ИМПОРТОЗАМЕЩЕНИЕ

УДК 621.395.34+004.421+621.391.1

Публикуется в порядке обсуждения

РАЗРАБОТКА СИСТЕМЫ 112 В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

М. А. Шнепс-Шнеппе, главный научный сотрудник ЦНИИС, д.т.н.; sneps@mail.ru

Разработка Системы 112 является сложнейшим проектом государственного значения, который затрагивает все стороны жизни общества. Сложность проекта объясняет, почему его реализация встречает такие трудности. С целью поиска решений рассмотрен опыт США по строительству подобных систем: глобальной информационной сети оборонного ведомства GIG (Global Information Grid) и NG9-1-1 — единой сети нового поколения для обслуживания экстренных вызовов. Рассмотрены стратегии российских связистов в условиях импортозамещения: 1) переход на технологию коммутации пакетов, базируясь на импортном оборудовании или 2) развитие сетей связи собственными силами, совершенствуя систему ОКС-7 и российскую интеллектуальную сеть.

Ключевые слова: *экстренная служба 112, коммутация каналов, коммутация пакетов, SS7, SIP, интеллектуальная сеть, GIG, NG9-1-1, импортозамещение.*

Текущий момент в российской отрасли связи, имеющей важнейшее значение как для гражданских, так и для специальных нужд, характеризуется следующими факторами:

- полноценные системные исследования путей модернизации сетей связи в России не ведутся уже, как минимум, два десятка лет;
- операторы связи и поставщики услуг копируют решения, реализованные в других странах, не имея адекватной оценки их положительных и отрицательных сторон;
- приемлемость зарубежных решений для различных применений, прежде всего для сетей специального назначения, не учитывается [1].

Система 112: невыполненные планы. Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Российской Федерации предназначена для оказания экстренной помощи населению при угрозах для жизни и здоровья, для уменьшения материального ущерба при несчастных случаях, авариях, пожарах, нарушениях общественного порядка и при других происшествиях и чрезвычайных ситуациях, а также для информационного обеспечения единых дежурно-диспетчерских служб муниципальных образований.

В настоящее время выполняется Федеральная целевая программа «Создание системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на 2013–2017 гг.». Согласно ФЦП, в 2013 г. систему 112 планировалось внедрить в трех субъектах России, в 2014 г.— в шести, в 2015 г.— в двух, в 2016 г.— в пяти, а в 2017 г.— в остальных 67 регионах. Но планы не выполняются. 25 сентября 2014 г. вице-премьер правительства РФ Д. Рогозин на селекторном совещании раскритиковал ход работы по внедрению системы 112, подчеркнув, что «в настоящее время система 112 функционирует только в Татарстане и Курской области, где проживает всего 2,5% населения Российской Федерации» [2].

Создание службы 112 началось более десяти лет назад — с принятия постановления Правительства РФ № 894 от 2004 г. Процесс пробуксовывает: еще в 2011 г. на заседании правительственной комиссии по транспорту и связи вице-премьер правительства РФ С. Иванов заявил, что создание системы экстренных вызовов по единому номеру «112» в России фактически сорвано. Он напомнил, что в 2009 г. данная система должна была быть реализована в 20 регионах, а в 2010 — на территории 44 субъектов РФ. «На самом деле мы имеем единичные и пилотные проекты функционирования системы»,— констатировал С. Иванов.

В официальном отчете Минкомсвязи России [3] перечислены задачи, не решенные к настоящему времени: «Ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей связи общего пользования (ССОП) для прохождения вызовов, поступающих в службу по номеру «112». Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений». Это означает, что данный системный проект до сих пор не готов, а все проведенные работы следует рассматривать как экспериментальные образцы.

Концепция системы 112. Представление о телекоммуникационной составляющей системы 112 дает рис. 1, взятый из концепции, разработанной с участием компании «Светец» [4] (здесь УОВЭОС — узел обработки вызовов экстренных оперативных служб).

На рис. 1 приведены пять интерфейсов системы 112, которые предполагалось уточнить еще на первом этапе проекта (до 2014 г.) в соответствии с постановлением Правительства РФ от 2004 г. Это исключительно сложная работа. Кроме того, представленную концепцию системы 112, на наш взгляд, следовало бы существенно доработать. Выскажем три замечания:

- О протоколе SIP. Сомнения вызывает его включение в систему 112 наряду с ОКС-7. Для этого он еще недостаточно

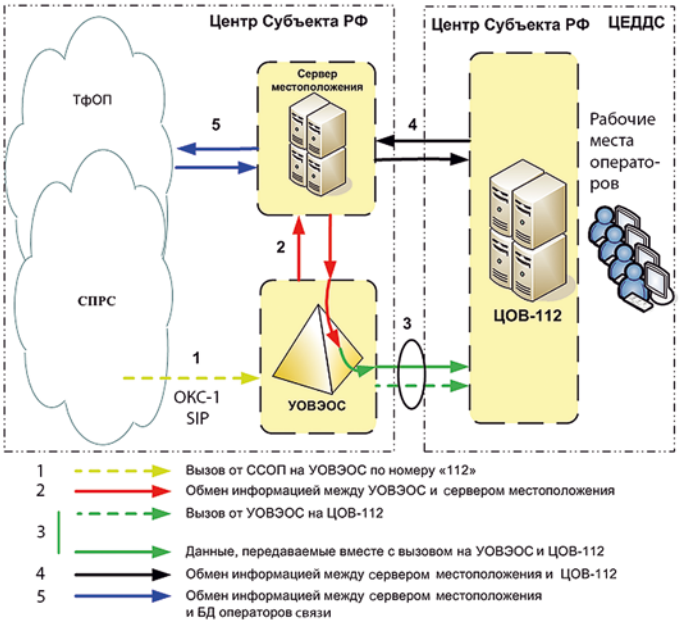

Рис. 1. **Пять интерфейсов системы 112**

апробирован — с учетом чрезвычайной важности системы для государства.

● О перегрузках. На рис. 1 показано прохождение отдельного вызова в системе 112. А как поступать в условиях реальных ЧП, когда из-за перегрузки имеющихся ресурсов экстренных служб часть вызовов может быть потеряна (что недопустимо)? В случаях действительно крупных ЧП в распоряжение МЧС должны были бы поступать и другие центры обработки вызовов (ЦОВ), в том числе ЦОВ «Ростелекома», что на схеме не показано.

● Не отмечены средства доступа (абонентские устройства) к системе 112, в том числе телематические средства защиты охраняемых объектов, которые также относятся к телекоммуникационной составляющей.

В создании системы 112 участвуют многие отечественные компании со своими собственными разработками: «Энвижн Груп», «Навигационно-информационные системы», «Сфера», НТЦ «Протей», «ИскраУралТел», «Светец» и др. Главным недостатком процесса разработки системы 112 является отсутствие единых нормирующих документов. Как следствие, по регионам России реализуются разные частные решения, унификацию которых вряд ли обеспечит использование облачной платформы «Ростелекома» «О7.112». Положительным фактором в данной ситуации является лишь предположение, что продукция отечественных разработчиков сможет соответствовать требованиям импортозамещения.

«Ростелеком» и международные санкции. На Всероссийской конференции «Взгляд в электронное будущее» (октябрь 2014 г., Сочи), организованной по инициативе «Ростелекома» и Правительства России, обсуждался вопрос импортозамещения в области ИТ [5]. «Ростелеком» является партнером множества проектов: государственных инфраструктурных (устранение «цифрового неравенства», ЕГЭ, электронное правительство), отраслевых (медицина и образование, «112», «Безопасный город», КСЭОН) и инновационных (геоинформационные системы, ЖКХ).

«Проектом импортозамещения мы занимаемся уже больше года, понимая, что национальный оператор должен иметь сегмент сети, построенный на национальном оборудовании и управляемый национальным программным продуктом. Мы приняли решение, что как минимум 30% оборудования, установленного на наших сетях, в ближайшем будущем должно быть поставлено российскими производителями и управляться российским софтом. Эта цель открывает большие возможности прежде всего для ИТ-компаний»,— заявил президент ОАО «Ростелеком» С. Калугин.

«Ростелеком», бесспорно, является главным действующим лицом во многих ИТ-проектах, но не забудем, что около 90% сетей связи в России построено на импортном телекоммуникационном оборудовании, причем основным поставщиком является Cisco. И в этом таится угроза.

Гордостью «Ростелекома» является высокоскоростная IP-магистраль, работающая по технологии MPLS (Multi-protocol Label Switching). IP/MPLS-инфраструктура «Ростелекома» имеет свыше 350 точек доступа на всей территории России, 10 опорных и около 150 локальных узлов в регионах РФ. Она построена с использованием магистральных маршрутизаторов Juniper T1600 производительностью до 1,6 Тбит/с и пограничных маршрутизаторов Juniper MX960, Juniper MX480, Juniper M320, Juniper M40. Общая протяженность магистральной сети составляет более 40 тыс. км, пропускная способность достигает 1 Тбит/с, емкость внешних каналов — 200 Гбит/с.

Повлияют ли санкции на бизнес «Ростелекома»? «КоммерсантЪ» сообщает [6], что Cisco Systems и Juniper Networks с апреля 2014 г. не могут поставлять продукцию некоторым российским госзаказчикам, которые имеют отношение к оборонно-промышленному комплексу. Так, Juniper остановила поставки оборудования в силовые структуры (МВД и Минобороны). Бюро по вопросам промышленности и безопасности (BIS) Министерства торговли США, отвечающее за исполнение законов в области экспорта коммерческих товаров, продукции двойного назначения, технологий и софта, с 1 марта приостановило выдачу лицензий на экспорт и реэкспорт в Россию сложного технологического оборудования. На импортозамещение сложного оборудования пакетной коммутации уйдут годы.

Подводя итоги обсуждению текущего момента, отметим, что построение системы 112 идет с большой задержкой и, главное, без должной системной проработки. На примере американских проектов GIG и NG9-1-1 покажем сложности реализации подобных проектов.

Особенности современной сети GIG. Вспомним, как закладывались основы сети GIG оборонного ведомства США, которые ныне стали тормозом ее модернизации.

Оборонная информационная сеть DISN (Defense Information Systems Network) разрабатывается с начала 1990-х. Назначение этой глобальной сети — предоставлять услуги по передаче различных видов информации (речь, данные, видео, мультимедиа) для эффективного и защищенного управления войсками, связью, разведкой и РЭБ. В 1996 г. состояние DISN было подвергнуто резкой критике. Прежде всего за низкий уровень интеграции входящих в состав DISN-NT сетей, что существенно ограничивает взаимодействие в рамках единой сети и препятствует эффективному общему управлению всеми ее ресурсами. В частности, отмечались сложности взаимодействия стационарного и полевого (мобильного) компонентов базовой сети из-за различия в используемых стандартах, типах каналов связи (аналоговых и цифровых), предоставляемых услугах, пропускной способности (у мобильного сегмента она значительно ниже, чем у стационарного).

При разработке принципов построения второй очереди сети DISN-NT пошли по пути использования готовых коммерческих продуктов в области новых информационных и сетевых технологий. При этом упор был сделан на открытые системы, основанные на национальных стандартах, и на новейшие коммерческие технологии и услуги (Commercial-off-the-Shelf). Эти требования нашли отражение в 15-летней программе развития вооружений Joint Vision 2010 [7], которую командование МО США (US Joint Chiefs of Staff) приняло в октябре 1996 г. В части средств связи основной выбор пал на интеллектуальные сети (Advanced Intelligent Network, AIN). Связующим звеном AIN служит система SS7 (рис. 2). Пользователями AIN могут быть абоненты как сети коммутации каналов, так и сети коммутации пакетов. Важная роль отводится интеллектуальной периферии (Intelligent Peripheral): в ее функции входит генерация тонов, распознавание голоса, сжатие речи и данных, распознавание набора номера и многое другое, включая тактические и стратегические сервисы по идентификации персонала.

Через десять лет — в 2006 г.— при составлении плана Joint Vision 2020 [8] состояние сети GIG вновь подвергли резкой критике. Было объявлено о переходе к сети GIG 2.0, в которой требовалось устранить выявленные недостатки:

● большое разнообразие сетей с различным оборудованием;

● несогласованность решений по обеспечению секретности;

● несогласованность программ по ведению боевых операций в разных родах войск;

● различия в информационных базах.

Один из видных американских генералов упрекал производителей военного оборудования в том, что в вооруженных силах имеется 40 различных систем связи: «Ящиков у нас хватает. Помогите нам, чтобы эти ящики умели говорить друг с другом». Основная задача GIG 2.0 формулировалась как создание единой базы данных для всех родов войск, чтобы поддерживать их оперативное взаимодействие. В сети требовалось обеспечить глобальную аутентификацию, контроль доступа и справочные сервисы.

Понадобилось четыре года объемной работы, чтобы в 2010 г. министерство транспорта опубликовало важнейший документ — об интерфейсах сети GIG 2.0 [9]. В нем подробно расписаны протоколы работы сети GIG 2.0, выделены четыре контрольные точки (рис. 3) и указаны протоколы, по которым должны выполняться три типа требований:

- четкое описание моделей структурированных (базы данных, картографические данные, форматы документов) и неструктурированных (презентации, картины, аудио, видео) данных для обеспечения их взаимодействия;
- требования к безопасности;
- требования к функциям шлюзов (Gateways).

В качестве примера опишем контрольную точку 2: это обмен данными на театре военных действий между командирами, солдатами и сенсорами. Для обеспечения взаимодействия используются: протоколы PKI, LDAP или Active Directory (аутентификация); протокол VMF (обмен сообщениями); стандарт VMF/MIL-STD 2525C (передача картографических данных). Что касается безопасности, то для шифрования допускаются решения, сертифицированные в NSA/NIST. Управление ключами осуществляется по решениям EKMS/KMI, охрана оконечных пунктов — по Host-Based Security System (HBSS), управление сервисами — по Remedy/ITSM и IP Management/SPECTRUM. Шлюзы обеспечивают трансляцию между протоколами XML/SOAP и VMF. Работа контрольных точек регламентируется длинным списком открытых и закрытых стандартов — всего на 20 страницах в документе [9].

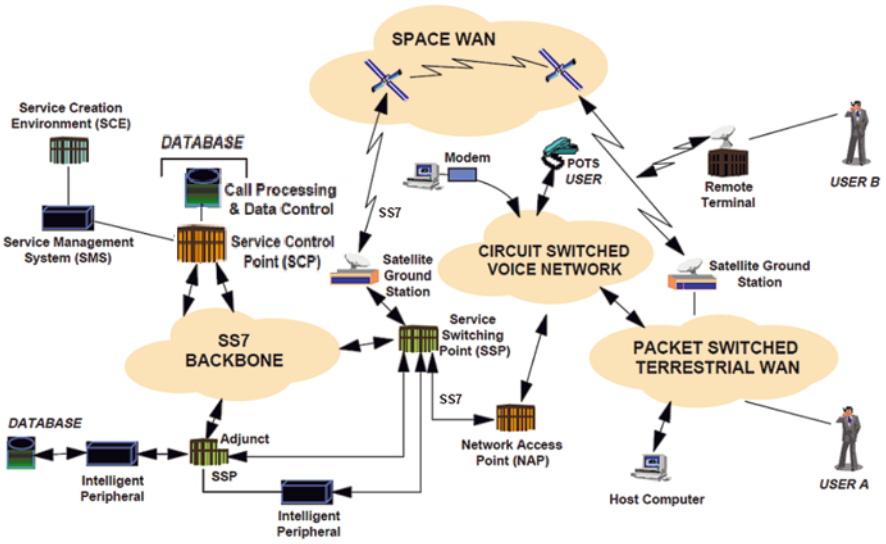

Рис. 2. **Архитектура Advanced Intelligent Network**

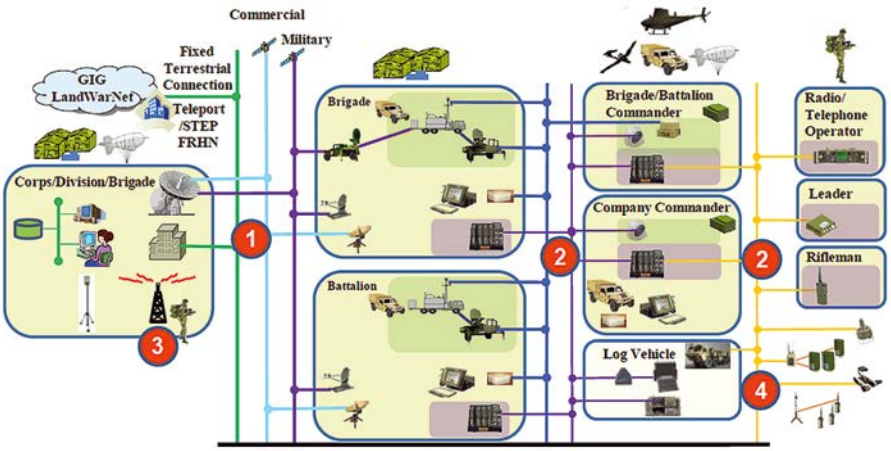

Рис. 3. **Тактическая сеть GIG 2.0 и ее контрольные точки**

Рис. 4. **Новое поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 911**

Сеть NG9-1-1. В США экстренные вызовы обслуживаются, как известно, по номеру 911. Внедрение единого номера экстренных служб, как и в России, там сопровождается трудностями, особенно это относится к определению номера вызывающего мобильного абонента и его местоположения.

Новейшее поколение службы экстренных вызовов в США — NG9-1-1 — будет реализовано в IP-сети (рис. 4). Но когда это произойдет, сказать трудно. В системе NG9-1-1 требуется обеспечить возможность любых сообщений реального времени, т.е. наряду с телефонным вызовом также передачу текста, данных, изображений и видео. Обратим внимание: на рис. 4 слева внизу отдельно указаны телематические вызо-

вы от оберегаемого имущества. Эти вызовы из области M2M-коммуникаций относятся, в частности, к противопожарным и охранным службам. К 2008 г. были завершены пилотные проекты по NG9-1-1. Однако широкое внедрение откладывается до перехода на IMS (IP Multimedia Subsystem). К тому же операторы связи не торопятся переходить на IP-протокол.

Подробное описание экстренной службы NG9-1-1 содержится в документе [10] от 2007 г., где приведены диаграммы прохождения экстренного вызова через все блоки официальной модели NG9-1-1.

Трудности внедрения NG9-1-1 обусловлены риском перехода на IP-протокол**.** 31 января 2014 г. Федеральная комиссия связи (FCC) издала документ о поддержке операторов, которые намерены отказаться от коммутации каналов (по технологии TDM) в пользу IP-протокола [11]. По свежим следам FCC заказала юридической фирме оценку возможных рисков такого перехода. Анализ истории нововведений в телефонных сетях и крупнейших сбоев за последние более чем 20 лет показал [12], что сбои появляются в основном из-за ошибок в программном обеспечении, что ведет к крупным авариям на телефонных сетях.

Наиболее широко известен коллапс сети AT&T, который случился 15 января 1990 г. Тогда из строя одновременно вышли все 114 станций 4ESS сети, принадлежащей AT&T. Устранить неполадки удалось только через 9 часов. Причина — в новом программном обеспечении, которое установили месяцем ранее на всех станциях 4ESS. Ошибка, вкравшаяся в работу системы SS7, проявилась при перегрузке одной из АТС и по принципу домино «вырубила» почти всю сеть оператора. Потеря 65 млн вызовов нанесла репутации компании трудно восполнимый ущерб.

Другая подобная катастрофа произошла через полтора года — 26 июня 1991 г. в Балтиморе, когда без связи на 6 часов остались 5 млн абонентов. И тоже из-за ошибки в программах SS7.

Впоследствии Конгресс США расследовал эти аварии сети связи, так как они были приравнены к угрозе национальной безопасности страны. Системе SS7 «вынесли приговор». В частности, в службе 911 отказались от применения сигнализации SS7 и интеллектуальной сети и сохранили прежнюю систему многочастотной сигнализации MF. В докладе юридической фирмы указаны также скандалы с переносом номеров мобильной связи, с внедрением бесплатного вызова по коду 888 и др.

Будут ли после этого операторы связи спешить с переходом на IP-протокол?..

Сравнение NG9-1-1 и GIG. В последнее время многие обращают внимание на аналогию между экстренной службой NG9-1-1, которую строит министерство транспорта США, с одной стороны, и инфокоммуникационной сетью GIG, создаваемой министерством обороны, с другой. Но как воспользоваться этой аналогией? И если таковая есть, то как совместить планы разработки этих двух систем многомиллиардной стоимостью?

Сошлемся на материалы Конференции по внутренней безопасности США (Homeland Security). Автор одной из статей напоминает, что оба проекта были объявлены практически одновременно — в 2007 г. [13]. Аналогии начинаются с высокого уровня архитектуры сетей NG9-1-1 и GIG. Обе архитектуры предполагают сбор информации от множества источников и передачу ее множеству пользователей. И, что важно, обе системы требуют высокой живучести. Необходимо передавать голос, данные и видео, причем с минимальной задержкой. Применения также сопоставимы.

Самым сложным применением оказывается передача данных. Например, согласно концепции NG9-1-1, больной вызывает скорую помощь текстовым сообщением. Это сообщение достигает центра обслуживания вызовов, оператор которого, используя сообщение, определяет местоположение больного, сообщает об этом скорой помощи и посылает подтверждение больному. Данные о местоположении передаются компьютеру и наносятся на карту.

В GIG-архитектуре похожая картина передачи и обработки данных. Данные могут быть любого типа, включая текст, файлы, снимки. Каждый военнослужащий должен быть доступен для обмена информацией. Например, если солдат обнаружил бункер, но не может распознать тип вооружения в нем, он передает картинку аналитику вооружения. Аналитик отвечает, а также может вызвать бомбардировщик и известить разведку для уточнения цели.

Аналогия между NG9-1-1 и GIG налицо. Но кто ею воспользуется и согласует планы строительства этих двух систем?

Российские разработчики из анализа NG9-1-1 и GIG могут сделать для себя следующие выводы:

1) системный проект системы 112 можно разработать на базе документа [10];

2) используя аналогию между NG9-1-1 и GIG, следовало бы рассмотреть создание единой сети не только для системы 112, но и для МЧС и МО.

Стратегии связистов России. Основой системы 112 является ССОП, точнее сеть «Ростелекома», и конечный успех внедрения сети 112 зависит от стратегии национального оператора.

Стратегия 1. В настоящее время основная стратегия «Ростелекома» — двигаться в сторону All-over-IP, т.е. продолжать строительство сетей связи средствами иностранных производителей. Образно говоря, надо «зажмуриться» и идти к All-over-IP, идти, опасаясь коллапса сети и потери управления страной.

Тут уместно обратиться к истории. В 1991 г. в ходе операции «Буря в пустыне» США продемонстрировали новые средства ведения информационной войны. С помощью электронных излучателей американцам, например, удалось нарушить радио- и телефонную связь практически на всей территории Ирака, что в значительной мере предопределило исход боевых действий. Вывести из строя систему управления противовоздушной обороны Ирака спецслужбам США позволила активация специальных вирусов, которые были «заранее» спрятаны в памяти принтеров, приобретенных для этой системы у одной коммерческой фирмы.

Анализ состояния сетей связи России в условиях импортозамещения позволяет развернуть дискуссию об обоснованности самой идеи повсеместного перехода на пакетную коммутацию [1, 14]. Основной выигрыш от коммутации пакетов состоит в более экономном использовании каналов — за счет заполнения пауз, а главное, что подчеркивают апологеты новой техники, это ее гибкость и универсальность. Достаточно ли этого для смены технологий?

Следует учитывать и недостатки коммутации пакетов:

1. Неопределенность времени передачи данных, так как задержки в очередях буферов зависят от загрузки сети.

2. Колебания времени передачи — из-за скачков загрузки сети.

3. Возможные потери пакетов — из-за переполнения буферов.

4. Удлинение «чистого» времени занятия канала из-за добавления заголовков в пакетах и ожидания в буферах: при коммутации каналов сигнальная информация передается один раз, при коммутации пакетов — добавляется к каждому пакету.

5. Усложнение алгоритмов передачи секретных данных, тем более для передачи приоритетных данных.

Заметим, что гибкость и универсальность новой технологии, к огорчению отечественных производителей, достигается

за счет применения в узлах коммутации (в маршрутизаторах) микросхем сверхвысокого быстродействия.

Сети «Ростелекома» сегодня стали ареной борьбы «за сферы влияния» двух американских компаний — Cisco и Juniper. Действительно, на базе такого оборудования можно строить современные сети. Но, к сожалению, такая стратегия приводит к зависимости национального оператора от этих компаний на обозримое будущее. И как быть с безопасностью страны? Как преодолеть санкции?

Стратегия 2 заключается в выборе курса на импортозамещение, т.е. на развитие сетей связи собственными силами. Для этого надо вернуться к состоянию знаний, достигнутому 20 лет назад, и развивать их далее. В данном случае такой точкой отсчета можно условно назвать систему ОКС-7. В России отставание от мирового уровня, конечно, большое, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника. Но тем более стоит оценить перспективы коммутации каналов, т.е. вспомнить прошлое и ускоренными темпами продолжить движение вперед (догонять-то проще). **Следует восстановить промышленность средств связи.**

Сеть «Ростелекома», по-видимому, будет мигрировать к архитектуре NGN**.** Поэтому важно рассмотреть возможности традиционной сети коммутации каналов и сигнализации SS7 «уживаться» с сетью NGN, где будет главенствовать протокол SIP. Наиболее сложным блоком в архитектуре NGN является IMS (IP Multimedia Subsystem), что представляет собой аналог SCP из архитектуры IN. Блок IMS обеспечивает мультимедийные сервисы в архитектуре мобильной сети UMTS (управляет сигнализацией, элементами транспортной сети и обеспечивает контроль сессии).

Попытку объединения IN и IMS предприняла компания Ericsson, разработав Ericsson Composition Engine в качестве нового поколения интеллектуальных сетей [15]. Это устройство, в котором предоставляются дополнительные сервисы по протоколам INAP, CAP и SIP, находится на стыке между сетями коммутации каналов и коммутации пакетов. Пока неизвестно, получит ли платформа Ericsson Composition Engine широкое распространение.

Наибольшие усилия по стыковке сигнализации SS7 и интеллектуальной сети с протоколом SIP и узлом IMS предприняты компанией Telcordia (США) [16]. Напомним, что Telcordia выступает продолжателем работ Bell Labs по интеллектуальным сетям. В начале 1990-х Telcordia разработала архитектуру AIN. Дальнейшие варианты сети объединяются группой документов AINGR Family of Requirements, FR-15, которые подводят итог 20-летней работы по развитию концепции AIN в условиях наступления IP-технологии, точнее SIP-протокола, а также фиксируют требования экстренных вызовов E 9–1–1 в архитектуре AIN. Данные документы могут служить основой для совершенствования российской интеллектуальной сети, чтобы на ее базе строить систему 112.

Заключение. Таким образом, комплексный проект системы 112 можно разработать, воспользовавшись документами американских сетей NG9-1-1 и GIG.

1) Используя аналогию между сетями NG9-1-1 и GIG, следует рассмотреть возможность создания единой сети не только для системы 112, но и для МЧС и МО.

2) С учетом курса на импортозамещение, т.е. на развитие сетей связи собственными силами, необходимо совершенствовать систему ОКС-7 и российскую интеллектуальную сеть.

3) С учетом конвергенции коммутации каналов и коммутации пакетов российскую интеллектуальную сеть можно совершенствовать на основе документов Telcordia и на базе интеллектуальной сети строить систему 112.

Послесловие. 25 февраля текущего года ComNews сообщил о важном событии в отраслевой науке [17]: «Ростелеком» и отечественный Центр прикладных исследований компьютерных сетей (ЦПИКС) анонсировали сотрудничество в области программно-конфигурируемых сетей (Software Defined Networks, SDN) и виртуализации сетевых функций (Network Functions Virtualization, NFV), что позволит оператору снизить операционные и капитальные затраты примерно на 30%. Направление SDN — модное слово в мировой науке. Но вряд ли «на волне SDN» удастся получить быстрый коммерческий успех и заменить импортируемые средства связи уже в ближайшие годы. Скорее, исследования в области SDN послужат стимулом развития отечественной науки и восстановления промышленности средств связи.

ЛИТЕРАТУРА

1. **Соколов Н. А**. Системные аспекты построения и развития сетей электросвязи специального назначения //International Journal of Open Information Technologies.— 2014.— Т. 2.— № 9.— С. 4–8.
2. В девяти субъектах РФ отложен запуск системы 112. Онлайновый ресурс: http://www.obeschania.ru/news/2014–01–28/112-zapusk#ixzz3H4Wlqitn.
3. Что мешает внедрению «Службы 112» // ИКС.— 2013. № 11.— С. 15.
4. **Полканов Е. И., Мазин И. Г**. Совместное использование информационных ресурсов: консолидация развития сетей// Электросвязь.— 2012.— № 3.
5. «Ростелеком» опубликовал карту магистральной сети IP/MPLS. Онлайновый ресурс: http://servernews.ru/597356.
6. Вендорам перекрыли госканал. Онлайновый ресурс: http://www.kommersant.ru/doc/2520423.
7. **Bennet. B. T**. Information Dissemination Management/ Advanced intelligent Network services for department of Defence// MILCOM, 1999.
8. The Global Information Grid (GIG) 2.0 Concept of Operations Version 1.1//11 March 2009, Joint Staff J6, Washington, D.C.
9. Common Operating Environment Architecture. Appendix C to Guidance for ‘End State’ ArmyEnterprise Network Architecture U.S. Army CIO/G-61 October 2010
10. Next Generation 9–1–1 (NG9-1-1) System Initiative, U.S. Department of Transportation, October 2007.
11. FCC. Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13–5, FCC 14–5 (rel. Jan. 31, 2014).
12. FCC. In the Matter of Technology Transitions GN Docket No. 13–5, March 19, 2014. http://apps.fcc.gov/ecfs/document/view?id=7521093879 Retrieved: Jun, 2014.
13. **Schmitt M.** Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE International Conference on Technologies for Homeland Security May 2008
14. **Шнепс-Шнеппе М.А., Намиот Д. Е.** Телекоммуникации для военных нужд: от сети GIG1 к сети GIG2 //International Journal of Open Information Technologies.— 2014.— Т. 2.— № . 9.— С. 9–17.
15. **Niemöller J. et al.** Ericsson Composition Engine — Next-generation IN// Ericsson review, № 2, 2009.
16. Telcordia Roadmap to Advanced Intelligent Network (AIN) Documents, Issue 2, August 2008.
17. «Ростелеком» на волне SDN //Онлайновый ресурс: http://www.comnews.ru/node/90305.

Получено 06.11.14