О телекоммуникационной инфраструктуре комплекса «Безопасный город»

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

***Аннотация*—Рассматривается опыт США по созданию двух сложных систем: глобальной информационной сети оборонного ведомства DISN и единой сети нового поколения для обслуживания экстренных вызовов NG9-1-1. Проведён анализ работы МЧС по созданию аппаратно-программного комплекса (АПК) «Безопасный город» и анализ работы Минкомсвязи. Высказаны соображения о построении Системы-112 и АПК «Безопасный город» в условиях импортозамещения, т.е. с упором на развитие сетей связи собственными силами. Это предполагает использование прошлого опыта коммутации каналов (каналы ISDN, система ОКС-7 и интеллектуальные сети). Сформулированы три задачи: по подготовке специалистов, разработке технических требований на информационную инфраструктуру АПК «Безопасный город» и по переходу в АПК «Безопасный город» от клиент-серверной архитектуры (ЦОД и терминалы), на полностью распределённую архитектуру, в которой каждый объект выступает в качестве терминала и сервера одновременно.**

***Ключевые слова*—безопасный город, распределенная архитектура, системы связи, система 112.**

I. Введение

Настоящая статья является продолжением работы[1] по анализу американских сетей DISN (Defense Information System Network) и NG-911, рассматривая их как прототип сети связи гражданской обороны нового поколения NG112(Система-112). А так как Система-112 является частью АПК «Безопасный город», то эти системы будем рассматривать совместно. Аппаратно-программный комплекс (АПК) «Безопасный город» должен объединить в себе системы экстренных оперативных служб (пожарная служба, ЕДДС, полиция, скорая медицинская помощь, тепло-газо-электро снабжение, ЖКХ, информационные, мониторинговые, оповещающие, приемопередающие средства муниципальных образований, соединив их с региональным Центром управления в кризисных ситуациях МЧС России и далее с Национальным ЦУКС МЧС России [2]. И самое главное, АПК «Безопасный город» должен иметь высокий уровень коммуникабельности и собственной информационной безопасности. Поэтому при его создании необходимо использовать российское аппаратное и программное обеспечение, изначально разрабатываемое под российские стандарты безопасности [2]. Тем самым настоящая статья ставит своей целью искать пути решения этой сложнейшей задачи – построения АПК «Безопасный город» на базе российского аппаратного и программного обеспечения. А за этой задачей следует еще более масштабная задача – построить Государственную информационную систему «Безопасный город», которая будет охватывать все население и всю территорию России.

Систему оповещения, Систему-112 в данной статье мы будем рассматривать как часть СПК «Безопасный город», так как все эти системы нуждаются в достаточно развитой телекоммуникационной инфраструктуре по схожей топологии.

Разработка Системы-112 представляет собой сложнейший проект государственного значения. Этот проект затрагивает все стороны жизни российского общества, и в ходе его реализации обнажаются многие недостатки хозяйства страны, накопившиеся за четверть века капиталистического строительства в России. В официальном отчете Минкомсвязи России от 2013 г. [4] перечислены нерешенные задачи: «Ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей связи общего пользования (ССОП) для прохождения вызовов, поступающих в службу по номеру „112”. Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений».

Построение «Системы-112» идет с большим трудом, а работы ведутся уже почти 20 лет. По состоянию на 13 мая 2016 года «Система-112» введена в промышленную эксплуатацию только в Калужской и Курской областях и в Республике Татарстан [3]. До сих пор так и не разработан единый системный проект службы 112, и тем самым все проведенные работы, скорее всего, следует рассматривать как экспериментальные образцы.

Рассмотрение опыта США по созданию двух подобных систем: глобальной информационной сети оборонного ведомства DISN и единой сети нового поколения для обслуживания экстренных вызовов NG9-1-1 – поможет понять, почему так трудно выполнить намеченные задачи и, надеемся, подскажет пути их решения. В качестве иллюстрации многообразия

Статья получена 10 мая 2016.

М.А. Шнепс-Шнеппе, AbavaNet (e-mail: sneps@mail.ru)
С.П. Селезнев, Фактор-ТС (e-mail: sergei.seleznev@gmail.com)
Д.Е. Намиот, МГУ имени М.В. Ломоносова (e-mail: dnamiot@gmail.com)
В.П. Куприяновский, МГУ имени М.В. Ломоносова (e-mail: vpkupriyanovsky@gmail.com)

требований сети NG9-1-1 и потенциальной связи с российскими проектами Безопасного города приведём схему деятельности NG9-1-1 отдельного штата США (рис. 1). Согласно официальным документам [5], будущие сети экстренных служб должны быть сетями пакетной коммутации. Особенно отмечается, что сеть NG9-1-1 должна поддерживать мультимедиа трафик и практически охватывать все стороны общественной жизни. Базовая сеть штата (State Backbone Network) объединяет:

- Традиционную телефонную сеть,
- Мобильную сеть,
- Экстренную службу 9-1-1,
- Полицию,
- Пожарную службу,
- Национальную гвардию,
- Школы,
- Госпитали,
- Аппарат губернатора и т.д.

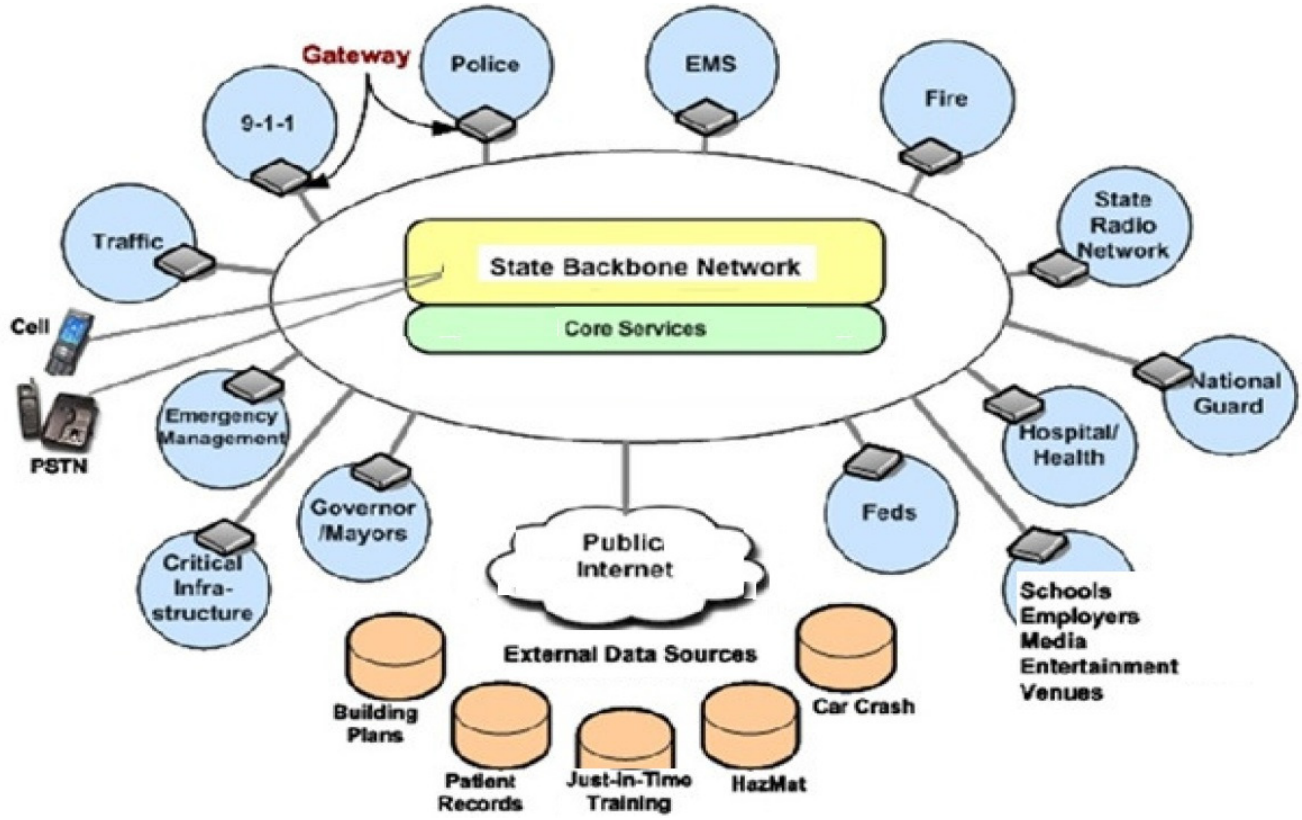


Рис. 1. Поле деятельности службы NG9-1-1 отдельного штата США в концепции «Безопасный город» [5].

Представление о трудоемкости программного обеспечения службы NG9-1-1 дает рис. 2.

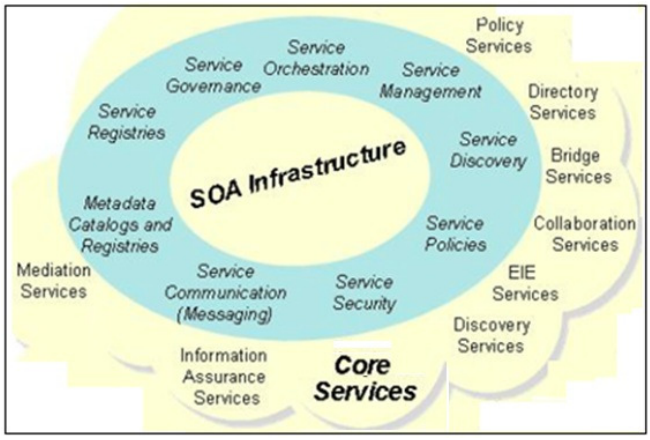


Рис. 2. Базовые сервисы (Core Services) пользуются услугами инфраструктуры SOA.

Базовые сервисы (Core Services) пользуются услугами сложной инфраструктуры SOA (Service-Oriented Architecture, сервисно-ориентированная архитектура) и включают такие программы, как metadata registries, service discovery, user authentication, machine-to-machine messaging, service management, orchestration, service governance и другие. А затем идут программы множества учреждений (по кругу на рис. 1) и выходы на фиксированную (PSTN) и мобильную сеть.

Более подробно вопросы программного обеспечения службы NG9-1-1 и DISN рассмотрены в наших статьях [6,7].

Далее, в разделах 2 – 4 рассмотрим опыт США по созданию двух сложных систем: глобальной информационной сети оборонного ведомства DISN и единой сети нового поколения для обслуживания экстренных вызовов NG9-1-1. В разделе 5 приведён анализ работы МЧС по созданию АПК «Безопасный город», а разделе 6 – анализ работы Минкомсвязи. В разделе 7 высказаны соображения о построении Системы-112 и АПК «Безопасный город» в условиях импортозамещения, т.е. с упором на развитие сетей связи собственными силами, что, на наш взгляд, предполагает использование опыта прошлых лет коммутации каналов (каналы ISDN, система ОКС-7 и интеллектуальные сети). В разделе 8 сформулированы три задачи: по подготовке специалистов и разработке

технических требований на информационную инфраструктуру АПК «Безопасный город» и по переходу в АПК «Безопасный город» от клиент-серверной архитектуры (ЦОД и терминалы), на полностью распределённую архитектуру, в которой каждый объект выступает в качестве терминала и сервера одновременно..

II Опыт США по созданию экстренной службы нового поколения NG9-1-1

Три поколения службы 9-1-1. На рис. 3 показана простейшая схема службы 9-1-1. Как и в России, внедрение единого номера экстренных служб в США проходит с трудностями, особенно определение номера вызывающего мобильного абонента и его местоположения, что регламентируют требования, объединенные под названием E9-1-1 и что относится ко второму поколению службы 9-1-1.

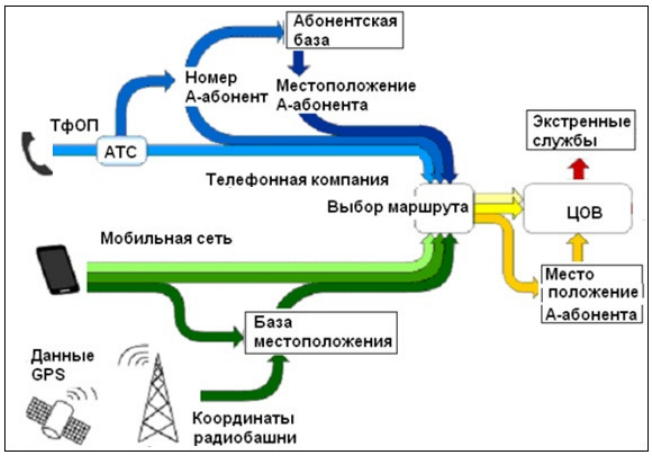


Рис. 3. Простейшая схема службы 9-1-1.

Но чему следовало бы поучиться, так это четкости действий Федеральной комиссии связи (FCC). Требования к операторам мобильной связи, объединенные названием E9-1-1, включали, например, требование передать в ЦОВ номер вызывающего абонента и номер станции мобильной сети в течение 6 мин (SSP – это очень долго!) 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, по вызовам в сети Sprint Nextel местоположение удалось определить только в 81% случаев, за что компанию оштрафовали на 1,33 млн. долл.

В настоящее время действует требование определить координаты вызывающего абонента с точностью до 300 м. Это полагалось внедрить к 11 сентября 2008 г., а затем срок перенесли на четыре года – на 11 сентября 2012 г. – из-за сложностей переоборудования базовых станций. В настоящее время это требование уже реализовано. Подобные же жесткие требования к определению местоположения предъявляются и к VoIP-вызовам.

Новейшее поколение службы экстренных вызовов в США имеет название NG9-1-1 [8] и должна быть реализована в IP сети (рис. 4). В системе NG9-1-1 требуется обеспечить возможность любых сообщений реального времени, т.е. наряду с телефонным вызовом, также передачу текста, данных, изображений и видео. Обратим внимание на рис. 4 слева внизу: там отдельно указаны телематические вызовы. Это, в частности, относится к противопожарным и охранным службам. Сегодня трудно определить, когда же система NG9-1-1 будет реализована, так как встречает исключительно большое сопротивление самих экстренных служб.

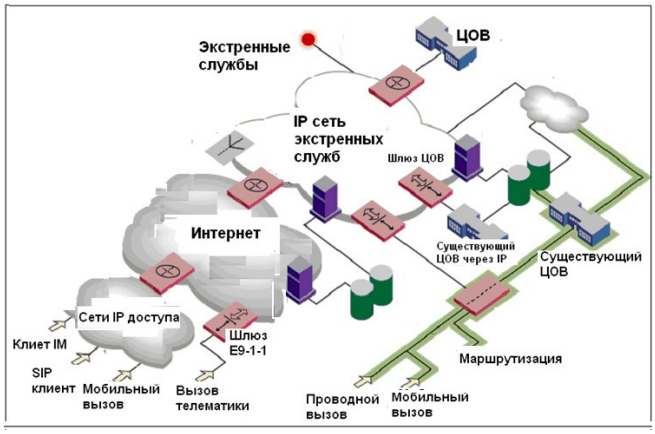


Рис. 4. Новое поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 9-1-1.

Текстовые сообщения. Федеральной комиссии связи ведет борьбу с мобильными операторами за внедрение вызова службы 9-1-1 текстовым сообщением, что можно сделать и без перехода на IP технологии. Передачу текста важно реализовать для поддержки слепых и для лиц с дефектами слуха и речи. По статистике, таких абонентов насчитывается 10% населения, точнее: 20% среди лиц старше 65 лет и 40% среди лиц старше 75. С этой целью FCC обязала к 15 мая 2014 г. дооборудовать ЦОВ службы 9-1-1 средствами приема текстовых сообщений от мобильных телефонов [9], и, по оценкам, 90% текстовых вызовов удастся обеспечить. Уже к 30 июня 2013 г. полагалось установить программы автоматического ответа на принятые текстовые вызовы. Нововведению сопротивляются операторы мобильной связи: в настоящее время существующие центры SMS-сообщений не выполняют требования по приоритетному обслуживанию экстренных вызовов и, мол, недостаточно надежны.

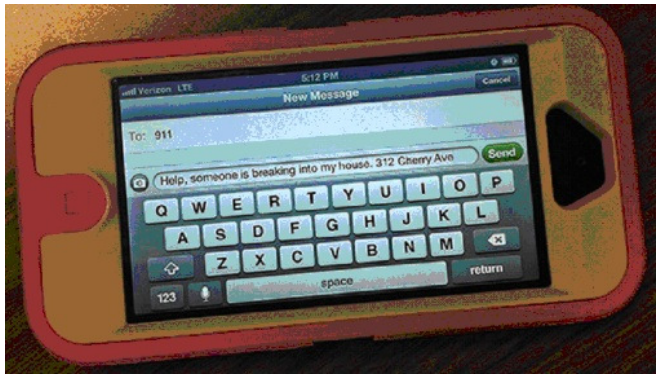


Рис. 5. Текстовый терминал.

Аналогия между DISN и NG9-1-1. Нетрудно заметить аналогию между экстренной службой NG9-1-1, которую пытается создавать Министерство транспорта США, с одной стороны, и строящейся военной инфокоммуникационной системой DISN, с другой. Сошлемся на материалы Конференции по внутренней безопасности (Homeland Security) США [10], где автор статьи разбирает эту аналогию и начинает с напоминания, что оба эти проекта (с ориентацией на IP технологию) были объявлены практически одновременно – в 2007 году.

Аналогия начинается с верхнего уровня архитектуры сетей NG9-1-1 и DISN. Обе архитектуры полагают сбор информации от множества источников и передачу ее множеству пользователей. И что важно, обе системы требуют высокой живучести. Полагается передавать голос, данные и видео и с минимальной задержкой. Применения также являются аналогичными.

Передача данных оказывается самым сложным применением. Например, пусть больной вызывает скорую помощь текстовым сообщением. Это сообщение достигает PSAP (Public Safety Answering Point, ЦОВ - центр обслуживания вызовов). Оператор PSAP, по этому сообщению, должен определить местоположение больного, сообщить об этом скорой помощи и послать подтверждение больному. Данные о местоположении передаются компьютеру и наносятся на карту.

В архитектуре DISN наблюдаем похожую картину передачи и обработки данных. Данные могут быть любого типа, включая текст, файлы, снимки. Каждый солдат должен быть доступен для обмена информацией. Например, если солдат обнаружил бункер, но не может распознать тип вооружения в бункере, он передает картинку в штаб, аналитику по вооружения. Аналитик изучает вопрос и передаёт решение командиру, который даёт приказ солдату, а также может вызвать бомбардировщик или известить разведку для уточнения цели.

Итак, аналогия между NG9-1-1 и DISN налицо, но как ею воспользуется? Как согласовать планы создания этих двух систем многомиллиардной стоимости?

Риски перехода на IP-протокол [11]. Согласно официальным документам, вызовы 9-1-1 должны быть доступны с любого типа устройств, а службам первой помощи должна быть доступна информация от других общественных служб (как на рис. 1). План модернизации NG9-1-1 стартовал в 2000 г. и к 2008 были завершены пилотные проекты. Однако реализация плана тормозится операторами связи и самими экстренными службами: они не торопятся переходить на протокол IP. Как и правительственная связь США (о чем речь пойдет ниже), служба 9-1-1 избегает экспериментирования с новыми протоколами SIP и AS-SIP, а ограничивается каналами ISDN.

Федеральная комиссия связи 31 января 2014 г. издала документ о поддержке операторов, которые будут переходить от коммутации каналов (по технологии TDM) к IP-протоколу. По свежим следам этого документа FCC заказала юридической фирме оценку возможных рисков такого перехода. Фирма проанализировала историю нововведений в телефонных сетях и перечислила крупнейшие сбои в телефонных сетях от введения новой техники за последние более 20 лет. 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 одновременно вышли из строя все 114 станций 4ESS сети AT&T. Устранить неполадки удалось только через 9 часов. Дело было в новой версии программного обеспечения, которое установили месяцем ранее на всех станциях 4ESS. Вкралась ошибка в работе системы SS7, которая проявилась при перегрузке одной из АТС и по принципу домино «вырубила» почти всю сеть AT&T. Были потеряны 65 млн. вызовов и нанесен трудно поправимый ущерб репутации компании. Другой подобный коллапс случился через полтора года – 26 июня 1991 г. в Балтиморе. На 6 часов остались без связи 5 млн. абонентов. Тоже из-за ошибки в программах SS7. Тогда коллапсы сети связи страны были расследованы Конгрессом США, так как их приравняли к угрозам национальной безопасности. Был вынесен «приговор» системе SS7. 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 LNP, с внедрением Бесплатного вызова по коду 888 и другие.

Будут ли операторы связи после подобных напоминаний спешить с переходом на IP протокол?

III Текущее состояние оборонной сети DISN

Ссылаясь на аналогию между DISN и NG9-1-1, воспользуемся новейшими методическими материалами по построению глобальной информационной сети DISN, в которых изложены:

- основы информационной архитектуры сети DISN [12,13],
- 916-страничный документ с описанием требования к унифицированным свойствам сервисов военной связи (Unified Capabilities, UC) от 2013 г. [14]
- 295-страничное описание основ UC для армии [15].

Напомним, как закладывались основы DISN, которые ныне являются тормозом ее модернизации.

Командование МО США (US Joint Chiefs of Staff) в 1996 году приняло 15-летнюю программу развития вооружений «Joint Vision 2010». В части средств связи основной выбор был сделан на интеллектуальные сети (Advanced Intelligent Network, AIN). При этом выборе подчеркивалось, что AIN обеспечивает пользователей любыми сервисами, как-то: голос, данные, e-mail, video, офисные приложения, вызовы «800». Отметим, что путь

к созданию интеллектуальной сети AIN был долгим. Прошло 25 лет до того, как в Bell Labs разработали и в 1982 году запустили в серию электронную АТС 5ESS, в которой реализованы принципы интеллектуальной сети и большой набор услуг Capabiliy Set 1 (CS1).

Простейшая схема сети SS7 и IN включает три узла (рис. 6а):

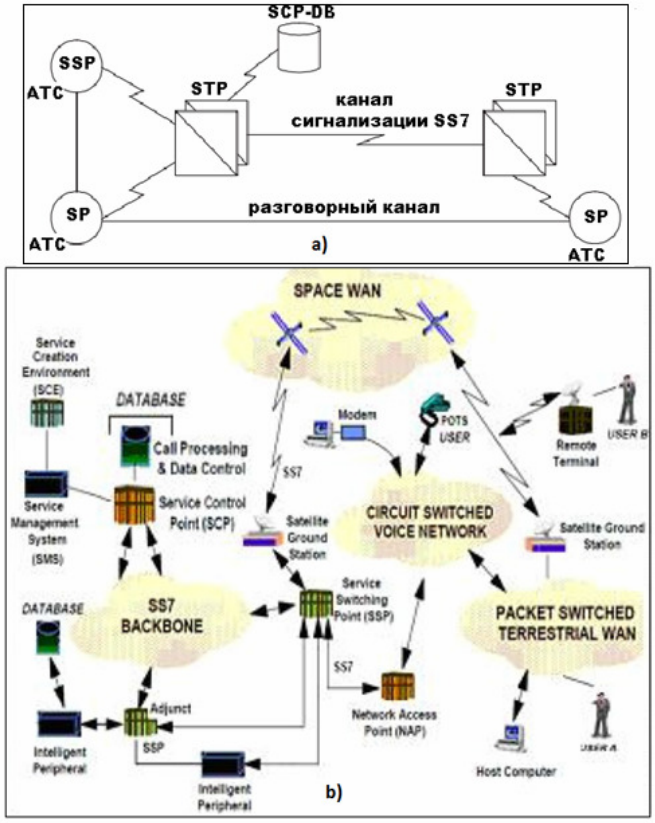


Рис. 6. a) Базовая архитектура сети SS7 и IN. b) Архитектура AIN в составе сети DISN.

• STP (Signaling Transfer Point) – транзитный узел сигнализации,

• SSP (Service Switching Point) – узел коммутации услуг, представляющий собой АТС с соответствующей версией программного обеспечения и выполняющий функцию управления вызовом и функцию коммутации услуги;

• SCP (Service Control Point) – контроллер услуг. SCP интерпретирует поступающие запросы, обрабатывает данные и формирует соответствующие ответы, общаясь с базой данных DB;

• каждая АТС имеет в своем составе пункт сигнализации SP.

Сеть сигнализации SS7 служит связующим звеном сети AIN (рис. 6b). Сеть SS7 обеспечивает доступ к базам данных (DATABASE). Пользователями AIN могут быть как абоненты сети коммутации каналов, так и коммутации пакетов. Важная роль отводится интеллектуальной периферии (Intelligent Peripheral): в ее функции входит генерация тонов, распознавание голоса, сжатие речи и данных, распознавание набора номера и многое другое, включая тактические и стратегические сервисы по идентификации персонала. Обратим внимание на очень существенную часть AIN – на среду разработки сервисов SCE (Service Creation Environment), которая содержит стандартные подпрограммы SIB (Service Independent Blocks). Например, имеется 17 SIB по версии ITU и 21 SIB по версии ETSI. На практике же их может быть более 100. По идее, эти интерфейсные средства позволяют привлекать сторонних программистов к разработке новых сервисов. Однако эти средства оказались слишком сложными и не получили распространения. Чтобы составить программу, программисту приходится знать детали телефонных сигнализаций.

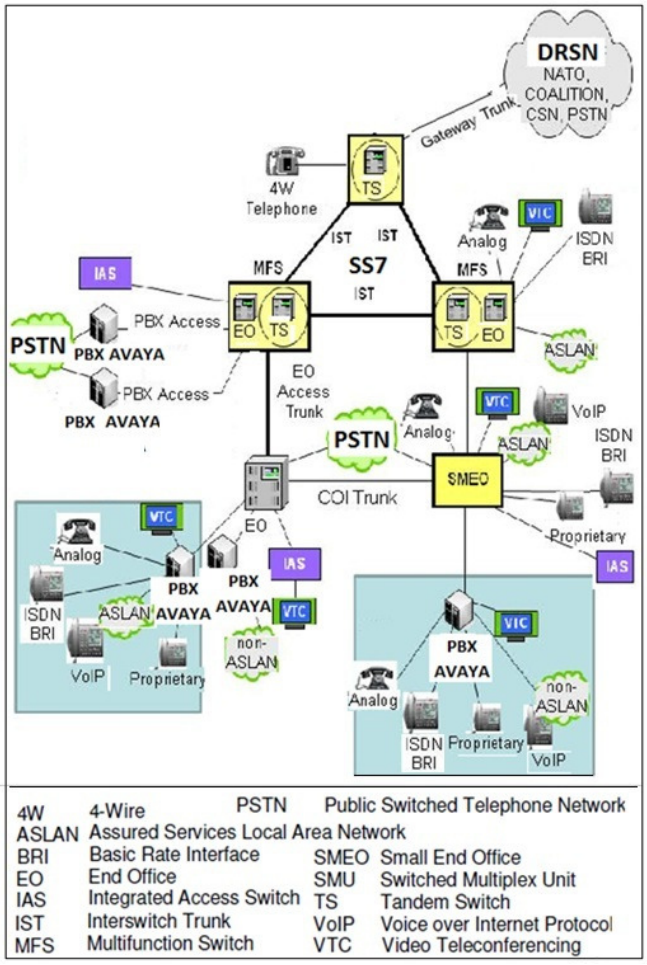


Рис. 7. Связь сервера PBX AVAYA с телефонными станциями MFS [16].

В те же 80е годы в мире разрабатывалась сеть ISDN (Integrated Services Digital Network) – цифровая сеть с интеграцией служб. ISDN позволяет совместить услуги телефонной связи и обмена данными. Основное назначение ISDN – передача данных по абонентской проводной линии и обеспечение интегрированных телекоммуникационных услуг (голос, данные, видео). В сети ISDN используется технология TDM. Для общения с Интернетом часто используют поток 128 кбит/с (объединяя два канала по 64 кбит/с). Соединения между абонентами ISDN устанавливаются посредством сигнализации SS7.

Архитектура сети DISN (на 2014 год) показана на рис. 7. Этот рисунок иллюстрирует тестирование коммуникационных серверов Avaya на сети DISN [16].

Серверы PBX Avaya включены в электронные АТС (на рис. 7 - это MFS, Multi-Functional Switch), которые имеют функцию SSP (в составе интеллектуальной сети AIN). Обратите внимание на сеть, изображенную на рисунке 7 в центре сверху. Это сеть сигнализации SS7. То есть на оборонной сети DISN соединения до сих пор устанавливаются при помощи сигнализации SS7.

Отсюда можно сделать важную рекомендацию для телекоммуникационных операторов России. Заметим, что пока неизвестно, когда планируется переход от сигнализации SS7 к протоколу AS-SIP. Тем самым не ясно, когда операторы связи откажутся от интеллектуальных сетей. Сеть AIN вполне может сосуществовать с сетью коммутации пакетов. При обсуждении технической политики «Ростелеком» следовало бы учесть опыт построения AIN и ее дальнейшее развитие в условиях наступления IP технологии. Наибольшие усилия по стыковке сигнализация SS7 и интеллектуальной сети с протоколом SIP предприняты компанией Telcordia (США). Напомним, что Telcordia является продолжателем работ Bell Labs по интеллектуальным сетям. В начале 1990х Telcordia разработала несколько версий архитектуры AIN. Результаты двадцатилетних разработок объединяет группа документов AINGR Family of Requirements, FR-15 [17]. Эти документы подводят итоги работ по использованию 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, в частности, Систему-112.

IV О ПЕРЕХОДЕ ОТ TDM К IP НА СЕТИ DISN

Следующий этап развития сети DISN начался в 2006 г., когда был принят новый план Пентагона «Joint Vision 2020» – на следующие 15 лет. В этом плане объявлена смена парадигмы сети DISN – переход от сигнализации SS7 к IP протоколу. Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями.

Согласно программе МО США о переходе на IP технологию к 2012 году установлено 22 мощнейших софтсвичей MFSS компании Cisco на американских базах по всему миру [18]. К 2016 г. планировалось довести эти узли до функциональности, представленной ниже на рис. 8B. Но пока неизвестно, когда же произойдет переход от сигнализации SS7 к протоколу AS-SIP на всей сети DISN.

Напомним, что SoftSwitch (программный коммутатор) обеспечивает стык коммутации каналов с коммутацией пакетов (рис. 8A). Он согласовывает протоколы сигнализации SS7 и SIP (посредством шлюза сигнализации SGW) и медиапотоки IP и TDM (посредством медиашлюза MGW). Рисунок 8A показывает, как многофункциональный софтсвич MFSS управляет вызовами:

- 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 Signalling).
- MFSS действует как медиашлюз (MG) между TDM каналами и IP каналами. Медиашлюзом управляет контроллер MGC посредством протокола H.248.
- Шлюз сигнализации SG (Signaling Gateway) обеспечивает взаимодействие между CCS7 и SIP.

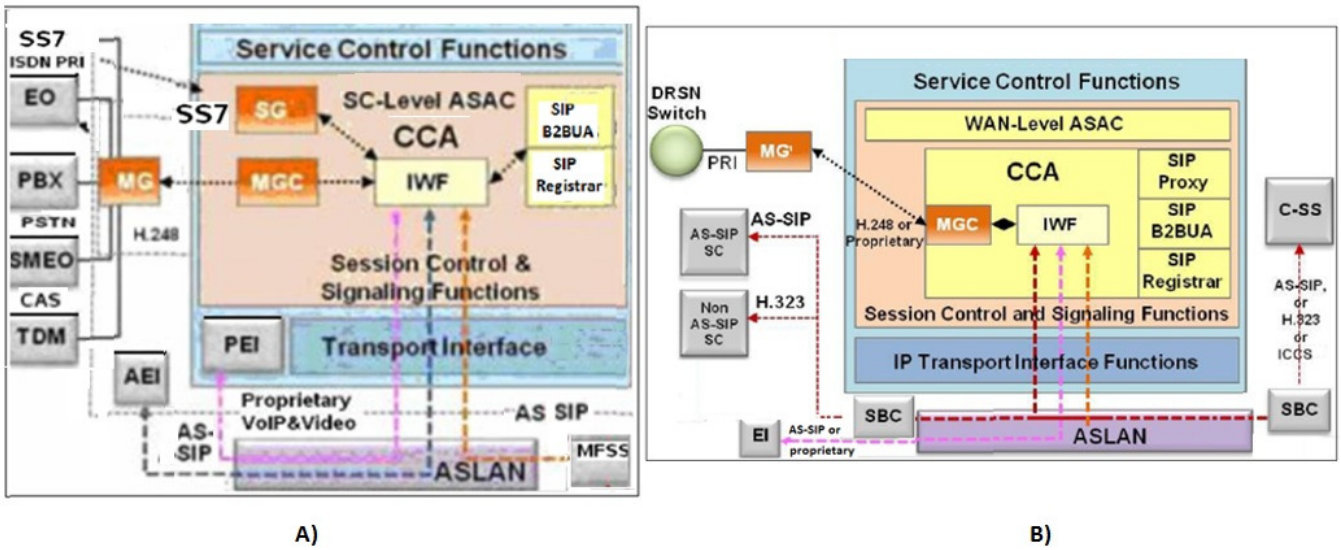


Рис. 8. A) Текущая версия MFSS (Multifunction SoftSwitch). B) Будущая версия MFSS (каналы ISDN сохраняются только на правительственной сети DRSN).

На рис. 8A еще указаны оконечные устройства EO (End Office) в сети коммутации каналов и два типа IP устройств: AEI (Assured Services End Instrument), работающие по протоколу AS-SIP, и нестандартные устройства PIE (Proprietary Internet Protocol Voice End Instrument). В будущем (рис. 8B) должен остаться единый протокол AS-SIP.

Отметим особенности протоколов SIP и AS-SIP. Протокол SIP (RFC 5638: Simple SIP) пользуется услугами 11 других протоколов, в том числе SOAP, HTTP, XML, VXML, WSDL, UDDI, SDP, RTP, что обеспечивает такие сервисы, как presence, instant messaging, audio и video communications. Протокол Assured Services SIP является намного более сложным[19]. Прежде всего он обеспечивает обслуживание приоритетных вызовов (до 6 приоритетов), пользуясь механизмом MLPP (Multi-Level Precedence and Preemption). Для выполнения требований информационных свойств UC (Unified Capabilities) протокол AS-SIP использует почти 200 других стандартов RFC.

Состав сервисов в перспективной структуре сети DISN определяет блок „Service Control Function", что раскрывает рис. 9.

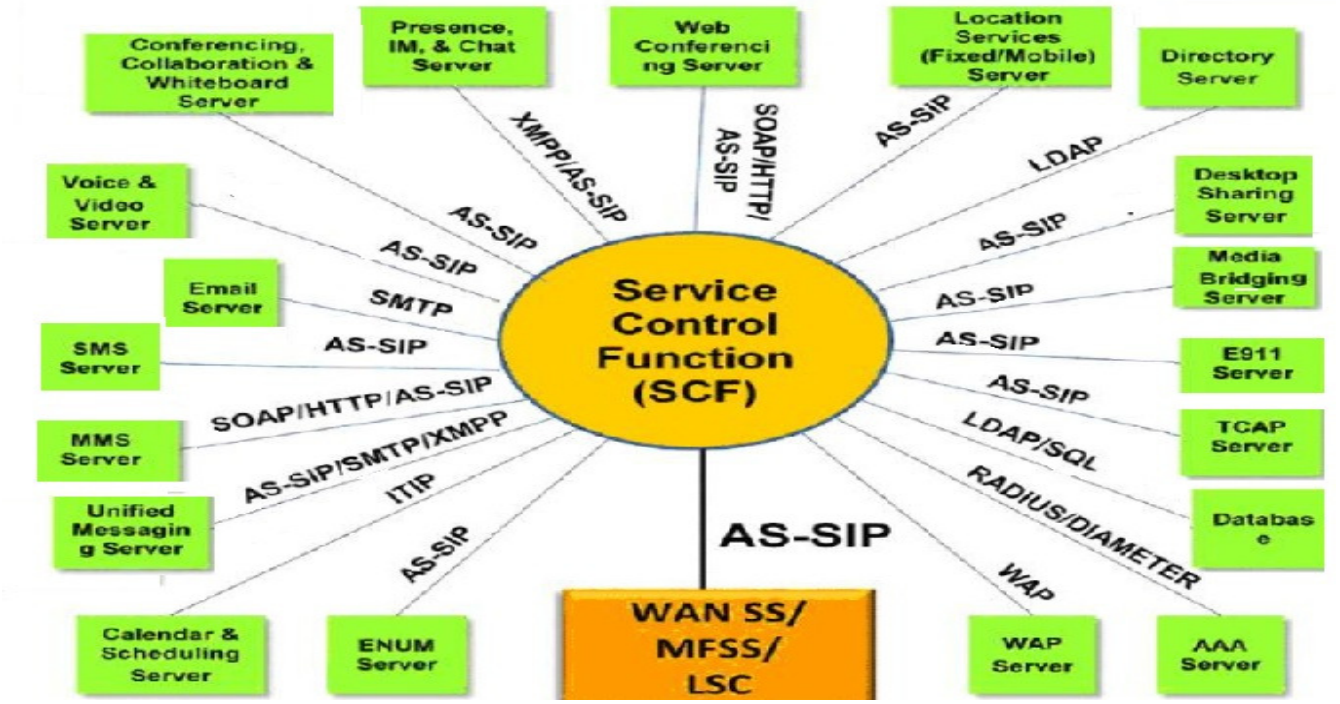


Рис. 9. Базовая модель функции контроля сессии SCF и ее 19 серверов.

Для общения с контроллерами MFSS узел SCF использует единый протокол AS-SIP, а для общения с серверами разных сервисов используется множество других протоколов:

- SOAP = Simple Object Access Protocol,
- HTTP = HyperText Transport Protocol,
- LDAP = Lightweight Directory Access Protocol,
- RADIUS = Remote Authentication Dial In User Service,
- DIAMETER = расширенная версия RADIUS,
- WAP = Wireless Access Protocol,
- ITIP = iCalendar Transport Independent Interoperability Protocol,
- SMTP = Simple Mail Transfer Protocol,
- AAA = Authentication, Authorization, and Accounting,
- TCAP = Transaction Capabilities Application Part,
- ENUM =E.164 Number,
- IM = Instant Messaging,
- MMS = Multimedia Messaging Service,
- SMS = Short Message Service,

На рис. 9 по кругу изображены 19 серверов. Это могут быть 19 программ в составе софтсвича как физического объекта, а могут быть и 19 удаленных объектов. Среди них имеются 16 серверов, которые представляют 16 сервисов реального времени (Real-Time Communications), и еще три выделенных сервера:

- TCAP сервер - обеспечивает выход на базы данных интеллектуальной сети AIN,
- AAA сервер - обеспечивает услуги Authentication, Authorization, and Accounting и пользуется протоколами RADIUS и DIAMETER,
- Database сервер - содержит данные, которые доступны по протоколам LDAP и SQL.

Унификация услуг связи. Обратим особое внимание на крупнейшую задачу DISN – на унификацию информационных свойств UC (Unified Capabilities). В будущей сети DISN все услуги (голос, видео и данные) должны предоставляться по IP протоколу. Новая архитектура унифицированных свойств UC [13] предлагает любому солдату и армейскому служащему богатый набор средств общения: e-mail, чат, голос, видео, поиск и многое другое, и все это доступно по единому адресу пользователя и в безопасной среде.

Управление сеансом связи происходит по единому протоколу AS-SIP. Сетевая архитектура унифицированных свойств основана на широкополосной IP сети (wide area IP backbone network) и на протоколе MPLS (multiprotocol label switching protocol), который обеспечивает требуемое качество связи QoS в сети коммутации пакетов. На основе унифицированных свойств UC реального времени предлагается создать восемь сервисов связи:

- Email and Calendaring
- Instant Messaging and Chat
- Rich Presence
- Unified Messaging
- Video Conferencing
- Voice and Video (Point-to-Point)
- Voice Conferencing
- Web Conferencing and Web Collaboration

В настоящее время только началось внедрение новых свойств и новых сервисов DISN. Время покажет, как из этих «строительных блоков» (Unified Capabilities) будут строиться новые сервисы и какие из них найдут применение.

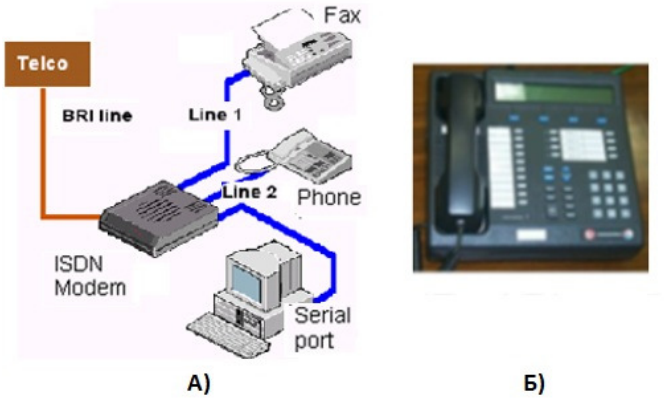


Рис. 10. А) Иллюстрация использования ISDN линии. Б) «Красный» телефон. (Обратите внимание на щель справа внизу – для криптокарты и на 4 кнопки наверху для выбора приоритетности разговора.) В) Схема правительственной сети DRSN.

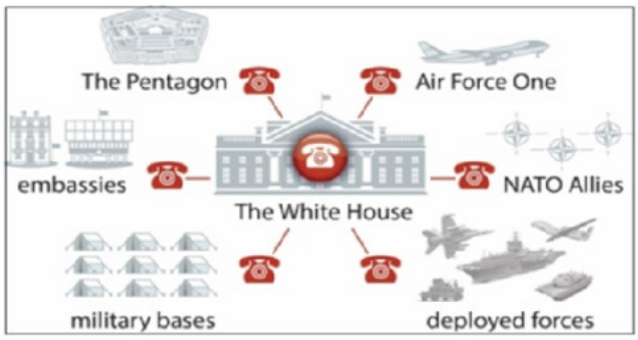
В качестве второй трудности (Таблица 1) укажем на дороговизну магистральных маршрутизаторов по сравнению с электронными АТС: ЭАТС мощностью 10 млн одновременных разговоров стоит 10 раз дешевле маршрутизатора такой же мощности [20].

Таблица 1. Сравнение TDM коммутатора и пакетного коммутатора [20].

	TDM коммутатор CIENA Core Director	Пакетный коммутатор CISCO CRS-1
Пропускная способность	640 Гб/с	640 Гб/с
Потребляемая энергия	1440 Ватт	9630 Ватт
Цена	$84,000	$884,000

О трудностях перехода к IP на сети DISN. Первая и очень важная трудность связана с правительственной связью DRSN (Defense RED Switched Network), которая является своеобразным «родимым пятном», сохраняя ISDN каналы на сети DISN, которая строится по единому протоколу AS-SIP.

Сверхсекретная сеть DRSN — это выделенная телефонная сеть, которая обеспечивает управление вооруженными силами США (рис. 10В). В текущих методических материалах по DISN [12] не предусмотрен перевод сети DRSN на коммутацию пакетов. Сеть DRSN, вопреки желанию идеологов DISN, сохраняет имеющуюся технологию коммутации каналов, точнее, ISDN (Integrated Services Digital Network) каналы (рис. 10А). Поэтому маршрутизатор сети DISN вынужден работать не только на сети коммутации пакетов, но и на сети коммутации каналов.



ПО	3 млн. строк	8 млн. строк

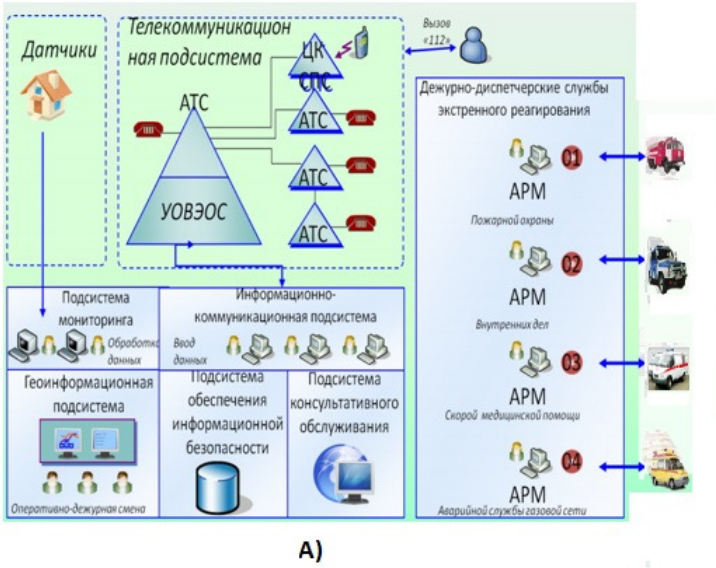
По крайней мере, в столько же раз дешевле обходится и программное обеспечение: сравните 3 млн. строк для TDM коммутатора с 8 млн. строк для маршрутизатора CISCO. Отметим, что пакетную коммутацию выгодно использовать на сетях доступа, но на магистральном звене (на потоках между узлами автоматической коммутации УАК), где обслуживается только транзитный трафик, коммутация каналов имеет несомненное преимущество.

V МЧС НЕ СПРАВЛЯЕТСЯ С РОЛЬЮ КООРДИНАТОРА

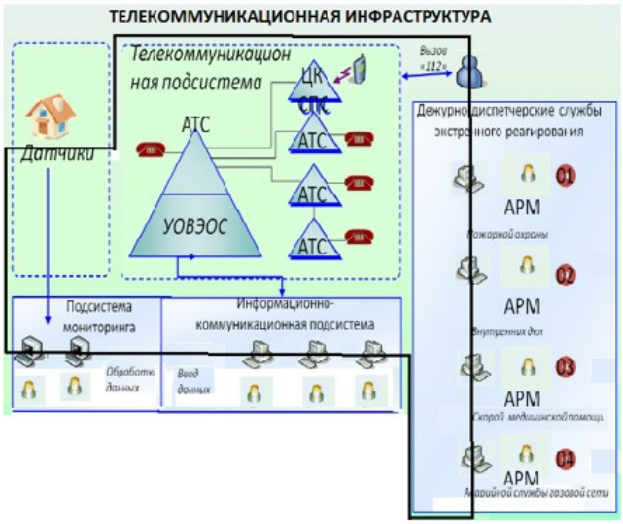
Несмотря на то, что разработка Системы-112 длится уде почти 20 лет, до сих пор отсутствуют технические требования на телекоммуникационную инфраструктуру (ТТ-ТИ) этой системы. В этом суть нашего упрека в адрес МЧС. Сошлемся на программный доклад заместителя начальника ФГБУ ВНИИ ГОЧС профессора С.А. Качанова [21].

Рис. 11А взят нами из этого доклада. Телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы (рис.

6Б). К тому же мы опустили три подсистемы (геоинформационную, информационной безопасности и консультационного обслуживания), которые тоже частью входят в телекоммуникационную инфраструктуру и должны быть подробно описаны в ТТ-ТИ.



А)



Б)

Рис. 11. А) Новейшее представление Системы-112 (по мнению МЧС): Минкомсвяь отвечает только за телекоммуникационную подсистему. Б) Телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы.

Процесс раздела ответственности по Системе-112 длился годами. Шел спор по разделению полномочий между ведомствами, отвечающими за построение системы. Только в декабре 2010 года президент России Дмитрий Медведев подписал указ [22], 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 не разработанными. 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 и АПК БГ. Введение зон ответственности различных ведомств, по нашему мнению, только служит формальным прикрытием «безответственности».

Рис. 12. Новый вид сервиса, обеспечивающий доступ к Системе - 112 всеми видами обращений: голос, видео и текстовые сообщения [21].

При таком положении дел вряд ли целесообразно говорить о новом поколении Системы-112, как это показано на рис. 12 (из выше упомянутого доклада [21]). Прототипом разработки технических требований для реализации архитектуры, представленной на рис 12, мог бы служить 916-страничный документ с описанием требований к унифицированным свойствам сервисов военной связи (Unified Capabilities, UC) от 2013 года [14].

Только в 2015 году МЧС и Минкомсвязь согласовали «Методические рекомендации по разработке системных проектов телекоммуникационной подсистемы системы обеспечения вызова экстренных оперативных служб по единому номеру «112» для субъектов Российской Федерации [23]. В этом документе утверждается, что «…системный проект является проектным документом стадии ПП (предпроектная проработка). Системный проект является основанием для разработки операторами связи проектной и рабочей документации на вновь вводимые, реконструируемые и модернизируемые узлы, линии и системы связи для создания телекоммуникационной подсистемы Системы-112». Отметим особо, что речь идет всего лишь о предпроектной проработке (!). «Методические рекомендации» появились как выполнение федеральной целевой программы [24], но заметим, что в ФЦП 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».

VI Минкомсвязь избегает ответственности

Такое впечатление создается после изучения соответствующих документов Минкомсвязи. Вот новейший пример. На сайте Минкомсвязи 18 января 2016 опубликованы «Методические рекомендации по обеспечению информации о месте нахождения пользовательского оборудования» [25]. Этот документ (см. рис. 13Б) повторяет прежнюю концепцию 2012 года (рис. 13А), разработанную с участием компании «Светец» [26]. Новым является интерфейс 6 для выхода на собственный узел ТСКС – технические средства коротких текстовых сообщений. И в новой версии упор делается на веб-технологии: протоколы SIP и HTTPS. Как и ранее, информационные потоки и интерфейсы предоставления информации в Систему-112 оператором связи недостаточно четко прописаны. Одним из недостатков документа [25] является отсутствие требований о точности местоположения абонента.

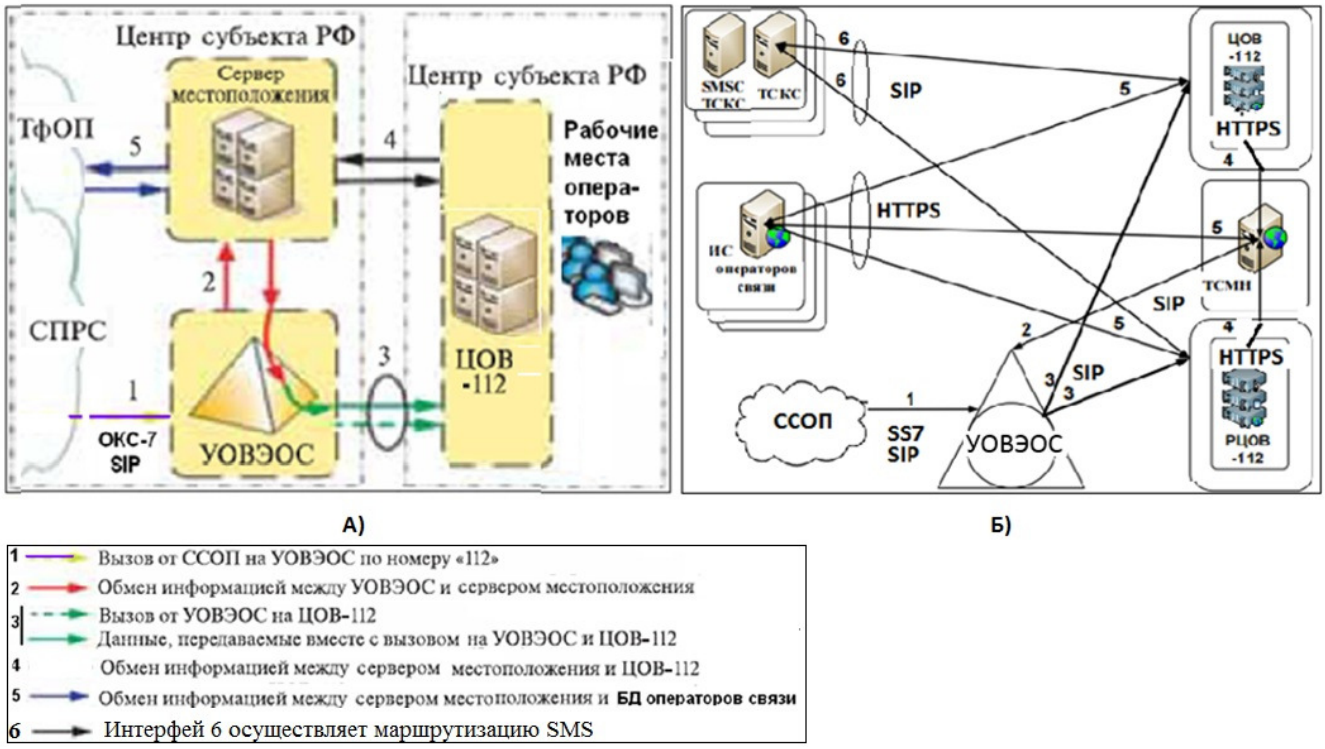


Рис. 13. А) Место сервера местоположения и пять интерфейсов информационных потоков в телекоммуникационной составляющей Системы-112 (2012). Б) Новейшее представление о взаимодействии в Системе-112 (2015).

Здесь:

УОВЭОС – узел обработки вызовов экстренных оперативных служб.

ОКС № 7 – система сигнализации по общему каналу № 7 (SS7).

ТСМН – технические средства местонахождения.

ТСКС – технические средства коротких текстовых сообщений.

УОВЭОС – узел обеспечения вызовов экстренных оперативных служб.

SMSC – центр SMS.

На рис. 13А приведены пять интерфейсов системы 112, которые предполагалось уточнить на первом этапе работ в соответствии с Постановлением (до 2014 г.). Это исключительно сложная работа. Кроме того, представленную концепцию Системы 112, на наш взгляд, следовало бы существенно доработать. Выскажем три замечания:

- О протоколе SIP. Сомнения вызывает его включение в систему 112 наряду с ОКС-7. Для этого он еще недостаточно апробирован – с учетом чрезвычайной важности системы для государства.
- О перегрузках. На схеме показано прохождение отдельного вызова в Системе-112. А как поступать в условиях реальных ЧП, когда из-за перегрузки имеющихся ресурсов экстренных служб часть вызовов может быть потеряна (что недопустимо)? В случаях действительно крупных ЧП в распоряжение МЧС должны были бы поступать и другие центры обработки вызовов (ЦОВ), в том числе ЦОВ «Ростелекома», что на схеме не показано.
- Не указаны средства доступа (абонентские устройства) к Системе-112, в том числе телематические средства защиты охраняемых объектов, которые также относятся к телекоммуникационной составляющей.

До сих пор совсем упущены вопросы программного обеспечения, сложность которых демонстрирует рис. 1.

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 [27].

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 АПК «Безопасный город».

VII Соображения о построении Системы-112 и АПК «Безопасный город»

Если взять курс на импортозамещение, т.е. на развитие сетей связи собственными силами, то, на наш взгляд, следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их дальше. Такой точкой отсчета условно можно назвать каналы ISDN, систему ОКС-7 и интеллектуальные сети.

Уровень разработок средств связи в России отстает от передового мирового уровня, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника. Но тем более стоит оценить перспективы коммутации каналов, где не требуются столь высокое быстродействие. Следовательно, мы предлагаем сосредоточиться на данном этапе на использование ранее апробированных технологий коммутации каналов.

Единая «Система-112» в масштабах страны, на наш взгляд, должна опираться на междугородную сеть России.

ISDN, SS7 и IN. Сделаем несколько важных замечаний к схемам на рис. 14.

1) Обратите внимание, что по сигнализации ISUP запрос на соединение “1a. IAM” идет через один STP, а согласие на ответ “2a. ACM” проходит через другой STP.

2) В классической схеме интеллектуальной сети (рис. 14Б) несколько коммутаторов услуг SSP выходят на общий контроллер услуг SCP, точнее, на единую базу данных. Например, в США за номером бесплатной услуги «800» идет номер услуги, т.е. вызов маршрутизируется на базу данных этой услуги «800», которая является единой на всю страну.

3) По другому принципу устроена российская интеллектуальная сеть. В действительности же в России в основном реализована упрощенная схема IN (рис. 14В). Коммутатор услуг SSP выходит непосредственно на собственной контроллер услуг SCP, поэтому указан совмещенный узел SSCP (обычно размещен на АМТС). А так как узлы SSP и SCP находятся в составе единого узла SSCP, то между ними не обязательно использовать протокол INAP-R.Поясним эту важную 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. Коммутатор услуг SSP и контроллер услуг SCP совмещены в едином узле SSCP и находится на АМТС. Следовательно, между SSP и SCP можно общаться не только по протоколу INAP, но и любому другому протоколу.

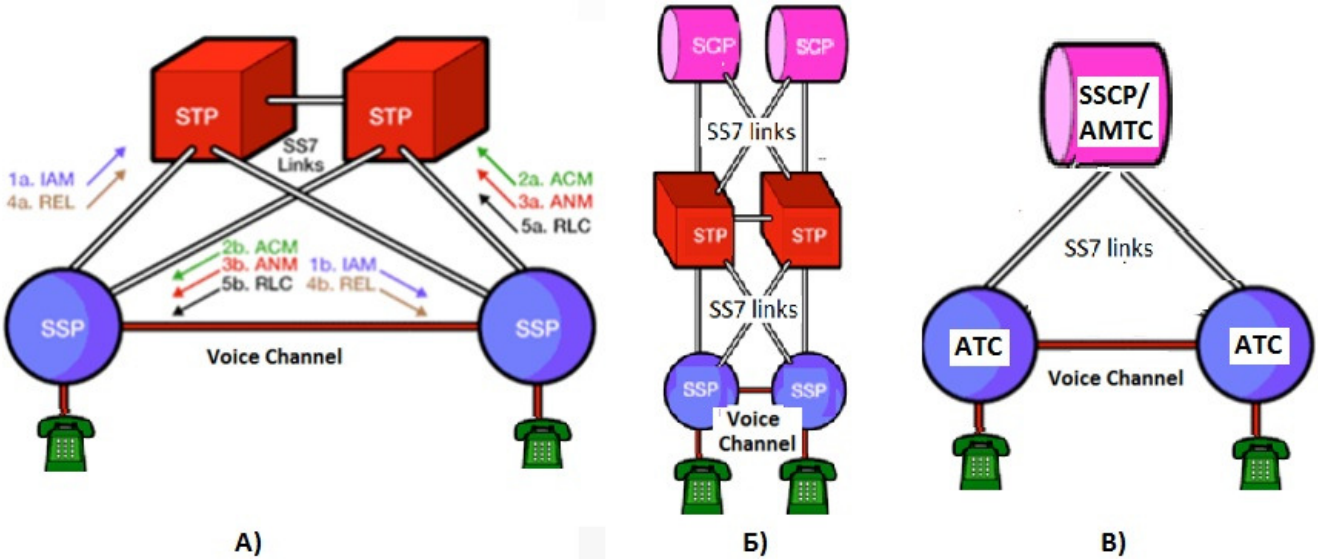


Рис. 14. А) Сигнализация ISUP в сети ISDN. Б) Классическая схема интеллектуальной сети. В)

Российская реализация интеллектуальной сети.

Сеть GSM [28]. Построение Системы-112 предполагает использование мобильных сетей, особенно для передачи сообщений SMS. Поэтому рассмотрим сеть GSM подробнее. Она представляет собой иерархическую структуру, принцип построения которой приведен на рис. 15. Первый уровень включает мобильные центры коммутации MSC. Взаимодействие сети GSM со стационарной сетью ТфОП осуществляется через шлюз мобильного центра коммутации GMSC, подключенный к АМТС. Второй уровень иерархии GSM – транзитная сеть, представляющая собой транзитные центры коммутации (ТЦК), выполняющие для мобильных абонентов те же функции, что и УАК для ТфОП.

Выделим два режима прохождения мобильного вызова. Первый режим. При взаимодействии федеральной сети GSM с фиксированной сетью ТфОП на международном уровне возможны соединения мобильной станции MS с телефонным аппаратом (ТА) стационарной сети ТфОП по цепочке:

MS - MSC - GMSC - ТЦК - УАК - АМТС - АТС - ТА

Второй режим. Кроме ТЦК уровень транзитной сети может включать также локальные центры коммутации (ЛЦК). ЛЦК является промежуточным уровнем иерархии федеральной сети GSM. ЛЦК является узлом доступа к транзитной сети и соединяется не менее чем с двумя ТЦК. В этом случае взаимодействие мобильной станции и стационарного телефонного абонента при междугородней связи осуществляется по схеме:

MS - MSC - GMSC - ЛЦК - ТЦК - УАК - АМТС - АТС – ТА

Важно отметить, что связующей сетью является сеть сигнализации SS7.

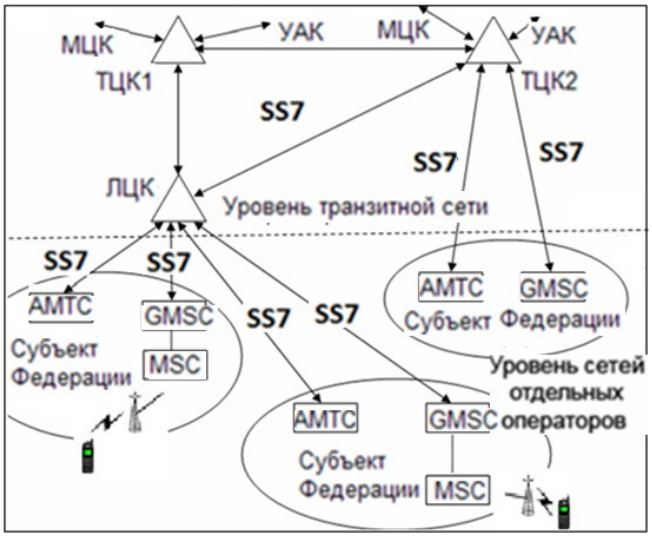


Рис. 15. Иерархия федеральной сети общего пользования GSM: ведущая роль SS7.

Как работает Центр SMS [29]. Отметим особенность передачи сообщений SMS. Они передаются по сети ОКС-7, как и сообщения об установлении телефонных соединений, но SMS не пользуются приоритетом. То есть при перегрузках сети будут обслужены в последнюю очередь или вовсе потеряны, что недопустимо для экстренных вызовов.

В процессе отправки/доставки SMS участвуют следующие элементы сети:

- MS (Mobile Station) – телефоны отправителя и получателя смс;
- MSC (Mobile Switching Centre) – коммутатор, который обслуживает подвижных абонентов - получателя и отправителя смс;
- SMSC (SMS Centre) – центр коротких сообщений. Находится в сети отправителя;
- HLR (Home Location Register) – узел сети GSM, который среди прочего хранит информацию о текущем коммутаторе (MSC) получателя SMS.

Рис. 16. Алгоритм обмена сообщениями SMS (упрощенная схема).

Пояснения к рисунку 16:

- Абонент А отправляет SMS абоненту В.
- В MS абонента А указан номер центра коротких сообщений (SMSC), через который и будет произведена доставка SMS.
- Сообщение отправляется на коммутатор абонента А, оттуда на SMSC.
- SMSC не знает текущий коммутатор абонента В, поэтому запрашивает эту информацию у HLR. поскольку адрес HLR тоже не известен, то сообщение Send Routing Info for SM отправляется на адрес абонента В. Сеть получателя отвечает за то, что сообщение SRI-SM будет смаршрутизировано на соответствующий HLR (в одной сети их может быть несколько).
- HLR возвращает в качестве ответа текущий MSC абонента, а также его мобильный номер - IMSI.
- SMSC отправляет SMS на коммутатор абонента В, а тот в свою очередь на терминал получателя.
- Если абонент А запросил отчёт о доставке, и

доставка была успешной, то SMSC генерирует отчёт о доставке и отправляет его абоненту А.

VIII Заключение

Если взять курс на импортозамещение, т.е. на развитие сетей связи собственными силами, то следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их дальше.

Поскольку за прошедшие 25 лет строительства капитализма в России операторы связи ориентировались на использование и эксплуатацию иностранной техники, то потеряны навыки разработки, не проводились исследования по стратегии развития телекоммуникаций. Регуляторы отрасли связи фактически пустили отечественное телекомо-строение на рыночные рельсы при почти полном отсутствии регуляции со стороны государства.

Задача 1. Для создания АПК «Безопасный город» необходимо организовать подготовку специалистов, способных:

- разрабатывать нормативные документы по созданию сетей связи с коммутацией каналов и с пакетной коммутацией;
- разрабатывать специализированные аппаратные средства сетей связи; разрабатывать программные средства сетей связи (в том числе следует внимательно отнестись к европейскому опыту, например, FIWARE [30]).

Задача 2. Необходимо разработать Технические требования на информационную инфраструктуру АПК «Безопасный город», включая Систему-112 и Систему оповещения. При этом следует учесть:

(1) чрезвычайную важность эвакуационной готовности населения,

(2) отсутствие разработанного системного проекта службы 112,

(3) наличие аналогии между сетями связи оборонного ведомства и экстренной службы.

Поэтому предлагаем рассмотреть возможность создания единой сети связи не только для Системы-112 и АПК «Безопасный город», но и для МЧС в целом, что будет представлять собой сеть связи гражданской обороны нового поколения NG112.

Задача 3. Для взаимодействия объектов сеть передачи данных АПК «Безопасный город» играет важнейшую роль. С целью увеличения надежности следует пересмотреть архитектуру взаимодействия объектов в сети передачи данных АПК «Безопасный город», перейти с клиент-серверной архитектуры (ЦОД и терминалы), на полностью распределённую архитектуру, в которой каждый объект выступает в качестве терминала и сервера одновременно. Все объекты должны взаимодействовать друг с другом в доменной одноранговой сети с использованием протоколов динамической маршрутизации, при которых выход из строя одного из объектов не приводит к остановке работы всей системы (например: DDS (publish/subscribe) с заданными QoS). То есть, в сети взаимодействующих объектов нет сетецентризма, как такового, на физическом уровне, но он есть на логическом уровне (как сетецентризм).

Это особенно относится к сенсорным сетям, подвижным объектам, оперативным штабам на месте ЧС и другим мобильным компонентам.

Зоны обмена сообщениями могут пересекаться с глобальными сетями передачи данных

Библиография

[1] Шнепс-Шнеппе М.А., Селезнев С.П., Куприяновский В.П. Сеть DISN как прототип сети связи гражданской обороны NG112//International Journal of Open Information Technologies ISSN: 2307-8162. 2016. – Т. 4. – №. 5. – С. 39-47.

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

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

[4] Определен формат маршрутного номера вызова экстренных оперативных служб http://minsvyaz.ru/ru/events/35141/

[5] Model State 911 Plan, National Association of State 911 Administrators, DOT HS 811 369 February 2013.

[6] Шнепс-Шнеппе М.А., Намиот Д.Е. Об эволюции телекоммуникационных сервисов на примере GIG // International Journal of Open Information Technologies. 2015. – Т. 3. –№1 – С.1-13.

[7] М.А. Шнепс-Шнеппе, Д.Е. Намиот, В.А. Сухомлин О создании единого информационного пространства общества // International Journal of Open Information Technologies. 2015. – Т. 3. – №2 – С.1-10.

[8] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative System Description and High-Level Requirements Document, Version 1.1. July 31, 2007.

[9] «911 text messaging service coming in 2014». http://edition.cnn.com/2012/12/07/tech/mobile/fcc-carriers-announce-text-to-911

[10] Michael Schmitt Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE International Conference on Technologies for Homeland Security May 2008 http://www.inl.gov/technicalpublications/Documents/3901033.pdf Retrieved: Mar, 2016

[11] М.А. Шнепс-Шнеппе “Разработка системы 112 в условиях импортозамещения”// Электросвязь, №4, 2015, с. 40-44.

[12] DoD Information Enterprise Architecture (IEA), Vol. I&II, Version 2.0, July 2012.

[13] Department of Defense Information Enterprise Architecture Unified Capabilities Reference Architecture, Version 1.0, January 2013.

[14] Department of Defense Unified Capabilities Requirements 2013 (UCR 2013) January 2013.

[15] 15U.S. Army Unified Capabilities (UC) Reference Architecture (RA), Version 1.0 11 October 2013.

[16] Special Interoperability Test Certification of Avaya S8300D. DISA Joint Interoperability Test Command (JTE), 17 April 12.

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

[18] Department of Defense. Unified Capabilities Framework 2013. January 2013. 12. Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Version 1.0, June 2007.

[19] Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP). Errata-1, July 2013.

[20] Saurav Das, Guru Parulkar, and Nick McKeown „Rethinking IP Core Networks” J. OPT. COMMUN. NETW./VOL. 5, NO.12/DECEMBER 2013 http://dx.doi.org/10.1364/JOCN.99.099999

[21] 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

[22] Указ Президента РФ от 28.12.2010 N 1632 «О совершенствовании системы обеспечения вызова экстренных оперативных служб на территории Российской Федерации».
[23] «Методические рекомендации по разработке системных проектов телекоммуникационной подсистемы системы обеспечения вызова экстренных оперативных служб по единому номеру «112» для субъектов Российской Федерации», МЧС и Минкомсвязь, Москва, 2015.
[24] Постановление Правительства Российской Федерации от 16 марта 2013 г. №223 «О федеральной целевой программе "Создание системы обеспечения вызова экстренных оперативных служб по единому номеру "112" в Российской Федерации на 2013-2017 годы»
[25] «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». Минкомсвязь, 18 января 2016.
[26] Полканов Е.И., Мазин И.Г. Совместное использование информационных ресурсов: консолидация развития сетей// Электросвязь. – 2012. – № 3.
[27] Меры по поддержке российского ПО http://minsvyaz.ru/ru/events/34921
[28] ОКС 7 в GSM http://ru.bmstu.wiki
[29] SMS forwarding http://www.mib.net.ua/2011/02/sms-forwarding.html
[30] Д.Е. Намиот, В.П. Куприяновский, С.А. Синягов Инфокоммуникационные сервисы в умном городе // International Journal of Open Information Technologies. 2016. – Т. 4. –№4. – С.1-9.

On telecom infrastructure for the “Safe City” program

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

Abstract— **In this paper, we consider the US experience in the creation of two complex systems: a global information network and the defense department DISN single network to service the new generation NG9-1-1 emergency calls. This paper provides the analysis of work of Ministry of Emergency Situations (Russia) on creating the hardware-software complex "Safe City" and analysis of the Ministry of Communications. We provide some considerations for the construction of systems and APC-112 "Safe City" in terms of import substitution, in other words, with an emphasis on the development of communication networks on their own. This involves the use of past experience of switching channels (ISDN channels, SS7 system, and the intelligent network). In this paper, we formulate three objectives: to train specialists, to develop the technical requirements for the information infrastructure of the "Safe City" program, and to transform the "Safe City" from the client-server architecture (data center and terminals) to a fully distributed architecture, in which each object appears in as the terminal and the server simultaneously.**

Keywords—safe city, distributed architecture, telecom, 112 system.