Об эволюции сети DISN с учетом кибербезопасности

М.А. Шнепс-Шнеппе

***Аннотация*—Рассмотрены трудности перехода от коммутации каналов к коммутации пакетов на примере информационной сети GIG Министерства обороны США – крупнейшей в мире ведомственной сети. Обсуждаются свойства многофункционального софтсвича MFSS как основы перехода от TDM к IP, унификация информационных услуг и целевая инфраструктура сети связи DISN. Детально описаны вопросы кибербезопасности сети DISN. Обсуждены задачи российских связистов по созданию Системы 112 и телекоммуникационной сети гражданской обороны.**

***Ключевые слова*— коммутация каналов; коммутация пакетов; многофункциональный софтсвич; DISN; импортозамещение; система 112.**

I. Введение

Цель настоящей статьи – изучить стратегию развития телекоммуникаций, особенно противоборстко двух поколений техники связи: коммутации каналов и коммутации пакетов. Для этого воспользуемся новейшими методическими материалами по построению Глобальной информационной сети Пентагона – GIG (Global Information Grid). Имеется богатый открытый материал, например, два тома изложения основ информационной архитектуры военного ведомства от 2012 г. [1], 916-страничный документ с описанием унифицированных услуг военной связи (Unified Capabilities, UC) от 2013 г. [2] и 295-страничное описание основ UC для армии [3]. Сеть GIG представляет собой крупнейшую и богатейшую в мире ведомственную сеть, и разбор трудностей, которые выявляются при переходе от коммутации каналов к коммутации пакетов, а в последнее время – и с учетом кибербезопасности, на наш взгляд, может быть весьма поучительным.

Цель статьи, по существу, состоит в выработке рекомендаций по развитию отечественного производства средств связи, по крайней мере, по созданию российской Системы 112 и телекоммуникационной сети гражданской обороны вообще. Разработка системы 112 представляет собой сложнейший проект государственного значения, затрагивающий все стороны жизни российского общества. В ходе его реализации обнажаются многие недостатки хозяйства страны, накопившиеся за четверть века капиталистического строительства. Рассмотрение опыта США по созданию двух подобных систем: глобальной информационной сети оборонного ведомства GIG (Global Information Grid) и единой сети нового поколения для обслуживания экстренных вызовов NG9-1-1 – помогает понять, почему так трудно выполнить намеченные задачи. В этой же плоскости лежит анализ стратегии российских связистов в условиях импортозамещения.

Рисунок 1 иллюстрирует главную проблему, которая стоит перед архитектами сети GIG. Сегодня основу GIG составляет коммутация каналов, точнее, стандарт SONET (в Европе сответствующий стандарт SDH), по которому работают оптические кабели, а информация кодируется согласно телефонному стандарту TDM (Time Division Multiplexing). По этой сети коммутации каналов сегодня работают основные сети связи Пентагона:

1) телефонная сеть DSN (Defense Switched Network),
2) закрытая правительственная коммутируемая сеть DRSN (Defense Red Switched Network),
3) сеть видеоконференсвязи DVS (DISN VIDEO).

Кроме того, на рис. 1 указаны четыре закрытые сети, 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) построены на базе коммутаторов ATM (техника ATM в настоящее время больше не производится). Все эти сети (и другие, непоказанные на рисунке) следует перевести на IP технологию (рис. 1 справа), точнее, все услуги (голос, видео и данные) в будущем должны предоставляться по IP протоколу.

Статья получена 7 февраля 2016.

М.А. Шнепс-Шнеппе д.т.н, профессор, генеральный директор ООО «ЦКБ-Абаванет» (e-mail: sneps@mail.ru).

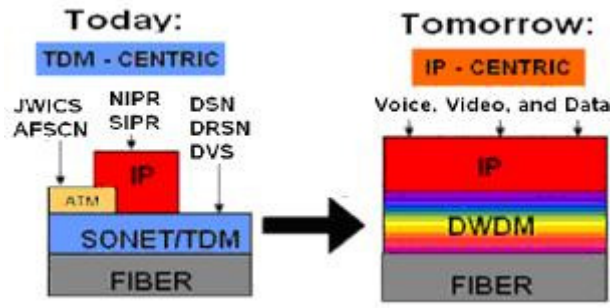

Рис. 1. Иллюстрация текущей проблемы GIG: как перейти от TDM сети к IP сети.

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 технологию означает и смену системы сигнализации – переход от базового ныне протокола SS7 на SIP протокол (точнее, на его новую расширенную версию – AS-SIP).

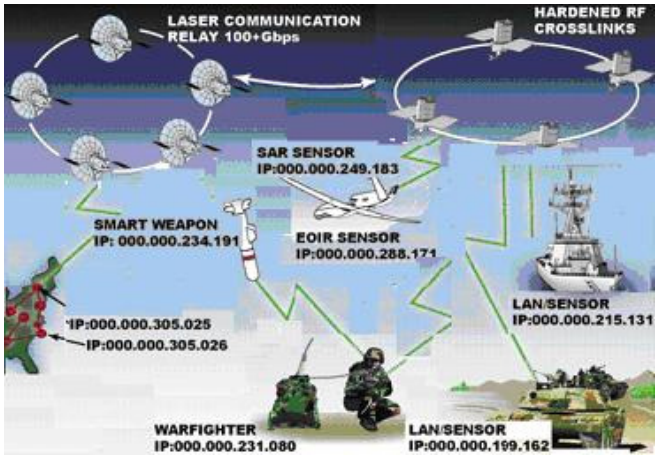

Рис. 2. В будущей сети DISN протокол IP будет объединять всех участников боевых действий: каждая платформа, каждый сенсор, даже ракета будут интегрированы в единой сети с солдатом [4].

В новейшей истории развития сети DISN можно выделить три этапа:

1) В 1996 г. командование МО США (US Joint Chiefs of Staff) приняло 15-летнюю программу развития вооружений «Joint Vision 2010». В этой программе в части средств связи основной выбор пал на протокол сигнализации SS7 и архитектуру интеллектуальных сетей (Advanced Intelligent Network, AIN),

2) В 2006 году был принят план Пентагона «Joint Vision 2020» о смене парадигмы сети DISN (Defense Information Systems Network) – переход от коммутации каналов к коммутации пакетов (рис. 2), точнее, от протокола сигнализации SS7 к IP протоколу AS-SIP, что требует кардинальной перестройки GIG.

3) А в 2010 году появилась новая инициатива – кибервойна, было создано киберкомандование, что задачу перехода к IP протоколу значительно усложнило, например, требуется резко сократить число крупных узлов на сети, чтобы упростить борьбу с киберугрозами. (Обсуждению кибервойны посвящены наши статьи [5, 6].)

Подобные же этапы развития проходят и будут проходить и на российских сетях. Вопрос только об импортозамещении – какая доля средств связи будет собственного производства.

Далее в разделе 2 мы рассматриваем многофункциональный софтсвич MFSS как основу перехода от TDM к IP, в разделе 3 – сеть DISN и потребности военного ведомства. В разделах 4 и 5 обсуждаем унификацию информационных услуг и целевую инфраструктуру DISN. Вопросам кибербезопасности сети DISN посвящены разделы 6 и 7. В завершении (раздел 8) обсуждаем задачи российских связистов.

II. Коммутатор MFSS – основа перехода от TDM к IP

Переход от сети коммутации каналов, где господствует протокол SS7, к коммутации пакетов и протоколу SIP (или к AS-SIP) требует установки шлюзов — программных коммутаторов MFSS (MultiFunction SoftSwitch).

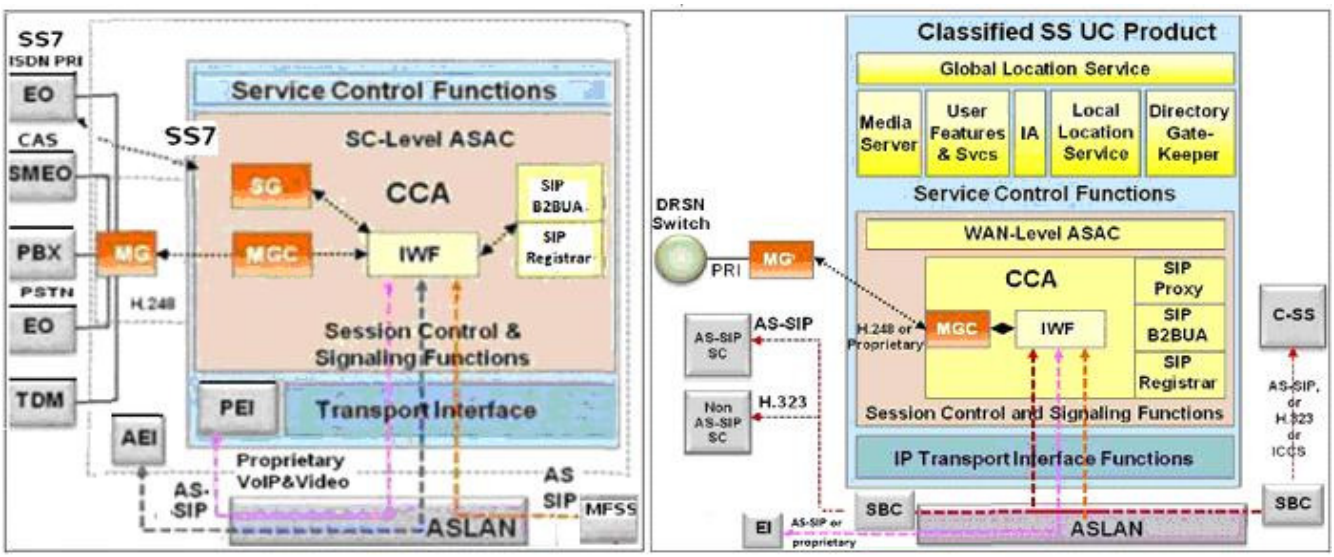

Рис. 3. Многофункциональный программный коммутатор MFSS: слева – текущая версия, справа – будущая версия, где господствует AS-SIP (за исключением «островка» правительственной связи DRSN с сигнализацией ISDN PRI)

Напомним, что SoftSwitch обеспечивает переход от сети коммутации каналов к сети коммутации пакетов, но не заменяет саму сеть коммутации каналов. Он только управляет согласованием протоколов сигнализации SIP и SS7 (посредством шлюза SG) и преобразованием IP пакетов в TDM посылки (посредством шлюза MGC). Объясним, как многофункциональный софтсвич MFSS управляет вызовами (рис. 3 слева):

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

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).

Укажем на различия в протоколе SIP (Session Initiation Protocol) и в его расширенной версии AS-SIP (Assured Service – Session Initiation Protocol). SIP протокол определяет установление интернет-сеанса связи (по стандарту IETF RFC 3261), что включает также обмен мультимедийным содержанием (видео- и аудиоконференции, мгновенные сообщения, онлайн-игры). Допускается добавление или удаление каналов в течение установленного сеанса, а также подключение и отключение дополнительных клиентов (конференц-связь). По существу, SIP участвует только в сигнальной части сеанса связи. При передаче информации протокол SIP использует ряд других протоколов: SDP, RTP, SOAP, HTTP, XML, VXML, WSDL, UDDI и другие.

Главными недостатками протокола SIP являются трудности с обслуживанием приоритетных вызовов, что важно для военных применений, для экстренной службы, а также трудности по обеспечению секретности (особенно в условиях кибервойны). Поэтому по заказу МО США разработали защищенный протокол AS-SIP. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC. И сам протокол AS-SIP еще далек от совершенства: в версии AS-SIP, обнародованной в июле 2013 г. [7], было внесено более 50 исправлений по сравнению с исходной версией, подготовленной полугодом ранее.

В основе протокола AS-SIP лежит стандарт RFC 4542 [8], в котором изложена архитектура многоуровневого прерывания и приоритетов (Multi-Level Preemption and Precedence, MLPP). В соответствии с нуждами оборонного ведомства DoD и экстренных служб предусмотрены шесть классов приоритетов (в порядке убывания):

1) Высший приоритет (Flash Override Override) имеют: главнокомандующий, министр обороны, начальник Объединенного комитета начальников штабов, высшие командиры (в состоянии войны и/или по распоряжениям Президента). Эти вызовы не могут быть прерваны.

2) Flash Override: те же пользователи и по распоряжениям Президента в случае войны и в чрезвычайных ситуациях. Вызовы Flash Override не могут быть прерваны в сети DSN.

3) Flash: этот уровень резервирован для телефонных звонков, относящихся к командованию и контролю военных сил, к важным действиям разведки, для ведения дипломатических переговоров, гражданского оповещения о событиях важных для национального

выживания, выполнения федеральных государственных функций важных для национального выживания, важных функций обеспечения внутренней безопасности, сообщений о катастрофических событиях национального или международного значения.

4) Срочные вызовы (Immediate): пожоже на класс Flash, но несколько менее важные; для телефонных звонков, относящихся к ситуациям, которые серьезно влияют на безопасность национальных и союзных войск, восстановление сил в период после атаки, менее важные данные разведки, проведение дипломатических переговоров по сокращению или ограничению угрозы войны, реализация федеральных государственных действий, необходимых для национального выживания, ситуации, которые серьезно влияют на внутреннюю безопасность государства, действия гражданской обороны, стихийные бедствия или события обширной серьезности, имеющие непосредственное и пагубное влияние на благосостояние населения, важная информация, что непосредственное влияет на самолеты, космические аппараты, пуск ракет.

5) Приоритет (Priority): для телефонных звонков, требующих оперативного действия для проведения государственных операций.

6) Обычные звонки (Routine): для официальной правительственнойе связи без требований прерывания ведущихся разговоров.

Для предоставления связи с учетом класса приоритета в протоколе AS-SIP сформулированы четкие правила прерывания и ожидания прерванных разговоров.

III. Сеть DISN и потребности военного ведомства

Информационная сеть DISN должна обслуживать гигантское хозяйство оборонного ведомства США и сил НАТО по всему миру (рис. 4). На это тратятся большие и очень большие деньги - общий бюджет только IT систем составляет 40 мрлд. долл. в 2014 г., в том числе 17,4 мрлд. долл. на развитие информационной инффраструктуры и 4,7 мрлд. долл. на создание системы кибербезопасности [1].

В 2004 году начались работы по расширению пропускной способности глобальной информационной сети (Global Information Grid Bandwidth Expansion, GIG-BE). Суть работ состояла в установке устройств DWDM – новой технологии использования стекловолоконных кабелей, и в этом году были модернизированы первые шесть участков сети GIG-BE. К концу 2005 года переоборудовали 87 участков, выбранных Генштабом на территории США и вне ее. Построенная сеть GIG-BE обеспечивает надежную оптическую наземную связь для высокоскоростной передачи несекретных IP сообщений по всему миру. Средствами DWDM был реализован принцип DoD "свой цвет каждой базе". Каждый узел на сети имеет аппаратуру OC-192 (10 Гбит в секунду). Конечная (будущая) цель проекта GIG-BE – довести пропускную способность GIG до 100 Гбит в секунду.

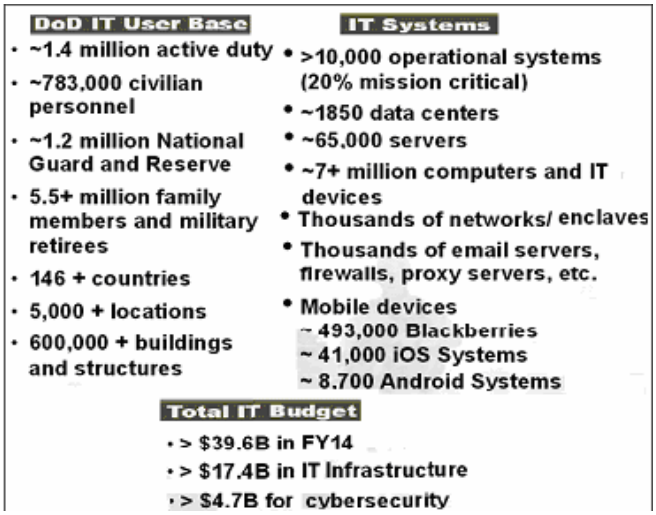

Рис. 4. Общая характеристика оборонного ведомства DoD (2014).

Программа GIG-BE является одним дорогостоящим, но довольно простым шагом к переходу DISN на сплошную IP технологию из-конца-в-конец. Контракт на работы по GIG-BE стоимостью в 877 млн. долл. в 2001 году выиграла компания SAIC (Science Applications International Corporation), а саму работу SAIC немедленно распределила по субконтракторам:

- Ciena Corporation строила оптической транспортной сегмент стоимостью 200- 300 млн. долл.
- Sycamore Networks – оптические кросс-коннекторы стоимостью 100- 150 млн. долл.
- Cisco Systems – мультисервисные платформы стоимостью 150- 200 млн. долл.
- Juniper Networks – базовые IP-маршрутизаторы часть стоимостью 150- 200 млн. долл.
- By Light – установка и обслуживание сети GIG-BE стоимостью 100- 150 млн. долл.

Проведение работ по контракту GIG-BE сопровождалось коррупционными скандалами, особенно по части компании By Light, которую создали отставные военные непосредственно к началу работ (по данным Wikipedia).

Следующим крупным шагом в развертывании DISN была установка коммутаторов MFSS и софсвичей WAN (Wide Area Network SoftSwitch), разработанных компанией Cisco Systems [9, 10]. На рис. 5 указаны места расположения 22 программных коммутаторов, а также четырех глобальных центров поддержки сетевых операций (Global NetOps Support Center, GNSC), установленные ранее. Миссия GNSC заключается в планировании сети и ежедневном слежения за работой GIG, особенно – за кибербезопасностью. Программные коммутаторы приходят на смену электронным АТС (по мере их вывода из эксплуатации).

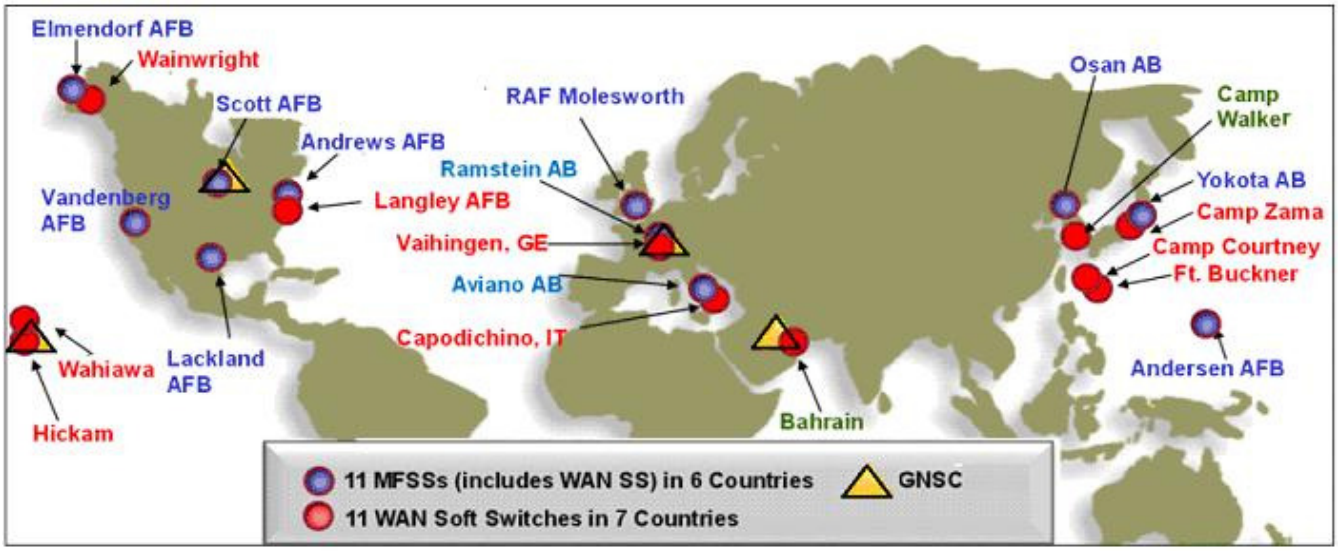

Рис. 5. Размещение 22 программных коммутаторов на сети DISN MFS

К 2016 г. планировалось довести новые узли MFSS до функциональности, представленной на рис. 3 справа, но задержка с работами по киберзащите эти сроки может сдвинуть.

Естественно, что сеть DISN развивается в соответствии с потребностями военного ведомства США и сил НАТО, поэтому полезно напомнить карту военных баз (рис. 6).

Рис. 6. Военные базы НАТО [11].

I. IV. Основная задача DISN – унификация информационных услуг UC

В будущей сети DISN все услуги (голос, видео и данные) должны предоставляться по IP протоколу. Воспользуемся новейшими методическими материалами по GIG (от 2013 г.), которые относятся к базовой архитектуре унифицированных сервисов (Unified Capabilities Reference Architecture) [3]. 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. Сетевая архитектура унифицированных сервисов основана на широкополосной IP сети (wide area IP backbone network) и на протоколе MPLS (multiprotocol label switching protocol), который обеспечивает требуемое качество связи QoS в сети коммутации пакетов.

Кроме рассмотренного выше протокола AS-SIP, для предоставления услуг UC используется протокол XMPP (UC Extensible Messaging and Presence Protocol), который обеспечивает сервисы Instant Messaging (IM), Chat и

Presence по требованиям DoD. На основе унифицированных сервисов (Unified Capabilities) реального времени предлагается создать восемь услуг связи (Таблица 1).

Таблица 1. Основные услуги GIG [3].

Услуги связи	Описание
Email and Calendaring	Обеспечивает передачу сообщений с указанием приоритета, условий доставки, цифрофой подписи и криптоключей. Календарь позволяет планировать расписание встреч.
Instant Messaging and Chat	Обеспечивает обмен сообщениями в реальном времени. Чат отличается от Instant Messaging групповым общением в специальном чат-пространстве.
Rich Presence	Позволяет устанавливать контакты на базе разнообразной информации о доступности в данный момент времени (IM, телефон, мобильные устройства).
Unified Messaging	Обеспечивает доступ к голосовой почте через e-mail или доступ к e-mail через голосовую почту.
Video Conferencing	Обеспечивает общение многих пользователей средствами видеоконференции.
Voice and Video (Point-to-Point)	Обеспечивает двух пользователей средствами общения посредством голоса и видео с возможностью дополнительных сервисов голосовой почты, переадресации вызова, подключения телефонистки и местной справочной службы.
Voice Conferencing	Обеспечивает организацию голосовой конференции многих пользователей.
Web Conferencing and Web Collaboration	На основе web страницы обеспечивает многих пользователей средствами общения голосом, по видео и передачей данных.

В предоставлении унифицированных услуг UC на сети DISN участвуют три сегмента (рис. 7): сегмент доступа (Customer Edge, CE), пограничный сетевой сегмент (Network Edge) и базовый сетевой сегмент (Core Segment). Сегмент CE включает оконечные устройства, локальные сети ASLAN или Non ASLAN, магистральные сети (Metropolitan Area Network, MAN), маршрутизаторы SBC и граничные усройства CE-R, которые подключаются к маршрутизаторам аггрегации (Aggregation Router, AR). Пограничный сетевой сегмент (Network Edge) в простейшем случае реализуется средствами Ethernet (100Base-T или 1000Base-T). Базовый сетевой сегмент (Core Segment) предоставляет транспортные IP услуги и состоит из высокоскоростных оптических линий.

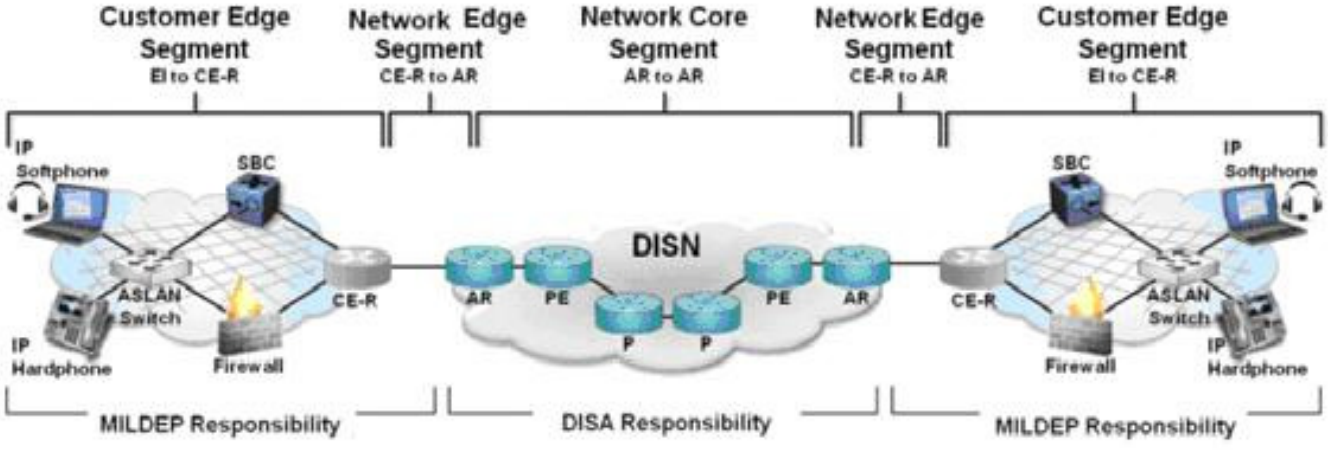

Рис. 7. Инфраструктура UC состоит из трех основных сегментов: CE, NE и DISN Core [12].

V. Целевая инфраструктура DISN

На рис. 8 показана целевая архитектура сети DISN. Она содержит два уровня: Tier 0 и Tier 1 [12]. Для бесперебойной работы сети DISN софтсвичи MFSS объединены в кластеры: каждый кластер Tier 0 содержит три софтсвича уровня Tier 0. Они соединены протоколом ICCS (Intra-Cluster Communication Signaling), по которому автоматически обновляются их базы данных. Кластер по существу представляет один 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 1860 миль. На нижнем, втором уровне DISN сети Tier 1 находятся два типа локальных сетей: защищенная ASLAN по протоколу AS-SIP и традиционная LAN по протоколу H.323.

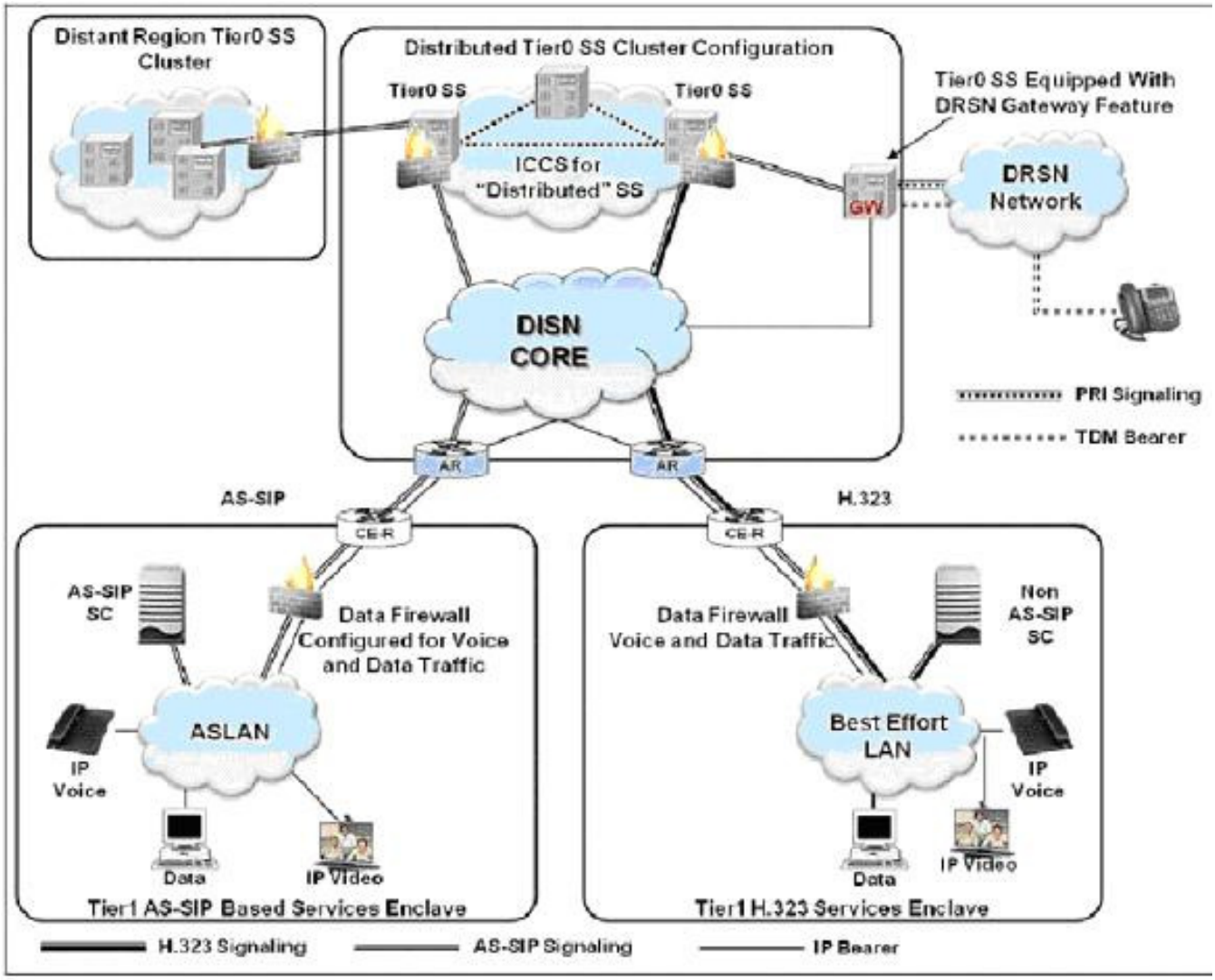

Рис. 8. Защищенная гибридная сеть DISN для передачи голоса и видео по протоколу IP (Voice and Video over Internet protocol, CVVoIP).

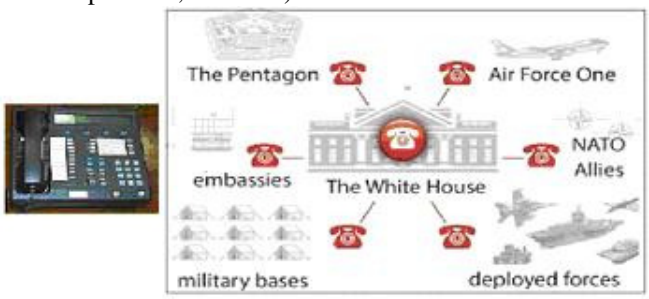

Рис. 9. Сеть DRSN: слева – телефон правительственной связи Red Phone, справа – основные абоненты DRSN.

Своеобразным «родимым пятном» на сети DISN, строящейся по единому протоколу AS-SIP, является сверхсекретная правительсвенная связь DRSN (Defense RED Switched Network), которая вопреки желанию идеологов DISN сохраняет имеющуюся технологию коммутации каналов, точнее, ISDN каналы. Сеть DRSN — это выделенная телефонная сеть, которая обеспечивает управление вооруженными силами США (рис. 9 справа). В текущих методических материалах по DISN [3] не предусмотрен перевод сети DRSN на коммутацию пакетов.

На рис. 9 слева показан т. наз. «красный телефон» (Secure Terminal Equipment, STE), который подключается к сети DRSN по ISDN линии и с использованием протоколов сигнализации ISDN PRI и CAS (Channel Associated Signaling). Red Phone работает на скорости 128 кб/с. Для передачи данных и факсимиле

встроен RS-232 порт. Вся криптографическая информация хранится на карте (щель для карты – на аппарате справа внизу). «Красные телефоны» общаются по протоколу SCIP (Secure Communications Interoperability Protocol). Это – межнациональный протокол сил НАТО для обеспечения закрытой передачи голоса и данных по множеству сетей: наземная телефонная сеть, радио военного назначения, спутниковая связь, интернет-телефония, разные стандарты мобильных сетей.

VI. Задачи обеспечения кибербезопасности сети DISN

Решение задач обеспечения кибербезопасности кардинально меняют все планы построения сети DISN. Иллюстрацией тому может служить наличие множества новых связей на рис. 10, которые следует установить по требованиям киберкомандования USCYBERCOM, созданного в 2010 году.

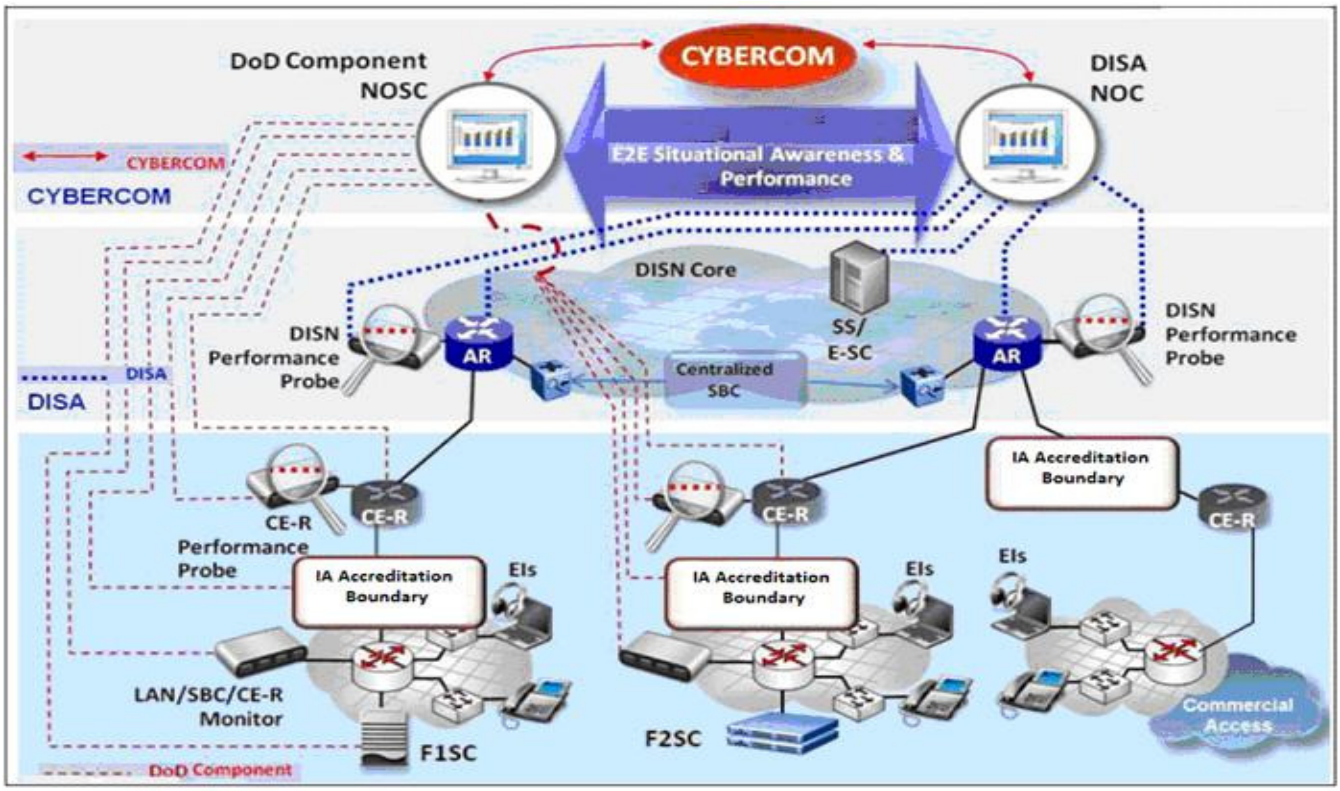

Рис. 10. Общий вид обеспечения безопасности услуг UC [12].

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.

Для обеспечения кибербезопасности услуг UC агентством DISA создана новая организация – Исследовательский центр кибербезопасности, в которой основными являются пять отделов (на рис. 11 выделены красным) [13]:

1) Отдел инфраструктуры программного обеспечения (Infrastructure Software Services Division) занимается облачными вычислениями. Этот отдел отвечает за собственное облако агентства DISA и облако milCloud.

2) Отдел кибербезопасности (Cyber Security Division) изучает средства безопасности нового поколения, особенно в связи с внешними облачными инфраструктурами. Этот отдел активно сотрудничает с платформой - DISA's big data analytics platform.

3) Отдел осведомленности о киберситуации (Cyber Situational Awareness and Analytics Division) следит за киберугрозами в сетях DoD, выявляет уязвимости в сетях Министерства обороны.

4) Наиболее активным является Отдел, обеспечивающий установку региональных стеков безопасности (Joint Regional Security Stacks (JRSS) Program). Эта программа является важнейшей частью по созданию единой информационной среды (Joint Information Environment).

5) Особо строгому контролю подвержены средства военной мобильной связи, за это отвечает Отдел Mobility Portfolio Management Office.

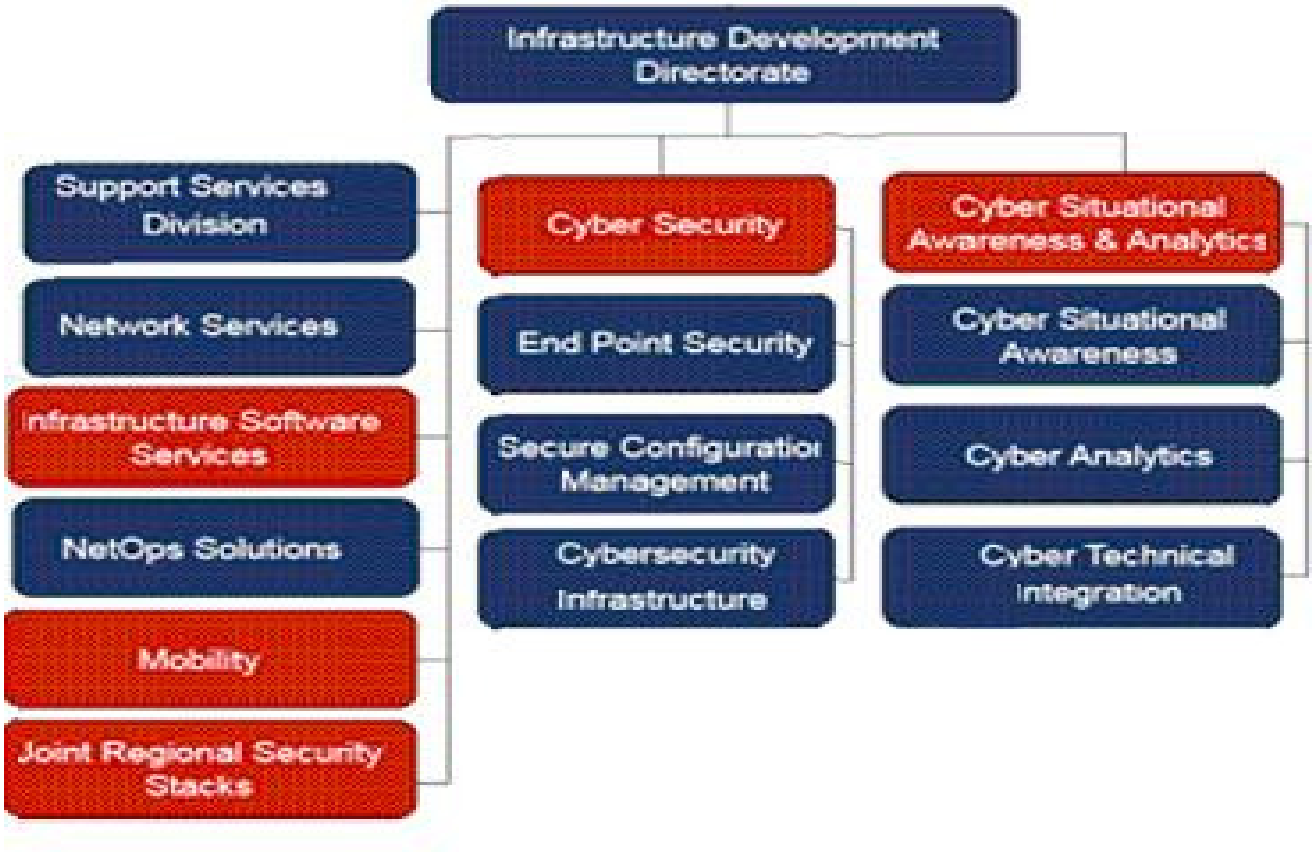

Рис. 11. Структура Исследовательского центра кибербезопасности.

Основная задача нового центра состоит в обеспечении кибербезопасности Единой информационной среды Пентагона (Joint Information Environment, JIE) 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).

Сама концепция Единой информационной среды JIE является чрезвычайно сложной, а требования кибербезопасности, как видно на рис. 10, 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.

VII Первые результаты по киберзащите

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 [14].

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.

В 2013 году команда GSM-O приступила к изучению состояния четыре центров управления сетью GIG, которые несут ответственность за техническое обслуживание и бесперебойную работу всех компьютерных сетей Пентагона – 8100 компьютерных систем в более чем 460 местах в мире, которые, в свою очередь, соединены 46000 кабелями. Первое дело по контракту состояло в модернизации системы управления компьютерными сетями GIG. Было принято решение о консолидации операционных центров – с четырех до двух. Расширяются центры на военно-воздушных базах Scott (штат Иллинойс) и Hickam на Гавайях, а центры в Бахрейне и Германии закрываются.

Следующее дело – решение основной задачи Исследовательского центра кибербезопасности, т.е. создание единой архитектуры безопасности SSA. С этой целью следует установить региональные стеки безопасности JRSS, которые, по сути, представляют собой IP маршрутизаторы со сложным комплексом программ киберзащиты (рис. 12).

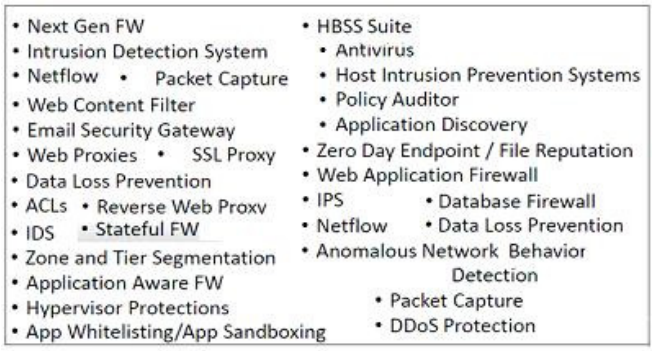

Рис. 12. Средства киберзащиты в сети SIPRNet в соответствии с единой архитектурой безопасности SSA [15].

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 (рис. 13).

Рис. 13. Состояние работ по установке стеков JRSS (2014) [16].

Общий объем работ включает установку 24 стеков JRSS на служебной сети NIPRNet и 25 стеков JRSS на секретной сети SIPRNet (рис. 14). К 2019 году планируется на эти стеки перенести программы кибербезопасности, которые сейчас размещены в более чем 400 местах.

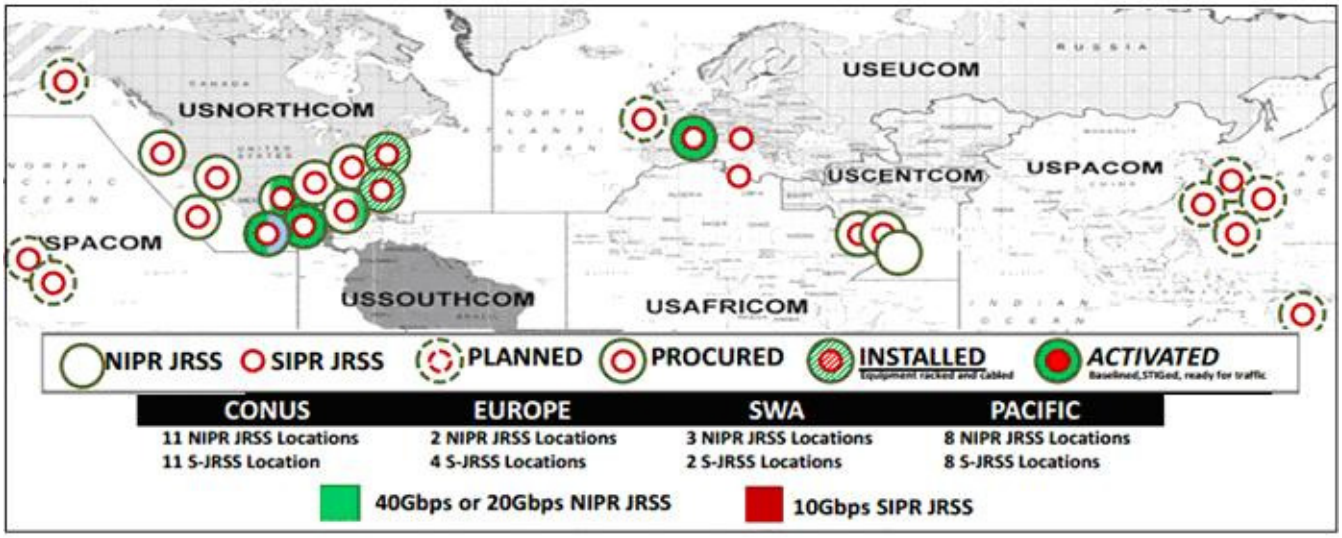

Рис. 14. Карта установки стеков JRSS [17].

Состояние дел по контракту GSM-O на 2014 год хорошо изложено в статье [18]. С момента объявления плана GSM-O около года назад представители трех организаций – агентства DISA, армии и ВВС работали совместно по установке стеков JRSS. Первый JRSS, установленный на военной базе Сан-Антонио, позволил увеличить пропускную способность маршрутизаторов сети MPLS (Multi-Protocol Label Switching) и взять на себя трафик от базы Fort Sam в Хьюстоне и авиационной базы Lackland. Планируется установка новых MPLS маршрутизаторы в более чем 100 местах в течение 2015 года.

На очереди стоят работы по соданию общих датацентров (DISA Core Data Centers, CDCs) с перемещением туда задач, выполняемых существующими датацентрами армии и ВВС. Пока отстают работы по внедрению унифицированных сервисов (Unified Capabilities), что предполанает переход на IP коммуникации для передачи голоса, телеконференций и видео. Планы этих работ должны быть объявлены в 2015 году.

Наиболее сложный раздел работ – проблемы обеспечения кибербезопасности (рис. 12). Задачи кибербезопасности являются высшим приоритетом Пентагона, но отсутствие необходимых стандартов тормозит выполнение всей программы GSM-O, прежде всего, тормозит создание общих датацентров CDC и внедрение унифицированных сервисов (Unified Capabilities). Остаются также нерешенными задачи использования облаков военного ведомства и перенос какой-то части приложений на коммерческие облака.

VIII. Заключение. Задачи для России

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.

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. Состояние разработки системы 112 описано в статьях [19-22].

В официальном отчете Минкомсвязи России [23] перечислены задачи, не решенные к настоящему времени: «Ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей связи общего пользования (ССОП) для прохождения вызовов, поступающих в службу по номеру 112. Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений». Это означает, что данный системный проект до сих пор не готов, а все проведенные работы следует рассматривать как экспериментальные образцы.

Импортозамещение предполагает развитие сетей связи собственными силами, еще больше – это предполагает восстановление промышленности средств связи. К сожалению, за боее 20 лет капиталистического строительства растеряны кадры и знания. Поэтому, на наш взгляд, следует вернуться к состоянию знаний, достигнутому лет 20 назад, и развивать их далее. В данном случае такой точкой отсчета можно условно назвать систему ОКС-7. В России отставание от 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 ускоренными темпами продолжить движение вперед.

Сеть «Ростелекома», по-видимому, будет мигрировать к архитектуре NGN. Поэтому важно рассмотреть, как традиционная сеть коммутации каналов и сигнализация SS7 будут «уживаться» с сетью NGN, где будет главенствовать протокол SIP. Наибольшие усилия по стыковке сигнализации SS7 и интеллектуальной сети с протоколом SIP и узлом IMS (IP Multimedia Subsystem) проведены компанией Telcordia (США) [24]. Напомним, что Telcordia выступала продолжателем работ Bell Labs по интеллектуальным сетям. В начале 1990-х Telcordia разработала архитектуру AIN. Дальнейшие варианты сети объединяются группой документов AINGR Family of Requirements, FR-15. Эти документы подводят итог 20-летней работы по развитию концепции AIN в условиях наступления IP-технологии, точнее SIP-протокола, а также фиксируют требования экстренных вызовов E9-1-1 в архитектуре AIN. Эти документы могут служить основой для совершенствования российской интеллектуальной сети, чтобы на ее базе строить систему 112.

Важно также отметить, что существует бесспорная аналогия между экстренной службой NG9-1-1, которую строит министерство транспорта США, с одной стороны, и инфокоммуникационной сетью GIG, создаваемой министерством обороны, с другой. Но как воспользоваться этой аналогией? И если таковая есть, то как совместить планы разработки этих двух систем многомиллиардной стоимости?

Сошлемся на материалы Конференции по внутренней безопасности США (Homeland Security). Автор одной из статей [25] напоминает, что оба проекта были объявлены практически одновременно – в 2007 г. Аналогии начинаются с высокого уровня архитектуры сетей NG9-1-1 и GIG. Обе архитектуры предполагают сбор информации от множества источников и передачу ее множеству пользователей. И, что важно, обе системы требуют высокой живучести. Необходимо передавать голос, данные и видео и с минимальной задержкой.

Применения также сопоставимы. Самым сложным применением оказывается передача данных. Например, согласно концепции NG9-1-1, больной вызывает скорую помощь текстовым сообщением. Это сообщение достигает центра обслуживания вызовов, оператор которого, используя сообщение, определяет местоположение больного, сообщает об этом скорой помощи и посылает подтверждение больному. Данные о местоположении передаются компьютеру и наносятся на карту.

В GIG-архитектуре имеем похожую картину передачи и обработки данных. Данные могут быть любого типа, включая текст, файлы, снимки. Каждый военнослужащий должен быть доступен для обмена информацией. Например, если солдат обнаружил бункер, но не может распознать тип вооружения в нем, он передает картинку аналитику вооружения. Аналитик отвечает, а также может вызвать бомбардировщик 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? Какие выводы из анализа NG9-1-1 и GIG могут сделать для себя российские разработчики? Используя аналогию между NG9-1-1 и GIG, следовало бы рассмотреть создание единой сети не только для системы 112, но и для МЧС и МО.

Библиография

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

[2] Department of Defense Unified Capabilities Requirements 2013 (UCR 2013), January 2013, 916 стр.

[3] U.S. Army Unified Capabilities (UC) Reference Architecture (RA) Version 1.0, 11 October 2013, 295 стр.

[4] http://www.disa.mil/Network-Services/Data Retrieved 2016-02-05

[5] М. А. Шнепс-Шнеппе, Д.Е. Намиот Телекоммуникации для военных нужд: от сети GIG1 к сети GIG2 //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 9. – С. 9-17.

[6] М. А. Шнепс-Шнеппе, Д.Е. Намиот, Ю.В. Цикунов Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 10. – С. 3-13.
[7] Department of Defense Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1.
[8] F. Baker J. Polk (Cisco Systems) Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite, RFC 4542, May 2006.
[9] Department of Defense. Unified Capabilities Master Plan. October 2011.
[10] Cisco LSC https://www.cisco.com/web/strategy/docs/gov/Cisco_LSC_Overview_Jan2011.pdf
[11] Ю. Жеглов Реконфигурация военного присутствия США за рубежом (2007) http://pentagonus.ru/publ/3-1-0-45
[12] Department of Defense Unified Capabilities Framework 2013 (UC Framework 2013). January 2013.
[13] L. McCoy Jr Five cybersecurity hotspots in a reorganized DISA, Apr 23, 2015. https://washingtontechnology.com/articles/2015/04/23/insights-mccoy-cyber-hotspots.aspx
[14] GIG-a-Bite: Lockheed Takes $4.6 Billion Contract from SAIC http://www.defenseindustrydaily.com/gig-a-bite-lockheed-takes-46-contract-from-saic-07452/
[15] D. Metz Joint Information Environment Single Security Architecture (JIE SSA), 12 May 2014.
[16] The JRSS program is underway, Oct. 1, 2014 http://archive.c4isrnet.com/article/20141001/C4ISRNET12/310010005/The-JRSS-program-underway
[17] W. Welsh New tools ahead for DOD's global grid, Sep 14, 2015 https://gcn.com/articles/2015/09/14/dod-global-information-grid.aspx
[18] S. Meloni The Future of the Joint Information Environment (JIE), SEPT 24, 2014 http://blog.immixgroup.com/2014/09/24/the-future-of-the-joint-information-environment-jie/
[19] Е.И. Полканов, И.Г. Мазин Совместное использование информационных ресурсов: консолидация развития сетей// Электросвязь, 2012, №3.
[20] М. А. Шнепс-Шнеппе Телекоммуникации для экстренных и военных нужд: параллели //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 7. – С. 25-36.
[21] М.А. Шнепс-Шнеппе Разработка системы 112 в условиях импортозамещения// Электросвязь, №4, 2015, с. 40-44.
[22] Система-112. http://www.sphaera.ru/index.php/solutions/s112
[23] Что мешает внедрению «Службы 112» // ИКС. – 2013. № 11. – С. 15.
[24] Telcordia Roadmap to Advanced Intelligent Network (AIN) Documents, Issue 2, August 2008.
[25] M. Schmitt Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE International Conference on Technologies for Homeland Security. May 2008.

On DISN evolution under cybersecurity needs

Manfred Sneps-Sneppe

Abstract— **This paper discusses the difficulties of transition from circuit switching to packet switching using as an example of an information network GIG US Department of Defense - the world's largest private network. The article describes the properties of multifunctional MFSS softswitch as the foundations of the transition from TDM to IP, standardization of information services and the target communication network infrastructure DISN. We target in detail the issues of cybersecurity DISN network. The conclusion provides the tasks for Russian signalers to create systems and telecommunication network 112 for Civil Defence.**

Keywords— **switching channels; packet switching; multifunctional Softswitch; DISN; import substitution; 112 system.**