# Multiplayer, *или* Правила игры


**Triple play, quadruple play, multiplay... Играть в эти «игры» надо по правилам. Правило первое: источник коммерческого благополучия оператора связи – конечный пользователь. Правило второе: только наращиванием пропускной способности сети и обеспечением ее мультисервисности сражение за абонента не выиграешь – нужны услуги, нацеленные именно на этого абонента. Тогда и схема распределения доходов оператора и провайдера могла бы измениться...**
**Но как создать такую «сервисную сеть»? С кем взаимодействовать? Правильные (в интересах конечного пользователя) ответы на эти вопросы сулят коммерческую выгоду и участникам рынка.**

**С. БЕЛОВА,**
генеральный директор компании Netville

## Клиент – залог благополучия оператора

Сегодня упоминания о triple play и даже quadruple play стали привычными, хотя данное явление, скорее, стоило бы называть multiplay. Без обсуждения темы мультисервисности сети не обходится ни одно профессиональное комьюнити. Обобщим мнения участников рынка:

- Операторская сеть должна обеспечивать доставку нескольких типов услуг (голос, видео, данные), на деле же «долженствование» сводится к оценке пропускной способности интерфейсов транспортного оборудования и обеспечению QoS.
- Интерпретация VPN, IP MPLS, CoS, QoS, RTP и других ставших привычными аббревиатур затруднений не вызывает. Торжествуют IP и вера представителей отраслевого бизнеса и технического сообщества в то, что операторская сеть должна быть универсальной и мультисервисной. Иногда, правда, спорят о том, что лучше: L2 или L3 – и как «правильно» построить сеть. В основном эти дебаты возникают на почве соперничества производителей оборудования. Реже вспоминают про NGN, и то применительно только к голосовым услугам.
- Много внимания уделяется IPTV. Ведутся резонные рассуждения о том, что рыночное требование предоставить именно эту услугу является решающим при формировании основных параметров сетевой архитектуры, полосы пропускания и качества обслуживания.
- Ключевым положением в контексте обсуждения мультисервисности оказывается пакетное предложение услуг: «три в одной» розетке или в одном абонентском устройстве доступа.
- Иногда встречаются обсуждения тех или иных технологий передачи данных на проводных сетях (ADSL, DOCSIS, Metro Ethernet).

Все эти положения важны и полезны, но только при условии, что есть точное понимание предмета потребительского интереса конечного пользователя – источника коммерческого благополучия любого оператора связи.

Еще не так давно господствовала уверенность в том, что услуга доступа в Интернет обеспечивает оператору традиционной (кабельной телевизионной, публичной телефонной, беспроводной...) сети необходимое конкурентное преимущество. Но довольно быстро стало ясно, что это преимущество легко достижимо всеми участниками рынка, и конкуренция на рынке доступа набрала новые обороты. Этим операторское сообщество в значительной степени обязано конечному пользователю, вернее, стремительному развитию его опыта, а значит – запросов.

## Новый вызов

Сегодняшний рынок услуг широкополосного доступа (ШПД) прирастает десятками процентов и в некоторых географических зонах, точнее в деловых центрах, приближается к насыщению. Конкуренция на рынке услуг доступа очень напоминает ту, которая была на рынке услуг мобильной связи, когда в борьбе за абонента операторы пришли к таким низким тарифам на услугу традиционной голосовой связи, что она стала массовой. Мы, безусловно, шагаем в ногу с мировым рын-

ком услуг мобильной связи, и в этом немалая заслуга МТС, сделавшей ставку на GSM.

Что касается рынка проводного широкополосного доступа, то в этом сегменте наши операторы отстали от мирового сообщества, хотя и ненамного. МГТС с ее СПДОП по праву может считаться пионером движения за широкополосный Интернет. Установлены сотни тысяч портов ADSL, построены сотни тысяч абонентских окончаний Ethernet и DOCSIS, набирают силу операторы беспроводных сетей. Океан сражений за абонента на рынке ШПД в Интернет наполнился кровью, крупные операторы поглощают мелких, провайдеры идут на любые ухищрения, чтобы предоставить абоненту контент для обеспечения пресловутого конкурентного преимущества.

Многие обладатели развитых распределительных сетей ШПД, завершив бурную деятельность по созданию сетевой инфраструктуры, остановились в раздумье – какими услугами наполнять сети. Государственные органы взялись за регулирование рынка, который раньше не хотели замечать. В процессе бурного обсуждения темы «смены парадигмы» звучит масса доводов в пользу того, что она (парадигма отрасли) действительно изменилась, только теперь надо определить новые правила жизни и выбрать такой способ взаимодействия с окружающим миром, который обеспечил бы процветание...

Утверждение о главенствующей роли ТВ-сервисов абсолютно справедливо в одном отношении: именно этот сервис наиболее требователен к полосе пропускания, задержкам, джиттеру, а значит, устанавливает самую высокую планку технических требований к качеству сетевой инфраструктуры. Однако нет каких-либо доказательств, что одно только его наличие определяет предпочтения абонента при выборе того или иного провайдера услуг. Опыт мирового телекома демонстрирует привычные потребительские предпочтения: возможности выбора и гибкого формирования собственного пакета услуг в сочетании с простотой получения и использования, качеством абонентского обслуживания и доставки услуг являются определяю-

**Сегодня оператор доступа теряет доходность – владелец портала повышает стоимость своего ресурса**

щими факторами конкуренции на рынке услуг, доставляемых по сетям связи.

Следует отметить, что для каждого персонального профайла конечного пользователя степень «важности» одной и той же услуги различна в зависимости от индивидуальных предпочтений. Последнее обстоятельство может оказать влияние на то, в каких случаях пользователю приходит сигнал «Абонент занят» или отказ в получении услуги, что, в свою очередь, должно находить адекватное отражение в формальном SLA оператора.

## Операторы не успевают за запросами абонентов

Почти все аналитики в мире сходятся в том, что основными параметрами конкуренции на рынке широкополосного доступа являются доступность мультимедийных приложений и полоса пропускания для их доставки абоненту. Так что только наращиванием пропускной способности сети и обеспечением ее мультисервисности сражения за абонента не выиграть – нужны еще и услуги, которыми эта полоса может быть наполнена, а их доставка требует определенных гарантий качества в зависимости от типа услуги.

Наличие собственного пакета услуг – определяющий фактор конкурентоспособности сетевого оператора

Необходимость обеспечения целевых значений для множества параметров сети предъявляет естественные требования одновременно к нескольким участникам рынка широкополосного доступа, и управление этими параметрами становится для сетевого оператора основной заботой. Целевая функция оператора сети доступа – управление полосой по требованию клиента; кроме того, он должен обеспечить широкий набор услуг и качественное абонентское обслуживание. Запросы конечных пользователей растут гораздо быстрее, чем операторы доступа могут обеспечить эти параметры предоставления услуг. Затрачивая основные усилия на техническую составляющую сети – инфраструктуру, инженерные компании расходуют весь свой ресурс на строительство сети и ее перманентную модернизацию – свободных средств и времени на создание сервисной базы у них не остается.

Отдельные операторы сознательно пренебрегают сервисной составляющей бизнеса, провозглашая расширение зоны сетевого охвата стратегической целью, другие делают ставку на «главную услугу», например доставку ТВ-контента в его традиционном формате, хотя и по нетрадиционным для доставки ТВ-сигнала распределительным сетям. Этим и пользуются известные порталы, зарабатывая рекламные деньги на базе зарегистрированных пользователей и анонимных посетителей. В этом же, кстати, заложено определенное противоречие, которое рано или поздно должно привести интернет-рынок к изменению модели бизнеса. А именно, оператор доступа теряет доходность на линию абонентского доступа, в то время как владелец портала повышает стоимость своего ресурса за счет роста числа посетителей и стоимости рекламных площадей, не возмещая оператору стоимость доступа. Схема распределения доходов могла бы измениться, если бы сетевой оператор уделял больше внимания созданию и развитию или адаптации собственного каталога управляемых услуг внутри собственной сети.

## Нужна кооперация

Альтернативой созданию собственных информационных ресурсов для удовлетворения развлекательных и познавательных аппетитов клиента может служить партнерство оператора сети с другими операторами (сетей, насыщенных сервисами) или со специализированными операторами, способными предложить готовый каталог. Этот последний вариант кооперации участников рынка, к слову, избавляет сетевого оператора от возможных рисков вложений в создание собственных сервисов, но позволяет повысить доходность абонентских линий. Опыт мобильных операторов, успешно сотрудничающих с так называемыми контент-агрегаторами по схеме разделения доходов, подтверждает справедливость и эффективность такой модели бизнеса.

Кто бы ни стал партнером сетевого оператора: другой сетевой оператор или агрегатор контента, обеспечивающий доступ к уникальному контенту на базе операторской сети доступа, в точках присоединения партнеров (interconnect'a) должны выполняться определенные условия (бизнес- и технологические), гарантирующие конечному пользователю комфортное получение услуг на соответствующей скорости, сквозную авторизацию и подключение услуг. Для выполнения этих условий сетевому оператору уже недостаточно обеспечить присоединение к своей сети – нужна уверенность в том, что в точке присоединения полоса будет выделена ровно с тем номиналом, который допустим для получения конкретной услуги, а система контрактных отношений учитывает дифференцирование услуг и выполнение SLA. Правильно (в интересах конечного пользовате-

**ЛИДЕРЫ ГОВОРЯТ...**

ля) выстроенная система отношений операторов/агрегаторов предъявляет определенные технологические требования к оборудованию маршрутизации в точках сопряжения и изменяет «размерность» бизнес-взаимодействия участников interconnect'a.

Единственного рецепта построения «правильной» сети, увы, не существует, однако движение в направлении создания сети с полным набором управляемых услуг позволяет оператору рассчитывать на высокое ARPU в сочетании с высоким показателем RGU (Revenue-Generating Unit – индикатор потенциала коммерческого роста компании, число доходных сервисов на одного абонента). Последний показатель – один из ключевых при оценке инвестиционной привлекательности компании-оператора.

## Производители оборудования раньше других чувствуют ветер перемен

Первыми заметили изменение запросов конечных пользователей и заявили о новых подходах к построению сетей широкополосного доступа следующего поколения Cisco, Juniper, Alcatel, употребив при этом блистательное маркетинговое определение – «сервисный маршрутизатор». Такие устройства, отвечающие системным требованиям, и предлагают сегодня самые активные участники рынка – производители сетевого оборудования операторского класса. Базовая концепция сервисной маршрутизации строится на предоставлении полосы по запросу, где параметры запроса (полосы и качества обслуживания) определяются типом услуги, затребованной конечным пользователем. Связанные в транспортную сеть доставки сервисов («сервисную сеть»), такие устройства обеспечивают гарантированную транспортировку услуг от источника к конечному потребителю с заданными параметрами качества и безопасности, обеспечивают соблюдение SLA во всех точках сопряжения сетей. Гибкость и совершенство подобного оборудования зависит в первую очередь от того, насколько универсальной в отношении вновь создаваемых сервисов явится архитектура сети, построенной на сервисных маршрутизаторах.

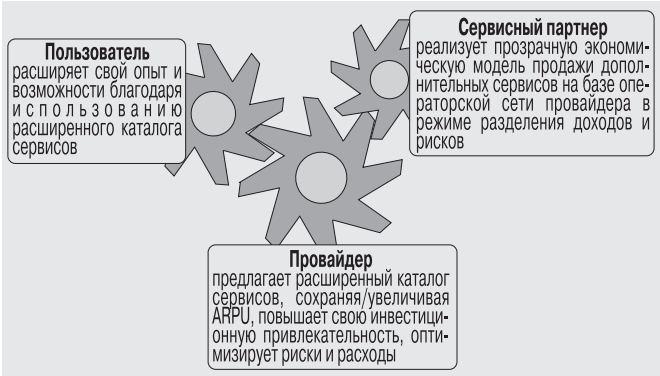
**Океан сражений за абонента на рынке доступа в Интернет наполнился кровью**

Что касается архитектуры «сервисной сети», то, формируясь как упорядоченное множество сервисных платформ, соединенных в наложенную сеть, она оказывает естественное влияние на инфраструктуру опорных сетей и сетей доступа. Бурный рост peer-to-peer-трафика в сетях широкополосного доступа заставляет операторов задумываться об управлении услугами и их централизации. Пренебрежение к peer-to-peer в отсутствие средств контроля может привести к невозможности планирования нагрузки на сеть и потере доходности из-за оттока клиентов. Несмотря на смену парадигмы в части стихийной децентрализации сервисов и развития абонентских информационных ресурсов (self generated content) на базе мощных абонентских компьютеров, оператор сети доступа вынужден создавать точки концентрации (тяготения) сервисов, чтобы не лишиться своей основной «операторской» (управляющей) функции, дающей ему права поставщика услуг. Весь опыт телекома убедительно свидетельствует об экономической эффективности централизованной архитектуры, обеспечивающей высокий уровень управляемости сети в противоположность архитектуре распределенной. Поощрение развития клиентского контента на базе абонентских подключений, игнорирование централизации источников услуг на основе создания собственных платформ или кооперации с другими операторами и агрегаторами сервисов ведут к снижению доходности и увеличению затрат на обслуживание и развитие сети.

## От «сервисной сети» к бизнес-взаимодействию

В связи с определением нового формата сетевого взаимодействия на технологическом уровне («сервисной сети») уместно рассмотреть возможности бизнес-взаимодействия, обеспечивающие коммерческую результативность этой новой сети. Такие схемы окончательно еще не определены, но многие операторы начали задумываться об изменении «размерности» бизнес-взаимодействия. Основные положения новой модели во многом определяются целями участников взаимодействия и их числом. В отличие от прежней (плоской) модели с одним сервисом, например «Интернет», которая обслуживала только двух участников – **п**ользователя и **п**ровайдера услуг, новая модель предполагает наличие дополнительных участников – сервисных **п**артнеров (кооператоров), обеспечивающих необходимое разнообразие услуг для пользователя на ресурсной базе провайдера. В новой модели **все** участники (**п–п–п**) взаимодействуют по схеме «победитель–победитель» (рисунок).

Все multiplayer'ы взаимодействуют по схеме "победитель—победитель"




Основные цели формирования новой модели взаимодействия связаны со следующими положениями:

- **Важнейшее:** каждый провайдер предлагает такой пакет услуг, который представляется ему целесообразным с учетом знания предпочтений клиентской базы, по своей собственной цене. Конкурентоспособность провайдера определяется местным рынком.
- Провайдер получает возможность защитить свои инвестиции в сетевую инфраструктуру, оптимизировать расходы и риски, связанные с созданием новых сервисов, на основе их разделения с партнером.
- Отношения участников схемы не зависят от технологических особенностей сетевой инфраструктуры.
- Каталог сервисов может быть сформирован из собственных сервисных ресурсов провайдера и партнеров.
- Для установления отношений провайдеру необходимо лишь анонсировать свои предпочтения во внешних связях с партнерами, которые он намерен поддерживать.

Новая система отношений ни в коей мере не является альтернативой свободному интернет-сообществу. Она лишь расширяет и дополняет ее в интересах конкретных участников рынка, увидевших свою коммерческую и техническую выгоду в формировании и поддержке централизованных каталогов сервисов, предоставление которых ограничено конкретной сетью абонентского доступа провайдера услуг связи. ИКС

# Что такое Externet VPN

**Сервисы, как известно, бывают разные – для массового пользователя, для операторов и для компаний. Externet VPN – это сервис для компаний с несколькими офисами. С его помощью абонент может напрямую, без участия секретарей позвонить по короткому номеру сотруднику другого офиса, расположенного даже в другом городе. Externet VPN работает со всеми типами офисных АТС, включая аналоговые. Эта технология запатентована и, по прогнозам экспертов, может быть скопирована не ранее 2007 г.**

**Е. САПОВА,**
руководитель службы технической поддержки оператора глобальной голосовой сети Externet

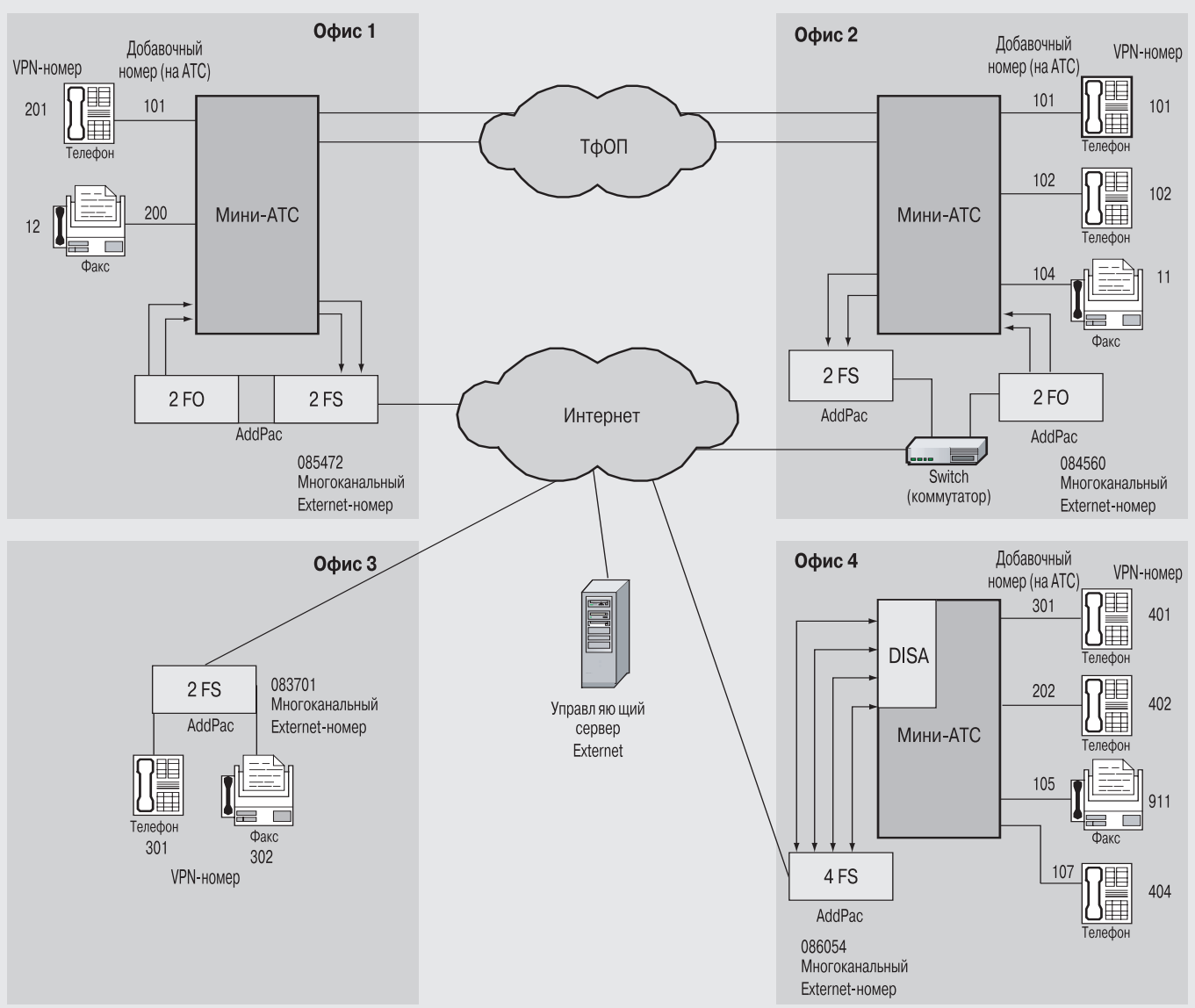
## Ноу-хау

Хорошо налаженное горизонтальное взаимодействие сотрудников разных офисов – важное условие четкого функционирования организации. От удобства и стоимости коммуникаций во многом зависит эффективность бизнес-процессов. Повысить эффективность взаимодействия сотрудников позволяет организация быстрого прямого дозвона, требующая единого плана нумерации, создать который можно как на цифровых, так и на IP-АТС. Цифровые АТС стоят, как правило, в головных организациях, а филиалы пользуются аналоговыми.

Сравнительно недавно появились офисные АТС с функцией IP, но в России они не получили широкого распространения. Нередко операторы даже не знают, как подключить абонента через IP. Для введения единого плана нумерации им нужно либо поставить IP-плату расширения, либо поменять АТС, но это дорого, да и нецелесообразно.

Гораздо проще создать единый план нумерации на офисных цифровых, аналоговых и IP-АТС путем подключения к глобальной голосовой сети Externet. Благодаря технологии Externet VPN объединять планы нумерации можно без замены существующих АТС. При этом желательно, чтобы внутренние номера сотрудников всех офисов не повторялись. Избежать повторов позволит виртуальный план нумерации, который может совпадать с внутренним планом номеров.

Реализация сервиса Externet VPN с единым корпоративным частным планом нумерации на примере объединения четырех офисов




Задача быстрой доставки прямых звонков от сотрудников из разных офисов без участия секретаря решается следующим образом. По виртуальному номеру поступает вызов, система принимает его и автоматически осуществляет донабор номера вызываемого абонента. Сигнал доставляется из офиса в офис напрямую по сети передачи данных. Степень конфиденциальности такой связи довольно высокая: голос не проходит через телефонную сеть общего пользования, а значит, прослушать разговоры намного сложнее. А если настроить зашифрованную передачу данных по VPN, то прослушивание таких переговоров становится вообще невозможным.



## Как работает

Работу сервиса Externet VPN с единым корпоративным частным планом нумерации рассмотрим на примере объединения четырех офисов (рисунок).

Допустим, абонент из офиса 1 (VPN номер 201) хочет поговорить с коллегой из офиса 2 (VPN номер 101). Со своего телефонного аппарата он набирает код выхода офисной АТС (например, 9) на услугу Externet. АТС в офисе 1 соединяет его с FS-портом Externet-шлюза, находящегося в этом же офисе. Услышав в трубке длинный гудок (ответ голосового шлюза), вызывающий набирает Externet VPN-номер 101 вызываемого абонента и нажимает на кнопку #. Эта информация посредством служебных сигналов поступает на управляющий сервер Externet, который проверяет,

разрешен ли данный звонок абоненту или нет. И в соответствии с ранее составленным списком Externet VPN-абонентов (см. таблицу) определяет, что при наборе номера 101 звонок следует направить на номер Externet 084560 в офис 2, а при поступлении сигнала на порт 084560 шлюза FO этого офиса – в тоновом режиме набрать добавочный номер вызываемого абонента (тоже 101) на АТС офиса 2.

Сервер проксирует соединение между шлюзом в офисе 1 и шлюзом в офисе 2. Шлюз FO офиса 2 выполняет донабор номера вызываемого абонента АТС этого же офиса. В свою очередь АТС, получив номер, соединяет с вызываемым Externet VPN-абонентом. Телефон с Externet VPN-номером 101 начинает звонить. Соединение между Externet VPN-номерами в разных офисах состоялось.

С помощью удобного и простого веб-интерфейса системный администратор компании может самостоятельно и оперативно изменять контакты и номера сервиса Externet VPN для всех пользователей, в каком бы офисе они ни находились.

## Варианты подключения

Итак, чтобы внедрить в компании услугу Externet VPN и организовать единый корпоративный план нумерации для разных офисов, нужно подключиться к глобальной голосовой сети Externet.

Для подключения к сервису Externet VPN через внутренние офисные АТС в каждом филиале необходимо иметь (или установить) либо оборудование FS/FO (см. рисунок, офис 1), либо два комплекта оборудования: 1) FS, подключаемое к внешним соединительным линиям офисной АТС, служит для организации исходящей связи из офиса); 2) FO, подключаемое к внутренним линиям офисной АТС, используется для согласования добавочных номеров офисной АТС и Externet VPN-нумерации, а также для организации входящей связи в офис (см. рисунок, офис 2).

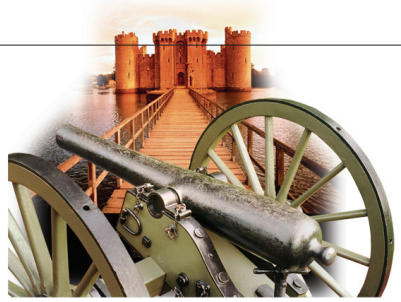
Единый список номеров Externet-абонентов

| Желаемый VPN-номер | Externet-номер | Внутренний номер АТС (Externet-номер) | Имя абонента, должность |
|---|---|---|---|
| 101 | 084560 | 101 | Иванов А.А., директор, Москва |
| 102 | 084560 | 102 | Петров С.В., менеджер, Новосибирск |
| 103 | 084570 | 103 | Смирнов В.Ю., исполн. директор, Новосибирск |
| 104 | 084570 | 123 | Бухгалтерия |
| 105 | 084580 | 220 | Тех. поддержка |

При наличии DISA-платы на офисной АТС используется FS-шлюз (см. рисунок, офис 4). Если подключение к Externet осуществляется через FS напрямую (минуя офисную АТС), то внедрение Externet VPN в таком офисе позволяет обойтись без замены оборудования (см. рисунок, офис 3).

Externet VPN – дополнительная услуга абонентов Externet. Все, что нужно для ее внедрения, это сформировать единый список номеров сотрудников и разослать его представительствам компании.

После активации сервиса Externet VPN сотрудникам компании для звонков из одного офиса в другой достаточно просто набрать на своем телефоне 3-, 4- или 5-значный короткий Externet VPN-номер нужного сотрудника. ИКС



# Модель угроз системы сигнализации SS7

**Технический прогресс, принесший многие связные «изыски» и сервисы, сделал операторские сети весьма уязвимыми для информационных атак, в том числе и со стороны SS7 (см. «ИКС» № 7'2005, с. 79–82). К сожалению, строгой методики противодействия угрозам системе SS7 (ОКС № 7) сегодня не существует. Поэтому важно знать, какие угрозы наиболее опасны для сети оператора и, в частности, для системы сигнализации, а также представлять, какие элементы сети наиболее им подвержены.**

**Д.В. КОСТРОВ,**
начальник отдела информационной безопасности ОАО «Межрегиональный ТранзитТелеком»

## Конкретика общих понятий

Угрозы готовности и целостности телекоммуникационной сети зависят от ее типа. Понятно, что угрозы, присущие учрежденческим, сотовым и мобильным сетям, и угрозы для сетей фиксированной телефонной связи общего пользования могут существенно различаться. Однако есть опасности, общие для всех сетей, включая системы SS7.

Наиболее критичные угрозы SS7 связаны:

- с потерей целостности сигнальных данных и ресурсов;
- с подменой («маскарадом») сигнальных сообщений или отдельных параметров и несанкционированным доступом;
- с подслушиванием и раскрытием сенситивной или важной для сети и бизнеса информации.

**Модель угроз**, как известно, содержит описание каждой угрозы, определение (по возможности) ее типа и описание последствий в случае реализации, а также перечень подверженных ей типов информации. Для SS7 – это параметры сигнальных сообщений или эксплуатационные параметры, хранящиеся в базе данных пункта сигнализации, статистическая и учетная информация и др. Кроме того, данные сигнализации могут включать конфиденциальную адресную информацию, а в некоторых случаях и криптографические ключи.

Другое общее понятие – **точка атаки**, определяющая функциональный компонент, откуда может быть произведена атака (например, эталонная точка в функциональной архитектуре или физическая точка атаки). И, наконец, **нарушитель** – злоумышленник, реализующий угрозу во внутренней или внешней сети.

## Потеря целостности и нарушение данных сигнализации

**Целостность данных** сигнализации означает, что никакая часть сигнальной единицы или данные, относящиеся к обработке сигнализации и хранящиеся в памяти узла коммутации, не были изменены непредусмотренным образом. В ряде случаев такие нарушения выявляются системой обработки и устраняются путем повторных передач.

**Предмет угрозы.** Подвержены ей главным образом данные, входящие в структуру сигнальных единиц и сигнальных сообщений протоколов сигнализации. Однако защиты отдельных сигнальных единиц и сообщений явно недостаточно – для управления соединением необходим лишь полный набор сигнальных операций.

Нарушить целостность может и дублирование или изменение порядка следования

### Общие угрозы для сетей

✓ Неавторизованное использование, неправильное применение информации, ресурсов, доступ к ресурсам без разрешения:
  – модификация данных или потеря их целостности, в том числе удаление или изменение информации;
  – добавление неверной информации.
✓ Задержка передаваемой информации и ответов на запросы.
✓ Изменение направления передачи информации.
✓ Отказ в обслуживании.

### Способы реализации угроз

✓ искусственное создание перегрузки сетевых элементов или систем;
✓ модификация данных в пользовательской части базы данных станции;
✓ нелегальный анализ трафика (тип, объем, время, источник и назначение) для раскрытия информации;
✓ конфликты взаимодействия.

сигнальных сообщений, а также задержка любого подтверждения, ведущая к нарушению процесса управления коммутацией.

В системе SS7 изначально заложены некоторые механизмы защиты от ошибок, достаточные для обеспечения не очень высокого уровня безопасности. Но они не способны обнаружить намеренную модификацию параметров сигнальных сообщений, а тем более – предотвратить ее. Для предотвращения атак, связанных с несанкционированной модификацией сигнальных единиц, следует применять методы фильтрации, основанные на статистическом анализе сообщений каждой конкретной сети. Такие средства защиты, как управление доступом или обеспечение конфиденциальности, не принесут желаемого результата, поскольку эта угроза может исходить и от авторизованных партнеров.

Заметим, что реализация подобных угроз на сети SS7 довольно сложна и требует значительных вычислительных и экономических ресурсов, поскольку эта сеть по своей природе закрыта для доступа извне. Однако при появлении точек взаимодействия на сетях SS7 и IP вероятность таких угроз резко возрастает.

**Последствия** же реализации подобных угроз для оператора сети могут быть самыми неожиданными и зависят от характера модификации того или иного параметра. Риск от случайных угроз, как правило, невелик и связан с возможной повторной передачей сигнального сообщения и привлечением дополнительных ресурсов на обработку. Вероятность серьезного ущерба при этом крайне мала. Если цель такой угрозы – получить свободный доступ к услуге или сети, появляется риск потерять часть дохода (хотя и небольшую). Наиболее часто подвергаемые модификации сигнальные единицы – MSU (например, изменение данных ISUP или MAP) и FISU (обеспечение отсутствия положительного подтверждения на определенную сигнальную единицу MSU).

Наибольшую опасность представляет угроза, цель которой – нарушение функционирования всей сети SS7. В этом случае ущерб оператора может «исчисляться» не только в больших суммах, но и в утрате доверия к нему со стороны клиентов. Подобные угрозы реализуются путем модификации сигнальных сообщений, отвечающих за управление сетью SS7 на уровнях MTP или SCCP.

**Точка атаки и нарушитель.** Атаки с нарушением данных сигнализации возможны как со стороны взаимодействующих операторов и поставщиков контента, так и со стороны внутренних врагов. Теоретически такие угрозы способны осуществить все категории злоумышленников.

## «Маскарад» и неавторизованный доступ

Для получения доступа к сети сигнализации или к какой-либо ее процедуре из другой сети-партнера последняя должна «идентифицировать» себя, а механизм сетевой защиты первой – произвести ее аутентификацию (проверку прав доступа). Идентификация и аутентификация выполняются на разных этапах процесса установления соединения или разъединения, при передаче сигнальных сообщений к различным узлам сигнализации в сети и др.

При отсутствии аутентификации или подмене идентификаторов злоумышленник может попытаться замаскироваться под авторизованного пользователя (атака типа «маскарад») и осуществить несанкционированный доступ (НСД) к сети. Правда, не всякий допущенный к ресурсам пользователь получает право неограниченного их использования. Авторизация четко определяет тип разрешенного к использованию ресурса и перечень допустимых операций.

**Предмет угрозы.** Поскольку сеть SS7 обеспечивает передачу сигнальных единиц и содержащихся в них сигнальных сообщений, то практически любое их искажение может в той или иной степени нарушить процесс предоставления услуг связи. Однако основную угрозу представляют изменения в сообщениях управления сетью сигнализации – MTP3 и SCCP. Хотя модификация сообщения управления соединением путем маскирования кода OPC в этикетке маршрутизации тоже малоприятна: недобросовестный оператор получает возможность передавать свой трафик под видом чужого.

Еще одна серьезная опасность – неавторизованный доступ пользователей к данным, содержащим установочные эксплуатационные параметры системы SS7 в пунктах сигнализации, особенно если атака осуществляется через систему управления сетью. Подмена полей OPC, DPC и SLS в этикетке маршрутизации обычно имеет целью несанкционированное использование оборудования сети SS7 или получение несанкционированного доступа к сенситивной сигнальной информации. В первом случае это грозит операто-

**Заложенные в системе SS7 механизмы защиты от ошибок не способны обнаружить намеренную модификацию параметров сигнальных сообщений**

ру потерей доходов и возникновением перегрузок на сети SS7 вследствие «лишних» объемов сигнального трафика, во втором – может нарушить конфиденциальность либо целостность информации.

Атака на систему управления сетью способна изменить состояние звена (пучка звеньев) сигнализации между двумя смежными пунктами как на сети SS7 основного оператора, так и на участках взаимодействия с другими сетями. Для противодействия такой атаке в системе управления должны быть предусмотрены следующие процедуры: активация и деактивация звена (пучка звеньев) сигнализации; запрещение ввода звена сигнализации с целью сделать его недоступным (и поддерживать в этом состоянии) для сигнального трафика, генерируемого подсистемами пользователей (сохраняя при этом возможность передачи сообщений тестирования и техобслуживания). Несанкционированный доступ к этим процедурам чреват потерей некоторых сообщений, что может нанести немалый экономический ущерб.

**Предотвратить угрозы** этого типа помогут аутентификация и управление доступом (разграничение прав доступа), причем последнее должно начать «работать» сразу же после выполнения успешной аутентификации. Меры противодействия: установка системы мониторинга SS7 и системы FMS; разработка процедур отслеживания нелегитимного трафика и нештатных ситуаций; установка межсетевых экранов при подключении к внешним сетям (входящий и исходящий трафик); полисинг; организация пунктов сигнализации с функцией переприема SCCP (SPR), обеспечивающих трансляцию (пересчет) глобальных заголовков в подсистеме SCCP для исключения нелегитимного трафика.

**Точка атаки и нарушитель.** Точкой атаки может стать любой пограничный пункт сигнализации в сети входящего оператора или поставщика услуг (контента), а в роли злоумышленника выступить собственный персонал. Нечаянное или умышленное воздействие возможно на любом узле коммутации.

При появлении точек взаимодействия на сетях SS7 и IP вероятность угроз резко возрастает

## Раскрытие конфиденциальных данных

Конфиденциальность данных SS7 означает, что они не должны быть использованы (ни в процессе передачи, ни при хранении) никакими иными способами, кроме предусмотренных протоколами и операциями SS7. Однако в реальной жизни возможен НСД к передаваемым в сигнальных сообщениях или хранимым данным, причем обнаружить подобный инцидент чаще всего не удается.

**Предмет угрозы:** параметры сигнальных сообщений, содержащие информацию об абонентах или операторе. К конфиденциальным данным абонентов относятся, в частности, номер вызывающего абонента в сообщениях IAM и ACM подсистемы ISUP, данные о регистрации местоположения абонента или короткие сообщения в протоколе MAP. Аналогичные операторские данные – информация об управлении конфигурацией сети. Конфиденциальными можно считать и данные мониторинга сети сигнализации как содержащие информацию о структуре, качестве и особенностях работы сети.

Кроме информации, содержащейся в сигнальных сообщениях, к сенситивным данным относятся таблицы маршрутизации, хранимые в памяти узлов коммутации, коды взаимодействующих пунктов сигнализации и т.п.

**Точка атаки и нарушитель.** Эти угрозы могут исходить только от внутреннего злоумышленника, имеющего доступ к терминалам систем техобслуживания и мониторингу сети сигнализации. Но иногда перехват сигнальных сообщений осуществляется подключением к линейному оборудованию сети. Обычно подобные нарушения организуют конкуренты оператора с целью подрыва доверия к его деятельности либо кто-то заинтересованный в дискредитации влиятельного (известного) лица. Как правило, такой организатор не стеснен в средствах и может завербовать сотрудника, имеющего авторизацию на доступ к соответствующей информации.

Между тем даже случайно раскрытая информация может привести к нежелательным последствиям, особенно если она получит широкое распространение, да еще со ссылкой на источник утечки.

## Использование альтернативных каналов для передачи управляющей информации

В случае передачи сигнальной информации SS7 по сети IP вероятность реализации описанных выше угроз резко возрастает.

Доступ к закрытой сети SS7, как правило, имеет только обслуживающий персонал оператора. Вероятность альтернативного доступа крайне мала, поскольку он трудно реализуем с технической точки зрения. Этот факт подтверждается и статистичес-

кими данными, согласно которым бóльшая часть угроз для сети SS7 исходит от обслуживающего ее персонала.

Однако при появлении сигнальных маршрутов, использующих в качестве транспорта сеть IP, картина резко меняется: наряду с традиционными для сети SS7 угрозами возникают новые опасности, ранее характерные для таких сетей, как, например, Интернет (атаки хакеров, вирусы и т.д.). В результате процентное соотношение внутренних (со стороны обслуживающего персонала оператора) и внешних угроз начинает выравниваться, что приводит к изменению политики безопасности оператора в отношении сети SS7.

В традиционной закрытой сети SS7 политика безопасности оператора строилась в основном на предотвращении возможных внутренних угроз (случайных или умышленных). Ставка делалась на использование различных паролей, прав доступа, инструктаж обслуживающего персонала и т.д., а фактическая безопасность передаваемой и хранящейся информации SS7 не удостаивалась столь пристального внимания.

Однако с появлением точек взаимодействия сетей SS7 и открытых сетей на основе IP теоретически становится возможным проникновение пользователей сети IP в сеть SS7. Этот аспект безопасности еще нуждается в изучении, поскольку данных по нему пока нет. Многообразие применяемых в IP-сети протоколов и использование общих транспортных ресурсов делает этот вопрос намного сложнее, нежели безопасность SS7 в традиционных телефонных сетях.

При передаче сигнальной информации SS7 через сеть IP безопасность обеспечивается традиционными для IP-сети средствами, такими как использование технологий VPN, семейства протоколов IPsec, межсетевых экранов и т.д.

## Наиболее чувствительные точки

Из всех каналов связи, по которым осуществляется обмен между оборудованием связи одного или разных операторов, сигнальные каналы наиболее чувствительны к нарушениям ИБ. Фактически последствия атак на каналы, передающие пользовательский трафик, не оказывают конкретного влияния на целостность и устойчивость функционирования всей сети. В то же время элементы сигнализации, и особенно SS7, являются главными точками доступа для нарушителя (вольного или невольного), способного негативно повлиять на работу сети или причинить оператору серьезный ущерб.

При определении угроз безопасности должен быть исследован как интерфейс между узлами, принадлежащими различным сетям сигнализации, так и интерфейс между узлами одной и той же сигнальной сети.

Сигнальный интерфейс между двумя узлами или оборудованием одной сети характеризуется тем, что доступ к нему весьма затруднен для нарушителя, не относящегося к персоналу данной сети. Для нападения извне требуется высокий уровень технической подготовки и зачастую специальное оборудование. Однако для сотрудников данной сети эта задача достаточно проста.

Основная точка доступа – терминал техобслуживания, позволяющий осуществлять все виды угроз. Другая точка в сети оператора – система мониторинга. Используется также доступ с подключением к физическим цепям передачи сигналов, хотя он требует специального оборудования, возможности скрытного его подключения и более высокой подготовки нарушителя.

Сигнальный интерфейс между узлами или оборудованием, принадлежащим сетям разных операторов, является одновременно и интерфейсом между двумя различными сетями. Этот интерфейс очень важен для сети сигнализации транзитной сети крупного оператора, поскольку последняя имеет большое количество взаимодействующих оконечных сетей. Каждый взаимодействующий оператор связи имеет свою бизнес-политику и политику безопасности. Именно через этот интерфейс может быть произведена атака из сети другого оператора или от оборудования поставщика контента (с открытого доступа). В ближайшем будущем число таких интерфейсов, по-видимому, будет расти. Вместе с тем анализ возможных угроз со стороны многочисленных партнеров по предоставлению услуг связи – весьма сложная и затратная задача.

Отсюда следует, что основное внимание необходимо уделить контролю сигнальной информации на пограничных узлах коммутации и в точках доступа поставщиков контента, особенно если последние взаимодействуют с транзитной сетью по открытым IP-протоколам. В собственной сети должно быть обеспечено строгое управление правами доступа с ведением журнала (истории) доступа, а также активный контроль лояльности персонала. ИКС

**Бóльшая часть угроз для сети SS7 исходит от обслуживающего персонала**

# На гребне встречного интереса

**Компания HP, «российская история» которой насчитывает более тридцати лет, уделяет повышенное внимание рынку телекоммуникаций: одни из первых решений операторского класса от HP были внедрены на сетях МТС и ОАО «Электросвязь» Тамбовской области (ныне Тамбовский филиал ОАО «ЦентрТелеком») более четырех лет назад (см. «ИКС» № 6'2004, с. 72). Сегодня телекоммуникационные решения составляют около 30% бизнеса «HP Россия», объем этого рынка за три года вырос по меньшей мере втрое. Очевидно, такая динамика возможна лишь при условии взаимной заинтересованности операторов и вендора.**

**С.Е. РАЗМАХАЕВ,**
директор по продажам Департамента телекоммуникаций «HP Россия»

## Путь к сердцу оператора лежал через... «предбиллинг»

«Хитом» 2005–2006 гг. в операторской среде стало решение класса Mediation – система сбора данных об использовании ресурсов сети HP IUM. После внедрения системы в Тамбовском филиале ОАО «ЦентрТелеком» ее заметили и другие компании «Связьинвеста». Сегодня интерес к HP IUM со стороны МРК материализуется в виде пилотных проектов либо подготовки к внедрению. Для чего операторам электросвязи нужна такая система?

Традиционные операторы оказывают услуги не только фиксированной телефонии, но и мобильной связи, доступа в Интернет. Поэтому нужна некая универсальная сетевая «прослойка», которая могла бы считывать с коммутационных систем разные виды информации, преобразовывать их в единый формат (при необходимости объединять все записи, относящиеся к одному абоненту) и затем передавать в «верхние» бизнес-системы – биллинга (у одного оператора может быть и несколько биллингов), маркетинга, управления службой эксплуатации, CRM. Причем система должна выдавать эту информацию в том формате, который воспринимают «вышестоящие» системы.

HP IUM позволяет операторам проводить глубокий анализ потребляемого заказчиками трафика: выявлять предпочтения в услугах разных групп пользователей, наиболее часто используемые каналы, время и направления прохождения звонков и т.д. Для оператора это хороший инструментарий при оценке эффективности бизнеса и его развития – можно разрабатывать гибкие тарифные планы и быстро внедрять новые сервисы, поскольку система позволяет оценивать технические возможности создания разного рода тарифных планов и алгоритмы обработки информации, поступающей из сети.

Внедрение систем Mediation в МРК хорошо вписывается в программу холдинга по преобразованию биллинговой системы. Каких-то два-три года назад слово «Mediation» мало что говорило операторам, понятнее был термин «предбиллинг». Поэтому мы предлагали тогда оператору «систему предбиллинга», а затем уж разъясняли все ее широкие возможности.

По сути, это аналитическая система, работающая с массивом данных. Сегодня, по нашим оценкам, 80% операторов, принимая решение о внедрении Mediation, выбирают HP IUM, которая окупается в среднем за полгода.

## От отдельных решений – к комплексу OSS/BSS

Вслед за Mediation на сетях некоторых российских операторов фиксированной и мобильной связи «поселились» системы автоматизации процессов технической поддержки и управления ИТ-услугами (HelpDesk). Такие проекты реализованы в ОАО «ВолгаТелеком» и ЗАО «Нижегородская сотовая связь». А в нынешнем году HP выиграла тендер на внедрение системы борьбы с мошенничеством в сетях связи (Fraud Management System), проведенный одним из крупнейших российских операторов. Сейчас завершается первая фаза реализации проекта, и по всем признакам это решение в ближайшей перспективе будет так же широко востребовано операторами, как и HP IUM.

Обе системы – часть концепции HP ISM (Integrated Service Management – интегрированное управление услугами), которая представляет собой комплекс проектно-методологических разработок, ПО и вычислительной техники для создания системы поддержки операционной деятельности и бизнеса оператора.

Первой российской операторской компанией, реализовавшей комплексный OSS-проект, была МТС (2005 г.). Про-

ект был ориентирован на мониторинг и улучшение качества предоставления услуг, автоматизацию процессов обнаружения и устранения сбоев на уровне сети, мониторинг ИТ-составляющей инфраструктуры. Выбор оператора обусловлен тем, что HP предлагает OSS-системы, разработанные в соответствии с открытыми рекомендациями TeleManagement Forum (NGOSS, eTOM, SID), обладающие открытыми интерфейсами и развитыми средствами управления, высокой надежностью, мультиплатформенностью. Кроме того, все эти системы представлены в московском Центре высоких технологий HP, где их можно протестировать. Немаловажно и то, что HP не ставит перед собой задачу просто продать продукт, главная цель – предоставить оператору реальный инструментарий для повышения эффективности бизнеса.

## Новые тенденции и реалии рынка

Сегодня HP активно работает на российском медиарынке, причем среди заказчиков – не только телеканалы (НТВ, ТВЦ, РТР), но и операторы, внедряющие медиауслуги. Так, «МТУ-Интел» реализует проект VoD с использованием серверного оборудования HP для подачи контента и платформу Digital Media, автоматизирующую процессы поиска, создания и предоставления контента. Летом этого года глобальная компания HP приняла решение о переименовании Департамента телекоммуникаций в Департамент телекоммуникаций и медиа. Значит, наравне с телекоммуникационным рынком компания направит усилия и на работу с контентом – будут и системы хранения, ориентированные на поиски больших объемов данных, и системы подачи видеоконтента, и услуги по сдаче в аренду распределенных вычислительных ресурсов (что сегодня популярно на Западе).

Мы ищем возможности для развития этого направления. Полагаем, что изменение названия департамента вполне отражает новый долгосрочный тренд – сближение телекоммуникационных и медийных технологий. Сегодня, когда на передний план выходит содержание услуги, требуется не просто доступ к ней (хотя далеко не везде и этот вопрос решен), – будущее за теми, кто сможет оперативно предоставлять абоненту интересующую его информацию. ИКС

Новый долгосрочный тренд рынка – сближение телекоммуникационных и медийных технологий

Мистер Зеленый человечек

# «Опс!», *или* Телеком глазами пришельца

**Каким бы увидели инопланетяне, оказавшиеся на третьей планете от Солнца, наше телекоммуникационное пространство и его внутреннее устройство? Хотите узнать?**
**В редакцию случайно попали записки Зеленого человечка, расшифровав которые, мы дружно воскликнули: «Ну и народец, эти опсы! Что за нравы, что за божества!».**
**А может, во Вселенной есть-таки вечные ценности и неча на зеркало пенять?..**

Операторы связи, или опсы, – загадочные существа, обычаи и поведенческие реакции которых до сих пор мало изучены. Известно лишь, что большинство из них поклоняются верховному божеству под названием УЕ, хотя есть и такие, кто боготворит идола, обозначаемого магическим символом $. Некоторые исследователи склонны думать, что это разные обозначения одного и того божества, просто второе является более архаичным по сравнению с первым.

Известно также, что опсы обожают кабели, кабельные соединения, стыки, патч-корды и другие подобные штучки, полагая, что по ним течет кровь божества, которому они поклоняются. Они любят кабелировать всегда и везде, и место, где не проложен их кабель, считают «нечистым», и вдвойне «нечистым», если там пролегает кабель другого опса. Друг друга опсы терпеть не могут, что, правда, не мешает им иногда стыковать свои кабели и создавать так называемые точки обмена трафиком.

Слова «трафик», «кабель», «канал связи» – для них божества более низкого уровня, чем УЕ, но без которых верховное божество существовать не может. Чем больше у опса каналов связи и чем запутаннее их система, тем более могущественным он считается. Мелкие опсы всегда горят желанием создать стык с каким-нибудь большим и могущественным собратом. Но нередко случается так, что более крупный опс съедает мелкого. Поглощение одного опса другим сами они называют слиянием, после которого съевшему опсу достаются каналы связи и клиентская база съеденного.

Клиентская база – также священное животное для опса. Каждый из них всеми правдами и неправдами стремится ее увеличить. Именно клиентская база является той самой субстанцией, откуда приносятся священные жертвы верховному божеству. Чем больше жертвоприношений, тем сильнее и могущественнее опс.

Для свершения обряда жертвоприношения опсы создают специальные ритуальные инструменты, называемые тарифными планами. Обычно эти инструменты очень сложны для восприятия и понимания. По мнению одних исследователей, запутанность тарифных планов обусловлена сакральной верой опсов в то, что эта сложность, магически воздействуя на клиентскую базу, помогает увеличить объем жертвоприношений. Другие же считают это следствием взаимодействия опса со сложной и запутанной системой кабелей и стыков, которое деформирует сознание опса, накладывая неизгладимый отпечаток на все его действия.

Для того чтобы иметь возможность осуществлять свои кабельные стыки и создавать точки обмена трафиком, опсы возводят специальные храмы, или, как называют их некоторые исследователи, телехаузы.

Особенность телехаузов – огромное количество телекоммуникационного оборудования, кабелей и кабельных стыков. Чем больше кабелей и запутаннее система кабельных соединений, тем более священным считается телехауз. К нему тянется множество внешних кабелей, так что непременным атрибутом телехауза является наличие возле него канализации. Если вы вдруг почувствовали характерный запах, знайте: скорее всего, неподалеку телехауз.

В последнее время наибольшая активность замечена у одной из разновидностей опсов, известных широкой публике под названием о́псосы (ударение на первом слоге; правда, иногда их называют опсо́сы, что похоже по сути, но неверно по форме). Эта чрезвычайно подвижная разновидность опсов проявляет поразительную активность и изощренность в манипуляциях с клиентской базой, демонстрируя завидную неутомимость в изобретении все новых и новых тарифных планов.

Таковы вкратце скудные и отрывочные сведения об опсах. Очень жаль, что удалось собрать так мало информации, тем более что их деятельность оказывает все большее влияние на нашу жизнь. Поэтому автор будет крайне благодарен всем, кто сможет предоставить хоть какие-то дополнительные сведения об этих таинственных и загадочных существах.

**Мистер Зеленый человечек**

**От «ИКС»: Зеленые человечки, адаптировавшиеся в телеком-среде (под землей ли, в эфире ли), – отзовитесь!**

От кого "ВКСС-2006"
Откуда г. Москва, "Гостиный Двор"

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

ВКСС 2006

Дирекция выставки: ООО "ПРОМЭКСПО ИТ"
107140, Москва, ул. В. Красносельская, д. 2/1, стр. 1
Телефон/факс: +7 (095) 970-18-04, 771-67-38
E-mail: info@vkss.ru www.vkss.ru

В отдел маркетинга
Рассмотреть возможность участия

**Уважаемый участник и посетитель!**

При поддержке Министерства информационных технологий и связи РФ с 21 по 24 ноября 2006 года в Комплексе "Гостиный Двор" г. Москва пройдет 9-я Международная выставка "Ведомственных и корпоративных информационных систем, сетей и средств связи" ("ВКСС-2006").

В 2006 году выставка "ВКСС" представит Вашему вниманию последние научные достижения и практические разработки в области информационных технологий и связи.

Главная задача "ВКСС-2006" - это наполнение и расширение тематической части деловой программы выставки путем проведения конференций, круглых столов, семинаров, презентаций и т.д.с участием представителей СМИ, компаний-участниц и руководителей министерств, ведомств и "силовых структур".

В рамках деловой программы выставки Вас ожидают:

- Студенческая конференция "Инфокоммуникации XXI века - будущее за тобой!"
- Семинар "Защита информационных и телекоммуникационных сетей и систем критически важных объектов"
- Круглые столы:
  - "СМИ и IT компании. Понимаем ли мы друг друга?"
  - "Внедрение волоконно-оптических технологий в технологичных сетях связи"
  - "Юридически значимый обмен электронными документами с использованием электронной цифровой подписи (ЭЦП)"
  - "Программа "Антитеррор": Защита ведомственных и корпоративных сетей и систем связи на физическом и информационном уровнях"
  - "Обеспечение надежности и безопасности при реализации комплексных проектов построения сложных промышленных систем"
  - "Энергетическая безопасность"

**Приглашаем Вас принять участие в работе выставки "ВКСС-2006"**

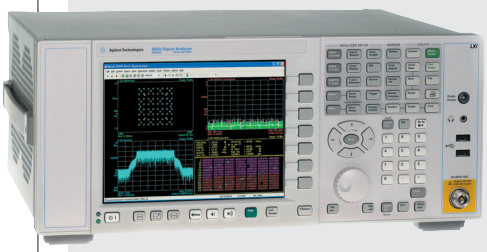
С уважением,
Дирекция выставки "ВКСС-2006"

**Бесплатный ПРИГЛАСИТЕЛЬНЫЙ БИЛЕТ на www.vkss.ru**

# Платформа Agilent MXA

## для анализа сигналов

позволяет осуществлять анализ сигналов и спектра при разработке и производстве устройств для беспроводных телекоммуникаций. Прибор поддерживает широкий спектр измерений на соответствие стандартам с использованием векторного ПО 89601A VSA.



Встроенное ПО 89601A VSA позволяет анализировать модулированные сигналы и множество форматов, включая 2G, 3G, 3,5G, WiMAX, WLAN, цифровое видео, Private Mobile Radio и др. Опционально устанавливаемое ПО обеспечивает заранее сконфигурированные стандартные процедуры измерения для тестирования 802.16e WiMAX, WCDMA, HSDPA/HSUPA и измерения фазовых шумов.

Главная особенность Agilent MXA – быстродействие, которое позволяет производить измерения со скоростью, превышающей показатели конкурентных моделей на 30–300%: скорость измерения WCDMA ACLR в быстром режиме – <14 мс; установка маркера на пик сигнала – <5 мс; скорость переключения режимов измерения – <75 мс.

Платформа MXA поддерживает диапазоны от 20 Гц до 3,6; 8,4; 13,6 и 26,5 ГГц при внутреннем усилении до 26,5 ГГц; полоса анализа – 10 или 25 МГц. При этом TOI – 15 дБм, средний уровень шумов – -151 дБм/Гц, динамический диапазон WCDMA ACLR – 72 дБ. Пользовательский интерфейс имеет шесть дисплеев трассировки, 12 маркеров, функции трассировки и автонастройки измерения. Соединение с ПК – через 100BaseT LAN, GPIB и семь портов USB 2.0.

**Agilent Technologies:**
**(495) 797-3900**

# Интерфейс для построения систем хранения данных

«Инпро Компьютерз» предлагает оборудование собственной разработки для построения систем хранения данных с использованием интерфейса SAS-Serial Attached SCSI.

Являясь преемником параллельного SCSI, новый интерфейс предоставляет ранее недоступные скорости передачи данных и возможности по коммутации устройств. Возможность объединения каналов, например четырех во внешнем кабеле, позволяет реализовать скорость 12 Гбит/с между компонентами сети. Использование коммутаторов SAS (Expander) позволяет подключать к сети до 64 тыс. устройств. Новый интерфейс программно совместим с интерфейсом SCSI. В качестве НЖМД возможно использование HDD SATA2 и SAS, а стоимость HBA и RAID-контроллеров аналогична цене на SCSI-контроллеры.

Специалистами «Инпро Компьютерз» разработана плата коммутатора (Expander) с использованием микросхем компании Vitesse. На базе этой платы представлены «SATA-SAS JBOD» и непосредственно коммутатор. JBOD является основой для построения больших систем хранения данных (СХД), SATA2-дисковым массивом с возможностью каскадирования, использующим SAS как внешний интерфейс. Коммутатор 12x3G позволяет объединять SAS-интерфейсом СХД и серверы.

Оборудование Expander и JBOD от «Инпро Компьютерз» находится в стадии тестирования. Появление в продаже коммерческих продуктов запланировано на 4-й квартал этого года.

**«Инпро Компьютерз»:**
**(495) 786-8144**

# Серия коммутаторов

## ProCurve Switch 2810

ProCurve 2810 доступны в популярных 24/48-портовых стекируемых конфигурациях и представляют собой управляемые гигабитные коммутаторы 2-го уровня, обеспечивающие высокопроизводительные и безопасные соединения. Оборудование может размещаться в небольших шкафах.

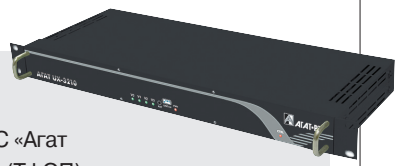
Каждый коммутатор имеет 4 порта двойного назначения для гигабитного подключения по интерфейсам 10/100/1000 Мбит/с или Mini-GBIC. Коммутаторы этой серии оптимальны для компаний, которым требуются расширенная приоритизация трафика, гибкость при идентификации пользователей, мониторинг сетевого трафика. ProCurve 2810 с легкостью обслуживает приложения, требующие широкой полосы пропускания, будь то обработка графических данных и потокового видео или масштабные операции с базами и хранилищами данных.

Заказчикам предоставляются стекируемый форм-фактор, обеспечивающий операционную гибкость для использования в небольших коммутационных шкафах; широкий набор функций 2-го уровня, включая обеспечение безопасности и конвергенции; различные способы контроля доступа в сеть. На весь срок владения продуктом предоставляется гарантия, которая предусматривает замену на следующий рабочий день (доступна в большинстве стран), бесплатную поддержку по телефону и электронной почте, а также бесплатные обновления ПО.

Ориентировочные цены для России: ProCurve 2810-24G – $2 097, ProCurve 2810-48G – $3 650.

**ProCurve Networking by HP:**
**(495) 797-3797**

## Новое ПО для IP-АТС «Агат UX»



Компания «Агат-РТ» выпустила новую версию внутреннего программного обеспечения для IP-АТС «Агат UX» 1.0.3.47, позволяющую организовывать голосовую связь как через обычные телефонные линии (ТфОП), так и через IP-сети. Функционал устройства расширен дополнительными сервисами AutomaticCallDistribution, CallRecording, VoiceNotification; добавлена поддержка цифровых системных телефонов Mitel; модифицированы функции VoiceMail и FaxMail и др.

**«Агат-РТ»: (495) 799-9069**

## Мультисервисное оборудование SI2000 MSAN

IskraTEL представила на российский рынок конструктивы SI2000 MSAN – одно- и трехслотовые шасси, которые существенно увеличивают гибкость, масштабируемость и модульность конфигурации оборудования. SI2000 MSAN эффективен не только в густонаселенном городе, но и в районах с малой плотностью населения. Систему можно выносить на площадки корпоративных клиентов в качестве оборудования пользователя.

Одновременно IskraTEL выпустила платы агрегирующих коммутаторов Gigabit Ethernet, которые расширяют возможности для построения сетей Metro Ethernet, позволяя подключить до 24 удаленных локаций на 1 плату по технологии Gigabit Ethernet. В одной версии доступны 4 электрических и 4 оптических SFP Gigabit-интерфейса, в другой – 12 электрических и 4 оптических SFP Gigabit-интерфейса. Каждая плата имеет соответственно 4 и 8 полнодуплексных Gigabit-интерфейсов для подключения к центральному коммутатору.

Компания также разработала 48-портовые платы ADSL2+ и 24-портовые платы доступа VDSL2, которые расширяют функциональность оборудования и значительно повышают плотность портов, позволяя в 20-слотовом конструктиве организовать до 912 цифровых абонентских линий. Каждая плата снабжена двумя полнодуплексными Gigabit-интерфейсами для подключения к центральному коммутатору.

Платы предназначены для предоставления полнофункциональных услуг triple play, поддерживают встроенные функции QoS, интеллектуальной многоуровневой многоадресной передачи для поддержки мультимедийных приложений, таких как IPTV и услуги обеспечения безопасности.

**«ИскраУралТЕЛ»: (343) 210-6951**

## Псевдопроводной шлюз AXN 800

Оборудование операторского класса AXN 800 от Axerra Networks (поставщик – РГРКОМ) – гибкая модульная платформа, поддерживающая все виды услуг в одной пакетной сети. С помощью AXN 800 можно прозрачно передавать любой вид сервиса по любой пакетной сети в любой среде, производить IP-агрегацию, кросс-коммутацию и IP-interworking.

Совместно с другими моделями этого семейства AXN 800 обеспечивает плавную миграцию к IP-сети с сохранением имеющихся сервисов и оборудования. ПО AxelerateOS вместе с модульной конструкцией позволяет конфигурировать любые псевдопроводные услуги в любую группу DSO.

Псевдопроводные шлюзы AXN 800 на технологии Multiservice over Packet (MSoP) полностью совместимы с другими устройствами AXN – масштабируемого семейства псевдопроводных шлюзов и устройств доступа.

Особенности AXN 800: соответствие IETF PWE3 (включая E1/T1 CESoPSN); динамическое регулирование полосы пропускания, CES, FR, HDLC и ATM; широкий спектр channelized (DSO) и unchannelized TDM-интерфейсов; полное резервирование; механизм QoS; оптимальный механизм CES, включая управление jitter.

Шлюзы совместимы с существующими CPE, коммутаторами и маршрутизаторами. Система управления AXNVision позволяет производить конфигурацию и настройку устройств и сети в режиме one click.

**РГРКОМ: (495) 775-2424**

# Аккумуляторные батареи DELTA от «Энергон-Телеком»

## АКБ DELTA серии FT

Новое поколение необслуживаемых герметизированных аккумуляторов DELTA серии FT во фронтальном исполнении разработано специально для использования с системами связи и характеризуется максимальной энергоотдачей: емкость DELTA FT – 50–155 Ач; номинальное напряжение – 12 В; тип электролита – AGM. Срок службы – 10 лет.


Особенности разработки – легкий доступ и монтаж в шкафах 19" и 23" и стойках питания. Оптимальная технология соединения элементов обеспечивает безопасность работы аккумуляторных батарей DELTA FT при возникновении высоких напряжений. Фронтальное расположение борнов создает удобства для монтажа и эксплуатации, возможны также монтаж и эксплуатация в горизонтальном положении.

Таким образом, аккумуляторные батареи DELTA серии FT отличаются надежностью и простотой в применении, обеспечивают гарантированное электропитание телекоммуникационного оборудования.



## АКБ DELTA по технологии GEL


Свинцово-кислотные гелевые аккумуляторные батареи DELTA серий GL, GS и GSC предназначены для электропитания телекоммуникационных систем. К их особенностям следует отнести тот факт, что благодаря использованию технологии с внутренней рекомбинацией газов эти АКБ не требуют обслуживания в течение всего срока службы. Кроме того, применение в качестве электролита загущенной серной кислоты (в виде геля) обеспечивает высокую цикличность пользования и устойчивость аккумуляторов к глубоким разрядам, а также более широкий диапазон температур эксплуатации. Номинальное напряжение - 12 В.

Характеристики АКБ DELTA серий GL, GS и GSC

| Марка | GL | GS | GSC |
|---|---|---|---|
| Диапазон емкостей, *Ач* | 10–200 | 32–180 | 100–3000 |
| Срок службы, *лет* | 5 | 10 | 15 |

## АКБ DELTA по технологии AGM


Свинцово-кислотные аккумуляторные батареи DELTA серий ST и STC предназначены для электропитания телекоммуникационных систем. Они изготовлены по технологии с использованием адсорбированного электролита (AGM), благодаря чему аккумуляторы DELTA ST и STC имеют низкое внутреннее сопротивление и высокую плотность энергии.

Характеристики АКБ DELTA серий ST и STC

| Марка | ST | STC |
|---|---|---|
| Номинальное напряжение, *В* | 12 | 2 |
| Диапазон емкостей, *Ач* | 33–180 | 100–3000 |
| Срок службы, *лет* | 10 | 15 |

Увеличение срока службы достигнуто за счет увеличения активной массы и использования особо чистого свинца при изготовлении пластин. Аккумуляторы DELTA серий ST и STC соответствуют требованиям EUROBAT и предназначены для работы как в буферном, так и в циклическом режимах. Возможны монтаж и эксплуатация этих аккумуляторных батарей в горизонтальном положении.

**«Энергон»: (495) 545-7738**

# Table of contents



# Список рекламодателей



# Указатель фирм




**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.