

О ЗАДАЧАХ в области связи

М.Шнепс-Шнеппе, д.т.н., генеральный директор компании AbavaNet,
Д.Намиот, к.ф.-м.н, доцент, МГУ имени М.В.Ломоносова,
С.Селезнев, к.т.н., главный специалист компании "Фактор ТС",
В.Куприяновский, МГУ имени М.В.Ломоносова

УДК 654.1

Обсуждаются основные новые задачи, стоящие перед российской отраслью связи: импортозамещение, разработка Системы 112 и комплекса "Безопасный город", Интернет вещей и защита объектов критической инфраструктуры. Уточняются задачи, стоящие перед МЧС и Минкомсвязью России, а также перед Ростелекомом.

Чем характерен текущий момент в российской связи – отрасли народного хозяйства, важнейшей как для гражданских, так и специальных нужд [1]? Во-первых, полноценные системные исследования путей модернизации сетей связи не ведутся в России как минимум два десятилетия. Во-вторых, операторы связи и поставщики услуг копируют принятые в других странах решения без адекватной оценки их положительных и отрицательных сторон. В-третьих, не учитывается приемлемость иностранных решений для различных групп пользователей, прежде всего сетей специального назначения, в том числе Системы 112 и комплекса "Безопасный город".

В то же время область телекоммуникаций многократно расширяется: абонентами становятся не только люди, но и окружающие нас вещи, охраняемые объекты. Это ставит новые задачи системного проектирования, многократно сложнее тех, что решались в СССР, когда писали системные проекты под названием "Факел".

СИСТЕМА 112 И КОМПЛЕКС "БЕЗОПАСНЫЙ ГОРОД"

В Положении об МЧС сказано, что 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.

Разработка Системы 112 представляет собой сложнейший проект государственного значения, практически непосильный в рамках существующей ныне рыночной экономики. Этот проект затрагивает все стороны жизни российского общества, и в ходе его реализации обнажаются многие недостатки хозяйства страны, накопившиеся за четверть века капиталистического строительства в России.

Построение Системы 112 идет с большим трудом, работы ведутся уже долгие 20 лет. И строится она по отдельным областям, а не для всей страны в целом. В официальном отчете Минкомсвязи России от 2013 года [2] перечислены нерешенные задачи: "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".

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 году Систему 112 планировалось внедрить

в трех субъектах России, в 2014-м – в шести, в 2015-м – еще в двух, в 2016-м – в пяти, а в 2017 году запустить в оставшихся 67 регионах. По состоянию на 13 мая 2016 года Система 112 введена в промышленную эксплуатацию только в Калужской и Курской областях и в Республике Татарстан. До сих пор так и не разработан единый системный проект Службы 112, и тем самым все проведенные работы, скорее всего, следует рассматривать как экспериментальные образцы.

Система 112 является частью АПК "Безопасный город", поэтому данные системы будем рассматривать совместно. Аппаратно-программный комплекс "Безопасный город" должен объединить любые системы (информационные, мониторинговые, оповещающие, приемопередающие) любого муниципального образования, а в перспективе – и всей страны. И, самое главное, АПК "Безопасный город" должен иметь высокий уровень собственной информационной безопасности. Поэтому при его создании необходимо использовать российское аппаратное и программное обеспечение, изначально разрабатываемое под российские стандарты безопасности.

В США уже продолжительное время строится единая сеть нового поколения для обслуживания экстренных вызовов NG9-1-1. Рассмотрение американского опыта помогает понять, почему так трудно выполнить намеченные задачи. В качестве иллюстрации многообразия требований экстренной службы рассмотрим деятельность нового поколения службы NG9-1-1 отдельного штата США. Согласно официальным документам [3], будущие сети экстренных служб должны быть сетями пакетной коммутации. Особо отмечается, что сеть NG9-1-1 должна поддерживать мультимедиа и практически охватывать все стороны общественной жизни. Единая сеть штата (State Backbone Network) объединяет: традиционную телефонную сеть, мобильную сеть, экстренную службу 9-1-1, полицию, пожарную службу, национальную гвардию, школы, госпитали, аппарат губернатора и т.д.

Служба NG9-1-1 отдельного штата (в случае России – это субъект Федерации) создается средствами Интернета. Следует ли нам идти по этому пути, т.е. переходить ли полностью на технологию пакетной коммутации? Это является важнейшим вопросом, который следует основательно обсуждать.

ИНТЕРНЕТ ВЕЩЕЙ

Кроме государственных проектов Системы 112 и комплекса "Безопасный город" в последнее время стал актуальным вопрос

индустриального Интернета, или, другими словами, Интернета вещей (Internet of Things, IoT) и межмашинного общения M2M. На пленарном заседании Международной промышленной выставки "ИННОПРОМ" 11 июля 2016 года Премьер-министр РФ Дмитрий Медведев предложил создать консорциум для развития в области индустриального Интернета с привлечением разработчиков, потребителей и научного сообщества. По его словам, такой консорциум должен консолидировать всю отрасль и вырабатывать предложения по стандартизации и нормативному регулированию и продвигать эти технологии, привлекать финансовых партнеров, в том числе из числа институтов развития. Д.Медведев заявил о необходимости понимания развития технологий на перспективу 10–20 лет и обратил внимание на развитие сферы Интернета вещей (концепции соединения физических объектов компьютерной сетью).

Странам мира необходимо совместно противостоять угрозам в сфере технологической безопасности, сказал Премьер-министр РФ. По его словам, риски в этой сфере сохраняются и множатся. Он призвал решать эти проблемы на различных площадках, и в качестве примера глава российского правительства привел такую универсальную площадку, как Международный союз электросвязи при ООН.

Премьер-министр напомнил, что в России подготовлен проект "дорожной карты" по развитию технологий в области индустриального Интернета. Эта "дорожная карта" предполагает реализацию пилотных отраслевых проектов, меры по разработке стандартов и обеспечение безопасности в радиочастотном урегулировании и развитии микроэлектроники. Медведев добавил, что к ноябрю 2016 года должны быть сформулированы предложения по формированию нормативной базы, которая необходима для внедрения индустриального Интернета.

Обратим внимание на эту важнейшую государственную инициативу, и прежде всего – на формирование нормативной базы, т.е. на разработку стандартов в области Интернета вещей, что представляет исключительно трудоемкую задачу, учитывая увлеченность иностранной техникой связи в постсоветский период.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Сегодня наиболее важная задача в сфере телекоммуникаций – обеспечение безопасности критической инфраструктуры (Critical Infrastructure

Protection, SIP), что представляет собой концепцию готовности противодействовать серьезным угрозам работы важных объектов инфраструктуры и объектов повышенной опасности в регионе или стране, особенно в условиях распространения информационных технологий и связанных с ними киберугроз.

Исторически первым шагом в этом направлении было создание в 1996 году Комиссии по защите жизненно важной инфраструктуры при президенте США: была поставлена задача разработать всеобъемлющую национальную стратегию по защите инфраструктуры от физических и кибернетических угроз. Похожая же директива издана в Европейском Союзе в 2008 году. В России основные направления государственной политики по защите критически важных объектов инфраструктуры утверждены в 2012 году [4]. В этом документе поставлена цель совершенствовать безопасность информационных и телекоммуникационных систем критической инфраструктуры и объявлен план работ до 2020 года. На практике на сегодня наибольшая активность в России сосредоточена в направлении "Безопасный город" [5].

Отметим, что ведущая роль в обеспечении кибербезопасности критической инфраструктуры принадлежит телекоммуникациям в обеспечении как собственной безопасности, так и всех важных объектов. К сожалению, следует отметить, что российские сети связи построены в основном на базе иностранного оборудования. Например, гордостью Ростелекома является сеть IP/MPLS, объединяющая всю страну и имеющая многие выходы на международные IP-сети. Она построена на базе маршрутизаторов компании Juniper. Всего имеется 150 узлов: несколько мощнейших Juniper router T1600 (1,6 Тбит/с) и множество меньших. Но в условиях кибервойны возникает закономерный вопрос: не является ли эта сеть американским кибероружием?

Новые задачи Минкомсвязи

"Методические рекомендации по обеспечению предоставления операторами связи информации о месте нахождения пользовательского оборудования (оконечного оборудования) операторам системы обеспечения вызова экстренных оперативных служб по единому номеру 112" опубликованы на сайте Минкомсвязи России только 18 января 2016 года, а работы по созданию Системы 112 во всех областях России, согласно требованиям

ФЦП, полагалось завершить в 2017 году. Ясно, что в срок их не удастся завершить.

Только в конце 2015 года МЧС и Минкомсвязь России согласовали "Методические рекомендации по разработке системных проектов телекоммуникационной подсистемы системы обеспечения вызова экстренных оперативных служб по единому номеру 112 для субъектов Российской Федерации" [6]. В этом документе утверждается, что "системный проект является проектным документом стадии ПП (предпроектная проработка). Системный проект является основанием для разработки операторами связи проектной и рабочей документации на вновь вводимые, реконструируемые и модернизируемые узлы, линии и системы связи для создания телекоммуникационной подсистемы Системы-112". Отметим особо, что речь идет всего лишь о предпроектной проработке (!). "Методические рекомендации" [6] появились как выполнение Федеральной целевой программы, которую полагалось завершить в 2017 году, и в этом документе дан перечень томов (всего их 19), которые должны быть в системном проекте по каждой области. Заметим, что в ФЦП исходно были поставлены более сложные задачи: создать телекоммуникационную инфраструктуру Системы 112; создать информационно-техническую инфраструктуру Системы 112.

Какова же будет "телекоммуникационная инфраструктура Системы 112", до сих пор так и нет ответа. К тому же до сих пор телекоммуникационные сети в значительной мере строятся на базе иностранного оборудования, что никак не соответствует требованиям АПК "Безопасный город".

Другим важным вопросом является нумерация - как для обслуживающего персонала Системы 112, так и для пользователей, особенно терминалов телематики, устройств Интернета вещей. В этом направлении сделан только первый робкий шаг: 4 мая 2016 года Минкомсвязь России издала приказ о нумерации экстренных оперативных служб, а именно введен формат маршрутного номера вызова экстренных оперативных служб в виде RNC=ABC1UVx1x2x6x7, где ABC - код географической зоны нумерации; UV - номер экстренной службы 112, 101, 102, 103 или 104; x1x2 - зональный телефонный номер; x6x7 - идентификатор дежурно-диспетчерской службы, равный 11.

До сих пор совсем упущены вопросы программного обеспечения, которые также входят в сферу ответственности Минкомсвязи

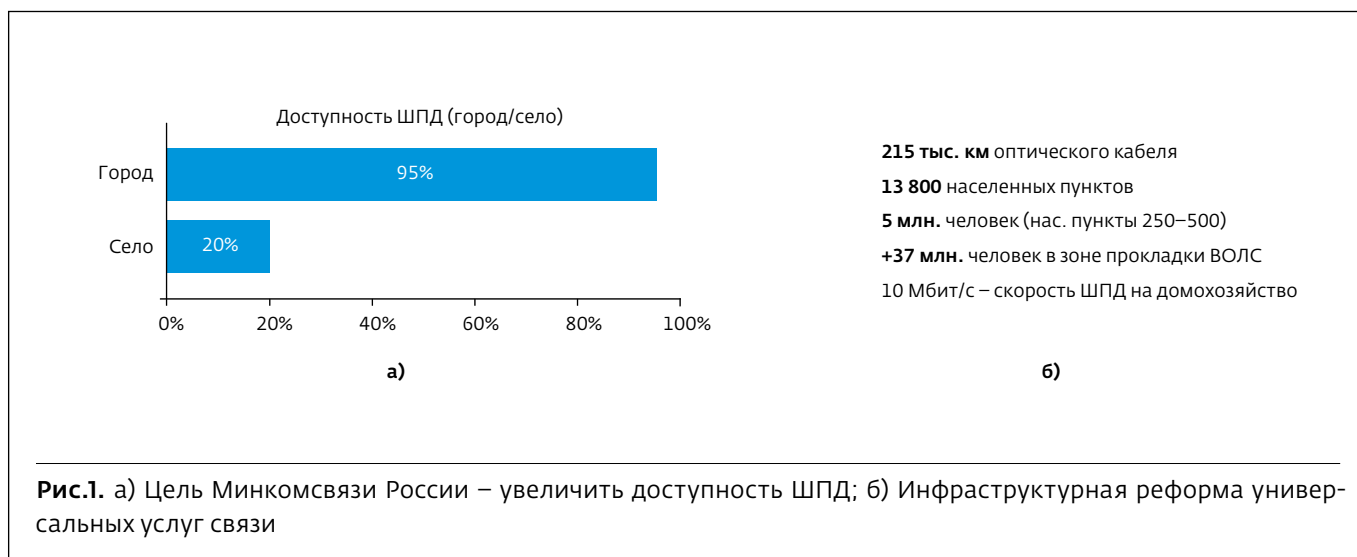


Рис.1. а) Цель Минкомсвязи России – увеличить доступность ШПД; б) Инфраструктурная реформа универсальных услуг связи

России. Например, 30 марта 2016 года министр Н.Никифоров доложил Президенту России о мерах поддержки российского ПО. "По данным отраслевых ассоциаций, объем продаж экспорта из России, в том числе ИТ-услуг, программного обеспечения, достиг уже почти семи миллиардов долларов, это очень существенная цифра. Теперь вместе с ФАС России будем ловить за руку тех госзаказчиков, кто все равно по старинке предпочитает закупать иностранное ПО несмотря на то, что появились аналогичные российские решения", – сказал глава Минкомсвязи России [7]. Заметим, что в данном случае речь шла всего лишь об офисном программном обеспечении. Пока же министерство даже не ставит целью разработать ПО для телефонных станций или маршрутизаторов, что требуется для Системы 112 и АПК "Безопасный город".

И еще. Следует по-новому взглянуть на универсальную услугу. Доступ к Системе 112 должен быть немедленным для любого жителя страны (а не в часе ходьбы до таксофона для удаленного жителя на селе, как записано в действующем Федеральном законе "О связи"), а также для любого датчика охраняемого объекта. В погоне за расширением доступа к интернету ущемляются права жителей мелких сел. 26 февраля 2015 года Н.Никифоров рассказал Правительству РФ об обеспечении доступности современных услуг связи [8]. Доклад начинается со слов об основной цели Минкомсвязи России – увеличить широкополосную доступность (рис.1а). К сожалению, уровни проникновения связи в городской и сельской местности пока еще сильно различаются.

На рисунке 1б даны основные параметры амбициозного инфраструктурного проекта по строительству оптики. "Не могу не отметить, что сегодня это действительно самый крупный в мире проект по строительству линий связи в малые населенные пункты – 215 тыс. км, 13,8 тыс. сел, около 5 млн. человек напрямую проживают в них, – отметил министр. – Но, еще раз подчеркну, это лишь села на 250–500 жителей. Очевидно, что кабель по пути к этим малым селам пройдет и через другие населенные пункты. Так вот, по пути к ним мы планируем охватить населенные пункты с 37 млн. жителей" (общий охват. – Ред.). Далее он добавил: "В нашей стране имеется 148 тыс. таксофонов, они установлены действительно практически в каждом селе и обеспечивают связь, в том числе в условиях чрезвычайных ситуаций. Это важнейшее инфраструктурное достижение, которое существует".

К сожалению, намеченные планы в какой-то мере увеличивают, а не уменьшают "цифровое неравенство", так как из общего числа 153 000 населенных пунктов (по переписи 2010 года): 36 200 имеют число жителей 1–10, 32 700 имеют число жителей 11–50, 13 800 имеют число жителей 51–100, т.е. более 8 тысяч сел практически остаются вне охвата средствами связи.

Напрашивается замечание: доступ к Интернету, несомненно, услуга привлекательная, но считаем, что доступ к службам "112" является более приоритетным – в смысле как социальной значимости, так и государственной важности. Поэтому в приоритетном порядке стоило бы снабдить жителей села радиосредствами, хотя бы

текстовыми терминалами, чтобы не требовалось тратить час ходьбы до таксофона.

Ведущая роль Ростелекома в построении информационного общества

Согласно распоряжению Правительства РФ № 453-р от 21 марта 2011 года, ПАО "Ростелеком" является единственным исполнителем работ по ряду мероприятий Федеральной целевой программы "Информационное общество (2011-2020 гг.)". В выполнении этих мероприятий используется Национальная облачная платформа О7 [9].

Важнейшим среди мероприятий является сервис "О7. 112", который обеспечивает обработку экстренных вызовов по номеру 112. Функции сервиса "О7. 112" включают:

- прием и обработку сообщений по единому номеру 112 для всех экстренных служб;
- координацию управления силами и средствами реагирования;
- межведомственную координацию (экстренные службы различных ведомств работают в едином информационном пространстве).

Использование платформы О7 предполагает:

- снижение потери населения до 15%;
- снижение времени комплексного реагирования в два раза;
- снижение экономического ущерба – до 5%;
- разгрузку операторов межведомственных служб за счет перехвата ложных и справочных вызовов оператором 112 – на 70%.

Приведенные показатели следуют, по-видимому, из бизнес-плана, который нам неизвестен. Но для убедительности хорошо бы по крайней мере привести архитектуру Системы 112 с указанием роли Ростелекома, в том числе платформы О7 и комплекса "О7. 112".

К проекту "О7. 112" примыкает сервис "О7. Медицина" как часть Системы 112. Цель его создания – автоматизация взаимодействия всех участников медицинского процесса: сотрудников лечебно-профилактических учреждений, пациентов, работников министерств и ведомств, отвечающих за здоровье граждан. Подключившись к сервису "О7. Медицина", любое лечебно-профилактическое учреждение получает доступ к системе электронной регистратуры, единым электронным медицинским картам пациентов, системе электронного документооборота.

Отметим еще сервис "О7. Сити", который непосредственно связан с АПК "Безопасный город". Цель создания сервиса – обеспечение

эффективного и безопасного функционирования городских служб и создание комфортных условий проживания в городе (регионе). Сервис "О7. Сити" включает:

- мониторинг городской инфраструктуры (ЖКХ, дорог, показаний приборов критических объектов городской инфраструктуры);
- мониторинг природных объектов (пожары, наводнения);
- видеонаблюдение и видеоаналитику (установка промышленных камер наблюдения в городе, а также обеспечение открытых интерфейсов, с помощью которых граждане смогут направлять для обработки информацию о происшествиях, собираемую бытовыми видеодустройствами);
- мониторинг и управление общественным транспортом и парковками;
- информирование населения об угрозах и чрезвычайных ситуациях.

Проекты "О7. 112", "О7. Медицина", "О7. Сити" и другие с участием Ростелекома (устранение "цифрового неравенства", ЕГЭ и образование, электронное правительство) – все эти проекты чрезвычайно важны и социально значимы, но вместе с тем и чрезвычайно сложны для реализации. К тому же облачная платформа "О7" – это всего лишь хранилище данных. А как обстоит дело в ответственной роли Ростелекома в самом проекте Системы 112, и не только для отдельных областей, а для всей страны?

Напомним, в "Методических рекомендациях" [6] дан перечень томов (всего их 19), которые должны быть в системном проекте Системы 112 для каждой области. На наш взгляд, Ростелекому полагалось разработать единый проект для всей страны (все эти 19 томов), а при строительстве Системы 112 по областям следовало бы только оговаривать отклонения от общего проекта. Такой подход способствовал бы как импортозамещению, так и развитию отечественной промышленности.

Текущие задачи российских связистов

Настоящая статья ставит своей целью искать пути решения сложнейшей задачи – построения Системы 112 и АПК "Безопасный город" на базе российского аппаратного и программного обеспечения. Что следует делать?

- Первоочередной задачей является разработка единых системных проектов Системы 112 и комплекса "Безопасный город" для всей страны (прежде всего Технических требований на информационную инфраструктуру),

что предполагает объединение усилий МЧС и Минкомсвязи России, а также Ростелекома.

- Выполнение этой задачи предполагает усиление ведущей роли МЧС, а также возрождение ведущих институтов Минкомсвязи России, в частности института ЦНИИС, который ослаблен взятым ранее курсом на приватизацию.
- Курс на импортозамещение предусматривает использование российского аппаратного и программного обеспечения, изначально разрабатываемого под российские стандарты безопасности, что в свою очередь предполагает усиление Минэкономразвития и Минкомсвязи России с восстановлением в определенном смысле функций бывшего МПСС.
- Если взять курс на импортозамещение, т.е. на развитие сетей связи собственными силами, то, на наш взгляд, следует вернуться к тому состоянию знаний, которые были достигнуты ранее, лет 20 назад, и развивать их дальше. Такой точкой отсчета условно можно назвать систему ОКС-7 и интеллектуальные сети. Учитывая отставание от передового мирового уровня, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника, стоит оценить перспективы коммутации каналов, где не требуются столь высокое быстродействие.
- Для создания Системы 112 и АПК "Безопасный город" необходимо организовать подготовку специалистов, способных разрабатывать нормативные документы по сетям связи с коммутацией каналов и с пакетной коммутацией, аппаратные и программные средства новых сетей связи.
- Особо отметим важность индустрии программирования услуг. Это относится к весьма болезненному для связистов вопросу об открытых интерфейсах программирования (Open API). Если будет открыт доступен набор API, то многие сторонние программисты включатся в разработку Системы 112 и комплекса "Безопасный город".
- И главное – следует разработать нормативные документы (стандарты) по новым гибридным сетям коммутации каналов и пакетов, учитывая также новейшие требования индустриального Интернета (Интернета вещей и межмашинного общения), что представляет собой исключительно трудоемкую задачу, учитывая увлеченность иностранной техникой связи в постсоветский период.

Более подробно вопросы создания Системы 112 и АПК "Безопасный город" рассмотрены в [10–12].

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. Что мешает внедрению "Службы 112" // ИКС. 2013. №11. С.15.
3. Model State 911 Plan, National Association of State 911 Administrators, DOT HS 811 369, February 2013.
4. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, 3 февраля 2012 г. URL : <http://www.scrf.gov.ru/documents/6/113.html>
5. Методическое пособие по разработке организационных документов по созданию и развитию аппаратно-программного комплекса "Безопасный город". Москва, 2016. URL : http://www.mchs.gov.ru/upload/site1/document_file/E4Na2VRWjW.pdf
6. Методические рекомендации по разработке системных проектов телекоммуникационной подсистемы системы обеспечения вызова экстренных оперативных служб по единому номеру "112" для субъектов Российской Федерации, Москва, 2015.
7. Меры по поддержке российского ПО. URL : <http://www.minsvyaz.ru/ru/events/32718/>
8. Обеспечение доступности современными услугами связи. URL : government.ru/gov/persons/192/
9. Национальная облачная платформа Ростелекома. URL : www.rostelecom.ru/projects/o7/
10. Шнепс-Шнеппе М.А., Селезнев С.П., Куприяновский В.П. Сеть DISN как прототип сети связи гражданской обороны NG112 // International Journal of Open Information Technologies. 2016. Т.4. №5. С.39–47.
11. Шнепс-Шнеппе М.А., Селезнев С.П., Намит Д.Е., Куприяновский В.П. О телекоммуникационной инфраструктуре комплекса "Безопасный город" // International Journal of Open Information Technologies. 2016. Т.4. №6. С.17–31.
12. Шнепс-Шнеппе М.А., Селезнев С.П., Намит Д.Е., Куприяновский В.П. О кибербезопасности критической инфраструктуры государства // International Journal of Open Information Technologies. 2016. Т.4. №7. С.22–31.