

IP-телефония с прицелом на triple play

Место действия – Зеленоград



С. АЛИМБЕКОВ

Схемы взаимодействия операторов разных уровней рожают новые бизнес-модели и – что важнее – услуги. В Зеленограде проводится «чистый эксперимент»: с 1 июля 2006 г. оператор телефонной связи ИАС (группа компаний «Комкор») начал в опытно-коммерческом режиме предоставлять услугу «цифровой телефон» на сети ведущего провайдера в Зеленограде – компании «Синс-Телеком» (абонентская база – 12 тыс. пользователей). Задача – предложить абоненту IP-телефонию и сервисы в дополнение к телефону МГТС. Цель триумвирата операторов – triple play. О путях достижения – беседа с Сергеем АЛИМБЕКОВЫМ, генеральным директором ОАО «ИАС».



– Сергей, каковы побудительные мотивы участников проекта, приведшие к созданию опытной зоны по предоставлению услуг IP-телефонии массовому пользователю?

– У каждого из участников проекта они свои. Компанию «Комкор», совместно с которой создавалась услуга «цифровой телефон», интересует выработка схемы партнерского взаимодействия оператора магистральной сети, оператора телефонии и оператора сети доступа.

Мы ставили перед собой задачу собрать статистику и найти оптимальные способы предоставления и продвижения услуг IP-телефонии на массовом рынке, наладить «обратную связь» с пользователем: узнать его мнение о качестве и наборе услуг и т.д. Это очень важно, поскольку мы рассчитываем, что внедрение услуг цифровой телефонии придаст новый импульс развитию бизнеса, позволит начать активно продавать имеющуюся у нас номерную емкость в коде «499» (110 тыс. номеров) абонентам домовых сетей.

Для домовых сетей, ранее фокусировавшихся на услугах широкополосного доступа в Интернет, появление в портфеле IP-телефонии – это возможность предложить пользователям новый сервис, а значит, получить дополнительное конкурентное преимущество.

С компанией «Синс-Телеком» корпорация «Комкор» связывают давние партнерские отношения. А поскольку Зеленоград представляет собой обособленный участок Москвы, где можно поставить абсолютно чистый эксперимент, опытную зону новой услуги решено было организовывать именно там.

– Как строятся взаимоотношения ИАС и «Синс-Телекома»?

– Между ИАС и «Синс-Телекомом» заключен агентский договор. «Синс-Телеком» работает с клиентами: занимается оформлением договоров, подключением, технической поддержкой и т.д. ИАС же поддерживает саму платформу предоставления услуг, обеспечивает биллинг услуг, берет на себя вопросы присоединения и межоператорского взаимодействия.

– С каким же предложением вышел триумвират операторов?

– Для абонентов доступны три тарифных плана на услугу «цифровой телефон». Все они предусматривают бесплатную установку, подключение и настройку оборудования, бесплатные звонки внутри сети по коротким – пятизначным – номерам, а также все входящие звонки. (Исходящие звонки на сотовые телефоны, в кодах «495» и «499», а также междугородные и международные звонки тарифицируются и оплачиваются поминутно.)

Различия же между тарифными планами – в наборе предлагаемых дополнительных услуг и, соответственно, в размере абонентской платы. За 199 руб. в месяц абонент получает московский телефонный номер в коде «499», а также может пользоваться АОН и ящиком голосовой почты. Заплатив на 91 руб. больше, он получит все возможности предыдущего тарифного плана, а кроме того, доступ к услугам переадресации (по времени, по состоянию линии, по АОН), трехсторонней конференц-связи и ряду других новых сервисов.

Для того чтобы воспользоваться услугой, абоненту необходимо заключить в дополнение к имеющемуся контракту с «Синс-Телекомом» контракт с ИАС на услуги местной телефонной связи и на услуги междугородной, международной связи с МТТ и приобрести устройство доступа стоимостью от 1500 руб.

– Получается, что абонент «Синс-Телекома» должен заключить три контракта?

– С формальной точки зрения именно так. Но во взаимоотношениях клиента с оператором доступа ничего принципиально не изменилось. «Синс-Телеком» является единой точкой входа для клиентов. По всем вопросам оплаты услуг, технической поддержки и т.д. клиент продолжает общаться именно с компанией «Синс-Телеком».

– Предшествовало ли запуску услуги «цифровой телефон» в тестовую эксплуатацию изучение потребностей пользователей?

– Результаты опроса, проведенного нами среди пользователей сети «Синс-Телеком» на сайте провай-

дера, свидетельствовали о готовности рынка. Судите сами, на вопрос: «Если бы на сети «Синс-Телеком» была развернута телефонная сеть, вы захотели бы стать ее абонентом?» – утвердительно ответили 86,6% опрошенных. Еще 89,1% принявших участие в опросе хотели бы пользоваться услугой АОН, 76,3% – управлять услугой из своего кабинета.

– Поскольку уровень телефонизации в Зеленограде очень высок, понятно, что в большинстве случаев услуга IP-телефонии предлагается абонентам МГТС. Какие аргументы вы приводите, убеждая их в полезности «цифрового телефона»?

– Выявление правильных путей продвижения услуги – основная задача. Пилотная зона в Зеленограде как раз и была развернута для оценки потенциала услуги и дальнейшей корректировки методов продвижения. Мы понимаем, что продаем даже не второй телефон, а третий, четвертый, а то и пятый: ведь наши пользователи не только абоненты МГТС, но и операторов сотовой связи. Вот почему мы стараемся донести до них, что «цифровой телефон» – это еще одна возможность быть «на связи» и пользоваться целым рядом полезных сервисов, предлагаемых по более конкурентоспособной цене по сравнению с предложениями МГТС, не говоря уж о тарифах сотовых операторов. Поверьте, для общества растущего потребления, которое формируется сегодня в Москве, 300 руб. – это не так уж и много, столько же стоит билет в кино. Ценовая конкуренция станет особенно заметной после повышения тарифов МГТС.

– Иными словами, вы не призываете абонентов отказываться от телефонов МГТС?

– Нет. Более того, мы планируем применять оборудование, позволяющее использовать не только нашу услугу, но и уже имеющийся в квартире обычный телефон. Таким образом, мы решаем проблему back-up для нашего телефона (если пропадает электричество – абонент сможет воспользоваться телефоном МГТС) и

одновременно проблему дополнительных сервисов для обычного телефона, как-то: переадресация вызовов, удаленное управление и т.д.

С другой стороны, абонент сам выбирает, с каким оператором работать, и мы, например, готовы предложить более высокий уровень обслуживания клиентов, в частности предоставить онлайн-детализацию счета, работу в кредит и проч.

– Сколько пользователей «Синс-Телекома» заключили контракт с ИАС на сегодняшний день и какое их количество подразумевает ваш оптимистический сценарий?

– За первый месяц опытно-коммерческой эксплуатации новой услуги нам удалось привлечь более 30 абонентов. До конца 2006 г. мы планируем увеличить клиентскую базу до 1000 абонентов. При таких показателях наш эксперимент можно считать успешным.

– Когда можно ожидать перенесения зеленоградского опыта на московские просторы?

– В настоящее время ведутся переговоры с рядом операторов сетей доступа. Технологически и организационно мы готовы к предоставлению услуг всем желающим: решение Nortel CS200 в нынешней конфигурации позволяет нам предоставить услуги для 30 тыс. абонентов с перспективой расширения до 500 тыс. абонентов.

– Кого вы видите в столице в качестве потенциальных партнеров?

– К их числу мы относим московские домовые сети, а также «Комкор-ТВ», совместный проект с которым мы планируем запустить в начале 2007 г. «Комкор-ТВ», в настоящее время получающий лицензию на местную связь, будет включать наши услуги в свои пакеты. В этом случае мы получим классическую реализацию концепции triple play – триединую услугу от одного оператора, за пользование которой абоненту будет выставляться единый счет.

Беседовала Александра КРЫЛОВА

21-24 ноября 2006

Комплекс «Гостиный Двор»

Москва

ВКСС

9-я международная выставка
**ВЕДОМСТВЕННЫХ И КОРПОРАТИВНЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ
СЕТЕЙ И СРЕДСТВ СВЯЗИ**

Под эгидой Министерства информационных технологий и связи РФ

ПРИГЛАСИТЕЛЬНЫЙ БИЛЕТ

Мобильный двигатель торговли

Мобильная связь – единственная телекоммуникационная среда, не насыщенная рекламой. Отчасти это связано с «интимным» характером мобильных коммуникаций, однако в большей степени объясняется недостатком адекватных способов доставки рекламы абоненту. Сегодня ситуация начинает меняться. Во всем мире в секторе мобильной рекламы ведется активный поиск подходов, технологий, средств, планируются инвестиции. В процесс вовлечены операторы, исследовательские группы, бизнес-аналитики, разработчики технологий, владельцы торговых марок и рекламные агентства. И хотя сегодня большая часть мобильной рекламы посвящена самым простым темам – контенту и другим операторским услугам, мобильный рекламный бум не за горами. Готовы ли к нему операторы?



С. ДАНФОРД,
генеральный директор
компании Celltick

Мобильная реклама в тестовом режиме

Продвижение операторами собственных услуг с помощью мобильной рекламы можно назвать тестовой площадкой, на которой происходит апробация технологий, механизмов и приемов, изучается реакция потребителей и нарабатываются стратегии мягкого вмешательства в жизнь абонентов мобильной связи. Вся эта деятельность ведется в преддверии ожидаемого перетекания в мобильные коммуникации внушительных средств из области телевизионной и прочей рекламы, к чему операторы должны своевременно подготовиться.

По данным исследовательского агентства Informa, в мире насчитывается более 2 млрд сотовых абонентов, что почти вдвое превышает число домашних телевизоров на всей планете. Такой мощный потенциал не дает покоя рекламным агентствам, так же как и объем доступной специфической информации о потребителе-абоненте, начиная с его физического местонахождения и заканчивая демографическими данными и покупательскими предпочтениями.

Мобильные операторы уже делают первые робкие шаги в применении мобильной рекламы, причем самыми активными в этой области являются виртуальные операторы – MVNO, ведущие свое происхождение от розничных торговых сетей и концернов телевидения. Эксперты агентства IDC объясняют это тем, что ментальность MVNO более гибкая и ориентированная на рынок, чем ментальность традиционных технократических поставщиков голосовых услуг. Обычные операторы осваивают мобильную рекламу несколько медленнее. Тем не менее в текущем году некоторые

западные крупные операторы (например, Vodafone, Orange, принадлежащий Hutchison оператор «3») отважились на рекламные проекты совместно с известными торговыми марками Adidas, Apple, BMW, Budweiser, Canon, L'Oreal, MasterCard, Puma и др. А какова позиция держателей денег – торговых марок?

По сведениям IDC, расходы американских торговых марок на мобильную рекламу в прошлом году удвоились. Аналитическое агентство Fathom Partners считает, что этот рынок вырастет к 2009 г. до \$4 млрд. Но произойдет это лишь в том случае, если владельцам торговых марок будет предоставлен убедительный способ установления эмоционального и делового контакта с потребителем путем мобильной рекламы. Над этим вопросом трудятся разработчики, создавая условия для того, чтобы достаточно зрелые технологии доставки рекламного содержания на мобильные устройства позволили сосредоточиться на взаимодействии с потребителем.

Рекламная модель для мобильной среды

Новые подходы к рекламе, наблюдаемые в Интернете, служат моделью и для мобильной среды. Первое условие успешного продвижения рекламного контента в Сети – так называемой рекламы Google (в России ее аналогом является реклама Yandex) – состоит в следующем: рекламный контент должен содержать существенно ценную для потребителя информацию. Это возможно при точной сегментации потребителей, которая позволяет направлять абонентам только адекватную информацию. Такой целенаправленный подход – единственное средство для поддержания

восприимчивости потребителей на уровне, достаточном для жизнеспособности мобильной рекламы.

Второе условие – мобильная реклама не имеет права мешать потребителю, несмотря на горячее желание операторов и рекламодателей навязать абоненту то или иное сообщение. Без соблюдения этого условия рекламный эффект может оказаться нулевым или даже отрицательным. Здесь существует несколько направлений, разрабатываемых компаниями мобильного маркетинга, в том числе креативное включение рекламируемых логотипов в мобильные развлекательные клипы, видео и игры. Еще одна возможность – предоставление абонентам бесплатного контента, игр и рингтонов в обмен на их согласие получать ежедневно несколько рекламных сообщений. Как показывает европейский опыт, количество абонентов, согласных «терпеть» рекламу в обмен на бесплатный контент, быстро растет.

Новая технология мобильного маркетинга

Разнообразие новых решений мобильного маркетинга впечатляет. Так, сегодня большинство производителей SIM-карт включают в чипы технологию LiveScreen Media, поддерживающую доставку сообщений на «спящие» экраны. Чтобы задействовать LiveScreen Media, операторы должны заключить лицензионное соглашение с ее поставщиком – компанией Celltick, разработчиком технологий на основе сотовой трансляции и услуг мобильного маркетинга. LiveScreen Media уже проверена на сетях 20 операторов во всем мире, которые используют ее для стимулирования доступа к своему контенту. Сообщения, рассылаемые с помощью сотовой трансляции, ненавязчивы: они бесшумны, приходят только на «спящий» экран, не расходуют память и питание мобильного устройства.

Действие рекламы основано на привлекательности самого сообщения. Потребители реагируют только на те сообщения, которые им интересны, и только в

удобное для себя время. Таким образом исключается спам и автоматически сегментируется аудитория для рекламы. Результаты такого воздействия впечатляют: около 90% абонентов не отказываются от услуги и около 40% абонентов генерируют в среднем по 6 транзакций потребления контента ежемесячно. Решение уже применяется в России. До недавнего времени его распространение сдерживалось эксклюзивным соглашением с «ВымпелКомом», однако с лета этого года оно доступно любому российскому оператору.

В Celltick считают, что технология LiveScreen Media способна произвести революцию в мобильном маркетинге, поскольку сочетает в себе много принципиально важных факторов: мягкое воздействие на пользователя, сегментирование и целенаправленную доставку, информативный контент, создающий эмоциональный контакт с потребителем, и, что немаловажно, низкую себестоимость доставки. А кроме того, самообучающаяся платформа запоминает, какие темы предпочитают абоненты, и в дальнейшем посылает только адекватные сообщения.

Сообщения могут рассылаться и в привязке к местонахождению абонента, рекламируя услуги или заведения в пределах улицы или квартала. Информация о предпочтениях может передаваться рекламодателям и будет способствовать более направленному воздействию на аудиторию. Поскольку решение обладает функциональностью реального времени, рекламодатели определяют момент отправки, регулярность своих сообщений и наиболее подходящий период (например, обеденный перерыв, когда абоненты более активно реагируют на сообщения). Таким образом, составляется временная сетка рекламного вещания, что соответствует привычной модели рекламы на телевидении или радио, но в отличие от последней мобильная реклама обладает высокой степенью персонализации. А себестоимость решения на базе LiveScreen Media, по оценкам Fathom Partners, составляет лишь 5% от стоимости телевизионной рекламы. ИКС



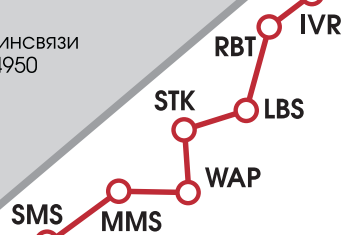
ЗАО "ИнКор"

| ядро мобильного бизнеса |

www.incore.ru | go@incore.ru

+ 7 (495) 982 38 86

Лицензия Минсвязи
России №34950



Двигаясь к результату, часто приходится преодолевать длинный и извилистый путь. Чтобы пройти его быстрее и напрямую, вам нужен помощник.

Мы поможем вам реализовать любой сервис в области мобильного контента. Мы обеспечим интеграцию вашего сервиса в сети сотовых операторов и доставку мобильного контента конечным абонентам.

Как ускорить ВВОД НОВЫХ УСЛУГ, или Управление жизненным циклом продукта



Как ускорить вывод на рынок новых услуг и при этом минимизировать издержки? Один из способов – повысить эффективность внутренней деятельности оператора. Решить эту задачу, по мнению авторов статьи, поможет внедрение на предприятии процесса управления жизненным циклом продукта/услуги связи – Product Lifecycle Management (PLM), построенного с учетом наработок и опыта международной организации TeleManagement Forum (TM Forum).



О.И. СКОКОВ,
генеральный директор
«БиАй Телеком»



В.А. ЛЁВИН,
руководитель проектов
«БиАй Телеком», к.т.н.

PLM в системе координат eTOM

Эффективная внутренняя деятельность современного оператора связи – это четкое, прозрачное взаимодействие структурных подразделений в рамках сквозных процессов предоставления услуг. Ключевым аспектом ее выстраивания является единый процессный подход к оказанию услуг как в подразделениях продаж и маркетинга, так и в технических службах. Более того, без постановки процессов управления жизненным циклом (PLM) выход на рынок перспективных услуг (NGS) для массового клиента практически нереален.

Понятие жизненного цикла продукта возникло довольно давно. Впервые процесс PLM был подробно исследован одним из гуру маркетинга Теодором Левитом в 1965 г. Развитие бизнеса многих компаний базируется на четко выстроенном процессе управления жизненным циклом продукта/услуги. Так, благодаря автоматизации PLM компания Ford сократила время выхода продукта на рынок почти наполовину и снизила расходы во время подготовки его к запуску – самом затратном периоде жизненного цикла продукта.

Циклический процесс PLM, включающий в себя семь этапов (рис. 1), пронизывает большинство подразделений предприятия, охватывая такие области, как «Стратегия, инфраструктура и продукт» и «Операционные про-

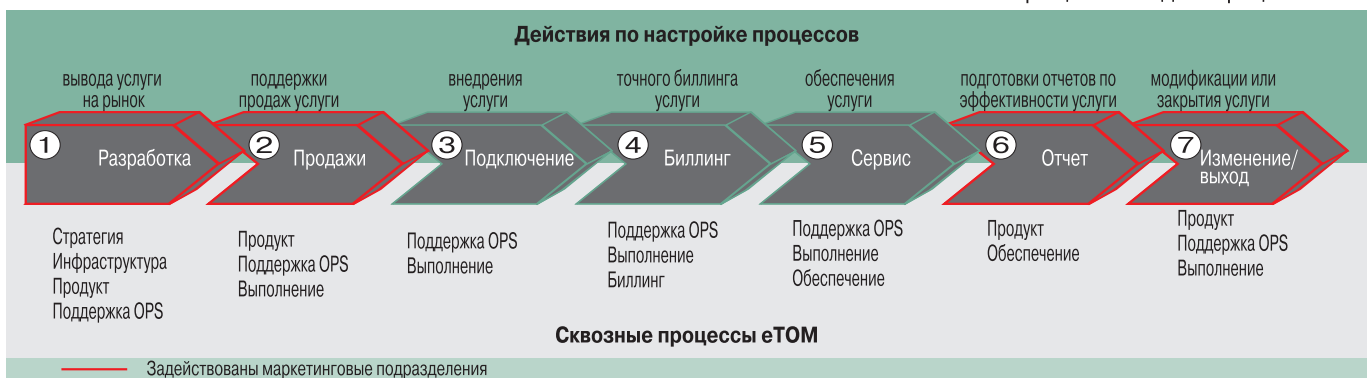
цессы» eTOM (enhanced Telecom Operations Map – Расширенная карта процессов оператора связи) (рис. 2).

Поскольку модель процессов eTOM представляет собой карту функциональной иерархии процессов телекоммуникационной компании, то с точки зрения процессного подхода именно PLM можно рассматривать как искомый многими консультантами метапроцесс компании. При этом становится очевидной роль eTOM как инструмента и системы координат, но не более того. Таким образом, именно метапроцесс PLM уникален для каждой компании-оператора связи и отражает специфику его деятельности, в то время как eTOM является референтной моделью.

Процесс PLM включает в себя ряд подпроцессов, которые необходимы для определения, планирования, проектирования, построения, доставки, сопровождения, пересмотра и выведения с рынка продуктов, составляющих корпоративное портфолио. Подпроцессы PLM являются сквозными, т.е. охватывают (пронизывают) горизонтальные области eTOM «Рынок, продукт, клиент», «Сервис», «Ресурс», «Поставщик/партнер».

Недочеты в процессе управления жизненным циклом продукта ведут к целому ряду последствий, негативно сказывающихся на всей деятельности оператора (таблица). При пра-

Рис. 1. Упрощенная модель процесса PLM



вильной постановке процесса PLM должны быть решены все приведенные в таблице проблемы.

Под **отсутствием процесса PLM** понимается следующее:

- существующие процессы разработки, внедрения и предоставления услуг подчинены техническим возможностям сети, а не потребностям рынка;
- отсутствует формализация (входы/выходы, описание процессов и информационного обмена, регламенты, метрики) и, как следствие, реализация процесса PLM;
- не сформированы единые принципы и подходы к формированию разных продуктов (услуг связи).

Используя лучший мировой опыт и учитывая специфику бизнеса операторов связи, TM Forum определил и продолжает развивать методологию построения процесса жизненного цикла услуги для телекоммуникационной отрасли.

Маркетинг – «заводила» и контролер процесса PLM

Согласно принципам TM Forum, процесс управления жизненным циклом услуги должен быть клиентоориентированным, т.е. выстроен от клиента. Процесс PLM дает оператору возможность управлять своими услугами по отношению к границам их рентабельности, удовлетворенности пользователей и соответствия нормам качества, а также позволяет ему под-

держивать стратегическое видение реальности и выстраивает основные бизнес-процессы так, чтобы компания соответствовала требованиям рынка и ожиданиям клиентов.

Маркетинг в PLM играет роль движущей силы и контролера, являясь одновременно завершающей точкой предыдущего витка развития услуги и отправной точкой нового витка (рис. 3). Кроме того, он отвечает за постановку задачи и формирование целевой функции разработки или модернизации услуги. После внедрения услуги в коммерческую эксплуатацию маркетинг проверяет соответствие действительного состояния продукта желаемому и корректирует направление его дальнейшего развития.

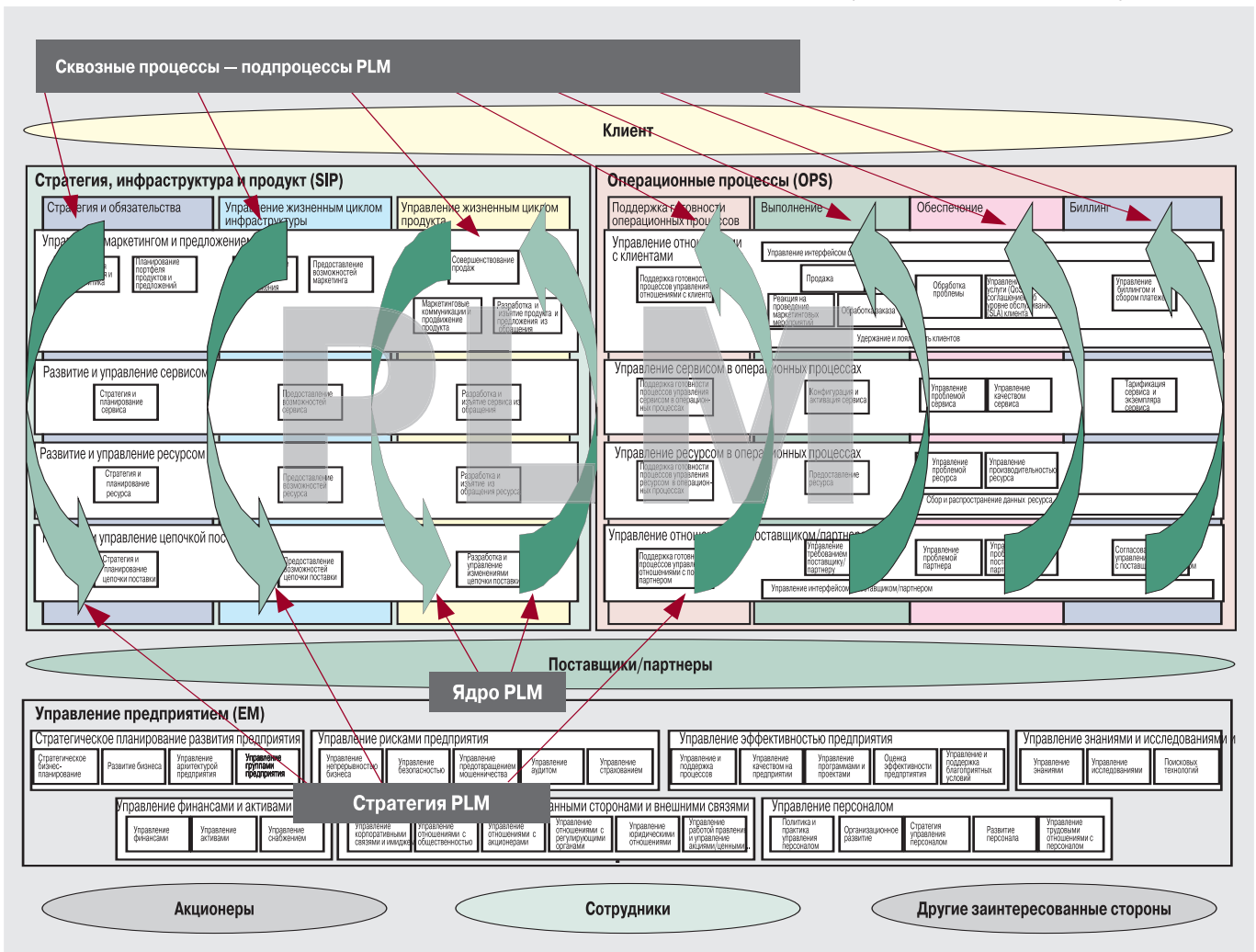
Реализация и отладка процесса PLM

Очевидно, что поставить весь процесс PLM у крупного оператора связи невозможно. Поэтому для внедрения новых услуг (NGS) целесообразно построить действующую модель PLM, которая должна в определенных границах обеспечивать измеримый результат, снижение рисков при развертывании NGN и служить основой для дальнейшего развития процесса управления жизненным циклом.

При разработке действующей модели PLM необходимо:

- заложить основу процесса PLM и обеспечить взаимосвязь маркетинговых, технических и управленческих аспектов в рамках определенных ограничений, например один филиал (го-

Рис. 2. Отображение PLM в системе координат eTOM

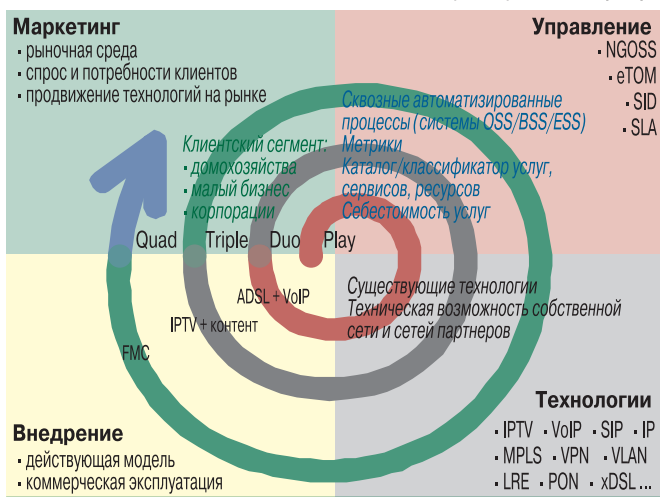


Н О Я Б Р Ь 2 0 0 6 , И К С

Типичные недочеты операторов в процессе управления жизненным циклом продукта

Недочет	Отсутствие сквозных процессов предоставления услуг через все уровни взаимодействия с клиентом, сервисов, ресурсов, взаимодействия с поставщиком
Следствие	Отсутствие прозрачного эффективного взаимодействия подразделений, отвечающих за работу с клиентом и рынком, и подразделений, отвечающих за техническое развитие сети. Отсутствие взаимосвязанных показателей выполнения процессов разными подразделениями для достижения ключевых целей компании. Не соответствующая задачам оргструктура компании. Затруднительность формирования схемы мотивации подразделений и сотрудников компании. Затруднительность взаимодействия с партнерами, поставщиками услуг. Лоскутная автоматизация процессов — невозможность выхода на массовый рынок услуг
Недочет	Отсутствие четкой взаимосвязи (разрыв) между услугами и ресурсами (нет уровня сервисов как связующего звена между уровнем услуг и уровнем ресурсов)
Следствие	Трудность формирования пакетов услуг, так как агрегация сервисов осуществляется клиентом, а ответственность за агрегацию сервисов лежит на операторе. Отсутствие обоснованной ценовой политики для пакетных продуктов, так как невозможно корректно определить себестоимость услуг. Сложность обоснования и отслеживания эффективности инвестиций в ресурсы (инфраструктуру, сети связи), так как напрямую нет привязки к бизнес-результату. Затруднительность развития партнерских отношений при формировании пакетов услуг из-за сложности агрегации сервисов от разных сетей и поставщиков
Недочет	Неоптимальный (не поставлен на постоянную основу) процесс PLM или его отсутствие
Следствие	Большое время вывода на рынок новых услуг, так как для каждой услуги заново разрабатывается свой жизненный цикл. Разрыв между маркетингом, внедрением технологий и управлением компанией

Рис. 3. Спираль развития услуг



род, район), один клиентский сегмент и ограниченное число клиентов, определенный вид продуктов (например, широкополосный доступ), ограниченный набор систем OSS/BSS и т.п.;

- построить единую информационную модель компании, в частности создать классификатор услуг, сервисов, ресурсов;
- формализовать и отработать сквозные процессы предоставления услуг для массового клиента с необходимой степенью их автоматизации;
- настроить имеющиеся у оператора системы OSS/BSS и произвести их интеграцию с другими системами в рамках модели.

На следующих этапах развития действующая модель может быть расширена по географии, клиентским сегментам, массовости и типу услуг, интегрированных OSS/BSS-систем и уровню автоматизации процессов.

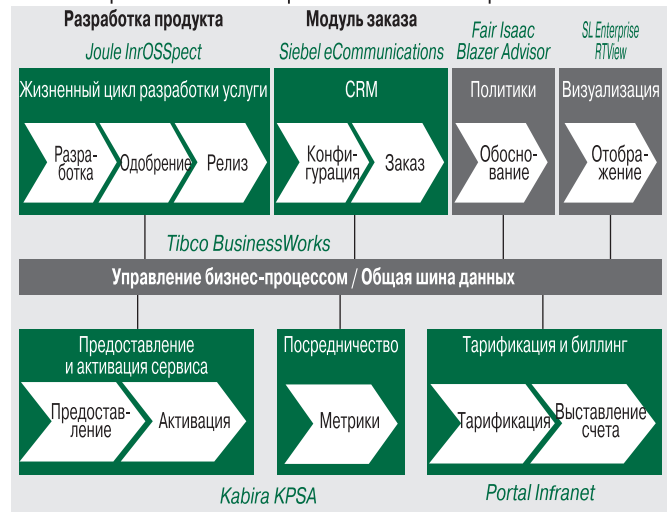
Пример разработки действующей модели PLM

Методологии и наработки TM Forum являются концентрацией практического опыта телекоммуникационной отрасли в части управления бизнесом, и их применение гарантирует оператору успех в достижении цели. На пилотных проектах-ускорителях (Catalyst) TM Forum обкатывает методологии с применением типовых услуг и решений OSS/BSS мировых производителей на базе ведущих телекоммуникационных операторов.

В рамках пилотного проекта «PLM вместе с NGOSS», представленного еще в 2003 г., для отладки и автоматизации процессов PLM использовалась методология NGOSS (Next Generation Operations Systems & Software – системы и программное обеспечение нового поколения) и ее составляющие: eTOM и SID (Shared Information/Data Model – общая информационная модель). Были поставлены и решены следующие задачи:

- разработка нового продукта на базе существующих сервисов, включая новую ценовую политику;
- создание цикла одобрения и выпуска нового пакета услуг;
- увязка пакета услуг с конкретным каналом дистрибуции;
- автоматическое обновление каталога продуктов в среде OSS;
- реализация множественности сервисов в пакете услуг;
- учет при формировании ценовой политики данных о стоимости ресурсов сети.

Рис. 4. Архитектура действующей модели PLM, реализованная в рамках пилотного проекта TM Forum



В результате реализации проекта на базе австралийского оператора связи Telstra была создана действующая модель PLM и отлажена на пакете услуг BigPond (www.bigpond.com). При этом для реализации и автоматизации необходимой функциональности процессов использовались реальные продукты OSS/BSS различных производителей (рис. 4).

Резюме

■ Отлаженный процесс PLM уникален для каждой компании и задействует все основные составляющие бизнеса оператора связи: управление, маркетинг и технологии.

■ Маркетинг – неотъемлемая составная часть процесса управления жизненным циклом продукта.

■ Для правильной и эффективной настройки процесса PLM целесообразно использовать имеющийся опыт и наработки TM Forum, часть которых рекомендована Международным союзом электросвязи в качестве эталонной модели. ИКС

Будущее наступит уже завтра, или Трудная дорога к 4G

Возможные пути развития технологий 4-го поколения (4G) сегодня волнуют многих экспертов. Похоже, специалисты уже довольно отчетливо представляют, что потребуется для подобной эволюции (как минимум более высокая пропускная способность и бесшовная интеграция) и каким будет набор переходных технологий.



Мори РАМНИ,
Agilent Technologies



Ким ТРАН,
Agilent Technologies

Пока четко определенного направления развития технологии 4G не существует. Хотя определение 4G, предложенное МСЭ, выглядит достаточно ясным: оно призывает к интеграции трех областей беспроводного доступа – домашнего, локального (ближайшего к работе и офису) и по всему миру, а также к единому подходу: везде высокая пропускная способность и бесшовная интеграция. Появляются технологии, которые могли бы стать движущей силой перехода на 4G и обладающие возделенными возможностями глобального взаимодействия, необходимой пропускной способностью и т.д., и т.п.

Провозвестники 4G

Системы на базе технологии Multiple Input Multiple Output (MIMO) позволяют **линейно увеличить пропускную способность и емкость системы** относительно числа передающих и принимающих сторон. Реализовать их можно двумя способами. Первый – разнесение приемопередачи для повышения устойчивости работы системы и расширения диапазона. Второй – передача нескольких отдельных потоков данных по параллельным (разделенным в пространстве) каналам. Возможна и комбинация этих методов.

Что касается радиointерфейсов, то для повышения эффективности использования спектра, устойчивости работы системы и достижения оптимальной мощности передачи сигнала в системах 4G предполагается реализовать **динамическую адаптацию метода модуляции и скорости кодирования**, исходя из состояния каналов и оценок их качества. Высокую пропускную способность также призваны обеспечить новые, более совершенные схемы модуляции и кодирования. Основной кандидат на роль 4G-радиointерфейса – OFDM, обладающий естественной устойчивостью к ухудшениям таких характеристик каналов, как, например, затухание.

Следующее требование 4G – **беспшовность среды связи**, обеспечение взаимодействия между разными системами и разными организациями. По всей вероятности, этим критериям может соответствовать технология программно-управляемого радиотерминала (Software-Defined Radio, SDR), позволяющая управлять несколькими методами модуляции, широкополосной и узкополосной работой, функциями безопасности связи (такими, как скачкообразная перестройка частоты) и формой сигналов в широком диапазоне частот в соответствии с существующими и развивающимися стандартами. С помощью SDR можно обеспечить гладкий роуминг, загрузку новых конфигураций и функций по радиоканалу, реализацию расширенных сетевых функций, т.е. создать действительно широкополосную мобильную связь.

В результате терминалы станут более сложными и более интегрированными, появятся новые функции для поддержки вертикальных и горизонтальных сетевых иерархий, различных радиointерфейсов и конфигурируемых архитектур. Это означает, что большинство функций следующего поколения будет создаваться в виде одной сложной «системы на чипе» (System on Chip, SoC) или «системного пакета» (System in Package, SiP). А реализованные в этой системе переносимые приложения будут включать фильтры, антенные и иные компоненты для работы в среде смешанного режима.

Однако на дороге, ведущей к 4G, немало серьезных препятствий.

«Стандартные» особенности

Некоторые из этих проблем порождены недалевидностью Международного союза электросвязи в отношении технологий следующего поколения. Несмотря на то что в середине 90-х целью инициативы МСЭ в области технологий 3G было создание единого стандарта радиосвязи с высо-

кой степенью мобильности, результатом работ стали пять, в сущности несовместимых, стандартов. Причина – столкновение интересов конкурентов, а по сути – реалии рынка. Ситуация с 4G аналогична, притом что сегодня проблемы сочетаемости разных технологий и IP значительно сложнее, чем 10 лет назад, а вероятность воплощения «унифицированной» технологии 4G еще меньше, чем для 3G. Самая же большая беда в том, что мы не всегда извлекаем уроки из прошлого опыта.

К сожалению, несмотря на «правильные» лозунги, МСЭ при описании потенциала новых технологий радиосвязи уделяет недостаточно внимания вопросам обеспечения высокой пропускной способности системы и качества обслуживания (QoS). Так, до сих пор не решены некоторые проблемы, связанные с переходом от GSM к WCDMA. Поэтому неудивительно, что из-за существующих преград гораздо больших инвестиций потребуют такие, например, области, как функциональная совместимость оборудования и управление радиоресурсами (Radio Resource Monitoring, RRM).

А между тем именно RRM отвечает за принятие решений по управлению мощностью радиоканалов, частот и эффективности кодирования для предоставления услуг с высоким качеством обслуживания (QoS) в условиях ограниченной пропускной способности радиоинтерфейса. Особое внимание при беспроводной связи следует уделить QoS. Превосходные инновационные технологии, такие как VoIP, PTT и UMA, могут помочь сэкономить средства. Но решающий фактор успеха 4G – качество связи и на-

дежность (в идеале сети 4G должны соответствовать наземным широкополосным каналам). Без надлежащего качества увеличение пропускной способности потеряет всякий смысл.

Что еще важно для конечных пользователей? Конечно же, роуминг. И здесь необходимо подумать о технологиях хэндовера. Успех любой системы беспроводной связи зависит не только от стоимости оборудования (инфраструктуры и мобильных телефонов), но и от алгоритмов внутрисистемного и межсистемного хэндовера. Очевидно, что с внедрением технологий 3G осуществлять хэндовер проще не стало.

Увы, но напрямую эта проблема не решается разработкой стандартов, определяющих правила выполнения хэндовера. Ведь стандарт никак не описывает временные алгоритмы его исполнения. Кроме того, стоящая перед технологиями 4G задача интеграции систем с высоким и низким уровнями мобильности означает, что обеспечить в них гладкий хэндовер гораздо сложнее, чем в сетях 3G.

В то же время органы по стандартизации, весьма преуспевающие в синтаксисе, лексике и в некоторой части грамматики стандартов беспроводной связи, остальное содержательное наполнение спецификаций оставили операторам и производителям оборудования. Они-то и должны попытаться превратить весь этот набор инструментов или правил в давно обещанный нам бестселлер под названием «Беспроводная утопия» или что-то близкое к нему.

Результат непредсказуем: тут и недовольство хэндовером со стороны клиентов, и опасность ввести их в заблуждение. Ведь на рынке мобильных беспроводных устройств царит полный разномыслие, а сложность среды прикладных систем постоянно возрастает.

Еще одна группа проблем связана с физическим уровнем организации связи, например с новыми методами модуляции и более высокой скоростью передачи данных. Главный вопрос сетей 4G: как заставить новые технологии работать в реальной среде радиосвязи? Ведь это уже не сеть GSM с одним-двумя диапазонами частот, одним сервисом голосовой связи и службой SMS. Управлять столь сложной средой, как 4G, – очень непростая задача.

В погоне за новыми технологиями физического уровня отрасль беспроводной связи продолжает поиски некоего приложения-«убийцы» (а по сути – спасителя), которое позволило бы окупить инвестиции. Однако с учетом существующих для 3G и появляющихся для 4G трудностей наиболее вероятно, что истинным убийцей 4G может стать сама сложность этих технологий и огромное их разнообразие.

Есть ли выход из этой ситуации? Возможно, проблеме удастся решить, разделив отрасль на группы «по стандартам» в попытке ограничить «количество переменных». Это позволит создать бизнес-модель ограниченного применения, но не поможет осуществить бесповоротную интеграцию беспроводных систем в мировом масштабе.

Другое решение – применение архитектуры UMA, которая позволяет оператору в рамках своей сети развернуть несколько закрытых корпоративных систем на базе «фирменных» протоколов в разных географических зо-


WWW.STI-EXPO.RU

Безопасность
Телекоммуникации
Информация




21-24 ноября 2006
Выставочный комплекс
им. П. Алабина, Самара

Организатор:

Москва
тел.: +7(095) 101 44 07
факс: +7(095) 101 44 17
e-mail: secure@rte-expo.ru

Самара
тел.: +7(846) 270 41 00
факс: +7(846) 270 41 72
e-mail: sti@expodom.ru



Официальная поддержка:



МЧС России
Самарская поисково-спасательная служба



Министерство транспорта,
связи и автомобильных дорог
Самарской области

нах. Но и оно ни на шаг не приближает нас к идеалу сотовой/беспроводной системы, которая работает везде и для всех.

Теоретически время для решения проблем еще есть. Но следует помнить, что потребителю не нужна связь на скорости 14 Мбит/с, если из-за проблем с QoS на нее нельзя положиться.

Измерить несуществующее

Это может показаться фантастикой, но некоторые работы по тестированию и измерениям технологий 4G уже осуществимы на практике. И все благодаря проекту 4G Radio Project (www.4G-radio.de), разрабатываемому совместно компаниями STMicroelectronics, Infineon Technologies, Agilent Technologies и другими производителями при участии университетов. Цель проекта – сократить сроки разработки передовых чипсетов и платформ SoC в области 4G-радиосвязи за счет создания стандартизованных библиотек схем и конфигурируемых цифровых компонентов. В рамках проекта разработаны решения производителей контрольно-измерительного оборудования, обеспечивающие имитацию всего приемопередающего тракта – от чипсета (DSP) до радиоинтер-

фейса – и позволяющие использовать собственные патентованные модели для имитационного моделирования систем и анализа схем.

Среди них и ПО Advanced Design System (Agilent), и платформа для автоматизации проектирования электронного оборудования, и ряд устройств в области генерации и анализа сигналов. Требования к такому оборудованию – возможность масштабирования по диапазону частот, полосе пропускания информации и динамическому диапазону, а также средства конфигурирования для проведения многоканальных измерений.

Однако пока нет «предмета исследования» целиком, неясно, сможет ли контрольно-измерительная отрасль помочь в создании эффективного оборудования, предложив сложные мультистандартные системы имитационного моделирования. Сегодня трудно предсказать, как будут решаться в сетях 4G такие системные вопросы, как управление радиоресурсами или взаимодействие приложений. А поскольку об упрощении пока и речи не идет, надо подготовиться к постоянной и все возрастающей зависимости производителя от дорогостоящих полевых испытаний. ИКС

Потребителю не
нужна связь на
скорости
14 Мбит/с, если
из-за проблем с
QoS на нее нельзя
положиться

Крупнейшее событие в области вещательных и телекоммуникационных технологий

9-я международная выставка и конференция

ССТВ - 2007

5-8 февраля
Крокус Экспо
Москва, 66 км МКАД

Контент для сетей платного ТВ
Кабельное и Спутниковое ТВ
Широкополосный доступ
Телерадиовещание
Спутниковая связь
ТВ по IP протоколу
Мобильное ТВ
HDTV

Виражи коммуникаций

Организатор: MID'expo
Генеральные партнеры: АКТЕР, iabm
Со-организатор конференции: ИКС
Генеральные информационные спонсоры: СПУТНИК, БИТВ
Отраслевые медиа-партнеры: BROADCASTING, КОММЕНС
Генеральный интернет-партнер: COMNEWS
Официальный туроператор: MID TRAVEL

За дополнительной информацией обращайтесь: тел.: (495) 737 74 79, факс: (495) 145 51 33, anastasia@midexpo.ru
www.cstb.ru
на правах рекламы

Контроль доступа вместо антивируса



Одна из ключевых проблем обеспечения информационной безопасности – защита ПК при его подключении к сети, когда сразу же появляется необходимость противодействия вредоносным кодам (троянам, червям и проч.), а также шпионским программам. И здесь нет различий между локальной или территориально распределенной ИС: место обитания всей этой «фауны» – компьютер. Поэтому и начинать защищать свою информацию надо с него.



А.Ю. ШЕГЛОВ,
гендиректор НПП
«Информационные
технологии в
бизнесе», д.т.н., проф.



К.А. ШЕГЛОВ,
менеджер НПП
«Информационные
технологии в бизнесе»

Все это вредоносное ПО может быть как «самостоятельным», так и частью вполне легального приложения (например, свободно распространяемого), которое разработчик вольно или невольно наделил подобными недекларируемыми возможностями. В общем случае атаки таких программ нацелены либо на хищение корпоративных данных, либо на вывод из строя компьютерных ресурсов. Следовательно, объекты защиты от данных угроз – ресурсы, как информационные, так и системные.

В наши дни для решения этих задач широко используются сигнатурные анализаторы (антивирусное ПО), призванные предотвратить возможность несанкционированного появления вредоносных кодов в ПК. Однако сигнатурный анализ не позволяет решить данную задачу в общем виде.

Противодействовать недекларируемым функциям приложений эти методы тем более не могут. А кто знает, что несет установленная на ПК программа, когда проявятся «закладки», и есть ли гарантии, что подобными «сюрпризами» не начинено не только свободно распространяемое, но и коммерческое (особенно зарубежное или заказное) ПО? Ведь недекларируемые возможности могут быть и результатом ошибок программирования. Очевидно, что в общем случае задача защиты компьютера намного шире потенциала антивирусов.

Но существует ли способ эффективно и всестороннего противодействия разнообразным вредоносным и шпионским кодам, включая недекларируемые функции, в том числе и от ошибок программирования? На наш взгляд, такое «противоядие» есть – это технология, основанная на реализации механизмов контроля доступа (разграничения прав доступа) к ресурсам. Заметим, что речь идет не о теории или некоей гипотетической технологии, а о решении, воплощенном в продукте «Панцирь-К», который его разработчик, НПП «Информационные технологии в бизнесе», позиционирует как комплексную систему защиты информации (КСЗИ). Комплексную, поскольку это СЗИ, ориентированное на работу с ОС Windows 2000/XP/2003, предназначено для противодействия как внешним, так и внутренним ИТ-угрозам.

Любой процесс может нести угрозу

В основе этой технологии лежит концепция: процесс может нести угрозу внешней атаки (из сети), а следовательно, необходимо гарантировать защиту компьютерной информации путем контроля запуска и локализации действий процессов на защищаемом компьютере. Регламент действий процессов обеспечивается за счет контроля доступа (разгра-

Немного статистики

Грэхем Ингрэм, главный управляющий австралийского подразделения Группы оперативного реагирования на чрезвычайные ситуации в компьютерной области (AusCERT), утверждает, что распространенные антивирусные приложения блокируют лишь около 20% недавно появившихся вредоносных программ. При этом популярные антивирусы пропускают до 80% новых троянов, шпионов и других вредоносных программ. Это означает, что в восьми случаях из десяти недавно появившийся вирус может проникнуть на компьютер пользователя.

Источник: www.itsec.ru

ничения прав доступа) к защищаемым ресурсам (информационным и системным), при котором субъектом доступа становится процесс.

Воплощение этой технологии требует принципиального изменения самой схемы назначения и исполнения политики разграничения доступа к ресурсам, используемой в современных ОС (в частности, семейства Windows). Ведь там субъектом доступа к ресурсам является пользователь (контроль доступа к ресурсам осуществляется на основании его учетных записей), а в данном случае речь идет о недоверии не к нему, а к процессу.

Программная среда в кольце защиты

Механизм обеспечения замкнутости программной среды – одно из наиболее эффективных средств противодействия запуску несанкционированных программ – используется практически всеми приложениями СЗИ. При защите от внутренних ИТ-угроз он запрещает исполнение какой-либо программы, которая может стать инструментом взлома системы защиты (подобную программу практически всегда можно создать, зная функциональные возможности и архитектурные принципы построения СЗИ).

В нашем случае механизм предназначен для противодействия запуску любого стороннего ПО на защищаемом ПК, в том числе внедренного из сети. Он допускает исполнение лишь разрешенного набора программ: любое ПО, кроме легитимного, не может быть запущено. Такой подход позволяет в принципе отказаться от какого-либо сигнатурного или иного подобного анализа исполняемого кода.

Создание замкнутой программной среды достигается за счет исполнения механизмом контроля доступа регламента запуска и обеспечения целостности ПО. При этом механизм считается реализованным корректно лишь при условии выполнения требований к полноте и корректности разграничений прав на запуск исполняемых файлов. Под полнотой разграничений понимается возможность регламентировать доступ для операции «выполнить» для всех ресурсов, откуда возможен запуск ПО, а под корректностью – способностью противодействовать любой модификации разрешенных к исполнению объектов, а также запуску под их именем других (несанкционированных) программ.

Реализовать механизм обеспечения замкнутости программной среды можно разными способами. Наиболее часто используется задание списков разрешенных к запуску процессов, а запрет модификации обеспечивается

путем контроля целостности исполняемых файлов перед запуском. Однако из-за сложности администрирования и увеличения загрузки вычислительного ресурса ПК их практическое использование ограничено.

В предлагаемой реализации для локализации программной среды необходимо регламентировать права доступа к папкам (каталогам, подкаталогам), из которых пользователям разрешено (запрещено) запускать исполняемые файлы. С учетом принятых правил размещения приложений и необходимости запуска системных процессов целесообразно разрешить выполнение программ из каталогов \Program Files и \WINNT (WINDOWS). А чтобы предотвратить возможность модификации санкционированных исполняемых файлов, запись в них, напротив, следует запретить.

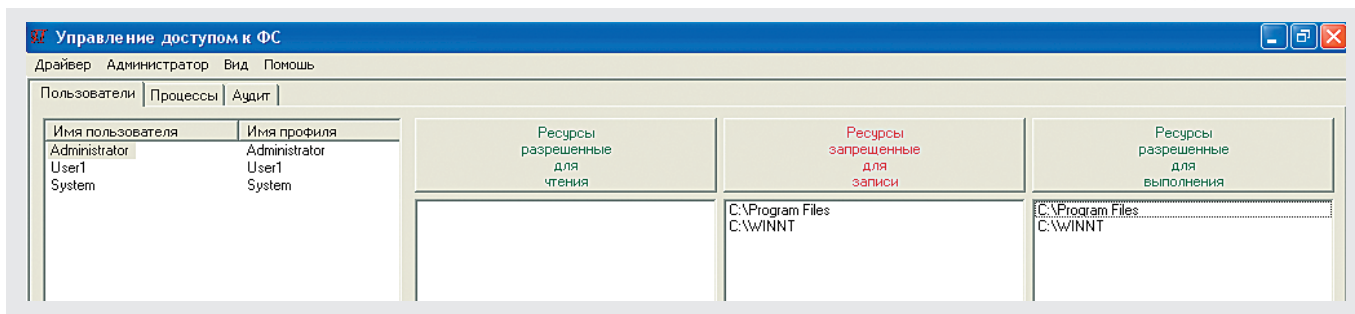
К достоинствам данного решения можно отнести простоту администрирования механизма защиты и отсутствие негативного влияния на вычислительную нагрузку ПК, так как контроль запуска процессов не требует исполнения каких-либо дополнительных ресурсоемких операций.

Заметим, что интерфейс настройки доступа (рис. 1) отличается от соответствующих интерфейсов универсальных ОС. Первое (и основное) различие: **права доступа назначаются пользователям, а не устанавливаются как атрибуты файла**. Кроме того, за основу принят разрешительный регламент, а также минимизирована номенклатура прав доступа (их всего три: чтение, запись, выполнение, а остальные устанавливаются системой автоматически).

Но есть и еще одна проблема «замыкания» среды, свойственная ОС Windows и приложениям, – невозможность разделить между пользователями ряд совместно используемых объектов, например папки All Users. Именно поэтому принципиально невозможно корректно задать разграничительную политику разных пользователей. Ведь все они имеют равные и полные права доступа к одним и тем же файловым объектам. Особенно критичной задача становится при необходимости организации противодействия внутренним ИТ-угрозам, если на одном ПК обрабатывается и открытая, и конфиденциальная информация и используются различные режимы ее обработки.

Но как быть с проблемой записи на системный диск? Некоторые приложения должны иметь право записи информации на системный диск, на который, согласно регламенту, запись должна быть запрещена (см. рис. 1).

Рис. 1. Экран "Управление доступом" (пример 1)



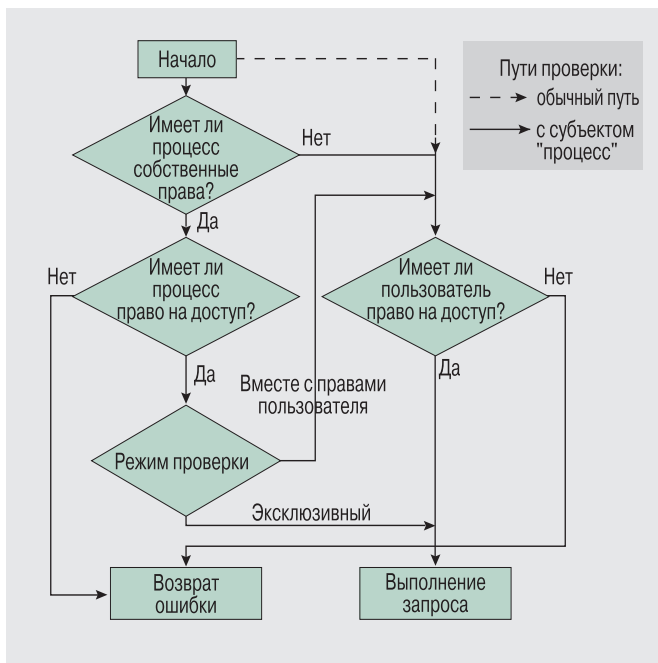
Все эти задачи могут быть решены с помощью механизма «переназначения путей к каталогам» (патент № 2234123). Идея его в том, что для каталога, доступ к которому следует либо переназначить (разделить между пользователями неразделяемый объект), либо переадресовать с системного на иной диск, создается несколько каталогов (для каждого пользователя) или (при переадресации) один на другом диске. Любое обращение к исходному каталогу механизмом Windows перехватывается и анализируется, чтобы выяснить, кто его владелец и кем произведено данное обращение. И только затем оно транслируется на созданный новый каталог пользователя (или другой диск).

Таким образом, исходный каталог становится виртуальным и никакое приложение не может получить к нему доступ. Приложение же, для которого данная переадресация «прозрачна», взаимодействует с созданным каталогом пользователя (или каталогом на другом диске) согласно правам доступа, назначенным в соответствии с политикой.

Всё под контролем

Как уже отмечалось, угрозу могут нести в себе не только сторонние программы, запуск которых гарантированно предотвращается механизмом обеспечения замкнутости программной среды, но и вполне легальное ПО, санкционированно установленное на защищаемом ПК. Ни один производитель не может дать гарантий, что его ПО не содержит недекларируемых возможностей. Ведь таковые могут являться не только следствием сознательного внесения подобных функций разработчиком, но и результатом ошибок программирования. Нельзя сбрасывать со счетов и возможность сознательного внесения закладок при создании ПО – прежде всего это касается свободно распространяемых продуктов.

Рис. 2. Пути проверки запроса



Очевидно, что при подключении к сети наиболее подвержены атакам сетевые службы, через которые злоумышленник потенциально способен получить несанкционированный доступ к информационным или системным ресурсам. Поэтому именно **права процесса** сетевого обмена при доступе к информационным и системным ресурсам следует регламентировать в первую очередь. Таким образом, при управлении доступом к ресурсам появляются два самостоятельных субъекта доступа – **пользователь** и **процесс**, причем управлять доступом (разграничивать права) необходимо не только для первого, но и для второго субъекта.

В нашей реализации задействованы три схемы задания политики разграничения доступа к ресурсам (патент № 2207619):

- для процессов без учета прав пользователей (эксклюзивный режим обработки запросов процессов: доступ к объекту разрешен, если он разрешен процессу);
- для пользователей без учета ограничений для процессов (эксклюзивный режим обработки запросов пользователей: доступ к объекту разрешен, если он разрешен пользователю);
- комбинированное разграничение: права доступа к объектам процессов разрешены в рамках ограничений для пользователей (доступ к объекту разрешен, если он разрешен и пользователю, и процессу).

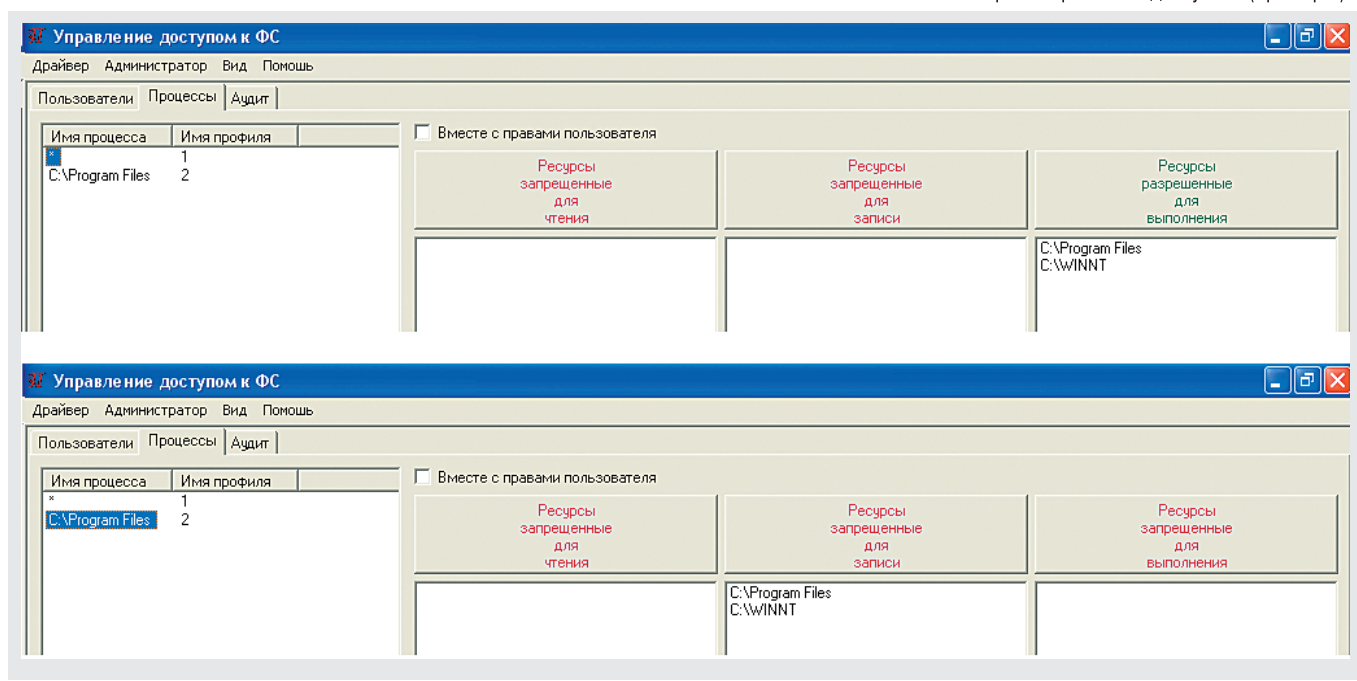
Последняя схема предполагает, что в любой системе угрозы могут исходить как со стороны пользователей, так и со стороны процессов. Таким образом, в качестве субъекта доступа может рассматриваться либо только пользователь, либо только процесс, либо пара процесс–пользователь (рис. 2).

Заметим, что реализованный механизм позволяет настраивать замкнутость программной среды не только для пользователей, но и для процессов, если последний становится субъектом доступа (рис. 3). Можно разрешить любому процессу (как субъекту) запуск исполняемых файлов только из каталогов \Program Files и \WINNT (WINDOWS) и запретить процессам запись в них. Очевидное достоинство этого решения – «равноправность» разграничений для всех пользователей вне зависимости от корректности их идентификации при доступе к ресурсам (в частности, атаки на расширение привилегий становятся невозможными).

Включение в разграничительную политику субъекта доступа «процесс» не только обеспечивает новые свойства защиты, но и позволяет принципиально изменить подходы к реализации базовых механизмов обеспечения компьютерной безопасности. Так, чтобы защитить хранящиеся на компьютере данные от возможных деструктивных действий соответствующего процесса (приложения), для работы с ним нужно выделить отдельный файловый объект (например, каталог) и разрешить процессу взаимодействовать только с этим объектом (установив соответствующие правила разграничения доступа для процесса).

Другими словами, файловые объекты следует подразделять на две категории – для хранения данных пользо-

Рис. 3. Экран "Управление доступом" (пример 2)



вателей и для работы с контролируруемыми процессами. Для копирования же данных из одного объекта в другой (если такая операция необходима) надо задействовать «проводник» (некритичный процесс), не несущий в себе угрозы.

Поскольку к системным ресурсам для ОС семейства Windows относятся и объекты реестра ОС, рассмотренная выше методология разграничения доступа к защищаемым ресурсам в полной мере распространяется и на системный реестр.

Таким образом, с помощью предлагаемой технологии, задавая соответствующие ограничения, можно добиться высокоэффективной защиты от вредоносных и шпионских программ, предотвратив хищение из ИС организации конфиденциальных данных и модификацию системных ресурсов. Для противодействия сетевым атакам контролировать следует в первую очередь сетевые компьютерные ресурсы, в частности сетевые службы и приложения.

Для дополнительной защиты от шпионского ПО (или потенциально обладающего подобными функциями) можно также задействовать механизм разграничения прав доступа пользователей и процессов к сетевым ресурсам (хостам). Он ограничит взаимодействие компьютеров рамками корпоративной сети и предотвратит передачу данных от шпионской программы вовне (заметим, если для подобной программы задан «регламент действий», то она сможет передать вовне лишь совсем неинтересную для злоумышленника информацию).



Итак, для защиты сети от вредоносных и шпионских программ методы сигнатурного анализа (поиск вредоносного кода), реализуемые антивирусами, малоприменимы (а об их эффективности говорить вообще не приходится). Намного целесообразнее использовать меха-

низмы контроля доступа к ресурсам. Однако применительно к решению данной задачи эти механизмы требуют кардинальной модификации (в частности, включения в разграничительную политику субъекта доступа «процесс»). В противном случае информационные ресурсы корпорации окажутся уязвимы. ИКС

РОСТОВСКИЙ ФОРУМ ВЫСОКИХ ТЕХНОЛОГИЙ
Телекоммуникации и Связь.
Компьютеры.
29 ноября-1 декабря 2006 г.

САПР
АСУТП
оргтехника
процессоры и микросхемы
настольные и мобильные ПК
радиоизмерительная техника
телекоммуникационное оборудование
системы и аппаратура радио и спутниковой связи
автоматизированные системы связи и управлением связью
сетевое оборудование и комплексные системы обеспечения телекоммуникационных систем связи
сетевая и коммуникационная продукция, программное обеспечение для телекоммуникаций

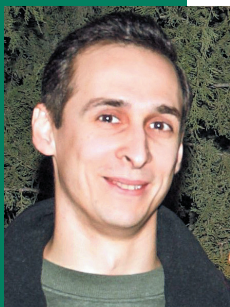
Организатор: **ВЫСТАВОЧНАЯ ПЛАЦА** ФИРМА **PLAZA**
344 082, Ростов-на-Дону, пр. Буденновский, 27, оф. 20
E-MAIL: INFO@PLAZA-EXPO.RU
ТЕЛ./ФАКС: (863) 266-34-46, 240-69-42,
240-66-83, 262-70-57

Информационная поддержка:
itnews **it** **Эксперт**
itnews.ru **it** **Эксперт.ru**

реклама

Риски мобильности можно снизить

В июне 2005 г. впервые в истории сотовой связи компьютерный червь, получивший название Cabir, атаковал мобильные устройства. Распространяясь через Bluetooth, он поражал сотовые телефоны и прочую мобильную технику с ОС Symbian. К счастью, червь оказался довольно безвредным и до широких эпидемий дело не дошло. И все же это был первый тревожный сигнал для директоров ИС и ИТ-менеджеров компаний. А главное, всем стало ясно, что и мобильные устройства не застрахованы от атак.



Антон РАЗУМОВ,
Check Point Software
Technologies

За первой атакой последовали и другие. Несмотря на то что они становятся все изощреннее и интенсивнее, пока угрозы глобальной эпидемии, вызванной мобильными червями или вирусами, слава Богу, нет. Но как только мобильные устройства перейдут на стандартные платформы, а вирусописатели изобретут новые способы наведения хаоса в корпоративном мире, ситуация, несомненно, ухудшится. Эксперты по безопасности из Gartner, Yankee Group и других аналитических компаний называют 2006 г. годом вирусов для мобильных устройств. Очевидно, что системным администраторам пора уже не просто фиксировать факты «мобильной» атаки, а активно работать над защитой мобильных устройств от вредоносного кода. Только это может спасти сеть, прежде чем будут материализованы мобильные угрозы следующего поколения.

Управление под контролем

Не секрет, что многие сотрудники компаний просматривают почту и выходят в Интернет через свои мобильные устройства. А в них, в отличие от обычных сотовых телефонов, где хранятся в основном номера телефонов и адреса, могут быть записаны файлы всех типов, какие только возможно записать на жестком диске ПК. Более того, на смартфонах часто работают программы, предоставляющие доступ к защищенным паролем онлайн-службам, что подвергает конфиденциальные данные еще большему риску.

Безопасность в сотовой связи – это баланс между риском и доступностью. Когда системные администраторы повышают безопасность се-

ти, пользователям становится труднее получить к ней доступ. А если упростить доступ, защищенность обычно резко ухудшается. Компании, позволяющие сотрудникам обращаться к своим сетям через персональные цифровые устройства (PDA) и другие карманные компьютеры, должны учитывать это и требовать, чтобы «мобильное чудо» подключалось через специально выделенный для таких целей брандмауэр. Где бы такое ПО ни находилось – в периметре ли сети или в самих устройствах – эти брандмауэры гарантируют, что трафик, прошедший через них, при достижении ядра сети будет безопасен.

Контроль доступа – забота не только корпоративных пользователей. Операторы сотовых и беспроводных сетей тоже способны повлиять на защиту – надо только этого захотеть. Но сегодня практически нет законов, обязывающих поставщиков услуг гарантировать безопасность. Видимо, поэтому многие из них предлагают такую защиту «опционно» и на платной основе.

Однако когда черви и вирусы начнут так же яростно штурмовать мо-



Стоит одному из пользователей нарушить инструкции, и скомпрометированной может оказаться вся сеть

бильные устройства, как сейчас Интернет, безопасность, по всей вероятности, станет главным дифференциатором мобильного рынка, а антивирусная защита – частью стандартных соглашений Service Level Agreements (SLA).

Все дело в политике

Здравый смысл подсказывает, что однородную сеть гораздо легче контролировать, чем неоднородную. Пре-

дусмотрительные системные администраторы понимают это и с самого начала вводят регламенты, регулирующие типы применяемых мобильных устройств. Однако задача не так проста, как может показаться на первый взгляд, главным образом потому, что многие сотрудники пользуются собственными устройствами. И тогда проведение такой политики мобильной безопасности становится почти невозможным.

Тем не менее, вступив в игру в самом ее начале, системные администраторы могут избежать этой проблемы. Установив требования к мобильным устройствам, они должны эффективно донести их до сотрудников. Большинство из них используют для этого рассылку предупреждений, которые пользователи должны прочесть, подписать и вернуть. Кроме того, пользователям необходимо разъяснить, как важно следовать этим правилам. Ведь стоит одному из них нарушить инструкции, и скомпрометированной может оказаться вся сеть. Не вредно будет предусмотреть и особое наказание.

Будьте архитектором

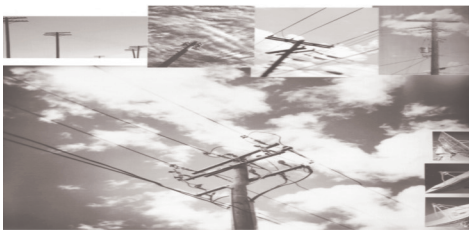
Наконец, нельзя добиться единой политики безопасности для мобильных устройств, не создав единую архитектуру защиты всего предприятия. Нередко в компании одна группа специалистов отвечает за безопасность сети, а другая – за мобильные и телекоммуникационные устройства. Подобная структура – прямой путь к взаимонепониманию и позорным провалам.

В тех компаниях, где заботятся о защите своей информации, одна и та же команда профессионалов занимается безопасностью и сети, и мобильных устройств. Но при этом избежать ошибок можно только в том случае, если для мобильных телефонов применяется одно решение безопасности, а для всех остальных элементов ИС – другое.

Но создание сильной внутренней защиты – только часть решения головоломки. Чтобы меры безопасности работали эффективно, необходимо наладить активную защиту самих мобильных устройств. Для этого есть специальное ПО, по крайней мере у двух компаний – Check Point Software Technologies и Trend Micro. **ИКС**

**Безопасность
сотовой связи –
это баланс между
риском и
доступностью**

BILLING **IT** TELECOM



Генеральный спонсор Конференции



OSS BSS
Telecom Forum

Платиновый спонсор Форума



12 - 14 декабря, 2006 Москва
Центр Международной Торговли

BSS сектор • Биллинг и поддержка клиента

- Биллинговые системы (Billing systems)
- конвергенция post/prepaid;
 - расчеты с партнерами (interconnect);
 - тарификация и биллинг новых сервисов;
 - противодействие мошенничеству (fraud management)
 - конвергентный пребиллинг (mediation)

Поддержка клиентов (Customer care)

- Help & service desk;
- самообслуживание;
- повышение лояльности и сокращение оттока;
- CRM.

OSS сектор • Поддержка сети

- Инвентаризация (Inventory)
- инвентаризация и учет ресурсов;
 - планирование сети.

Управление ошибками (Fault Management)

- регистрация неисправностей в сети;
- управление неисправностями в сети.

Управление производительностью (Performance management)

- производительность сети
- производительность IT систем

Управление и сетевой мониторинг (Network monitoring)

- сбор информации
- GPRS мониторинг
- SS7 мониторинг

OSS сектор • Поддержка услуг

- Управление заказами (Order Management)
- заказ услуг;
 - активация услуг.

Управление уровнем сервиса (SLA management)

- Мониторинг услуг (Services monitoring)
- мониторинг сервисов и контента (end-to-end мониторинг)
 - управление качеством голосовых услуг

INTEC

Золотые спонсоры

COMPTEL
INTELLIGENT LINK

NetCracker
Transforming the Service Layer™

Спонсор - экспонент

amdocs

Ассоциированный спонсор



Информационные партнёры

BROADCASTING



ИКС

СЕРВИС

МОБИЛЬНЫЕ

NEWS

Устроитель

eposystems

www.exposystems.ru/bitt/

+7 495 995 8080

Географические VSAT-опыты «ИКС» (№ 7'2006, с. 46–57) вызвали бурную реакцию читателей: звонили, узнавали, просили данные, писали... Не только письма, но и статьи. Таким образом географический VSAT-ФОКУС пополнился историческим. Причем события 10-летней давности продолжают проецироваться на карту рынка.

VSAT: красные дни календаря

История в приказах и программах



По поводу истории VSAT в России есть два мнения: официальное и «народное». Согласно первому, правила применения VSAT в России существенно упрощены и этот сегмент рынка успешно развивается. «Народ», иначе – игроки рынка, считают, что заявленная простота – лишь ретушь на полотне суровой действительности, а все прежние препоны остались и серьезно мешают развитию сети малых земных станций.

Все участники означенного сегмента рынка спутниковой связи сходятся лишь в том, что VSAT-технологии для России архиважны, а их использование зачастую является единственным способом организации удаленного доступа к информационным ресурсам и ликвидации информационного неравенства регионов. Поэтому о том, надо ли упрощать, не спорит никто.

Еще год-полтора, и процесс упрощения использования VSAT отметит свой 10-летний юбилей. Точкой отсчета можно считать Решение ГКРЧ от 27 июля 1998 г. (протокол № 8/5) «О применении на территории Российской Федерации малых земных станций спутниковой связи с диаметром антенн 3,8 м и менее». Хотя в нем еще не было обозначения станций VSAT как технологического объекта, подразумевались именно они. Это решение отменило необходимость регистрации начала строительства ЗССС с антеннами не более 3,8 м и предоставило возможность использования типовых проектов и заводских инструкций. В том же году появился и ОСТ 45.98-98 «Станции земные вида VSAT (ВИСАТ) спутниковых сетей связи. Основные технические требования».

В международном фарватере...

В самом конце 90-х процесс упрощения в нашей стране застыл. Но в 2000 г. Правительство РФ

все же определило генеральную линию: сблизить российские регламенты с европейскими, отдавая предпочтение европейским стандартам и Району 1 при частотном планировании и выборе технологий (Постановление Правительства РФ от 26 мая 2000 г. № 413).

Реакция Минсвязи в части стандартизации последовала в 2001 г. Выпущенный регулятором РД 45.192-2001 «Правила технической эксплуатации спутниковых линий передачи» установил (п. 3.5.5), что отдельный класс земных станций составляют станции ВИСАТ (VSAT), которые относятся к общей категории малых земных станций спутниковой связи (антенна не более 3,8 м).

В апреле 2001 г. вопросы упрощения процедуры применения VSAT-станций достигли уровня Совета межправительственной ассамблеи государств – членов СНГ. Решение круглого стола № 7 «Перспективы развития и возможности сотрудничества в области спутниковой связи» (от 18 апреля 2001 г.), в котором указана «приоритетность для стран Содружества разработки нормативной правовой базы и широкого внедрения новых информационных технологий на базе земных станций типа VSAT» было направлено в ООН, ОБСЕ и МСЭ. Таким образом, СНГ пять лет как вышло на международную арену в отношении намерений развития и широкого внедрения VSAT.



СЕПТ (European Conference of Postal and Telecommunication Administrations), Европейская конференция администраций почты и электросвязи, представила на обсуждение Европе два новых проекта решений по упрощению применения VSAT-станций Ku- и Ka-диапазонов.

1. Согласно проекту ECC/DEC(05)JJ, предлагается разрешить применение низкоэнергетических VSAT (тип LEST), работающих в полосах частот 10,7–12,75/19,7–20,2 ГГц на прием и 14–14,25/29,5–30,0 ГГц на передачу с уровнем ЭИИМ не более 34 дБВт, **без какой-либо регистрации со стороны администраций связи**. В отдельных случаях (если возникают проблемы с национальной

таблицей распределения частот) предусматривается только фиксация частотных назначений. Причиной разработки документа стало внедрение интерактивного ТВ при использовании перспективных КА. Таким образом, VSAT-станцию с ЭИИМ не более 34 дБВт предлагается «нормативно» приравнять к сотовому телефону.

2. Проект ECC/DEC(05)II предлагает администрациям связи начать применение высокоэнергетических VSAT (тип HEST), работающих в полосах частот 10,7–12,75/19,7–20,2 ГГц на прием и 14–14,25/29,5–30,0 ГГц на передачу с уровнем ЭИИМ выше 34 дБВт, но не более 60 дБВт, **по упрощенной форме регистрации** администраций связи.

Отметим, что международное сообщество, интересы которого в Районе 1 представляет организация СЕРТ, давно решило текущие нормативно-правовые проблемы применения VSAT, а теперь выдвигает и реализует все более революционные инициативы в этой сфере (см. врезку). Их цель – развитие более ранних решений СЕРТ, ограничивающих, например, ЭИИМ для VSAT Ku величиной 50 дБВт при мощности передатчика максимум 2 Вт.

...и в российском русле

Необходимость изменений в нормативной правовой базе не подвергалась сомнению и в России, особенно в свете федеральных целевых программ.

В 2002 г., по данным ГП «Космическая связь», в России насчитывалось всего 2 тыс. VSAT-«тарелок», из которых 1 тыс. находилась в собственности Центробанка РФ. Бывший в то время генеральным директором ГП «Космическая связь» (а ныне заместитель министра информационных технологий и связи)

Б.Д. Антонюк прогнозировал, что «если госорганы разберутся с лицензированием, то к 2007 г. число VSAT-«тарелок» может вырасти до 50 тыс., причем из них 31 480 будут «школьными». Если же этого не произойдет, число терминалов за пять лет вырастет лишь в 4–5 раз» (см. «Известия» от 20 апреля 2002 г., «Тарелка для Ваньки Жукова»)*.

Однако по сей день принципиальных изменений нормативной правовой базы в отношении упрощения применения VSAT не произошло, несмотря на оптимистические заверения Мининформсвязи. Так, на пресс-конференции в ходе итоговой коллегии 4 марта 2003 г. министр РФ по связи и информатизации Л.Д. Рейман заявил: «Сегодня этот вопрос (услуг VSAT-сетей. – *Авт.*) становится гораздо более актуальным, чем два-три года назад... Я не думаю, что в сегодняшних условиях нужно предпринимать какие-то специальные меры для развития «висатовских» станций и технологий, поскольку, мне кажется, существуют одно принци-

Министерство

образования

Мексики

планирует

в 2006 г.

установить

VSAT в 40% школ

По оценкам «ИКС», на май 2006 г. в России насчитывалось от 4 до 5,3 тыс. VSAT-станций (см. «ИКС» № 7'2006, с. 48–49), а по данным ГРЧЦ – все те же примерно 2 тыс.

бизнес- партнер

Спутниковая связь в сети общего пользования Республики Саха (Якутия)

Компания «КЛАССИКА» (www.classics.ru) – крупный российский системный интегратор, специализирующийся на создании телекоммуникационных сетей операторского класса, в том числе и с применением спутниковых технологий.

В этом году «КЛАССИКА» приняла участие в реализации Программы развития высоких технологий Республики Саха (Якутия). Специалистами компании в партнерстве с одним из ведущих операторов Дальневосточного федерального округа – ОАО «Сахателеком» – спроектирована и построена внутризоновая система цифровой связи на базе больших земных спутниковых станций, которая охватывает 17 районных центров республики. В результате такой модернизации телекоммуникационной инфраструктуры региона города Мирный, Удачный, Ленск, а также населенные пункты Хону, Черский, Оленек, Алыта и другие объединены современной цифровой сетью телефонной связи и передачи данных. Это привело к повышению качества обслуживания абонентов в регионе и расширению спектра услуг по предоставлению новых телефонных номеров, цифровых каналов связи и доступа в Интернет.

Итогом еще одного проекта ОАО «Сахателеком» и компании «КЛАССИКА» стало создание обширной спутниковой сети передачи данных и голоса на основе технологии малых земных спутниковых станций (VSAT). Жители более 70 удаленных и труднодоступных населенных пунктов республики получили возможность пользоваться телефоном через спутниковый хаб в Якутске.

В ходе выполнения – очередной совместный проект по реализации программы универсальной услуги связи на территории Республики Саха (Якутия). Первая очередь сети из 60 VSAT-терминалов, которые обеспечивают таксофонную связь для отдаленных сел, должна быть запущена в эксплуатацию в ближайшее время.

Реализация проекта цифровизации связи в Республике получила высокую оценку правительства Саха (Якутия). Президент Республики отметил работу компании «КЛАССИКА» персональной благодарностью.

В настоящее время «КЛАССИКА» развивает сотрудничество с ОАО «Сахателеком» и другими операторами связи, а также продолжает разработку решений для поддержки национальных проектов по медицинской, образовательной и другим программам, где спутниковые технологии, несомненно, будут востребованы.

Компания «КЛАССИКА»: (495) 956-34-37

реклама

пиальное препятствие и одна принципиальная проблема – сроки и стоимость рассмотрения заявки на «висатовскую» станцию. Я думаю, что нашей приоритетной задачей в 2003 г. является решение этого вопроса... В прошлом году мы решали вопросы, связанные с разрешением на сотовые телефоны, в этом году решим на «висатовские» станции... Это согласованное решение целого ряда заинтересованных министерств и ведомств... Думаю, что к середине года мы к этому решению подойдем».

В 2002–2006 гг. вышло немало постановлений Правительства РФ и решений ГКРЧ, посвященных упрощению нормативной правовой базы. В сфере VSAT практическим достижением можно считать лишь два решения ГКРЧ. Первое – о выделении полосы частот для VSAT Ku, включая нормативную формулировку существенных признаков, выделяющих VSAT-станции из общей категории малых земных станций спутниковой связи (от 6 декабря 2004 г.). Второе – обобщенное решение об использовании полос частот фиксированной спутниковой связи в C- и Ku-диапазонах для всех типов ЗССС, соответствующих определенным параметрам (от 4 июля 2005 г.). Оба действуют исключительно при использовании спутниковых сетей «Экспресс» (орбитальные позиции ГСО, закрепленные за Россией).

Если взглянуть на ситуацию в целом, эти нормы потенциально позволяют перейти к упрощению нормативных документов в части применения VSAT. Но потенциальному не суждено было реализоваться, поскольку появился ряд нормативных документов, прямо этому препятствующих. Следует особо выделить приказ Мининформсвязи от 29 октября 2004 г. № 25 «Об утверждении форм документов для регистрации и учета радиоэлектронных средств и высокочастотных устройств гражданского назначения». Он, в частности, требует представлять протоколы измерения технических параметров излучения радиоэлектронных средств с указанием измеренных географических координат и приложением копий лицензий Роскартографии на осуществление геодезической деятельности.

Все это напоминает басню про лебедя, рака и щуку. Гармонизации с Европой в сфере правовой основы VSAT не наблюдается, намерения не реализуются, дела откладываются. До новых инициатив СЕРТ нам вообще как до Кассиопеи.

О федеральных целях и их воплощениях

Особые надежды на развитие VSAT в России с 2001 г. возлагаются на программы работ в рамках федеральных целевых программ. Особо выделим ФЦП «Развитие единой образовательной информационной среды (2001–2005 гг.)» (утверждена в сентябре 2001 г.). В 2002 г. В.И. Матвиенко, тогда вице-премьер, доложила о завершении компьютеризации сельских школ, но, как справедливо отметил президент, школьникам нужен и удаленный доступ к общим информационным ресурсам. Для решения проблемы предлагались разные технологические подходы, в том числе VSAT. Победителем открытого конкурса на создание телеком-

муникационной системы удаленного доступа школ к информационным образовательным ресурсам в рамках федеральной программы было объявлено НПО «Кросна». И с середины 2002 г. работа «закипела». Согласно программе, в 2005 г. все сельские школы должны были получить доступ в Интернет. Но итогом благих намерений стал отчет Счетной палаты РФ, в котором констатировалось, что выявлены нарушения конкурсных условий при выборе поставщика, а государственные контракты заключены и исполнены с нарушениями действующего законодательства. Вместо ввода в эксплуатацию 13 745 абонентских приемных VSAT-станций, фактически было установлено 7 648, т.е. половина сельских школ так и остались ни с чем. Заметим, что по этому проекту было зафиксировано «неэффективное использование бюджетных средств» и их перерасход «на 73,6%, по сравнению с первоначальной стоимостью проекта (340 млн руб.) без учета расходов по установке, вводу и дальнейшей эксплуатации неустановленного оборудования» (см. решение Коллегии Счетной палаты РФ от 4 июня 2004 г. № 19 (389), <http://procurement.e-management.ru/state-sp5.htm>).

Итак, налицо печальный пример развития технологической VSAT в рамках социально значимых федеральных программ. А сегодня развернуты работы по новым программам, в том числе по ФЦП «Развитие единого образовательного информационного пространства». В ее рамках на развитие единого образовательного информационного пространства и совершенствование управления в системе образования предполагается выделить в 2006–2010 гг. более 3 млрд руб., а оснастить доступом в Интернет планируется 53 тыс. школ.

Во всем мире решение таких задач связывают с VSAT. В национальном проекте «Образование» для них место тоже есть: «за два года школы, не имеющие доступа к Интернету, получат качественное подключение к Глобальной сети», – декларирует государство (таких школ до 30 марта 2007 г., по данным Федерального агентства по образованию, должно быть около 22 тыс.).

На 2006 г. по всем ФЦП запланированы затраты более 363 млрд руб. (www.programs.gov.ru). Любая из этих программ подразумевает развитие телекоммуникационной инфраструктуры, а на обширных территориях без VSAT не обойтись. Причем не только в России. Так, Министерство образования Мексики планирует в 2006 г. установить VSAT в 40% школ, а Hughes Networks Systems в начале 2006 г. подписала контракт с бразильским оператором Copel Telecom на подключение к Интернету 800 государственных школ штата Парана с помощью VSAT-терминалов (остальные 1300 школ получают доступ через наземные коммуникации). Мировая практика показывает, что именно масштабные проекты национального уровня пробивали брешь в стройных рядах чиновников, стоящих на страже устаревших нормативных догм. Один раз у нас это не сработало. Получится ли на новом образовательном витке, покажет ближайшее будущее.

И.И. СИДОРОВ

Радиомодули слежения и навигации

В декабре 2006 г. Siemens планирует вывести на рынок два новых модуля для использования в приложениях слежения и навигации – XT75 и XT65, оснащенных GPS-приемниками. Эти 4-диапазонные устройства со встроенной поддержкой Java можно использовать во всех глобальных мобильных сетях GSM.

Радиомодули предназначены для применения в навигации, управления парком транспортных средств, экстренных вызовов, определения местоположения (можно устанавливать точное местонахождение людей, автомобилей, товаров при их транспортировке или конечных устройств). Информация может передаваться также по мобильной сети.

Определение местоположения объекта с помощью спутника выполняется по 16 параллельным каналам с использованием данных системы A-GPS. Интегрированный протокол связи TCP/IP (TCP/IP stack) преобразует данные в пакеты и передает их

по технологии EDGE (XT75) или GPRS (XT75 и XT65) в мобильную сеть. Оба модуля могут обмениваться данными на частотах 850, 900, 1800 и 1900 МГц. Скорость передачи XT75 почти втрое превышает скорость сети ISDN.

Используются энергосберегающие режимы, предусмотренные GSM и GPS. Встроенный драйвер RIL обеспечивает простое подключение к оконечным устройствам, где установлена операционная система Microsoft Windows Mobile.

Благодаря поддержке Java обоими модулями разработчики могут программировать разнообразные приложения. Встроенные процессор и блок памяти снижают общую стоимость разрабатываемых продуктов и гарантируют их быстрый вывод на рынок. Все стандартные датчики и узлы могут соединяться как по цифровым, так и по аналоговым интерфейсам.

Siemens: (495) 737-1000

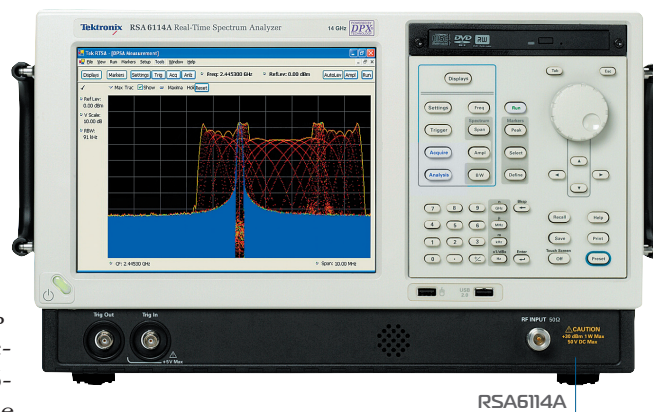
Анализатор спектра реального времени

Tektronix выпустила анализаторы спектра с оптимальным сочетанием ширины полосы анализа и динамического диапазона. Приборы этой серии – RSA6106A (до 6,2 ГГц) и RSA6114A (до 14 ГГц) обеспечивают ширину полосы анализа в реальном времени 110 МГц и динамический диапазон без паразитных составляющих 73 дБ, делая возможной разработку РЧ-систем с широкой полосой захвата.

С помощью технологии DPX можно получать изображение спектра в реальном времени путем обработки более 48 тыс. измерений в секунду. Сведение к минимуму пробелов в информации о сигнале значительно повысило оперативность отображения РЧ-сигнала при 100%-ном перехвате сигналов длительностью до 24 мкс.

Интерфейс анализатора имеет настройки по умолчанию для каждо-

го измерения, в результате прибор можно оптимизировать для выполнения первичных измерений. Применяемая синхронизация по частотной маске (FMT) позволяет запускать из-



мерения при появлении в спектре уникального набора событий. Приборы RSA6100A способны быстро обнаружить и произвести анализ трудноуловимых сигналов и событий радиочастотного спектра в присутствии других РЧ-сигналов.

Tektronix: (495) 748-4900

SkyMAN NG –

концепция BWA
нового поколения

InfiNet Wireless предложила новую концепцию построения систем широкополосного беспроводного доступа – SkyMAN NG, в которой осуществлен переход от отдельных базовых станций BWA к сети базовых станций различных сетей доступа, объединенных подсистемой InfiMetro.

В сети SkyMAN NG обеспечивается сквозной QoS, единая система AAA и прозрачное управление из единого центра. Все оборудование – на универсальной аппаратной платформе, что обеспечивает защиту инвестиций (возможность развития исключительно программными средствами).

Возможности SkyMAN NG: уникальное сочетание в рамках одной системы беспроводной опорной сети многослойной MESH-топологии и сетей доступа; сквозной показатель QoS на опорной сети и сетях доступа; простота интеграции с проводными сетями MPLS и интеграция в операторские сети с полной поддержкой сервисов, систем управления и биллинга; работа вне прямой видимости за счет топологии MESH, OFDM и MIMO. Кроме того, высокое качество передачи голоса в сети доступа WiMAX при минимальном использовании ресурсов сети за счет использования режима TDM.

**InfiNet Wireless:
(495) 784-7312**

Инфракрасная IP-камера

НОЧНОГО ВИДЕНИЯ

Компактная и мощная интернет-камера ICA-106 от Planet оборудована инфракрасной подсветкой, которая позволяет видеть в полной темноте и вести видеонаблюдение круглые сутки. С помощью



удобного настенного комплекта крепления ICA-106 устанавливается в любое положение и под любым углом.

Датчик изображения CMOS, поддержка режимов MPEG4 и MJPEG создают аудио- и видеосигналы высокого качества. Одновременно можно управлять 4 камерами и выполнять регистрацию, контролируя выполнение задачи через сеть.

IP-камера ICA-106 может транслировать «живое» видео и звук через Интернет, имеет функцию автоматической отправки кадров изображения по электронной почте при фиксации движения.

Planet:
(495) 190-1202

Устройство управления трафиком

NetEnforcer AC 2500 от Allot Communications (поставщик РГРКОМ) представляет собой устройство управления трафиком с пропускной способностью 5 Гбит/с. Использование технологии DPI (Deep Packet Inspection) позволяет производить мониторинг и контроль сетевого трафика и работы клиентов.

Находясь в сети между маршрутизатором и коммутатором, устройство пропускает через себя весь трафик (чем облегчает работу центрального сервера), выполняет мониторинг и управление трафиком. NetEnforcer AC 2500 определяет аномальный трафик, а также атаки на сеть, мгновенно изолирует их без разрыва канала.

Характеристики оборудования: порты – 1000BaseT; пропускная способность – от



310 Мбит/с до 2,5 Гбит/с; обслуживаются 2–4 линии, до 80 тыс. виртуальных каналов и до 500 тыс. одновременных соединений; устанавливаются 40 тыс. политик обслуживания.

NetEnforcer AC 2500 позволяет настроить приложения в соответствии с индивидуальными требованиями, что повышает производительность, качество контроля и приоритизации пользователей сети, способствует вводу новых тарифных планов и т.д.

РГРКОМ: (495) 775-2424

Программно-аппаратный комплекс

удаленного мониторинга

Комплекс удаленного мониторинга параметров энергообеспечения объектов связи и телекоммуникаций от «Интеграл-Электро» предназначен для сбора данных о состоянии объектов, а также для отображения параметров в режиме реального времени для предупреждения и оперативного устранения аварийных ситуаций. Система позволяет отслеживать работу выпрямительных установок, ИБП и аккумуляторных батарей, дизель-генераторных систем, коммутационных шкафов, электросетей и подстанций и др.

Комплекс реализован на базе промышленных контроллеров ABB и ПО Citech SCADA, может использоваться для подключения любого типа энергооборудования, масштабируется, позволяет вести архив, имеет дружелюбный пользовательский интерфейс. Мониторинг параметров можно производить при нормальном или аварийном функционировании подконтрольных объектов, обмениваться данными с различными спецустройствами. В электронном журнале событий фиксируются контролируемые параметры и управляющие действия диспетчера.

«Интеграл-Электро»: (495) 980-7205

VoIP-шлюзы NSGate-3900



Оборудование NSGate-3900 – это многопортовые VoIP-шлюзы с поддержкой протоколов SIP и H.323 (на выбор, без обновления ПО). Модульная структура позволяет создавать различные комбинации аналоговых портов с возможностью замены модулей: 8FXS, 6FXS+2FXO, 4FXS+4FXO, 8FXO.

Шлюзы можно использовать при любом типе подключения к Интернету, для внутренней сети обеспечиваются

функции NAT, виртуального сервера и сервера DHCP.

Поддерживаются режимы работы как с регистрацией на сервере (гейткипер H.323 или прокси-сервер SIP), так и «точка-точка», в том числе с поддержкой прозрачного выноса абонентских линий. Шлюзы могут работать как гейткиперы или прокси-серверы для 200 конечных устройств при замене ПО с обеспечением функций клиента Syslog (CDR) и аутентификации пользователей.

Есть возможность сохранения и восстановления конфигурационного файла, обновления ПО шлюзов по протоколу FTP.

NSGate: (495) 363-6317

Решение для тестирования PCI Express 2.0

Agilent Technologies представила законченное решение для анализа протоколов и тестирования PCI Express 2.0 от x1 до x16. Достигается скорость 5 Гбит/с, что отвечает потребностям современного рынка, обусловленным большими объемами графической и другой информации, которую требуется передавать по этому протоколу. Прибор E2960B состоит из анализатора и тестера, поддерживающих как PCIe 1.0, так и PCIe 2.0. Решение дополняется многочисленными вариантами применения зондов и шлюзом Agilent P2L для перехода от протокола к логике.

Возможности анализатора:

- тестирование от x1 до x16 для PCIe 1.0 и PCIe 2.0 с помощью пробников midbus серии 2.0 с использованием технологии Softtouch, что позволяет добиться емкостной нагрузки менее 0,15 пФ и чувствительности 60 мВ;

- широкий набор функций, включая расширенную настройку запуска;

- удобное представление данных с помощью настраивающихся колонок;

- сочетание в одном приборе логического анализатора и анализатора протоколов позволяет понимать механизмы прохождения данных, начиная с физичес-

кого уровня и заканчивая уровнем транзакций.

Тестирующее устройство способно подавать сигнал-стимул на устройства PCIe 2.0 и отслеживать их реакцию.

Agilent Technologies:
(495) 797-3900

3G-телефон V710

Huawei Technologies выпустила модель сотового телефона третьего поколения V710 под брендом Vodafone. Huawei в партнерстве с Vodafone разработала спецификации, конфигурацию и внешний дизайн модели, спроектированной с учетом потребительских запросов.

Двухдиапазонная модель V710 представляет собой телефон-раскладушку массой 99 г, который работает в сетях стандартов WCDMA/GPRS/GSM. С помощью V710 можно быстро получить доступ к услугам сетей сотовой связи третьего поколения: Vodafone Radio DJ, мобильному ТВ, музыкальным файлам, видеотелефонии и Vodafone live! Кроме того, в телефон встроены музыкальный MP3-плеер, камера на 1,3 мегапикселя и Bluetooth.

Huawei Technologies: (495) 956-8689




broadband
RUSSIA & CIS SUMMIT
2006

21 - 22 Ноября

Россия, Москва, Марриотт Грандь Отель

www.broadband-conference.com

- ИКТ ШИРОКОПОЛОСНЫЕ СЕТИ СВЯЗИ
- БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ
- СПУТНИКОВАЯ И МОБИЛЬНАЯ СВЯЗЬ
- 3G ТЕХНОЛОГИИ
- КАБЕЛЬНЫЕ ТЕХНОЛОГИИ
- СИСТЕМЫ ТЕЛЕ-РАДИО-ВЕЩАНИЯ



ITE LLC Moscow
Виктория Шлепикова
Тел.: (495) 935 7350
Факс: (495) 935 7351
E-mail: shlepikova@ite-expo.ru

Table of contents

News
Editor's Column 3
Topical Commentary
 The Government Invites Business to New Economy 6
Profiles 8
Person of the Issue
 Hyperborean Georgy PACHIKOV 9
Companies
 Company News 14
Events
 Ye. VOLYNKINA. Russian CIO Summit: Information Technologies and IT Directors are Changing Business 20
 A. KRYLOVA MVNO: Will it be Possible to Use New Opportunities for Business? 24
 L. PAVLOVA. From the Life of the Fourth Dimension. Vatoutinky Get-Togethers-2006 27
 V.I. DROZHGINOV. Strictly Confidential: the Strategy of Russia's Electronic Industry Development 29
 A. KRYLOVA. Time for Wideband Solutions 32
 Ye. VOLYNKINA. IBM Lotus is Heading for Hanover 34
 A. KRYLOVA. An Alloy of Oriental Wisdom and Western Pragmatism 35
Subject of Federation
 K. ANKYLOV. Novosibirsk: Telecommunication Wealth of Siberia 37
Calendar of Events 38
New Products 93

Cover Story
Russia's Transport Corridors
One IT Season Ticket is Required 40
Market in Transition
 Russia-Transit: How to Become Real? ... 41
 A.S. MISHARIN. IT Integration as the Light at the End of the Tunnel. Or at the Beginning? ... 45
 K. KONDRASHOV. Customs in the Epicenter of Information Exchange ... 47
IT Engine
 B.L. KOUNIN. IT Across Barriers in Railroad Tracks 49
 Logic Behind National Logistics: Railroad Men are in the Vanguard 52
 A. BOGATOV. Lawyers are Rooting Out Stumps 53
On the Other Side of Transport: Comments Made by Non-Strangers 54
 Not on the Subject
 S.V. PCHYELIN. Dangerous Rivers of Russia 56

Focus
GPS, GLONASS, Galileo – Three Space Beacons Not to Lose the Way
 Sky Triumvirate in Close-up 58
 Services with Different Subordination 59
 Orbital Group 60
 Accuracy is the Politeness of Navigation 62
 Space Triangle: Integration

is Profitable! 64
 Navigation Receivers 65
 News from the Earth 60

Aspect
ISO 9000 as a Mirror of Russian Management 68
 Quality to Communications, or Six Questions About Quality Management Systems (QMSs) 70
 Close-up of QMSs 72

Business Services
 IP Telephony Aiming at Triple Play. Location – Zelenograd. Interview with S. ALYMBEKOV 74
 S. DANFORD. Mobile Driving Force Behind Trade 76
Management
 O.I. SKOKOV, B.A. LYEVIN. How to Speed Up the Introduction of New Services, or Product Lifecycle Management 78
Horizons
 M. RAMNY, K. TRAN. The Future Will Come Tomorrow, or A Hard Road to 4G 81
Lines of Defense
 A.Yu. SCHEGLOV, K. A. SCHEGLOV. Access Control Instead of Antivirus 84
 A. RAZOUMOV. Mobile Risks Can be Reduced 88
Problem
 I.I. SIDOROV. VSAT: Red-Letter Days of the Calendar. History in Orders and Programs 90

Указатель фирм

«ИКС-Консалтинг» 37
 «Авантел» 37
 «Авиалрибор» 66
 «Айти» 21
 ЗАО «Алкатель» 32
 ЗАО «АМТ» 18
 «Арктел» 18
 Ассоциация 3G 24, 26
 Ассоциация документальной электросвязи 27
 Ассоциация связистов речного транспорта РФ 8, 57
 Ассоциация-800 25
 «Аэрофлот» 55
 «Бий Ай Телеком» 78
 «Би-Эй-Си» 12
 «Борлас» 16
 «БЭТО-Нашеи» 36
 «ВИМ-Авиа» 55
 ВНИИМАШ 69, 71
 ВНИИС 69
 «Вокорд Телеком» 18
 «Волга-Днепр» 55
 «Волготелеком» 18
 «Волгатранстелеком» 8
 «ВымпелКом» 14, 17, 77
 «Голден Лайн» 12
 «Голден Телеком» 12, 13, 16
 «Гудвин-Европа» 17
 ЕБРР 16
 «Евросеть» 25, 26
 ОАО «ИАС» 74
 Ижевский радиозавод 66, 67
 «Интеграл-Электро» 94
 «Интернет Сибири» 37
 ЦССК
 «Интерком» 69, 71, 72
 «ИНФИН» 18
 НПП «Информационные технологии в бизнесе» 84
 «ИскраУралТЕЛ» 70-73
 «Комкор» 13, 15, 18, 74
 «Комкор-ТВ» 75
 «Компания ТрансТелеКом» 8, 14, 18, 36, 42-51
 «Компас» 66
 «Комстар-ОТС» 12
 «Корпорация ЮНИ» 18
 ФГУП «Космическая связь» 91
 «Космос-ТВ» 16
 «Котлини» 66, 67
 «Крафтсвязь-Новосибирск» 37
 КРОК 14, 70-72
 «Кросна» 27, 92
 «Магистраль Телеком» 37
 «Мастертел» 18
 МГТС 75
 «МегаФон» 37
 «МегаФон-Москва» 17
 «МегаФон-Сибирь» 14
 «Микрогест» 18
 ММТ 66
 МТТ 74
 МТУСИ 27
 «НАВИС» 66, 67
 «Народный мобильный телефон» 24, 26
 «Наунет СП» 28
 ИК «Некстер» 53
 «Новая телефонная компания» 17
 «Новотелеком» 37
 «Норильск-Телеком» 27
 НПО «Оборонительные системы» 67
 «Объединенные кабельные системы» 16
 НПО ПМ им. М.Ф. Решетнева 61
 РБК Daily 44
 РГРКОМ 94
 «Ринет» 37
 РИО-Центр 6
 «РИСС-Телеком» 37
 РНИИ КП 67
 «Российская венчурная компания» 7
 ОАО «Российские железные дороги» 40-42, 44, 51, 53-55
 Российский институт радионавигации и времени 67
 «Ростелеком» 14, 36
 «РТК-Лизинг» 12
 РТКОММ 12, 70-72
 «Русский регистр» 69
 «Северо-Западный Телеком» 17
 «Сеть цифровых каналов» 12
 «Сибирьтелеком» 12, 18, 37
 «Синкс-Телеком» 74, 75
 «Синтерра» 12
 «Система Масс-Медиа» 16
 АФК «Система» 16
 «Ситроникс» 30
 «Скай Линкс» 37
 «Старт Телеком» 15
 ЗАО «Стрим-ТВ» 16
 «Термотек» 66
 «Т-Платформы» 16
 «Трансойл» 55
 «Трафикаланд» 17
 «Форт-Росс» 20
 «Центр связи, информатики и радионавигации» 8
 «ЦентрТелеком» 15, 36
 «Центр-ТрансТелеКом» 8
 «Цифровое телерадиовещание» 16
 «Энфорте» 37
 «Эриксон» 14
 ЮТК 32
 «Яндекс» 6, 28
 «З» 76
 3S Navigation 67
 ABI 58
 Netgear 18
 NEUF 36
 Nokia 14
 Technologies 81, 83, 95
 Alcatel 12, 14, 32
 Alcatel Space 65
 Allot Communications 94
 Anritsu 17
 Apple 76
 Ashtech 67
 AT&T 32
 Avaya 12, 14
 BMW 76
 Boeing 60, 65
 British Telecom 35
 BSI MS CIS 70
 Budweither 76
 Canon 76
 Carphone Warehouse 26
 C-DOT 32
 Celltick 76, 77
 Check Point Software Technologies 18, 88, 89
 China Mobile 35
 China Telecom 35
 Cisco Systems 6, 15, 16
 Comptek 38
 Comptel 18
 Comverse 18
 Copel Telecom 92
 CTI 38
 Debitel 26
 Dell 12
 Dialogic Corporation 16
 Disney 25
 Disney Mobile 25
 DocsVision 16
 Draka Comtek 17
 Easy Mobile 26
 Eicon Networks 16
 Eventica 6
 FhG 35
 Ford 78
 Fujitsu Siemens Computers 17
 Galileo Industries 59
 Galileo Joint Undertaking 59
 Galileo Sistemas y Servicios 59
 Gartner Group 88
 Gate5 14
 GMCS 12
 Google 76
 GPS Laboratory 60
 H.A.B.I.T. Research Ltd. 62
 Hay Group 35
 Hewlett-Packard 12, 17
 Huawei Technologies 17, 35, 36, 95
 Huber+Suhner 17
 Hughes Networks Systems 92
 Hutchison 76
 IBM 13, 34, 35
 Infineon Technologies 83
 Infinet Wireless 93
 Inline Technologies 26
 Intel 13, 16, 32
 ITPA 22
 JPS 67
 Juniper 15
 Klamobil 26
 Leicka 67
 LETA IT-company 12
 Lindex Technologies 17
 Lucent Technologies 16, 26
 Maravedis 32
 MasterCard 76
 Mercury 17
 Microsoft 13, 34, 56, 93
 Mobilcom 26
 Mobile ESPN 25
 Mobitel 14
 Motorola 13
 Naumen 54
 Netgear 18
 NEUF 36
 Nokia 14
 Nortel 13, 15, 75
 NovAtel 62
 NTC Gate 94
 NSI Com 18
 Oracle 16
 Orange 76
 ParallelGraphics 9, 10
 Peregrine Systems 17
 Planet 94
 Plus Communications 12
 Puma 76
 PwC 35
 RAD Data Communications 15
 Samsung 32
 SAP 55, 56
 SIA PMT 26
 Siemens 14, 93
 Softline Consulting Services 55
 Sokkia 67
 Spectra Precision 67
 SSTL 60
 STMicroelectronics 83
 Swisscom 32
 Syrus Systems 17
 Tektronix 93
 Telstra 80
 T-Mobile International 26
 Topcon Positioning Systems 64
 Trend Micro 89
 Trimble Navigation 14
 Trustgenix 17
 Vodafone 35, 76, 95
 Yandex 76
 Yankee Group 88

Реклама в номере

MASTERHOST
 Тел. (495) 772-9720
 E-mail: info@masterhost.ru
<http://masterhost.ru> c. 21

AGAT-PT
 Тел./факс (495) 799-9069
 E-mail: info@agatrt.ru
www.agatrt.ru c. 48, 50

AMT-ГРУП
 Тел. (495) 725-7660
 Факс (495) 725-7663
 E-mail: info@amt.ru
www.amt.ru c. 19

ВЕКТОР
 Тел. (343) 375-4360
 Факс (343) 349-5066
 E-mail: market@vektor.ru
www.vektor.ru c. 22

ДИАЛОГ-СЕТИ
 Тел. (495) 917-7955
 Факс (495) 917-7069
www.dialogseti.ru c. 27

ЗЕЛАКС
 Тел./факс (495) 748-7178
 E-mail: direct@zelax.ru
www.zelax.ru c. 16

ИМАГ
 Тел. (495) 362-7705
 Факс (495) 362-7773
 E-mail: info@emag.ru
www.emag.ru c. 13

КЛАССИКА
 Тел./факс (495) 956-3437
 E-mail: sale@classics.ru
www.classics.ru c. 91

КОМКОР
 Тел. (495) 250-7454
 Факс (495) 250-7455
 E-mail: info@mtk.comcor.ru
www.comcor.ru c. 2

КРОНИКС
 E-mail: info@cronyx.ru
www.cronyx.ru c. 12

ЛАБОРАТОРИЯ КАСПЕРСКОГО
 Тел./факс (495) 797-8700
 E-mail: sales@kaspersky.com
www.kaspersky.ru c. 23

МТА
 Тел. (812) 331-1555
 Факс (812) 331-1550
 E-mail: m-200@m-200.com
www.m-200.com c. 14

НЕВА КАБЕЛЬ
 Тел. (812) 558-6781
 Факс (812) 592-7779
 E-mail: sales@nevacables.spb.ru
www.nevacables.ru c. 26

РГРКОМ
 Тел./факс (495) 775-2424
 E-mail: info@rgrcm.ru
www.rgrcom.ru c. 25

РОССИЙСКАЯ ТЕЛЕКОМУНИКАЦИОННАЯ СЕТЬ
 Тел. (495) 781-3344
 Факс (495) 781-3311
 E-mail: rtn@rosnet.ru
www.rosnet.ru c. 33

РОСТЕЛЕКОМ
 Тел. (495) 972-8283
 Факс (495) 787-2850
 E-mail: info@rostelecom.ru
www.rt.ru c. 1

СВЯЗЬИНВЕСТ
 Тел. (495) 248-3187
www.svzayinvest.ru 2-я обл.

КОМПАНИЯ ТРАНСТЕЛЕКОМ
 Тел. (495) 784-6670
 Факс (495) 784-6671
 E-mail: info@transstk.ru
www.transstk.ru 1-я обл., 4, 40, 42-57

ШТИЛЬ ГК
 Тел./факс (4872) 24-1362
 E-mail: company@shtyl.ru
www.shtyl.ru c. 29

COMPTЕК
 Тел. (495) 785-2525
 Факс (495) 785-2526
 E-mail: sales@comptek.ru
www.comptek.ru c. 15

ELTEL NETWORKS
 Тел. (495) 974-8237, 974-8238, (812) 334-4300
www.eltelnetworks.ru c. 69, 71

IBM
 Тел. (495) 258-6348
 Факс (495) 258-6363
www.ibm.com/ru c. 11

INCORE
 Тел. (495) 982-3886
 Факс (495) 982-3887
 E-mail: start@incore.ru
www.incore.ru c. 77

NETVILLE
 Тел. (495) 232-2636
 Факс (495) 961-1278
<http://netville.ru> c. 31

NEXTER
 Тел. (495) 411-6424
 Факс (495) 411-6415
 E-mail: nexter@nexter.ru
www.nexter.ru c. 73

POWER-ONE РОССИЯ
 Тел. (495) 245-5774
 Факс (495) 245-9590
 E-mail: sales.russia@power-one.com
www.power-one.com c. 24

RADIUS GROUP
 Тел./факс (495) 641-0410
 E-mail: info@radius-group.ru
www.radius-group.ru c. 17

SYRUS SYSTEMS
 Тел./факс (495) 937-5959
 E-mail: sale@syrus.ru
www.syrus.ru 4-я обл.

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
 127091, Москва, ул. Делегатская, д. 5а;
 тел. (495) 337-0222.

ЗАО «ИКС-холдинг»:
 127254, Москва,
 ул. Добролюбова, д. 3/5;
 тел. (495) 204-4888, 502-5080.

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