные телекоммуникационные шкафы;
- ▶ шкафы для размещения электропитающих установок;
- ▶ шкафы OUTDOOR для оборудования мобильной связи и оборудования ШПД;
- ▶ монтажные стойки;
- ▶ вводно-распределительные устройства и щиты питания для оборудования телекоммуникаций.

Отвечая всем нормативно-техническим требованиям, продукция торговой марки «Энергомера» воплощает в себе высокую надежность, законченность решений и разумный подбор комплектующих.

На шаг вперед

Основополагающий принцип деятельности нашей компании – повышение степени удовлетворенности каждого потребителя качеством нашей продукции. Для этого у нас есть все условия.

- ▶ Вся продукция производится с помощью высокотехнологич-

ного европейского оборудования – мы обеспечиваем высокое качество нашей продукции.

- ▶ Ставропольский электротехнический завод «Энергомера» является отечественным производителем – по сравнению с иностранными производителями мы предлагаем рынку привлекательные цены и короткие сроки поставки при высоком уровне качества продукции.
- ▶ Наша компания имеет собственный корпоративный институт, поддерживающий современный уровень разработок, – мы обеспечиваем возможность производства оборудования в соответствии с конкретными требованиями потребителя.

Качество – превыше всего

Важнейшей задачей, решаемой компанией, является повышение стандартов качества услуг.

Высокий рейтинг Ставропольского электротехнического завода «Энергомера» стал одним из важных факторов в развитии сотрудничества с компаниями мирового класса – Siemens, ELTEK, General Electric – и крупнейшими операторами связи («ВымпелКом», МТС).

Устремленные в будущее

Опираясь на высококвалифицированный персонал и накопленный опыт, наша компания предлагает заказчикам полный спектр услуг и выполняемых работ.



Производство без ручного труда

Для производства нашей продукции мы используем современное высокотехнологичное оборудование, в том числе линию обработки металла Salvagnini и металлообрабатывающее оборудование TRUMPF.

Линия Salvagnini – не просто автоматическая линия по обработке листового металла. Это гибкая производственная система для пробивки, резки и гибки металла. В совокупности с автоматизированным складом система позволяет воплотить в жизнь идею производства без ручного труда.

Основные машины в системе – пробивная и гибочная – могут работать не только как автоматическая линия, но и независимо друг от друга, выполняя собственные производственные задания. Система способна выпускать партии даже из одной детали.

Конечно же, и у этой производственной системы есть некоторые технологические ограничения, но в совокупности с имеющимся у нас оборудованием для вырубки и гибки TRUMPF мы получили мощный универсальный комплекс по обработке листового металла в составе Ставропольского электротехнического завода «Энергомера», позволяющий воплотить в жизнь самые смелые проекты наших потребителей.



В 2012 г. мы значительно расширили линейку производимого оборудования: к ранее выпускаемым моделям добавились шкафы INDOOR для размещения электропитающих установок, шкафы OUTDOOR, щиты питания базовых станций. Был существенно расширен модельный ряд антивандалных шкафов.

В 2011 г. наш завод был оснащен дополнительными мощностями для производства телекоммуникационного оборудования – была установлена автоматизированная линия Salvagnini, которая позволила значительно увеличить объем производства продукции.

Лучшие предложения

Наша компания предлагает широкий спектр оборудования, способного выполнять различные задачи. Производство оборудования осуществляется с учетом передовых технологий, требований и пожеланий потребителей.

Мы стремимся к тому, чтобы самое современное оборудование и передовые решения стали доступны каждому потребителю. Европейский дизайн оборудования, постоянное активное внедрение новых технологий, процессов, материалов, быстрое и эффективное реагирование на изменения рынка – лучшее тому подтверждение.

Мы готовы к исполнению различных индивидуальных заказов на оборудование торговой марки «Энергомера». Подробную информацию о телекоммуникационном, промышленном оборудовании и другой продукции нашей компании можно найти на официальном сайте – www.energomera.ru.

ЭНЕРГОМЕРА

Ставропольский
электротехнический завод
«Энергомера»

Россия, 355008, Ставрополь,
ул. Апанасенковская, 4
Тел.: (8652) 95-12-72
Факс: (8652) 28-13-90
E-mail: etz@energomera.ru

Квалифицированный персонал

основа операционной устойчивости ЦОДа



Заурбек АЛЕХИН,
независимый консультант

Устойчиво функционирующий ЦОД – это объект, параметры функционирования которого сохраняются в заданных пределах сколь угодно долго, независимо от отрицательного влияния предсказуемых и случайных событий.

Помимо собственно реагирования на разного рода отказы и отклонения от целевых режимов текущая эксплуатация дата-центра предполагает выполнение большого числа разнообразных операций, лишь малая часть которых может производиться автоматически – и то с оговорками. Большинство же операций требуют непосредственного и активного участия сотрудников службы эксплуатации, которые для этого, безусловно, должны обладать необходимыми знаниями и навыками.

Значительная часть инцидентов и нарушений параметров функционирования ЦОДов происходят вследствие ошибок персонала, совершенных при обслуживании оборудования и при действиях в нестандартных ситуациях. Поэтому достаточная численность и квалификация персонала в службе эксплуатации – один из ключевых элементов операционной устойчивости ЦОДа.

Устойчиво функционирующий ЦОД – это объект, параметры функционирования которого

В прошлой статье* мы обсудили понятие «эксплуатация» и получили представление о перечне задач, подлежащих решению в ходе эксплуатации дата-центра. В основе рассматриваемой модели эксплуатации лежит операционная модель, описанная в разработанном Uptime Institute стандарте «Data Center Site Infrastructure Tier Standard: Operational Sustainability»** (Стандарт операционной устойчивости).

В соответствии с данным стандартом основные элементы, формирующие операционную устойчивость ЦОДа, – это обеспечение человеческими ресурсами, наличие необходимых процессов и контроль и управление реализацией процессов. Справедливости ради отметим, что помимо перечисленных авторами стандарта обозначены и иные важные элементы. Но с точки зрения общей модели они не являются определяющими для дата-центров, не име-

Квалификация и компетенция

Большой российский энциклопедический словарь определяет в интересующем нас смысле квалификацию как уровень подготовленности, степень годности к какому-либо виду труда, а компетенцию – как знания, опыт в той или иной области.

Квалификация зависит от наличия у сотрудника соответствующих профессиональных знаний и трудовых навыков, необходимых для исполнения задач на конкретном рабочем месте. Для того чтобы иметь возможность сравнивать сотрудников и наиболее адекватно их использовать, вводятся разнообразные шкалы и рейтинги квалификации. Показателем квалификации рабочих и служащих, как правило, является разряд. Результаты труда работника находятся в зависимости

от уровня его квалификации: в общем случае сотрудник с более высокой квалификацией выполняет работу быстрее, качественнее, с меньшими затратами энергии. Стоит отметить также, что отдельные работы в принципе не могут выполняться сотрудниками низкой квалификации ввиду отсутствия у них требуемых знаний.

Понятие компетенции, т.е. наличие у сотрудника знаний и опыта в той или иной области, органично дополняет понятие квалификации, конкретизируя, в какой именно области работник имеет соответствующий уровень подготовки.

Итак, компетенция – это набор личных качеств специалиста, его способность решать профессиональные задачи определенной группы. Обычно

оценка компетенции направлена на выявление наличия или отсутствия нужной для работы составляющей, а не степени ее выраженности. Многие организации разрабатывают модели компетенций, представляющие собой структурированные наборы компетенций, на базе которых формируются требования к претендентам на занятие тех или иных должностей.

На практике используются различные варианты классификации компетенций. В настоящее время модели компетенций и квалификационные рейтинги – основной инструмент, применяемый многими компаниями на всех этапах управления персоналом, включая подбор, организацию текущей деятельности, обеспечение профессионального роста и развития.

* З. Алехин. Операционная устойчивость ЦОДа: новое увлечение или реальная потребность? «ИКС» № 1–2'2013, с. 76; № 3'2013, с. 84.

** См. <http://uptimeinstitute.com/publications>.

ющих сертифицированной Ur-time Institute инженерной инфраструктуры.

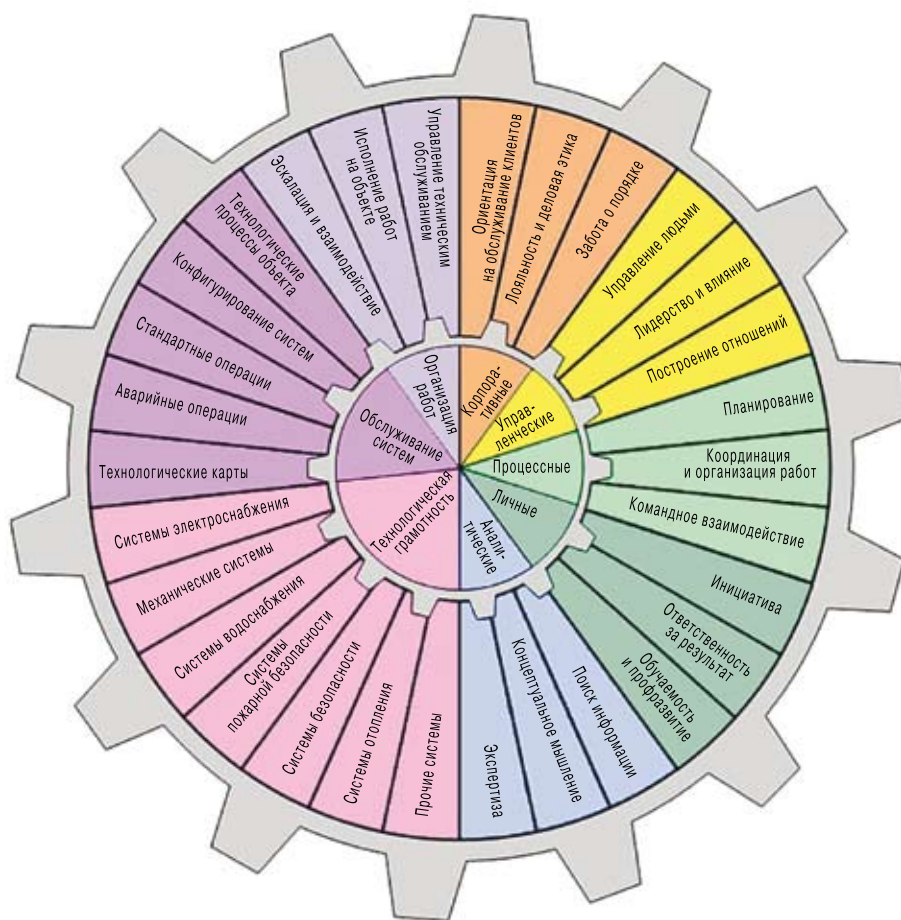
Группы компетенций

Компетенции, требуемые для поддержания бесперебойного функционирования дата-центра, можно разделить на технологические, организационные, управленческие и т.д. (рис. 1). В зависимости от типа ЦОДа, выбранной модели эксплуатации такие группы могут быть дополнены и детализированы.

В связи с большим числом систем ЦОДа и еще большим количеством вариантов конкретного оборудования, составляющего эти системы, наиболее сложной является группа технологических компетенций. Служба эксплуатации ЦОДа вовлечена в выполнение большого числа различных задач, что требует наличия разноплановых навыков и компетенций. Ядро составляют опыт и знания в области обслуживания конкретного оборудования: сложность систем в дата-центрах высока, и малоопытный самоучка не только бесполезен, но и порой просто вреден. В первую очередь речь идет об умении силами службы эксплуатации квалифицированно обслуживать и эффективно устранять сбои в наиболее критичных системах, к которым относятся системы электроснабжения, охлаждения и вентиляции. Современные решения, хотя и обладают существенным запасом надежности, все же подвержены отказам, и потому требуют качественного и своевременного ухода. Работа с ними без соответствующих знаний, регулярных тренировок, отслеживания рекомендаций производителей может привести к нежелательным и даже опасным последствиям. Таким образом, технологические компетенции необходимы для выполнения основных операций обслуживания, поиска и устранения неисправностей и отказов, настройки, регулирования, модернизации систем.

Не менее важны навыки и умения работать в команде, что обусловлено наличием глубоких взаимозависимостей систем и тем, что один и тот же элемент может быть составной частью разных систем. Поскольку дата-центр – объект комплексный, даже обслуживание одной системы не может выполняться полностью изолированно. В ситуации сбоя критичность качественного взаимодействия персонала вырастает кратно, так как для сохранения целевых параметров требуется не только быстро устранить сбой конкретной системы,

Рис. 1. Компетенции персонала службы эксплуатации дата-центра



Источник: Tier Advisor Group

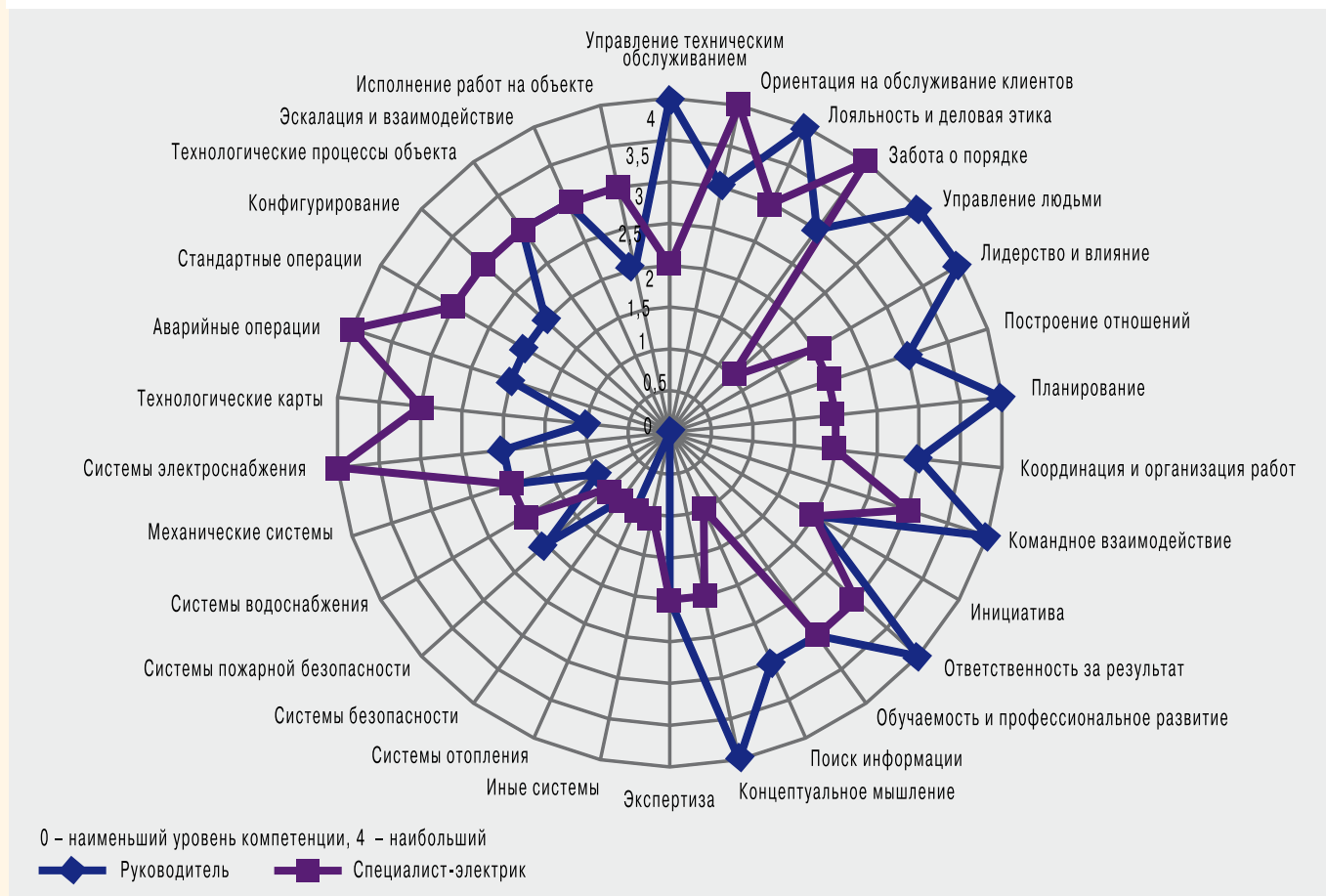
но и одновременно перевести на другую схему работы и взаимодействия смежные системы.

Отдельно стоит группа компетенций по координации работ. Редко кто возражает против необходимости диспетчерской службы, хотя бы в минимальном варианте. В реальности кажущийся на первый взгляд простым набор действий в случае сложного объекта и высокого уровня ответственности становится не только обязательным, но и критичным. Важность навыков и опыта в сфере организации работ еще более возрастает в условиях привлечения внешних исполнителей.

И, конечно, не стоит забывать о том, что служба эксплуатации зачастую является выделенным структурным подразделением. Обеспечение его нормальной работы требует навыков общего менеджмента. Персонал надо подбирать, развивать, создавать ему нормальные условия труда и отдыха, организовывать и контролировать исполнение обеспечивающих процессов. В общем, выполнять комплекс действий, который объединяется понятием «руководить подразделением». В зависимости от масштабов и обособленности структуры для этих задач может потребоваться от одной до нескольких штатных единиц, а в крупных структурах – до десятков сотрудников и даже нескольких подразделений.

Безусловно, невозможно требовать наличия всех перечисленных компетенций в максимальном объеме от

Рис. 2. Примеры профилей компетенций для руководителя и специалиста-электрика



всех сотрудников службы эксплуатации дата-центра. Тем более что персонал службы эксплуатации может быть разделен на несколько групп: менеджмент, технические специалисты, инженеры-аналитики, диспетчеры, вспомогательный персонал. Но и это деление вовсе не окончательное. Часто специалисты умеют обслуживать только один-два типа систем, обладая по остальным лишь поверхностными знаниями, либо способны качественно настроить оборудование, но быстро обнаружить и устранить неисправность — к сожалению, нет...

Учитывая конфигурацию дата-центра, реальные потребности в обслуживании оборудования, указанные и иные особенности, руководство службы эксплуатации может составить типовый профиль компетенций для каждого штатного специалиста (рис. 2).

Требования к персоналу согласно Стандарту операционной устойчивости

В целом требования и ограничения Стандарта операционной устойчивости (рис. 3) направлены на управление операционными рисками. Рассмотрим их с точки зрения тех угроз и проблем, которые может создать для устойчивого и качественного функционирования дата-центра их несоблюдение.

Достаточность численности. Могут ли быть выполнены в полном объеме все необходимые процессы и операции обслуживания в случае, если людских ресурсов недостаточно? Конечно, нет. Оплата сверхуроч-

ных работ проблему не решает: персонал физически устает, теряет внимание к мелочам, совершает ошибки. Поэтому должны быть предусмотрены ресурсы с учетом неравномерности выполнения работ, а также возможных аварий и авралов.

Нельзя ограничиться только формированием штатного расписания, поскольку большее значение имеет фактическое присутствие сотрудников на объекте, т.е. структура и состав рабочих смен.

Достаточность квалификации. В стандарте достаточность квалификации персонала определяется следующими основными группами требований:

- требования регуляторов — лицензии, допуски и т.п.;
- отраслевые требования — стандарты и нормативы отрасли;
- требования производителей оборудования — специфичные процедуры и регламенты;
- корпоративные требования — внутренний порядок и организация работ;
- функциональные требования — ограничения выбранной модели обслуживания.

Неисполнение требований создает как технологические, так и иные риски, включая правовые и экономические.

Четкое и корректное разграничение ответственности. Требование явного обозначения, кто конкретно и за что именно отвечает, есть даже в Трудовом кодексе РФ. Его неполное исполнение связано, как пра-

Рис. 3. Элементы стандарта, связанные с людскими ресурсами



вило, с большим объемом и сложностью исчерпывающего перечня функций, а также с динамичностью объекта, постоянно происходящими изменениями и корректировками. Опасны обе возможные ошибки: и отсутствие ответственных за какой-либо элемент, и попадание одного и того же элемента в зону ответственности двух и более специалистов/подразделений. В первом случае все понятно: нет ответственного – значит, никто ничего не делает. Второй случай более изощренный: ответственные есть, но каждый делает какие-то операции по-своему, и к тому же возникают споры о том, «кто главнее».

Эффективное взаимодействие. Наличие достаточного количества квалифицированного персонала – условие для качественного функционирования ЦОДа необходимое, но не достаточное. Сложности часто возникают в ходе взаимодействия разных служб и отдельных сотрудников между собой. Проблем, как правило, не бывает, пока организация небольшая. Но в крупных коллективах с различными подразделениями, с привлечением внешних партнеров на отдельные работы слабоорганизованный информационный обмен однозначно приведет к неудачам.

Управление будущими рисками. Успешное решение всех проблем сегодня, к сожалению, не гарантирует, что завтра они не возникнут снова. В отношении персонала основным будущим риском яв-

ляется потеря специалиста. Это может произойти по разным причинам, многие из которых не подконтрольны работодателю. Соответственно, управлять таким риском можно только путем обеспечения готовности к потерям сотрудников: например, путем планомерной подготовки ряда сотрудников к исполнению обязанностей более опытных коллег и руководителей, т. е. формированием собственного кадрового резерва.

Обратим еще раз внимание на то, что в стандарте явно обозначены требования к квалификации персонала службы эксплуатации, и их соблюдение – важный элемент поддержания операционной устойчивости ЦОДа.

Практическое применение модели компетенций

Основываясь на всем комплексе требований, которые изложены в разделе Стандарта операционной устойчивости, посвященном квалификации персонала, можно рекомендовать следующий подход к их выполнению:

- сформировать обобщенную модель компетенций персонала службы эксплуатации дата-центра;
- детализировать требования модели компетенций с учетом установленного оборудования, требований к функционированию дата-центра и выбранной модели обслуживания;
- разработать и применять детальные карты компетенций по отдельным ролям исполнителей процессов службы эксплуатации;
- обеспечить прием сотрудников и привлечение внешних исполнителей с учетом соответствия профилям компетенций;
- построить и поддерживать регулярное инструктирование привлекаемых к работам специалистов согласно их зонам ответственности и требованиям к квалификации;
- организовать периодическое обновление профилей компетенций;



- сформировать и исполнять программу обучения и переподготовки персонала с учетом требований к компетенциям.

Напомним, что в стандарте требования к квалификации явно обозначены только в части необходимости наличия требуемых регулятором лицензий, и то без соответствующей конкретизации. При этом имеется широкий перечень иных требований, касающихся квалификации персонала косвенно. В большей степени они ориентированы на выработку требуемых навыков и компетенций путем проведения регулярного обучения и инструктирования.

Именно на это в основном направлены соответствующие положения стандарта Uptime Institute. Логика здесь следующая: действуя планомерно и непрерывно, можно обеспечить необходимую подготовку сотрудников и быть уверенным в ее качестве, в то время как ориентация на привлечение уже готовых специалистов извне несет в себе большой объем сложностей и рисков, не говоря уже о том, что всякий объект имеет свои особенности реализации и обслуживания инженерной инфраструктуры, которые, как правило, не афишируются.

Каналы подготовки специалистов по эксплуатации дата-центров в России и в мире

Хотя в настоящее время явное упоминание дата-центров в программах российских учебных заведений обнаружить нелегко, ситуация вовсе не безнадежна. В соответствии с Общероссийским классификатором специальностей по образованию, средние профессиональные учебные заведения готовят специалистов с квалификацией «техник» и «старший техник», в том числе по следующим направлениям: техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям); эксплуатация средств связи; строительство и эксплуатация зданий и сооружений; монтаж и эксплуатация внутренних сантехнических устройств и вентиляции; техническое обслуживание и ремонт радиоэлектронной техники (по отраслям); техническое обслуживание средств вычислительной техники и компьютерных сетей.

Таким образом, возможности для получения базовых знаний по эксплуатации и обслуживанию основных инженерных систем дата-центра имеются. Правда, дальнейшее образование по данному направлению в нашей стране систематизировано слабо. В основном оно сводится к краткосрочным (один-два дня) тренингам по обслуживанию конкретного оборудования, проводимым представителями его производителей и/или поставщиков. Главные недостатки такого подхода – слабое понимание персоналом комплексной картины обслуживаемого объекта и составляющих его систем, «заточенность» на работу с оборудованием конкретного вендора, использование несовпадающей терминологии и т.д. В результате подавляющее большинство дата-центров испытывают затруднения при поиске нужных специалистов на рынке и вынуждены готовить их непосредственно на рабочих местах, в

основном передачей опыта и знаний от старших товарищей и самообразованием сотрудников.

За рубежом ситуация отличается в лучшую сторону. Управление дата-центрами, обеспечение их качественного обслуживания там осознали как отдельный вид деятельности намного раньше, чем у нас. Результатом стало не только формирование специализированных образовательных компаний, но и целого класса услуг обучения и консультирования по тематике обслуживания и эксплуатации инженерных систем ЦОДов.

И, как принято на Западе, факт прохождения обучения и успешной сдачи экзамена (который почти во всех случаях обязателен) подтверждается выдачей соответствующего сертификата. Как правило, сертификат выдается той же компанией, которая учила, хотя имеются примеры и независимой (от обучающей компании) сертификации специалистов. В результате этого названия сертификатов пока не согласованы и не стандартизованы. Есть среди них, например, Data Centre Professional, Data Centre Cooling Professional, Mission Critical Operations Professional, Data Centre Facilities Operations Manager... Даже созвучные Data Centre Professional, выдаваемый одним учебным центром, и Data Centre Cooling Professional, выдаваемый другим, подразумевают серьезно различающийся уровень квалификации, включая существенную разницу в объеме подготовки, требованиях к опыту специалистов и др.

Помимо этого, на зарубежном рынке работает ряд крупных консалтинговых организаций, которые не только помогают эксплуатирующим структурам выстраивать правильную операционную модель, но и проводят специализированное обучение как эксплуатации отдельных систем, так и общей организации эксплуатации и управлению этой деятельностью.



Очевидно, что надежное и качественное функционирование дата-центра непосредственно связано с квалификацией персонала службы эксплуатации. О большой роли персонала свидетельствует и внимание, которое уделено ему в Стандарте операционной устойчивости. Изложенные в нем требования ориентированы не только на текущий квалификационный уровень сотрудников, но и на наличие организационных механизмов, гарантирующих сохранение этого уровня в течение длительного времени.

Сегодня каждая организация самостоятельно формирует перечень требований к сотрудникам службы эксплуатации дата-центров. Единая модель отсутствует не только в России, но и в мире. В то же время определенные условия для выработки единых требований сформировались, существуют несколько видов обучения и сертификации специалистов. Важно, чтобы в период идущего в нашей стране активного роста объема и зрелости рынка ЦОДов всем процессам, связанным с квалификацией персонала, было уделено должное внимание. ИКС

Формализуем работу ИТ-подразделений

Переход к процессному управлению требует от компаний функционального описания сфер деятельности их ИТ-подразделений, но далеко не все на практике справляются с этой задачей. Тем не менее существуют определенные методы составления формализованного описания. Один из важных моментов – применение технического, организационного и правового анализа для организации деятельности ИТ-службы.



Павел КАНЕВ

Анализируя в компаниях положения о подразделениях ИТ, нередко сталкиваешься с отсутствием в них ключевых разделов, например раздела «Полномочия», а также с абстрактными формулировками функций и задач. Казалось бы, руководителю нет ничего проще, чем сформулировать в положении об отделе, какую работу он фактически выполняет (см. левый столбец табл. 1).

Табл. 1. Функции и задачи подразделения

До формализации	После формализации
Функция: участие в развитии межсистемных решений по оптимизации функционала	Функция: управление разработкой ИС Задача: создание интерфейсов интеграции Объект: СЭД, CRM-, ERP-системы
Задача: оказание содействия в заключении договоров с внешними поставщиками	Функция: договорная деятельность Задача: согласование спецификации Объект: материалы

Как видно из табл. 1, в результате формализации все получается не так однозначно, как хотелось бы. Непросто увидеть различия между данными в левом и правом столбце, но вот как перейти от первого варианта ко второму? За кажущейся простотой темы скрывается весьма сложная методическая работа, которой часто не уделяется должного внимания.

Система ценностей

Для начала необходимо определить используемую систему ценностей – именно логически взаимосвязанную систему (например, такую, как на рисунке), а не фрагменты знаний из различных систем.

Примем, что в приведенной модели сфера деятельности рассматривается как работа, выполнение которой базируется на компетентности сотрудников и компетенциях подразделения (иногда вместо «сферы деятельности» употребляют термин «зона ответственности»). Навыки здесь в явной форме не указаны, поскольку они являются производными от умений.

Объекты – то, чем/кем управляет или что/кого контролирует подразделение. Объекты делятся на программное обеспечение, аппаратное, организационное и кадровое.

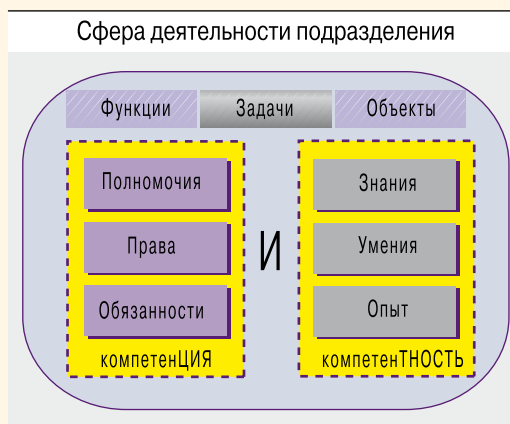
Функция – деятельность объекта в рамках некоторой системы и конкретные действия, совершаемые над управляемым или контролируемым объектом. В технике и в психологии, выражаясь обычным языком, функция обозначает принадлежность к чему-либо, что применяется для устремлений, решения задач, намерений, достижения цели. Функция может являться частью процесса. В рамках подразделения функции бывают основными и дополнительными.

Задача – проблемная ситуация с заданной в явном виде целью, которую необходимо достичь/выполнить. В отличие от функции, которая может осуществляться постоянно, задача должна быть успешно завершена. Более узкое определение называет задачей ситуацию с известным начальным состоянием системы (как есть) и ее конечным состоянием (как будет), причем алгоритм достижения конечного состояния при движении от начального известного. Задачу возможно декомпозировать на операции.

Теперь нам необходимы средства сбора информации. Таким средством служит технический аудит, проводимый при помощи автоматизированных систем и/или интервьюирования сотрудников. Определим его область применения следующим образом:

- ✓ цель – выявить объекты управления и контроля подразделений ИТ;
- ✓ вид – первичный;
- ✓ охват – сплошной;
- ✓ метод – фактический.

Подробно останавливаться на методах проведения аудита и анализа здесь не представляется возможным.



Функции и задачи

Итак, информация собрана и структурирована. Далее мы будем ее формализовать, распределив по таблицам. Взаимосвязь функций, задач и объектов (контроля или управления) при описании деятельности подразделения показана в табл. 2.

Надо учитывать, что между управлением и контролем существует значительная разница: управление без контроля невозможно, тогда как контроль объекта осуществляется без воздействия на него. Другими словами, контроль объекта не предполагает активного взаимодействия с ним.

Табл. 2. Контроль и управление

Функция	Задача	Объект
Разработка ИС (основная)	Проектировать логический дизайн Создавать программный код Тестировать Создавать интерфейсы интеграции Вводить в эксплуатацию и выводить из эксплуатации	Платформы разработки Разрабатываемые системы Поддерживаемая аудитория
Разработка регламентов (основная)	Создавать: техническое предложение техническое задание аналитическую записку положение о системе руководство пользователя	
Зарплата и кадры (дополнительная)	Указать требования к персоналу Заполнить табель учета	
Договорная (дополнительная)	Согласовать спецификацию Верифицировать факт поставки	

Рассмотрим пример: если система мониторинга реагирует на выход параметров объекта за установленные рамки только путем визуализации/оповещения о его состоянии, то она системой контроля и остается. Но если она окажет корректирующее воздействие, возвращая параметры объекта в установленные пределы, ее уже можно классифицировать как систему DCIM (но это тема отдельного обсуждения). Следовательно, управление и контроль необходимо разнести по разным таблицам – на основании их существенного отличия.

В качестве аналогии здесь можно привести различия в целях между разработкой и сопровождением ПО: сопровождение (цель) – это обеспечение неизменности характеристик эксплуатируемой системы, а разработка (цель) – улучшение характеристик эксплуатируемых и создание новых систем.

Разделение разработки и сопровождения между разными подразделениями обеспечивает выполнение принципа сдержек и противовесов, что становится очевидным при сравнении целей подразделений.

Из приведенных примеров также следует, что необходимо использовать терминологию, соответствующую данному контексту. Если мы действуем в сфере разработки прикладного ПО, то и знания следует применять из этой области.

Компетентность

Далее будем считать, что выполнять описанные выше функции над объектами и решать задачи должны сотрудники, для чего им потребуются определенные знания, умения (навыки как их производная) и опыт. В качестве примера сформулируем требования к компетентности руководителя отдела (табл. 3, перечень неполный).

Подчеркнем, что сотруднику вовсе необязательно иметь энциклопедические знания по всем областям, достаточно держать в памяти ключевую информацию, а что касается остального – знать, где и как эти данные можно оперативно получить. Следует также помнить,

что если сотрудник обладает знаниями, это еще не означает, что он сможет применить их на практике.

При выборе необходимо определиться, какие именно навыки потребуются для выполнения работ – двигательные, интеллектуальные, перцептивные. Навыки являются логическим продолжением умений, когда человек уже выполняет какие-то действия неосознанно, автоматически. Для практического осознания разницы наденьте очки/линзы, зрительно переворачивающие изображение, и попробуйте поиграть в баскетбол. Этот опыт покажет, как важно выбирать сотрудников, уже обладающих требуемыми навыками.

Требования к подчиненным в должностных инструкциях можно составлять аналогично. На описание каждой должности достаточно страницы формата А4.

Компетенции

Переходим к завершающей стадии – это формирование полномочий, прав и обязанностей подразделения, а также связанной с ними ответственности, которые реализует руководитель.

Мы не будем здесь углубляться в тонкости использования терминологии, отметим только, что важно не приравнивать обязанности к правам, поскольку распоряжение, поступающее от уполномоченного лица, обязательно для исполнения, тогда как рекомендация, данная сотрудником, имеющим на это право, может и не выполняться. Это только часть различий, поскольку полномочия включают в себя свойства прав, как управление включает контроль.

Табл. 3. Компетентность (на примере руководителя отдела)

Знания	Опыт применения
Высшее техническое образование	Опыт работы ведущим инженером не менее 5 лет
Платформы	Список платформ. Разработка СЭД
Системы	Внедрение и сопровождение PDM/PLM/ERP-систем не менее 3 лет
Моделирование доступа	Модели – мандатная, дискреционная, ролевая. Не менее 2 лет
Создание документов	Аналитическая записка. Техническое задание. Не менее 2 лет
Управление рисками	Идентификация и анализ рисков. Не менее 2 лет
Умения	Опыт применения
Дипломатичность	Тактично взаимодействовать с людьми. Вести переговоры. Не менее 2 лет
Самостоятельность	Проявлять независимость действий и суждений, инициативу, решительность, адекватную самооценку и чувство личной ответственности. Самостоятельное принятие организационных решений. Не менее 2 лет
Формирование требований	Преобразовывать потребности в функциональные требования и далее в архитектурные. Не менее 2 лет
Навыки	Опыт применения
Английский язык уровня Intermediate	Взаимодействие с технической поддержкой вендора. Не менее 2 лет
Вождение ТС категории Б	Не менее 3 лет

К примеру, владелец процесса разработки не уполномочен утверждать внедрение новых систем в эксплуатацию, но имеет право это согласовывать. Владелец процесса сопровождения не уполномочен утверждать разработку новых систем, но имеет право это согласовывать. Каждый из руководителей уполномочен приказывать предоставить административные права доступа в своих системах, но у него нет технических прав сделать это самостоятельно. При возникновении спорной ситуации каждый из руководителей имеет право воспользоваться вертикальной эскалацией.

Полномочия утверждать внедрение новых систем принадлежат вышестоящему руководителю, который принимает решение на основании данных и виз обоих подчиненных ему руководителей. Отметим, что «утверждающий» может согласиться с визой «согласующего», а может принять решение вопреки этой визе.

В столбце «Ответственность» необходимо задать уровень негативных последствий в случае нарушения установленных требований. Можно применять следующие виды ответственности – дисциплинарную, материальную, моральную; можно также уточнить, в какой именно мере. При привлечении к ответственности важным условием является наличие вины. Вряд ли правильно, например, привлекать к ответственности сотрудника, действия которого хотя и привели к отрицательным последствиям, но были вызваны прямым приказом непосредственного руководителя.

Завершив описание требований к сотрудникам, в последующем можно перейти к объективной оценке их деятельности. Это будет уже процесс оценки и мотивации персонала, который реально автоматизировать, если характеризовать его измеряемыми величинами. Так, добавив к табл. 4 столбец «Поощрения за достиже-

ния», мы получим систему положительной и отрицательной мотивации.

Вернемся к нашей теме и сформулируем цель деятельности. Отметим, что использовать принципы SMART не следует, поскольку требуется в большей степени описание области применения подразделения, т.е. его назначения, в соответствии с которым должны поступать приказы и распоряжения руководства.

Цель: Разработка и внедрение прикладного программного обеспечения.

Следствие 1: Исходя из цели, руководитель подразделения использует все имеющиеся у него ресурсы для ее достижения, т.е. разрабатывает и внедряет ИС. В противном случае, например если подразделение разрабатывает систему (KPI – разработано пять новых компонентов за три месяца) и не внедряет (KGI – внедрен один компонент системы из пяти за три месяца), оно будет иметь высокий KPI и низкий KGI. А это уже метрики процессного управления, указывающие на низкую результативность деятельности подразделения (в нашем случае в части Release Management).

Следствие 2: Становится очевидной балансировка ресурсов, т.е. руководитель будет выделять большее их количество на основные функции и задачи, обеспечивающие достижение цели, что потребует перераспределения функций и задач между подразделениями, исходя из критерия специализации.

Итоговый документ

В результате мы должны получить положение о подразделении объемом 15–20 страниц формата А4, примерно с таким оглавлением:

- Нормативные ссылки
- Термины и определения

Табл. 4. Компетенции руководителя подразделения (разработка систем)

Полномочия	Ответственность за превышение
Давать инженерам указания по сопровождению разработанных ИС	Дисциплинарная, материальная, моральная. Пример моральной ответственности: «худший советчик месяца» на доске «почета» (совет давать меньше надо) – выполнение указания привело к массовому сбою в работе систем
Утверждать решение о делегировании привилегированных прав доступа в сопровождаемых ИС	
Согласовывать разработку и сопровождение систем	
Принимать решение об изменении приоритета разработки	
Привлекать внешних и внутренних специалистов и консультантов для реализации согласованных с руководством проектов разработки ИС	
Права	Ответственность за злоупотребление
Использовать предоставленные подразделению информационные и материальные ресурсы	Дисциплинарная, материальная, моральная. Пример материальной ответственности: депремирование за порчу материального имущества и потерю данных компании
Привлекать сотрудников подразделения к дисциплинарной и материальной (депремирование) ответственности	
Проводить горизонтальную и вертикальную эскалацию запросов	
Инициировать, проводить и участвовать в совещаниях, связанных со сферой деятельности подразделения	
Не имеет прав регистрировать запрос на разработку	
Не имеет прав (технических) делегирования доступа в системах	
Обязанности	Ответственность за неисполнение
Обеспечивать достижение целей (KPI&KGI)	Дисциплинарная, материальная, моральная. Пример дисциплинарной ответственности: выговор за недостижение целевых показателей в течение 6 месяцев подряд
Визировать документы подразделения	
Предоставлять подразделению внутреннего контроля запрошенные данные, в соответствии с приказом о его авторизации и планом проведения аудита	

- Общие положения
- Позиция в оргструктуре
- Требования к руководителю
- Функции и задачи
- Полномочия, права, обязанности, ответственность
- Показатели качества
- Календарный план систематически выполняемых задач (приложение).

Здесь можно дать следующие рекомендации: сформируйте содержание документа по принципу «от общего к частному» и используйте метод ветвления. Положение является документом тактического уровня и требует соотнесения с целями компании.

После завершения работ над положением о подразделении декомпозируем его в должностные инструкции сотрудников (это документы оперативного уровня).

Таким образом, мы видим, что для формализации работы подразделений следует применять как технические, организационные, так и правовые знания.

Отметим, что положения о подразделениях должны предоставлять данные, необходимые для организации

совместной деятельности подразделений. Но они будут использоваться по прямому назначению, только если будет видна практическая отдача от них.

Вместо заключения

Формализация сфер деятельности часто приводит к интересным результатам. Например, при их описании приведенными выше методами руководитель отдела может осознать, что примерно 40% ресурсов его подразделения расходуется на дополнительные функции, задачи и объекты. Часто в результате аудита выявляются и случаи вменения обязанностей без предоставления должных полномочий. И этого оказывается достаточно для возникновения интереса к документированию деятельности.

Далее, использование описанных выше методов формализации может стать базой для постепенного перехода от функционального к процессному управлению. А результаты могут использоваться для оценки эффективности системы управления компаний. ИКС

Некоторые особенности проектирования чиллерных систем



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

Чиллерные системы для охлаждения ИТ-оборудования – наиболее обоснованный на сегодня выбор для крупных проектов. Но в работе таких систем есть ряд тонкостей, которые зачастую остаются за рамками учебников и пособий по проектированию.

Преимущества чиллерных систем – это и практически неограниченная мощность стойки, и стабильная работа при значительных перепадах нагрузки по месту и времени, и беспроблемное «свободное охлаждение», и простота

реализации бесперебойного охлаждения. При этом размеры и стоимость системы остаются в разумных пределах.

Гибкость возможных решений является в этом случае и достоинством и недостатком. При том что сама по себе чиллерная трасса устроена подобно обычному водопроводу, имеется достаточно много вопросов, на которые следует обратить внимание, и фактически неограниченное число вариантов исполнения системы. Это и хорошо и плохо: с одной стороны, есть способы решения любой задачи, а с другой – очевидно, что можно допустить любое количество ошибок.

Сначала несколько слов о том, что же представляют собой чиллерные системы, или, в отечественной терминологии, системы с «ледяной водой». Основной их признак – использование для охлаждения холодной воды. Она, в свою очередь, производится чиллером – по сути, обычным кондиционером, только его испаритель отбирает тепло у жидкости, а не у воздуха. В зим-

ний период жидкость может охлаждаться напрямую, за счет холодного внешнего воздуха.

Типичный диапазон температур применяемой воды – от 5 до 20°C. Помимо воды могут использоваться растворы этиленгликоля и пропиленгликоля. Проходя через теплообменники кондиционеров, жидкость нагревается на 5–15°C и возвращается в чиллер.

Сам чиллер может быть как с гликолевой схемой (что типично для систем со свободным охлаждением), так и с воздушной. Размещается он либо в помещении, либо на улице, в виде моноблока, объединенного с теплообменником.

Подбор концентрации раствора гликоля

Чтобы предотвратить замерзание жидкостных трасс, к воде добавляют антифриз – гликоль. Как правило, это этиленгликоль (он слегка токсичен, но относительно дешев и не слишком вязок) либо пропиленгликоль (он представляет собой безвредную пищевую добавку, но дороже и более вязкий). Один из определяющих для проекта вопросов – концентрация гликоля. От нее зависит температура замерзания раствора, и порой наивные проектировщики пытаются добиться, чтобы она была ниже, чем минимальная проектная температура на улице.

Концентрация гликоля, достаточная для того, чтобы раствор не замерзал при минимальной внешней температуре, вовсе не гарантирует работоспособности системы. Дело в том, что, будучи охлажденным, гли-

коль становится очень вязким. Такой студень, формально жидкий, плохо поддается перекачиванию, более того, может вызвать поломку насосов. Следовательно, требуется непрерывная прокачка жидкости, с подогревом неработающих контуров. И разумеется, все внешние магистрали должны иметь качественную теплоизоляцию, желательно по принципу теплоцентралей, с жестким внешним защитным кожухом.

Минусов у высоких концентраций гликоля много – цена, вязкость, пониженная теплоемкость, приводящая к падению мощности и необходимости увеличения объема прокачки. Для предотвращения разрыва труб достаточно раствора с массовой концентрацией выше 35,5% для пропиленгликоля и 32,5% для этиленгликоля. Единственно, что не следует закрывать замерзающие контуры наглухо, при замерзании раствор гликоля все равно расширяется, просто, в отличие от воды, не только в радиальном направлении.

Выбор температуры теплоносителя

Чиллерный контур характеризуется парой значений температуры, записываемых через дробь, к примеру, традиционные 7/12°C или более современные 10/15°C. Для источника холода это соответственно создаваемая им температура и температура возвращаемой от потребителей жидкости. В свою очередь, с точки зрения потребителей холода это температуры получаемой жидкости и жидкости, сбрасываемой обратно в систему. Поскольку система замкнута, такое представление, естественно, симметрич-

но. Важны как сами значения температуры, так и разница между ними – дельта. К сожалению, зачастую при проектировании так и останавливаются на стандартных значениях, поскольку именно они приводятся в каталогах.

Сначала рассмотрим первое число в паре – температуру подаваемого теплоносителя. Как ее повышение, так и понижение имеют свои положительные и отрицательные стороны (см. врезку «Плюсы и минусы изменения температуры теплоносителя»).

Второе число важно в первую очередь как допустимый предел. Если на чиллер подавать слишком теплую воду, он просто остановится – по той же причине, что и обычный кондиционер при перегрузке. Впрочем, и при слишком холодной воде на входе чиллер откажется работать. Собственно, обычные проблемы фреонового цикла – слишком высокое или слишком низкое давление в испарителе.

Понимание этих ограничений важно не только при проектировании, но и при эксплуатации. В общем случае ни зимой в морозы, ни летом в жару чиллерную систему так просто запустить не получится.

И наконец, дельта – разница температур. Произведение ее на теплоемкость жидкости и расход дает фактическое количество переносимого тепла. Для воды, по грубой оценке, один литр в секунду, нагреваемый/охлаждаемый на 5°C, переносит 20 кВт тепла.

По факту перепад температур регулируется путем изменения расхода. При большом потоке дельта меньше, при малом больше.

б и з н е с - п а р т н е р

Выбор чиллера – без стереотипов



Виктор ГАВРИЛОВ,
технический директор,
«АМДтехнологии»

На что нужно обратить внимание, если система охлаждения ЦОДа строится на базе холодильных машин – чиллеров? Прежде всего не стоит следовать сложившимся стереотипам. Скажем, подбирать чиллер на температуру воды 7–12°C, как это принято в системах комфортного кондиционирования, точно не стоит. Важнейшим фактором оценки работы ЦОДа является его энергоэффективность; соответственно, чем выше температура воды в контуре охлаждения, тем раньше система кондиционирования ЦОДа перейдет в режим фрикулинга. Следовательно, гораздо выгоднее подбирать чиллеры, рассчитанные на поддержание температуры воды на выходе из холодильной машины около 10 или 12, в ряде случаев даже 18°C.

Еще один фактор, влияющий на потребляемую мощность системы кондиционирования, – это расчетный перепад температуры воды. Стандартно принятое его значение составляет 5°C. Например, систему холодоснабжения рассчитывают на температурный график 7–12 или 10–15°C. Практически любой чиллер может работать в более широком

диапазоне – с допустимым перепадом температур от 3 до 8°C. Соответственно, пересчитав систему на график температуры воды в контуре холодоснабжения 10–16 или 12–18°C, можно снизить потребляемую мощность не только холодильной машины, но и циркуляционных насосов, а также уменьшить диаметры трубопроводов.

Весьма важно определиться с типом применяемых компрессоров и с конфигурацией холодильной машины. Моноблочный чиллер занимает меньше места, но позже переходит в режим фрикулинга. Для чиллера внутренней установки можно подобрать наружные блоки таким образом, что режим 100%-ного свободного охлаждения будет доступен уже при температуре на улице ниже +10°C. Используя высокотемпературный потенциал воды в совокупности с чиллером внутренней установки и турбокомпрессором, вполне реально получить значение PUE примерно 1,16–1,18.



Плюсы и минусы изменения температуры теплоносителя



Понижение температуры

Увеличивается производительность кондиционеров, что позволяет уменьшать их количество. Баки-накопители можно проектировать на два-три прохода, в соответствующее число раз уменьшая их размер. Проще использовать перепад температур входа и выхода больше 5°C, что пропорционально уменьшает общий расход, в свою очередь, уменьшая диаметр магистралей и мощность насосов. Легко удаляется избыточная влажность, если инсталляция этого требует. Даже если у кондиционеров нет специального режима осушения, они будут удалять излишек воды за счет конденсации.



Более поздний фрикулинг и меньшая производительность чиллеров. Выше требования к теплоизоляции магистралей и элементов системы (на практике при повреждении изоляции трубы с теплоносителем с нее тут же начинает капать конденсат). Для многих кондиционеров падает коэффициент явной производительности за счет ненужной конденсации воды на теплообменниках. Это уменьшает полезную производительность кондиционеров и увеличивает нагрузку на систему увлажнения.

Повышение температуры

Выше производительность чиллеров и фрикулинга. Менее строгие требования к теплоизоляции за счет меньшего перепада температур и более высокой температуры (может означать отсутствие конденсата в принципе).

Большее число кондиционеров или их больший типоразмер. Большие баки-накопители (из расчета штатного расхода). Перепад температур воды входа и выхода ограничен. К примеру, далеко не всякий чиллер способен работать с температурой воды на входе 25°C. Возникают и потенциальные проблемы при перезапуске с горячим баком. Невозможно осушение слишком влажного воздуха (но эту задачу можно переложить на систему приточной вентиляции).

Как ни парадоксально на первый взгляд, производительность оборудования выше при малой разнице температур: хотя перепад их и небольшой, количество теплоносителя при этом велико и процессы теплообмена максимально эффективны.

Важно понимать, что значение дельта ограничено и сверху и снизу. Как правило, для чиллеров перепад составляет от 4 до 8°C, и связано это с устройством применяемых теплообменников. При меньшем перепаде поток жидкости слишком сильный, что вызывает заметное падение давления и опасные вибрации. При большем перепаде, наоборот, слишком сильно уменьшается эффективность теплообмена из-за недостаточной турбулентности. В итоге есть риск локально переохладить жидкость в чиллере, в случае воды – даже заморозить ее.

Соответственно выигрыш от уменьшения перепада температур состоит в том, что растет производительность кондиционеров, что позволяет уменьшить их количество, и немного увеличивается производительность чиллеров и фрикулинга.

Недостатки малого перепада температур таковы:

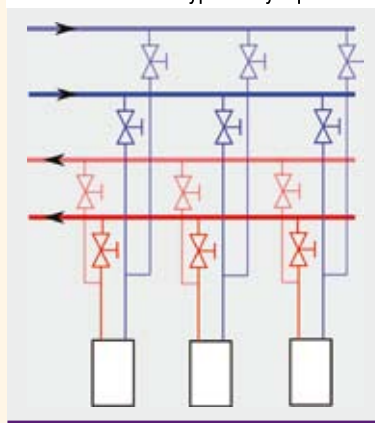
- большой расход, а соответственно более мощные насосы, круглый год потребляющие больше энергии;
- большее падение давления на оборудовании, соответственно еще более мощные насосы;
- большой диаметр труб и их обвязки, что, разумеется, стоит дороже;
- шум теплообменников.

Кратко резюмируем вышеизложенное: на сегодня в качестве первой итерации можно ориентироваться на пару значений 10/16°C. Это, с одной стороны, позволяет применять осушение, с другой – практически любое

оборудование работает с такими значениями без сильной деградации параметров. Далее следует ориентироваться на задачу. При наличии требований по максимальной компактности нужно снижать температуру и перепад. При наличии требований по максимальной энергоэффективности – наоборот, повышать значения обоих параметров. Разумеется, следует учитывать упомянутые предельные ограничения. Ну и в очередной раз напомним, что следует пользоваться специализированными программами подбора или диаграммами из руководств, а не просто данными из общих каталогов.

И еще одна ремарка по теме. Современное оборудование охлаждения, особенно внутристоечное, может требовать достаточно экзотических значений температур теплоносителя, которые не реализуются при помощи обычного чиллера. Никаких проблем с этим нет, просто устраивается второй контур, с собственным насосом и, возможно, с промежуточным теплообменником.

Рис. 1. Переключение на уровне устройств



Выбор отказоустойчивой топологии

К особенностям нашей отрасли относится достаточно частое наличие в проектах требований по отказоустойчивости. Соответственно, согласно

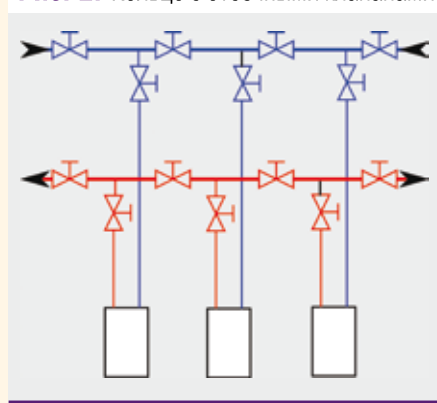
стандартам Uptime Institute, для уровня отказоустойчивости Tier II требуется формальная избыточность активного оборудования (в нашем случае это чиллеры, насосы и кондиционеры), для Tier III – возможность заменить на работающей системе любой из элементов, включая трубы, а для Tier IV – автоматическое парирование любого единичного отказа.

Реализовать параллельное подключение оборудования для Tier II несложно, Tier IV в простейшем варианте достигается дублированием независимых систем,

поэтому больше всего вопросов возникает с Tier III. Кроме того, это наиболее часто встречающийся уровень требований.

Для решения задачи применяют три схемы. Первая – переключение на уровне устройств (рис. 1). Ее недостатки – требования по согласованному переключению и потенциальная множественность точек отказа. Кроме того, если это внешний контур, то, согласно требованиям по незамерзанию, придется либо регулярно выполнять переключение, либо предусматривать какой-либо иной способ подогрева не работающих в данный момент труб.

Рис. 2. Кольцо с отсечными клапанами



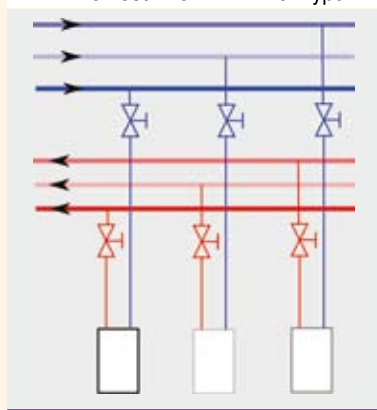
Вторая схема, кольцо с отсечными клапанами (рис. 2), заметно более рациональна и имеет значительно меньше уязвимых точек. Ее недостаток – относительная дороговизна вентилей большого диаметра. Кстати, эта же схема является естествен-

ным переходником между участками N+1, N+2, 2N и обратно.

Третья схема – внешнее резервирование с несколькими независимыми контурами (рис. 3). Эту схему, по мнению автора, можно рекомендовать в большинстве случаев – но при этом она, к сожалению, реже всего используется. Дополнительные краны в ней не нужны вообще, и логика работы системы проста и прозрачна. Ее недостаток – необходимость устраивать не менее трех независимых систем, хотя и относительно маломощных. Обычно вызывает трудность и прокладка труб, занимающих много места.

Кстати, все приведенные здесь схемы могут быть использованы и для реализации Tier IV, несмотря на отсутствие полного дублирования. Требуется только автоматизировать переключение кранов в первых двух схемах, что само по себе нетривиально. Третья схема никакой дополнительной автоматики не потребует. ИКС

Рис. 3. Внешнее резервирование с независимыми контурами



Аудит инженерной инфраструктуры ЦОДа

зачем
и как?

В последние два года востребованность аудита в области строительства, эксплуатации и сервисного обслуживания ЦОДов значительно повысилась. Получить объективную оценку состояния инфраструктуры дата-центра его владельца подталкивает неизбежное устаревание оборудования на фоне непрерывного роста требований к «инженерке».

Интенсивное развитие рынка ЦОДов в совокупности с растущими потребностями в оперативном внедрении новых сервисов и бизнес-процессов зачастую не позволяет владельцам и топ-менеджменту дата-центров своевременно оценить риски несоответствия мощностей инженерной инфраструктуры стоящим перед ней задачам. Вместе с тем инженерное оборудование ЦОДов, построенных в 2005–2008 гг., сегодня активно устаревает и нуждается в модернизации. Избежать аварий и простоев бизнеса может помочь услуга аудита ЦОДа, предлагаемая системными интеграторами рынка инженерных систем.

Проведение аудита дает возможность получить объективную оценку состояния инженерной инфраструктуры и принять меры для поддержания безаварийной работы оборудования, устранить недоработки или скрытые недостатки отдельных систем и всего объекта в целом. Такое обследование помогает определить па-

раметры, необходимые для непрерывной и правильной эксплуатации критичного оборудования и приложений.

Перед топ-менеджментом ЦОДа встает вполне логичный вопрос – чьими силами проводить аудит? Своими? Силами интегратора? Определенно, наилучшим вариантом будет связка заказчик – интегратор. Никто лучше службы эксплуатации заказчика не знает всех нюансов работы аудируемого объекта, так же, как никто лучше интегратора, предоставляющего услугу аудита инженерной инфраструктуры ЦОДа, и, самое главное, принимавшего участие во всех этапах строительства дата-центра, не представляет, как именно инженерные системы должны работать.



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

Когда нужен аудит?

Практика показывает, что нагрузка на инженерное оборудование приближается к критической точке примерно через четыре-пять лет после начала эксплуатации ЦОДа. Конечно, для каждого ЦОДа этот срок индивидуален, но, как правило, за это время основное инженерное оборудование устаревает, а плотность ИТ-оборудования возрастает.

Для заказчиков, чьи бизнес-процессы не стоят на месте, а совершенствуются и требуют год от года все больших и больших ресурсов, модернизация – процесс

неизбежный. Для того чтобы сформулировать требования, в соответствии с которыми нужно будет модернизировать инженерную инфраструктуру, и необходимо проводить аудит.

Этапы аудита

Обычно аудит инженерной инфраструктуры ЦОДа состоит из нескольких этапов. Первый из них – анализ проектных решений и исполнительной документации.

Не нужно путать этот этап с экспертизой проекта, которая проводится после выпуска проектной доку-

Методика проведения аудита системы кондиционирования ЦОДа

№	Вид работ	Предполагаемая продолжительность работ, ч	Возможные риски
1	Проверка состава и комплектности системы прецизионного кондиционирования на соответствие проектной спецификации	1	Нет
2	Проверка правильности установки и монтажа системы прецизионного кондиционирования: поиск ошибок монтажа, которые могут приводить к снижению функциональных характеристик или неработоспособности оборудования; проверка соответствия размещения оборудования проектной документации	3	Нет
3	Проверка внешнего состояния оборудования системы прецизионного кондиционирования (проводится как на внешних, так и на внутренних блоках кондиционеров): осмотр оборудования на предмет выявления загрязнений, следов ударов, воздействия жидкости, химических веществ, высокой температуры, трещин, вмятин и др. повреждений; изучение надежности крепления механических частей оборудования	2	Нет
4	Проверка работы оборудования системы прецизионного кондиционирования в автоматическом режиме: проверка точности поддержания заданной температуры и относительной влажности в помещении; проверка совместной работы прецизионных кондиционеров в штатном режиме (попеременная работа кондиционеров или работа с постоянным резервом, цикл работы кондиционеров); проверка совместной работы кондиционеров в аварийном режиме (включение резервных кондиционеров при имитации аварии работающих). Проверка проводится при включенной системе stand by на всех кондиционерах, объединенных в сеть. Авария имитируется на каждом из работающих кондиционеров по очереди, пока не будут проверены все кондиционеры. Имитация аварии высокого давления производится путем размыкания вручную соответствующего цифрового входа. При моделировании аварий вредного воздействия на систему не оказывается. После имитации аварий испытываемая система возвращается в номинальное рабочее состояние	7	При резервировании по схеме N + 1 есть риск остаться без горячего резерва в случае аварийной остановки оборудования
5	Проверка параметров работы каждого кондиционера системы	3 ч для каждого кондиционера:	
5.1	Проверка рабочих параметров холодильного контура: измерение давления всасывания и нагнетания холодильным манометром; контроль перегрева всасываемых паров (цифровым контактным термометром); контроль переохлаждения жидкости после конденсатора (цифровым контактным термометром); измерение температуры нагнетания цифровым контактным термометром; измерение рабочих и пусковых токов компрессоров при помощи токоизмерительных клещей, мультиметра; измерение сопротивления обмоток компрессоров при помощи токоизмерительных клещей, мультиметра; проверка наличия влаги в контуре; проверка наличия (отсутствия) кислоты в масле при помощи теста кислотности масла	1,5	При резервировании по схеме N + 1 есть риск остаться без горячего резерва в случае аварийной остановки оборудования
5.2	Контроль поддержания в допустимых пределах относительной влажности в помещении и состояния рабочего цилиндра парувлажнителя	0,25	Нет
5.3	Проверка состояния электрических и электронных компонентов: срабатывания контакторов и пускателей; отсутствия вибраций электрических компонентов; корректной работы дисплея контроллера (исправность всех кнопок, отображение всех необходимых меню)	0,25	Нет
5.4	Проверка состояния и работоспособности дренажной системы: отсутствие протечек в местах крепления дренажных труб; проверка отвода конденсата путем принудительного слива	0,25	Риск протечки
5.5	Проверка состояния системы подачи воздуха: визуальный контроль состояния воздушных фильтров кондиционера; измерение фактического расхода воздуха через кондиционер при помощи анемометра; измерение температуры воздуха на выходе из кондиционера при помощи цифрового термометра	0,25	Нет
5.6	Проверка срабатывания защитных устройств: проверка срабатывания дифференциального реле давления воздуха (моделирование аварии засорения воздушного фильтра путем перекрытия поверхности фильтра воздухопроницаемым материалом); проверка корректного срабатывания реле низкого давления; проверка корректного срабатывания реле высокого давления (моделирование аварии высокого давления выключением автомата на вентиляторах наружного блока)	0,5	При резервировании по схеме N + 1 есть риск остаться без горячего резерва в случае аварийной остановки оборудования
6	Занесение результатов измерений и проверок в протокол	24	Нет
7	Оформление заключения по результатам экспертизы и выдача рекомендаций по дальнейшей эксплуатации оборудования	72	Нет

ментации, но ДО начала строительства. Экспертиза проекта – это, по сути, рассмотрение проекта с целью определения качества проектных решений, соответствия их заданию на проектирование и действующим нормам проектирования.

Анализ проектных решений уже построенного ЦОДа направлен в первую очередь на то, чтобы понять, насколько правильно выбраны проектные решения, достаточно ли хорошо проработаны детали проекта и насколько результат соответствует проектной документации и общепринятым нормам цодостроения. По результатам анализа проектных решений составляется отчет, в котором указываются выявленные погрешности проектирования и даются рекомендации по их устранению.

Следующий этап – собственно аудит инженерных систем жизнеобеспечения ЦОДа – требует участия большой экспертной команды со стороны аудитора, поскольку в него входят обследование помещений, инструментальные замеры основных технических параметров инженерных систем. Помимо проведения непосредственных испытаний и оценки работоспособности оборудования аудит включает в себя углубленное изучение воздушных потоков в серверном помещении, а также термическое моделирование, помогающее определить места перегрева.

Необходимо подчеркнуть, что проведение аудита инженерных систем не должно влиять на функционирование ЦОДа. Любые работы, влияющие на производительность сервисов ЦОДа, должны быть согласованы заранее и указаны в методике проведения обследования для каждой из аудируемых инженерных систем. Этот момент должен быть заказчиком заранее оговорен.

Методика проведения аудита

Под методикой в данном случае подразумевается алгоритм выполнения работ по обследованию и проведению испытаний для анализа работоспособности инженерных систем ЦОДа. Этот алгоритм должен быть разработан для каждой инженерной системы ЦОДа до начала работ и должен включать в себя подробное описание действий, их продолжительность и возможные риски (см., например, таблицу). После составления методика согласовывается всеми заинтересованными сторонами.

Все выявленные в ходе обследования отклонения от проектной документации, технического задания, ГОСТов, межотраслевых правил, документа-

ции завода – изготовителя оборудования фиксируются в отчете.

Что получит заказчик

Результатом проведения аудита проектной документации и инженерных систем ЦОДа обычно являются следующие документы:

- отчет о соответствии проектной документации техническому решению и о соответствии проектного решения нормам (ГОСТам и СНИПам), применяющимся для аудируемых систем;
- отчет о текущем состоянии инженерной инфраструктуры, ресурсе компонентов основного инженерного оборудования, выявленных проблемах и возможных рисках их влияния на отказоустойчивость. В случае проведения измерений в отчет по каждой инженерной системе включается протокол измерений;
- отчет о термическом моделировании с указанием мест перегрева;
- рекомендации по устранению обнаруженных проблем;
- заключение о соответствии ЦОДа уровню надежности по стандарту TIA/EIA-942 и стандартам, принятым на территории РФ;
- рекомендации по модернизации инженерной инфраструктуры ЦОДа, учитывающие планы заказчика по масштабированию.

Помимо отчетов аудитор может предоставить свою оценку качества выполнения работ сервисной компанией и/или службой эксплуатации. Эта информация поможет трезво оценить сложившуюся ситуацию и принять превентивные меры, которые уберегут ЦОД от простоев и других неприятных инцидентов в будущем. Не говоря уже о том, что выявление в ходе аудита проблем и слабых мест инженерной инфраструктуры (а точнее, устранение таковых) способствует продлению срока службы системы жизнеобеспечения ЦОДа. ИКС

EPV™ - Быстро. Просто. Разумно.

- Достоверная картина кабельных соединений в режиме реального времени
- Установка и эксплуатация системы без специально подготовленного персонала
- Встроенное ПО (не требует внешнего сервера)



За дополнительной информацией обращайтесь в Российское представительство RiT Technologies:
+7.495.363.9528
mkt@rit.ru | www.rit.ru

Реклама

Интернет-центры с поддержкой нескольких провайдеров

Линейка интернет-центров для домашних пользователей ZyXEL Keenetic пополнилась тремя моделями – Keenetic II, Keenetic Giga II и Keenetic Ultra. В них использован более быстродействующий процессор MediaTek RT6586 (700 МГц), поддерживающий многопоточную обработку данных, объем флеш-памяти увеличен вдвое (до 8 Мбайт), а ОЗУ – вчетверо (до 128 Мбайт).

Новые модели поддерживают функцию автоматической установки защищенного Wi-Fi-соединения WPS, на боковой панели имеются

два горизонтально расположенных и широко разнесенных USB-порта, что позволяет подключать габаритные 3G/4G-модемы. Кроме того, обеспечивается возможность одновременного подключения к нескольким кабельным интернет-провайдерам (максимум их может быть пять – по числу имеющихся Ethernet-портов).

Новые Keenetic поддерживают не только протокол IPv6, но и аппаратное ускорение передачи данных по этому протоколу. Также добавлены возможности подключения домаш-



него интернет-центра к корпоративной сети пользователя через защищенное VPN-соединение, организации Wi-Fi-точки доступа с поддержкой четырех Wi-Fi-сетей и одновременной работы в режимах точки доступа и Wi-Fi-подключения к интернет-провайдеру.

ZyXEL: + 7 (495) 542-8920

Серверная платформа для облачных вычислений

Kontron SYMKLOUD MS2900 Web предназначена для сетевых веб-приложений и приложений класса M2M в облачных вычислительных средах. Обладая высотой 2U и глубиной 21" (533,4 мм), платформа SYMKLOUD MS2900 Web имеет единственную или избыточную коммутацию L4–L7, до двух подсистем балансировки (выравнивания) нагрузки и до де-

вяти независимых четырехъядерных процессоров Intel Xeon E3-1265 Lv2. Все подсистемы коммутации, балансировки нагрузки и процессорные подсистемы допускают возможность «горячей» замены.

Для хранения данных предусмотрено подключение 2,5" жестких дисков (HDD) или 2,5" твердотельных накопителей (SSD) общим объемом до 13,5 Тбайт.

SYMKLOUD MS2900 Web поддерживает кластеры из восьми устройств высотой 2U и до 2,5 кластеров на стойку высотой 42U, если она не заполнена другим оборудованием. Для работы одного кластера требуется только одна подсистема балансировки нагрузки. Такая конфигурация предусматривает применение 186 многоядерных процессоров в стандартной стойке высотой 42U.

«РТСофт»: +7 (495) 967-1505



Процессорный модуль для высокоскоростных приложений

Модуль Kontron CPS3003-SA в стандарте 3U CompactPCI Serial (PICMG S.0) на процессоре Intel Core i7 3-го поколения доступен в различных версиях. Его вычислительная мощность масштабируется от двухъядерного процессора Intel Core i7 3517UE (1,7 ГГц) до четырехъядерного Intel Core i7 3612QE. Возможно использование до 16 Гбайт памяти ECC SDRAM DDR3. Интегрированный чипсет Mobile Intel QM77 Express имеет большое количество интерфейсов. Периферийные модули, активно выполняющие обработку данных, могут соеди-

няться по двум интерфейсам PCI Express Gen 3.0 (x8 или x4) с высокой пропускной способностью. Дополнительно имеется пять каналов PCIe x1. Модули – носители для жестких дисков могут соединяться по четырем интерфейсам SATA (два из которых SATA 6 Гбит/с). Кроме того, имеются два разъема USB 3.0 и шесть – USB 2.0, разведенные на объединительной магистрали. Работа в сетях обеспечивается двумя портами Gigabit Ethernet, которые могут коммутироваться на переднюю панель модуля или на объединительную магистраль.



Процессорный модуль CPS3003-SA может применяться в приложениях для промышленной автоматизации, контрольно-измерительном оборудовании, системах транспортного, медицинского и оборонного назначения.

«РТСофт»: +7 (495) 967-1505

Коммутаторы второго уровня с поддержкой IPv6

ECS3510-28T (ECS3510-52T) имеют 24 (48) портов FastEthernet и 4 CG-порта, CPU с тактовой частотой 333 МГц, объем ОЗУ – 128 Мбайт, флеш-память – 32 Мбайт. Объем таблицы MAC-адресов – 16 кбайт.

Коммутаторы поддерживают управление на базе протокола IPv6, в том числе:

- двойное стекирование протоколов IPv4/IPv6, что позволяет IPv4 и IPv6 сосуществовать в одном устройстве;
- протоколы SNMP / HTTP на базе IPv6;
- IPv6 Neighbor Discovery для определения других узлов IPv6 в сети.



В набор L2-функций входят функции, реализующие требования стандартов IEEE 802.1w и IEEE 802.1s для устранения петель и обеспечения быстрого восстановления после сбоя; MVR для видеопотоков по запросу;

IGMP для повышения пропускной способности при интенсивном потоке IPTV-трафика в сети.

ОАМ включает в себя IEEE 802.1ag, IEEE 802.3ah и ITU-T Y.1731. Будучи совместимыми с этими протоколами, устройства ECS3510-28T и ES3510-52T позволяют поставщикам услуг отслеживать неисправности соединений в мультивендорной сети и реагировать на сбой с высокой скоростью. Кроме того, G.8032 ERPS обеспечивает защиту кольца и восстановление в течение 50 мс.

Для обеспечения безопасности портов устройства ES3510-28T и ES3510-52T дают возможность получить доступ к ним на основе MAC-адреса. Это ограничивает количество устройств, использующих порт, и защищает от атак MAC flooding. Кроме того, списки управления доступом (ACL) могут служить для ограничения доступа к чувствительным ресурсам сети, запрещая прохождение пакетов на основе исходного и конечного MAC-адреса, IP-адреса или TCP / UDP-порта.

Коммутаторы поддерживают SNMP-управление, удобный веб-интерфейс и интерфейс командной строки (CLI) для продвинутых пользователей.

Edge-Core Networks: +7 (916) 625-8272

Энергоэффективный суперкомпьютер

MBC-10П – прототип суперкомпьютера 10-петафлопсного диапазона, создаваемого в МЦЦ РАН группой компаний РСК при поддержке Intel. Сейчас его пиковая производительность – 523,8 TFLOPS (триллионов операций в секунду), а на тесте Linpack – 375,7 TFLOPS.

Суперкомпьютер состоит из 208 вычислительных узлов на базе архитектуры «РСК Торнадо» с прямым жидкостным охлаждением, процессоров Intel Xeon E5-2690 и сопроцессоров Intel Xeon Phi, серверных плат Intel S2600JF и твердотельных дисков Intel SSD. Его вычислительное поле состоит из 3328 вычислительных ядер процессоров Xeon E5-2690 и 25376 ядер сопроцессоров Xeon Phi SE10X. В каждом узле обеспечивается поддержка 64 Гбайт энергоэффективной оперативной памяти (DDR3-1600, low voltage green memory), что составляет 4 Гбайт на каждое вычислительное ядро Xeon и 13,2 Тбайт ОЗУ для системы в целом. Суммарная дисковая память вычислительных узлов – 24,8 Тбайт.

Высокоскоростная сеть передачи данных основана на технологии FDR Infiniband (56 Гбит/с, максимальная задержка – 2 мкс). Сервисная сеть состоит из двух независимых сенсорных и управляющих сетей.

Оптимизацию скорости работы приложений в распределенных и гибридных средах обеспечивает программный пакет Intel Cluster Studio XE 2013.

Энергопотребление суперкомпьютера составляет 222 кВт при пиковой производительности, а энергоэффективность достигла 1949,3 MFLOPS/Вт. Используется технология гибкого управления энергопотреблением «РСК ЭКОсистема», которая позволяет уменьшить суммарную стоимость владения на 25%.

Применение системы жидкостного охлаждения для стандартных серверных плат на базе процессоров Intel Xeon, изначально созданных для традиционных систем с воздушным обдувом электронных компонентов, обеспечивает вычислительную плотность 181 TFLOPS на одну стойку 80 см × 80 см × 42U или 141 TFLOPS/куб. м.



Площадь, занимаемая вычислителем, системами электропитания, коммутации и хранения данных – 20 кв. м.

РСК: +7 (495) 640-3107

АМДТЕХНОЛОГИИ

Тел.: (495) 963-9211
Факс: (495) 225-7431
E-mail: info@amd-tech.ru
www.amd-tech.ru с. 89

ИК ГУЛЛИВЕР

Тел/факс: (495) 663-2172
E-mail: info@ikgulliver.ru
www.ikgulliver.ru с. 83

НРТБ

Тел.: (495) 748-3187
Факс: (495) 230-1856

E-mail: info@nrtb.ru
www.nrtb.ru с. 60–61

РТСОФТ

Тел.: (495) 967-1505
Факс: (495) 742-6829
E-mail: rtsoft@rtsoft.ru
www.rtsoft.ru с. 17

ТРИКОЛОР ТВ

Тел/факс: (495) 984-5124
www.tricolor.tv 2-я обл.

ЭНЕРГОМЕРА

Тел/факс: (8652) 56-6690

E-mail: concern@energomera.ru
www.energomera.ru . . . с. 78–79

EMERSON NETWORK POWER

Тел.: (495) 981-9811
Факс: (495) 981-9810
E-mail: sales@emerson.com
www.emersonnetworkpower.com . . с. 75

ENERSYS

Тел.: (495) 925-5648
Факс: (495) 925-5649
E-mail: info@ru.enersys.com
www.enersys-hawker.com c. 15

NETGEAR

Тел./факс: (495) 799-5610
www.netgear.ru с. 13

RADIUS GROUP

Тел/факс: (495) 641-0410
E-mail: info@radiusgroup.ru
www.radius-group.ru . . с. 54–55

RIT

Тел./факс: (495) 684-0319
E-mail: marketing@rit.ru
www.rit.ru с. 93

RITTAL

Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
**www.rittal.ru 1-я обл.,
. с. 11, 76–77**

SONY ELECTRONICS

Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu с. 7

VERIMATRIX

Тел.: (926) 525-7624
www.verimatrix.com . . . с. 53

Указатель фирм

2ГИС	22	Microsoft	13, 20, 72	«Аладдин Р.Д.»	18	«Мосводоканал»	16	САПРАН	72
A&NN	13	MobeyForum	8	Альфа-Банк	35, 44, 50	Московская междугородная телефонная станция № 9 . . .	13	«Салсан»	67
Aberdeen Group	73	MTS	40	«АльфаСтрахование»	16	МТС	8, 12, 13, 14, 25, 26, 27, 35, 41, 51, 52, 71, 78	Сбербанк	12, 35, 37
Acer	48	MTS BV	13	«АМДтехнологии»	89, 91	МТС Банк	13, 41	«Связной»	46
Alcatel	41, 50	NetApp	70	«Аптека ОЗ»	16	МТТ	8, 12	«Связьинвест»	51
Allied Telesis	12	Omnicomm	66, 67	«Арт Телеком»	13	«Мультинет»	27	«Северсталь»	16
AMD	20	ГК Optima	47	НП «Ассоциация медицинской информатики»	9	«Национальная спутниковая компания»	13	«Сиблинк»	27
Apple	48, 50	Optima Infosecurity	47	ГК «Астерос»	12	«Национальные		«Синтерра»	8
Berg Insight	68	Oracle	63	Африканский банк развития . . .	18	РадиоТехническое Бюро» . .	60, 61	«Система Телеком»	8
BitCoin	49	Orange Business Services . . .	18	Банк Москвы	44	«Объединенная компания		АФК «Система»	8, 35, 52
BlackBerry	74	Orascom Telecom Algeria . . .	52	Банк России	8, 26, 54, 72	«Одноклассники»	21	БФ «Система»	12
Bosch	63	Orsiola-KD	16	«БАРС Групп»	12	Оренбургская государственная медицинская академия . . .	16	«Скартел»	51
Brent	51	Panasonic	14	«Био-Витрум»	74	«Орион Телеком»	27	«Скаут»	67
Cable City	27	PayCash	8	«Взлетка.Net»	27	«Панасоник Рус»	14	«Сколково»	8
Cisco	16, 20, 63, 64, 70	PayPal	38, 39, 40, 44	«ВКонтакте»	21	Первый МГМУ	66	«Смартфин»	8, 36, 49
Citrix	71, 72	Ponemon Institute	24	Военно-космическая академия им. А.Ф. Можайского .	9	им. Сеченова	16	НП «Содействие	
Cloud4Y	71	QIWI	40, 44, 45	ВТБ24	14, 16	«Норильск Телеком»	27	и использование	
CNews Analytics	34	QIWI Кошелек	35, 44, 46	«ВТБ Капитал»	13	«Объединенная компания		навигационных технологий» .	14
DataLine	13, 73, 74	QIWI-Банк	39	«ВымпелКом»	8, 12, 13, 14, 18, 27, 35, 36, 38, 41, 50, 52, 65, 72, 74, 78	«Орион Телеком»	27	СПбГЭТУ	8
DataSpace	12	Radware	70, 71	«Газпром нефть»	16	«Афиши» и «Рамблера» . . .	13	ГК «Старт»	62
DEAC	74	Rittal	76, 77	«Газпром-телеком»	16	«Одноклассники»	21	«Стартап Академия»	8
Dell	20	Riverbed	18	«ГалилеоСкай»	67	Оренбургская государственная медицинская академия . . .	16	«Старый лекарь»	16
DEPO Computers	18	Ruigion	22	«Гамма Технологии»	18	«Панасоник Рус»	14	«СТС Медиа»	16
Djezzy	52	RunMyProcess	13	«Группа Связной»	8	Первый МГМУ	66	«СУП Медиа»	13
E1.ru	21, 22	Salvagnini	79	«ДальгеоКом»	12	«Платина»	39	«Таврический»	39
Edge-Core Networks	95	Samsung Electronics	41, 42, 50	«Даньги@Mail.ru»	44	«Портлинк»	27	«Телеком-Экспресс»	13
eKassir	8, 45	SAP	63, 73	Департамент информационных технологий Москвы	12, 43	ФГУП «Почта России» . . .	6, 7, 12	«Территория контактов» . . .	13
ELTEK	78	Schneider Electric	13	«Единый кошелек»	36	ТТК	48	«Техноком»	66, 67
Emerson Network Power	88	Siemens	16, 78	ЕМС	70	«Прогноз»	18	«Техносерв»	47
EPAM	14	Siemens Enterprise Communications	16	«Енисейтелеком»	27	«ПрофМедиа»	13	«ТехноТон»	67
Ericsson	13, 63	Sistema Shyam		«Золотая корона»	42	ОАО «ПСКБ»	8	«ТрансКредитКарт»	54
Facebook	35	TeleServices Limited	52	«Игра-Сервис»	27	«Радиус Групп»	54	Триколор ТВ	13, 15
Ferrari	16	Skype	72	«Интеррос»	13	«Радуга ТВ»	12	ТТК-Дальний Восток	12
Financial Regulation International	8	Softline	47	Инфокоммуникационный союз .	8	«Радуга Интернет»	36	«Утилекс»	18
Fujitsu	13, 63	Sony	41, 48	Технический комитет ТК-468 .		«Райт Сайд»	27	УК «Финам Менеджмент» . . .	51
General Electric	78	SonyEricsson	50	«Информатизация здоровья» . .	9	НКО «Рапида»	39	«Фирма «Релакс»	9
Global Payments Group	54	Square	49, 50	«Инфосистемы Джет»	16, 18	РАСПО	20	ФСК ЕЭС	16
Globale Wireless	52	Sun	63	ИТ-ГРАД	70	«Расчеты и операционная работа в коммерческом банке»	8	«Холдинг МРСК»	71, 72
Google	21, 36, 37, 39	Symantec	73	«ИТ-парк»	12	РАЭК	21	«Хомм Кредит	
GSMA	8	Sysnet Global Solutions	47	Клиника промышленной медицины	16	РБК	52	энд Финанс Банк»	16, 34, 74
HP	14, 20, 70	Tele2	51, 52	«Корус Консалтинг ИТ»	20	РЖД	14, 16	«Центр безопасности	
HP Software	14	Telekom Srbija	52	КРОК	12, 20, 46, 73	РКС	67	информации»	20
HTC	41, 50	Teltonika	67	«Лаборатория Касперского» . .	16	«Ростелеком»	12, 14, 27, 51, 52, 60, 65	Центр космических услуг . . .	14
Huawei	50	TNS Россия	21	«Лайф»	50	РСК	95	Центральный научно-	
IBS	73	TRUMPF	79	ЛЭТИ	8	«РТ Лабс»	56	исследовательский институт	
IDC	20	Uptime Institute	12, 13, 80, 81, 84, 90	«М2М телематика»	67	«РТСОфт»	15, 94	организации и информатизации	
i-Free	42	Vipont.Ru	36	«Манго Телеком»	73	«Русат»	36	здравоохранения	9
iKS-Consulting	27	Visa	35, 39, 40, 41, 42, 44, 49, 50, 55	«Мастер-Банк»	39	«Русские навигационные технологии»	67	Центризибком РФ	12
Intel	12, 20, 94, 95	W1	36	МГПС	16	«Самолотровский нефтеперерабатывающий завод»	10	ЦНИИ Минобороны	9, 10
J'son & Partners	34, 35	WebMoney	44, 45	МГУ им. М.В. Ломоносова . . .	12	ФНБ «Самрук-Казына» . . .	18	ГК ЦФТ	42
Kontron	15, 94	WebMoney Transfer	40	«МегаФон»	14, 16, 26, 27, 39, 40, 52, 60			«Чайка»	71
Kraslan	27	Yandex N.V.	52	«Медианн-Решения»	24			«Элекснет»	44
Leta	23	ZyXEL	18, 65, 94	МИИТ	8			«Электронные деньги»	8, 37
LG	48	«Аверс Телеком»	27	ММА им. И.М. Сеченова	9			«ГК «Электроштит» —	
Mail.Ru Group	21, 52	«Авиадвигатель»	73					ТМ Самара»	13
Marshall Capital	51	АДЭ	25					«Энвижн Групп»	25
MasterCard	40, 41, 42, 44, 48, 49, 50, 55	«Ай-Теко»	12					«Энергомера»	78
ГК MAXIMA	27							«ЭР-Телеком»	27
MegaCom	17							«Юнистрим»	28
MegaLabs	16, 35, 36, 39, 41							«Яндекс.Деньги»	35, 37, 40, 46
								«Яндекс»	18, 21, 29, 35

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство

«ИнформКурьер-Связь»:

127273, Москва, Сигнальный проезд, д. 39, подъезд 2,
офис 204; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:

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

МНТОРЭС им. А.С. Попова:

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