УДК 004.75 DOI 10.25559/SITITO.2017.3.360

Шнепс-Шнеппе М.А.[1], Сухомлин В.А.[2], Намиот Д.Е.[2]

[1] ЦКБ-АбаваНет, г. Москва, Россия
[2] Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия

ОБ ИНТЕРФЕЙСАХ ИНФОРМАЦИОННЫХ СЕТЕЙ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация

Рассматривается принципиальный вопрос о телекоммуникациях (информационных сетях) как решающем звене цифровой экономики. Подробно изучаются интерфейсы информационных сетей, что обеспечивает взаимодействие отдельных подсистем друг с другом. Сравнивается российская сеть экстренных вызовов 112 с американскими аналогами: NG9-1-1 и FirstNet. Опыт США показывает, что сеть нового поколения для обслуживания экстренных вызовов NG9-1-1 имеет те же требования в части приложений, что и глобальная информационная сеть оборонного ведомства GIG (Global Information Grid). Подробно рассмотрены интерфейсы сети GIG в условиях боевых действий. Анализируются планы создания общей операционной среды армии США. Отмечается необходимость учета международных стандартов при создании информационных сетей цифровой экономики.

Ключевые слова

Цифровая экономика, телекоммуникации, информационная сеть, интерфейсы, сеть экстренных вызовов 112, NG9-1-1, FirstNet. сеть оборонного ведомства GIG, общая операционная среда армии США.

Sneps-Sneppe M.A.[1], Sukhomlin V.A.[2], Namiot D.E.[2]

[1] CKB-AbavaNet, Moscow, Russia
[2] Lomonosov Moscow State University, Moscow, Russia

ON INTERFACES OF INFORMATION NETWORKS OF THE DIGITAL ECONOMY

Abstract

The principal issue of telecommunications (information networks) as a decisive link in the digital economy is considered. The interfaces of information networks are studied in detail, which ensures the interaction of individual subsystems with each other. The Russian emergency call network 112 is compared with the US counterparts: NG9-1-1 and FirstNet. The US experience shows that the NG9-1-1 new generation emergency service network has the same requirements for applications as the global information network of the GIG (Global Information Grid). The interfaces of the GIG network in the context of combat operations are examined in detail. The paper analyzes the plans to create a common operating environment for the US Army. There is a need to take into account international standards when creating information networks of the digital economy.

Keywords

Digital economy, telecommunications, information network, interfaces, emergency network 112, NG9-1-1, FirstNet. GIG Defense Network, General Operating Environment of the US Army.

1 Введение

Приступая к реализации Государственной программы «Цифровая экономика», полезно оглянуться на советский опыт, начиная от Плана ГОЭЛРО и работы Госплана СССР до громадной работы по созданию Общегосударственной автоматизированной сети (ОГАС) и наиболее известных имен ее создателей А.И. Китова (1920–2010) и В.М. Глушкова (1923—1982). Мы же ограничимся весьма частным, хотя и важным, и очень сложным вопросом – об интерфейсах

информационных сетей цифровой экономики[2]. Статья продолжает наше исследование глобальных информационных систем [1].

В настоящее время наиболее крупным проектом государственного значения в области телекоммуникаций, который строится за государственные деньги, является это разработка системы экстренных вызовов 112. Эта система затрагивает все стороны жизни российского общества и представляет собой важнейшую часть цифровой экономики. В ходе реализации Системы 112 обнажаются многие недостатки хозяйства страны, накопившиеся за четверть века капиталистического строительства, и их анализ может быть полезным для реализации Государственной программы «Цифровая экономика» в целом. В первую очередь это касается стандартизации: без наличия государственных стандартов нельзя возродить производство, выполнить планы импортозамещения.

Ранее мы рассматривали принципиальный вопрос о телекоммуникациях (информационных сетях) как решающем звене цифровой экономики [2, 3]. Естественно, следующим важным вопросом является изучение интерфейсов, то есть, как отдельные подсистемы информационных сетей взаимодействуют друг с другом. В разделе 2 мы рассматриваем сеть экстренных вызовов 112. Разделы 3 и 4 посвящены американскому аналогу сети экстренных вызовов: NG9-1-1 и FirstNet. Опыт США показывает: сеть нового поколения для обслуживания экстренных вызовов NG9-1-1 имеет те же требования в части приложений, что и глобальная информационная сеть оборонного ведомства GIG (Global Information Grid), поэтому в разделах 5-8 мы рассматриваем нормативные документы по разработке вычислительных средств сети GIG.

Заранее обращаем внимание на один важный аспект – необходимость учета международных стандартов при создании информационных сетей цифровой экономики. Заметим, к примеру, что работа контрольных точек только тактической информационной сети (см. раздел 5) регламентируется длинным списком открытых и закрытых стандартов – общим объемом 20 страниц текста. Это замечание указывает на ту громадную работу, которую предстоит совершить при реализации Государственной программы «Цифровая экономика».

2 Сеть экстренных вызовов 112

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. Но планы не выполняются.

В официальном отчете Минкомсвязи России [7] 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.

Представление о телекоммуникационной составляющей системы «112» дает рис. 1, который взят нами из концепции Системы112, разработанной с участием компании «Светец» [8]. Здесь УОВ ЭОС — узел обработки вызовов экстренных оперативных служб.

На рис. 1 приведены пять интерфейсов Системы 112, которые предполагается уточнить в рамках выполнения ФЦП. Заметим, что выбор

[2] Отметим, что авторы настоящей статьи придерживаются сути «цифровой экономики», отличной от точки зрения Минкомсвязи. На прошедшем 1-3 июня 2017 года ПМЭФ глава Минкомсвязи Николай Никифоров сообщил о первоочередных проектах программы «Цифровая экономика». «Мы должны сфокусировать эту программу на так называемых сквозных технологиях. Это и большие данные, машинное обучение, искусственный интеллект, дополненная реальность, так называемые туманные вычисления и, конечно же, технология распределенных реестров, то, что мы называем блокчейн», — сказал министр. Источник:
http://d-russia.ru/prezident-poruchil-pravitelstvu-dorabotat-proekt-programmy-tsifrovaya-ekonomika.htm

интерфейсов – это исключительно сложная работа, требующая учета множества международных стандартов. Представленную концепцию Системы 112, на наш взгляд, следовало бы существенно доработать.

Рис. 1. Пять интерфейсов Системы-112

Выскажем три замечания:

- О протоколе SIP. Сомнения вызывает его включение в Систему 112 наряду с ОКС-7. Для этого он еще недостаточно апробирован – с учетом чрезвычайной важности Системы 112 для государства. Главными недостатками протокола SIP являются трудности с обеспечением секретности (в условиях кибервойны) и обслуживанием приоритетных вызовов, что важно для экстренной службы, военных применений. Поэтому по заказу МО США разработан защищенный протокол AS-SIP [9]. Протокол AS-SIP получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP пользуется услугами почти 200 стандартов RFC.
- О перегрузках. На рис. 1 показано прохождение отдельного вызова в Системе 112. А как поступать в условиях реальных ЧП, когда из-за перегрузки имеющихся ресурсов экстренных служб часть вызовов может быть потеряна (что недопустимо)? В случаях действительно крупных ЧП в распоряжение МЧС должны были бы поступать и другие центры обработки вызовов (ЦОВ), в том числе ЦОВ «Ростелекома», что на схеме не показано.
- Не указаны средства доступа (абонентские устройства) к Системе 112, в том числе телематические средства защиты охраняемых объектов, которые также относятся к телекоммуникационной составляющей.

3 О трудностях создания сети NG9-1-1

В США экстренные вызовы обслуживаются, как известно, по номеру 911. Внедрение единого номера экстренных служб, как и в России, там сопровождается трудностями, особенно это относится к определению номера вызывающего мобильного абонента и его местоположения.

Новейшее поколение службы экстренных вызовов в США – NG9-1-1 – предполагается реализовать в IP-сети (рис. 2). Но когда это произойдет, сказать трудно. В системе NG9-1-1 требуется обеспечить возможность любых сообщений реального времени, т.е. наряду с телефонным вызовом, также передачу текста, данных, изображений и видео. Обратим внимание: на рис. 2 слева внизу отдельно указаны телематические вызовы от оберегаемого имущества. Эти вызовы относятся г области M2M-коммуникаций, в частности, к противопожарным и охранным службам. В США уже к 2008 г. были завершены пилотные проекты по проекту NG9-1-1, но широкого внедрения IP протокол не получил. Подробное описание экстренной службы NG9-1-1 содержится в документе [10] от 2007 г., где приведены диаграммы прохождения экстренного вызова через все блоки официальной модели NG9-1-1.

Рис. 2. Новое поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 911

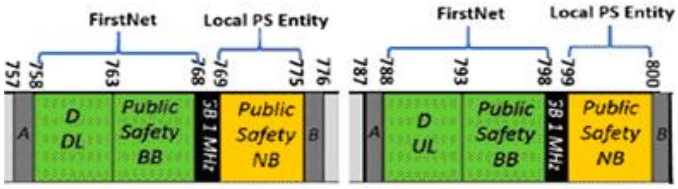

Рис. 3. Национальная сеть FirstNet в диапазоне 700 MHz

В последнее время многие обращают внимание на аналогию 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 напоминает, что оба проекта были объявлены практически одновременно – в 2007 г. [11]. 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, пусть следуя 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 похожая картина 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?

1) системный проект Системы 112 можно разработать на базе документа [10];

2) 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.

4 Планы создания сети FirstNet

В 2012 году в США создали Управление сетью первой помощи (First Responder Network Authority, FirstNet). Это управление является независимым органом в рамках Национального управления телекоммуникаций и информации. Ее цель – создать общенациональную высокоскоростную широкополосную сеть для обеспечения экстренных служб и общественной безопасности. FirstNet предоставит единую совместимую платформу пакетной коммутации и обеспечит взаимодействие с другими государственными, местными и федеральными сетями, включая существующую сеть 911 и Интернет. Сеть FirstNet должна обеспечивать защищенную передачу голоса, текстовых сообщений, изображений и видео, а также сигнализацию к базовым станциям радиосвязи в базовой сети.

О необходимости создания сети типа FirstNet заговорили сразу после терактов 2001 года в Нью-Йорке, но дело не продвигалось в течение 16 лет (!). Для сети FirstNet даже выделен общенациональный частотный ресурс в области 700 МГц (рис. 3), чтобы положить конец многолетним спорам о взаимодействии мобильных операторов связи, а также сохранить безопасность общения населения с экстренными и аварийными службами. Блоки зеленого цвета представляют собой широкополосную систему общественной безопасности (BroadBand, BB) в диапазоне от 758 МГц до 768 МГц и от 788 МГц до 798 МГц. Узкополосный (NB) спектр представлен в оранжевых цветовых блоках от 769 МГц до 775 МГц и от 799 МГц до 805 МГц. Эта часть полосы частот доступна для голосовой связи местных органов общественной безопасности. Предполагается, что сеть FirstNet будет построена по стандартам LTE. Первоначальное моделирование показало, что для покрытия не менее 99% населения и национальной системы скоростных дорог потребуется построить десятки тысяч новых базовых радиостанций.

Признавая важность предоставления эффективных услуг 911, Конгресс США ранее принял три важных закона:

1) Закон о беспроводной связи и общественной безопасности (1999 года) о едином номере 911 для вызовов чрезвычайных ситуаций и дал полномочия Федеральной комиссии связи (FCC) регулировать многие аспекты обслуживания.

2) Закон ENHANCE 911 (2004 года) – о требованиях к определению местоположения мобильных пользователей.

3) Самый последний из этих законов, Закон об усовершенствовании NET 911 (2008 года), потребовал подготовки Национального плана перехода в сети 911 на IP протокол.

К сожалению, как следует из новейшего доклада Конгрессу США [12], система 911 до сих пор пользуется инфраструктурой аналоговых технологий.

И вот только 30 марта 2017 года наступил переломный момент – последовало решение компании AT&T о создании сети FirstNet [13]. По заключенному контракту, Управление FirstNet предоставляет частотный ресурс и заплатит AT&T 6,5 млрд долл в течение следующих пяти лет. Компания же AT&T, в свою очередь, заявила, что потратит около 40 миллиардов долларов собственных денег в течение срока действия 25-летнего контракта – на строительство, развертывание, эксплуатацию и обслуживание сети. Партнерами FirstNet и AT&T являются: Motorola Solutions, General Dynamics, Sapient Consulting и Inmarsat Government. Совместными усилиями они намерены охватить все 56 территориальных объектов США: 50 штатов, пять территорий и округ Колумбия.

Для окупаемости развития мобильной сети в малонаселенных сельских районах полагается, что сеть FirstNet обеспечит, например, улучшение транспорта, образование, поиск работы, управление сельским хозяйством и лесным хозяйством, повысит эффективность муниципального управления и обеспечит экономический рост.

Мы привели столь подробные сведения о сети FirstNet, чтобы очертить тот громадный объем работ, который предстоит совершить по российской Системе 112.

5 Интерфейсы информационной сети в боевой обстановке

В 2010 г. Министерство обороны США опубликовало важнейший документ – об интерфейсах сети GIG 2.0 [14]. В нем подробно расписаны протоколы работы сети GIG в боевой обстановке, выделены четыре контрольные точки (рис. 4) и указаны протоколы, по которым должны выполняться три типа требований:

- четкое описание моделей данных: структурированных (базы данных, картографические данные, форматы документов) и неструктурированных (презентации, картины, аудио, видео), что обеспечивает их взаимодействие;
- требования к безопасности;
- требования к функциям шлюзов.

Эти требования о взаимодействии, безопасности и устройстве шлюзов, которые обмениваются информацией через контрольные точки, должны оптимизировать производительность сети и минимизировать частотный ресурс сети.

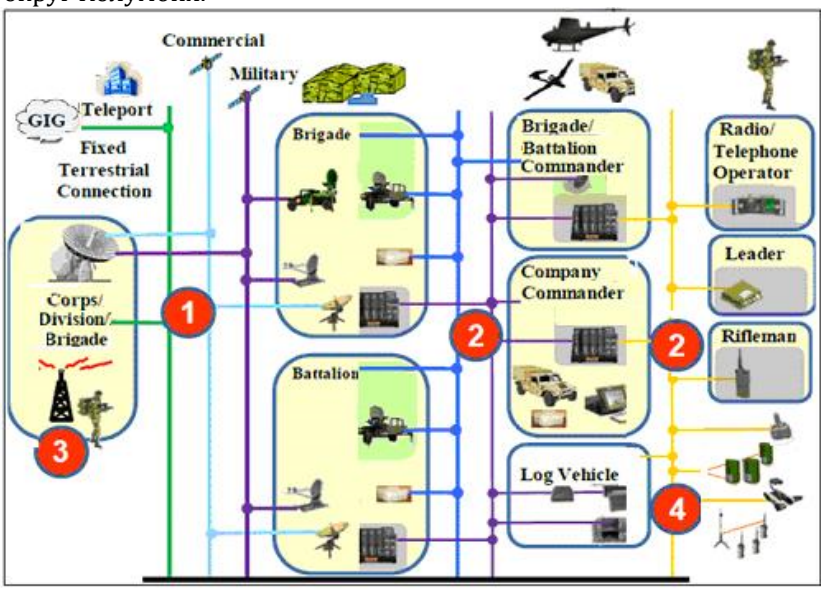

Рис. 4. Тактическая сеть GIG 2.0 и ее контрольные точки

В качестве примера опишем контрольную точку 2: это обмен данными на театре военных действий между командирами, солдатами и сенсорами. Для обеспечения взаимодействия используются:

- протоколы PKI, LDAP или Active Directory (для аутентификации);
- протокол VMF (для обмена сообщениями);
- стандарт VMF/MIL-STD 2525C (для передачи картографических данных).

Что касается безопасности, то:

- для шифрования допускаются решения, сертифицированные в NSA/NIST;
- управление ключами осуществляется по решениям EKMS/KMI,
- охрана оконечных пунктов – по Host-Based Security System (HBSS),
- управление сервисами – по Remedy/ITSM и IP Management/SPECTRUM.

Шлюзы обеспечивают трансляцию между протоколами XML/SOAP и VMF. Работа контрольных точек регламентируется длинным списком открытых и закрытых стандартов – всего на 20 страницах в документе [14].

6 Основные положения армейской информационной сети армии США

Полистаем описание архитектуры армейской информационной сети армии США [15]. Ее основная цель – обеспечивать боеспособность армии в современных условиях сете-центрической войны. В предыдущем разделе мы рассматривали архитектуру общей операционной среды (Common Operating Environment, COE) в одном частном случае – на фронте боевых действий. В документе [14] содержатся также указания разработчикам в части выбора и использования утвержденных вычислительных технологий и стандартов для обеспечения интеграции и совместимости на фронте боевых действий.

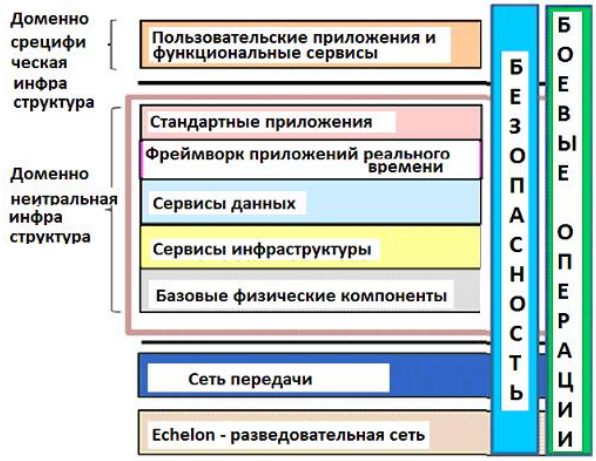

Рис. 5. Архитектура общей операционной среды COE

Рис. 5 дает общее представление о стандартных компонентах общей армейской информационной сети. Это базовая модель вычислительных средств (Computing Environments, CE). Она показывает взаимосвязь между стандартами, указанными в этом документе [15], и определяет план реализации всей сети COE.

Стандарты вида данных в общей операционной среде COE подразделяются на четыре категории, как показано на рис. 6:

1) Наиболее фундаментальными стандартами являются стандарты базовых данных (низший уровень), касающиеся шаблонов уровня битов и байтов для представления примитивной информации и структуры. Эти стандарты широко известны и используются в индустрии информационных технологий.

2) Вторая категория – стандарты данных об инфраструктуре, относящиеся к технологии и ее использованию. Эти стандарты применяются во всей сети COE и не привязаны к конкретному домену.

3) Третья категория стандартов определяет форматы обмена для информации, специфичной для использования (домена).

4) Стандарты четвертой категории определяют доступ к данным. Эти стандарты не касаются требований к информационному контенту или структурированию данных, а сосредоточены на методах доступа для извлечения данных.

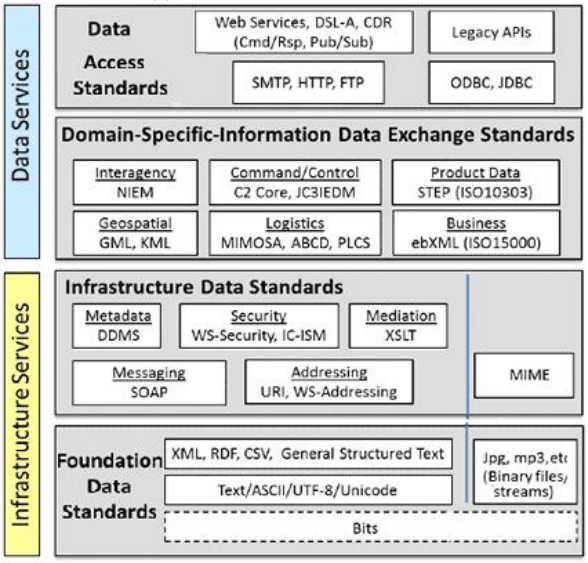

Рис. 6. Классификация стандартов работы с данными

В приложении к архитектуре армейской информационной сети [15] дана общая схема (рис. 7). Она представляет собой методическое пособие к разработке информационных сервисов и состоит из шести этапов: планирование (два этапа), сама разработка (три этапа) и внедрение (один этап).

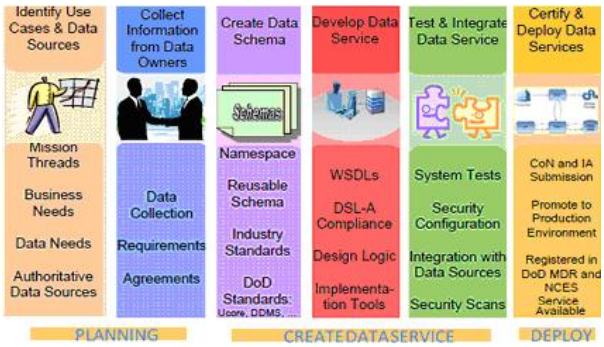

Рис. 7. Процесс разработки информационных сервисов

7 Контрольные точки в общей операционной среде армии США

Общая операционная среда (Common Operating Environment, COE) – это утвержденный набор вычислительных технологий и стандартов, которые позволяют быстро и эффективно создавать безопасные и совместимые приложения в различных вычислительных средах

Документ [16] описывает организацию разработки армейской информационной среды COE между шестью подразделениями министерства (рис. 8), отвечающими, соответственно, за разработку шести типов вычислительных средств (Computing Environments, CE):

1) Центр данных / Облако / Генерирующая сила (Data Center, DC)
2) Командные пункты (Command Post, CP)
3) Монтированное оборудование (Mounted, MC)
4) Мобильные/носимые средства (Mobile/Hand Held, MHH)
5) Датчики (Sensor)
6) Критические средства реального времени (RT/Safety Critical/Embedded, RTSCE)

Рис. 8. Общая операционная среда COE и шесть областей CE

Координация работ между этими шестью подразделениями требует очень жесткой, четко стандартизованной дисциплины. Требуется обеспечить выполнение требований по пятнадцати контрольным точкам общей операционной среды COE (рис. 9).

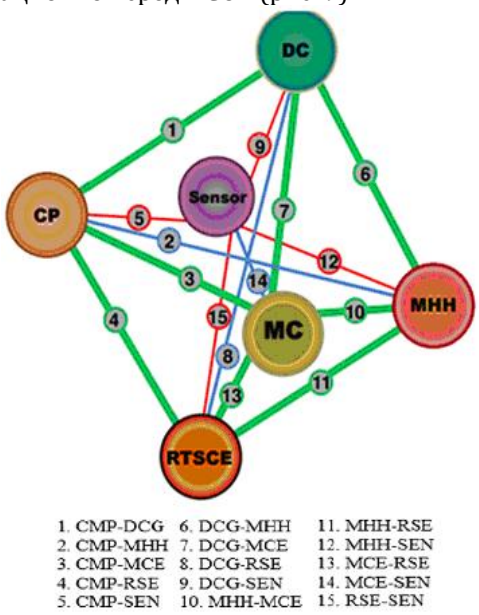

Рис. 9. Пятнадцать контрольных точек общей операционной среды COE

COE Baseline as of Jan 2012					
Governance Group	Capabilities and Critical Enablers	2012	2014	2016	2018
TAB/CCC	Common Overlay			◊	
	Access Policy Key Mngt		◊		
	Database Interoperability				◊
	Common Authentication				◊
	Single Geospatial			◊	
Data Center/ Cloud CE	Initial Limited Cloud	◊			
	IaaS			◊	
	Cloud Management Services			◊	
	Mobile Data Center		◊		
	PaaS		◊		
	SaaS			◊	
Command Post CE	Tactical Edge Mini-Cloud		◊		
	Virtualization		◊		
Mounted	Platform Services		◊		
Mobile CE	Mobile COTS Framework		◊		
RTSC CE	Interoperability Framework			◊	
Sensor CE	Data Exchange Model		◊		
	Service Framework			◊	
	Compliance Tool			◊	

Рис. 10. План внедрения средств COE (Technical Roadmap, одобрено в 2013)

На рис. 10 приводится план внедрения вычислительных средств COE. Ромбик указывает на сроки интеграции данного средства в общую операционную среду COE.

8 Трудности разработки и внедрения средств COE

В докладе [17] от 2015 года обсуждаются трудности разработки и внедрения средств COE.

Отмечается, что:

- до 2010 года разработка средств COE велась по двум параллельным, но различным направлениям инвестиций, что было неприемлемо;
- не обеспечивалась должная координация работ между шестью подразделениями по разработке средств COE.

Сложность координации работ иллюстрирует рис. 11. Там указано число разрабатываемых первичных армейских систем по подразделениям:

1) Центр данных / Облако / Генерирующая сила (DC) – 65 систем,
2) Командные пункты (CP) – 26 систем,
3) Монтированное оборудование (Mounted) – 6 систем,
4) Мобильные/носимые средства (M/HH) – 10 систем,
5) Датчики (Sensor) – 38 систем,
6) Критические средства реального времени (RTSCE) – 44 системы.

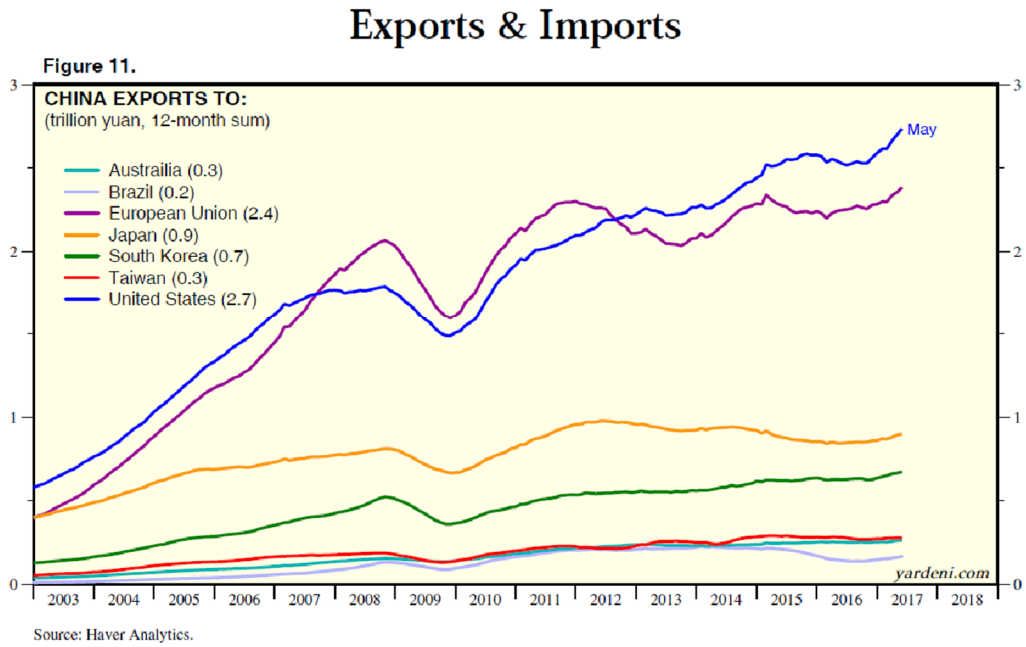

Рис. 11. Характеристика работ по разработке вычислительных средств COE (по состоянию на 28 августа 2014)

Особого внимания и координации требуют кросс-средства (Cross-Cutting Capabilities, CCC), которые необходимы для работы нескольким вычислительным средам (CE). На рис. 12 указаны пять важнейших кросс-средств.

Capability Name
Common Overlay Capability
IA Access Policy and Key Management Extension
Database Interoperability Extension
Common Authentication Capability
Single Geospatial Capability

Рис. 12. Важнейшие кросс-средства (по планам 2012)

Рис. 13 показывает состояние разработки кросс-средств CCC (по планам на август 2013). В эксплуатации находятся пять кросс-средств:

- Голосовая связь,
- Общая аутентификация,
- Аварийная сигнализация сенсоров,
- Аутентификация пользователей по паролям,
- Общая рабочая среда.

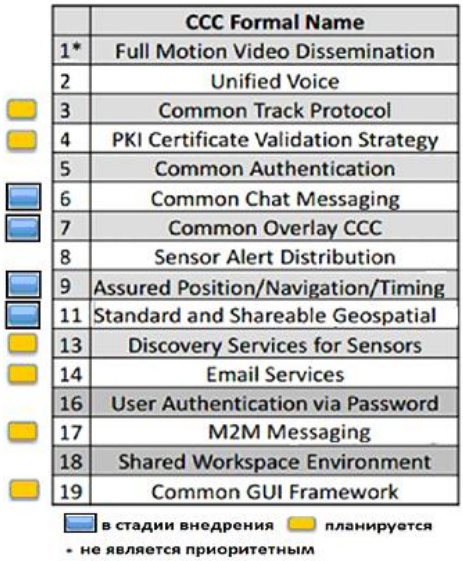

Рис. 13. План разработки кросс-средства CCC (одобрен в авг. 2013)

Четыре кросс-средства находятся в стадии разработки, а шесть кросс-средств планируются к разработке. Самое сложное средство – рассылка видеоматериалов – не является приоритетным направлением, что вызывает удивление, так как рассылка видеоматериалов является исключительно важной услугой.

Выводы

1. Телекоммуникации (информационные сети) являются решающим звеном цифровой экономики.
2. Следует разработать интерфейсы информационных сетей цифровой экономики, чтобы обеспечивать взаимодействие отдельных подсистем друг с другом.
3. При создании российской сети экстренных вызовов 112 следует учитывать опыт американских аналогов: NG9-1-1 и FirstNet.
4. Опыт США показывает, что сеть нового поколения для обслуживания экстренных вызовов NG9-1-1 имеет те же требования в части приложений, что и глобальная информационная сеть оборонного ведомства GIG (Global Information Grid).
5. Подробно рассмотрены интерфейсы сети GIG в условиях боевых действий, что следует учитывать в аналогичных российских разработках.
6. Проведенный анализ планов создания общей операционной среды армии США и выявленные при этом просчеты могут быть полезны при организации работ по созданию общей операционной среды цифровой экономики.
7. Особое внимание следует обратить на учет международных стандартов при создании информационных сетей цифровой экономики.

Литература

1. Шнепс-Шнеппе М. А., Сухомлин В. А., Намиот Д. Е. О глобальных информационных системах // International Journal of Open Information Technologies. — 2017. — Т. 5, № 4. — С. 55–62.
2. Шнепс-Шнеппе М. А. и др. Телекоммуникации как решающее звено цифровой экономики. Опыт США //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 5.
3. Соколов И.А. и др. Телекоммуникации как решающее звено цифровой экономики. Опыт России//International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6.
4. Шнепс-Шнеппе М. А., Селезнев С. П., Куприяновский В. П. Сеть DISN как прототип сети связи гражданской обороны NG112 //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 5.
5. Шнепс-Шнеппе М. А. и др. О телекоммуникационной инфраструктуре комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 6.
6. Шнепс-Шнеппе М. А. и др. К системному проектированию Системы 112 и комплекса «Безопасный город» //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 9.
7. Что мешает внедрению «Службы-112» // ИКС. 2013 ноябрь, с. 15.
8. Полканов Е.И., Мазин И.Г. Совместное использование информационных ресурсов: консолидация развития сетей // Электросвязь. 2012. № 3.
9. Department of Defense Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1, July 2013.
10. Next Generation 9-1-1 (NG9 1 1) System Initiative. Concept of Operations. The U.S. Department of Transportation. Washington D.C. Version 2. April 6, 2007
11. Schmitt M. Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE International Conference on Technologies for Homeland Security May 2008. — http://www.inl.gov/technicalpublications/ Documents/3901033.pdf Retrieved: July, 2017.
12. Lennard G. Kruger. The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress. January 26, 2017. Congressional Research Service 7-5700 www.crs.gov
13. Mike Dano FirstNet: All AT&T LTE bands to be available to public safety this year, May 1, 2017 http://www.fiercewireless.com/wireless/firstnet-all-at-t-lte-bands-to-be-available-to-public-safety-year
14. U.S. Army CIO/G-6. Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, 1 Oct 2010. [CAC required] https://www.us.army.mil/suite/doc/38201362
15. Army Information Architecture (AIA). Version 4.1, Office of the Army Chief Information Officer, 5 June 2013 https://www.us.army.mil/suite/doc/38201362
16. Engineering a Common Operating Environment for the US Army, 29 February 2012 http://www.ieee-stc.org/proceedings/2012/pdfs/2921JoyceTokar.pdf
17. Army Common Operating Environment (COE), March 11, 2015 http://www.afcea-aberdeen.org/files/presentations/AFCEA_Aberdeen_COE%20Update_11March2015.pdf.

References

1. Shneps-Shneppe M. A., Suhomlin V. A., Namiot D. E. O global'nyh informacionnyh sistemah // International Journal of Open Information Technologies. — 2017. — T. 5, # 4. — S. 55–62.
2. Shneps-Shneppe M. A. i dr. Telekommunikacii kak reshajushhee zveno cifrovoj jekonomiki. Opyt SShA //International Journal of Open Information Technologies. – 2017. – T. 5. – #. 5.
3. Sokolov I.A. i dr. Telekommunikacii kak reshajushhee zveno cifrovoj jekonomiki. Opyt Rossii//International Journal of Open Information Technologies. – 2017. – T. 5. – #. 6.
4. Shneps-Shneppe M. A., Seleznev S. P., Kuprijanovskij V. P. Set' DISN kak prototip seti svjazi grazhdanskoj oborony NG112 //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 5.

5. Shneps-Shneppe M. A. i dr. O telekommunikacionnoj infrastrukture kompleksa «Bezopasnyj gorod» //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 6.
6. Shneps-Shneppe M. A. i dr. K sistemnomu proektirovaniju Sistemy 112 i kompleksa «Bezopasnyj gorod» //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 9.
7. Chto meshaet vnedreniju «Sluzhby-112» // IKS. 2013 nojabr', s. 15.
8. Polkanov E.I., Mazin I.G. Sovmestnoe ispol'zovanie informacionnyh resursov: konsolidacija razvitija setej // Jelektrosvjaz'. 2012. # 3.
9. Department of Defense Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1, July 2013.
10. Next Generation 9-1-1 (NG9 1 1) System Initiative. Concept of Operations. The U.S. Department of Transportation. Washington D.C. Version 2. April 6, 2007
11. Schmitt M. Coordinating the Global Information Grid Initiative with the NG9-1-1 Initiative // IEEE International Conference on Technologies for Homeland Security May 2008. — http://www.inl.gov/technicalpublications/ Documents/3901033.pdf Retrieved: July, 2017.
12. Lennard G. Kruger. The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress. January 26, 2017. Congressional Research Service 7-5700 www.crs.gov
13. Mike Dano FirstNet: All AT&T LTE bands to be available to public safety this year, May 1, 2017 http://www.fiercewireless.com/wireless/firstnet-all-at-t-lte-bands-to-be-available-to-public-safety-year
14. U.S. Army CIO/G-6. Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, 1 Oct 2010. [CAC required] https://www.us.army.mil/suite/doc/38201362
15. Army Information Architecture (AIA). Version 4.1, Office of the Army Chief Information Officer, 5 June 2013 https://www.us.army.mil/suite/doc/38201362
16. Engineering a Common Operating Environment for the US Army, 29 February 2012 http://www.ieee-stc.org/proceedings/2012/pdfs/2921JoyceTokar.pdf
17. Army Common Operating Environment (COE), March 11, 2015 http://www.afcea-aberdeen.org/files/presentations/AFCEA_Aberdeen_COE%20Update_11March2015.pdf.

Поступила: 15.08.2017

Об авторах:

Шнепс-Шнеппе Манфред Александрович, доктор технических наук, профессор, генеральный директор компании ЦКБ-АбаваНет, sneps@mail.ru

Сухомлин Владимир Александрович, доктор технических наук, профессор, заведующий лабораторией открытых информационных технологий факультета вычислительной математики и кибернетики, Московский государственный университет имени М.В. Ломоносова, sukhomlin@mail.ru

Намиот Дмитрий Евгеньевич, кандидат физико-математических наук, старший научный сотрудник факультета вычислительной математики и кибернетики, Московский государственный университет имени М.В. Ломоносова, dnamiot@gmail.com

Note on the authors:

Sneps-Sneppe Manfred A., Doctor of Engineering Sciences, Full Professor, CEO of CKB-AbavaNet, sneps@mail.ru

Sukhomlin Vladimir A., Doctor of Engineering Sciences, Full Professor, head of the laboratory of open information technologies faculty of computational mathematics and Cybernetics, Lomonosov Moscow State University, sukhomlin@mail.ru

Namiot Dmitry E., PhD, Senior Researcher faculty of computational mathematics and Cybernetics, Lomonosov Moscow State University, dnamiot@gmail.com