Телекоммуникации для экстренных и военных нужд: параллели

Шнепс-Шнеппе М.А.

***Аннотация*—Сегодня идеалом единого мира телекоммуникаций и компьютеров выступает IP протокол. В настоящее время в Соединенных Штатах на базе IP протокола строятся две мощнейшие сети: GIG (Global Information Grid) – глобальная информационная сеть оборонного ведомства и NG9-1-1 – единая сеть нового поколения для обслуживания экстренных вызовов к любым общественным службам, в том числе – как от людей, так и от оберегаемого имущества. Подобные же задачи решаются и в России, только более робко: строительство единой экстренной службы 112 и переход на цифровую технику в вооруженных силах. В статье сравниваются две стратегии развития сетей связи в России. Первая стратегия – продолжение строительства сетей связи средствами иностранных производителей. Суть же второй стратегии заключается в выборе курса на замещение импорта, т.е. на развитие сетей связи собственными силами.**

***Ключевые слова*— SS7; интеллектуальная сеть; IP протокол; глобальная сеть GIG; NG9-1-1.**

I. Введение

Сегодня идеалом единого мира телекоммуникаций и компьютеров выступает IP протокол. Но суждено ли ему действительно стать единым стандартом? Перед связистами всего мира стоит одна и та же задача – как переходить на IP протокол, и трудность этой задачи порождает законный вопрос - переходить ли вообще на IP протокол. Главным, заинтересованным «игроком» на этом поле смены парадигмы телекоммуникаций является индустрия: производители оборудования собираются заработать многие миллиарды долларов и платят журналистам многие миллионы на популяризацию новой парадигмы.

Сети телекоммуникаций сегодня напоминают Вавилонскую башню, которая вот-вот развалится. Слишком много стандартов (языков). По Библии, Бог обиделся за гордыню вавилонского народа, который имел один язык и посмел дружно строить башню до небес. Бог создал новые языки для разных людей, они перестали понимать друг друга и не смогли продолжить строительство башни.

Статья получена 18 июня 2014.

М.А. Шнепс-Шнеппе – ведущий научный сотрудник ЦНИИС (email: sneps@mail.ru).

Переход во всем мире на IP протокол, – не напоминает ли он гордыню вавилонян. Подобное дерзкое действо в настоящее время предпринимается в Соединенных Штатах – строятся две мощнейшие сети на базе IP протокола:

- GIG (Global Information Grid) – глобальная информационная сеть оборонного ведомства [1],
- NG9-1-1 – единая сеть нового поколения для обслуживания экстренных вызовов к любым общественным службам, в том числе – как от людей, так и от оберегаемого имущества [2].

Подобные же задачи решаются и в России, только более робко: строительство единой экстренной службы 112 и переход на цифровую технику в вооруженных силах. Сложности этих задач мы ранее рассматривали в работах [3][4]. Цель настоящей статьи – проанализировать опыт США и попытаться найти ответ на вопрос – что делать с телекоммуникациями в России?

II. Опыт США. Сеть GIG

Рисунок 1 иллюстрирует главную проблему, которая стоит перед строителями сети GIG. Сегодня основу GIG составляет коммутация каналов, точнее, стандарт SONET, 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 DRSN (Defense Red Switched Network),
3) сеть видеоконференцсвязи DVS (DISN VIDEO).

Кроме того, на рис. 1 указаны четыре закрытые сети JWICS, AFSCN, NIPRNet и SIPRNet:

- 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.

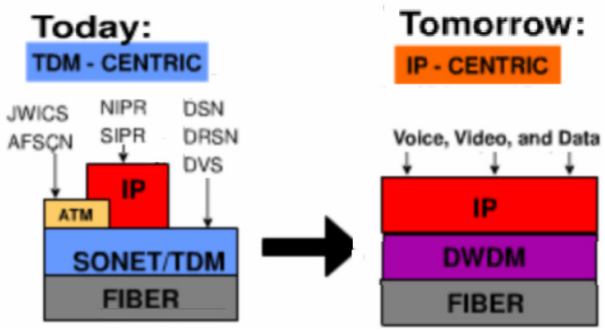


Рисунок 1. Иллюстрация текущей проблемы GIG: как перейти от TDM сети к IP сети.

Первые две сети JWICS и AFSCN построены на базе коммутаторов ATM (техника ATM в настоящее время больше не производится).

Согласно текущей стратегии Пентагона «Joint Vision 2020» провозглашен переход на IP протокол (рис. 2). Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями.

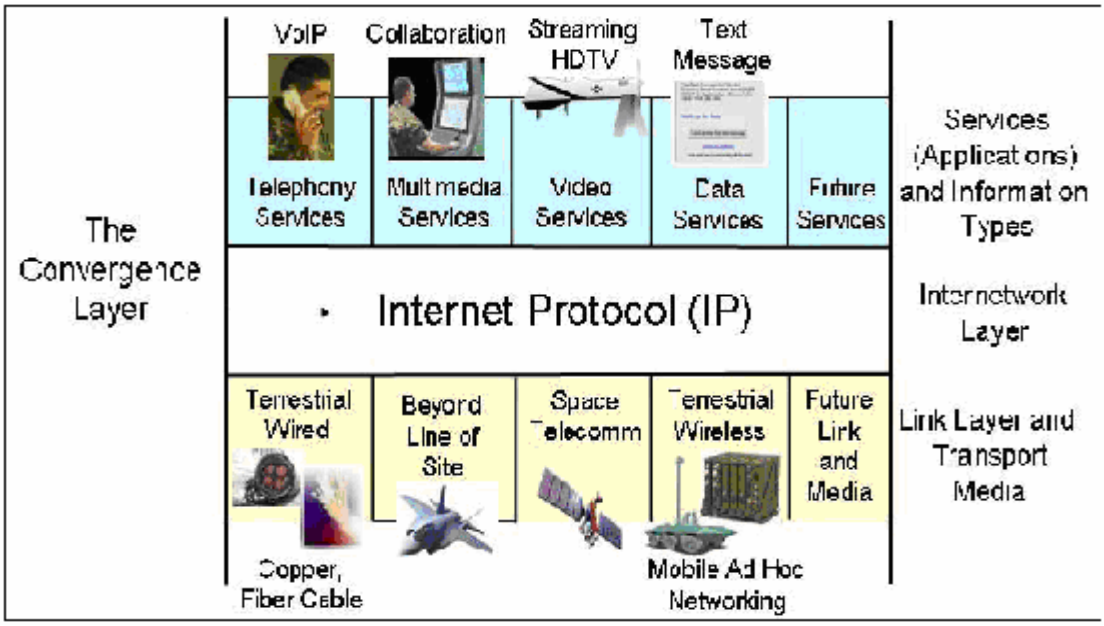


Рисунок. 2. IP протокол – единый протокол сети GIG.

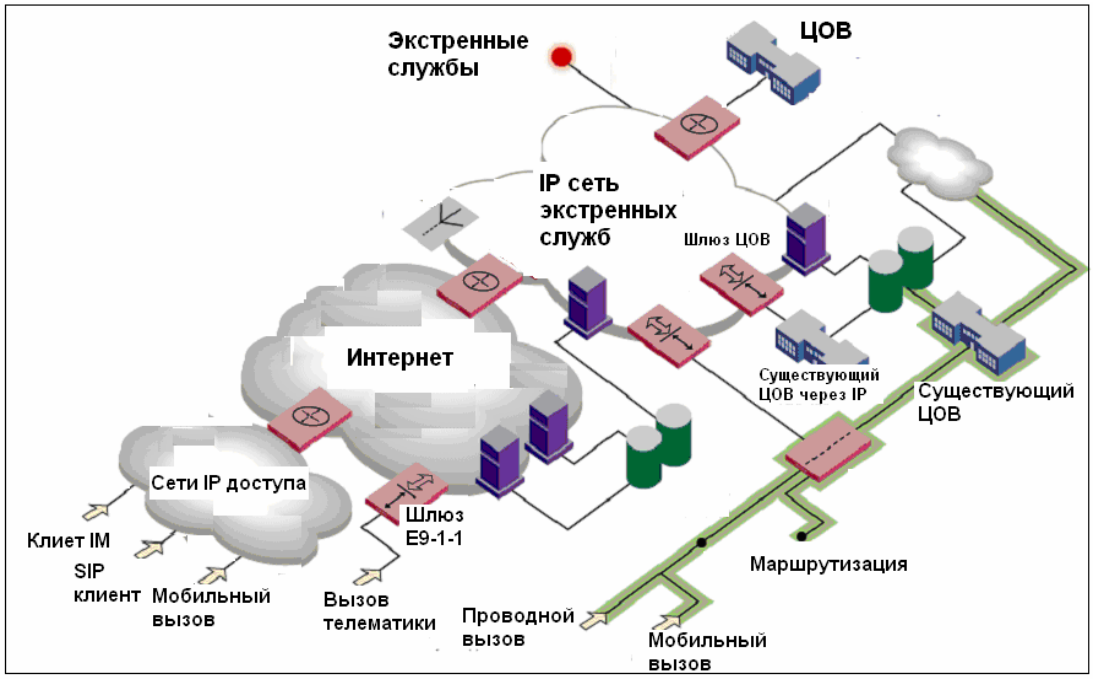


Рисунок 3. поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 911.

III. Опыт США. Сеть NG9-1-1

В США экстренные вызовы обслуживаются по номеру 911. Как и в России, внедрение в США единого номера экстренных служб проходит с трудностями, особенно определение номера вызывающего мобильного абонента и его местоположения.

Новейшее поколение службы экстренных вызовов в США имеет название NG9-1-1 и будет реализована в IP сети (рис. 3). Но когда будет реализовано, – это сегодня определить трудно. 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. 3 слева внизу: там отдельно указаны телематические вызовы. Эти вызовы из области M2M коммуникаций и относятся, в частности, к противопожарным и охранным службам. К 2008 были завершены пилотные проекты по проекту NG9-1-1. Однако широкое внедрение откладывается до перехода на IMS (IP Multimedia Subsystem). К тому же операторы связи не торопятся с переходом на IP протокол.

Риски перехода на IP протокол. 31 января 2014 г. Федеральная комиссия связи FCC издала документ о поддержке операторов, которые будут переходить от коммутации каналов (по технологии TDM) к IP протоколу [5]. По свежим следам этого документа FCC заказала юридической фирме оценку возможных рисков такого перехода. Фирма проанализировала историю нововведений в телефонных сетях, а также перечислила крупнейшие сбои в телефонных сетях от введения новой техники за последние более 20 лет [6]. 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 новом программном обеспечении, 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.

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

IV. Опыт США. Сравнение NG9-1-1 и GIG

В последнее время многие обращают внимание на аналогию между экстренной службой NG9-1-1, которую пытается создавать Министерство транспорта США, с одной стороны, и строящейся военной инфокоммуникационной системой GIG, с другой. Но как воспользоваться этой аналогией? И если аналогия есть, то, как согласовать планы создания этих двух систем многомиллиардной стоимости?

Сошлемся на материалы Конференции по внутренней безопасности (Homeland Security) США[7], где автор статьи разбирает эту аналогию и начинает с напоминания, что эти два проекта были объявлены практически одновременно – в 2007 году.

Аналогии начинаются с высокого уровня архитектуры сетей NG9-1-1 и GIG. 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, согласно концепции NG9-1-1, больной вызывает скорую помощь текстовым сообщением. Это сообщение достигает PSAP (Public Safety Answering Point, 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 GIG архитектуре 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 аналитику вооружения. Аналитик сообщает ответ солдату, а также может вызвать бомбардировщика и известить разведку для уточнения цели.

Аналогия между NG9-1-1 и GIG налицо, но кто ею воспользуется и согласует планы строительства этих двух систем?

V. Особенности современной сети GIG

Вспомним, как закладывались основы GIG, которые ныне являются тормозом ее модернизации? Оборонная информационная сеть DISN (Defense Information Systems

Network) разрабатывается с начала 1990-х. 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 1996 г. состояние сети DISN было подвергнуто резкой критике. Прежде всего, это – низкий уровень интеграции входящих в состав DISN-NT сетей, что существенно ограничивает взаимодействие в рамках единой сети и препятствует эффективному единому управлению всеми ее ресурсами. В частности, отмечались сложности взаимодействия стационарной и полевой (мобильной) компонент 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). Это порождает дополнительные трудности материального обеспечения боевых сил, технического обслуживания и подготовки специалистов. Кроме того, используемые сетевые технологии недостаточно масштабируемы и не в состоянии, в должной мере, предоставлять пропускную способность по требованию. Из-за отсутствия общей архитектуры и стандартов затруднена передача данных в интересах разведки и РЭБ. Несовместимость оборудования усложняет применение различных средств засекречивания и криптозащиты. В целом базовая архитектура DISN-NT недостаточно гибкая и масштабируемая, особенно для мобильных сил, оперативно развертываемых в различных точках мира.

Поэтому при разработке принципов построения второй очереди сети DISN-NT агентство DISA пошло по пути использования готовых коммерческих продуктов в области новых информационных и сетевых технологий. При этом упор был сделан на открытые системы, которые основаны на национальные стандарты, и на новейшие коммерческие технологии и услуги (Commercial-Off-the-Shelf) [8].

Эти требования нашли отражение в 15-летней программе развития вооружений «Joint Vision 2010» , которую командование МО США (US Joint Chiefs of Staff) приняло в октябре 1996 г. В части средств связи основной выбор пал на интеллектуальные сети (Advanced Intelligent Network, AIN), о чем представитель агенства DISA доложил в 1999 г. на международной конференции по военным коммуникациям MILCOM'99 [9]. Вот цитата из его выступления: «Будущие сети DISA будут пользоваться преимуществами программных средств IN. Сервисы AIN станут ядром технологии развития, технологии оценки (assessment) и технологии передачи информации МО. Результаты сервисов AIN обеспечат командиров боевых действий способностью собирать, обрабатывать и передавать информацию без перерывов в работе сети. Возможности AIN станут краеугольным камнем информационного превосходства МО».

На той же конференции MILCOM'99 выступил представитель компании Lockheed Martin Missiles & Space [10], компании, которая является головным разработчиком глобальной информационной сети сил НАТО. В этом докладе подчеркивается, что AIN обеспечивает пользователей любыми сервисами, как то: голос, данные, e-mail, video, офисные приложения, вызовы «800». А главное, в докладе подробно описывается ключевая роль протокола SS7: он обеспечивает предоставление перечисленных сервисов, включая спутниковую связь.

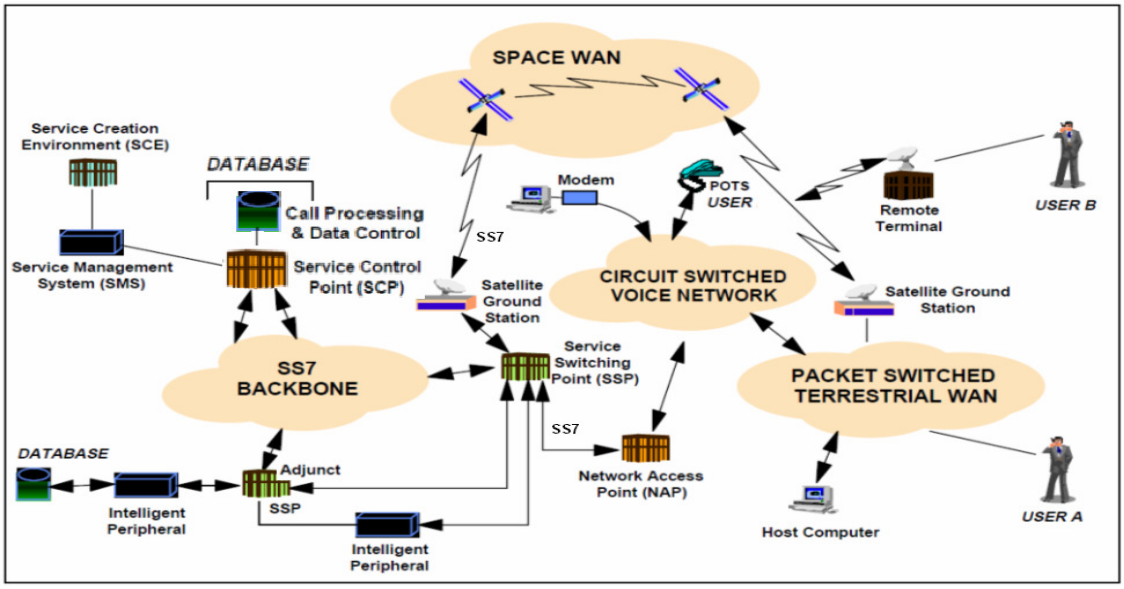
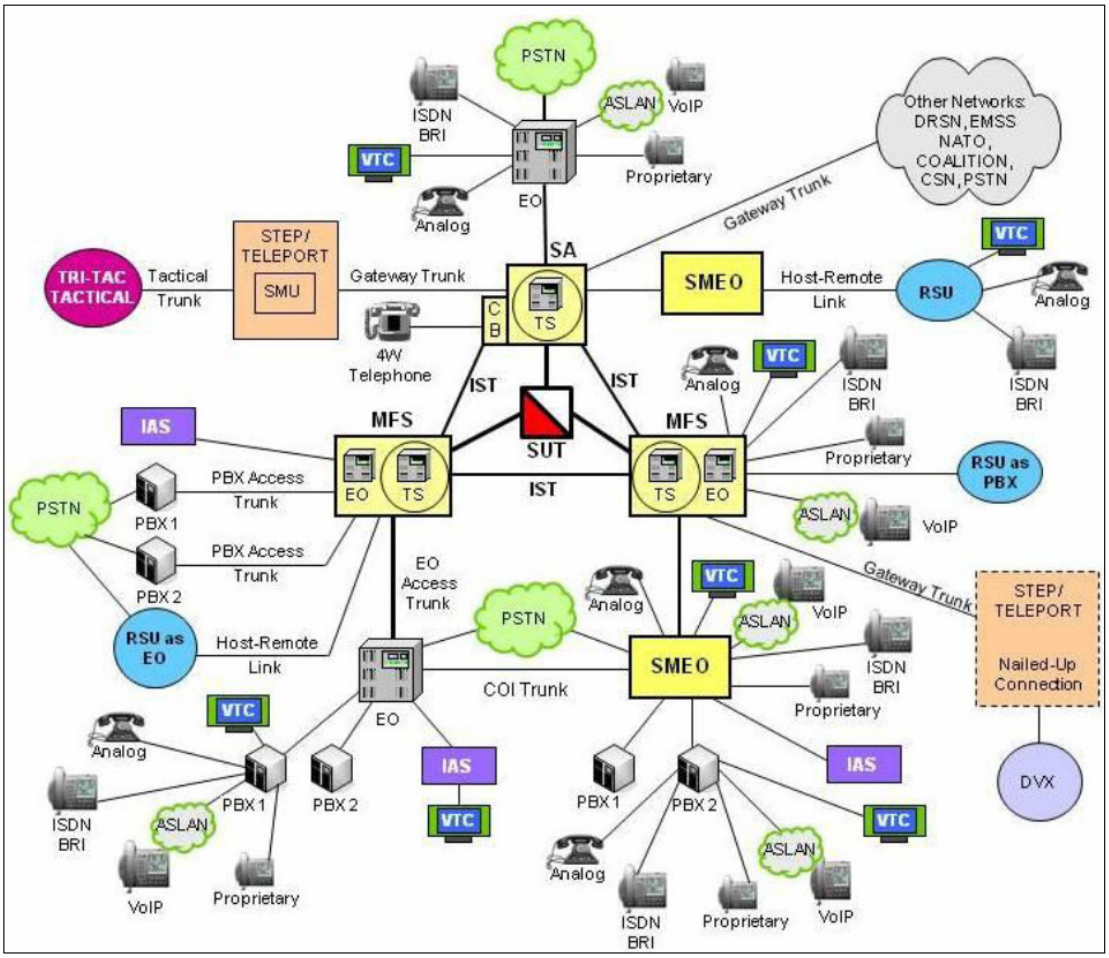


Рисунок 4. Архитектура Advanced Intelligent Network (AIN).

Связующим звеном сети AIN служит система SS7 (рис. 4). 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.

Сеть SS7 является, образно говоря, нервной системой DISN. Рисунки 5 и 6 взяты нами из документации по тестированию сети SS7 в составе DISN, которое в 2011 году проводила компания Tekelec [11]. В центре схемы размещен блок SUT (System Under Test), это тестируемая сеть SS7. То есть на оборонной сети DSN соединения устанавливаются при помощи сигнализации SS7, а на периферии используются устройства любого типа. На сети появляются все новое оконечное оборудование, в значительной мере это IP средства, а сеть SS7 сохраняет свое центральное место. Устройства подключаются по любым протоколам: 4W – 4х проводной, ASLAN – засекреченная локальная сеть, ISDN BRI, VoIP – интернет-телефония, VTC – видеоконференцсвязь, proprietary – любой нестандартный протокол.



LEGEND:

4W	4-Wire
ASLAN	Assured Services Local Area Network
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switch Network
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multifunction Switch
NATO	North Atlantic Treaty Organization
PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PSTN	Public Switched Telephone Network
RSU	Remote Switching Unit
SA	Standalone
SMEO	Small End Office
SMU	Switched Multiplex Unit
STEP	Standardized Tactical Entry Point
SUT	System Under Test
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Рисунок 5. Архитектура DSN (Defence Switched Network).

Рис. 6 раскрывает производителей используемого телефонного оборудования на оборонной сети DSN: на уровне контроллеров SCP используются станции производства компаний Alcatel-Lucent и Siemens. Отметим, что справа на рис. 6 показаны две локальные компьютерные сети (LAN), которые общаются и через сеть коммутации каналов передают зашифрованную информацию по протоколу SSH (Secure Shell).

Отсюда делаем важный вывод: наличие сети SS7 не препятствует переходу на IP протоколы, а скорее наоборот – облегчает переход на пакетную коммутацию, делает его постепенным. Лишь базы данных на весь

период перехода будут размещаться не в узлах IMS, а в IN и будут доступны как по протоколу SS7, так и по протоколу SIP.

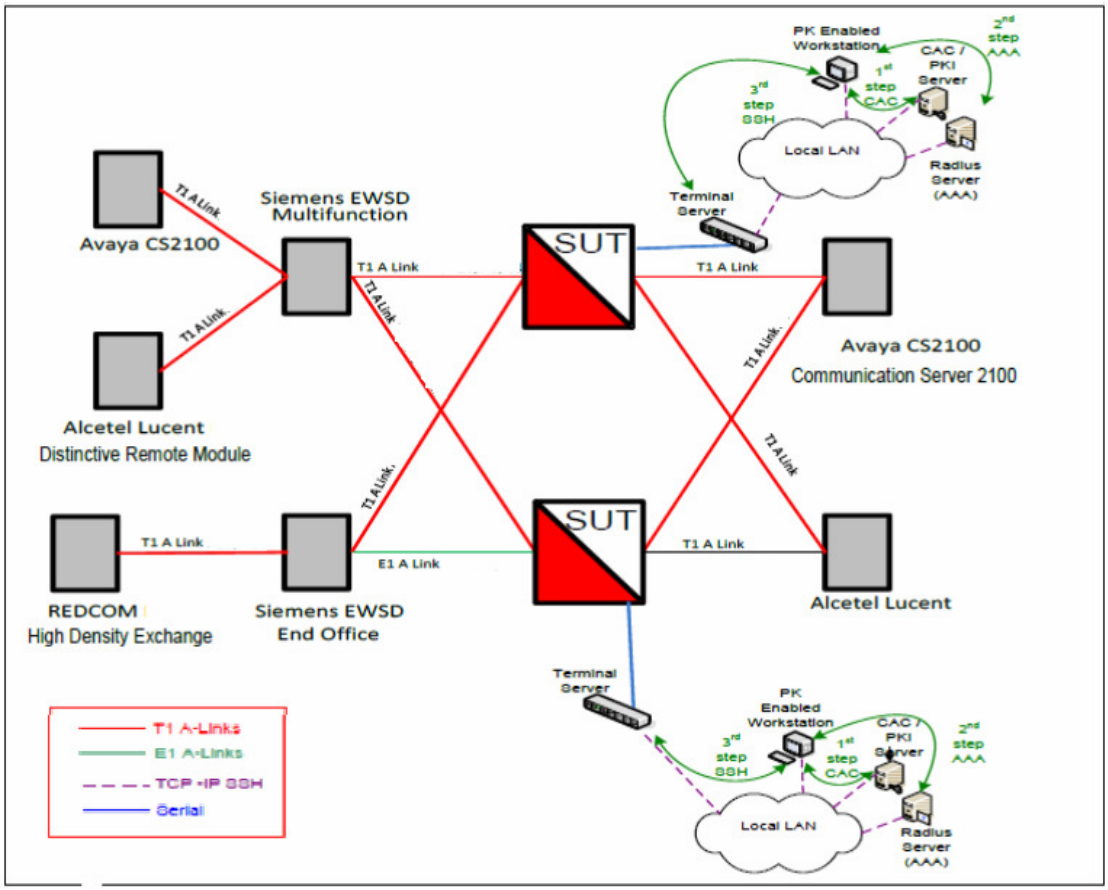


Рисунок 6. Конфигурация тестируемой сети SS7.

VI. Трудности с поддержкой AIN

Напомним, что средства интеллектуальной сети (Advanced Intelligent Network, AIN) были разработаны в Bell Labs в начале 1980х, и на сети связи США их внедряла компания Bellcore (наследница Bell Labs после 1984 г.). И вот сейчас – через 20-30 лет – обнаружились чрезвычайные сложности с поддержкой сети AIN.

С самого начала принятия программы «Joint Vision 2010» за интеллектуальную сеть AIN в составе глобальной оборонной 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, например, сайт для ветеранов: lockheedmartin-veterans.jobs. Там названы требования к набору аналитиков информационных систем для работы в оборонном агентстве DISA (Форт Мид, штат Мэриленд):

• Необходимо понимать оборонную доктрину США и как эффективно использовать тактические и стратегические телекоммуникационные системы,

• Применять специальные знания военных свойств, встроенных в аппаратную и программную часть сети, для обеспечения боевых действий,

• Внедрять и расширять возможности AIN,

• Обеспечить выполнение требований криптографических систем, используемых в сети,

• Иметь опыт работы с одной или более системами: IP маршрутизация; QoS/MPLS; расчеты трафика; расчеты каналов сети; DNS; ATM коммутация; VPN; TDM коммутация; волоконная техника; Crypto; сетевые применения (WAN ускорители и др.); голосовые и видеосервисы.

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.

Другой факт. МО США в 2012 г. заключило крупнейший 7-летний контракт на сумму в 4,6 млрд. долл с Lockheed Martin, в задачах которого входит модернизация, управление и эксплуатация глобальной информационной сети министерства обороны США [12]. Сумма контракта неявно свидетельствует о том, что Пентагон имеет трудности с поддержкой сети GIG, что порождает сомнения в ее жизнеспособности. Не сообщено, имеются в контракте работы по переводу ядра GIG на IP протокол.

VII. Опыт России. Из истории разработки АТС

Рассмотрим развитие отечественных сетей связи с точки зрения технологий. Каковы основные достижения

российских связистов постсоветского периода? На ум, прежде всего, конечно, приходят мобильная связь и Интернет. Но следовало бы назвать систему телефонной сигнализации ОКС-7 (SS7), которая является связующим звеном интеллектуальной сети (IN). Ныне много говорят о переносимости телефонного номера и обслуживании экстренных вызовов. Это ведь 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.

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

Разработка советской системы ОКС-7 началась в 1970-х годах с созданием квазиэлектронных междугородных АТС. В квазиэлектронных АТС коммутация осуществляется герконами, а управление является электронным. 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, в том числе:

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

КЭАМТС «Кварц» успешно производилась и эксплуатировалась до распада СССР.

С начала 1980х годов разрабатывались 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 система телефонных станций 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.

Причин неудач разработки IT&T было несколько, в том числе: высокая интеграция микросхем (опережающая уровень развития микроэлектроники того времени), недоработки программного обеспечения. Естественно, что даже широкая кооперация не могла спасти сложнейший проект ЕССКТ, хотя бы потому, что в социалистическом лагере отставала микроэлектронная промышленность, и проект ЕССКТ перестал существовать с распадом СССР и СЭВ.

VIII. Как проходило внедрение ОКС-7 в России

Обратимся к статье Н. С. Мардера и А. С. Аджемова от 1997 г. [13]: «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 [14]. На территории России размещены восемь УАК, как показано на рис. 7.

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

Оказывается, что уже изначально сеть ОКС № 7 не планировалась на охват всех АТС страны, так как для нумерации пунктов сигнализации ОКС № 7 выбраны 14-битные номера (т.е.214 = 16384). В США же для сети SS7 выбраны 24-битные номера. Как замечает Н.С. Мардер [15], «требуется разработка нового плана нумерации национальной сети сигнализации ОКС-7».

Для построения 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, как оказалось, было требованием чрезмерным, так как для этого пришлось бы переработать программное обеспечение множества станций. Тем самым, единая интеллектуальная сеть

России осталась недостроенной, что и сказывается ныне на построение Системы-112.

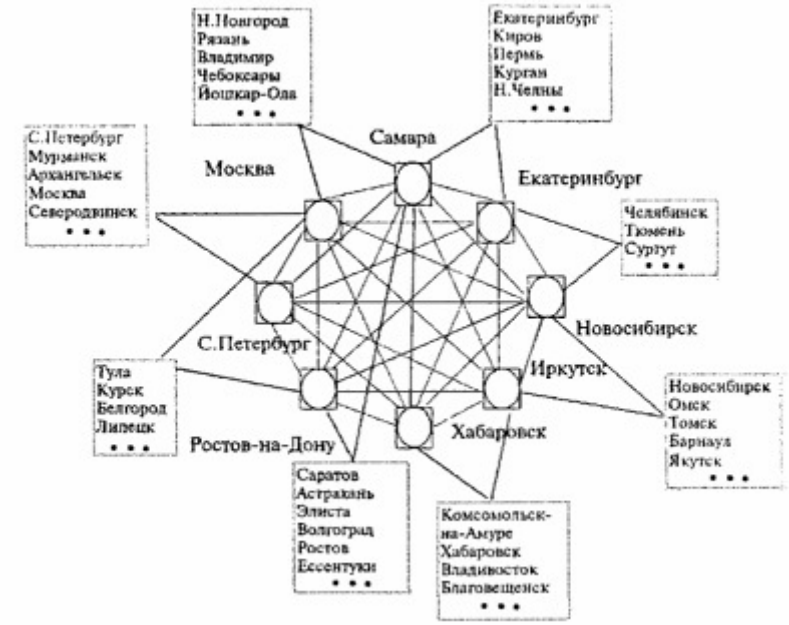


Рисунок 7. Структура междугородной сети ОКС № 7.

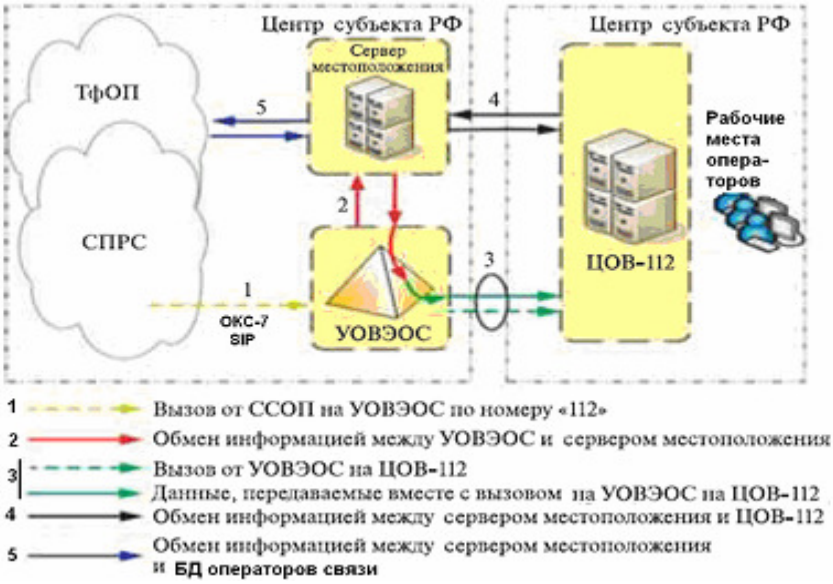


Рис. 8. Пять интерфейсов Системы-112.

IX. Состояние Системы 112

В настоящем разделе обсудим вопросы создания Системы-112 с точки зрения развития средств связи и сформулируем некоторые задачи, которые, на наш взгляд, следовало бы включить в Программу работ [16]. Воспользуемся иллюстрацией (рис. 8), которая дает представление о телекоммуникационной составляющей системы "112" [17]. Здесь УОВЭОС – узел обработки вызовов экстренных оперативных служб.

На рис. 8 указаны пять интерфейсов Системы-112, которые предполагается уточнить уже на первом этапе работ по Постановлению (до 2014), что представляет собой исключительно сложную работу. Кроме того, представленную концепцию Системы-112, на наш взгляд, следовало бы существенно доработать. Выскажем три замечания:

1) О протоколе SIP. Сомнения вызывает его включение наряду с ОКС-7. Протокол SIP еще недостаточно апробирован для использования в Системе-112, учитывая ее чрезвычайную государственную важность,

2) О перегрузках. На рис. 8 показано прохождение отдельного вызова в Системе-112. А как поступать в условиях реальных ЧП, когда из-за перегрузки имеющихся ресурсов экстренных служб часть вызовов могут быть потеряны (что не допустимо)? В случаях действительно крупных ЧП в распоряжении МЧС должны были бы поступать и другие ЦОВ, в том числе ЦОВ Ростелекома, что на схеме не показано.

3) Не указаны средства доступа (абонентские устройства) к Системе-112, которые также относятся к телекоммуникационной составляющей.

В официальном отчете Минкомсвязи [18] перечислены нерешенные задачи: «Ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей общего пользования для прохождения вызовов, поступающих в службу по номеру «112». Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений».

Это означает, что системный проект Системы-112 до сих пор не разработан, и все проведенные к настоящему времени работы следует рассматривать как экспериментальные образцы. И еще. Единая «Система-112» в масштабах страны, на наш взгляд, должна опираться на междугородную сеть России, подобному тому, как устроена мобильная сеть вообще.

X. ОАО «Ростелеком» идет к «All-over-IP»

В настоящее время намечается приватизация ОАО "Ростелеком». Государство рассчитывает выручить от сделки не менее 5 миллиардов долларов. Возникает вопрос: оправдана ли ожидаемая выручка с точки зрения не сиюминутных, а долгосрочных интересов государства? Отметим, что «Ростелеком» является крупнейшим оператором связи в России, обслуживающим более 100 миллионов абонентов в 80 регионах страны. Если компания остается государственной, то на нее можно возложить еще нерешенные задачи государственной важности в области связи, в том числе создание Системы 112. Такое будет затруднительно делать, если она переходит в частные руки.

Вот подтверждение этим сомнениям. По информации "Коммерсанта", президент Владимир Путин 31 мая 2013 года одобрил идею ФСБ о создании интегрированной сети связи для нужд обороны, обеспечения безопасности и правопорядка [19]. В частности, речь идет о федеральной целевой программе "Создание интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка".

Но такой проект обойдется необоснованно дорого. В составе выделенной сети специальной связи для всех силовых структур должны быть коммутаторы, наземные и спутниковые каналы связи, отдельный спутник и единый центр управления, рассказал бывший гендиректор "Ростелекома" Антон Колпаков: "Строительство подобной сети будет сопоставимо по масштабам со строительством второго "Ростелекома", но с меньшей пропускной способностью. Такая сеть будет стоить десятки миллиардов долларов".

С целью обеспечения доходов от мультимедийного трафика «Ростелеком» взял курс на стратегию «All-over-IP», т.е. перестраивает сеть под IP протокол. Эти планы иллюстрирует презентация «Развитие сети IP телефонии Ростелекома» [20]. На рис. 9 показано взаимодействие традиционных операторов ТфОП с интернет-операторами ITSP. При этом предполагается, что сохранятся имеющиеся услуги интеллектуальных сетей связи с доступом по кодам DEF: Бесплатный вызов, Телеголосование и другие.

Типовой узел новой IP сети полностью построен на оборудовании Cisco. Общение с узлом УАК/МЦК производится посредством системы ОКС-7 (по каналам F-links) и по B-каналам системы ISDN. Для общения с системой ОКС-7 указан узел SLT (Cisco Signaling Link Terminal). Подобная IP сеть строится вокруг каждого УАК/МЦК, что на рис. 7.

Важнейшим проектом «Ростелекома» является высокоскоростная IP-магистраль, которая построена на базе ресурсов собственной первичной сети по технологии MPLS (Multi-protocol Label Switching) и обеспечивает конвергенцию услуг по передаче видео, речи и данных.

IP/MPLS-инфраструктура имеет свыше 350 точек доступа на всей территории России, десять опорных и около 150 региональных узлов в регионах РФ, построена с использованием маршрутизаторов компании Juniper - магистральных маршрутизаторов T1600 производительностью до 1,6 Тбит/с и менее мощных пограничных маршрутизаторов.

Общая протяженность магистральной сети составляет более 40 тыс. км., пропускная способность достигает 1 Тбит/с, емкость внешних каналов составляет 200 Гбит/с. Компания также присутствует на зарубежных узлах (в Стокгольме, Лондоне, Гонконге, Франкфурте, Амстердаме), имеет сеть собственных дата-центров в Москве, Казани, Екатеринбурге, Новосибирске, Хабаровске.

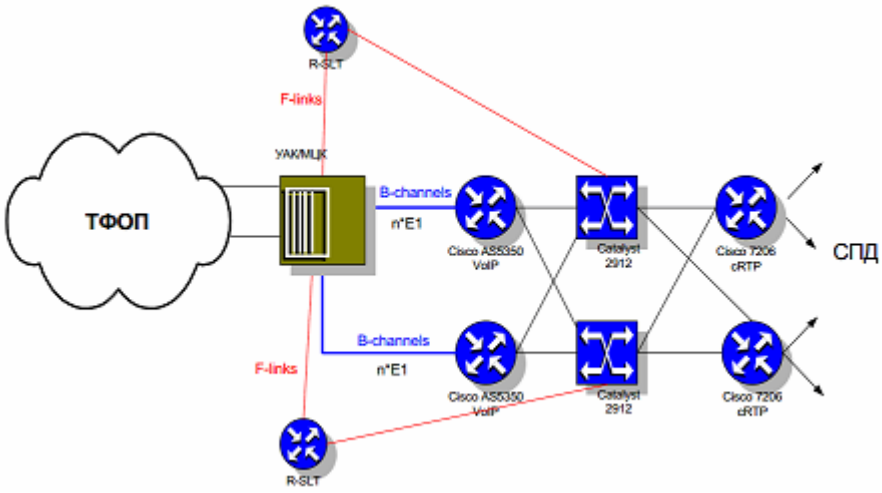


Рисунок. 9.Типовой узел IP сети.

Рисунок 10. IP/MPLS сеть ОАО «Ростелеком» [21]

XII. Две стратегии связистов России

Стратегия 1. Это – продолжить курс Ростелекома. Суть этой стратегии - продолжение строительства сетей связи средствами иностранных производителей. Образно говоря, это означает – «зажмуриться» и идти к «All-over-IP», идти, опасаясь – не случиться ли коллапс сети и потеря управления страной.

Тут уместно вспомнить историю. В 1991 г. в ходе операции "Буря в пустыне" США продемонстрировали новые средства ведения информационной войны. С помощью электронных излучателей американцам, например, удалось нарушить радио- и телефонную связь практически на всей территории Ирака, что в значительной мере предопределило исход боевых действий. Вывести из строя систему управления противовоздушной обороны Ирака спецслужбам США удалось с помощью активации специальных вирусов, которые были «заранее» спрятаны в памяти принтеров, приобретенных для этой системы у одной коммерческой фирмы.

Основной выигрыш от коммутации пакетов состоит в более экономном использовании каналов – за счет заполнения пауз, а главное, что подчеркивают пропагандисты новой техники, – это ее гибкость и универсальность. Достаточно ли этого для смены технологий.

Следует учитывать и недостатки коммутации пакетов:

1. Неопределенность времени передачи данных, так как задержки в очередях буферов зависят от загрузки сети.
2. Колебания времени передачи – из-за скачков загрузки сети.
3. Возможные потери пакетов – из-за переполнения буферов.
4. Из-за добавления заголовков в пакетах и ожидания в буферах «чистое» время занятия канала удлиняется: при коммутации каналов сигнальная информация передается один раз, при коммутации пакетов – добавляется к каждому пакету.
5. Усложняются алгоритмы передачи секретных данных, тем более для передачи приоритетных данных.

Заметим, что гибкость и универсальность новой технологии, к огорчению отечественных производителей, достигается за счет применения в узлах коммутации (в маршрутизаторах) микросхем сверхвысокого быстродействия.

Сети «Ростелекома» сегодня стали ареной борьбы двух американских компаний Cisco и Juniper. Действительно, на базе такого оборудования можно строить современные сети. Но, к сожалению, эта стратегия приводит к зависимости от этих компаний на все обозримое будущее. И как быть с безопасностью страны?

Стратегия 2. Суть этой стратегии заключается в выборе курса на импорто-замещение, т.е. на развитие сетей связи собственными силами. Для этого надо вернуться к тому состоянию знаний, которые были достигнуты ранее – лет 20 назад и развивать их далее. В данном случае такой точкой отсчета условно можно назвать систему ОКС-7. В России отставание от передового мирового уровня, конечно, большое, особенно по технике коммутации пакетов, где требуется мощная микроэлектроника. Но тем более стоит оценить перспективы коммутации каналов, т.е. вспомнить прошлое и продолжить движение вперед ускоренными темпами (догонять-то проще). Наше предложение – восстановить промышленность средств связи.

XIII. Примечание редактора

Эта статья является продолжением целой серии интересных статей, опубликованных автором ранее [3][4][12]. Что здесь можно заметить? Во-первых, автор, очевидно, является последовательным пропонентом системы SS7. Эти, а также другие статьи автора, например, [22][23][24], объединены общей идей – переиспользования заделов традиционной телефонии в современных системах. Кажется, что это весьма интересная тема для дискуссий относительно архитектуры телекоммуникационных систем. Очевидно, что, по крайней мере, практический (экономический) эффект от использования существующего задела [25] явно присутствует. А что еще? Готовы предоставить страницы нашего журнала для дискуссии.

В данной же статье автор пошел еще дальше и (см. раздел XII) раскритиковал коммутацию пакетов. На самом деле, с той же самой про-SS7 позиции – возможные трудности управления. Это также видится хорошим поводом для дискуссии. Было бы интересно, например, рассмотреть этот вопрос в свете бурного роста SDN. Да и MLPS никуда не пропадал.

В целом, нам кажется, что до последнего слова здесь еще далеко.

Библиография

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

[2] Next Generation 9-1-1 (NG9-1-1) System Initiative Concept of Operations. U.S. Departament of Transportation. April 6, 2007, Version 2.

[3] Шнепс М. А. От IN к IMS. О российской Системе-112: нерешенные задачи //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 1. – С. 1-11.

[4] Шнепс М. А. О сетях телекоммуникаций для Системы 112, МЧС и МО //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 3. – С. 1-10.

[5] FCC. Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13-5, FCC 14-5 (rel. Jan. 31, 2014) .

[6] FCC. In the Matter of Technology Transitions GN Docket No. 13-5, March 19, 2014. http://apps.fcc.gov/ecfs/document/view?id=7521093879 Retrieved: Jun, 2014.

[7] 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: Jun, 2014.

[8] В. Жигадло. Телекоммуникационные сети военного назначения США и стран НАТО. Особенности и тенденции развития // Электроника НТБ. Выпуск #4/1999

[9] B.T. Bennet. Information Dissemination Management/ Advanced intelligent Network services for department of Defence// MILCOM, 1999.

[10] W.W. Chao. Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters// MILCOM, 1999

[11] http://jitc.fhu.disa.mil/tssi/cert_pdfs/tekeleceagle_tn1030701.pdf Retrieved: Jun, 2014.

[12] Шнепс М. А. От IN к IMS. О сетях связи военного назначения //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 2. – С. 1-11.

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

[14] http://www.gosthelp.ru/text/PolozhenieOsnovnyepolozhe2.html/ Retrieved: Jun, 2014.

[15] Н.С. Мардер «Современные телекоммуникации», Москва, 2006.

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

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

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

[19] 19. http://hitech.newsru.com/article/28aug2013/fsb_bound Retrieved: Jun, 2014

[20] http://support.comptek.ru/download/index.xhtml/255/rostelekom_burkov.pdf Retrieved: Jun, 2014

[21] http://servernews.ru/Rostelekom-opublikoval-kartu-magistralnoy-seti-IPMPLS Retrieved: Jun, 2014

[22] Волков А. А., Намиот Д. Е., Шнепс-Шнеппе М. А. О задачах создания эффективной инфраструктуры среды обитания //International Journal of Open Information Technologies. – 2013. – Т. 1. – №. 7. – С. 1-10.

[23] Шнепс-Шнеппе М., Намиот Д. Интеграция СМИ и телекоммуникаций //International Journal of Open Information Technologies. – 2013. – Т. 1. – №. 8. – С. 7-12.

[24] Sneps-Sneppe, Manfred, Anatoly Maximenko, and Dmitry Namiot. "On M2M communications standards for smart metering." arXiv preprint arXiv:1306.4133 (2013).

[25] Schneps-Schneppe, M., Namiot, D., Maximenko, A., & Malov, D. (2012, October). Wired Smart Home: energy metering, security, and emergency issues. In Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on (pp. 405-410). IEEE.

Telecommunications for emergency and military needs: in parallels

Sneps-Sneppe M.A.

***Abstract*— Nowadays, an ideal unified world of telecommunications and computers uses IP protocol. Currently in the United States, IP-based network built two powerful nets: GIG (Global Information Grid) - a global information network of the defense department and NG9-1-1 - a single next-generation network services for emergency calls to any public services. It covers calls from both humans and protected property. Similar problems can be solved in Russia, only more timidly by building a single emergency number 112 and the transition to the digital technology in the armed forces. The article compares the two strategies of development networks in Russia. The first strategy - the continuation of the construction of communication networks by means of foreign vendors. The essence of the second strategy is to choose a course of import substitution, in other words, on the development of communication networks by the local firms.**

***Keywords*— SS7, intelligent network, IP protocol, global network GIG, NG9-1-1.**