К системному проектированию Системы 112 и комплекса «Безопасный город»

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

***Аннотация*— В статье обсуждаются основные новые задачи, стоящие перед отраслью связи: импортозамещение, разработка Системы 112 и комплекса «Безопасный город», интернет вещей и защита объектов критической инфраструктуры. Уточняются задачи, стоящие перед ведомствами МЧС и Минкомсвязь, а также Ростелеком. Анализируется развитие отрасли связи: внедрение интеллектуальных сетей, сигнализации ОКС-7 и системы IMS. Рассмотрена сеть DISN как прототип Системы 112 и комплекса «Безопасный город», а также проблемы разработки программного обеспечения, что затрудняет реализацию проектов модернизации сети DISN. В заключении перечисляются первоочередные задачи российских связистов.**

***Ключевые слова*—связь, Система 112, безопасный город, сигнализация ОКС-7, интеллектуальная сеть.**

I. Введение

Чем характерен текущий момент в российской отрасли связи, в отрасли народного хозяйства, важнейшей как для гражданских, так и специальных нужд [1]:

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 том числе Системы 112 и комплекса «Безопасный город».

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

Далее, в настоящем Разделе 1 обсуждаются основные новые задачи, стоящие перед отраслью связи: импортозамещение, разработка Системы 112 и комплекса «Безопасный город», вопросы интернета вещей и межмашинного общения M2M, защита объектов критической инфраструктуры. В Разделе 2 уточняются задачи, стоящие перед ведомствами МЧС и Минкомсвязь, а также Ростелеком. В Разделе 3 анализируется развитие отрасли связи: внедрение интеллектуальных сетей, сигнализации ОКС-7 и системы IMS. В Разделе 4 рассматривается сеть DISN как прототип Системы 112 и комплекса «Безопасный город». Раздел 5 посвящен проблемам разработки программного обеспечения, что затрудняет реализацию проектов модернизации сети DISN. В Разделе 6 перечисляются первоочередные задачи российских связистов.

Статья получена 10 июля 2016.

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

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

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

Куприяновский В.П., МГУ имени М.В. Ломоносова, (email: vpkupriyanovsky@gmail.com).

A. Импортозамещение – момент истины для «Ростелеком»

На Всероссийской конференции «Взгляд в электронное будущее», прошедшей в октябре 2014 г. в Сочи по инициативе «Ростелекома» и Правительства России, обсуждался вопрос импортозамещения в области ИТ. «Ростелеком» является партнером множества проектов: государственных инфраструктурных (устранение «цифрового неравенства», ЕГЭ, электронное правительство), отраслевых (медицина и образование, «112», «Безопасный город», КСЭОН) и инновационных (гео-информационные системы, ЖКХ).

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

Необходимость импортозамещения – это одна из сторон текущего момента в области телекоммуникаций. Другая касается сути импортозамещения – на какую же технику направлять усилия: на традиционную коммутацию каналов КК или на новомодную коммутацию пакетов КП, которую агрессивно продвигают иностранные производители. Это очень сложный выбор, это своеобразное противостояние поколений, как «отцы и дети».

Международные санкции стали, можно сказать, поворотным моментом в российской экономике новейшего времени, тем более для средств связи, которые, как правило, имеют двойное применение.

B. Система 112 и комплекс «Безопасный город»

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

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

Построение Системы 112 идет с большим трудом, а работы ведутся уже долгие 20 лет. И строится она по отдельным областям, а не для всей страны в целом. В официальном отчете Минкомсвязи России от 2013 г. [2] перечислены нерешенные задачи: «Ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей связи общего пользования (ССОП) для прохождения вызовов, поступающих в службу по номеру „112”. Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений».

В настоящее время выполняется Федеральная целевая программа «Создание системы обеспечения вызова экстренных оперативных служб по единому номеру 112 на 2013–2017 гг.». Согласно ФЦП, в 2013 г. Систему 112 планировалось внедрить в трех субъектах России, в 2014 г. – в шести, в 2015 г. – в двух, в 2016 г. – в пяти, а в 2017 г. запустить в оставшихся 67 регионах. По состоянию на 13 мая 2016 года Система 112 введена в промышленную эксплуатацию только в Калужской и Курской областях и в Республике Татарстан. До сих пор так и не разработан единый системный проект службы 112, и тем самым все проведенные работы, скорее всего, следует рассматривать как экспериментальные образцы.

Система 112 является частью АПК «Безопасный город», поэтому эти системы будем рассматривать совместно. Аппаратно-программный комплекс «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.

В США строится единая сеть нового поколения для обслуживания экстренных вызовов NG9-1-1, строится уже продолжительное время. Рассмотрение опыта США помогает, на наш взгляд, понять, почему так трудно выполнить намеченные задачи. В качестве иллюстрации многообразия требований экстренной службы приводим схему деятельности нового поколения службы NG9-1-1 отдельного штата США. Согласно официальным документам [3], будущие сети экстренных служб должны быть сетями пакетной коммутации. Особенно отмечается, что сеть NG9-1-1 должна поддерживать мультимедиа и практически охватывать все стороны общественной жизни, как показывает рис. 1. Единая сеть штата (State Backbone Network) объединяет:

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

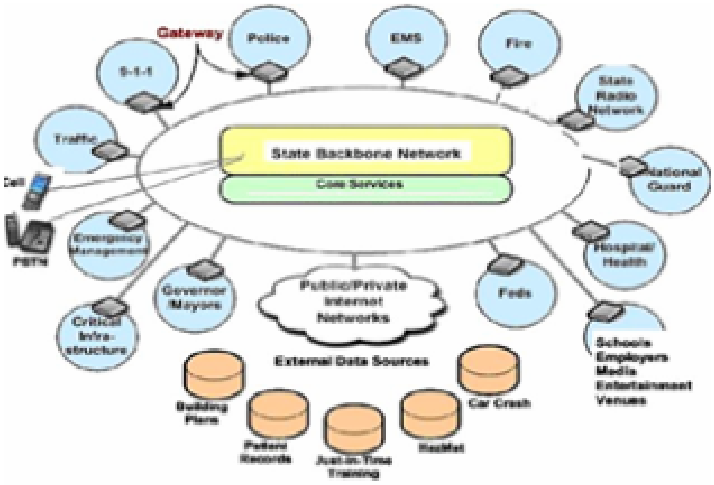


Рис. 1. Поле деятельности службы NG9-1-1 отдельного штата США [3].

Служба NG9-1-1 отдельного штата (в случае России – это, скажем, область) создается средствами Интернета. Следует ли нам идти по этому пути, т.е. переходить ли полностью на технологию пакетной коммутации? Это является важнейшим вопросом, который мы постараемся обсудить ниже.

C.Интернет Вещей

Кроме государственных проектов Системы 112 и комплекса «Безопасный город» в последнее время стал актуальным вопрос индустриального интернета или, другими словами, интернета вещей (Internet of Things, IoT) и межмашинного общения M2M.

11 Июля 2016 года на пленарном заседании

Международной промышленной выставки ИННОПРОМ Премьер-министр РФ Дмитрий Медведев предложил создать консорциум для развития в области индустриального интернета с привлечением разработчиков, потребителей и научного сообщества. По его словам, такой консорциум должен был бы "консолидировать всю отрасль и вырабатывать предложения по стандартизации и нормативному регулированию и продвигать эти технологии, привлекать финансовых партнеров, в том числе из числа институтов развития". Медведев заявил о необходимости понимания развития технологий на перспективу 10-20 лет и обратил внимание на развитие сферы "интернета вещей" (концепции соединения физических объектов компьютерной сетью).

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

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

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

D. Критическая инфраструктура

Наиболее важной среди новых областей телекоммуникаций является обеспечение безопасности критической инфраструктуры (Critical Infrastructure Protection, CIP), что представляет собой концепцию готовности противодействовать серьезным угрозам работы важных объектов инфраструктуры и объектов повышенной опасности в регионе или стране, особенно в условиях распространения информационных технологий и связанных с ними киберугроз.

Исторически, первым шагом в этом направлении было создание в 1996 году Комиссии по защите жизненно важной инфраструктуры при президенте США: была поставлена задача разработать всеобъемлющую национальную стратегию по защите инфраструктуры от физических и кибернетических угроз. Похожая же директива издана в Европейском Союзе в 2008 году. В России основные направления государственной политики по защите критически важных объектов инфраструктуры утверждены в 2012 г. [4]. В этом документе 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» [5].

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

E.О защите объектов критической инфраструктуры

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.

По данным МЧС Российской Федерации в 2010 г. на территории страны произошли 338 чрезвычайных ситуаций (ЧС) природного, техногенного и биолого-социального характера, а также 12 крупных террористических актов. Анализ общего количества ЧС природного, техногенного и биолого-социального характера показывает, что по количеству доминируют техногенные ЧС — 199. При этом наиболее проблемной отраслью является электроэнергетика. Так, количество аварий на объектах электроэнергетики за первые восемь месяцев 2010 года выросло, в среднем, на 20 % по сравнению с аналогичным периодом 2009 г. Аналогичная 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.

II О разработке Системы 112 и комплекса «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.

C. 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). В этом суть нашего упрека в адрес МЧС. Сошлемся на программный доклад заместителя начальника ФГБУ ВНИИ ГОЧС профессора С.А. Качанова [6]. Рис. 2А взят нами из этого доклада. По нашему мнению, телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы (рис. 2Б). 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 [7]. Все эти подсистемы должны быть охвачены единым системным проектом. Встает неприятный вопрос: почему МЧС как координатор соглашается на такое ущемление своих прав?

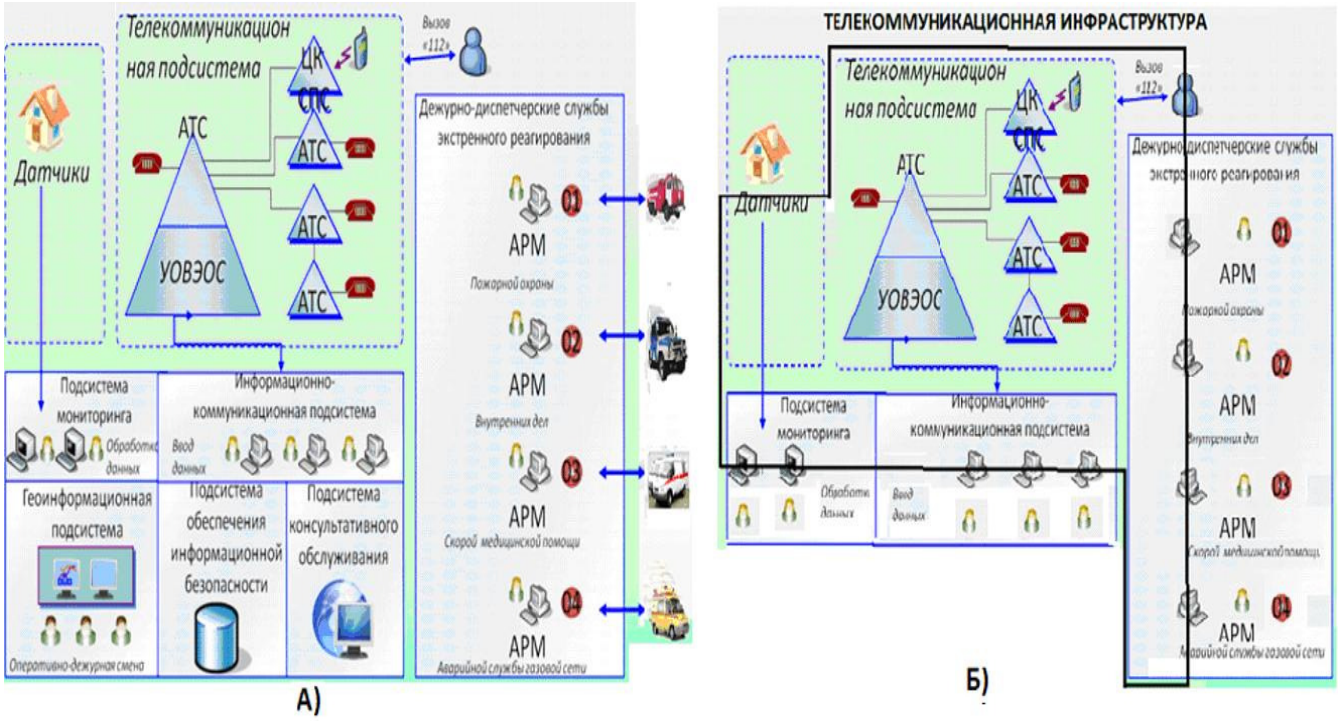


Рис. 2. А) Новейшее представление Системы-112 (по мнению МЧС): Минкомсвязь отвечает только за телекоммуникационную подсистему. Б)Телекоммуникационная инфраструктура выходит далеко за пределы телекоммуникационной подсистемы.

Ведомственная «борьба» за раздел сфер ответственности по Системе 112 длится годами. Только 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 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. Введение зон ответственности различных ведомств, по нашему мнению, только служит формальным прикрытием «безответственности».

С учетом новейших требований к Системе 112 (рис. 3), 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 (рис. 3 взят нами из вышеупомянутого доклада [6]) 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, представленной на рис. 3, на наш взгляд, мог бы служить 916-страничный документ с описанием требований к унифицированным свойствам сервисов военной связи США от 2013 года [8].

Рис. 3. Новые средства доступа к Системе 112 [8].

В.Минкомсвязь избегает ответственности

«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 их не удастся завершить.

Только в конце 2015 года 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» [7]. 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, которую полагалось завершить в 2017 г. И в «Методических рекомендациях» [7] дан перечень томов (всего их 19), которые должны быть в системном проекте по каждой области.

Заметим, что в ФЦП исходно были поставлены более сложные задачи:

- создать телекоммуникационную инфраструктуру Системы 112;
- создать информационно-техническую инфраструктуру Системы 112.

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

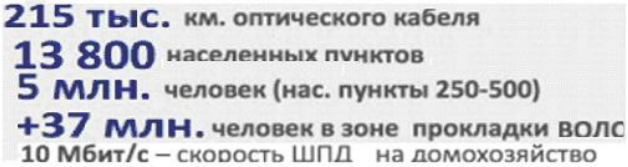
Другим важным вопросом является нумерация – как для обслуживающего персонала Системы 112, так и пользователей, особенно терминалов телематики (см. датчики на рис. 2), устройств интернета вещей. В этом направлении сделан только первый робкий шаг: 4 мая 2016 г. Минкомсвязь издала приказ о нумерации экстренных 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 [9]. 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».

И еще. Следует по-новому взглянуть на универсальную услугу. Доступ к Системе 112 должен быть немедленным для любого жителя страны (а не в часе ходьбы до таксофона для удаленного жителя на селе, как записано в действующем Законе о связи), а также для любого датчика охраняемого объекта. В погоне за расширением доступа к интернету, ущемляются права жителей мелких сел. 26 февраля 2015 г. Министр связи и массовых коммуникаций Николай Никифоров рассказал Правительству РФ об обеспечении доступности современными услугами связи [10]. Доклад начинается со слов об основной цели Минкомсвязи - увеличить широкополосную доступность (рис. 4А). К сожалению, уровни проникновения связи в городской и сельской местности пока еще сильно различаются.

А)



В)

Рис. 4. А) Цель Минкомсвязи – увеличить доступность ШПД. В) Инфраструктурная реформа универсальных услуг связи.

Как сказал министр, на рисунке 4В «вы видите основные параметры нашего амбициозного инфраструктурного проекта по строительству оптики. Не могу не отметить, что сегодня это действительно самый крупный в мире проект по строительству линий связи в малые населенные пункты — 215 тыс. км, 13,8 тыс. сел, около 5 млн. человек напрямую проживают в них. Но, еще раз подчеркну, это лишь села на 250–500 жителей. Очевидно, что кабель по пути к этим малым селам пройдет и через другие населенные пункты. Так вот по пути к ним мы планируем охватить связью населенные пункты с 37 млн. жителей».

Далее он добавил: «В нашей стране имеется 148 тыс. таксофонов, они установлены действительно практически в каждом селе и обеспечивают связь, в том числе в условиях чрезвычайных ситуаций. Это важнейшее инфраструктурное достижение, которое существует».

К сожалению, намеченные планы в какой-то мере увеличивают, а не уменьшают «цифровое неравенство», так как из общего числа 153000 населенных пунктов (по переписи 2010 г.): 36200 имеют число жителей 1 – 10, 32700 имеют число жителей 11 – 50, 13800 имеют число жителей 51 – 100, т.е. более 8 тысяч сел практически остаются вне охвата средствами связи.

Напрашивается замечание: доступ к интернету – несомненно, услуга привлекательная, но считаем, что доступ к службам «112» является более приоритетным – как в смысле социальной значимости, так и государственной важности. Поэтому в приоритетном порядке стоило бы снабдить жителей села радиосредствами, хотя бы текстовыми терминалами, чтобы не требовалось тратить час ходьбы до таксофона.

С. Ведущая роль «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 [11].

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, по крайней мере, привести архитектуру Систему 112 с указанием роли Ростелекома, в том числе платформы О7 и комплекса «О7. 112».

К этому проекту «О7.112» примыкает сервис «О7. Медицина» – как часть Системы 112. Цель его создания — автоматизация взаимодействия всех участников медицинского процесса: сотрудников лечебно-профилактических учреждений, пациентов, работников министерств и ведомств, отвечающих за здоровье граждан. Подключившись к сервису «О7.Медицина», любое лечебно-профилактическое учреждение получает доступ к системе электронной регистратуры, 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 «Методических рекомендациях» [7] 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.

III. Как развивались телекоммуникации

A. Достижения коммутации каналов

Bell Laboratories (сокращенно Bell Labs) – бывшая американская, потом франко-американская компания в составе Alcatel-Lucent (ее остатки ныне принадлежат Ericsson) – это был крупнейший исследовательский центр в области телекоммуникаций, электронных и компьютерных систем. За годы своей деятельности компания разработала множество революционных технологий, включая радиоастрономию, транзистор, лазер, кварцевые часы, теорию информации, операционную систему UNIX и языки программирования C, C++. Ученые Bell Labs были удостоены семи Нобелевских премий. От Bell Labs идут такие мировые достижения в области электронной коммутации, как сигнализация SS7 и интеллектуальные сети. Свою роль мирового центра науки Bell Labs утратили в 1984 году, когда был расформирован концерн Bell System.

Телефонная сигнализации SS7 (Signaling System №7) является, образно говоря, нервной системой сети связи. Сигнализация SS7 – это набор сигнальных телефонных протоколов, используемых для установления телефонных соединений по всему миру. Основная особенность SS7 состоит в том, что передача сообщений о требованиях по установлению телефонных соединений вынесена в отдельный сигнальный канал. Протоколы SS7 разрабатывались в Bell Labs, начиная с 1975 года и в 1981 году были определены как стандарты МСЭ.

Изначально сигнализация SS7 использовались не для установления соединений, а для доступа к базам данных, т.е. для построения интеллектуальных сетей. Интеллектуальная сеть IN – это сеть связи, позволяющая предоставлять дополнительные телекоммуникационные услуги, в том числе, управляемые абонентом. История внедрения дополнительных услуг в современном понимании IN началась с "Услуги 800". В 1967 г. компания Bell System, в то время практически монопольно владевшая рынком услуг связи США, ввела в план нумерации код доступа "800", по которому можно установить телефонное соединение с оплатой за счет вызываемого абонента. Это оказалось исключительно прибыльной услугой. (Заметим, что ныне международная сеть SS7 используется в мобильных сетях для другой крайне прибыльной услуги – передачи сообщений SMS.)

Путь к созданию IN 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). Заверяют, что в разработке 5ESS приняли участие 5000 сотрудников Bell Labs.

Простейшая схема сети SS7 и IN включает три узла сигнализации (рис. 5):

- 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.

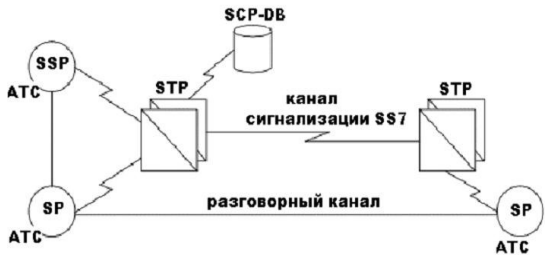


Рис. 5. Базовая архитектура сети SS7 и IN.

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 коммутации каналов TDM. Для общения с интернетом часто используют поток 128 кбит/с (объединяя два канала по 64 кбит/с).

Концепция ISDN возникла в Японии, в компании NTT. В 1984 в Японии построили первую сеть ISDN и подготовили международный стандарт, который МСЭ опубликовал в 1988 году.

B. О развитии российских сетей связи

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 (российский аналог SS7), которая является связующим звеном интеллектуальной сети (IN). Ныне много говорят о переносимости телефонного номера и обслуживании экстренных вызовов. Это всего лишь две услуги интеллектуальной сети. Но так как в России интеллектуальная сеть осталась недостроенной, то сейчас для внедрения этих двух услуг приходится городить специальные сети.

Разработка советской системы ОКС-7 началась в 1970х с созданием квазиэлектронных междугородных АТС. В квазиэлектронных АТС коммутация осуществляется герконами, а управление – электронное. В качестве прототипа для КЭАМТС «Кварц» использовалась станция 1ESS, разработанная в Bell Labs; первый экземпляр 1ESS был установлен в 1965 г. В разработке КЭАМТС «Кварц» принимали участие многие коллективы: ЦНИИС, Москва; Институт кибернетики АН Украины; завод Robotron, Дрезден, ГДР; ЛОНИИС, Ленинград; завод ВЭФ, Рига, Латвия. Оборудование КЭАМТС «Кварц» успешно производилось и эксплуатировалось до распада СССР.

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 с широкой кооперацией между странами-членами стран СЭВ. Координирующей организацией выступал НИИ ВЭФ (Рига). В качестве прототипа была выбрана телефонная станция System 12 компании IT&T. Следует признать, что выбор прототипа был неудачен, хотя, по замыслу, System 12 обладала многими положительными свойствами. Первая АТС System 12 была установлена в 1982 в Бельгии. Но полноценное серийное производство не удалось наладить, и в преддверии банкротства в 1986 компания IT&T продала всю разработку System 12 (включая заводы) французско-голландской компании Alcatel Alsthom, наследницей которой сегодня является Alcatel-Lucent. Проект ЕССКТ перестал существовать с распадом СССР и СЭВ.

Наиболее крупным достижением постсоветского периода является внедрение ОКС-7 в России. Обратимся к статье Н. С. Мардера и А. С. Аджемова от 1997 г. [12]: «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 [13]. На территории России тогда были размещены восемь УАК, имеющие важное стратегическое значение (рис. 6А). Заметим, что все они построены на базе цифровых АТС типа AXE шведской фирмы Ericsson. В настоящее время магистральная сеть России является более сложной.

На интеллектуальной сети России были установлены АТС разных производителей: 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 требование для отечественных производителей было чрезмерным, так как для этого пришлось бы переработать программное обеспечение множества станций. Тем самым, единая интеллектуальная сеть России осталась недостроенной, что и сказывается ныне, например, на построение Системы 112.

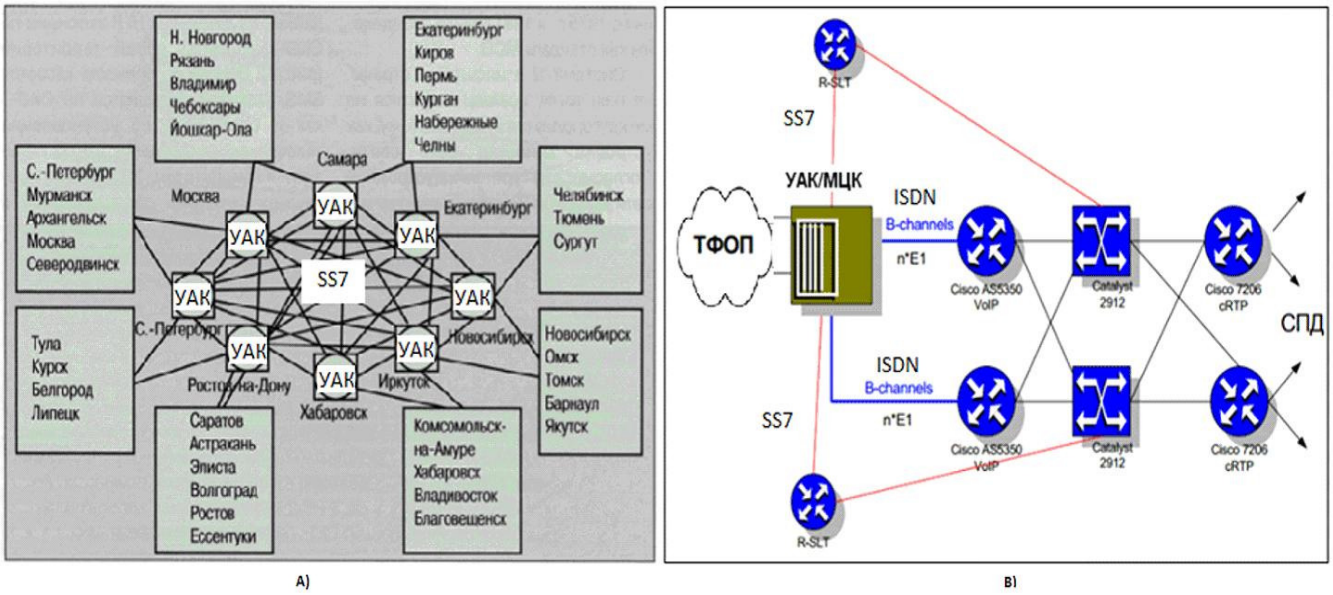


Рис. 6. A) Структура междугородной сети ОКС № 7 (1997). B) Проектируемый узел IP сети (на оборудовании CISCO).

В настоящее время «Ростелеком» взял курс на стратегию «All-over-IP», т.е. сеть перестраивается под IP протокол. На рис. 6B показан проект типового узла новой IP сети. Узел предполагается построить на оборудовании Cisco. Общение с узлом УАК/МЦК производится посредством системы SS7 и по B-каналам системы ISDN. Для общения с сетью SS7 указан узел SLT (Cisco Signaling Link Terminal). Подобная IP сеть строится вокруг каждого УАК/МЦК (узел автоматической коммутации/международный центр коммутации).

Вряд ли в условиях международных санкций подобные планы (на базе изделий Cisco или Juniper) удастся реализовать.

C.Состоится ли технология IMS

Сегодня актуальным стал вопрос: каким же будет сеть, построенная на основе протокола IP. Наиболее популярным претендентом на эту роль является технология IMS (IP Multimedia Subsystem), которая приходит на смену интеллектуальным сетям. История IMS началась в 2002 году, когда организация 3GPP, разрабатывающая стандарты мобильных сетей 3го поколения, предложила концепцию IMS. В качестве основного протокола сигнализации выбран протокол SIP. Ядро сети по технологии IMS основано на коммутации пакетов и обеспечивает транзит (обмен) трафика независимо от его происхождения (голос, данные, мультимедийные файлы, видео).

Базовыми элементами опорной сети архитектуры IMS являются два блока (рис. 7):

• CSCF (Call Session Control Function) – блок управления сеансами и маршрутизацией,

• HSS (Home Subscriber Server) – сервер домашних абонентов, является базой пользовательских данных и обеспечивает доступ к индивидуальным данным пользователя, связанными с услугами.

Для доступа к серверам приложений (SIP application server) предполагается использовать протокол INAP (на фиксированной интеллектуальной сети), CAMEL (на интеллектуальной сети для мобильных абонентов) и интерфейсы Parlay. Само же программирование предполагается вести в web-среде.

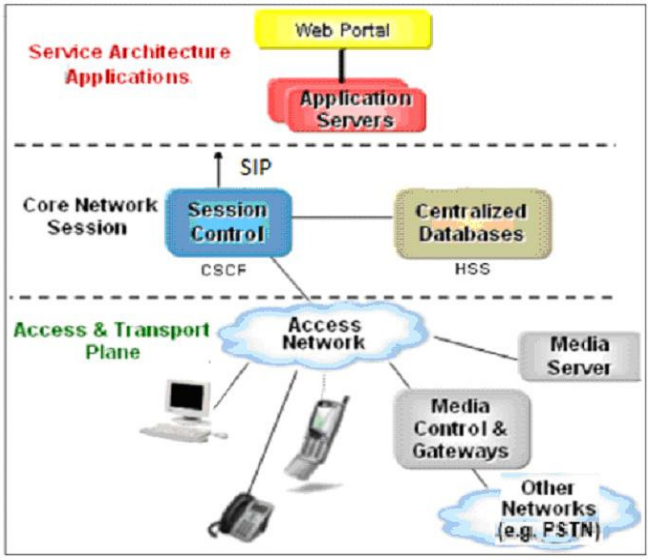


Рис. 7. Упрощенная архитектура IMS.

Будущее сетей IMS сегодня трудно предсказать. В условиях международных санкций закономерно возникает вопрос: не следует ли развивать отечественное производство, особенно для нужд Системы 112 и «Безопасного города», и сосредоточиться на коммутации каналов, достраивать интеллектуальную сеть.

IV.Сеть DISN как прототип Системы 112 и комплекса «Безопасный город»

Имеется аналогия между сетями связи DISN (Defense

Information System Network) оборонного ведомства США и экстренной службы нового поколения NG911 [14]. Считаем, что сеть DISN может служить прототипом Системы 112 и комплекса «Безопасный город», поэтому рассмотрим развитие сети DISN подробнее. Особенно поучительно разобраться в крупнейших просчетах в построении DISN.

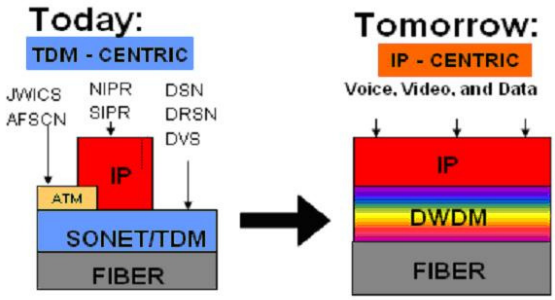


Рис. 8. Иллюстрация текущей проблемы DISN: как перейти от TDM-сети к IP-сети.

Основу DISN сегодня составляет коммутация каналов, точнее, стандарт SONET (в Европе – SDH), по которому работают оптические кабели, а информация кодируется согласно телефонному стандарту TDM (Time Division Multiplexing). По этой сети коммутации каналов сегодня работают основные военные сети связи Пентагона:

1) телефонная сеть DSN (Defense Switched Network),

2) закрытая коммутируемая сеть правительственной связи DRSN (Defense Red Switched Network),

3) сеть видеоконференцсвязи DVS (DISN VIDEO).

Кроме того, на рис. 8 указаны четыре закрытые сети JWICS, AFSCN, NIPRNet и SIPRNet, которые используют выделенные магистральные каналы:

• Объединённая глобальная сеть разведывательных коммуникаций (Joint Worldwide Intelligence Communications System, JWICS) – для передачи секретной информации по протоколам TCP/IP.

• Сеть управления спутниками AFSCN (Air Force Satellite Control Network),

• NIPRNet (Non-classified Internet Protocol Router Network) – сеть, используемая для обмена несекретной, но важной служебной информацией между «внутренними» пользователями,

• SIPRNet (Secret Internet Protocol Router Network) – система взаимосвязанных компьютерных сетей, используемых МО для передачи секретной информации по протоколам TCP/IP.

Первые две сети (JWICS и AFSCN) используют коммутаторы ATM (а не электронные АТС).

Переход к IP протоколу на сети DISN– мероприятие чрезвычайно сложное и дорогое. Кроме перехода от TDM кодирования на IP пакеты, предусмотрена и модернизация кабельной сети – от режима SONET/TDM к спектральному уплотнению каналов DWDM (dense wavelength-division multiplexing). Переход на IP протокол означает и смену системы сигнализации – переход от SS7 на SIP протокол.

A. Попытка внедрения технологии ATM

Обратимся к истории развития DISN. Оборонная информационная сеть DISN разрабатывается с начала 1990х. Это – глобальная сеть. Ее назначение – предоставлять услуги по передаче различных видов информации (речь, данные, видео, мультимедиа) для эффективного и защищенного управления войсками, связью, разведкой и РЭБ.

В середине 1990х вскрылось множество недостатков DISN. Прежде всего, это – низкий уровень интеграции многих сотен сетей, входящих в состав DISN, что существенно ограничивает взаимодействие в рамках единой сети и препятствует эффективному единому управлению всеми ее ресурсами. В частности, отмечались сложности взаимодействия между стационарной и полевой (мобильной) компонентами базовой сети из-за различия в используемых стандартах, типах каналов связи (аналоговых и цифровых), предоставляемых услугах, пропускной способности (у мобильной компоненты она значительно ниже, чем у стационарной).

Возник принципиальный вопрос: на базе какой технологии далее строить DISN. Основным претендентом считалась технология ATM (Asynchronous Transfer Mode). В 1990 г. в МСЭ был одобрен базовый набор рекомендаций технологии ATM. И в начале 1990х она стала наиболее популярной. Так, агентство DISA еще в 1993–1994 годах создало широкополосную сеть передачи информации на Гавайских островах. Эта сеть явилась прототипом второго этапа DISN и строилась по требованиям широкополосной сети B-ISDN (Broadband Integrated Services Digital Network) в сочетании с ATM и SONET/SDH технологиями.

Напомним, что ATM совмещает две технологии: КК и КП. Через коммутатор ATM передаются пакеты фиксированной длины в 53 байта (48 информационных и 5 байтов заголовка) – в режиме коммутации пакетов. Для исторической справки укажем, что основы технологии ATM были разработаны в 1970-х независимо во Франции и США: в исследовательской лаборатории France Telecom и в Bell Labs. К концу 1998 сеть DATMS (DISN ATM SERVICE) охватила 125 военных баз, в 1999 планировалось расширить сеть ATM до 200 объектов. Но предполагаемому расширению помешало решение агентства DISA о переходе на интеллектуальную сеть.

Немалую роль против продвижения коммутаторов ATM сыграл и интернет: изделия коммутации пакетов оказались более дешевыми. Ключевым моментом стало появление веб технологии, точнее, – в 1993 году появился веб браузер Mosaic и молниеносно стал захватывать рынок. Началась острая борьба между сторонниками «старой» технологии коммутации каналов и новой технологии коммутации пакетов. Началась борьба, которая продолжается по сей день.

B. Выбор архитектуры AIN

В условиях технологической неопределенности агентство DISA приняло принципиальное решение – строить военные сети связи США с использованием «открытой архитектуры» и программно-аппаратных средств коммерческого назначения (Commercial-Off-the-Shelf). В результате выбор пал на «старые» разработки Bell Labs, точнее, на протокол телефонной сигнализации SS7 и на интеллектуальную сеть (Advanced Intelligent Network, AIN). Заметим, что к тому времени институт Bell Labs давно был ликвидирован – 15 лет назад. За то разработки Bell Labs по сигнализации SS7 и интеллектуальной сети AIN к тому времени были всесторонне апробированы (и живут по сей день).

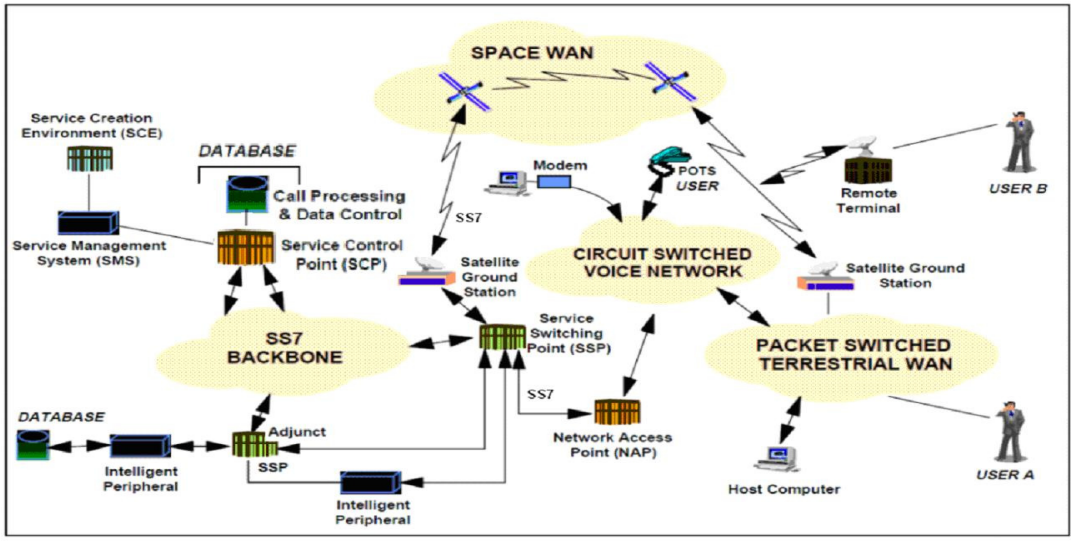


Рис. 9. Архитектура AIN применительно к оборонному ведомству.

В 1996 году утвердили «Joint Vision 2010» – план стратегического развития военных ведомств США на 15-летний период, который вошел в историю как план преобразования военного ведомства США в единую большую и эффективную военную силу, объединенную цифровыми средствами связи. Связующим звеном сети AIN служит система сигнализации SS7 (рис. 9). 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. Еще более существенным является наличие среды разработки сервисов SCE (Service Creation Environment), которая содержит стандартные подпрограммы SIB (Service Independent Block). По идее, эти интерфейсные средства позволяют привлекать сторонних программистов к разработке новых сервисов. На деле же средства оказались слишком сложными, так как программисту приходится знать детали телефонных сигнализаций.

C.О ведущей роли сигнализации SS7

Рис. 10 показывает схему тестирования оборудования AVAYA на сети DISN в недавнем прошлом – в 2012 г. [15]. Это оборудование может служить прототипом ЦОВ для Системы 112, поэтому остановимся на нем подробнее. Тестировалась PBX Avaya S8300D с набором шлюзов G450. Каждый шлюз G450 поддерживает средства доступа в любой комбинации: IP телефоны, аналоговые каналы (даже сигнализацию CAS), цифровые и ISDN каналы (BRI). Общая емкость шлюза G450: 8 медиа модули, до 450 IP линий, 192 аналоговые/цифровые линии, 128 BRI линий. Всего PBX Avaya S8300D может иметь до 50 шлюзов G450. Оборудование PBX Avaya включено в MFS (MultiFunctional Switch): в электронные АТС Nokia-Siemens EWSD и Alcatel-Lucent 5ESS сети DISN и в сеть общего пользования PSTN. Как показывает рис. 10, несмотря на призывы к переходу на IP технологию, основу сети DISN до сих пор составляет сигнализация SS7.

По нашему мнению, рис. 10 являет собой схему, которой не хватает в «Методических материалах" [11], схему, которая показывала бы включение средств Системы 112 в общую архитектуру сети связи России.

D.Переход на IP протокол

Прошло всего четыре года с появления плана «Joint Vision 2010», как лоббисты интернет-технологий убедили руководство Пентагона в обновлении программы вооружений, и в 2000 году появился документ «Joint Vision 2020». В нем провозглашалось достижение информационного превосходства военных сил США во всем мире. Детали плана затем разрабатывались долгие семь лет: в 2007 году издали фундаментальную программу „Global Information Grid. Architectural Vision” [16], в которой находим три основных положения:

• во-первых, следует строить единую оборонною информационную сеть GIG (Global Information Grid),

• во-вторых, сеть должна быть ориентирована на ведение сете-центрической войны,

• в-третьих, и это главное, сеть GIG должна быть построена на базе IP протокола. Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями.

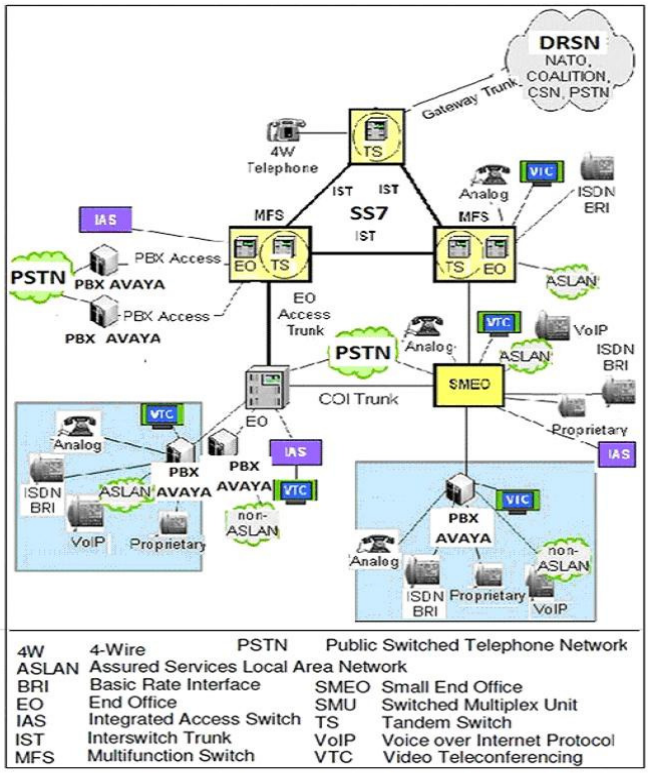


Рис. 10. Как сочетается «новая» PBX AVAYA со «старой» сетью DISN.

Переход от сети коммутации каналов, где ныне господствует протокол SS7, к коммутации пакетов и протоколу SIP (или к его защищенной версии AS-SIP, Assured Service – Session Initiation Protocol) требует установки шлюзов – программных коммутаторов MFSS (MultiFunctional SoftSwitch).

Эту работу взяла на себя компания CISCO. По планам CISCO установили 22 крупных MFSS на военных базах НАТО по всему миру. Напомним, что SoftSwitch обеспечивает переход от сети коммутации каналов к сети коммутации пакетов, но не заменяет саму сеть коммутации каналов. Он управляет только согласованием протоколов сигнализации SIP и SS7 (посредством шлюза SGW) и преобразованием IP пакетов в TDM посылки (посредством шлюза MGW).

Объясним, как многофункциональный софтсвич MFSS будет управлять вызовами (рис. 11):

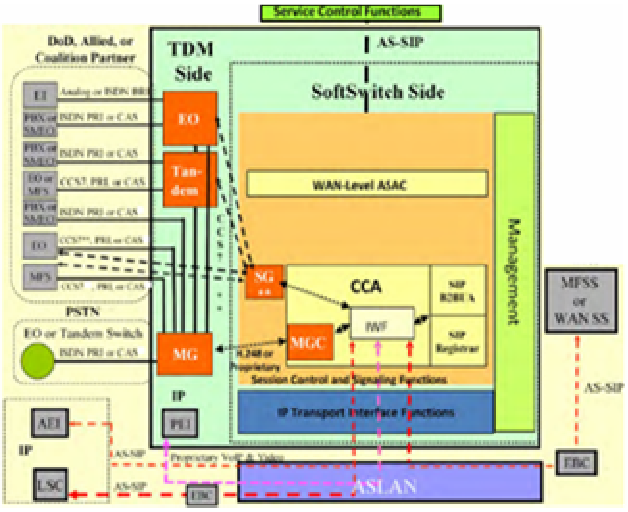


Рис. 11. Многофункциональный программный коммутатор (софтсвич) MFSS.

• В сторону внешней публичной сети PSTN или сети ISDN используется функция IWF (ISUP-SIP interworking function).

• Контроллер MFSS обеспечивает «старые» сигнализации PSTN/ISDN, включая ISUP, CCS7/SS7 и CAS (Channel Associated Signaling).

• MFSS действует как медиашлюз (MG) между TDM каналами и IP каналами. Контроллер MGC управляет медиашлюзом – посредством протокола H.248.

• Шлюз сигнализации SG (Signaling Gateway) обеспечивает взаимодействие между SS7 и SIP.

В окружении MFSS имеются еще оконечные устройства EI (End Instrument): AEI (Assured Services End Instrument), работающие по протоколу AS-SIP и нестандартные устройства PIE (Proprietary Internet Protocol Voice End Instrument).

E.Архитектура новейшей сети DISN

Воспользуемся новейшими методическими материалами по GIG (от 2013 г.), которые относятся к базовой архитектуре унифицированных сервисов (Unified Capabilities Reference Architecture) [8]. Эта новая архитектура унифицированных сервисов UC 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 (Session Control) происходит по единому протоколу AS-SIP.

Сетевая архитектура унифицированных сервисов базируется 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.

Целевая архитектура сети DISN содержит два уровня: Tier 0 и Tier 1 (рис. 12). Кластеры уровня Tier 0 отвечает за неуязвимость всей сети DISN. Каждый кластер содержит по три софтсвича, соединенных протоколом

ICCS (Intra-Cluster Communication Signaling), по которому автоматически обновляются их базы данных. Кластер, по существу, представляет обин распределенный софтсвич. Требуется, чтобы задержка в обмене содержимом баз данных не превышала 40 мс. Так как передача сигнала занимает 6 микросекунд на 1 км, то расстояние между софтсвичами не может превышать 6600 км. На нижнем, втором уровне DISN сети Tier 1, находятся два типа локальных сетей: защищенная локальная сеть ASLAN по протоколу AS-SIP и традиционная LAN по протоколу H.323 (который является аналогом ISDN в IP сети).

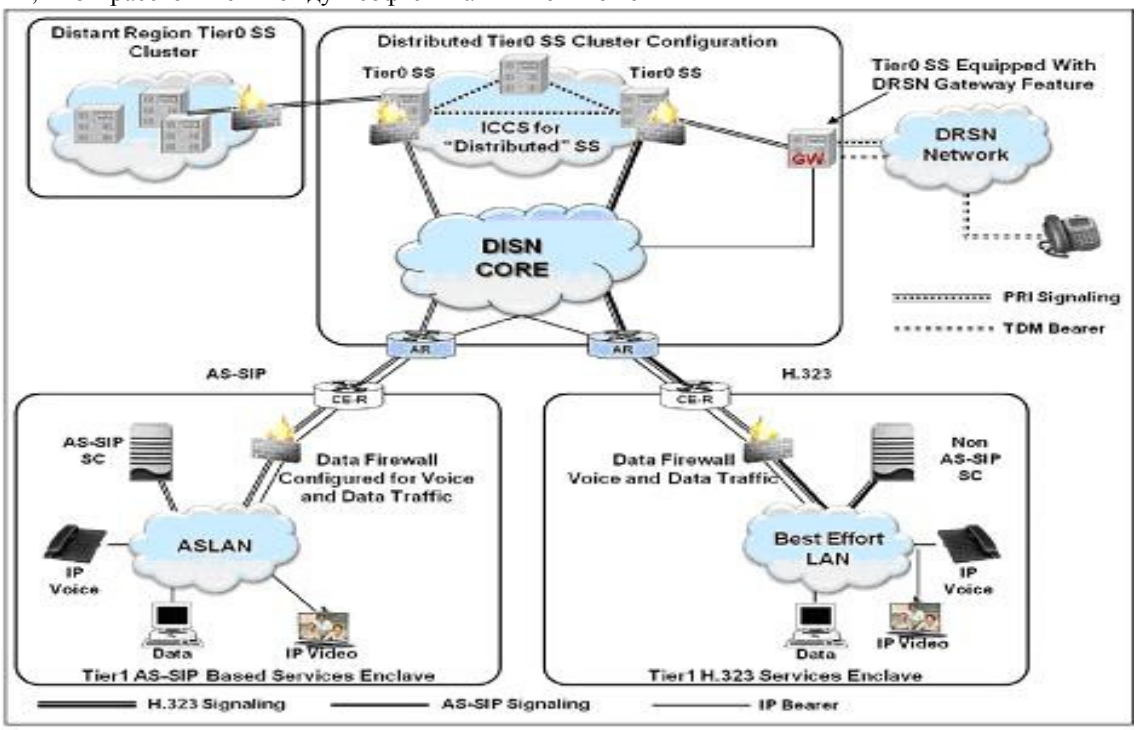


Рис. 12. Двухуровневая защищенная гибридная сеть DISN для передачи голоса, данных и видео.

Создается среда AS-SIP, но переход от SIP к протоколу AS-SIP оказался весьма дорогостоящим мероприятием. Главными недостатками протокола SIP являются трудности с обеспечением секретности (особенно в условиях кибервойны) и обслуживанием приоритетных вызовов, что важно для военных применений, для экстренной службы. Поэтому по заказу МО США разработали защищенный протокол AS-SIP [17]. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC. К тому же сам протокол AS-SIP еще далек от совершенства: в версии протокола AS-SIP, обнародованной в июле 2013 г., внесено более 50 исправлений по сравнению с исходной версией, обнародованной полугодом ранее. Но, тем не менее, протокол AS-SIP, по всей вероятности, в будущем вытеснит применяемый сегодня протокол SIP, и тогда многие сети придется перестраивать.

F.Правительственная связь DRSN

Опыт построения сети DISN – крупнейшей и богатейшей в мире ведомственной сети связи – преподносит всем нам поучительные «уроки» по смене парадигмы телекоммуникаций, по переходу от режима КК к КП, но одновременно ставит под сомнение саму возможность полного перехода на коммутацию пакетов.

Сеть DRSN (Defense Red Switch Network) — это выделенная сверхсекретная телефонная сеть, которая обеспечивает управление вооруженными силами США (рис. 13). Вопреки требованиям агентства DISA на ней сохраняется технология коммутацию каналов, точнее, ISDN каналы и протоколы сигнализации ISDN PRI и CAS (Channel Associated Signaling). Эта сеть приобрела особую значимость после событий 11 сентября 2001 г. и создания Министерства внутренней безопасности (U.S. Department of Homeland Security, DHS). По новым требованиям киберзащиты сети связи приходится перестраивать.

Сеть DRSN стала своего рода «родимым пятном» на сети DISN, строящейся по единому протоколу AS-SIP. В методических материалах по DISN пока даже не предусмотрен перевод сети DRSN на коммутацию пакетов.

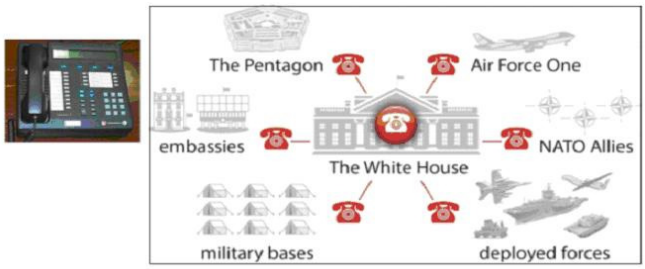


Рис. 13. Телефон правительственной связи и схема сети DRSN.

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

V. Разработка программного обеспечения – камень преткновения

A. *Как состыковать AIN и IP сети*

Наиболее сложной частью существующей сети DISN является интеллектуальная сеть AIN. Эту сеть стали строить после 1996 г. – согласно требованиям Программы развития вооружений МО США «Joint Vision 2010». С самого начала принятия программы «Joint Vision 2010» за интеллектуальную сеть AIN в составе сети DISN отвечает компания Lockheed Martin. Появление все новых боевых средств и новых сервисов требует непрерывного совершенствования средств AIN. Об этом свидетельствуют приглашения на работу в Lockheed Martin.

Длинный список вакансий на сайте компании Lockheed Martin свидетельствует о трудностях в подборе специалистов. На первом месте в списке вакансий значится поиск аналитиков мультифункциональных информационных систем для DISA. Требуются умения разработки новых сервисов для AIN и опыт работы с оборудованием CISCO, Juniper, Promina, Safenet, Ciena, Sycamore, Ericsson. Уровень секретности работы – высший.

Подтверждением нехватки персонала служит сайт для ветеранов: lockheedmartin-veterans.jobs. И самое важное – приглашаются на работу ветераны с 28-летним работы, т.е. имеющие опыт работы с сетями коммутации каналов. Молодые специалисты, выросшие в среде веб-программирования, по-видимому, не в силах поддержать и развивать существующие сети AIN, построенные на технике коммутации каналов. То есть, нужны специалисты по усовершенствованию «старого» секретного ядра сети AIN (которому насчитывается уже лет 30) и его взаимодействию с новым разнородным оборудованием множества поставщиков.

B. *Трудности с модернизацией управления сетью DISN*

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

Суть контракта GSM-O состоит в модернизации системы управления сетью GIG по требованиям киберзащиты. Стоимость работ составляет громадную сумму – 4.6 млрд. долл. в течение 7 лет. Соисполнителями контракта GSM-O являются компании AT&T, ACS, Serco, BAE Systems, Mantech и ряд других специализированных и малых предприятий. Это является крупнейшим в истории телекоммуникаций проектом модернизации.

В 2013 году команда GSM-O приступила к изучению состояния четырех центров управления сетью GIG, которые несут ответственность за техническое обслуживание и бесперебойную работу всех компьютерных сетей Пентагона – 8100 компьютерных систем в более чем 460 местах в мире, которые, в свою очередь, соединены 46000 кабелями. Первое дело по контракту состояло в модернизации системы управления, было принято решение о консолидации операционных центров – с четырех до двух. Расширяются центры на военно-воздушных базах Scott (штат Иллинойс) и Hickam на Гавайях, а центры в Бахрейне и Германии закрываются (рис. 14). Другими словами, управление оборонной сетью NATO переводится на территорию США. Но это требует небывалого ранее преобразования сети связи, охватывающей весь мир.

Рис. 14. Проект модернизации управления сетью DISN.

Для обеспечения кибербезопасности услуг UC агентством DISA создана новая организация – Исследовательский центр кибербезопасности. Основная задача нового центра состоит в обеспечении кибербезопасности Единой информационной среды Пентагона (Joint Information Environment, JIE) и в соответствии с правилами единой архитектуры безопасности (single security architecture, SSA). В архитектуре SSA ключевую роль играют региональные стеки безопасности (Joint Regional Security Stacks, JRSS). Стеки безопасности JRSS, по сути, представляют собой IP маршрутизаторы со сложным комплексом программ киберзащиты.

Первый стек JRSS был установлен и успешно эксплуатируется на военной базе Сан-Антонио, штат Техас. В 2014 году велась работу по установке 11 стеков

JRSS на территории США, 3 стеков на Ближнем Востоке и одного – в Германии. Общий объем работ включает установку 24 стеков JRSS на служебной сети NIPRNet и 25 стеков JRSS на секретной сети SIPRNet. К 2019 году планируется на эти стеки перенести программы кибербезопасности, которые сейчас размещены в более чем 400 местах.

На очереди стоят работы по соданию общих дата-центров (DISA Core Data Centers, CDCs) с перемещением туда задач, выполняемых существующими дата-центрами армии и ВВС. Пока отстают работы по внедрению унифицированных сервисов (Unified Capabilities), что предполагает переход на IP коммуникации для передачи голоса, телеконференций и видео.

Но уже через два года после начала работ – в 2015 году мир телекоммуникаций потрясла новость: Lockheed Martin не справляется с модернизацией сети DISN, т.е. с выполнением многомиллиардного контракта GSM-O, и свое подразделение LM Information and Global Solutions продает конкурирующей фирме Leidos. Провалом работ, скорее всего, послужила неспособность набрать разработчиков, способных сочетать «старое» оборудование коммутации каналов с новейшими системами пакетной коммутации.

Отметим, что проект GSM-O представляет всего лишь одним из крупнейших проектов Министерства обороны США, которые обусловлены стремлением к доминированию во всем мире, и сроки его выполнения оказались сорванными. Не ожидает ли подобная судьба и другие проекты, о чем речь пойдет ниже. Все они требуют наличия многих тысяч программистов, имеющих не только навыки работы с новейшими системами программирования, но и способные входить в детали систем связи нескольких поколений, да еще в условиях работы «совершенно секретно».

C. Единое информационное пространство Министерства обороны США

Успех военных операций зависит от способности командования действовать оперативно и на базе наиболее точных и своевременных данных о противнике и собственных силах. С целью обеспечения условий для будущих войн Министерство обороны США приняла амбициозный многолетний план IT модернизации и создания Единой информационной среды JIE [18]. Этот план предполагает кардинальную перестройку существующих IT сетей и систем оборонного ведомства.

Основу JIE составляет DODAF (Department of Defense Architecture Framework) – информационная архитектура военного ведомства. Ее новейшая редакция создавалась уже в условиях развертывания кибервойны. Поэтому на первом месте стоит создание единой архитектуры безопасности (Single Security Architecture, SSA), которая должна обеспечить внутреннюю безопасность сети и предотвращать внешние киберугрозы.

На втором месте – создание единой, защищенной информационной среды для безопасного, надежного взаимодействия на поле боя.

На третьем – управление идентификацией и доступом, как между участниками боя, так и между организациями.

На четвертом – унифицированный набор сервисов (Unified Capabilities, UC).

На пятом – облачные вычисления (Cloud Computing), что будет управлять тысячами компьютеров, обеспечит киберсекретность, миграцию приложений в облаке.

На шестом – консолидация дата-центров. В 2014 г. имеется 2000 дата-центров, а в 2017 г. их число сократится до 500 (на четырех уровнях иерархии).

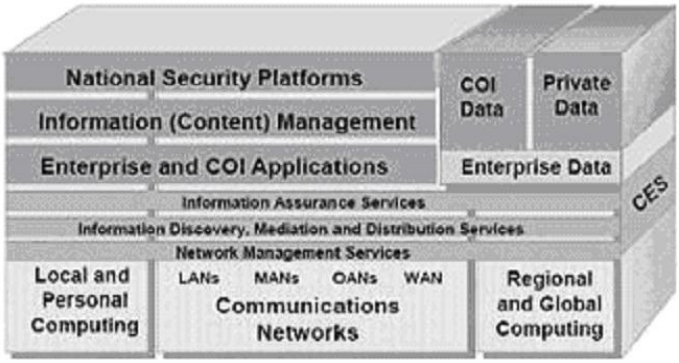


Рис. 15. Целевая архитектура единой информационной среды DoD.

На рис. 15 представлена семиуровневая модель Единой информационной среды DoD. К данному моменту она стандартизована только частично. Принято решение в части единых коммуникационных сетей (нижний уровень): это – широкополосная IP сеть (wide area IP backbone network) и протокол MPLS (multiprotocol label switching protocol). Выбрана базовая архитектура унифицированных сервисов (Unified Capabilities Reference Architecture), что относится к уровню Distribution Services. Наиболее важной и трудоемкой работой при создании единой информационной среды является стандартизация уровня приложений (Enterprise and Community-of-Interest Applications).

D. Мета–модель DoDAF

При описании уровня приложений прежде всего следует говорить о мета–модели DoDAF. Единая мета–модель DoDAF разрабатывается с 1990 г. Мы рассмотрим текущую версию 2.0 (с 2009 г.). Рис. 16 иллюстрирует взаимосвязи между основными понятиями мета–модели DoDAF. Модель содержит шесть описаний, которые объединены ключевым понятием Activity:

• Описание данных (Data Description) — отвечает на вопрос What (что включает и описание Resources, кроме самих Data)

• Описание функции (Function Description) — отвечает на вопрос How (содержит также описание исполнителя (Performer), который выполняет Function и

учитывает связанные с ней Measures, Rules и Conditions)

- Описание сети (Network Description) — Where
- Описание участников (People Description) — Who
- (что включает Organizations)
- Описание времени (Time Description) — When
- Описание мотивации (Motivation Description) — Why (с расширением, что включает описание Capability requirements)

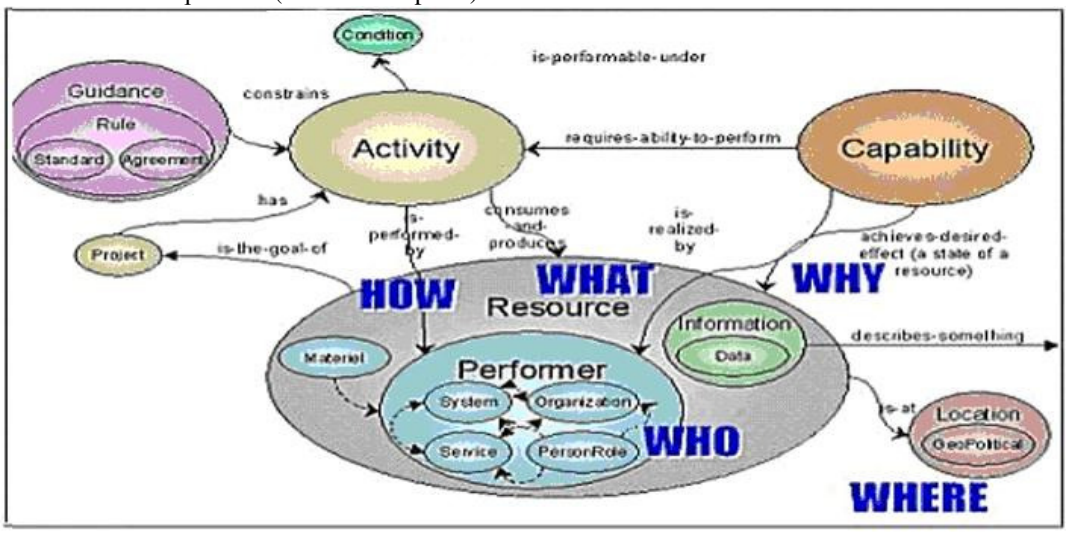


Рис. 16. Иллюстрация мета-модели DoDAF.

Описание Единой информационной среды JIE получилось чрезвычайно сложным. Рис. 17 дает представление о документации JIE. Она представлена с восьми точек зрения (Viewpoint), что изложено в 52 томах:

- Общее описание (All Viewpoint) – 2 тома,
- Описание сервисных компонентов (Capability Viewpoint) – 7 томов,
- Описание данных и информации (Data and Information Viewpoint) – 3,
- Описание операций (Operational Viewpoint) – 9,
- Описание проекта (Project Viewpoint) – 3,
- Описание сервисов (Services Viewpoint) – 13,
- Описание системы (System Viewpoint) – 13,
- Описание стандартов (Standard Viewpoint) – 2.

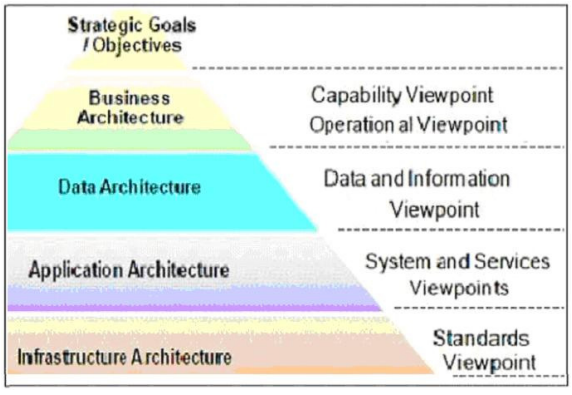


Рис. 17. Описание Единой информационной среды GIG содержит 52 тома.

E.Язык моделирования

Для упрощения работы с документацией JIE требуются графические средства. За прошедшие годы были апробированы различные средства. В итоге выбран графический язык SysML (Systems Modeling Language). Напомним его предысторию. Язык UML давно уже стал стандартом общения между участниками разработки программного обеспечения крупных проектов. Его богатые выразительные средства и широкий спектр поддерживающих продуктов способствовали тому, что UML начал проникать в другие области деятельности, связанные с моделированием бизнес-процессов. В итоге появился язык SysML — клон UML, позволяющий проектировать программно-аппаратные комплексы. Средств языка UML оказалось недостаточно для моделирования аппаратуры. Понадобилось добавить ряд новых графических элементов и диаграмм, которые позволяют описывать нюансы каждого элемента модели и взаимосвязи между элементами, а также строго задавать границы модели. С другой стороны, в UML имеется некоторая избыточность, поэтому не все его элементы вошли в новый клон. Изменения были специфицированы в виде профиля UML 2.0 и названы новым именем — SysML (System Modeling Language). В спецификацию этого языка вошли новые диаграммы: требований, внешних и внутренних блоков, времени, параметрическая.

В 2012 г. агентство DISA опубликовало руководящий документ GCMP 2012 [19]. Это уже третья версия требований по методологии построения GIG. Первая версия появилась в марте 2006 г. и, в соответствии с «Joint Vision 2020», была ориентирована на переход к IP протоколу: объявлялся переход на IP протокол в приложениях, сервисах и ставилась цель следовать концепции сете-центрической войны. Новая архитектура базируется на модель облачных вычислений, и этим отличается от прежних моделей, которые были сете-центрическими. К сожалению, в документе [19] ничего не сказано о судьбе прежних архитектурных решений: о сигнализации SS7, сети AIN и протоколе IP. Но в процессе программирования потребуются знания

различного оборудования этих решений, что, на наш взгляд, является крупнейшим препятствием.

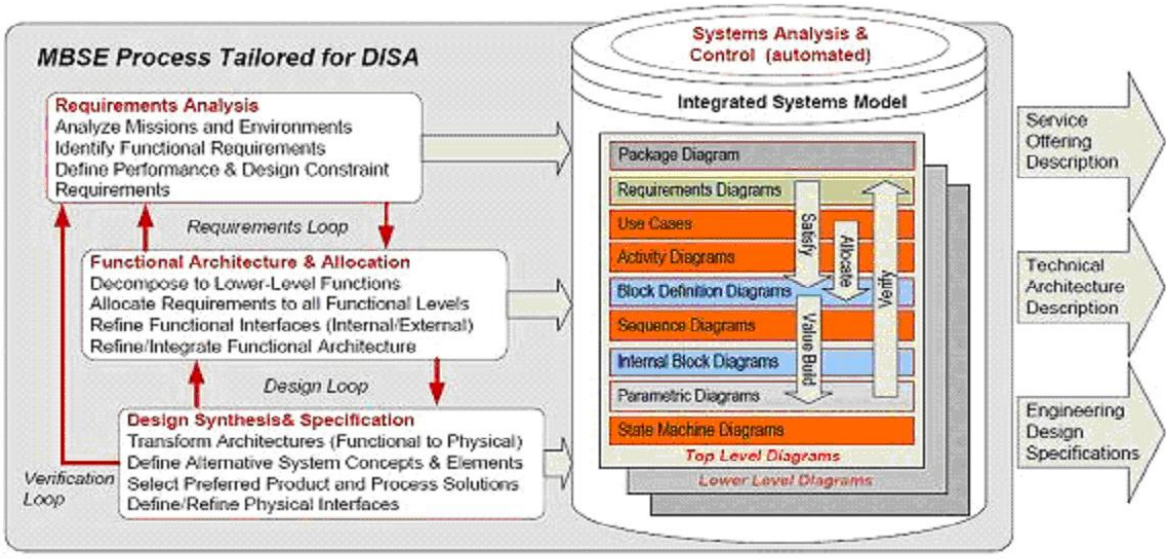


Рис. 18. Модель MBSE сети DISN.

Общие требования DISA к разработке концепции JIE иллюстрирует рис. 18. В основе концепции лежит модель MBSE (Model based Systems Engineering) и язык SysML (Systems Modeling Language). Сама модель MBSE представляет собой коллекцию диаграмм на языке SysML. Результатом разработки являются три типа документов:

- Описание сервисов (Service Offering Description),
- Описание архитектуры (Technical Architecture Description),
- Технические спецификации разработки (Engineering Design Specification).

Как заверяют разработчики Единой информационной среды [20], по документации MBSE можно не только моделировать систему и изучать ее производительность, но даже генерировать исполнимый код.

F. Задачи обеспечения кибербезопасности сети DISN

Новая инициатива кибервойны потребовала кардинальной перестройки GIG. В октябре 2010 года была создано киберкомандование USCYBERCOM. К 2016 году Cybercom планирует иметь 6000 высоко-квалифицированных сотрудников, образующих 133 команды, способные выполнять следующие три основные миссии:

1) национальные киберсилы, способные охранять критическую инфраструктуру и ключевые ресурсы страны,
2) боевые киберсилы, обеспечивающие киберзащитой боевых командиров по всему миру,
3) силы киберзащиты, охраняющие информационные сети Министерства обороны США.

Итак, Военное ведомство США ставит перед собой исключительно амбициозные цели:

1) по всей сети GIG перейти от телефонного стандарта TDM к интернет-протоколам, в том числе уйти от телефонной сигнализации SS7, которая является «нервной системой» сети, соединяющей всех пользователей с «мозгом» сети – интеллектуальной сетью AIN и перестроить сеть по правилам интернета;

2) 40 различных систем связи в сети GIG перепрограммировать по единым правилам модели MBSE;

3) перепрограммировать сеть с учетом требований кибервойны.

Программа развития GIG также чрезвычайно амбициозна. Что касается работ по программированию, то ключевым является человеческий ресурс. Найдутся ли многие тысячи программистов, способные такую работу выполнить и следовать при этом жестким правилам MBSE? Кто возьмется за такую работу? Тем самым ставится под сомнение само создание Единой информационной среды Министерства обороны США на базе информационной архитектуры DoDAF и мета–модели DoDAF.

Ситуацию осложняют требования обеспечения кибербезопасности (рис. 19). Задачи кибербезопасности являются высшим приоритетом Пентагона, но отсутствие необходимых стандартов тормозит выполнение всей программы GSM-O, прежде всего, тормозит создание общих дата-центров CDC и внедрение унифицированных сервисов (Unified Capabilities). Остаются также нерешенными задачи использования облаков военного ведомства и перенос какой-то части приложений на коммерческие облака. Решение задач обеспечения кибербезопасности кардинально меняют все планы построения сети DISN. Иллюстрацией тому может служить наличие множества новых связей на сети DISN (рис. 19), которые следует установить по требованиям киберкомандования

USCYBERCOM.

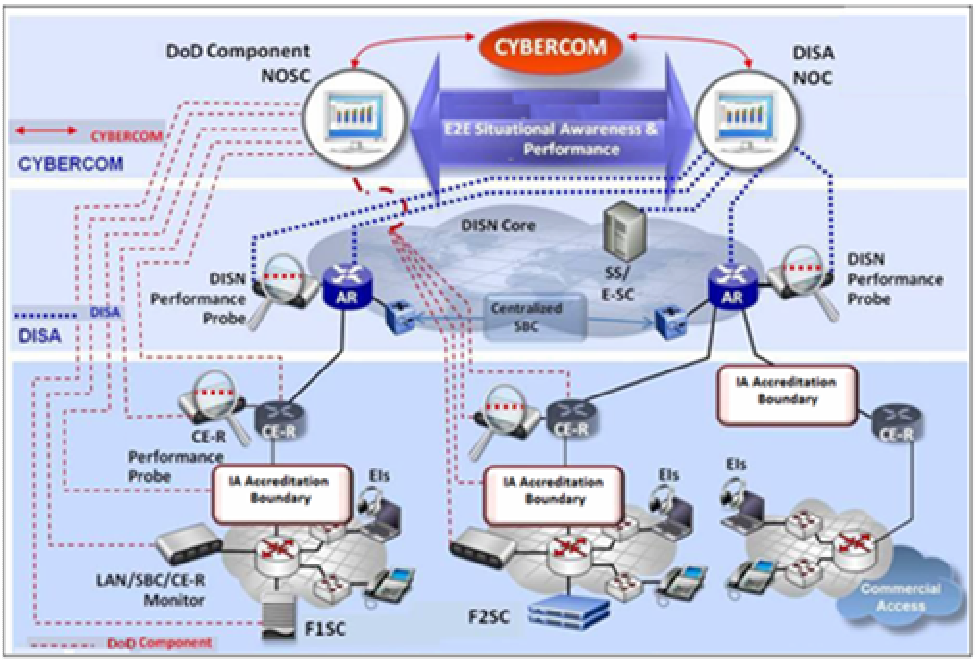


Рис. 19. Общий вид обеспечения безопасности услуг UC [19].

Киберкомандование USCYBERCOM получает информацию о ситуационной безопасности от двух центров:

(1) Центр безопасности министерства обороны (DoD Component Network Operations and Security Center, NOSC) и (2) Центр управления сетью агенства DISA (DISA Network Operation Center, NOC).

Агентство DISA и другие компоненты DoD несут ответственность за сквозное предоставление услуг UC, включая качество обслуживания, обнаружение ошибок, настройку, администрирование, производительность и безопасность, и все это должно проходить по новым требованиям киберзащиты, что существенно тормозит планы модернизации DISN.

Резюме. Сама концепция Единой информационной среды JIE является чрезвычайно сложной, а требования кибербезопасности, как показывает рис. 19, ее еще больше усложняет. Суть концепции JIE состоит в создании общей инфраструктуры вооруженных сил, обеспечения корпоративных услуг и единой архитектуры безопасности, а стеки JRSS являются основными компонентами среды JIE, которые обеспечивают единый подход к структуре кибербезопасности и защиту компьютеров и сетей во всех военных организациях.

VI. Текущие задачи российских связистов

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

• Первоочередной задачей является разработка единых системных проектов Системы 112 и комплекса «Безопасный город» для всей страны (прежде всего, Технических требований на информационную инфраструктуру), что предполагает объединения усилий МЧС и Минкомсвязь, а также Ростелекома.

• Выполнение этой задачи предполагает усиление ведущей роли МЧС, а также возрождения ведущих институтов Минкомсвязи, в частности института ЦНИИС, который ослаблен взятым ранее курсом на приватизацию.

• Курс на импортозамещение полагает использование российского аппаратного и программного обеспечения, изначально разрабатываемого под российские стандарты безопасности, что, в свою очередь, предполагает усиление Минэкономразвития и Минкомсвязи с восстановлением, в определенном смысле, функций бывшего МПСС.

• Если взять курс на импортозамещение, т.е. на развитие сетей связи собственными силами, то, на наш взгляд, следует вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их дальше. Такой точкой отсчета условно можно назвать систему ОКС-7 и интеллектуальные сети. Учитывая отставание от передового мирового уровня, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника, стоит оценить перспективы коммутации каналов, где не требуются столь высокое быстродействие.

• Для создания Системы 112 и АПК «Безопасный город» необходимо организовать подготовку специалистов, способных: разрабатывать нормативные документы по сетям связи с коммутацией каналов и с пакетной коммутацией и разрабатывать аппаратные и программные средства новых сетей связи.

• Особо отметим важность индустрии программирования услуг. Это относится к весьма болезненному для связистов вопросу об открытых интерфейсах программирования (Open API). Если будет отрыто доступен набор API, то многие сторонние программисты включатся в разработку Системы 112 и комплекса «Безопасный город».

• И в первую очередь – следует разработать нормативные документы (стандарты) по новым гибридным сетям коммутации каналов и пакетов, учитывая также новейшие требования индустриального интернета (интернета вещей и межмашинного общения), что представляет собой исключительно трудоемкую задачу, учитывая увлеченность иностранной техникой связи в постсоветский период.

Отметим особо, что перечисленные здесь проблемы и задачи также актуальны и для стран Евразийского экономического союза и, следовательно, вполне могут быть предметом интереса **Евразийской экономической комиссии.**

Более подробно отдельные материалы статьи опубликованы в [22-26].

Библиография

[1] Соколов Н.А. Системные аспекты построения и развития сетей электросвязи специального назначения //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 9. – С. 4-8.

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

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

[4] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, 3 февраля 2012 г. http://www.scrf.gov.ru/documents/6/113.html

[5] МЕТОДИЧЕСКОЕ ПОСОБИЕ по разработке организационных документов по созданию и развитию аппаратно-программного комплекса «Безопасный город» Москва – 2016 http://www.mchs.gov.ru/upload/site1/document_file/E4Na2VRWjW.pdf

[6] 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

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

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

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

[10] Обеспечение доступности современными услугами связи// http://government.ru/gov/persons/192/

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

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

[13] Основные положения системы сигнализации ОКС № 7 для сети связи Российской Федерации http://www.gosthelp.ru/text/PolozhenieOsnovnyepolozhe2.html/ Retrieved: Oct, 2014.

[14] M. Schmitt Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE

[15] О кибербезопасности критической инфраструктуры государства//International Conference on Technologies for Homeland Security. May 2008.

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

[17] Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Department of Defense. Version 1.0 June 2007.

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

[19] The Department of Defense. Strategy for Implementing the Joint Information Environment. September18, 2013.

[20] DISA. Global Information Grid (GIG) Convergence Master Plan (GCMP), Vol. 1, 02 August 2012.

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

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

[23] 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.

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

[25] 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. 2016.-Т.4.- №6 С.17-31.

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

On system design for System-112 and the "Safe City" system

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

Abstract— **This paper discusses the key new challenges faced by the communications industry: import substitution, development of System-112, the "Safe City" system, the Internet of Things and protection of a critical infrastructure. We specify the tasks of the departments of EMERCOM and the Ministry of Communications, as well as RosTelecom company. This article analyzes the development of the communication industry: the introduction of intelligent networks, SS7 signaling, and IMS system. DISN network is considered as a prototype of the System-112 and the "Safe city" system. Also, we discuss the problems of software development, which complicates the implementation of projects of modernization of the network DISN. In conclusion, this paper lists the priorities of the Russian communications industry.**

Keywords— **telecom, Safe City, SS-7, cyber defense, cyber security.**