Телекоммуникации как решающее звено цифровой экономики. Опыт России

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

***Аннотация* – Обсуждаются задачи цифровой экономики и роль телекоммуникаций. В части 1 проведен анализ развития сетей связи, советских систем связи и управления: ЕАСС и ЕГСВЦ, разработки телефонной техники в советское время: КЭАМТС и ЕССКТ; как в постсоветский период проходило внедрение сигнализации ОКС-7 и интеллектуальной сети. В части 2 рассмотрены очередные задачи: создание системы экстренных вызовов «112», обеспечение кибербезопасности критической инфраструктуры, создание аппаратно-программного комплекса «Безопасный город», ведущая роль «Ростелекома» в построении информационного общества, две стратегии связистов России – продолжение строительства сетей связи средствами иностранных производителей или развитие импортозамещения и собственного производства.**

***Ключевые слова* — цифровая экономика; ЕАСС; ЕГСВЦ; Кварц; ЕССКТ; ОКС-7; интеллектуальная сеть; система экстренных вызовов «112»; критическая инфраструктура; АПК «Безопасный город»; Ростелеком; информационное общество; импортозамещение**

I. Часть 1. Анализ развития сетей связи

Программа цифровой экономики как новый План 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.

Пора возродить производство средств связи. В настоящее время подавляющее большинство средств связи в России имеют иностранное происхождение. Например, сети «Ростелекома» сегодня стали ареной борьбы «за сферы влияния» двух американских компаний – Cisco и Juniper. С ними конкурирует китайская компания Huawei. Рисунок раскрывает состояние мирового рынка телекоммуникационного оборудования. Участие России тут близко к нулю. В последнее десятилетие лидирует Китай – и в большой мере за счет того, что производство этого оборудования США перенесли в Китай. А ведь в советское время было мощное Министерство промышленности средств связи.

Статья получена 10 мая 2017

И.А.Соколов - Федеральный исследовательский центр «Информатика и управление» РАН (email:isokolov@ipiran.ru)

М.А.Шнепс-Шнеппе АбаваНет (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)

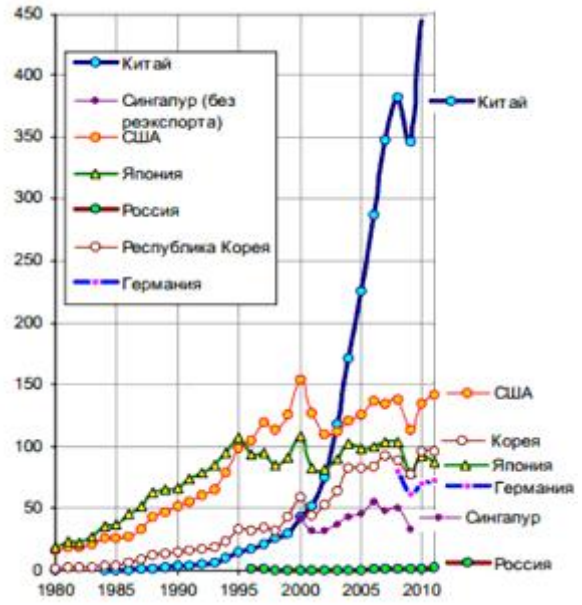


Рис. 1. Объемы экспорта офисного и телекоммуникационного оборудования в мире, млрд. долл [3] .

Важнейшим проектом «Ростелекома» является высокоскоростная IP-магистраль, которая построена на базе ресурсов первичной сети по технологии MPLS (Multi-protocol Label Switching), и обеспечивает конвергенцию услуг по передаче видео, речи и данных. IP/MPLS-инфраструктура имеет свыше 350 точек доступа на всей территории России, десять опорных и около 150 региональных узлов в регионах РФ. Использованы маршрутизаторы компании Juniper: магистральны маршрутизаторы T1600 производительностью до 1,6 Тб/с и менее мощные пограничные маршрутизаторы. Общая протяженность магистральной сети составляет более 40 тыс. км, пропускная способность достигает 1 Тбит/с, емкость внешних каналов составляет 200 Гбит/с. Компания присутствует и на зарубежных узлах (в Стокгольме, Лондоне, Гонконге, Франкфурте, Амстердаме), имеет сеть собственных датацентров в Москве, Казани, Екатеринбурге, Новосибирске, Хабаровске.

II. Сеть IP/MPLS – гордость «Ростелекома».

О разоблачениях Сноудена. Благодаря разоблачениям Э. Сноудена (Washington Post, 30.98.2013), стало известно о шпионской программе GENIE, разработанной Агентством национальной безопасности (АНБ), которая проникает в зарубежные сети и ставит их под контроль США. К концу 2013 года было заражено как минимум 85 тыс. стратегических серверов. Сейчас АНБ внедряет более мощную систему – TURBINE, которая будет управлять имплантами для сбора разведывательной информации в автоматическом режиме. К началу 2014 года она заразила до 100 тыс. серверов [4]. Система TURBINE составляет основу крупнейшей программы кибервойны Quantum, которую АНБ реализует в содружестве с телефонными операторами и пользуясь услугами мощной серверной сети. Головной офис Quantum находится в штаб-квартире АНБ (Форт Мид, штат Мэриленд), а отделения - в Японии и Великобритании.

В свете разоблачений Э. Сноудена и в условиях кибервойны возникает провокационный вопрос: не является ли сеть IP/MPLS «Ростелекома» американским кибероружием?

Отсутствие системных исследований по телекоммуникациям. Телекоммуникации представляют собой яркий пример технологий двойного применения. В мирное время телекоммуникации входят в сферу ответственности сил гражданской обороны и, по идее, должны обеспечивать мобилизационную готовность населения на случай чрезвычайных ситуаций. В военное же время системы связи могут перейти под полный контроль военного ведомства. По крайней мере, службы Ростелекома, как федерального оператора должны иметь двойное подчинение и, например, при крупных чрезвычайных мероприятиях Центры обслуживания вызовов Ростелекома, а также сети мобильных операторов должны работать на нужды МЧС.

Чем характерен текущий момент в российской отрасли связи, в отрасли народного хозяйства, важнейшей как для гражданских, так и специальных нужд [5]:

1) Полноценные системные исследования путей модернизации сетей связи не ведутся в России, как минимум, два десятилетия.

2) Операторы связи и Поставщики услуг копируют решения, принятые в других странах, без адекватной оценки их положительных и отрицательных сторон.

3) Не учитывается приемлемость иностранных решений для различных групп пользователей, прежде всего сетей специального назначения.

В настоящее время, подавляющее большинство средств связи в России имеют иностранное происхождение. Действительно, на базе лучшего иностранного оборудования можно строить современные сети. Но, к сожалению, эта стратегия приводит к зависимости от этих компаний на необозримое будущее. И как быть с безопасностью страны, как преодолеть международные санкции?

В предыдущей статье [6] мы рассматривали телекоммуникации как решающее звено цифровой экономики, используя опыт США. В настоящей же статье обратимся к состоянию отрасли связи в России. Учитывая стратегическую роль средств связи для суверенитета страны и вытекающую отсюда важность возрождения промышленности средств связи, начнем с анализа советского периода (Часть 1) и попытаемся сформулировать очередные задачи в области инфокоммуникаций в свете Государственной программы цифровой экономики (Часть 2).

Настоящая статья является продолжением наших прежних работ, обзор которых дан в [7].

III. О СОВЕТСКИХ СИСТЕМАХ СВЯЗИ И УПРАВЛЕНИЯ

Единая автоматизированная сеть связи. В наши дни, согласно Федеральному Закону "О связи", применяются два термина: «сеть связи общего пользования (ССОП)» и «взаимоувязанная сеть связи Российской Федерации». Как гласит Статья 7 Закона "О связи",

«Сеть связи общего пользования как составная часть взаимоувязанной сети связи Российской Федерации предназначена для предоставления услуг связи всем физическим и юридическим лицам на территории Российской Федерации и включает в себя все сети электросвязи, находящиеся под юрисдикцией Российской Федерации, кроме выделенных и ведомственных сетей связи, независимо от их принадлежности и форм собственности. Ответственность за функционирование и развитие сети связи общего пользования возлагается на федеральные органы исполнительной власти в области связи».

В советское время использовался другой термин – «Единая автоматизированная сеть связи (ЕАСС)», а главное, – было множество томов с изложением сути ЕАСС. К сожалению, до сих пор не разработаны документы, регламентирующие работу ССОП. На наш взгляд, подошло время положение исправить. Пора разработать документы, регламентирующие работу ССОП, точнее, пора разрабатывать новую, постсоветскую версию ЕАСС. В поиске подсказки заглянем в историю – как все это делалось в советское время.

Единая автоматизированная сеть связи (ЕАСС) сыграла большую роль в развитии электросвязи и информатизации страны. На ее основе решались сложнейшие задачи по передаче и распределению различных видов информации для народного хозяйства, населения и обороны. На базе ЕАСС и Государственной сети вычислительных центров (ГСВЦ) формировалась Общегосударственная система сбора и обработки информации для учета, планирования и управления народным хозяйством (ОГАС), объединявшая отраслевые и территориальные автоматизированные системы управления (АСУ) основных министерств, ведомств и союзных республик.

Судя по опубликованным данным, – пишет В.М. Дмитраченко [8] – основные принципы создания Единой сети связи (ЕСС) впервые в мире выдвинул известный советский ученый академик АН СССР А. А. Харкевич в статье "Информация и техника" (журнал "Коммунист", 1962, № 12), вошедшей в 3-томный сборник его трудов (М., Наука, 1975). В этой статье А. А. Харкевич обосновал основные пути организационно-технического объединения сетей, предугадав важность цифровых методов передачи и коммутации различных видов информации в цифровой форме. ЕСС, по его мнению, должны представлять собой крупнейший инженерный комплекс, который объединит всю существующую сеть связи и будет развиваться путем планомерного ее наращивания в органическом взаимодействии с системой вычислительных, управляющих и справочных центров. Разработкой научных основ ЕАСС занимался возглавляемый А. А. Харкевичем Институт проблем передачи информации Академии наук СССР. В 2004 году институту присвоено имя А. А. Харкевича.

В 1963 г. постановлением ЦК КПСС и СМ СССР создание ЕАСС было возложено на Минсвязи СССР, при котором был образован Межведомственный координационный совет (МВКС). МВКС согласовывал основные принципы построения ЕАСС, этапы ее развития, необходимые НИОКР, объемы производства оборудования. Большое внимание уделялось разработке и утверждению норм и правил, обеспечивающих надежность сети и высокое качество передаваемой информации. Эти нормы и правила соответствовали рекомендациям международных организаций по электросвязи.

Научные основы развития ЕАСС разрабатывал Центральный научно-исследовательский институт связи (ЦНИИС) Минсвязи СССР. Первый проект ЕАСС был завершен в 1965 г. под руководством С. А. Аджемова, начальника ЦНИИС.

В последующие годы комплексные планы составлялись на каждую пятилетку. С 1980 г. прогноз развития связи дополнялся "Комплексными программами научно-технического прогресса СССР" на 1980-2000 гг., затем на 1986-2005 гг. и на 1991-2010 гг.

Единая государственная сеть вычислительных центров и трагедия полковника Китова. По мнению В.М. Дмитраченко, в бытность видного сотрудника ЦНИИС и Минсвязи СССР, принципы создания ОГАС и ГСВЦ в СССР возникли в 1962 г. на базе идей академика В. М. Глушкова о "безбумажной информатике", обобщенных в его последнем фундаментальном труде "Основы безбумажной информатики" (М., Наука, 1982). Уже в 1964 г. под его руководством был разработан первый эскизный проект Единой государственной сети вычислительных центров (ЕГСВЦ, позднее ГСВЦ), предназначенной для перестройки на основе безбумажной технологии организационно-экономического управления на всех уровнях (от отдельных предприятий и учреждений до Госплана СССР).

С практической же реализацией планов ОГАС и с внедрением вычислительной техники в СССР вообще, оказывается, дела шли не так гладко. В этой связи следует вспомнить имя инженер-полковника Анатолия Ивановича Китова (1920-2010). Он первый, кто поставил перед высшим руководством Советского Союза и научной общественностью вопрос о необходимости управления экономикой СССР в масштабах всей страны на основе повсеместного применения электронных вычислительных машин (ЭВМ). Он предложил создать Общегосударственную автоматизированную систему управления на основе ЕГСВЦ. Вот как излагает историю ЭВМ Б. Н. Малиновский [9] - «осенью 1959 года А. И. Китову пришла в голову идея о целесообразности создания единой автоматизированной системы

управления для Вооружённых Сил и народного хозяйства страны на базе общей сети вычислительных центров, создаваемых и обслуживаемых Министерством обороны. При большом отставании в производстве ЭВМ от США концентрация выпускаемых машин в мощных вычислительных центрах и их чёткая и надёжная эксплуатация военным персоналом позволили бы сделать резкий скачок в использовании ЭВМ».

Оказывается, идеи Китова намного лет опередили время: он описывал то, что в США потом легло в основу глобальной информационной системы вооруженных сил GIG. Научный руководитель НПО «Квант», академик РАН В. К. Левин пишет [10]:

«*Большой резонанс имело письмо Анатолия Ивановича Китова в правительственные инстанции в 1959 г., где им было выдвинуто предложение об объединении между собой ЭВМ, распределённых на территории всей страны, и о создании тем самым сети ВЦ общегосударственного значения в интересах народного хозяйства и обороны. По существу, предопределялось то, что впоследствии получило мировое развитие и сейчас называется Grid-технологиями − объединение многих вычислительных ресурсов для решения задач глобального масштаба*».

Общение А.И. Китова с высшим руководством страны обернулось ему личным несчастьем. 7 января 1959 г. он послал письмо в ЦК КПСС главе СССР Н. С. Хрущёву. В этом письме Китов предложил создать общенациональную компьютерную сеть многоцелевого назначения, предназначенную для планирования и управления экономикой в масштабе всей страны.

Осенью 1959 г. Китов послал Хрущёву второе письмо, в котором он предложил способ существенного сокращения затрат государства на создание Общегосударственной автоматизированной системы управления экономикой СССР на основе ЕГСВЦ. Это второе письмо Китова содержало разработанный им ещё более радикальный 200-страничный проект «Красная книга» — проект создания Общесоюзной сети ВЦ двойного назначения — военного и гражданского, для управления экономикой страны в мирное время и Вооружёнными силами СССР в военное.

И далее, в 1959—1962 гг. Китов продолжал отстаивать и пропагандировать свои взгляды в докладах и публикациях. Китов убеждал руководство страны, что реализация его проекта «Красная книга» позволит СССР обогнать США в области разработки и использования вычислительной техники, не догоняя их (как он говорил «Обогнать, не догоняя»). У Китова нашлись уважаемые покровители в лице академика адмирала А.И. Берга [11] (Аксель Иванович Берг (1893 - 1979) - адмирал-инженер, заместитель министра обороны СССР. Академик АН СССР (1946). С 1959 — председатель научного совета по комплексной проблеме «Кибернетика» при Президиуме АН СССР. Возглавлял координацию исследований по кибернетике) и известного математика А. А. Ляпунова [12]. К сожалению, проект «Красная книга» был отвергнут, а сам Китов был подвергнут гонениям: его исключили из КПСС, сняли с должности начальника созданного им ВЦ-1 МО – без права занимать руководящие должности.

Гонения на кибернетику. Сегодня трудно представить атмосферу научной жизни 50х годов того века, в том числе представить, что было запрещено заниматься кибернетикой. Например, в «Философский словарь» 1954 года издания попала характеристика кибернетики как «реакционной лженауки», что заклеймило кибернетику и ученых, ею занимающихся. Откуда такое кощунство? Эту оценку можно объяснить тем, что кибернетика вторгалась в «святую святых» правящего аппарата — управление государством, что и вызывало категорическое неприятие. Уже через год ученые пытались дать отпор марксистам-ортодоксам, так как такое отношение к применениям ЭВМ тормозило развитие народного хозяйства. В 1955 году в журнале «Вопросы философии» вышла статья С. Л. Соболева, А. И. Китова и А. А. Ляпунова «Основные черты кибернетики» [13]. Тем не менее еще несколько лет ученые-кибернетики подвергались гонениям. Поломанная судьба А.И. Китова – яркий тому пример.

К научным страстям того времени относится дискуссия на тему "Может ли машина мыслить". 25 августа 1961 г. академик А.Н. Колмогоров – крупнейший математик XX века – выступил в МГУ с докладом "Автоматы и жизнь". Он обращался к аудитории с вопросом: можно ли построить машину, которую нельзя было бы отличить от человека? В завершении Андрей Николаевич говорил слова, которые и сегодня могут вызвать неприятие:

«*Человек является действительно сложной материальной системой, но системой конечной сложности и весьма ограниченного совершенства и поэтому доступной имитации. Это обстоятельство многим кажется унизительным и страшным*».

Оригинальные идеи А. И. Китова далее развил директор Института кибернетики АН УССР академик Виктор Михайлович Глушков (1923—1982). Он переосмыслил проект А. И. Китова и заручился в 1962 году поддержкой А. Н. Косыгина (работавшего в то время заместителем Председателя СМ СССР) о целесообразности проекта автоматизации управления советской экономикой. В стране началась масштабная кампания по созданию АСУ в государственных ведомствах и на предприятиях, которая продолжалась вплоть до Перестройки.

При создании документации проекта ОГАС следует выделить два периода времени: до и после перехода от территориальных методов управления экономикой СССР к отраслевым. С 1965 г. создание ОГАС начало проектироваться с учётом применяемых в СССР отраслевых методов управления экономикой. Планировалось, помимо территориальной системы Госснаба СССР, также создание территориальных АСУ союзных республик (РАСУ) во главе с вычислительными центрами (ВЦ) при республиканских Госпланах и территориальная сеть вычислительных

центров ЦСУ СССР. В связи с переходом от территориальной структуры управления к отраслевой, предполагалось, что ОГАС, будет базироваться на отраслевых АСУ (ОАСУ), которые планировались, чтобы обеспечить автоматизированное компьютерное экономическое управление в рамках каждой отдельной отрасли СССР, с одной стороны, и территориальных АСУ, принадлежащих Госснабу СССР, ЦСУ СССР и Госпланам союзных республик, с другой.

В дальнейшем, до 1991 г. продолжалась планомерная работа по созданию ОГАС, ГСВЦ, ЕАСС и ОГСПД, и эта громадная работа была прекращена в связи с переходом страны от социалистических методов управления экономикой к рыночным, что привело к разрушению промышленности в угоду импортным закупкам.

Пришло, на наш взгляд, время переосмыслить советский опыт планового хозяйства, пришло время восстанавливать учреждения типа Госплан и Госснаб. Без них никакие федеральные целевые программы не выполнить, тем более - когда горизонт планирования ограничен текущим бюджетом всего на год вперед. Это же относится к отрасли связи и промышленности средств связи.

IV. О разработках АТС в советское время

Квазиэлектронная междугородная АТС. Курс страны в наше время направлен на импортозамещение, что предполагает, в том числе, восстановление отечественной индустрии средств связи. Пришла пора вспомнить опыт советского времени.

Рассмотрим развитие отечественных сетей связи с точки зрения технологий. Каковы основные достижения российских связистов постсоветского периода? На ум, прежде всего, конечно, приходят мобильная связь и Интернет. Но следовало бы назвать систему телефонной сигнализации ОКС-7 (SS7), которая является связующим звеном каналов ISDN и интеллектуальной сети (IN).

Разработка советской системы ОКС-7 началась в 1970х с создания квазиэлектронных междугородных АТС (КЭАМТС). В квазиэлектронных АТС коммутация осуществляется герконами, а управление – электронное. В качестве прототипа для КЭАМТС «Кварц» использовалась американская станция 1ESS, разработанная в Bell Labs; первый экземпляр 1ESS был установлен в 1965 г.

В разработке КЭАМТС «Кварц» принимали участие многие коллективы, в том числе:

- координацию работ и разработку прикладного ПО осуществлял ЦНИИС (Москва),
- операционную систему центрального процессора - Институт кибернетики АН Украины (Киев),
- сам центральный процессор производил завод Роботрон (Дрезден, ГДР),
- периферийный процессор разрабатывал ЛОНИИС (Ленинград),
- коммутационное оборудование производилось на заводе ВЭФ (Рига, Латвия).

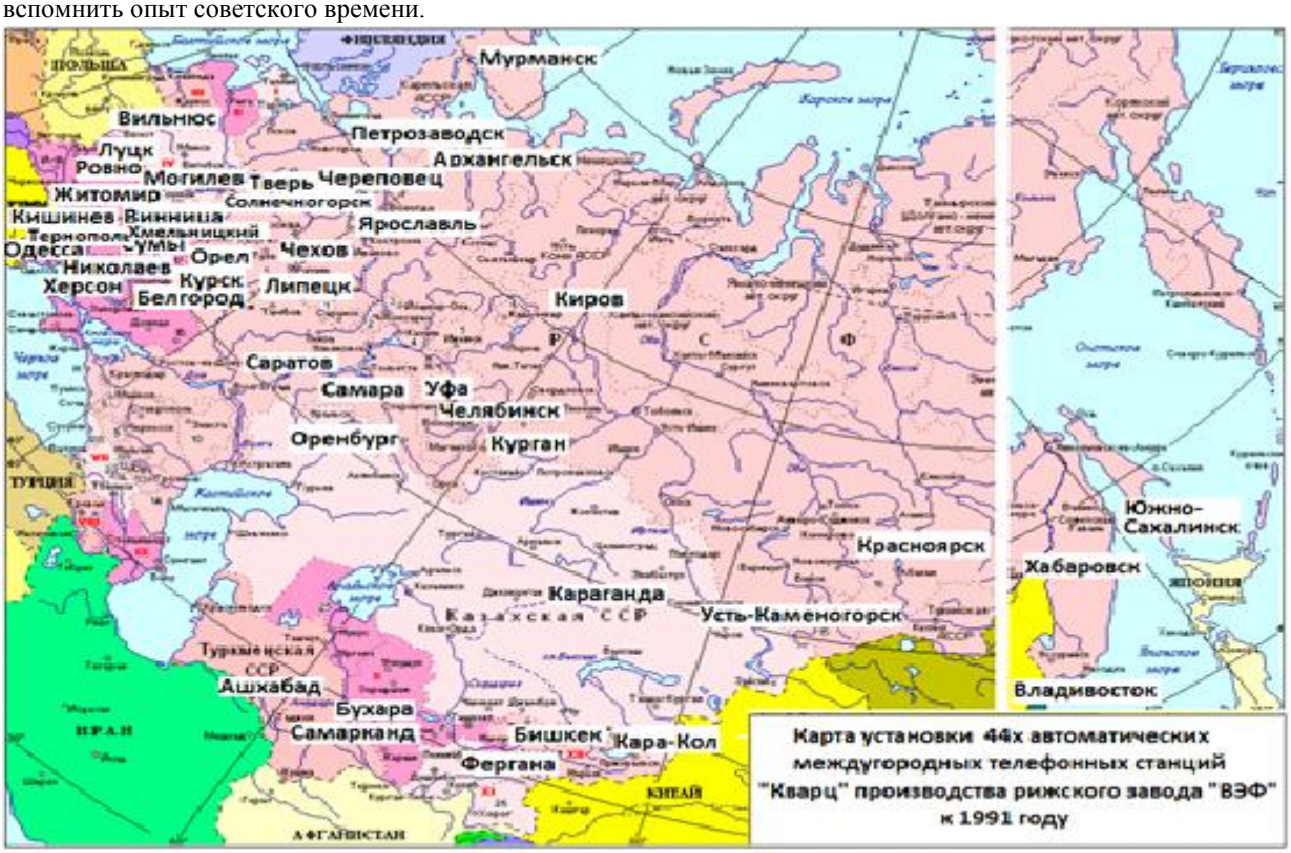


Рис. 2. Карта размещения КЭАМТС «Кварц» в городах СССР

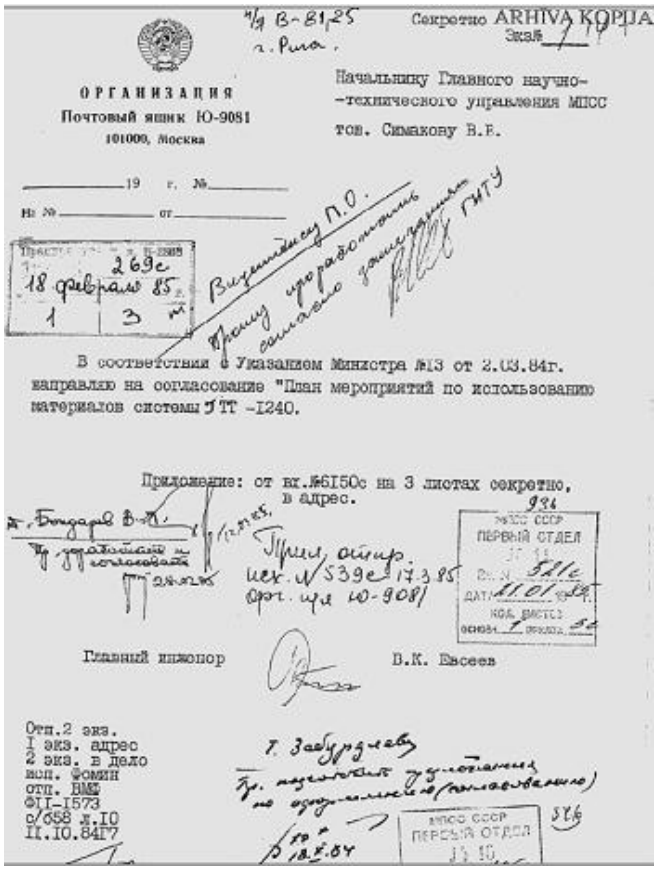
КЭАМТС «Кварц» производилась серийно и успешно эксплуатировалась до распада СССР. На рижском заводе ВЭФ были произведены и в кооперации с соисполнителями установлены 44 междугородные АТС «Кварц».

Международный проект ЕССКТ. С начала 1980х разрабатывалось следующее поколение телефонных станций – электронные АТС. Это был проект ЕССКТ (Единая Система Средств Коммутационной Техники), о нем сейчас мало кто помнит. Этот проект был аналогом ЕС ЭВМ – другого, хорошо известного проекта, целью которого было копировать IBM 360. Система телефонных станций ЕССКТ разрабатывалась в широкой кооперации со странами-членами СЭВ. Координирующей организацией выступал НИИ ВЭФ (Рига). В качестве прототипа, по указанию директивных органов, была выбрана система телефонных станций System-12 компании International Telephone and Telegraph (по другим обозначениям – ITT 1240). Следует признать, что выбор прототипа был не совсем удачным, хотя, по замыслу разработчиков, сама станция System-12 обладала многими положительными свойствами.

Первая АТС System 12 была установлена в 1982 в Бельгии. Но полноценное серийное производство не удалось наладить, так как не удалось в срок сдать первую АТС System 12 в США, что обеспечило бы крупномасштабное производство. В преддверии банкротства в 1986 компания ITT продала всю разработку System-12 (включая заводы) французско-голландской компании Alcatel Alsthom, наследницей которой сегодня является Alcatel-Lucent. Можно указать несколько причин неудач компании ITT, в том числе чрезмерно высокую интеграцию микросхем (что опережало уровень развития микроэлектроники того времени), недоработки программного обеспечения и другое. В странах СЭВ проект такой сложности в намеченные сроки повторить было нереально. Хотя бы потому, что в социалистическом лагере отставала микроэлектронная промышленность. Даже широкая кооперация не могла спасти сложнейший проект ЕССКТ, и проект перестал существовать с распадом СССР и СЭВ.

О проекте ЕССКТ сохранилось совсем мало сведений. При ликвидации НИИ ВЭФ в архив попали только материалы по разработкам, которые проходили по Первому отделу, т.е. по военным заказам. Так как работы по ЕССКТ проходили всего лишь с грифом «Для служебного пользования», то при ликвидации ВЭФ груды документов пошли в мусор. И сегодня историки, изучая советское прошлое по архивам, «обоснованно» говорят о заводе ВЭФ, точнее, об «Ордена Ленина и Ордена Октябрьской революции имени В.И. Ленина Рижском производственном объединении ВЭФ» как о чисто оборонном заводе. Вот так и делается история. Подсчитываются потери Латвии из-за работы на военную промышленность, потери из-за советской оккупации.

В архиве нашлись только два листочка по ЕССКТ, которые дают указание на наличие материалов по телефонной системе ITT-1240. Первое – это запрос из министерства МПСС, т.е. из п/я Ю-9081 с требованием согласовать план использования материалов по ITT-1240. Это касается документации по ITT-1240, которую нелегальным путем добывали агенты КГБ СССР и поставляли в НИИ ВЭФ как головную организацию по всему проекту ЕССКТ. Второе письмо – обращение к НИИ ВЭФ (т.е. п/я В-8125) передать войсковой части 32152 отчет по НИР «Союз» (так кодировалась программа ЕССКТ). В письме указан объем работы, выполненный к концу 1984 года странами-членами СЭВ; это – общий объем 62 (!) книги документации. Книги эти, к сожалению, в архив не были сданы. Итак, для истории мы имеем всего две пожелтевшие страницы в архиве - вместо 62-х томов технической документации!



ОРГАНИЗАЦИЯ
Почтовый ящик Ю-9081
101000, Москва

Начальнику Главного научно-технического управления МПСС
тов. Симакову В.Е.

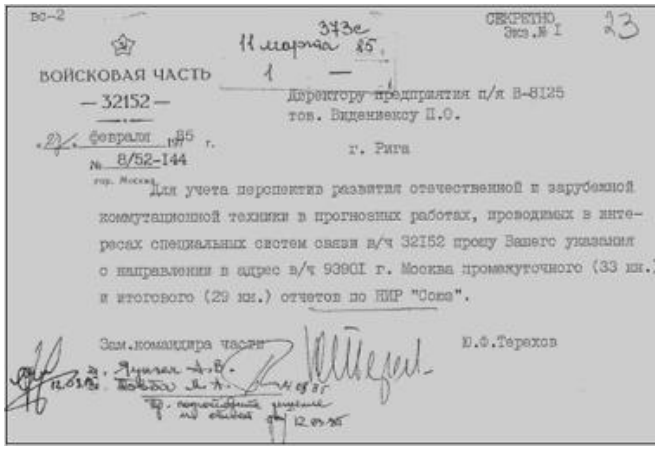
В соответствии с Указанием Министра №13 от 2.03.84г. направляю на согласование "План мероприятий по использованию материалов системы ITT -1240.

Приложение: от вх.№6150 на 3 листах секретно, в адрес.

Главный инженер В.К. Евсеев

Рис. 3. Указание из Министерства промышленности средств связи директору НИИ ВЭФ тов. П.О. Видениексу согласовать план использования материалов по ITT-1240.

От всего колоссального проекта ЕССКТ в архиве сохранились лишь эти два пожелтевших листочка, которые только участнику тех событий советского времени могут вызвать воспоминания, но ничего не скажут постороннему посетителю



ВОЙСКОВАЯ ЧАСТЬ
— 32152 —

Директору предприятия п/я В-8125
тов. Видениеку П.О.

г. Рига

№ 8/52-144

Для учета перспектив развития отечественной и зарубежной коммутационной техники в прогнозных работах, проводимых в интересах специальных систем связи в/ч 32152 прошу Вашего указания о направлении в адрес в/ч 93901 г. Москва промежуточного (33 кн.) и итогового (29 кн.) отчетов по НИР "Союз".

Зам.командира части Ю.Ф.Терехов

Рис. 4. Обращение в НИИ ВЭФ о передаче 62 книг документации по НИР «Союз» (1985).

V О РАЗВИТИИ СЕТЕЙ СВЯЗИ В ПОСТСОВЕТСКИЙ ПЕРИОД

Как проходило внедрение ОКС-7 в России. В 1991 году наступило новое – постсоветское время. Сети связи бурно развивались – в основном за счет закупок иностранного оборудования (что продолжается и по сей день).

Обратимся к статье Н. С. Мардера и А. С. Аджемова от 1997 г. [14]:

«В настоящее время заканчивается реализация схемы опытной зоны внедрения. В рамках этой зоны по ОКС № 7 взаимодействует между собой следующее коммутационное оборудование:

EWSD фирм Siemens и Iskratel,
Alcatel 1000 S12 фирмы Alcatel Telecom,
AXE-10 фирм Ericsson и Ericsson-Nikola Tesla,
5ESS фирмы Lucent Technologies,
ODEX-100 фирмы Hanwha,
Linea UT фирмы Italtel и др».

Эти станции были использованы в качестве междугородных станций АМТС и узлов автоматической коммутации УАК на междугородной сети России. Согласно структуре междугородной сети России, каждая АМТС страны включена в два УАК и общается по протоколу ОКС № 7. На территории России были размещены восемь УАК, имеющие важное стратегическое значение [15]. Заметим, что они построены на базе цифровых АТС типа AXE шведской фирмы Ericsson и EWSD фирмы Siemens.

Отметим, что Цифровые АТС до сих пор господствуют в сетях связи, выдерживая жесткую конкуренцию с оборудованием коммутации пакетов. Наиболее известны АТС типа AXE шведской фирмы Ericsson, разработанные в 1970х. Они наследовали опыт разработки координатных АТС типа ARF, ARM, ARK и ARE (разработки 1950х), которые также до сих пор местами находятся в эксплуатации. Второе место еще недавно занимал французско-голландско-американский концерн Alcatel-Lucent. С его именем связаны АТС: Alcatel E10 (собственно разработка Alcatel), Alcatel 1000-S12 (создана после приобретения компании ITT) и Western Electric 5ESS (после слияния с Lucent, а восходит к работам Bell Laboratories). В последние годы на второе место мирового телекоммуникационного рынка вырывается китайская фирма Huawei.

При построении сети АМТС требовалось обеспечить их взаимодействие по протоколу ОКС-7, что было нелегким делом, так как сама реализация международного протокола SS7 на станциях разных производителей в деталях различалась. Тем более различались системы управления сетью SS7.

В результате сеть ОКС-7 получилась с существенным изъяном. Оказалось, что уже изначально сеть ОКС-7 не планировалась на охват всей страны, так как для нумерации пунктов сигнализации ОКС-7 выбраны 14-битные номера (т.е.214 = 16384), что не хватает для такой большой страны как Россия. В США же для сети SS7 выбраны 24-битные номера. Как замечает Н.С. Мардер [16], *«требуется разработка нового плана нумерации национальной сети сигнализации ОКС-7»*.

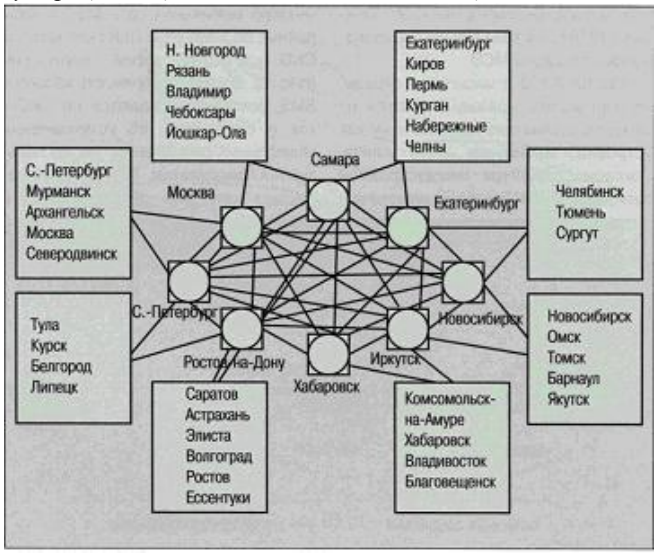


Рис. 5. Структура междугородной сети ОКС № 7.

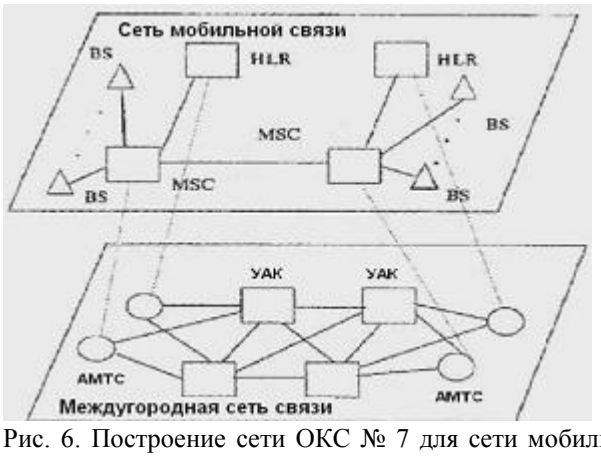


Рис. 6. Построение сети ОКС № 7 для сети мобильной связи.

Отметим две особенности использования ОКС-7 в мобильных сетях, что важно учесть ныне – при проектировании Системы-112. Первая особенность – каждый коммутатор мобильной сети MSC и база данных об абонентах HLR включены по сети ОКС-7 в АМТС своей территории. Вторая особенность касается передачи сообщений SMS. Они передаются по сети

ОКС-7, как и сообщения об установлении телефонных соединений, но не пользуются приоритетом. То есть при перегрузках сети будут обслужены в последнюю очередь или вовсе потеряны. В случаях чрезвычайных ситуаций будут неизбежны перегрузки сети, следовательно, для экстренных сообщений SMS следует ввести приоритеты, то есть доработать программное обеспечение АМТС и УАК.

Единая Система-112 в масштабах страны, на наш взгляд, должна опираться на междугородную сеть России, подобному тому, как устроена мобильная сеть вообще.

Особенности российской IN: можно обойтись без протокола INAP. Проанализируем далее упомянутую выше статью Н. С. Мардера и А. С. Аджемова:

«*В настоящее время активно проводятся работы по внедрению услуг интеллектуальной сети. В сентябре 1996 г. крупнейшие поставщики коммутационной техники и операторы связи ТфОП по взаимной договоренности с Министерством связи подписали в Москве меморандум взаимопонимания по вопросу внедрения оборудования, программного обеспечения и услуг интеллектуальной сети на ТфОП России. В соответствии с данным меморандумом был определен первый набор услуг интеллектуальной сети для внедрения на сети России, а именно:*

- *свободный телефон (Freephone);*
- *информационная услуга с дополнительной оплатой (Premium rate);*
- *услуги с альтернативной оплатой (Virtual credit card);*
- *телеголосование (Televoting).*

Для внедрения услуг интеллектуальной сети меморандум определил единый протокол на базе ОКС № 7 – INAP-R, спецификации которого соответствуют в основном стандартам ETSI с учетом требований сети связи России и перспектив ее развития».

При построении интеллектуальной сети России были установлены АТС разных производителей, в том числе:

- EWSD фирмы Siemens (в Москве),
- Alcatel S12 фирмы Alcatel (в Перми),
- платформы китайской фирмы Huawei,
- отечественные платформы компаний Светец, Протей, Беркут и другие.

Требовалось, чтобы все они работали по единому протоколу INAP-R. Это, как оказалось, было требованием чрезмерным, так как для этого пришлось бы переработать программное обеспечение множества станций. Тем самым, единая интеллектуальная сеть России осталась недостроенной, что сказывается до сих пор, в частности, при построении Системы-112.

Поясним одно важное обстоятельство. Рассмотрим классическую схему IN из Руководящего документа [17]: несколько коммутаторов услуг SSP выходят на общий контроллер услуг SCP, и SSP общается с SCP по протоколу INAP-R (поверх ОКС-7). В действительности же в России в основном реализована упрощенная схема IN. Коммутатор услуг SSP выходит непосредственно на собственной контроллер услуг SCP, поэтому указан совмещенный узел SSCP. Эта национальная особенность порождает одно важное последствие: так как узлы SSP и SCP находятся в составе единого узла SSCP, то между ними не обязательно использовать протокол INAP-R (тем самым к отечественным разработчикам Светец, Протей, Беркут и другим производителям были предъявлены необоснованно высокие требования).

Поясним эту особенность на примере выхода к услуге IN. В России используется нумерация типа 8-DEF-x1x2x3x4…x7, где DEF является кодом услуги (например, 800), x1x2x3 – код оператора IN, точнее, это код узла SSCP, а цифры x4x5x6x7 отводятся под код поставщика услуги. Тем самым, общее число узлов может быть до 1000, и каждую услугу могут абонировать до 10000 поставщиков.

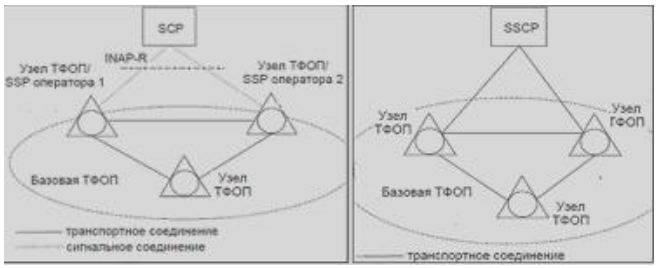


Рис. 7. Две архитектуры IN: а) классическая (по требованиям ITU): несколько коммутаторов услуг SSP выходят на общий контроллер услуг SCP, б) российская: коммутатор услуг SSP выходит на свой контроллер услуг SCP, т.е. устанавливается совмещенный SSCP.

Следует также заметить, что российские операторы закупили иностранное оборудование интеллектуальных сетей без средств программирования новых услуг, так называемой среды создания услуг SCE (Service Creation Environment). Тем самым пришлось ограничиваться только теми услугами, которые поставляла компания-производитель.

Итак, подведем итоги российской специфики построения интеллектуальной сети: с одной стороны, из-за закупки иностранного оборудования интеллектуальных сетей без средств программирования не создана российская школа программирования услуг, но с другой стороны, из-за отказа от классической схемы интеллектуальной сети возникла дополнительная возможность программирования услуг без обязательного использования протокола INAP-R. К сожалению, эта возможность не была реализована, так как формально потиворечила стандартам. В результате опыт многих коллективов (Аудиотеле, Светец, Беркут, Протей и другие), которые создавали сервера услуг (без использования INAP-R), остался невостребованным для развития рынка дополнительных услуг и развития российской интеллектуальной сети в целом.

VI Часть 2. Очередные задачи. О создании системы экстренных вызовов «112»

Невыполненные планы. Разработка Системы-112 является крупнейшим российским государственным проектом. Это проект сложнейший, так как Система-112 в современном понимании затрагивает все стороны жизни общества. И не удивительно, что в процессе его реализации обнажаются многие недостатки хозяйства России, накопившиеся за 25 лет капиталистического строительства.

Из социально значимых достижений постсоветского времени следует упомянуть универсальную услугу, гарантирующую, как замышлялось, каждому жителю страны доступ к телефонной связи, в том числе и к экстренным службам 112, а из организационных мероприятий последнего времени – воссоздание «Ростелекома» как федерального оператора связи, который и обеспечивает базовую инфраструктуру Системы-112.

Внедрение единого номера 112 вместо прежних 01, 02, 03, 04 (или параллельно с ними) идет с большим трудом, идет столь медленно, что уже сменилось поколение техники связи: от коммутации каналов с ее «венцом» – интеллектуальной сетью – «Ростелеком» в настоящее время пытается перескочить к коммутации пакетов, где протоколом сигнализации является SIP, а центральным элементом сети является IMS (IP Multimedia Subsystem). Смена поколений техники связи в условиях отсутствия собственного производства, а также отсутствия должной государственной дисциплины – все это еще более тормозит внедрение Системы-112. Подобные же трудности встречают связисты, которые строят сети связи для МЧС и МО.

Система-112 – это система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Российской Федерации. Она предназначена для обеспечения 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 плану программы, в 2013 г. система «112» должна была быть внедрена в трех субъектах России, в 2014 г. – в шести, в 2015 г. – в двух, в 2016 г. – в пяти, а в 2017 г. она должна быть запущена в оставшихся 67 регионах. Но планы срываются. 25 сентября 2014 г. вице-премьер Дмитрий Рогозин на селекторном совещании раскритиковал работы по внедрению системы 112, подчеркнув, что «в настоящее время система 112 функционирует только в Татарстане и Курской области, а это всего 2,5 процента от населения Российской Федерации» [18].

Конечно, было бы заманчиво строить Систему-112 по новейшим стандартам IMS, но этому препятствуют экономические соображения: еще не исчерпаны возможности IN, с одной стороны, и еще недостаточно апробированы новые средства IMS, с другой. На наш взгляд, текущие задачи Системы-112 могут быть реализованы на базе существующего поколения средств интеллектуальной сети и на коммутации каналов вообще. Одновременно отметим, - мы уверены, что Система-112 обязательно будет создана, так как от этого зависит эвакуационная готовность страны, и вместе с тем считаем, что из-за ее государственной важности следует использовать только апробированные технологии.

Согласно Распоряжению Правительства РФ [19], Система-112 должна обеспечить информационное взаимодействие органов повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, в том числе единых дежурно-диспетчерских служб муниципальных образований, а также дежурно-диспетчерских служб экстренных оперативных служб, в том числе шести служб:

- пожарной охраны;
- реагирования в чрезвычайных ситуациях;
- полиции;
- скорой медицинской помощи;
- аварийной службы газовой сети и
- службы "Антитеррор".

Создание службы «112» идет уже более 10 лет – с постановления Правительства РФ №894 от 2004 г. Идет трудно: еще в 2011 году на заседании правительственной комиссии по транспорту и связи вице-премьер Сергей Иванов заявил, что создание системы экстренных вызовов по единому номеру "112" в России фактически сорвано. Он напомнил, что в 2009 году данная система должна была быть реализована в 20 регионах, а в 2010 – на территории 44 субъектов Федерации. "На самом деле мы имеем единичные и пилотные проекты функционирования системы", – констатировал Иванов.

В официальном отчете Минкомсвязи [20] 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 системный проект Системы-112 до сих пор не разработан, и все проведенные работы следует рассматривать как экспериментальные образцы.

Концепция Системы 112. Представление о телекоммуникационной составляющей системы "112"

дает рисунок, который взят нами из концепции Системы 112, разработанной с участием компании Светец [21]. Здесь УОВЭОС – узел обработки вызовов экстренных оперативных служб.

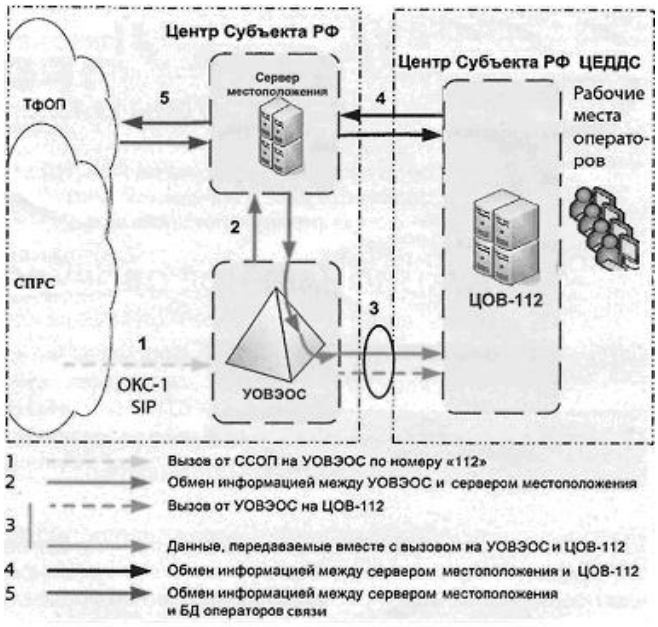


Рис.8. Пять интерфейсов системы 112

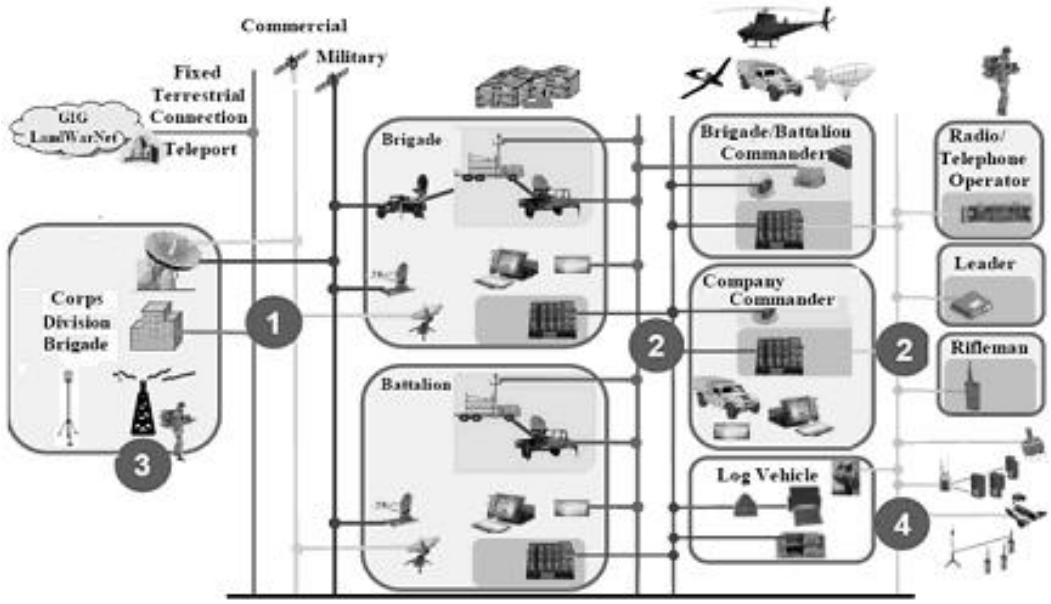


Рис. 9. Тактическая сеть GIG и ее контрольные точки

Потребовалось четыре года объемной работы, чтобы в 2010 г. Министерство обороны подготовило и опубликовало важнейший документ – об интерфейсах сети GIG [22]. В нем подробно расписаны протоколы работы сети GIG, выделены четыре контрольные точки:

1) между главным штабом и бригадами/батальонами,

2) обмен данными на театре военных действий между командирами, солдатами и сенсорами,

3) между командованием и отдельными солдатами средствами коммерческой связи,

4) обмен данными на марше.

По концепции, имеется пять интерфейсов Системы-112, которые предполагалось уточнить на первом этапе работ по Постановлению (до 2014). Это представляет собой исключительно сложную работу.

Прототипом российской Системы-112 могли бы служить работы по определению контрольных точек информационной сети GIG военного ведомства США и по построению американской сети NG9-1-1.

Указаны протоколы, по которым должны выполняться три типа требований:

- четкое описание моделей данных: структурированных (базы данных, картографические данные, форматы документов) и неструктурированных (презентации, картины, аудио, видео) и правил 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 упомянутом документе об интерфейсах сети GIG. В частности, в качестве стандартных приложений выбраны:

- email client;
- chat client;
- browser;
- document viewer;
- document editor;
- presentation editor;
- VPN client (по протоколу SSL).

О доступе к Системе-112. Доступ к Системе-112 относится к Универсальной услуге телефонной связи. Согласно Федеральному закону "О связи" (Статья 57) в Российской Федерации гарантируется оказание следующих универсальных услуг связи:

1) услуга телефонной связи с использованием таксофонов; в каждом поселении должно быть установлено не менее чем один таксофон с обеспечением бесплатного доступа к экстренным оперативным службам; время, в течение которого пользователь достигает таксофона без использования транспортного средства, не должно превышать один час;

2) услуги по передаче данных и предоставлению доступа к сети Интернет с использованием пунктов коллективного доступа; в поселениях с населением не менее чем пятьсот человек должен быть создан не менее чем один пункт коллективного доступа к сети Интернет.

Рассмотрим варианты доступа к Системе-112.

Связь на селе. Конечно, возможность добраться до таксофона за один час ходьбы (как того требует Закон) не может удовлетворить экстренные службы. Простейшим выходом из положения является раздача сельским жителям мобильных текстовых приставок и дооборудование таксофонов средствами радио-удлинителей для общения с такими приставками.

Связь в городе. Дело с городскими жителями тоже не простая задача. В последние годы на рынке появляются прототипы домовых терминалов (в виде планшетов). Но в случае пожара мобильная связь затруднена, и вряд ли такой терминал сможет обеспечить связь со спасателями. Следовало сохранить телефонную связь «по меди».

M2M коммуникации. В сферу ответственности Системы-112 входит и охрана недвижимого имущества: охрана жилья, пожары, протечки и т.п. Это затрагивает область M2M-коммуникаций и представляет собой крупнейшее направление индустрии связи. В связи с этим следует предусмотреть в концепции Системы-112 общение с M2M-устройствами, в частности, для противопожарных и охранных служб и следует выделить номерную емкость для идентификации M2M-устройств.

VII О КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Обеспечение безопасности критической инфраструктуры (Critical Infrastructure Protection, CIP) 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 [23] .

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 [24].

Европейский Союз. На перспективу предусмотрено расширение забот по защите критической инфраструктуры (CIP) [6]. Эту работу курирует ERNCIP (European Reference Network for Critical Infrastructure Protection) Office. Работа ведется в восьми тематических группах:

- Прикладная биометрия для CIP
- Безопасность авиационной техники
- Промышленная автоматизация и системы управления
- Химические и биологические риски в водном секторе
- Оборудование для обнаружения взрывчатых веществ (неавиационных)
- Радиологические угрозы критической инфраструктуры

- Устойчивость конструкций к взрывному воздействию
- Видео аналитика и наблюдения.

Пример Германии: телекоммуникации и атомные электростанции одинаково важны. В качестве примера реализации программы ERNCIP укажем на опыт Германии в области кибербезопасности [7]. В феврале 2016 г. принят новый Закон «IT SECURITY ACT», который имеет шесть разделов: (1) Энергетика, (2) IT и телекоммуникации, (3) Транспорт и перевозки, (4) Здравоохранение, (5) Пища и вода, (6) Финансы и страхование.

Согласно новому закону, 2000 немецких компаний имеют критически важные объекты инфраструктуры и подлежат государственному регулированию силами BSI (IT security department of the Bundestag and the Federal Office for Information Security). Закон об информационной безопасности не только обязует защитить свои веб-сайты, но и защищать другие свои ИТ-системы. Закон предписывает внедрять законом предусмотренные меры безопасности ИТ-систем в течение двух лет, а их выполнение будет проверяться не реже одного раза в два года.

Кроме того, в течение шести месяцев необходимо создать внутреннюю структуру отчетности, чтобы в BSI сообщать об инцидентах IT-безопасности. В настоящее время эта отчетность является обязательной только для операторов атомных электростанций и телекоммуникационных компаний. Невыполнение предписаний по IT-безопасности подлежат штрафным санкциям. Штрафы в размере до 100 000 евро могут быть наложены на операторов критической инфраструктуры, которые допускают ИТ-инциденты в сфере безопасности, не сумев реализовать предписанные меры ИТ-безопасности.

VIII Аппаратно-программный комплекс «Безопасный город»

В России основные направления государственной политики по защите критически важных объектов инфраструктуры утверждены в 2012 г. В этом документе [25] поставлена цель совершенствовать безопасность информационных и телекоммуникационных систем критической инфраструктуры, и объявлен план работ до 2020 года. Практически на сегодня наибольшая активность в России сосредоточена в направлении «Безопасный город» [26].

Аппаратно-программный комплекс (АПК) «Безопасный город» должен объединить в себе 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 [27]. А за этой задачей следует еще более масштабная задача – построить Государственную информационную систему «Безопасный город», которая будет охватывать все население и всю территорию России.

Сравним состояние комплексной безопасности объектов критической инфраструктуры в России и в других промышленно развитых странах. Показатель «социальный риск» (частота ЧС, приводящих к поражению определенного числа людей) показывает, что в России его значение в 10-100 раз выше, чем в развитых странах [28].

Неблагоприятная картина наблюдается практически во всех отраслях российской экономики, хотя справедливости ради надо сказать, что во всех секторах есть контрольные органы, деятельность которых координирует правительство РФ: Ростехнадзор – опасные производственные объекты, Ространснадзор – объекты транспорта, Россвязьнадзор – связь, информация и коммуникации, Россельхознадзор, Росфиннадзор, Роспожнадзор, Роспотребнадзор, Росздравнадзор, надзорные органы в МЧС, МВД, ФСБ, Минобороны. То есть, кибербезопасностью критически важных объектов занимается множество ведомств, но их взаимодействие тормозится несовершенством законодательной базы, ее ведомственностью. Только в последнее время начинается разработка технологий оценки ситуаций и планов реагирования, паспортов безопасности. Происходящие события характеризуются слабой координацией ведомств по вопросам безопасности объектов критической инфраструктуры, в том числе, их взаимодействие с АПК «Безопасный город».

Справедливости ради отметим, что после чернобыльской аварии, по рекомендациям и при участии МАГАТЭ были разработана и функционирует защищённая сеть передачи данных и система мониторинга атомных электростанций, ситуационный центр которой размещён в Ростехнадзоре и позволяет отслеживать все технологические процессы на станциях. Чем не пример для подражания?

Тем не менее, до сих пор Россия не имеет национальной программы аналогичного масштаба и значимости, как в США и ЕС. Есть только ведомственные законы, СНИПы и другие, несогласованные нормативно-правовые документы, регламентирующие процесс создания систем комплексной безопасности объектов критической инфраструктуры.

МЧС - координатор АПК «Безопасный город». Система-112 является частью АПК «Безопасный город», поэтому эти системы будем рассматривать совместно и начнем их анализ с обсуждения недостатков, важных для системного проектирования этих систем. Несмотря на то, что разработка Системы-112 длится уде почти 20 лет, до сих пор отсутствуют технические требования на

телекоммуникационную инфраструктуру (ТТ-ТИ). В этом суть нашего упрека в адрес МЧС. Сошлемся на программный доклад ФГБУ ВНИИ ГОЧС [29]. По нашему мнению, телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы. Рабочие места АРМ ДДС, подсистемы мониторинга, датчики охраняемых объектов – все это составные части современных инфо-коммуникаций. К тому же мы опустили три подсистемы (геоинформационную, информационной безопасности и консультационного обслуживания), которые тоже частично входят в телекоммуникационную инфраструктуру и должны быть подробно описаны в ТТ-ТИ. Описаны подробно, а не кратко – несколькими предложениями, как в «Методических рекомендациях по разработке системных проектов» [30]. Все эти подсистемы должны быть охвачены единым системным проектом. Встает неприятный вопрос: почему МЧС как координатор соглашается на такое ущемление своих прав?

Ведомственная «борьба» за раздел сфер ответственности по Системе-112 длился годами. В декабре 2010 года президент России Дмитрий Медведев подписал указ, где были прописаны зоны ответственности различных ведомств. В соответствии с этим документом МЧС России должно координировать действия по созданию, развитию и эксплуатации Системы-112, а Минкомсвязи отвечает за организацию взаимодействия с сетью связи общего пользования. Однако общее видение системы, т.е. ТТ-ТИ так и остались неразработанными. По нашему мнению, в этом обстоятельстве и кроется неудача МЧС с руководящей ролью координатора работ по Системе-112, а тем более по теме АПК «Безопасный город». Без единых, детально разработанных ТТ-ТИ не может быть и речи о построении единой Системы-112. Введение зон ответственности различных ведомств, по нашему мнению, только служит формальным прикрытием «безответственности».

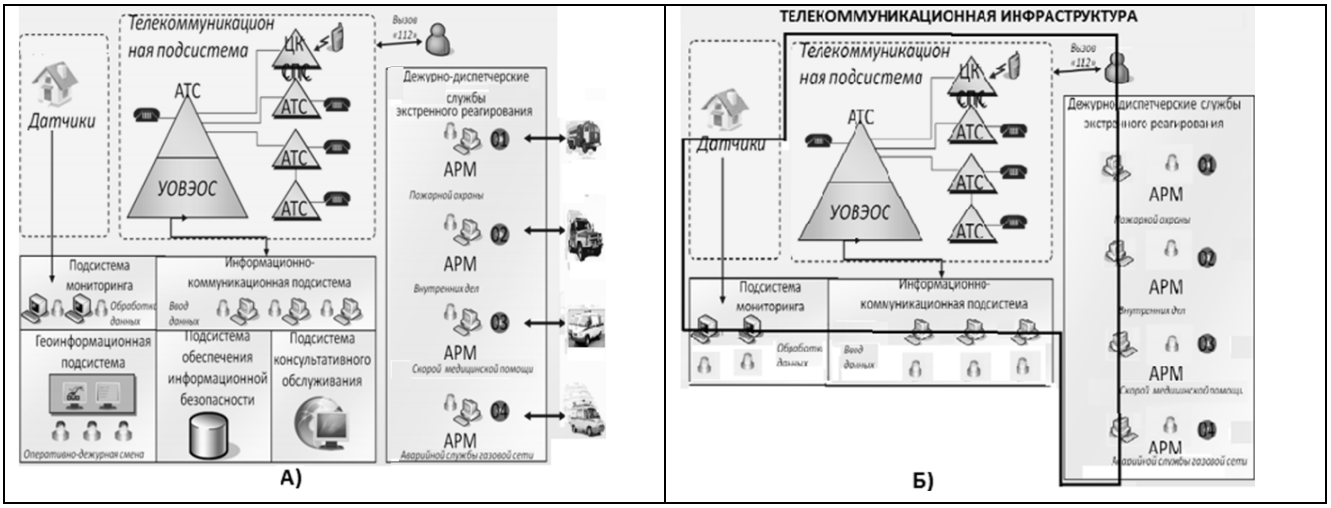


Рис. 10. А) Текущее представление Системы-112: Минкомсвязь отвечает только за телекоммуникационную подсистему. Б) Но при этом телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы.

С учетом новейших требований к Системе-112, когда значительно расширяется набор средств, доступных пользователю: кроме речи и SMS, как ранее, с ЦОВ можно будет общаться по видео, MMS, Web-chat, E-mail и Факс, следует полностью переработать системные документы по Системе-112. Ведомство МЧС встает перед сложнейшей задачей. Когда еще не видно конца текущей версии Системы-112, приходится говорить о новом поколении Системы-112.

Бурное развитие телекоммуникаций: Система-112, Безопасный город, Интернет вещей, M2M – все это требует новой методологии работ. Прототипом разработки технических требований для реализации архитектуры будущей Системы-112 и АПК «Безопасный город», на наш взгляд, мог бы служить, например, 916-страничный документ с описанием требований к унифицированным свойствам сервисов военной связи США от 2013 года [31].

Рис. 11. Новые средства доступа к будущей Системе-112

Ответственность 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 только 18 января

2016, а работы по созданию Системы-112 во всех областях России, согласно требованиям ФЦП, полагалось завершить в 2017 г. Ясно, что в срок уложиться не удастся.

Только в конце 2015 года МЧС и Минкомсвязь согласовали упомянутые выше «Методические рекомендации по разработке системных проектов». 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 (!) и что эти «Методические рекомендации» появились как выполнение федеральной целевой программы, которую полагалось завершить в 2017 г. К тому же, в «Методических рекомендациях» дан лишь 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 пользователей, особенно терминалов телематики, устройств интернета вещей. В этом направлении сделан только первый робкий шаг: 4 мая 2016 г. Минкомсвязь 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;

1UV – номер экстренной службы 112, 101, 102, 103 или 104;

x1x2 – зоновый телефонный номер;

x6x7 – идентификатор дежурно-диспетчерской службы, равный 11.

До сих пор совсем упущены вопросы программного обеспечения, которые также входят в сферу ответственности Минкомсвязи. 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 [32]. Заметим, что в данном случае речь шла всего лишь об офисном программном обеспечении. Пока же Минкомсвязь даже не ставит целью разработать программное обеспечение для телефонных станций или маршрутизаторов, что требуется для Системы-112 и АПК «Безопасный город».

IX О ВЕДУЩЕЙ РОЛИ «РОСТЕЛЕКОМА» В ПОСТРОЕНИИ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Согласно распоряжению Правительства РФ № 453-р от 21 марта 2011 года ОАО "Ростелеком" является единственным исполнителем работ по ряду мероприятий Федеральной целевой программы "Информационное общество (2011-2020 годы)". В выполнении этих мероприятий используется Национальная облачная платформа О7 [33].

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 2 раза,
- снижение экономического ущерба – до 5%,
- разгрузку операторов межведомственных служб за счёт «перехвата» ложных и справочных вызовов оператором 112 – на 70%.

Приведенные показатели следуют, по-видимому, из бизнес-плана, который нам неизвестен. Но для убедительности следовало бы, по крайней мере, привести архитектуру Систему-112 с указанием роли Ростелекома, в том числе место и роль платформы О7 и комплекса «О7.112».

К этому проекту «О7.112» примыкает сервис «О7. Медицина» – как часть Системы-112. Цель его создания состоит в автоматизации 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, к единым электронным медицинским

картам пациентов, к системе электронного документооборота.

Отметим еще сервис «О7.Сити», что непосредственно связано с АПК «Безопасный город». Цель создания сервиса – обеспечение эффективного и безопасного функционирования городских служб и создания 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 видеоустройствами), 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 с ответственной ролью «Ростелекома» в самом проекте Системы-112, и не только для отдельных областей, а для всей страны?

В упомянутых выше «Методических рекомендациях по разработке системных проектов» 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.

X Две стратегии связистов России

Необходимость импортозамещения – это одна из важнейших сторон текущего момента в области телекоммуникаций. Другая относится к стратегии развития техники связи в России – на какую же технику направлять усилия по импортозамещению: на традиционную коммутацию каналов или на новомодную коммутацию пакетов, агрессивно продвигаемую иностранными производителями. Это очень сложный выбор.

Стратегия 1. В настоящее время основная стратегия Ростелекома – идти курсом «All-over-IP. Суть этой стратегии – продолжение строительства сетей связи средствами иностранных производителей. Образно говоря, это означает – «зажмуриться» и идти к «All-over-IP», идти, опасаясь – не случится ли коллапс сети и потеря управления страной.

Тут уместно напомнить историю. 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. Кроме того, спецслужбам США удалось вывести из строя систему управления противовоздушной обороны Ирака с помощью активации 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. Основной выигрыш от коммутации пакетов состоит в более экономном использовании каналов – за счет заполнения пауз, а главное, что подчеркивают пропагандисты 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. Из-за добавления заголовков в пакетах и ожидания в буферах «чистое» время занятия канала удлиняется: при коммутации каналов сигнальная информация передается один раз, при коммутации пакетов – добавляется к каждому пакету.

5. Усложняются алгоритмы 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 американских компаний Cisco и Juniper, а в последнее время и китайской компании Huawei. Действительно, на базе такого оборудования можно строить современные сети. Но, к сожалению, эта стратегия приводит к зависимости от этих компаний на все обозримое будущее. И как быть с безопасностью страны, как преодолеть санкции?

Стратегия 2. Суть этой стратегии заключается в выборе курса на импортозамещение, т.е. на развитие сетей связи собственными силами. Для этого надо вернуться к тому состоянию знаний, которые были

достигнуты ранее – лет 20 назад и развивать их далее. В данном случае такой точкой отсчета условно можно назвать систему ОКС-7. В России отставание от передового 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 продолжить движение вперед ускоренными темпами (догонять-то проще). Наше предложение – восстановить промышленность средств связи.

По-видимому, сеть «Ростелекома» будет мигрировать к архитектуре NGN. Поэтому важно рассмотреть, как будет «уживаться» традиционная сеть коммутации каналов и сигнализация SS7 с сетью NGN, где будет главенствовать протокол SIP (или AS-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 предприняли в компании Ericsson и разработали Ericsson Composition Engine [34], что задумано как новое поколение интеллектуальных сетей. В этом устройстве предоставляются дополнительные сервисы по протоколам INAP, CAP и SIP, и находится оно на стыке между сетями коммутации каналов и коммутации пакетов. Пока неизвестно, получит ли платформа Ericsson Composition Engine широкое внедрение.

Наибольшие усилия по стыковке сигнализации SS7 и интеллектуальной сети с протоколом SIP и узлом IMS предприняты компанией Telcordia (США) [35]. Напомним, что Telcordia является продолжателем работ Bell Labs по интеллектуальным сетям. В начале 1990х Telcordia разработала архитектуру AIN. Дальнейшие варианты сети объединяются группой документов AINGR Family of Requirements, FR-15. Эти документы подводят итоги 20-летней работы Telcordia по развитию концепции AIN в условиях наступления IP технологии, точнее, SIP протокола, а также учет требований экстренных вызовов E9-1-1 в архитектуре AIN. На основе этих документов можно совершенствовать российскую интеллектуальную сеть и на ее основе строить Систему-112.

Если идти курсом импортозамещения, то следует учесть отставание России от мирового уровня в области микроэлектроники, особенно для разработки техники коммутации пакетов. В связи с этим стоит оценить перспективы «старой» коммутации каналов и ускоренными темпами идти вперед, реализуя цифровую трансформацию. Новейший анализ развития техники связи на примере глобальных проектов не дает однозначного ответа о путях глобальной цифровизации, а показывает целесообразность сочетания коммутации каналов и коммутации пакетов, что существенно упрощает решение поставленной выше задачи.

БИБЛИОГРАФИЯ

[1] В. Гвоздецкий. План ГОЭЛРО. Мифы и реальность. https://www.nkj.ru/archive/articles/5906/

[2] Цифровая экономика для устойчивого экономического роста //Мосты, Volume 9, Number 4, 20 June 2016 http://www.ictsd.org

[3] Экспорт оборудования http://kaivg.narod.ru/exp.pdf/ Retrieved: May, 2017

[4] From Turbine to Quantum: Implants in the Arsenal of the NSA. // GENERAL SECURITY, MARCH 24, 2014. http://resources.infosecinstitute.com/turbine-quantum-implants-arsenal-nsa/

[5] 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.

[6] Шнепс-Шнеппе М.А., Куприяновский В.П., Намиот Д.Е., Селезнев С.П. Телекоммуникации как решающее звено цифровой экономики. Опыт США// International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 5, 2017, 17-31.

[7] Куприяновский В.П., Намиот Д.Е., Синягов С.А., Добрынин А.П. О работах по цифровой экономике// Современные информационные технологии и ИТ-образование. Том 12, №1, 2016, С. 243-249

[8] В. М. Дмитраченко К истории создания Единой автоматизированной сети связи СССР (1963-1991 гг.) http://www.computer-museum.ru/connect/eass.htm

[9] Б. Н. Малиновский История вычислительной техники в лицах. Киев: фирма «КИТ», ПТОО «А. С. К.», 1995. 384 с.

[10] А.И. Китов http://www.computer-museum.ru/galglory/kitov_3.htm

[11] Берг А. И., Китов А. И., Ляпунов А. А. Радиоэлектронику — на службу управления народным хозяйством // Коммунист. 1960. № 9. С. 21-28;

[12] Берг А. И., Китов А. И., Ляпунов А. А. О возможностях автоматизации управления народным хозяйством // Проблемы кибернетики. Выпуск 6. М.: Физматгиз, 1961. С. 83-100.

[13] С. Л. Соболев, А. И. Китов, А. А. Ляпунов. «Основные черты кибернетики» // «Вопросы философии». — 1955. — № 4. — С. 147.

[14] Н. С. Мардер, А. С. Аджемов. Развитие российской сети ОКС № 7 — основа современных услуг связи// Сети и системы связи, 1997, №9.

[15] ОКС-7 http://www.gosthelp.ru/text/PolozhenieOsnovnyepolozhe2.html Retrieved: May, 2017

[16] Н.С. Мардер «Современные телекоммуникации», Москва, 2106.

[17] РД 45.126-99. «Концепция взаимодействия операторов интеллектуальных сетей связи и их присоединение к базовой телефонной сети общего пользования». Минсвязи России

[18] ФСБ создает единую систему связи для защиты от кибератак и утечки секретов http://hitech.newsru.com/article/28aug2013/fsb_bound

[19] Распоряжение Правительства Российской Федерации от 4 мая 2012 г. N 716-р. Концепция федеральной целевой программы "Создание системы обеспечения вызова экстренных оперативных служб по единому номеру "112" в Российской Федерации на 2012 - 2017 годы".

[20] Что мешает внедрению «Службы 112» // ИКС, 2013, ноябрь, с. 15.

[21] Е.И. Полканов, И.Г. Мазин «Совместное использование информационных ресурсов: консолидация развития сетей» // «Электросвязь», 2012, №3

[22] Common Operating Environment Architecture. Appendix C to Guidance for ‘End State’ Army Enterprise Network Architecture U.S. Army CIO/G-6, 1 October 2010

[23] Шнепс-Шнеппе М.А., Селезнев С.П., Намиот Д.Е., Куприяновский В.П. О кибербезопасности критической инфраструктуры государства// International Journal of Open Information Technologies. – 2016. – Vol 4, No 7 - С. 22-31.

[24] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[25] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803. http://www.scrf.gov.ru/documents/6/113.html

[26] Шнепс-Шнеппе М.А., Селезнев С.П., Намиот Д.Е., Куприяновский В.П. О телекоммуникационной инфраструктуре комплекса «Безопасный город» // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 4, no. 6, 2016, 17-31.

[27] Концепция построения и развития аппаратно-программного комплекса «Безопасный город» http://www.pravo.gov.ru/ 11.12.2014

[28] М.А. Шнепс-Шнеппе, Д.Е. Намиот, С.П. Селезнев, В.П. Куприяновский. К системному проектированию Системы 112 и комплекса «Безопасный город» // International Journal of Open Information Technologies. 2016.-Т.4.- №9, С.44-63.

[29] С.А. Качанов «Основные положения по созданию системы обеспечения вызова экстренных оперативных служб по единому номеру 112» ftp://ftp.infor-media.ru/210612/Kachanov.pdf

[30] Методические рекомендации по разработке системных проектов телекоммуникационной подсистемы системы обеспечения вызова экстренных оперативных служб по единому номеру «112» для субъектов Российской Федерации, Москва, 2015.

[31] Department of Defense Unified Capabilities Framework 2013 (UC Framework 2013). January 2013

[32] Меры по поддержке российского ПО http://www.minsvyaz.ru/ru/events/32718/

[33] Национальная облачная платформа Ростелекома http://www.rostelecom.ru/projects/o7/

[34] Niemöller J. et al. Ericsson Composition Engine – Next-generation IN// Ericsson review, № 2, 2009.

[35] Telcordia Roadmap to Advanced Intelligent Network (AIN) Documents, Issue 2, August 2008.

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

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

Abstract – **In this paper, the tasks of the digital economy and the role of telecommunications are discussed. In part 1, we provide the analysis of the development of communication networks, the Soviet communications and control systems: EASC and UGCC, the development of telephone equipment in the Soviet era: CEAMTS and ESKTT. As per the post-Soviet period, we provide the introduction of signaling of the SS-7 (OKS-7 in Russia) and an intelligent network. Part 2 deals with the following tasks: creating an emergency call system "112", ensuring the cyber-security of the critical infrastructure, creating a hardware and software complex "Safe City", the leading role of Rostelecom in building the information society. Also, we discuss two communications strategy for Russia – rely on foreign manufacturers or the development of import substitution and own production.**

Keywords – Digital economy; SS-7; Intelligent network; Emergency call system "112"; Critical infrastructure; Safe City; Rostelecom; Information society; Import substitution