Телекоммуникации как решающее звено цифровой экономики. Опыт США

М.А. Шнепс-Шнеппе, В.П. Куприяновский, Д.Е.Намиот, С.П.Селезнев

***Аннотация* – Данная статья является первой в серии работ, посвященных роли телекоммуникаций в цифровой экономике. По всем признакам, именно телекоммуникации будут играть решающую роль в цифровой экономике. Перед связистами всего мира стоит одна и та же задача – как полностью перейти от коммутации каналов к коммутации пакетов. Трудности перехода от коммутации каналов к коммутации пакетов иллюстрируют примеры из опыта телекоммуникационных сетей США, а именно: сеть первой помощи FirstNet, экстренной службы NG911 и оборонной информационной сети Пентагона. Накапливаются факты о том, что обе технологии будут еще долго сосуществовать. Это ставит под сомнения саму целесообразность смены парадигмы телекоммуникаций.**

***Ключевые слова* — Internet of Things, Network of Things, цифровая экономика, FirstNet, служба 911, DISN, DRSN, протокол AS-SIP**

I. О текущем моменте: вспомним о плане ГОЭЛРО

Когда-то словосочетание "план ГОЭЛРО" было известно каждому школьнику. Государственный план электрификации России – это детище Октябрьской революции и лично В. И. Ленина. План был разработан в декабре 1920 года и ставил задачи ускоренного развития народного хозяйства.

В 1913 году в России на душу населения вырабатывалось всего 14 кВт.ч, тогда как в США - 236 кВт.ч. Обладая огромными природными богатствами, Россия добывала во много раз меньше полезных ископаемых - угля, железной руды и даже нефти, чем США, выплавляла гораздо меньше чугуна и стали. К концу пятнадцатилетнего срока плана ГОЭЛРО - к 1935 году советская энергетика вышла на уровень мировых стандартов и заняла третье (после США и Германии) место в мире [1].

Сегодня судьба ставит перед Россией новый вызов. 3 апреля 2017 года Президент Российской Федерации Владимир Путин утвердил рабочую группу Экономического совета по направлению «Цифровая экономика». Цифровая экономика – это грандиозное, по замыслу, государственное движение, предполагающее разработку своего рода «нового плана ГОЭЛРО». Станет ли это движение базой модернизации России – покажет ближайшее будущее. Цифровая экономика в мире развивается быстрыми темпами – 10% в год, что более чем в три раза выше показателя глобального экономического роста. Многие понимают, что цифровая экономика может способствовать экономическому росту и устойчивому развитию. Корпорация Huawei составила Индекс глобальной связанности 2016 года, который показывает уровень цифровой экономики по странам [2]. Страны были распределены по трем группам: лидирующие, проходящие адаптацию и начинающие. Первую группу возглавили США, Сингапур и Швеция. В середине второй группы расположились Китай (23-е место), Россия (26-е место) и Бразилия (30-е место).

Задача правительства России – войти в группу лидирующих стран по цифровой экономике. Удастся ли это сделать в ближайшем будущем - не ясно. Пока «новый план ГОЭЛРО» не составлен. Настоящая статья является продолжением наших прежних работ, обзор которых дан в [3].

Далее, в разделе 2 приведены основные понятия цифровой экономики. Разделы 3 и 4 посвящены сети FirstNet и трудностям с ее созданием. В разделах 5 и 6 рассмотрены три поколения службы 911 и трудности с переходом на коммутацию пакетов. В разделе 7 приведена целевая архитектура оборонной информационной сети НАТО и указаны два примера сложностей: правительственная сеть DRSN как «родимое пятно» в среде AS-SIP (раздел 8) и пример неудачи с модернизацией информационной сети NATO (раздел 9). Российский опыт планируется рассмотреть в следующей статье данной серии.

II. Основные понятия цифровой экономики

Направление «Цифровая экономика» объединяет множество разделов народного хозяйства, которые связаны с широким применением компьютеров и средств связи (иначе говоря, инфокоммуникаций): умный дом, промышленный интернет, интернет вещей, безопасный город, электронное здоровье и множество других. Практически с понятием цифровая экономика связаны все сферы жизни. Мы же остановимся только на одной из множества областей – на внутреннюю безопасность государства как важнейшую область.

Начнем с основных понятий интернета вещей (Internet of Things, IoT) или, другими словами, сети вещей (Network of Things, NoT), как рекомендует NIST -

Статья получена 25 марта 2017

М.А. Шнепс-Шнеппе – AbavaNet (email:sneps@mail.ru).

В.П. Куприяновский – Национальный центр компетенций в области цифровой экономики (email: vpkupriyanovsky@gmail.com)

Д.Е.Намиот – МГУ имени М.В. Ломоносова (email:dnamiot@gmail.com).

С.П.Селезнев - Фактор ТС (e-mail: spseleznev@yandex.ru).

Институт стандартов и технологий США [4]. NIST вводит примитивы NoT (рис. 1), это:

1) датчик (Sensor),
2) агрегатор (Aggregator),
3) канал связи (Communication channel),
4) внешнее устройство (external utility, eUtility) и
5) решающий триггер (Decision trigger).

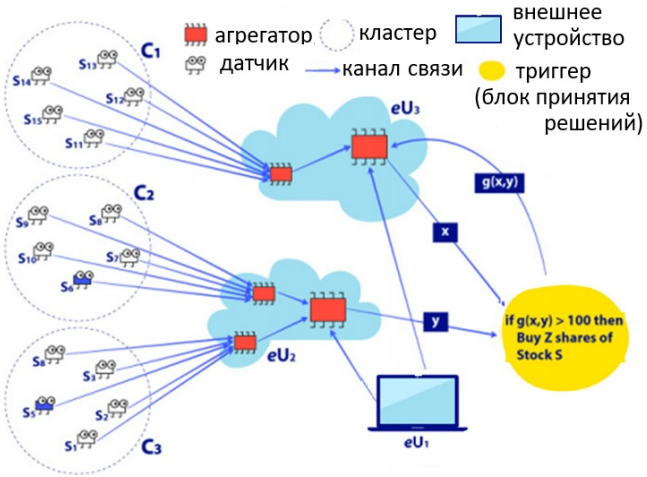

Рис. 1. Общая схема NoT: основные понятия, включая решающий триггер с обратной связью [4]

III. Что такое FirstNet

С точки зрения государства ключевым понятием цифровой экономики является обеспечение критической инфраструктуры государства и обеспечение сервисов безопасности общества (рис. 2).

Рис. 2. Роль критической инфокоммуникационной инфраструктуры в обеспечении сервисов NoT

На рис. 3 представлена подробная архитектура безопасности государства с тоски зрения приложений, что соответствует верхнему уровню на рис 2. Показаны прикладные области (приложения), которые упорядочены по государственной важности, принятой в США. Во всех этих областях имеются сенсоры, которые через средства связи общаются с приложениями, как показано на рис. 2.

Центральное место на рис. 3 занимает служба ПЕРВАЯ ПОМОЩЬ (First Responders), что по российскому законодательству соответствует аппаратно-программному комплексу «Безопасный город», и включает пожарную охрану, отравляющие материалы (газовая служба), экстренную медицинскую службу, правонарушения (полицию) и службу 911 (в России – 112).

Следующий круг - ЭКСТРЕННЫЕ СЛУЖБЫ. Всего насчитывается 12 разделов жизнедеятельности, которые охвачены экстренными службами: Грузоперевозки, Национальная гвардия, Спасатели, Управление экстренными службами, ЖКХ, НГО, Общественная экстренная помощь, Психические заболевания, Сельхоз/пищевая безопасность, Федеральное вмешательство, Общественная медпомощь, Госпитали.

Внешний круг - ПРЕДПРИЯТИЯ ЭКСТРЕННОГО ОБСЛУЖИВАНИЯ. В схеме указаны: Школы/приюты, Борьба с насилием, Общественные работы, Парки, Социальные службы, Служба погоды, Химические, нефтяные и газовые компании, Вспомогательные услуги охраны здоровья, Правительственные учреждения, Порты, Транспорт, Медиа, Контроль отравлений, Охрана животных и растений, Телекоммуникационные компании.

Рис. 3. Архитектура безопасности государства

Подробнее остановимся на центральном звене ПЕРВАЯ ПОМОЩЬ (First Responders), что по законам США обладает высшим приоритетом для обеспечения безопасности общества. Проблема национальной безопасности крайне обострилась после терактов 11 сентября 2001 года. После долгих 11 лет – в 2012 году – было создано Управление сетью первой помощи (First Responder Network Authority, сокращенно – FirstNet). Оно является независимым органом в рамках Национального управления по телекоммуникациям и информации (National Telecommunications and Information Administration), созданного для предоставления аварийным службам общенациональной высокоскоростной широкополосной сети, предназначенной для обеспечения общественной безопасности. Управление FirstNet утверждает, что она предоставит единую функционально совместимую платформу для экстренных и ежедневных сообщений для общественной безопасности.

FirstNet отвечает за создание базовой сети с пакетной коммутацией - ключевого компонента для обеспечения единой национальной совместимой платформы. Ядро сети настроено на взаимодействие с другими государственными, местными и федеральными сетями, включая 911 и Интернет. По данным компании FirstNet,

ядро сети служит гигантским зонтиком, охватывающим все Соединенные Штаты. Ядро подключено к сетям радиодоступа в каждом штате через транзитный уровень сети.

Первоначальное моделирование показало, что необходимы десятки тысяч базовых радиостанций для охвата, по меньшей мере, 99% населения и национальной сети автомагистралей.

Для пользователей FirstNet будет разработано все - от смартфонов до ноутбуков, планшетов, разнообразных специализированных устройств (рис. 4). Цель состоит в том, чтобы создавать устройства, достаточно прочные, чтобы выдерживать многие экологические проблемы общественной безопасности, но при этом быть легкими в использовании и удобными в переноске. Устройства также должны быть безопасными. Транспортная сеть переносит пользовательский трафик, такой как голос, данные и видео, и сигнализацию от радиостанций в базовую сеть.

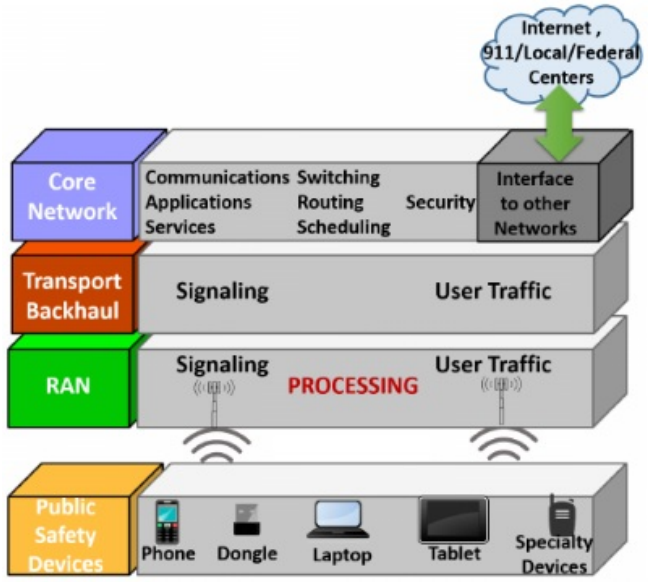

Рис. 4. Инфраструктура FirstNet [5]

Для сети FirstNet в 2012 году выделен общенациональный спектр в области 700 МГц (рис. 5), чтобы обеспечить безопасную связь для населения и аварийных служб. Этим был положен конец многолетним спорам о взаимодействии сетей связи при предоставлении экстренных услуг населению.

Предполагается, что сеть FirstNet должна строиться по техническим требованиям LTE. На данный момент для сети FirstNet выделена полоса 20 МГц. Точнее, для широкополосной связи выделены частоты от 758 до 768 МГц и от 788 до 798 МГц. Для узкополосной местной связи (передачи голоса) выделены частоты от 769 до 775 МГц и от 799 до 805 МГц.

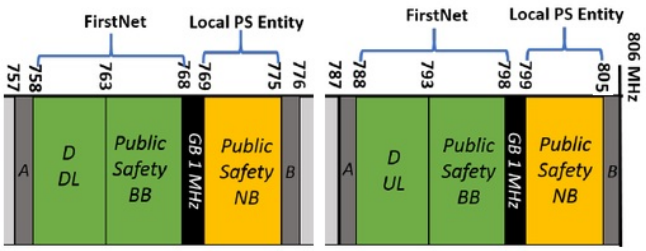

Рис. 5. FirstNet: общенациональный спектр в области 700 МГц шириной в 20 МГц

IV. Трудности с созданием сети FirstNet

В 2016 году в журнале Atlantic появилась негативная статья о FirstNet: «Сеть стоимостью в 47 миллиардов долларов, которая уже устарела» [6]. Статья ссылается на отчет Счетной палаты США (U.S. Government Accountability Office), мол – бесцельно истрачены от 12 до 47 млрд. долларов. Действительно, разработка сети FirstNet и экстренной сети NG9-1-1 продвигалась чрезвычайно медленно. Решение о создании FirstNet обсуждалось еще 15 лет назад – сразу после терактов 2001 года, но технические решения даже не сформулированы.

Сошлемся на документ Конгресса США [7]. В чем причина медленного прогресса FirstNet?

Управление FirstNet, мол, утверждает, что федеральная сеть является «единственным решением», что и является неудачей на рынке телекоммуникаций. Предлагается использовать выделенные частоты и для других нужд в сельских или отдаленных районах, кроме экстренной помощи. Эксперты полагают, что в дополнение к обеспечению общественной безопасности, мобильная сеть в небольших населенных пунктах может поддерживать, например, улучшение транспортной системы, образование, поиск работы, управление сельским и лесным хозяйством, повышение эффективности муниципальных органов власти и услуг и экономический рост.

И вот, наконец, решение по сети FirstNet сдвинулось с мертвой точки – 30 марта 2017 г. объявлено [8], что компания AT&T официально выбрана в качестве коммерческого партнера, который будет строить и поддерживать общенациональную сеть LTE для сети общественной безопасности First Responders. Соисполнителями работ AT&T по сети FirstNet названы компании Motorola Solutions, General Dynamics, Sapient Consulting и Inmarsat Government.

AT&T теперь должен представить сетевой план губернаторам всех 50 штатов, пяти территориям США и округу Колумбия, охваченному FirstNet [9]. Эти губернаторы должны решить в течение 90 дней, хотят ли они участвовать в FirstNet или отказываются от сети. В случае, если они откажутся, эти штаты должны затем разработать и построить свою собственную сеть радиодоступа, которая должна взаимодействовать с остальной частью сети и ядром FirstNet.

Будущее покажет, сможет ли AT&T с соисполнителями Motorola Solutions, General Dynamics,

Sapient Consulting и Inmarsat Government совершить столь неудачный до сих пор проект сети FirstNet.

V. Три поколения службы 911

В США экстренные вызовы обслуживаются по номеру 911, и в простейшем случае это вызовы от абонента фиксированной линии. Дополнительные требования к операторам мобильной связи объединены названием E911 (Enhanced 911), и это относится ко второму поколению службы 911. Третье, новейшее поколение службы экстренных вызовов имеет название NG911, и оно относится к коммутации пакетов.

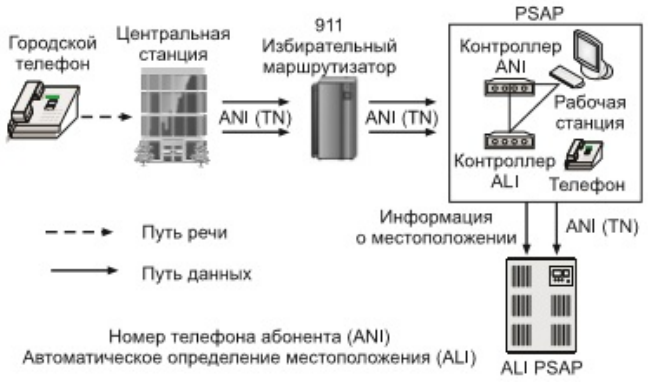

Рис. 6. Прохождение экстренного вызова от абонента фиксированной линии: простейший вариант

Как и в России, внедрение единого номера для фиксированных и мобильных абонентов в США проходит с трудностями, особенно определение номера вызывающего абонента и его местоположения. Но чему у них следовало бы поучиться, так это четкости действий Федеральной комиссии связи FCC. Например, дополнительные требования к операторам мобильной связи E911 включают условие — передать в ЦОВ номер вызывающего абонента и номер базовой станции мобильной сети в течение 6 мин после запроса из ЦОВ, и к 31 декабря 2005 г. это требование должно было быть выполнено в 95% случаев. За невыполнение этого требования операторы были оштрафованы. Например, в сети Sprint Nextel местоположение вызовов удалось определить только в 81 % случаев, за что компанию оштрафовали на 1,33 млн. долларов. В настоящее время действует требование определить координаты вызывающего абонента с точностью до 300 м. Это полагалось внедрить к 11 сентября 2008 г., но по жалобам операторов связи срок перенесли на четыре года — на 11 сентября 2012 г.

Рис. 7. Система Enhanced 911

Подобные же жесткие требования к определению местоположения предъявляются и к VoIP-вызовам.

Новейшее поколение службы экстренных вызовов NG911 [10] будет реализовано в IP-сети. План NG911 стартовал в 2000 г., и к 2008 г. были завершены пилотные проекты. Но когда План NG911 будет реализован в полном объеме, — это сегодня определить трудно, так как служба первой помощи не хочет рисковать. Переход на интернет-технологии может сопровождаться сбоями в сети, как уже ранее случалось при попытке внедрить сигнализацию SS7. Рисунок показывает схему стыковки экстренной службы NG911 с существующей службой 911. В системе NG911 требуется обеспечить возможность любых сообщений реального времени, т.е. наряду с телефонным вызовом обеспечить передачу текста, данных, изображений и видео. Обратим внимание на телематические вызовы. Это относится к M2M коммуникациям, в частности к противопожарным и охранным службам.

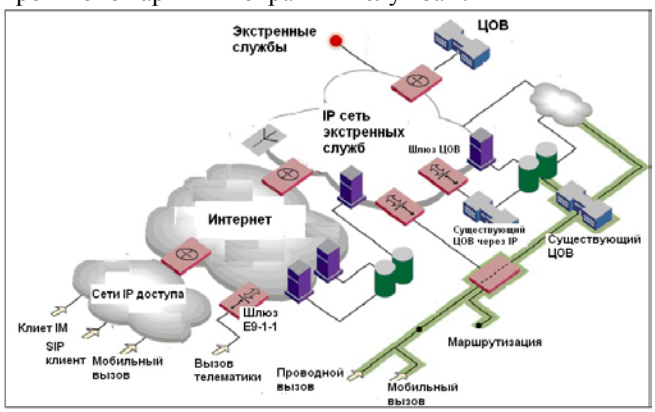

Рис. 8. Новое поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 911

VI. Трудности с созданием сети NG911

Трудности внедрения NG911 обусловлены, прежде всего, риском перехода на IP-протокол. 31 января 2014 г. Федеральная комиссия связи издала документ о поддержке операторов, которые намерены отказаться от коммутации каналов (по технологии TDM) в пользу IP-протокола [11]. Кроме того, FCC заказала юридической фирме оценку возможных рисков такого перехода, что, к сожалению, не рассеяла опасения экстренных служб. 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 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 крупный ущерб репутации компании.

Другой подобный коллапс случился 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 их приравняли к угрозе национальной безопасности страны. Системе SS7 «был вынесен 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?

Как сказано в докладе Конгрессу США [7], до настоящего времени система 911 построена на инфраструктуре аналоговых технологий, которая не поддерживает многие функции, которые большинство американцев ожидают от службы первой помощи. Следует модернизировать центры 911, известных как пункты общественного реагирования (Public Safety Answering Points, PSAP). Новые технологии, именуемые в совокупности «Новое поколение 911» или «NG911», должны включать стандарты Интернет-протокола.

Признавая важность предоставления эффективных услуг 911, Конгресс ранее принял три основных законопроекта, поддерживающих усовершенствование обработки экстренных вызовов:

1) Закон о беспроводной связи и общественной безопасности от 1999 года установил 911 как единый номер для вызова в чрезвычайных ситуациях и дал полномочия Федеральной комиссии связи (FCC) регулировать многие аспекты экстренной службы.

2) Закон ENHANCE 911 от 2004 года - для мобильных пользователей и требований к местоположению.

3) В третьем документе – в Законе об улучшении сети 911 от 2008 года - требовалось подготовить Национальный план перехода на экстренную сеть с поддержкой IP-протокол.

Как оказалось, наибольшим тормозом внедрения NG911 оказались новые требования по киберзащите [13]. Традиционные службы 911 до сих пор работают по «старым» телефонным сетями для голосовой связи и используют программное обеспечение, такое как автоматизированные системы диспетчеризации, которые работают в закрытых внутренних сетях, практически не связанных с другими системами. Ограниченные средства входа в традиционную сеть 911 значительно ограничивали потенциальные кибер-атаки, и малое количество кибер-риска можно было легко контролировать. Соединения NG911 представляют новые векторы для атаки, которые могут нарушать или отключать операции PSAP, затрудняя управление кибер-рисками на всех уровнях государственного управления.

Например, злоумышленники нарушают доступ к традиционным системам 911, используя автонаборщики. Они подключаются к телефонным линиям PSAP и вызывают перегрузку, не допуская прохождения законных вызовов 911 и доступа к базам данных, в том числе к записям о местоположении. Это называется атаками на отказ в обслуживании по телефону (Telephone Denial of Service, TDoS).

Полный обзор стандартов NG911 можно найти на веб-сайте Национальной программы 911 [14]. См. также работы [15, 16].

VII. Целевая архитектура оборонной информационной сети НАТО

Укажем на трудности перехода от сети коммутации каналов в сети DISN (Defence Information Service Network), где господствует протокол SS7, к новой сети с коммутации пакетов и протоколу SIP (или к AS-SIP). Этот переход потребовал установки шлюзов — программных коммутаторов MFSS (MultiFunction SoftSwitch).

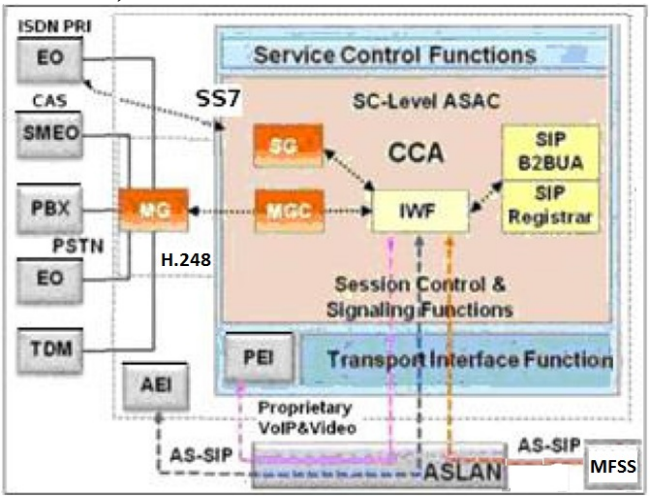

Рис. 9. Многофункциональный программный коммутатор MFSS – основа перехода от TDM к IP

Напомним, что SoftSwitch обеспечивает переход от сети коммутации каналов к сети коммутации пакетов, но не заменяет саму сеть коммутации каналов. Он только управляет согласованием протоколов сигнализации SIP и SS7 (посредством шлюза SG) и преобразованием IP пакетов в TDM посылки (посредством шлюза MGC). Объясним, как многофункциональный софтсвич MFSS управляет вызовами (рис. 9 слева):

- В сторону внешней публичной сети PSTN или сети ISDN (Integrated Services Digital Network) используется функция IWF (ISUP-SIP interworking function).
- Контроллер MFSS обеспечивает «старые» сигнализации PSTN/ISDN, включая ISUP, CCS7/SS7 и CAS (Channel Associated Signaling).
- MFSS действует как медиашлюз (MG) между TDM каналами и IP каналами. Контроллер MGC управляет медиашлюзом – посредством протокола H.248.
- Шлюз сигнализации SG (Signaling Gateway) обеспечивает взаимодействие между SS7 и SIP.

Укажем на различия в протоколе SIP (Session Initiation Protocol) и в его расширенной версии AS-SIP (Assured

Service – Session Initiation Protocol). Главными недостатками протокола SIP являются трудности с обслуживанием приоритетных вызовов, что важно для военных применений, для экстренной службы, а также трудности по обеспечению секретности (особенно в условиях кибервойны). Поэтому по заказу МО США разработали защищенный протокол AS-SIP. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC.

По мере «старения» сети DISN традиционные электронные АТС будут заменены на маршрутизаторы с сигнализацией AS-SIP, но не полностью, так как на правительственной сети DRSN сохранятся ISDN каналы (см. рис 10 справа наверху).

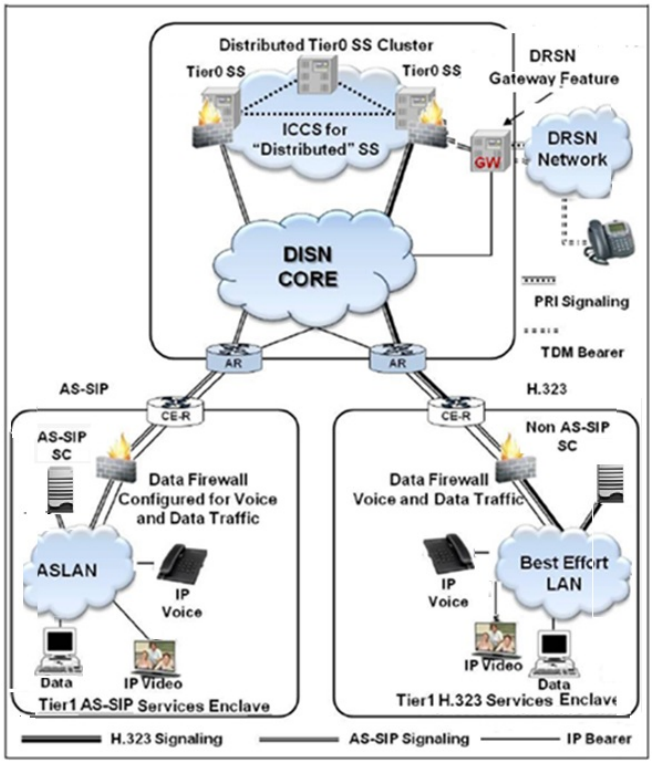

Рис. 10. Двухуровневая защищенная гибридная сеть DISN для передачи голоса, данных и видео

Целевая архитектура сети DISN, которая создается в настоящее время, должна содержать IP маршрутизаторы двух уровней: Tier 0 и Tier 1 (рис. 10). Кластеры уровня Tier 0 отвечают за неуязвимость всей сети DISN. Каждый кластер содержит по три маршрутизатора, соединенных протоколом ICCS (Intra-Cluster Communication Signaling), по которому автоматически обновляются их базы данных. Кластер по существу представляет собой один распределенный маршрутизатор. Требуется, чтобы задержка в обмене содержимом баз данных не превышала 40 мс. Так как передача сигнала занимает 6 микросекунд на 1 км, то расстояние между маршрутизаторами не может превышать 6600 км. На нижнем, втором уровне DISN сети Tier 1 находятся два типа локальных сетей: защищенная локальная сеть ASLAN, работающая по протоколу AS-SIP, и традиционная LAN, работающая по протоколу H.323 (который является аналогом ISDN в IP сети).

VIII. Правительственная сеть DRSN как «родимое пятно» в среде AS-SIP

Сеть DRSN (Defense Red Switch Network) — это выделенная телефонная сеть, которая обеспечивает управление вооруженными силами США. Эта сеть приобрела особую значимость после событий 11 сентября 2001 г. и создания Министерства внутренней безопасности (U.S. Department of Homeland Security, DHS).

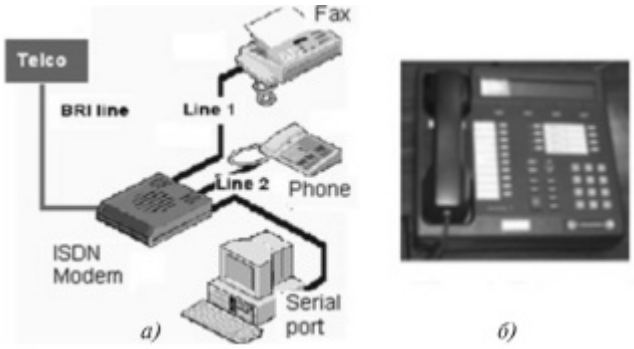

Рис. 11. Иллюстрация использования ISDN линии (а) и «красный» телефон (б).

«Красный телефон» (Secure Terminal Equipment, STE) подключается к сети по ISDN линии и работает на скорости 128 кбит/с. Для передачи данных и факсимиле встроен RS-232 порт. Вся криптографическая информация хранится на карте (щель для карты — справа внизу на изображении телефона). Обратите внимание на 4 кнопки наверху телефона — для выбора приоритетности разговора. «Красные телефоны» общаются по протоколу SCIP (Secure Communications Interoperability Protocol). Это — межнациональный протокол сил НАТО для обеспечения закрытой передачи речи и данных по множеству сетей: наземная телефонная сеть, радио военного назначения, спутниковая связь, интернет-телефония, разные стандарты мобильных сетей.

Рис. 12. Схема правительственной сети DRSN

IX. Пример неудачи с модернизацией информационной сети NATO

В июне 2012 г. компания Lockheed Martin выиграла крупнейший тендер на разработку IT-сервисов управления сетью DISN (Global Services Management-Operations, GSM-O). На этом тендере Lockheed Martin опередила компанию SAIC (Science Applications International Corp.), которая поставляла подобные услуги Пентагону в продолжении 15 лет. Естественно, что SAIC резко протестовала против решения Пентагона, но после длительного разбирательства в Правительстве решение Пентагона не было отменено [17].

Суть контракта GSM-O состоит в модернизации системы управления сетью DISN по требованиям киберзащиты. Стоимость работ составляет громадную сумму — 4,6 млрд. долл. в течение 7 лет. Соисполнителями контракта GSM-O являются компании AT&T, ACS, Serco, BAE Systems, Mantech и ряд других специализированных и малых предприятий. В 2013 г. команда GSM-O приступила к изучению состояния четырех центров управления сетью GIG, которые несут ответственность за техническое обслуживание и бесперебойную работу всех компьютерных сетей Пентагона — 8100 компьютерных систем в более чем 460 местах в мире, которые, в свою очередь, соединены 46000 кабелями. Первое дело по контракту состояло в модернизации системы управления компьютерными сетями GIG. Было принято решение о консолидации операционных центров — с четырех до двух (рис. 13). Расширяются центры на военно-воздушных базах Scott (штат Иллинойс) и Hickam на Гавайях, а центры в Бахрейне и Германии закрываются.

Рис. 13. План консолидации операционных центров DISN — с четырех до двух

Наиболее сложным делом оказалось обеспечение киберзащиты, т.е. создание единой архитектуры безопасности SSA. С этой целью следует установить региональные стеки безопасности JRSS, которые, по сути, представляют собой IP маршрутизаторы со сложным комплексом программ киберзащиты. Первый стек JRSS был установлен и успешно эксплуатируется на военной базе Сан-Антонио, штат Техас. В 2014 году велась работу по установке 11 стеков JRSS на территории США, трех стеков на Ближнем Востоке и одного – в Германии. Общий объем работ включает установку 24 стеков JRSS на служебной сети NIPRNet и 25 стеков JRSS на секретной сети SIPRNet. К 2019 году планируется на эти стеки перенести программы кибербезопасности, которые сейчас размещены в более чем 400 местах. Состояние дел по контракту GSM-O на 2014 год хорошо изложено в статье [18].

Задачи кибербезопасности являются высшим приоритетом Пентагона, но отсутствие необходимых стандартов тормозит выполнение всей программы GSM-O, прежде всего, тормозит создание общих датацентров и внедрение унифицированных сервисов (Unified Capabilities). Остаются также нерешенными задачи использования облаков военного ведомства и перенос какой-то части приложений на коммерческие облака.

Но уже через два года после начала работ по контракту GSM-O – в 2015 году – мир телекоммуникаций потрясла новость: Lockheed Martin не справляется с модернизацией управления сетью DISN, то есть с выполнением многомиллиардного контракта GSM-O, и свое подразделение LM Information and Global Solutions продает конкурирующей фирме Leidos. Провалом работ, скорее всего, послужила неспособность набрать разработчиков, способных сочетать «старое» оборудование коммутации каналов с новейшими системами пакетной коммутации, тем более с учетом новых требований киберзащиты и подключения стеков JRSS.

Будут ли грандиозные планы Пентагона выполнены?

X. Выводы

Перед связистами всего мира стоит одна и та же задача – как перейти от коммутации каналов (КК) к коммутации пакетов (КП). Операторы связи взяли ориентацию на “All-over-IP” с надеждой заработать на мультимедийных услугах. А главным, заинтересованным «игроком» на этом поле смены парадигмы телекоммуникаций является, прежде всего, индустрия: производители оборудования коммутации пакетов собираются заработать многие миллиарды долларов и платят инженерам и журналистам многие миллионы за популяризацию новой парадигмы. Но жизнь вносит коррективы в этом стремлении к наживе. Накапливаются факты о том, что обе технологии – КК и КП – будут еще долго сосуществовать и ставят под сомнения саму целесообразность смены парадигмы телекоммуникаций.

Приведенные выше примеры на опыте телекоммуникационных сетей США показывают трудности перехода от коммутации каналов к коммутации пакетов, а именно: рассмотрена сеть первой помощи FirstNet, экстренной службы NG911 и оборонная информационная сеть Пентагона.

БИБЛИОГРАФИЯ

[1] Гвоздецкий В. План ГОЭРЛО. Мифы и реальность //Наука и жизнь. – 2001. – №. 5. – С. 102-109.

[2] Цифровая экономика для устойчивого экономического роста //Мосты. -2016.-Т. 9.- №. 4.

[3] В. П. Куприяновский, Д. Е. Намиот, С. А. Синягов, А. П. Добрынин. О работах по цифровой экономике // Современные

информационные технологии и ИТ-образование. — 2016. — Т. 12, № 1. — С. 243–249.

[4] Jeffrey Voas. Networks of ‘Things’. NIST Special Publication 800-183. July 2016

[5] Phillip Tracy. Understanding FirstNet, the post-9/11 public safety initiative, August 31, 2016 http://www.rcrwireless.com/20160831/fundamentals/firstnet-tag31-tag99, Retrieved: Apr, 2017

[6] 47 billion network https://www.theatlantic.com/magazine/archive/2016/09/the-47-billion-network-thats-already-obsolete/492764/ Retrieved: Apr, 2017

[7] Lennard G. Kruger. The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress, January 26, 2017, Congressional Research Service 7-5700 http://www.crs.gov

[8] AT&T wins FirstNet network contract, March 30, 2017. https://forums.radioreference.com/community-announcements-news/350888-t-wins-firstnet-network-contract.html Retrieved: Apr, 2017

[9] FirstNet's national public safety network may finally become a reality Mar 31, 2017 https://www.policeone.com/ Retrieved: Apr, 2017

[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: Apr, 2017.

[13] FCC White Paper. Cybersecurity Risk Reduction. Public Safety & Homeland Security Bureau. January 18, 2017

[14] 911 Standards http://www.911.gov/pdf/NG911-Standards-Identification-and-Analysis-March2015.pdf. Retrieved: Apr, 2017

[15] Шнепс-Шнеппе М. А. и др. О телекоммуникационной инфраструктуре комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 6. – С. 17-31.

[16] Шнепс-Шнеппе М. А. и др. О кибербезопасности критической инфраструктуры государства //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 7. – С. 22-31.

[17] GIG-a-Bite: Lockheed Takes $4.6 Billion Contract from SAIC http://www.defenseindustrydaily.com/gig-a-bite-lockheed-takes-46contract-fromsaic-07452/ Retrieved: Apr, 2017

[18] S. Meloni. The Future of the Joint Information Environment (JIE), SEPT 24, 2014 http://blog.immixgroup.com/2014/09/24/the-futureof-the-joint-information-environment-jie Retrieved: Apr, 2017

[19] Шнепс-Шнеппе М. А. и др. К системному проектированию Системы 112 и комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 9.- С.44-63.

Telecommunications as a decisive link in the digital economy. Experience of the USA

Manfred Sneps-Sneppe, Vasily Kupriyanovsky, Dmitry Namiot, Sergey Seleznev

Abstract – This article is the first in a series of papers devoted to the role of telecommunications in the digital economy. By all indications, it is telecommunications that will play a decisive role in the digital economy. The world's telecom companies have the same task - how to completely replace switching channels infrastructure to switching packets. The difficulties of the transfer from circuit switching to packet switching are illustrated by examples from the experience of US telecommunications networks, namely FirstNet's first-aid network, emergency service NG911 and the Pentagon's defense information network. Nowadays, we have more and more facts that both technologies will continue to coexist for a long time. This raises doubts about the expediency of changing the telecommunications paradigm.

Keywords – Internet of Things, Network of Things, Digital Economy, FirstNet, 911, DISN, DRSN, AS-SIP protocol