Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны

Шнепс-Шнеппе М.А., Намиот Д.Е., Цикунов Ю.В.

***Аннотация* — Статья посвящена рассмотрению планов развития сети связи министерства обороны США. Это крупнейшая в мире ведомственная сеть. Естественно, что опыт развития такой сети является очень ценным для всех, причастных к развитию сетей связи. В статье собраны и проанализированы представленные и доступные для исследователей планы развития Глобальной Информационной сети (GIG), перечислены все ее определяющие программы. Основное внимание уделено вопросам так называемой кибервойны и обеспечению информационной безопасности.**

***Ключевые слова* — GIG, кибервойна, телекоммуникационная сеть, пакетные технологии, сеть специального назначения.**

I. Введение

В настоящей статье рассмотрим новейшие тенденции развития Глобальной информационной сети Пентагона – GIG (Global Information Grid) в связи с требованиями условий кибервойны.

В 2006 г. Пентагон объявил необходимость модернизации информационной сети GIG [1]. Были выявлены недостатки существующей сети GIG:

- Множество сетей с различным оборудованием,
- Несогласованные решения по обеспечению секретности,
- Несогласованные программы по ведению боевых операций в разных родах войск,
- Различия в информационных базах.

Были сформулированы задачи, которые подлежат решению в новом поколении сети GIG 2.0 [2].

Один существенный недостаток сети GIG иллюстрирует рис. 1. В настоящее время основным связывающим звеном сети GIG между серверами вне театра боевых действий и участниками боевых действий является спутниковая группировка, которая не справляется с передачей данных в условиях боевых действий:

- Солдатам недоступны новейшие разведданные,
- Дроны собирают данные, которыми не в силах воспользоваться командиры тактических операций,
- Корабли не в силах взаимодействовать с наземными частями,
- В итоге – штаб, развернутый на театре боевых действий, не в силах синтезировать общую картину боевой операции.

Сейчас наступил следующий этап модернизации GIG – GIG-3.0 [4], что мы и будем обсуждать.

В целом развитие сети GIG определяют шесть ключевых программ [5], что иллюстрирует рис 2.

Программа 1: формирование наземного компонента GIG. Это – глобальная система наземных ВОЛС (волоконно-оптических линий связи), получившая название DISN-Core.

Программа 2: формирование космического сегмента GIG. Эта программа включает строительство перспективной объединенной системы спутниковой связи, базовыми компонентами которой станут пять группировок космических аппаратов связи. Основными ныне действующими являются две группировки: 1) AEHF (Advanced Extremely High Frequency), это - аппаратура связи миллиметрового диапазона способна передавать информацию со скоростью до 8,2 Мбит/с, и 2) MUOS (Mobile User Objective System). Система MUOS создается с применением технологий гражданской спутниковой связи и ориентирована на применение единых пользовательских терминалов проекта JTRS (Joint Tactical Radio Systems). К 2030 году планируется создать новую группировку космических аппаратов TSAT (Transformational Satellite). Группировка TSAT задумана для широкополосной спутниковой связи с использованием межспутниковых каналов лазерной связи, что позволит устранить недостаток сети GIG, который иллюстрирует рис. 1.

Программа 3: система телепортов. Телепорт объединяет наземный и космический сегменты GIG, является телекоммуникационным пунктом сбора и распределения информации, который обеспечивает боевые подразделения широкополосным, мультимедийным и глобальным доступом к DISN.

Программа 4: разработка тактического радиосегмента GIG. Программа предполагает разработку широкополосных радиостанций нового поколения, структура и функциональные возможности которых реализуются на программно-настраиваемых компонентах(SDR – Software Defined Radio) и удовлетворяет новым, повышенным требованиям АНБ США к системам шифрования сигналов.

Пятая программа предусматривает разработку унифицированного комплекса сетевых сервисов корпоративного информационного обслуживания NCES

Статья получена 7 сентября 2014.
Шнепс-Шнеппе М.А. - главный научный сотрудник ЦНИИС, д.т.н. email: sneps@mail.ru
Намиот Д.Е. – старший научный сотрудник МГУ имени М.В. Ломоносова, email: dnamiot@gmail.com
Цикунов Ю.В. – директор по развитию ЦНИИС, email: tsikunov@zniis.ru

(Net-Centric Enterprise Service). Комплекс предназначен для обеспечения любого пользователя, имеющего доступ к GIG, стандартным набором информационных услуг по своевременному и безопасному доступу к необходимой информации высокого качества. На данный момент эта программа является сложнейшей, тем более из-за новейших требований кибервойны.

Шестая программа: обеспечение информационной безопасности в GIG. Ее ключевым элементом является программа модернизации криптографических средств защиты СМР (Crypto Modernization Program), которая предполагает создание новых методов и способов засекречивания и защиты информационных ресурсов.

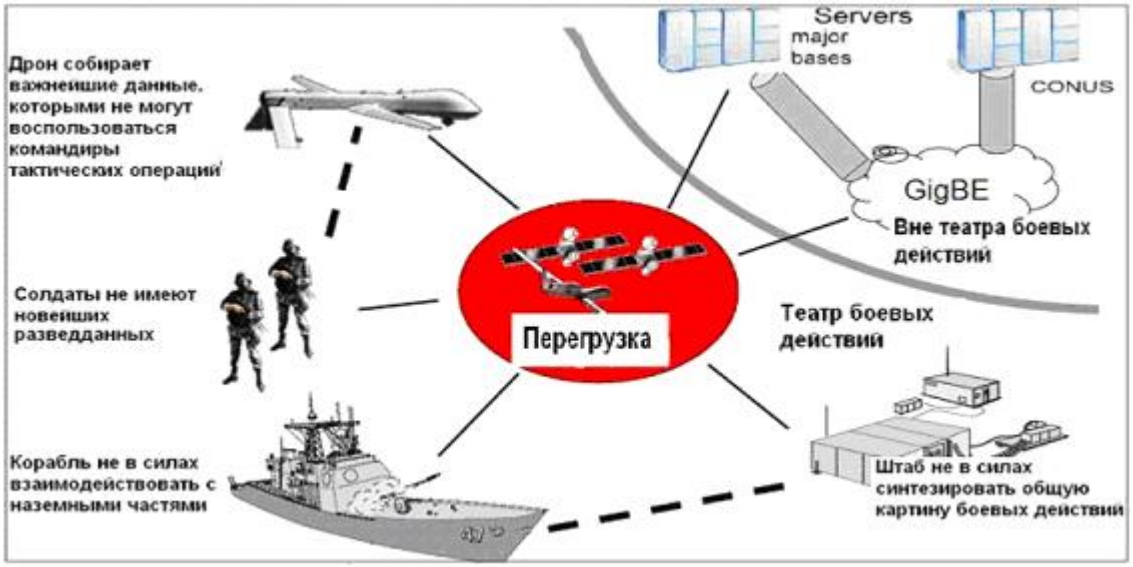

Рис. 1. Пропускная способность спутниковой группировки растет медленнее других частей сети GIG [3].

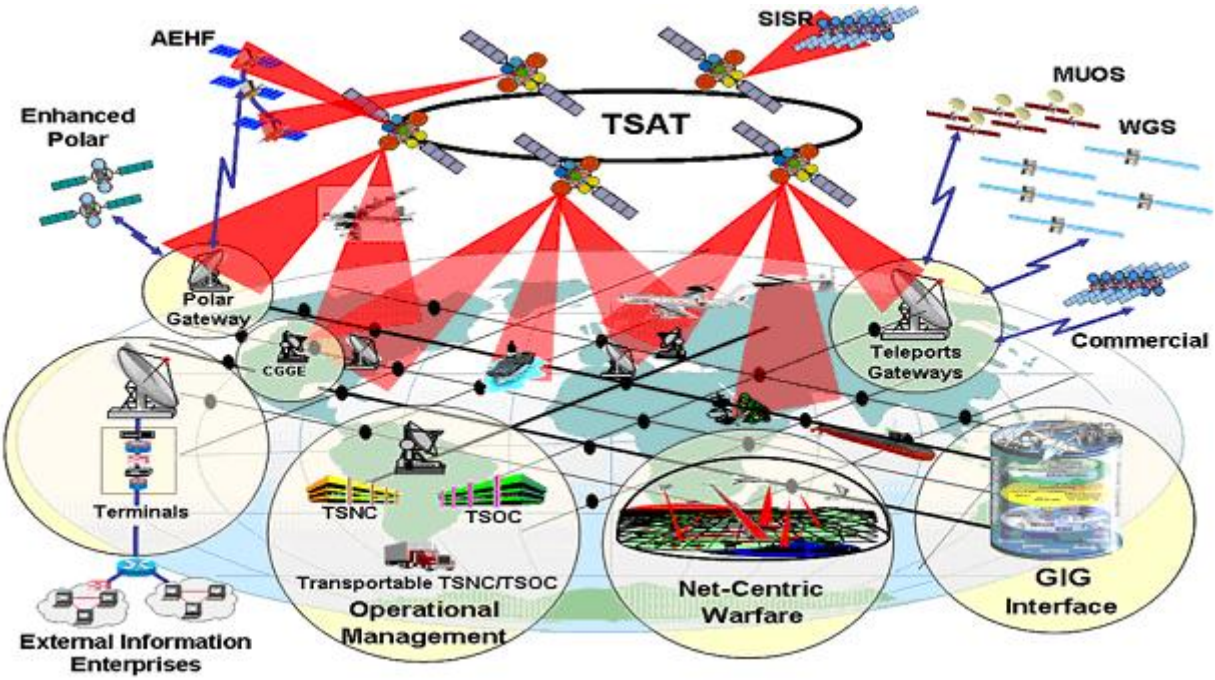

Рис. 2. Общая схема перспективной сети GIG [6].

Настоящая статья посвящена обсуждению шестой программы: рассмотрению информационной безопасности в сети GIG, образно говоря, вопросам кибервойны (рис. 3). Центральной задачей киберкомандования является охрана периметра театра боевых действий, точнее, интерфейсов шлюза DNDG (Dedicated Network Domain Gateway), который в действительности состоит из множества шлюзов по периметру театра боевых действий (Operational Network Domain) и множества других устройств внутри сети.

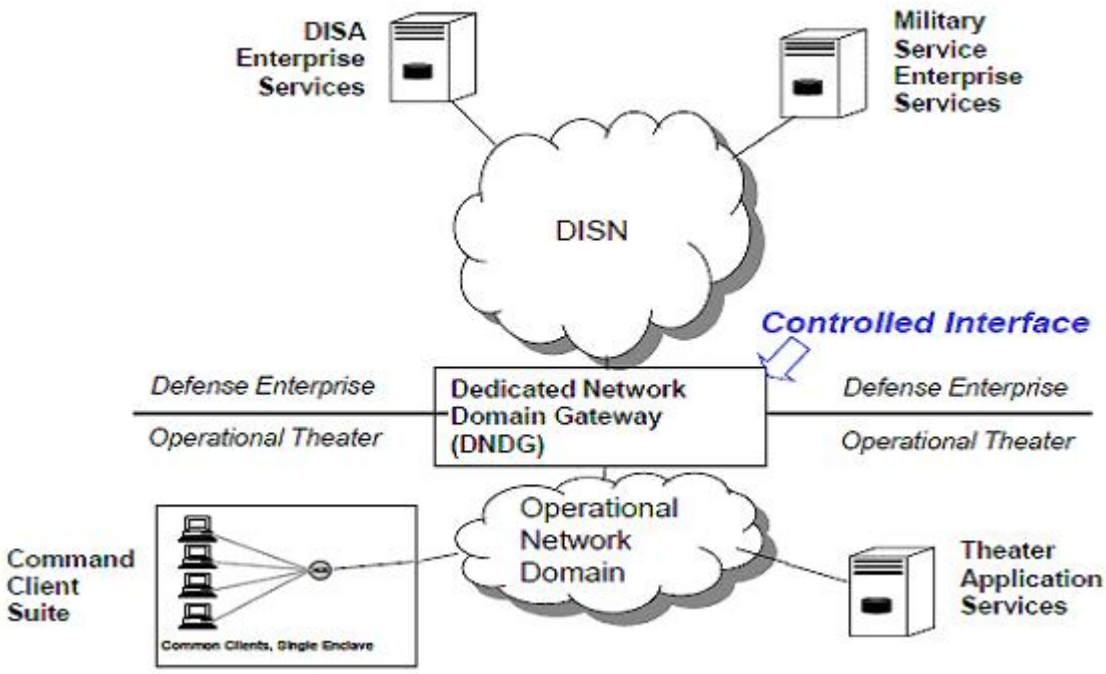

Рис. 3. Киберкомандование охраняет периметр театра боевых действий, т.е. контролирует интерфейсы шлюза DNDG [4].

Материалы данной статьи расширяют наше предыдущее описание телекоммуникаций для экстренных и военных нужд [7] [8].

II. Организация кибервойны в США

Министерство внутренней безопасности США

После террористических атак 11 сентября 2001 года в США приняли ряд мер по пресечению возможной террористической активности в будущем. Так как террористические атаки представляют угрозу для всего международного сообщества, необходимы четкие меры для противостояния терроризму. Для обеспечения должного уровня безопасности была создана принципиально новая структура, включившая в себя множество служб безопасности. Ее цель — достичь оптимального взаимодействия всех ведомств, предотвращать террористические акты и бороться с последствиями бедствий.

По свежей памяти о разрушении Всемирного торгового центра – 20 сентября 2001 года, в своей речи перед нацией и Конгрессом, президент США Джордж Буш заявил о создании нового ведомства для координации обеспечения национальной безопасности — Управления внутренней безопасности (Office of Homeland Security). Новое ведомство объединило более дюжины служб безопасности. 1 марта 2003 года Управление внутренней безопасности было преобразовано в Министерство внутренней безопасности (Department of Homeland Security, DHS). По состоянию на 2009 год число сотрудников — 225 тыс. человек, бюджет — 52 миллиарда долларов.

В структуру Министерства внутренней безопасности входят многочисленные агентства и офисы, многие из которых были созданы задолго до их интеграции с этой структурой:

- По части национальной безопасности: Береговая охрана, Иммиграционная и таможенная полиция США, Служба гражданства и иммиграции, Пограничная и таможенная охрана, Федеральное агентство по управлению в чрезвычайных ситуациях, Секретная служба США, Администрация безопасности на транспорте и другие;
- По части кибер-безопасности: Офис кибер-безопасности и коммуникаций, Система национальных коммуникаций, Национальное отделение кибер-безопасности, Офис защиты инфраструктуры и другие;
- По науке и технологиям – 9 отделов, в том числе по взрывчатым веществам.

В связи с расширением фронта работ по внутренней безопасности в США сегодня еще не ясно, как будут взаимодействовать три министерства, которые связаны с безопасностью страны (рис. 4):

- Министерство внутренней безопасности DHS,
- Министерство обороны DoD и
- Министерство транспорта DoT, куда входит служба экстренных вызовов NG9-1-1.

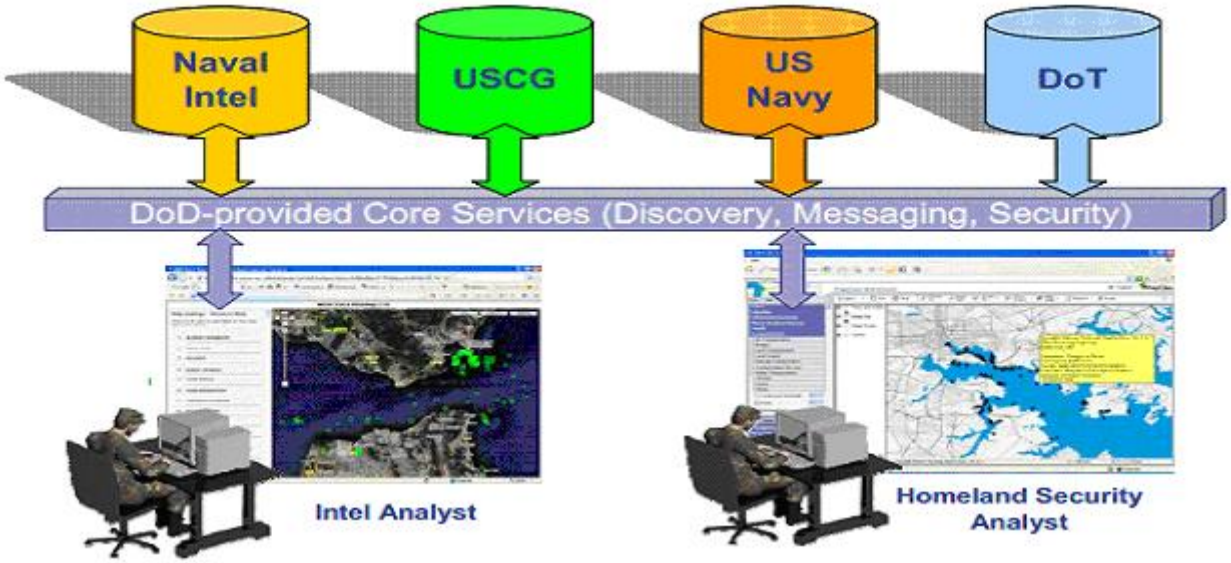

Рис. 4. Иллюстрация взаимодействия подразделений трех министерств – DoD, DHS и DoT: военной разведки со службой внутренней безопасности и экстренной службой.

Например, создается программа CAPTAIN (The Cyber and Physical Threat and Risk Analysis to Improve the NPSBN) [9], которая обеспечивает киберзащиту Национальной широкополосной сети NPSBN (Nationwide Public Safety Broadband Network). Согласно этой программе, DHS будет информировать о киберрисках многие организации, в том числе Службу первой помощи FirstNet (First Responder Network Authority) и Федеральную комиссию связи FCC (Federal Communications Commission).

Киберкомандование

В октябре 2010 года была создано киберкомандование, 2-я армия США (US Army Cyber Command/2nd Army). Это ведомство объединило в себе подразделения киберзащиты Пентагона и вошло в состав Агентства национальной безопасности. Планируется, что число военных и гражданских лиц армии достигнет 21 тыс. человек. Причем, согласно последним сообщениям, киберкомандование все больше стремится стать самостоятельным подразделением и постепенно обретает очертания отдельного рода войск. По замыслу, киберкомандование «планирует, координирует, интегрирует, синхронизирует и управляет сетевыми операциями и защитой армейских сетей». Для поддержки полномасштабных операций ведомство будет работать в киберпространстве и будет обеспечивать в сети GIG свободу действий силам США и союзников и лишать тавой возможности противника.

Киберкомандование сейчас входит в единое Стратегическое командование наравне со стратегическими ядерными силами, ПРО и космическими войсками. Этим признается, что киберпространство является таким же полем военных действий, как и сухопутное, морское и воздушное. Киберкомандование США будет ориентировано также на ведение наступательных операций [10], и для этого создано специальное подразделение боевых операций (Combat Mission).

По состоянию на август 2014 г. (со слов главнокомандующего кибервойсками и директора Агенства национальной безопасности адмирала Майка Роджерса [11]), к 2016 году Cybercom будет иметь 6000 высококвалифицированных сотрудников, образующих 133 команды, способные выполнять следующие три основные миссии:

- Национальные киберсилы, способные охранять критическую инфраструктуру и ключевые ресурсы страны,
- Боевые киберсилы, обеспечивающие киберзащитой боевых командиров по всему миру,
- Силы киберзащиты, охраняющие информационные сети Министерства обороны США.

Адмирал Роджерс подчеркнул важность запланированных учений по киберзащите всех служб страны, включая Министерство внутренней безопасности и ФБР.

III Криптография в ядре GIG

Оборонное ведомство DOD обсуждает две архитектуры обеспечения секретности в ядре GIG: полосатое ядро (striped core) и черное ядро (black core) [12]. Предполагается, что поток данных в ядре сети (DISN Core) охраняется протоколом Internet Protocol Security (IPSec) или подобными протоколами.

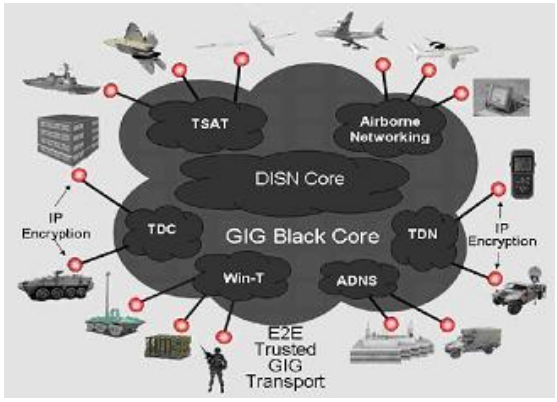

Рис. 5 Место черного ядра в сети GIG

В случае черного ядра (black core) все данные остаются в форме IPSec encrypted и в таком виде передаются через ядро. В случае полосатого ядра (striped core) данные дешифруются и повторно шифруются, проходя через каждый компонент сети. Между компонентами сети размещены шлюзы (red gateways), которые обеспечивают функцию дешифрования и повторного шифрования.

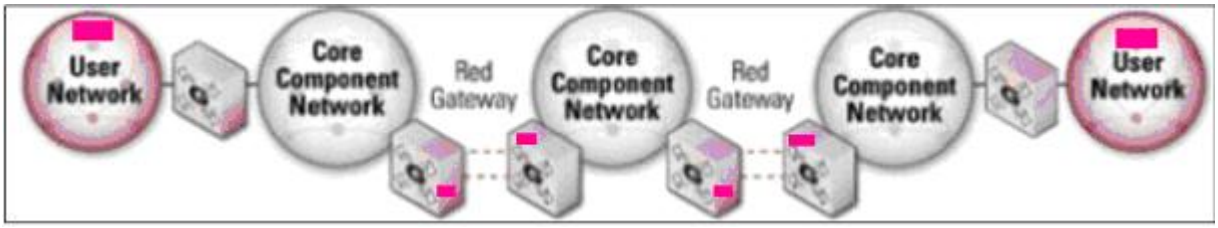

Рис.6. Упрощенная схема полосатого ядра (striped core).

В черном ядре (black core) все данные передаются через ядро в зашифрованном виде (IPSec encrypted), и все компоненты сети связаны напрямую. Здесь часто применяются узлы HAIPE (High Assurance Internet Protocol Encryptor). Например, в сети высшей секретности JWICS (Joint Worldwide Intelligence Communications System) узлы HAIPE размещаются для шифрования междугородных телефонных соединений на входе и выходе телефонной сети.

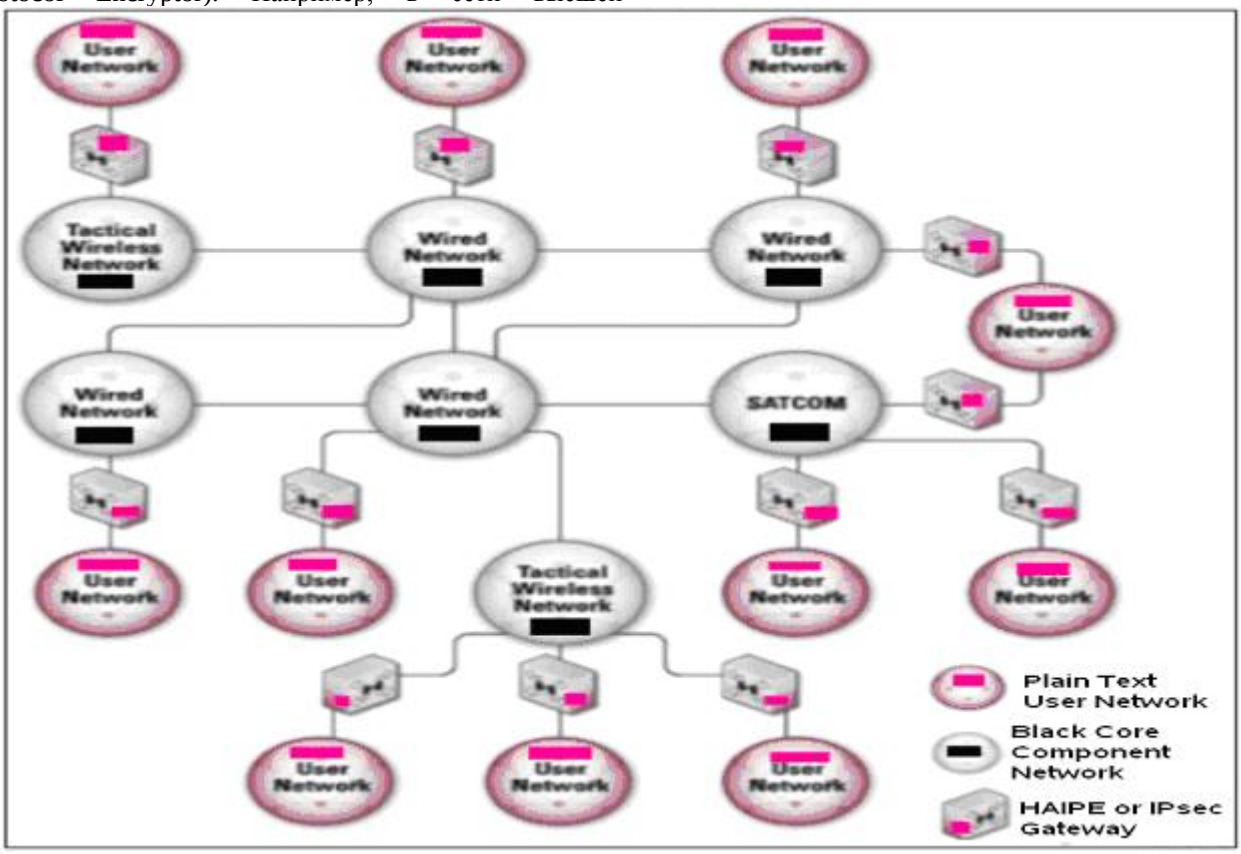

Рис. 7. Сеть GIG при наличии черного ядра.

В случае полосатого ядра схема шифрования становится сложнее. На схеме показан сравнительно простой случай – пользователи имеют только один уровень секретности. Если же уровней секретности несколько, то, соответственно, вместо одного узла приходится ставить несколько узлов шифрования-дешифрования, и сеть многократно усложняется.

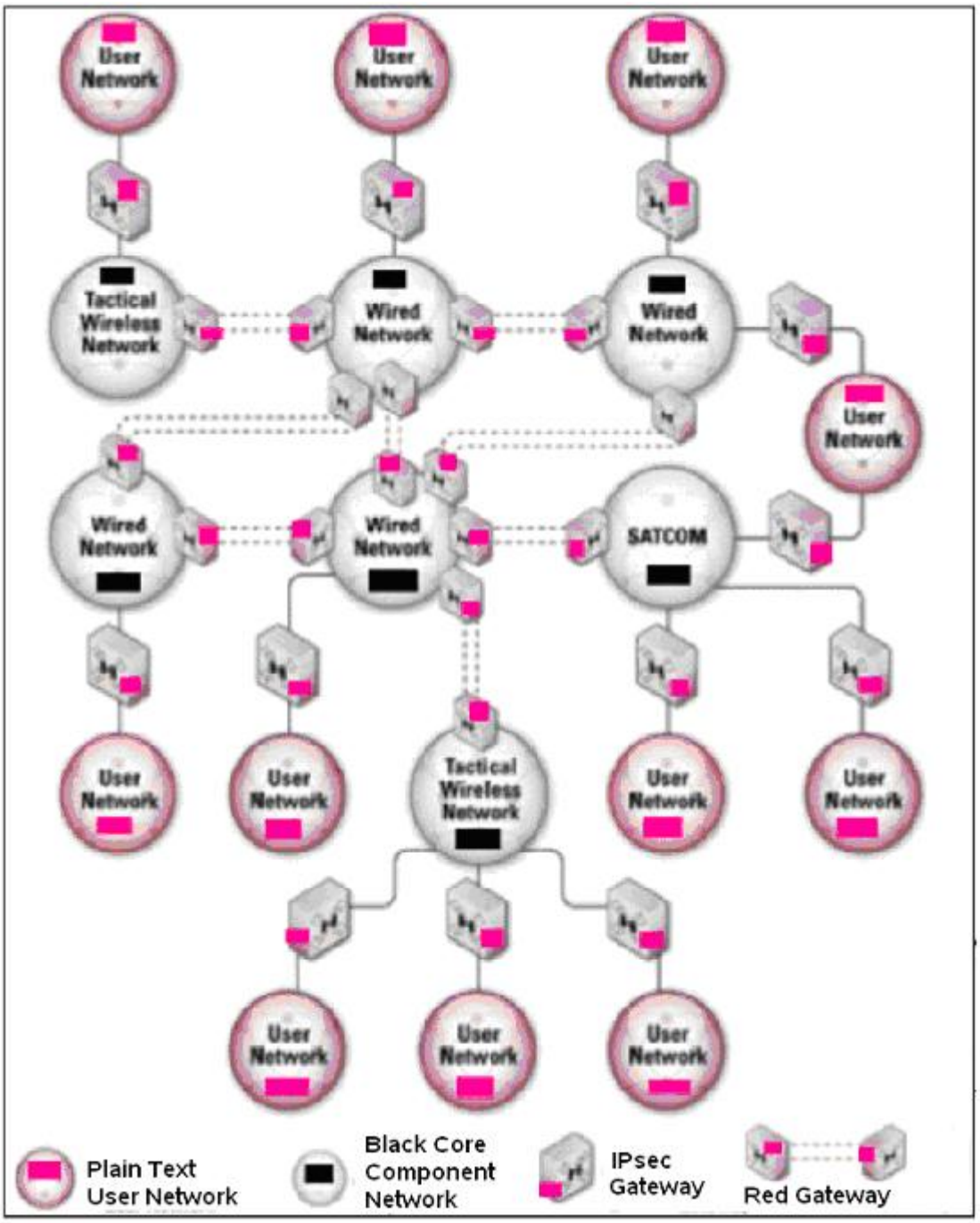

Рис. 8. Сеть GIG при наличии полосатого ядра

Представителям Пентагона предлагается выбрать одну из двух концепций криптографии в ядре GIG. Предлагается тщательно взвесить все аспекты (например, IPSec gateway discovery, routing и QoS). На данный момент (точнее, 2008) их мнение однозначно: вариант черного ядра предпочтительнее – в силу простоты реализации и экономичности, а главное – более безопасный, так как имеет меньшее число мест для злостного проникновения в сеть.

По свежим следам публикации изложенной версии Пентагона (2008) появилась статья [13] с указанием слабых мест выбора черного ядра как более предпочтительной версии построения сети GIG. Прежде всего, это сложности с обеспечением синхронных сеансов связи для передачи речи или видео через IP сеть. При наличии полосатого ядра данные многократно шифруются-дешифруются, при этом раскрываются заголовки пакетов (и адреса получателей), что уменьшает безопасность, но позволяет устанавливать приоритеты передачи. И еще – в случае перегрузки сети (например, во время боевых действий) сообщения командира должны иметь безусловный приоритет, что невозможно обеспечить в случае черного ядра.

Эту сложность понимают и в МО США: автор статьи ссылается на документ "Net-Centric Enterprise Solutions for Interoperability", опубликованный командованием морских сил (Navy's Space and Naval Warfare Command), в котором отмечается, что официальная версия DISA о предпочтении черного ядра еще не «повзрослела».

Еще большие проблемы связаны со спутниковой связью, где применяется шлюзы PEP (Performance Enhancing Proxy). Технология PEP связана с ускорением работы протокола TCP, точнее, с изменением данных заголовка TCP до и после линии спутниковой связи,

чтобы скрыть недопустимо большое время ожидания спутникового канала от TCP-сессии. Для работы PEP требуется раскрыть заголовок каждого пакета, что недопустимо в случае черного ядра.

IV. GIG-3: КОМПОНЕНТЫ СЕКРЕТНОЙ СЕТИ

Сеть GIG-3: содержит несколько секретных подсетей, каждая из которых образует свой анклав (Enclave). Пример устройства такого анклава показан на рис. 9.

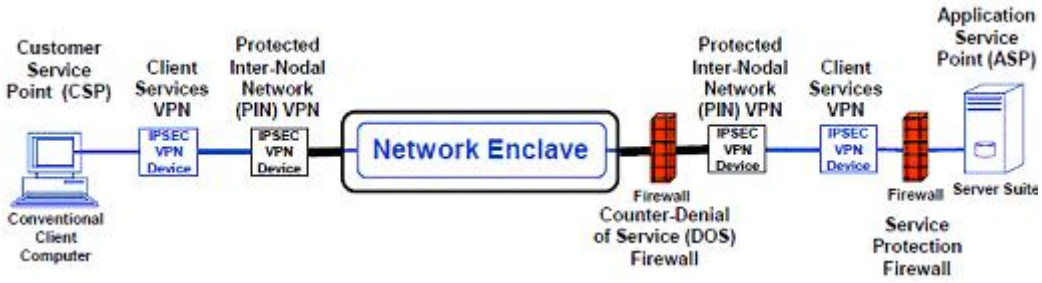

Рис. 9. Компоненты виртуального секретного анклава (Virtual Secure Enclave, VSE), работающего по протоколу IPSec [4].

Пояснения обозначений на рис. 9:

- Сетевой анклав (Network Enclave) содержит единый домен безопасности.
- Application Service Point (ASP) – это набор серверов приложений, относящихся к данному домену (например, сервисы Web, E-Mail и др.).
- Customer Service Point (CSP) – интерфейс пользователя к анклаву.
- Client Services VPN – виртуальная сеть клиента, защищенная сертифицированным IPSec шифрованием.
- Protected Internodal Network (PIN) VPN – блок защиты виртуальной сети VPN от опасностей внутри анклава.
- ASP Firewalls – браундмауэры от DOS атак и для защиты серверов приложений.

Каждый анклав имеет свой шлюз DNGW к Центру управления и безопасности (Network Operations & Security Center рис.10). Этот центр определяет риски каждого анклава и следит за качеством обслуживания (Quality of Service), предупреждая перегрузки сети и реализуя приоритеты обслуживания.

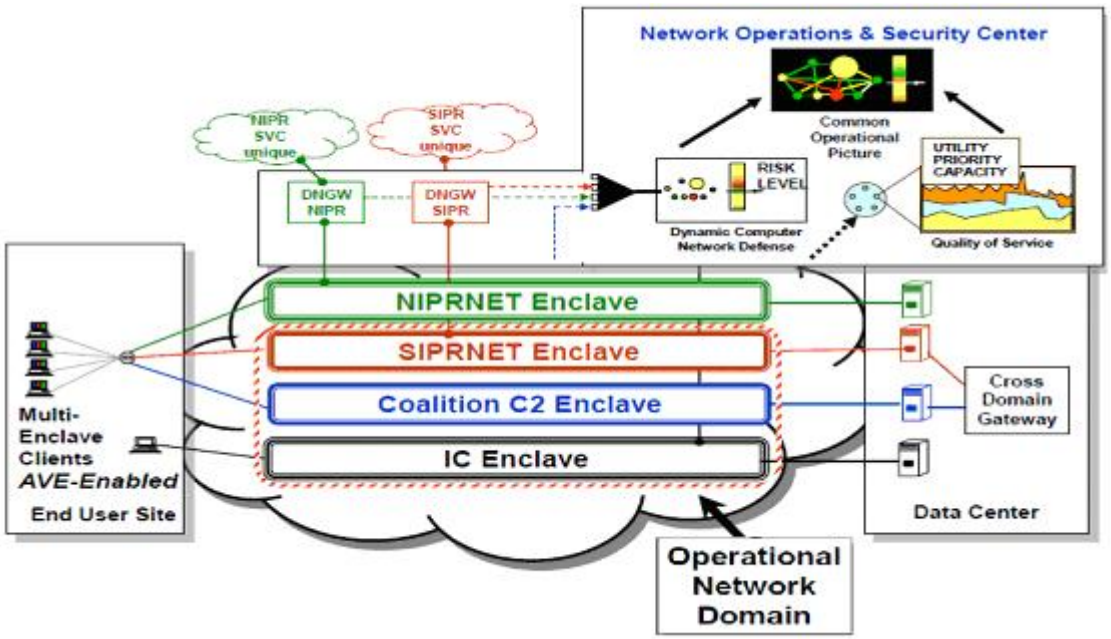

Рис. 10. Схема мониторинга и управления сетью на театре боевых действий (Operational Network Domain).

Условия работы в штабе боевой операции демонстрирует рис. 11: офицер является мультианклавным клиентом (Multi-Enclave Client). Ему доступны четыре секретные (Classified) сети , в том числе: объединённая глобальная сеть разведывательных коммуникаций (Joint Worldwide Intelligence Communications System , JWICS) — для передачи секретной информации по протоколам TCP/IP, виртуальный секретный анклав (VSE) и SIPRNet (Secret Internet Protocol Router Network) — система взаимосвязанных компьютерных сетей, используемых МО для передачи секретной информации по протоколам TCP/IP, а также две несекретные (Unclassified) сети: NIPRNet (Non-classified Internet Protocol Router Network) — сеть, используемая для обмена несекретной, но важной служебной информацией между «внутренними» пользователями и обычный Интернет.

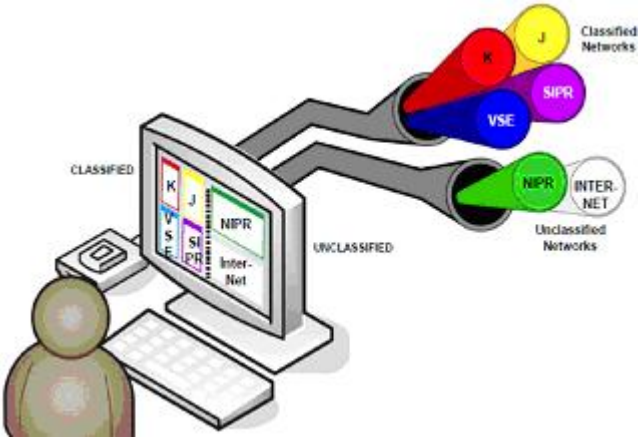

Рис.11. Мультианклавный терминал.

V.Пилотная зона GIG-3 в Южной Корее

В Южной Корее создается пилотная зона KOR для апробации решений GIG-3 на базе IP протокола (рис. 12).

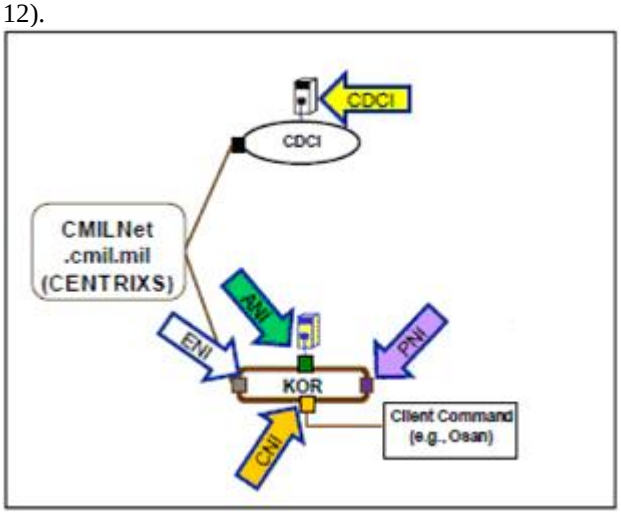

Рис. 12. Общий вид сети GIG-3 в Южной Корее [4].

Обозначения на рис. 12:

• ANI – Application Network Interface: маршрутизатор, который соединяет ASP с сетью,
• PNI – Partner Network Interface: фильтр высокой безопасности, который контролирует поток информации от сети партнера США (например, CENTRIXS) к ASP других партнеров (PNSP),
• CNI –Client Network Interface: содержит блок IPSec crypto виртуального секретного анклава (VSE), и маршрутизатор, который соединяет ASP с виртуальной сетью клиента (Client VPN), служит иньерфейсом к мультианклавному терминалу (MEC),
• ENI –Enterprise Network Interface: содержит блок IPSec crypto виртуального секретного анклава (VSE), межсетевой экран и маршрутизатор
• CDCI –Cross-Domain Controlled Interface: фильтр высокой безопасности, который контролирует поток информации между анклавами (например, между CENTRIXS-KOR и CENTRIXS-UNCK).

«Черное ядро» соединяет все военные базы НАТО на территории Южной Кореи (рис. 13).

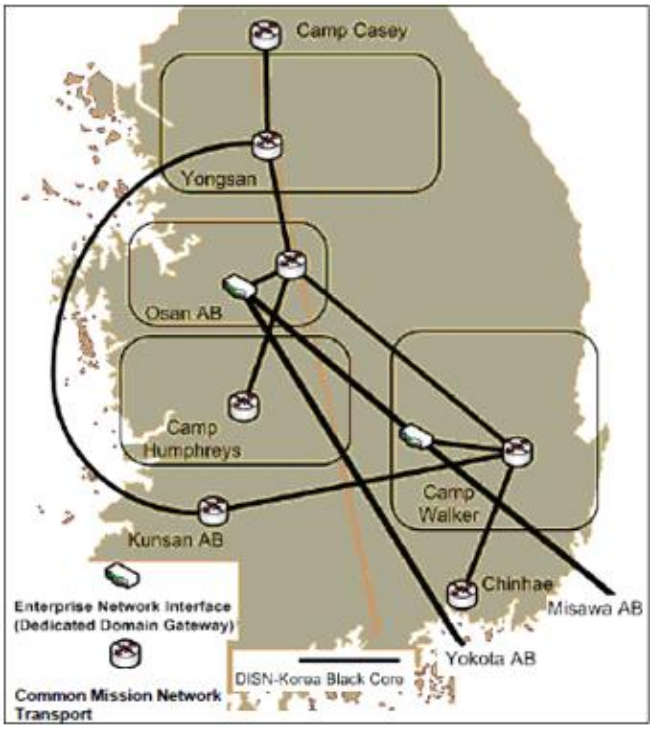

Рис. 13. «Черное ядро» на территории Южной Кореи.

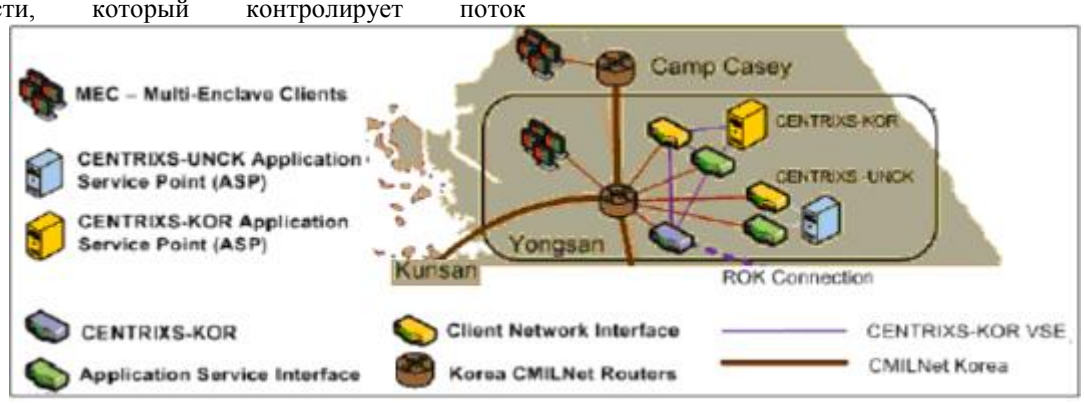

Рис. 14. Фрагмент пилотной сети GIG-3 на территории военной базы Yongsan.

VI. Обсуждение

Остановимся на особенностях программирования сети GIG.

В 2012 г. агентство DISA опубликовало руководящий документ GCMP 2012 [14]. 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 от сигнализации SS7 к IP протоколу: объявлялся переход на IP протокол в приложениях, сервисах и ставилась цель следовать концепции сетецентрической войны. Новая архитектура базируется на модель облачных вычислений, и этим отличается от прежних моделей, которые были сетецентрическими.

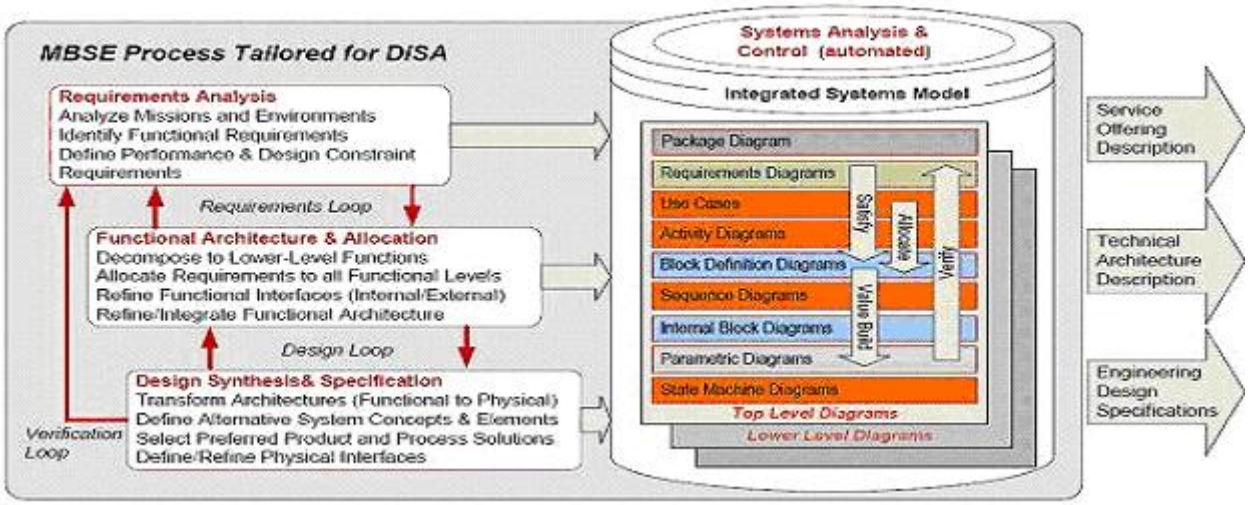

Рис. 15. Процесс разработки новейшей версии GIG2 по модели MBSE.

Общие требования DISA к разработке концепции GIG-2 и GIG-3 иллюстрирует рис. 15. В основе концепции лежит модель MBSE (Model based Systems Engineering) и язык SysML (Systems Modeling Language) [16]. Сама модель MBSE представляет собой коллекцию диаграмм на языке SysML.

Результатом разработки являются три типа документов:

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

В заключении отметим. Военное ведомство США ставит перед собой исключительно амбициозные цели:

1) во всей сети GIG перейти от телефонного стандарта TDM к интернет-протоколам, т.е. уйти от телефонной сигнализации SS7, которая является «нервной системой» сети, соединяющей всех пользователей с «мозгом» сети – интеллектуальной сети (AIN, Advanced Intelligent Network) и перестроить сеть по правилам Интернета;

2) 40 различных систем связи в сети GIG1 перепрограммировать по единым правилам модели MBSE для сети GIG-2;

3) а затем еще раз перепрограммировать с учетом требований кибервойны для сети GIG-3.

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?

Сомнения вызывает также возможный уход от высшего достижения коммутации каналов – интеллектуальной сети AIN и замена ее высшим достижением коммутации пакетов – IMS (IP Multimedia Subsystem). Кто возьмется за такую работу?

Необходимо провести серьезные исследования, позволяющие научно обосновать основные принципы построения и долгосрочной эволюции ССН. В силу объективных и субъективных причин значительная часть отраслевых научно-исследовательских центров уже не располагает коллективами, способными на высоком научно-техническом уровне выполнить необходимые исследования. Тем не менее, формирование временного коллектива высоко-квалифицированных специалистов, работающих в разных городах России, пока еще представляется посильной задачей

Библиография

[1] Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Department of Defense. Version 1.0 June 2007.
[2] The Global Information Grid (GIG) 2.0 Concept of Operations Version 1.1//11 March 2009, Joint Staff J6, Washington, D.C.
[3] John Chapin Reengineering the GIG to Support the Warfighter// IEEE COMSOC Boston Chapter, 8 January 2009.

[4] Randy Cieslak GIG 3.0 Design Factors. An Architecture Proposal for Aligning NetOps to the Operational Chain of Command U.S. Pacific Command 11 January 2011 https://info.publicintelligence.net/USPACOM-GIG.pdf
[5] Перспективы создания глобальной информационной сети МО США. http://www.modernarmy.ru/article/321 Retrieved: Jul, 2014.
[6] David A. Fritz et al Military Satellite C ommunications: Space-Based Communications for the Global Information Grid //Johns Hopkins APL Technical Digest, Volume 27, Number 1 (2006).
[7] Шнепс-Шнеппе М. А. Телекоммуникации для экстренных и военных нужд: параллели //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 7. – С. 25-36.
[8] Шнепс-Шнеппе М.А., Намиот Д.Е. Телекоммуникации для военных нужд: от сети GIG1 к сети GIG2 // International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 9. – С. 9-17.
[9] Cyber and Physical Threat and Risk Analysis to Improve the NPSBN (CAPTAIN) May 7, 2014 http://www.911.gov/pdf/State_of_911_Webinar_050714.pdf Retrieved: Jul, 2014.
[10] В. Микрюков Информационная война http://nvo.ng.ru/concepts/2014-05-23/1_theory.html Retrieved: Jul, 2014.
[11] Rogers: Cybercom Defending Networks, Nation http://www.defense.gov/news/newsarticle.aspx?id=122949
[12] Julie Tarr and Tony DeSimone Defining the GIG Core (2008) http://iac.dtic.mil/csiac/download/Vol11_No2.pdf Retrieved: Jul, 2014.
[13] David F. Carr Building a protective black core for the Global Information Grid (2009) http://defensesystems.com/articles/2009/09/02/cyber-defense-black-core.aspx Retrieved: Jul, 2014.
[14] DISA. Global Information Grid (GIG) Convergence Master Plan (GCMP), Vol. 1, 02 August 2012.
[15] Namiot, D., & Sneps-Sneppe, M. (2014). On M2M Software Platforms. International Journal of Open Information Technologies, 2(8), 29-33.
[16] Friedenthal S., Moore A., Steiner R. A practical guide to SysML: the systems modeling language. – Elsevier, 2011.

Telecom for militaries: GIG-3 network for cyber-warfare

Sneps-Sneppe M.A., Namiot D.E., Cikunov Y.V.

***Abstract* — This article is devoted to the development plans of the communication network of the US Ministry of Defense. It is the world's largest private network. Naturally, the experience of the development of such a network is very valuable for all engineers involved in the development of communication networks. The paper collected and analyzed the presented and available for researchers plans for development of the Global Information Network (GIG), lists all its defining program. Main attention is paid to the so-called cyber-warfare and information security.**

***Keywords* — GIG, cyber-warfare, telecom networks, packets, military telecom.**