О создании единого информационного пространства общества

М.А. Шнепс-Шнеппе, Д.Е. Намиот, В.А. Сухомлин

***Аннотация*— В построении информационного общества России ведущая роль принадлежит ОАО "Ростелеком". Нами рассмотрен опыт создания единого информационного пространства Министерства обороны США и изложены методические материалы, которые могут быть полезны при построении информационного общества в России, в том числе разработка мета-модели единого информационного пространства, применение языка SysML.**

***Ключевые слова*— информационное общество, Ростелеком, IP, софтсвич, DoD, GIG, JIE, мета-модель, SysML.**

I. «Ростелеком» и международные санкции

На всероссийской конференции «Взгляд в электронное будущее», прошедшей в октябре 2014 г. в Сочи по инициативе «Ростелекома» и Правительства России, обсуждался вопрос импортозамещения в области ИТ [1].

«Проектом импортозамещения мы занимаемся уже больше года, понимая, что национальный оператор должен иметь сегмент сети, построенный на национальном оборудовании, и управляемый национальным программным продуктом. Мы приняли решение, что как минимум 30 % оборудования, установленного на наших сетях, в ближайшем будущем должно быть поставлено российскими производителями и управляться российским софтом. Эта цель открывает большие возможности прежде всего для ИТ-компаний», - заявил президент ОАО «Ростелеком» Сергей Калугин.

Задачи «Ростелекома» в связи с импортозамещением и разработкой отечественных средств связи мы рассматривали в статье [2]. Там же приведен список новых сервисов, которые обусловлены сближением технологий коммутации каналов и пакетов и могут найти отражение в новой редакции российского закона «О связи».

На конференции обсуждалась также роль «Ростелекома» в построении информационного общества. Согласно распоряжению Правительства РФ № 453-р от 21 марта 2011 года ОАО "Ростелеком" является единственным исполнителем работ по ряду мероприятий Федеральной целевой программы "Информационное общество (2011-2020 годы)". В выполнении этих мероприятий используется Национальная облачная платформа О7 [3].

Важнейшим среди мероприятий является сервис «О7. 112», который обеспечивает обработку экстренных вызовов по номеру 112. Функции сервиса «О7. 112» включают:

- прием и обработку сообщений по единому номеру 112 для всех экстренных служб,
- координацию управления силами и средствами реагирования,
- межведомственную координацию (экстренные службы различных ведомств работают в едином информационном пространстве).

Использование платформы О7 предполагает:

- снижение потери населения до 15%,
- снижение времени комплексного реагирования в 2 раза,
- снижение экономического ущерба – до 5%,
- разгрузку операторов межведомственных служб за счёт «перехвата» ложных и справочных вызовов оператором 112 – на 70%.

К проекту «О7. 112» примыкает сервис «О7. Медицина». Цель его создания — автоматизация взаимодействия всех участников медицинского процесса: сотрудников лечебно-профилактических учреждений, пациентов, работников министерств и ведомств, отвечающих за здоровье граждан. Подключившись к сервису «О7. Медицина», любое лечебно-профилактическое учреждение получает доступ к системе электронной регистратуры, к единым электронным медицинским картам пациентов, к системе электронного документооборота.

Отметим еще сервис «О7. Сити». Цель создания сервиса – обеспечение эффективного и безопасного функционирования городских служб и создания комфортных условий проживания в городе (регионе). Сервис «О7. Сити» включает:

- мониторинг городской инфраструктуры (ЖКХ, дорог, показаний приборов критических объектов городской инфраструктуры),

Статья получена 10 декабря 2014.
Переработанный вариант – 20 декабря 2014

М.А. Шнепс-Шнеппе - профессор, главный научный сотрудник ЦНИИС. (email: sneps@mail.ru).

Д.Е. Намиот. - старший научный сотрудник лаборатории ОИТ, факультета ВМК МГУ имени М.В.Ломоносова. (email: dnamiot@gmail.com)

В.А. Сухомлин. - заведующий лабораторией ОИТ, факультета ВМК МГУ имени М.В.Ломоносова. (email: sukhomlin@mail.ru)

• мониторинг природных объектов (пожары, наводнения),

• видеонаблюдение и видеоаналитику (установка промышленных камер наблюдения в городе, а также обеспечение открытых интерфейсов, с помощью которых граждане смогут направлять для обработки информацию о происшествиях, собираемую бытовыми видеоустройствами),

• мониторинг и управление общественным транспортом и парковками,

• информирование населения об угрозах и чрезвычайных ситуациях.

Проекты «О7. 112», «О7. Медицина», «О7. Сити» и другие с участием «Ростелекома» (устранение «цифрового неравенства», ЕГЭ и образование, электронное правительство) – все эти проекты чрезвычайно важны и социально значимы, но вместе с тем и чрезвычайно сложны для реализации. В частности, создание Системы 112 длится уже более 10 лет, но находится еще далеко о завершения [4]. Вряд ли будут достигнуты целевые показатели по проекту «О7. 112». Не мало горьких слов звучит и о состоянии ЖКХ.

Оглядываясь на неудовлетворительный ход проектов по построению информационного общества в России, на ум приходит нетривиальное суждение: состояние дел может привести, на наш взгляд, к тому, что «Ростелеком» будет не только предоставлять облачную платформу О7 и хранить данные информационного общества, но и станет головным исполнителем проектов, привлекая другие ведомства в качестве соисполнителей. В предыдущей статье [2] мы рассматривали задачи «Ростелекома» с части средств связи, проводя параллели с опытом Пентагона по новым сервисам телекоммуникаций в связи с переходом на пакетную коммутацию и IP технологии. В настоящей же статье рассмотрим положение дел с созданием единого информационного пространства Министерства обороны США (Department of Defense, DoD) и расскажем о методических материалах, которые, на наш взгляд, могут быть полезны при построении информационного общества в России.

II. О ЕДИНОЙ ИНФОРМАЦИОННОЙ СРЕДЕ DOD

Рис. 1 представляет схему из войны будущего – как будет выглядеть поле боя в условиях единой информационной среды [5]:

• Все действующие лица - участники боя (в самом широком смысле) общаются в едином информационном поле, которое определяется единым набором сервисов (UC, Unified Capabilities), о чем рассказано в [2].

• IP адреса имеют все «участники» боя: солдаты, сенсоры, ракеты, прикладные программы.

• Полный набор данных хранится в базах данных Агенства национальной безопасности (см. на рисунке внизу справа).

• Спутники обеспечивают оперативную связь между командирами, солдатами, беспилотниками и т.п.

• Летающие объекты (рисунок слева наверху) пользуются живучей IT инфраструктурой, способной обнаруживать вражеские сети.

• И солдат, главное действующее лицо любой войны, обладает возможностью быстрого приспособления к меняющимся условиям боя.

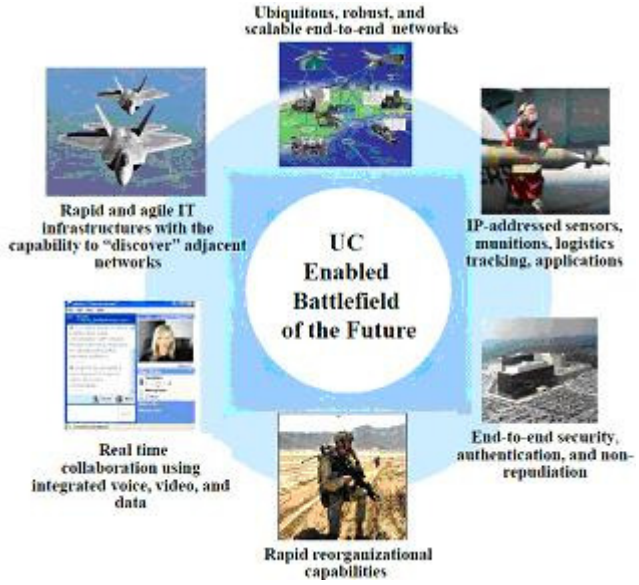

Рис. 1. Будущее поле боя в единой информационной среде [5].

Успех военных операций зависит от способности командования действовать оперативно и на базе наиболее точных и своевременных данных о противнике и собственных силах. С целью обеспечения условий для будущих войн Министерство обороны США приняла амбициозный, многолетний план IT модернизации и создания единой информационной среды (Joint Information Environment, JIE) [5]. Этот план предполагает кардинальную перестройку существующих IT сетей и систем оборонного ведомства. В настоящее время (рис. 2 слева) штабы разных родов войск (армия, ВВС, ВМС, спецвойска) «живут» в разных информационных средах. Цель модернизации (рис. 2 справа) состоит в создании единого командного центра в единой информационной среде, который обеспечит операционную работу и безопасность штабов всех родов войск.

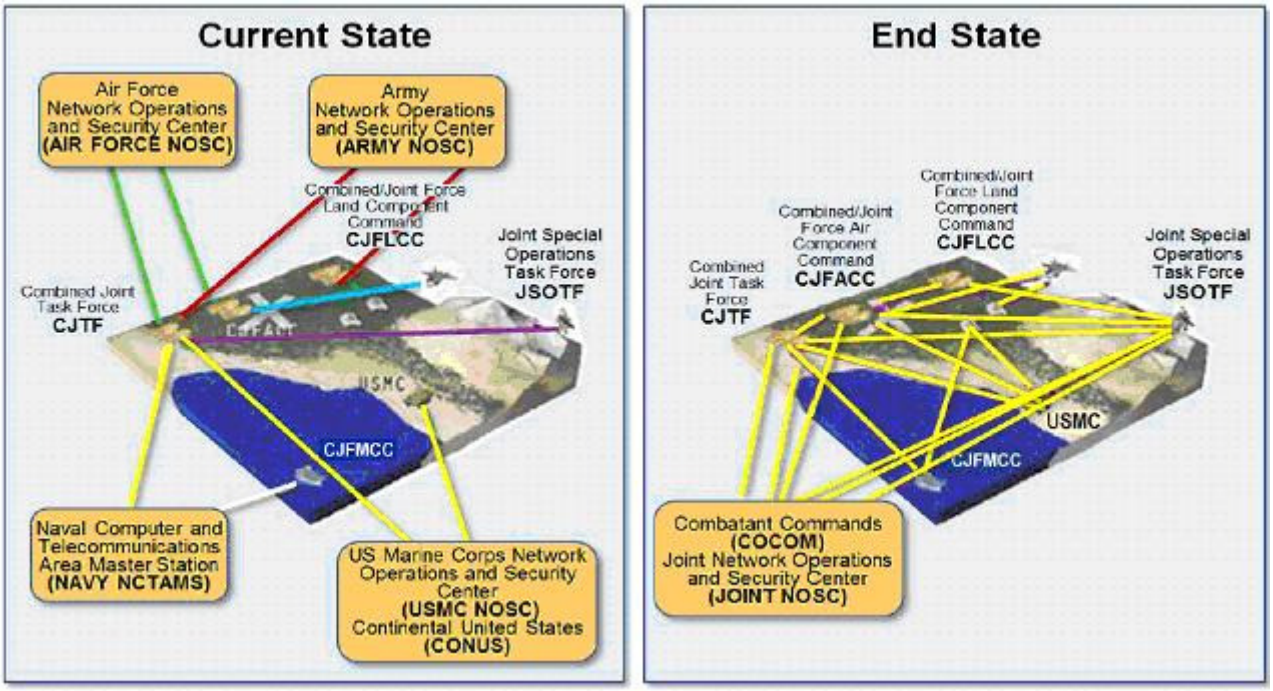

Рис. 2. Штабная работа в единой информационной среде [5].

Создание единой информационной среды Министерства обороны США – задача беспрецедентно трудоемкая и сложная. Она объединяет более 10000 операционных систем, 2000 датацентров, 65000 серверов, более 7 миллионов компьютеров и вычислительных уствойств (рис. 3). В 2014 году на содержание информационной сети, которая размещена в 146 странах, в 5000 местах и 600000 строениях, отводится 39,6 млрд долл, на расширение ее инфраструктуры – 17,4 млрд долл, и отдельной статьей выделены средства на кибербезопасность – 4,7 млрд долл [6].

DoD IT User Base	IT Systems
~1.4 million active duty	>10,000 operational systems (20% mission critical)
~783,000 civilian personnel	~1850 data centers
~1.2 million National Guard and Reserve	~65,000 servers
5.5+ million family members and military retirees	~7+ million computers and IT devices
146 + countries	Thousands of networks/ enclaves
5,000 + locations	Thousands of email servers, firewalls, proxy servers, etc.
600,000 + buildings and structures	Mobile devices ~ 493,000 Blackberries

Рис. 3. Характеристика информационной сети Министерства обороны США [6].

III Что такое DoDAF

DoDAF (Department of Defense Architecture Framework) – это информационная архитектура военного ведомства [7], и ее новейшая редакция создавалась в условиях развертывания кибервойны. Поэтому на первом месте стоит создание единой архитектуры безопасности (Single Security Architecture, SSA), которая должна обеспечить внутреннюю безопасность сети и предотвращать внешние киберугрозы.

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

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

На четвертом – унифицированный набор сервисов (например, email и ряд новых сервисов, что рассмотрено в [2], а также в разделе 6 ниже).

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

На шестом – консолидация датацентров. В 2014 г. имеется 2000 датацентров, а в 2017 г. их число сократится до 500 (на четырех уровнях иерархии). Пилотный проект этой работы рассмотрен ниже в разделе 5.

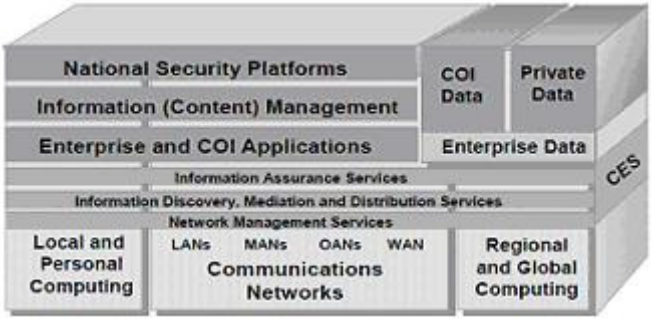

Рис. 4. Целевая архитектура единой информационной среды DoD [8].

На рис. 4 представлена семиуровневая модель единой информационной среды DoD. К данному моменту она стандартизована только частично. Принято решение в части единых коммуникационных сетей (нижний уровень): это - широкополосная IP сеть (wide area IP backbone network) и протокол MPLS (multiprotocol label switching protocol). Выбрана базовая архитектура унифицированных сервисов (Unified Capabilities

Reference Architecture), что относится к уровню Distribution Services. Наиболее важной и трудоемкой работой при создании единой информационной среды является стандартизация уровня приложений (Enterprise and Community-of-Interest Applications), о чем и пойдет разговор.

Мета–модель DoDAF. При описании уровня приложений прежде всего следует говорить о мета–модели DoDAF (Department of Defense Meta-Model). Единая мета–модель DoDAF разрабатывается с 1990 г. Мы рассмотрим текущую версию 2.0 (с 2009 г.). Рис. 5 иллюстрирует взаимосвязи между основными понятиями мета–модели DoDAF . Модель содержит шесть описаний, которые объединены ключевым понятием Activity:

1. Описание данных (Data Description) — отвечает на вопрос What (что включает и описание Resources, кроме самих Data)
2. Описание функции (Function Description) — отвечает на вопрос How (содержит также описание исполнителя (Performer), который выполняет Function и учитывет связанные с ней Measures, Rules и Conditions)
3. Описание сети (Network Description) — Where
4. Описание участников (People Description) — Who (что включает Organizations)
5. Описание времени (Time Description) — When
6. Описание мотивации (Motivation Description) — Why (с расширением, что включает описание Capability requirements)

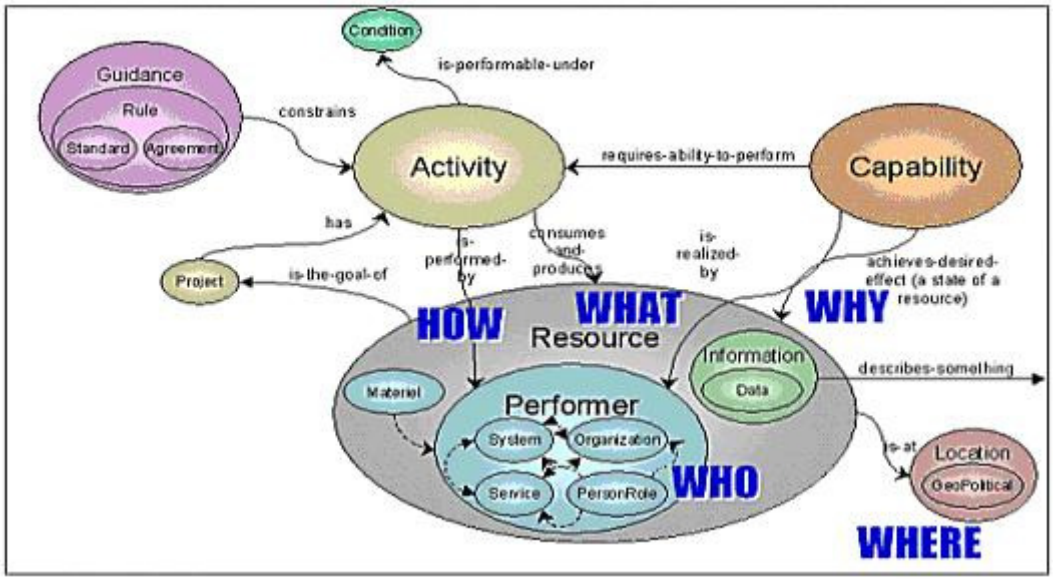

Рис. 5. Иллюстрация мета-модели DoDAF [7].

Единая информационная среда. Рис. 6 дает представление о документации по единой информационной среде GIG. Она представлено с восьми точек зрения (Viewpoint), что изложено в 52 томах:

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

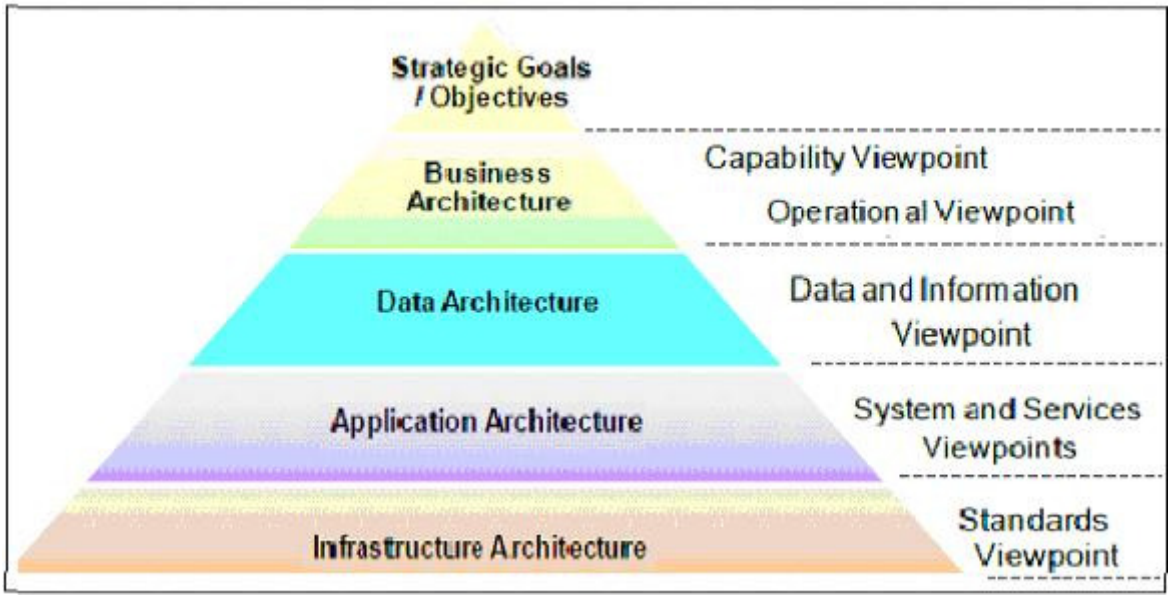

Рис. 6. Описание единой информационной среды GIG содержит 52 документа [7].

IV Язык SysML

Для упрощения работы с документацией JIE GIG требуются графические средства. За прошедшие годы апробированы различные средства. В итоге выбран графический язык SysML (Systems Modeling Language). Напомним его предысторию [9]. Язык UML давно уже стал стандартом общения между участниками разработки ПО крупных проектов. Его богатые выразительные средства и широкий спектр поддерживающих продуктов способствовали тому, что UML начал проникать в другие области деятельности, связанные с моделированием бизнес-процессов. В итоге появился язык SysML — клон UML, позволяющий проектировать программно-аппаратные комплексы. Средств языка UML оказалось недостаточно для моделирования аппаратуры. Понадобилось добавить ряд новых графических элементов и диаграмм, которые позволяют описывать нюансы каждого элемента модели и взаимосвязи между элементами, а также строго задавать границы модели. С другой стороны, в рамках поставленной задачи UML характеризуется некоторой избыточностью, поэтому не все его элементы вошли в новый клон (рис. 7). Изменения были специфицированы в виде профиля UML 2.0 и названы новым именем — SysML (System Modeling Language). В спецификацию этого языка вошли новые диаграммы — требований, внешних и внутренних блоков, времени, параметрическая.

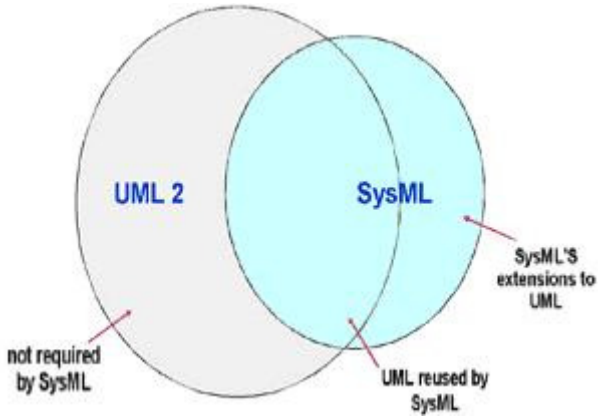

Рис. 7. Взаимоотношения между UML и SysML.

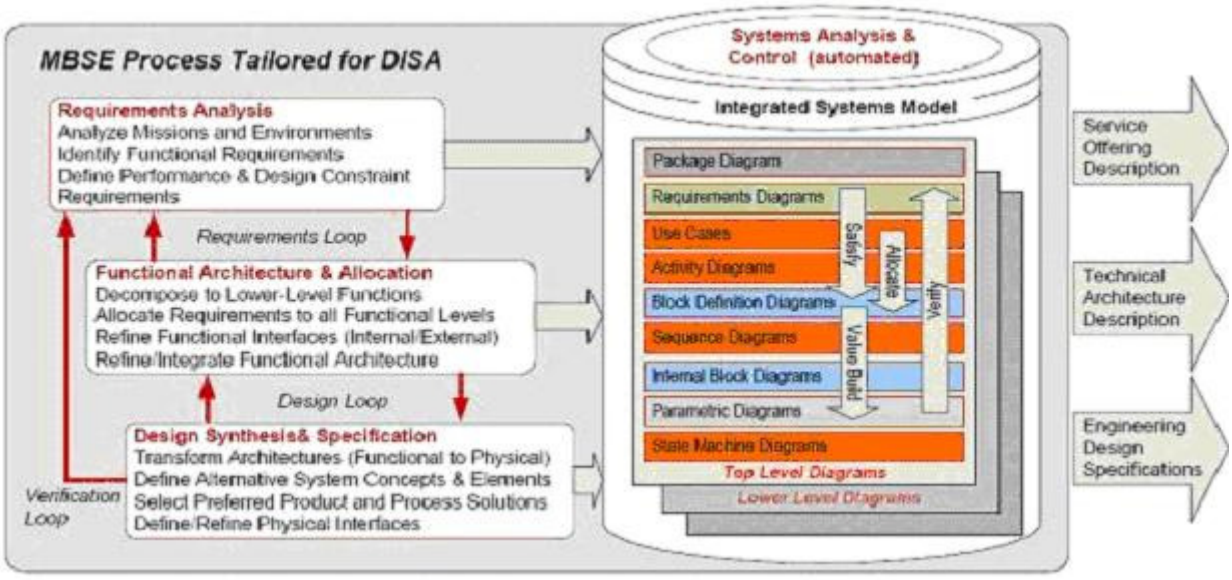

Рис. 8. Процесс разработки новейшей версии GIG по модели MBSE [10].

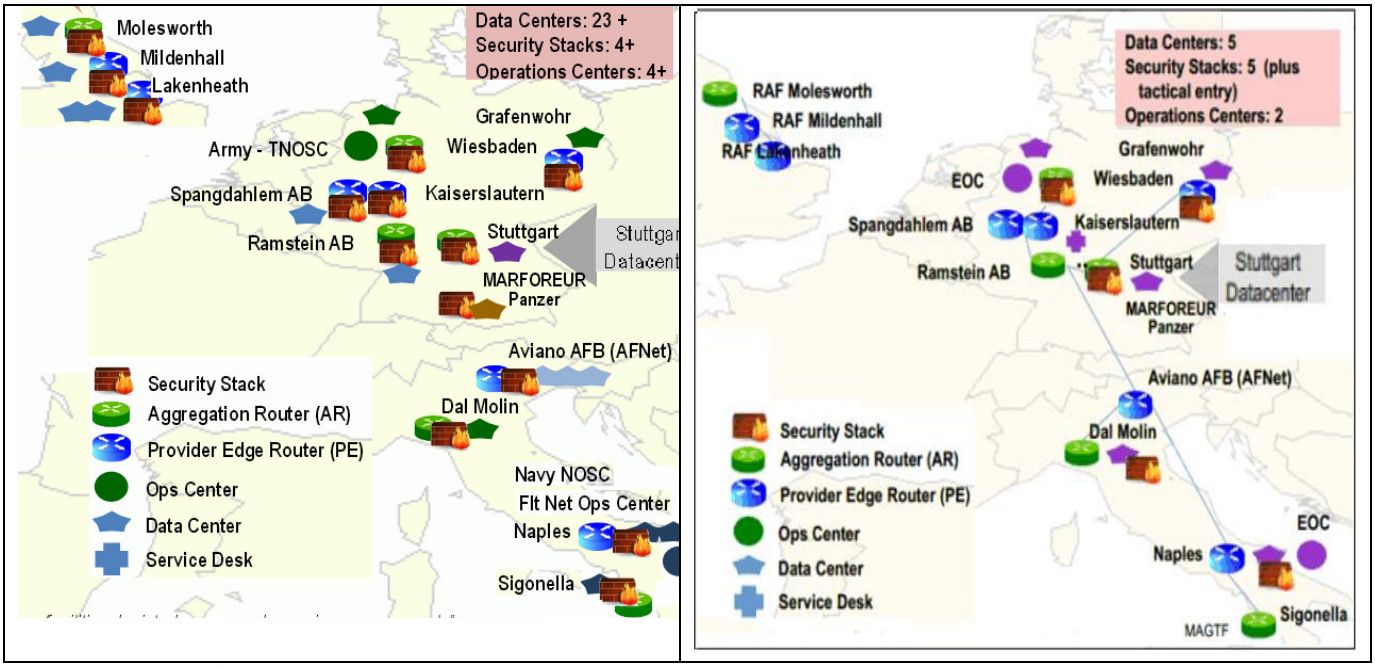

Рис. 9. Состояние Информационная сеть американских баз в Европе [6]: а) текущее состояние, б) план модернизации к 2016 г.

Общие требования DISA к разработке единой информационной среды иллюстрирует рис. 8. В основе концепции лежит модель MBSE (Model based Systems Engineering) и язык SysML (Systems Modeling Language). Сама модель MBSE представляет собой коллекцию диаграмм на языке SysML.

Результатом разработки являются три типа документов:

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

Как заверяют разработчики единой информационной среды [10], по документации MBSE можно не только моделировать систему и изучать ее производительность, но даже генерировать исполнимый код.

V Модернизация информационной сети

В качестве пилотного проекта модернизации информационной сети DoD выбраны американские базы в Европе (рис. 9). Центральным звеном модернизации выступает Главный датацентр в Штутгарте. На рис. 9а показано текущее состояние информационной сети американских баз в Европе, а на рис. 9б – после модернизации, что запланировано завершить в 2016 г. В итоге преобразований число датацентров в Европе уменьшится с 23 до 5. Особенно важно уменьшение узлов безопасности (Security Stacks) – с 14 узлов сегодня до 5 узлов после модернизации, что повысит безопасность работы сети.

VI Трудности GIG на пути к единой инфраструктуре

Воспользуемся новейшими методическими материалами по GIG (от 2013 г.), которые относятся к базовой архитектуре унифицированных сервисов (Unified Capabilities Reference Architecture) [11]. Эта новая архитектура унифицированных сервисов UC предлагает любому солдату и армейскому служащему богатый набор средств общения: e-mail, чат, голос, видео, поиск и многое другое, и все это доступно по единому адресу пользователя и в безопасной среде. Управление сеансом связи (Session Control) происходит по единому протоколу AS-SIP (Assured Service – Session Initiation Protocol). Сетевая архитектура унифицированных сервисов базируется на широкополосной IP сети (wide area IP backbone network) и на протоколе MPLS (multiprotocol label switching protocol), который обеспечивает требуемое качество связи QoS в сети коммутации пакетов.

Программу перехода на IP технологию МО США приняло уже в 2009 г. [12]. Но в настоящее время в армии США еще господствует традиционная коммутация каналов, т.е. TDM сети, и еще долгое время они будут сосуществовать со строящимися IP сетями. Для перехода на IP технологию будут установлены шлюзы (софтсвичи).

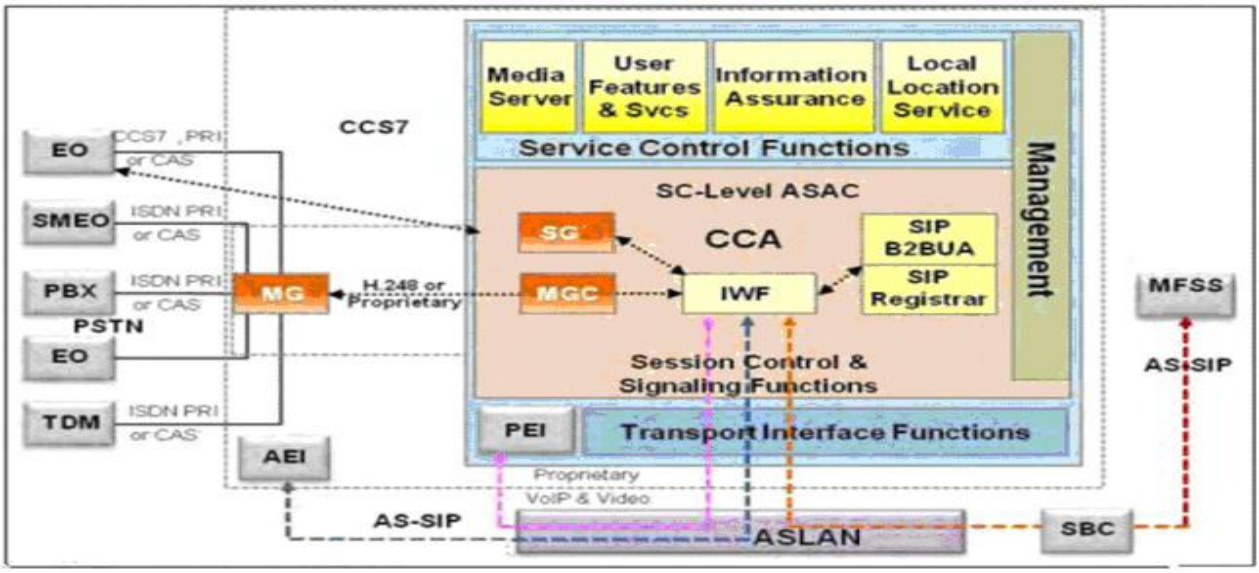

Рис. 10. Многофункциональный программный коммутатор (софтсвич) MFSS [13].

Рис. 11. Карта размещения 22 MFSS и WAN SS (2012) [13].

На рис. 10 показано, как многофункциональный софтсвич MFSS будет управлять вызовами:

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

На рис. 10 еще указаны оконечные устройства EO (End Office) в сети коммутации каналов и два типа устройств в IP сети: AEI (Assured Services End Instrument), работающие по протоколу AS-SIP, и

нестандартные устройства PIE (Proprietary Internet Protocol Voice End Instrument).

К 2012 г. объявлена установка 22 мощнейших софтсвичей MFSS и WAN SS компании Cisco на американских базах по миру (рис. 11). К 2016 г. планируется довести эти узлы до функциональности, представленной на рис. 10.

VII Обсуждение

Сейчас появилась новая инициатива – кибервойна, что потребовало кардинальной перестройки GIG. В октябре 2010 года была создано киберкомандование, 2-я армия США (US Army Cyber Command/2nd Army). По планам на август 2014 г. [14], к 2016 году Cybercom будет иметь 6000 высококвалифицированных сотрудников, образующих 133 команды, способные выполнять следующие три основные миссии:

1) национальные киберсилы, способные охранять критическую инфраструктуру и ключевые ресурсы страны,

2) боевые киберсилы, обеспечивающие киберзащитой боевых командиров по всему миру,

3) силы киберзащиты, охраняющие информационные сети Министерства обороны США.

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

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

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

3) перепрограммировать сеть с учетом требований кибервойны.

Программа развития GIG чрезвычайно амбициозна. Что касается работ по программированию, то ключевым является человеческий ресурс. Найдутся ли многие тысячи программистов, способные такую работу выполнить и следовать при этом жестким правилам MBSE? Сомнения вызывает также возможный уход от высшего достижения коммутации каналов – интеллектуальной сети AIN и замена ее высшим достижением коммутации пакетов – IMS (IP Multimedia Subsystem), но еще недостаточно апробированным. Кто возьмется за такую работу?

Задачей еще более сложной, невообразимо более сложной является создание единой информационной среды Министерства обороны США на базе информационной архитектуры DoDAF и мета–модели DoDAF.

Построение информационного общества в России сопоставимо по сложности с перечисленными задачами оборонного ведомства США и потребует сопоставимых людских и финансовых ресурсов. Сегодня трудно ответить на вопрос, какова будет роль «Ростелекома» в построении информационного общества. Это покажет ближайшее будущее, успехи в модернизации народного хозяйства страны и, прежде всего, успехи импортозамещения в отрасли связи.

В завершении назовем одну конкретную задачу для «Ростелекома», которая относится к индустрии программирования услуг. В руководящем документе по разработке GIG [5] сказано, что среда разработки услуг SCE (service creation environment) должна входить в состав средств разработки армейских приложений, чтобы сокращать время разработки новых услуг, указано на целесообразность привлечения сторонних программистов. Это предложение относится к весьма болезненному для связистов вопросу об открытых интерфейсах программирования (Open API). Если будет доступен открыто объявленный набор API, то многие сторонние программисты включатся в разработку, а дело армейских связистов будет состоять в тестировании предложенных услуг и включении их в состав сети GIG. Эта задача в полной мере относится к разработке сервисов информационного общества и к «Ростелекому», в частности.

В данной работе также использованы материалы из статей [16][17].

Библиография

[1] http://servernews.ru/597356 Retrieved: Jan, 2015.
[2] Шнепс-Шнеппе М.А., Намиот Д.Е. Об эволюции телекоммуникационных сервисов на примере GIG// International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 1. – С. 1-13.
[3] http://www.kommersant.ru/doc/2520423 Retrieved: Jan, 2015.
[4] http://www.rostelecom.ru/projects/innovations/o7/ Retrieved: Jan, 2015.
[5] Парфенов Б.А. Система-112: сроки и цели корректируются// Вестник связи. – 2014. – №. 11. – С. 4-8.
[6] The Department of Defense. Strategy for Implementing the Joint Information Environment. September18, 2013.
[7] D. DeVries. DoD Joint Information Enterprise
[8] http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-DeVries.pdf Retrieved: Jan, 2015.
[9] http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf Retrieved: Jan, 2015.
[10] Department of Defense. Information Enterprise Architecture. Unified Capabilities Reference Architecture. Version 1.0. January 2013.
[11] Николаев А., Зыль С. Визуальное проектирование на основе SysML//Открытые системы. – 2006. – № 5.
[12] DISA. Global Information Grid (GIG) Convergence Master Plan (GCMP), Vol. 1, 02 August 2012.
[13] Department of Defense. Unified Capabilities Framework 2013. January 2013. 12. Global Information Grid. Architectural Vision for a Net-Centric, Service-Oriented DoD Enterprise. Department of Defense. Version 1.0, June 2007.
[14] Department of Defense. Unified Capabilities Master Plan. October 2011.
[15] http://www.defense.gov/news/newsarticle.aspx?id=122949 Retrieved: Jan, 2015.
[16] 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.

[17] Шнепс-Шнеппе М.А., Намиот Д.Е, Цикунов Ю.В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны//International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 10. – С. 3-13.

On creation of an unified information space for the society

M.A. Sneps-Sneppe, D.E. Namiot, V.A. Suhomlin

Abstract— **"Rostelecom" plays the leading role in building the information society of Russia. We have considered the experience of creating an unified information space US Department of Defense and presented educational materials that can be useful in building the information society in Russia, including the development of a meta-model of a single information space, and the use of SysML language.**

Keywords— **information society, Rostelecom, IP, softswitch, DoD, GIG, JIE, meta-model, SysML.**