О сложностях киберзащиты информационных систем

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

***Аннотация*— В статье рассматриваются вопросы, связанные с кибербезопасностью для информационных систем. В работе рассматриваются информационные системы, которые строятся, в основном, по модели Захмана. Основная идея модели заключается в том, чтобы обеспечить возможность последовательного описания каждого отдельного аспекта системы в координации со всеми остальными. Для любой достаточно сложной системы общее число связей, условий и правил обычно превосходит возможности для одновременного рассмотрения. В то же время отдельное, в отрыве от других, рассмотрение каждого аспекта системы чаще всего приводит к неоптимальным решениям, как в плане производительности, так и стоимости реализации. По этой модели в мире сделано множество попыток создания сложных информационных систем – от крупнейших корпораций до электронных правительств. В данной статье в качестве примера выбрали проект модернизации управления киберзащитой сети DISN (Defense Information System Network) МО США. Также в работе рассматривается язык SysML - клон языка UML, позволяющий проектировать программно-аппаратные комплексы. Рассмотрение касается новых диаграмм из спецификацию этого языка: требований, внешних и внутренних блоков, времени, параметрической.**

***Ключевые слова*—цифровая экономика, кибербезопасность, информационные системы.**

I. Введение

Настоящая работа является продолжением наших предложений по цифровой экономике России [1] и связана с обсуждением сложностей разработки программного обеспечения информационных систем.

Начнем с примера - весьма характерного для сложных информационных систем, которые в мире уже более 30 лет строятся, в основном, по модели Захмана [2], которая, в свою очередь, восходит к компании IBM. По модели Захмана в мире сделано множество попыток создания сложных информационных систем – от крупнейших корпораций до так называемых электронных правительств. В качестве примера мы выбрали проект модернизации управления киберзащитой сети DISN (Defense Information System Network) МО США. Выбрали в силу того, что этот проект строится за счет налогоплательщиков и поэтому имеет достаточно много открытой информации. К тому же он контролируется Счетной палатой США (Government Accountability Office, GAO), отчеты которой также имеются в открытом доступе.

Приводим краткую историю вопроса.

Июнь 2012 года. Компания Lockheed Martin выиграла крупнейший тендер на разработку ИТ-сервисов управления сетью DISN (Global Services Management-Operations, GSM-O). Суть контракта GSM-O состоит в модернизации системы управления сетью DISN по требованиям киберзащиты. Стоимость работ составляет громадную сумму – 4.6 млрд. долл. в течение 7 лет.

В 2013 году команда GSM-O приступила к изучению состояния четырех 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 (рис. 1).

Рис. 1. Проект GSM-O по модернизации управления сетью DISN.

2015 год. Через два года мир телекоммуникаций потрясла новость [3]: Lockheed Martin не справляется с модернизацией управления сетью DISN, то есть с выполнением многомиллиардного контракта GSM-O, и свое подразделение LM Information and Global Solutions продает конкурирующей фирме Leidos. Провалом работ, скорее всего, послужила неспособность набрать разработчиков, способных сочетать «старое»

Статья получена 21 апреля 2018.
М.А. Шнепс-Шнеппе - AbavaNet (email: sneps@mail.ru)
В.А. Сухомлин - Московский Государственный Университет имени М.В. Ломоносова (e-mail: sukhomlin@mail.ru)
Д.Е. Намиот - Московский Государственный Университет имени М.В. Ломоносова (e-mail: dnamiot@gmail.com)

оборудование коммутации каналов с новейшими системами пакетной коммутации, тем более с учетом требований недавно созданного Киберкомандования Пентагона, в частности, с подключением сложнейшего (но еще недоработанного) оборудования киберзащиты - стеков JRSS (Joint Regional Security Stacks).

Июль 2016. Появляется отчет Счетной палатой США GAO-16-593 [4], требующий усиления контроля над расходованием средств по создания Единой информационной среды (Joint Information Environment, JIE) МО США. В отчете GAO указано: «Министерство обороны (DOD) планирует потратить почти 1 миллиард долларов к концу этого финансового года для внедрения всего лишь одного элемента JIE; однако отдел не полностью определил сферу охвата JIE или ожидаемую ее стоимость. Должностные лица сообщили, что оценка стоимости JIE является сложной из-за размера и сложности инфраструктуры отдела и подхода к внедрению JIE. Однако, без информации об ожидаемых расходах JIE, способность чиновников контролировать и принимать эффективные решения о ресурсах ограничена».

Ноябрь 2016. Начальник ИТ-отдела Министерство обороны Терри Халворсен идет в наступление на Счетную палату [5], мол, они не понимают, что такое Joint Information Environment: «То, что мы пытались сказать GAO, заключается в том, что в данном случае не следует измерять JIE - вам следует измерять ее компоненты».

JIE, по его словам, является концептуальным термином, используемым для описания модернизированной инфраструктуры ИТ-инфраструктуры DOD, а не одной программы. Скорее, JIE состоит из различных программ, таких как стеки безопасности JRSS и среды стран-партнеров. Например, JRSS нацелен на консолидацию 1000 устаревших сетевых стеков безопасности в 48 стандартизированных стеков в 25 точках мира. По словам Халворсена, существуют определенные показатели для измерения их эффективности.

Февраль 2017. Ответ не удовлетворил чиновников Счетной палаты, и начальник ИТ-отдела Халворсен подал в отставку (ныне занимает пост менеджера в компании Самсунг).

Январь 2018. В январе Главный контроллер вооружения Пентагона в Годовом отчете сказал, что МО должно прекратить развертывание своей новой сетевой платформы безопасности JRSS, пока JRSS не продемонстрирует, что она способна помочь защитникам сети обнаруживать и оперативно реагировать на реальные кибератаки.

Февраль 2018. Руководство Пентагона не сдается [6]: 27 февраля, выступая на Конференции по кибербезопасности, заместитель министра обороны Эсси Миллер сказал, что программа по установке оборудования JRSS уже более чем наполовину завершена. Миллер сказал, что установлено 14 из 25 стеков безопасности, запланированных по всей сети в США, Европе, а также в тихоокеанских и юго-западных регионах Азии. Эту программу завершат к концу 2019 года. Также планируется еще 25 стеков для секретных сетей.

Еще раз были подчеркнуты огромные масштабы деятельности JIE [7]. Эта среда включает в себя 65 000 американских серверов и 7 миллионов оконечных точек - все они размещены в 15 000 различных сетях, используемых 1,3 миллионами военнослужащих и 742 000 гражданских лиц, которые базируются на более чем 555 000 объектах, разбросанных по всему земному шару.

Итак, Пентагон продолжает тратить свой многомиллиардный бюджет на развитие ИТ-инфраструктуры.

Далее, в Разделе 2 мы поясняем суть модели Захмана, а в разделе 3 - что такое единая информационная среда JIE. Разделы 4-6 посвящены описанию сети DISN: ее наземному сегменту, целевой архитектуре и программному коммутатору MFSS – как основе перехода к сети коммутации пакетов. Оборудование киберзащиты JRSS и трудности его внедрения описаны в разделе 7. Разделы 8 и 9 посвящены программному обеспечению JIE.

II. Модель Захмана

В 1987 г. появилась статья Дж. А. Захмана «Структура архитектуры информационных систем» и впервые было введено понятие «архитектура предприятия» [1]. Джон Захман много лет занимался внедрением информационных систем IBM и переосмыслил их архитектуру. Он стал «отцом» архитектуры предприятия (Enterprise Architecture).

Основная идея модели заключается в том, чтобы обеспечить возможность последовательного описания каждого отдельного аспекта системы в координации со всеми остальными [8]. Для любой достаточно сложной системы общее число связей, условий и правил обычно превосходит возможности для одновременного рассмотрения. В то же время отдельное, в отрыве от других, рассмотрение каждого аспекта системы чаще всего приводит к неоптимальным решениям, как в плане производительности, так и стоимости реализации.

Собственно, модель представляется в виде таблицы, имеющей пять строк и шесть столбцов, которая приведена на рис. 2.

Рис. 2. Модель Захмана

Первые три уровня формируют бизнес-руководители.

Первая строка соответствует уровню планирования бизнеса в целом (бизнес-модель). На этом уровне вводятся достаточно общие основные понятия, определяющие саму суть бизнеса (продукты, услуги, клиенты), а также формулируется бизнес-стратегия.

Вторая строка (концептуальная модель) предназначена для определения (в терминах менеджеров) структуры организации, ключевых и вспомогательных бизнес-процессов.

Третий уровень (логическая модель) соответствует рассмотрению с точки зрения системного архитектора. Описываются типы данных, правила их преобразования и обработки для выполнения бизнес-функций.

Уровни с четвертого и далее описывают детали, которые представляют интерес для ИТ-менеджеров и проектировщиков, но ведущую роль играют разработчики.

На четвертом уровне — технологической (физической) модели — осуществляется привязка данных и операций над ними к выбранным технологиям реализации. Например, выбор реляционной СУБД, средств работы с неструктурированными данными или объектно-ориентированной среды.

Пятый уровень соответствует детальной реализации системы, включая конкретные модели оборудования, топологию сети, производителя и версию СУБД, средства разработки и собственно готовый программный код.

Шестой уровень описывает работающую систему: инструкции для работы с системой, фактические базы данных, работу службы HelpDesk и т.д.

III. Что такое единая информационная среда JIE

Единая информационная среда GIG представлена в виде семиуровневой модели (рис. 3) [9]. К данному моменту она стандартизована только частично. Принято решение в части единых сетей связи (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 Услуги распределения информации. Наиболее важной и трудоемкой работой при создании Единой информационной среды является стандартизация уровня приложений (Ведомственные и приложения COI, Community-of-Interest). Уровни от 2го до 4го предоставляют промежуточные сервисы CES (Core Enterprise Services).

Рис. 3. Целевая архитектура единой информационной среды JIE.

Следуя модели Захмана, строится метамодель DoDAF (Department of Defense Meta-Model) [10]. Она разрабатывается с 1990 г. На рис. 4 дана версия 2.0 (разрабатывается с 2009 г.). Рисунок иллюстрирует взаимосвязи между основными понятиями метамодели DoDAF.

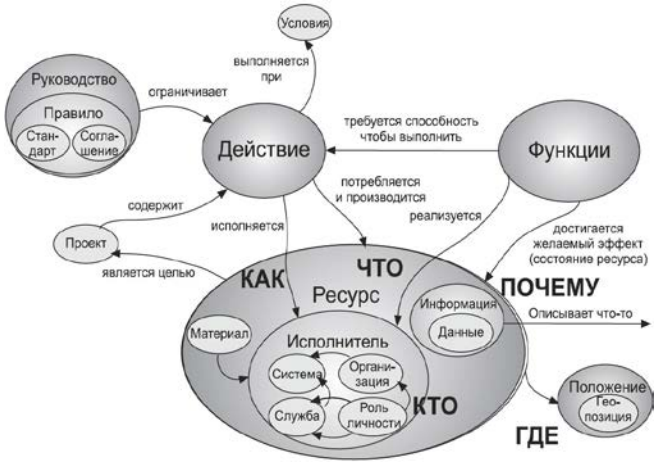

Рис. 4. Иллюстрация метамодели JIE.

Модель содержит шесть описаний, которые объединены ключевым понятием Действие:

1. Описание данных (Data Description) — отвечает на вопрос ЧТО;
2. Описание функции (Function Description) — отвечает на вопрос КАК (содержит также описание Исполнителя), который выполняет Функции;
3. Описание сети (Network Description) — ГДЕ;
4. Описание участников (People Description) — КТО (что включает Организации);
5. Описание времени (Time Description) — КОГДА;
6. Описание мотивации (Motivation Description) —

ПОЧЕМУ.

Документация по Единой информационной среды JIE состоит из 52 томов и представлена с восьми точек зрения (Viewpoint) [11]:

- 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.

IV. Наземный сегмент DISN

Строительство наземного сегмента сети DISN завершена. Это – глобальная система наземных ВОЛС (волоконно-оптических линий связи), получившая название DISN-Core. Эти кабели обеспечивают поток данных в 10 Гб/с между любыми базами НАТО. Планируется скорость передачи увеличить до 100 Гб/с.

DISN-Core начали строить в 2004 году. Это было расширение 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 "каждой военной базе свой цвет". Каждый узел на сети имеет аппаратуру OC-192 (10 Гб/с). Конечная (будущая) цель проекта GIG-BE – довести пропускную способность GIG до 100 Гб/с.

Программа GIG-BE является одним дорогостоящим, но довольно простым шагом в программе перехода DISN на сплошную IP технологию из-конца-в-конец.

V. Целевая архитектура сети DISN

В настоящее время строится новая сеть DISN. Это – сеть коммутация пакетов (по протоколам IP). Ее целевая архитектура содержит два уровня: Tier 0 и Tier 1. Кластер Tier 0 отвечает за неуязвимость всей сети DISN. Он содержит три софтсвича (маршрутизаторы) уровня Tier 0, соединенных 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 содержимым 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. Тем самым защищенная гибридная сеть DISN обеспечивает передачу голоса и видео по протоколу IP (Voice and Video over Internet protocol, CVVoIP).

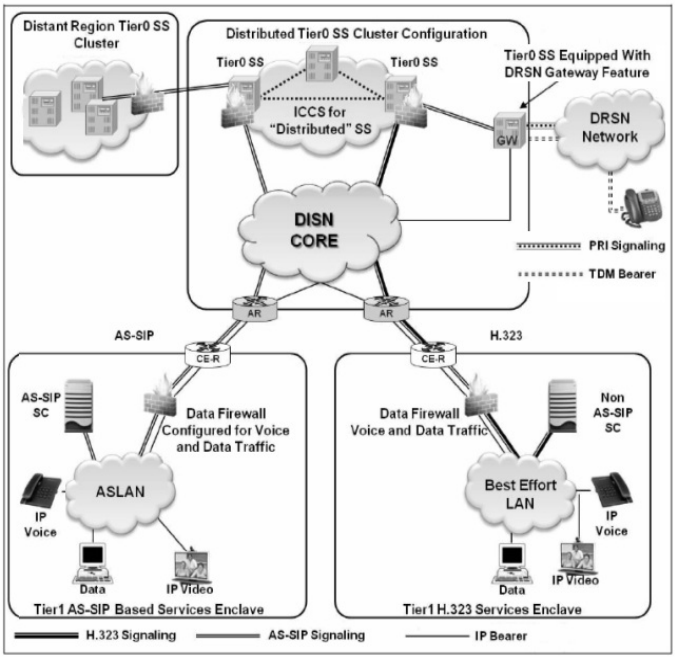

Рис. 5. Целевая архитектура сети связи DISN.

Своеобразным «родимым пятном» сети DISN, строящейся по единому протоколу AS-SIP, является сверхсекретная правительственная связь DRSN (Defense RED Switch Network), которая сохраняет технологию коммутацию каналов, точнее, ISDN каналы и протоколы сигнализации ISDN PRI и CAS (Channel Associated Signaling). В методических материалах по DISN [12] не предусмотрен перевод сети DRSN на коммутацию пакетов.

VI. MFSS - основа перехода к сети коммутации пакетов

Переход от сети коммутации каналов, где ныне господствует протокол SS7, к коммутации пакетов и протоколу SIP (или к его защищенной версии AS-SIP) требует установки шлюзов - программных коммутаторов SoftSwitch [13]. Программные коммутаторы (маршрутизаторы) становятся основным элементом архитектуры сети связи DISN.

Компании CISCO – крупнейшей подрядчик Пентагона - устанавлила 22 крупных программных коммутаторов (Softswitch) на военных базах по всему миру. Имеются два типа софтсвичей верхнего уровня: WAN SS = Wide Area Network SoftSwitch, MFSS = MultiFunction SoftSwitch. На рис 6 указаны так же четыре центра управления сетью (Global Network Support Center, GNSC) – два в США (на авиабазе Scott и на Гавайях), в Германии и Бахрейне, о чем речь шла в начале статьи.

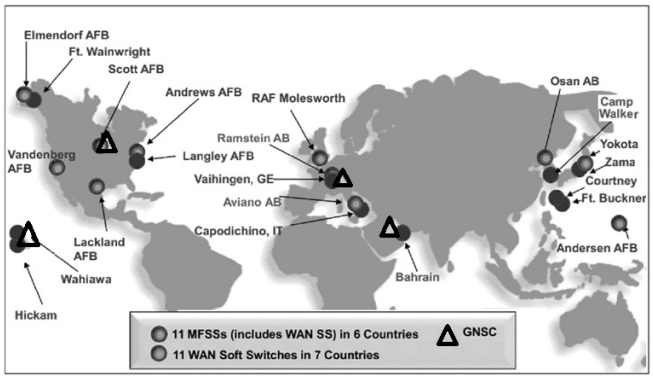

Рис. 6. Планы по установке 22 крупных программируемых коммутаторов (Softswitch) [14].

VII. Оборудование киберзащиты JRSS

Основная задача Киберкомандования Пентагона состоит в обеспечении кибербезопасности Единой информационной среды JIE, и в этом ключевую роль играют региональные стеки безопасности (Joint Regional Security Stacks, JRSS). Оборудование JRSS, по сути, представляют собой IP-маршрутизаторы со сложным комплексом программ киберзащиты.

В настоящее время устанавливаются стеки JRSS для сети NIPRNet (Non-classified Internet Protocol Router Network). Это — сеть, используемая для обмена несекретной, но важной служебной информацией между «внутренними» пользователями. Планируется установка стеков и для сети SIPRNet (Secret Internet Protocol Router Network). Это — система взаимосвязанных компьютерных сетей, используемых МО для передачи секретной информации по протоколам TCP/IP.

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. 7). Состояние дел по контракту GSM-O на 2014 год хорошо изложено в статье [15].

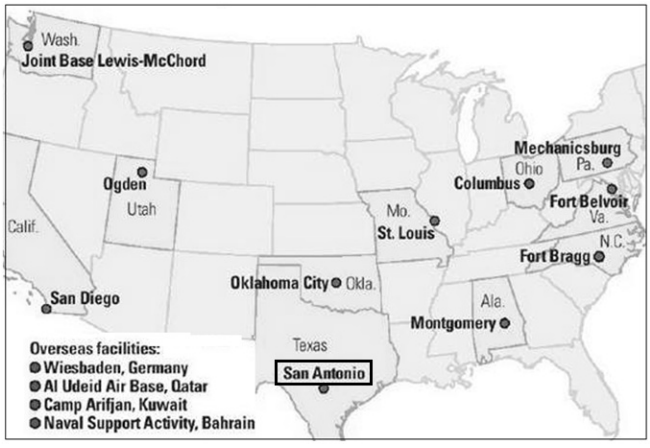

Рис. 7. Состояние работ по установке стеков JRSS на территории США (2014) [16].

Общий объем работ включает установку 24 стеков JRSS на служебной сети NIPRNet и 25 стеков JRSS на секретной сети SIPRNet (рис. 8). К 2019 году планируется на эти стеки перенести программы кибербезопасности, которые сейчас размещены в более чем 400 местах.

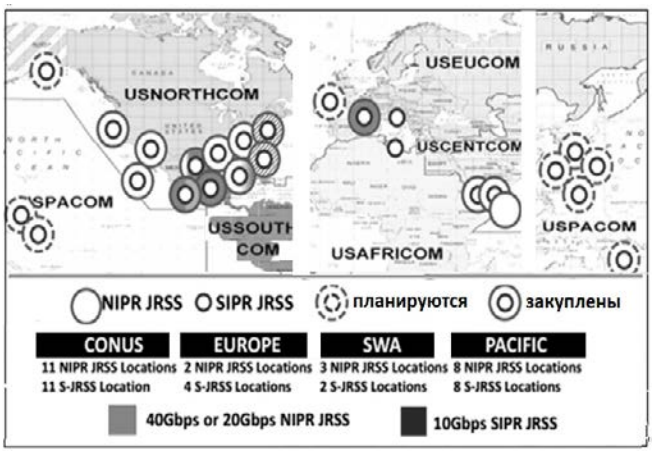

Рис. 8. Карта установки стеков JRSS [17].

Уже разработано несколько версий программного обеспечения JRSS. Представление о сложности задач киберзащиты дает рис. 9.

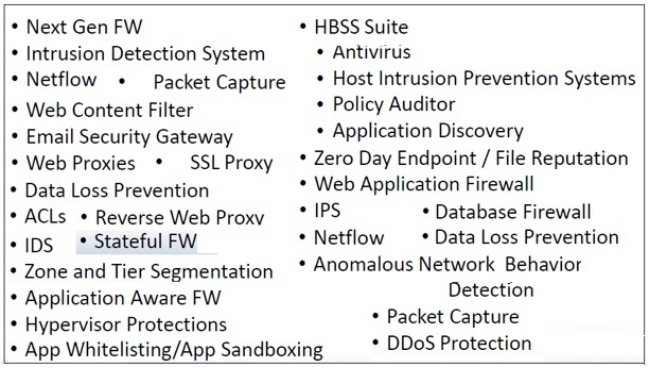

Рис. 9. Средства киберзащиты в сети SIPRNet в соответствии с единой архитектурой безопасности [18].

Будут ли грандиозные планы Пентагона выполнены? Сложность задачи, в частности, характеризует набор требований к потенциальным разработчикам JRSS, которые перечислены в приглашениях на работу компанией Leidos [19]. Требуется опыт работы в течение 12-14 лет и знания, по крайней мере, двух или более продуктов компаний ArcSight, TippingPoint, Sourcefire, Argus, Bro, Fidelis XPS, Niksun FPCAP, Lancope, NetCool, InfoVista и Riverbed. Заметим, что каждая из этих компаний предоставляет свой сложный комплекс средств киберзащиты. Как их обэъединить?

Напоминаем претензии Счетной палаты к состоянию дел по JIE и JRSS (из упомянутого выше отчета GAO-16-593):

- Учитывая текущие опасения по поводу кибербезопасности, а также обширную ИТ-инфраструктуру DOD и бюджет на ИТ-инфраструктуру в размере 38 млрд. долларов, важно, чтобы DOD добился успехов в достижении цели JIE.
- В ответ на нашу рекомендацию DOD заявила, что к

декабрю 2016 года она представит смету расходов и исходные данные по оборудованию JRSS. Однако, DOD этого не сделал, но поскольку JRSS является ключевым компонентом JIE, неясно, как в отделе будет разработана надежная общая оценка стоимости JIE.

• Заключение. Без стратегии, которая идентифицирует ресурсы, необходимые для выполнения стратегии JIE, и графика завершения оценки, Счетная палата не имеет уверенности в том, что необходимые оценки будут завершены.

VIII. О программном обеспечении JIE

Программное обеспечение JIE строится по идеологии сервис-ориентированная архитектура SOA (Service Orieted Architecture). Сервис-ориентированная архитектура — это модульный подход к разработке программного обеспечения, основанный на использовании распределённых, слабо связанных заменяемых компонентов, оснащённых стандартизованными интерфейсами для взаимодействия по стандартизованным протоколам (рис. 10).

Архитектура SOA не привязана к какой-то определённой технологии. Она может быть реализована с использованием широкого спектра технологий, включая такие технологии как REST, RPC, DCOM, CORBA или веб-сервисы. Главное, что отличает архитектуру SOA — это использование независимых сервисов с чётко определёнными интерфейсами, которые для выполнения своих задач могут быть вызваны неким стандартным способом. К тому же, эти сервисы заранее ничего не знают о приложении, которое их вызовет, а приложение не знает, каким образом сервисы выполняют свою задачу.

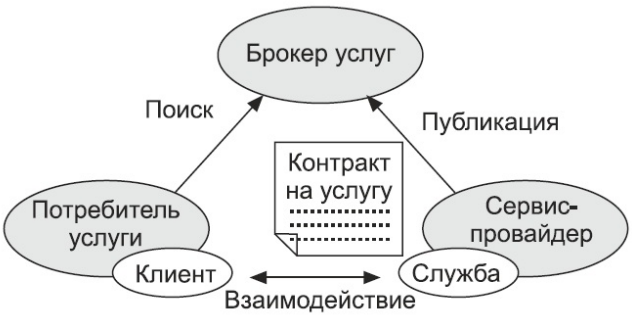

Рис. 10. Основная схема сервис-ориентированной архитектуры.

Комплекс программного обеспечения JIE позволяет участникам боевых действий и специалистам по анализу информации упростить доступ к информационным сетям МО и разведывательного сообщества США для целенаправленного поиска и совместного использования данных о состоянии сил, средств и ресурсов, а также о вероятных намерениях и действиях противника вне зависимости от их принадлежности к конкретной организационной структуре вида ВС или какому-либо роду войск.

Рис. 11. Организация программного обеспечения в сервис-ориентированной архитектуре DISN.

Инфраструктура SOA основана на девяти службах (см. в центре рис. 11):

служба сетевого управления информационным пространством DISN;

служба обмена сообщениями;

служба поиска информации;

служба посреднических услуг;

служба координации, предоставляющая набор средств, благодаря которым пользователи могут работать коллективно и в совместном режиме использовать отдельные возможности в сети;

служба хранения данных;

служба приложений, предназначенная для организации инфраструктуры и обеспечения возможностей по распределенной обработке данных в темпе их поступления (режим онлайновой обработки);

служба обеспечения безопасности информации;

служба непосредственной поддержки пользователя.

Кроме перечисленных девяти служб SOA, которые являются базовыми для программирования приложений, имеются небольшие промежуточные сервисы CES (Core Enterprise Services). Их более 9 групп. Они облегчают программирование приложений для четырех областей:

• Warfighter (планирование военных операций),

• Business (управление финансами, человеческими ресурсами, медицинскими службами и др.),

• Defense Intelligence (разведка) и

• Network Operations (управление боевыми действиями).

Инфраструктура SOA и базовые сервисы CES следуют точным определениям и стандартам, что должно обеспечить согласованность сетей и программ (если, конечно, программисты справятся с таким колоссальным объемом работ).

IX. 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)

[20].

Язык UML давно уже стал стандартом общения между участниками разработки программного обеспечения 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. Исходных средств языка UML оказалось недостаточно для моделирования аппаратуры, поэтому 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. 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. 12. Процесс разработки новейшей версии GIG по модели MBSE [21].

Общие требования DISA к разработке концепции GIG трудно представить одним рисунком. 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 (рис. 12).

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 плана развития GIG, по документации MBSE можно моделировать систему, изучать ее производительность, даже генерировать исполнимый код.

Библиография

[1] Sneps-Sneppe, Manfred, Vladimir Sukhomlin, and Dmitry Namiot. "On the Program" Digital Economy of the Russian Federation": how to create an Information Infrastructure." International Journal of Open Information Technologies 6.3 (2018): 37-48.

[2] John A. Zachman (1987). "A Framework for Information Systems Architecture". In: IBM Systems Journal, vol 26, no 3.

[3] Leidos-Lockheed merger changes the face of federal IT https://www.federaltimes.com/it-networks/2016/02/05/leidos-lockheed-merger-changes-the-face-of-federal-it/ Retrieved: May, 2018

[4] Joint Information Environment: DOD Needs to Strengthen Governance and Management. GAO-16-593: Published: Jul 14, 2016

[5] Pentagon Tech Chief Says He'll 'Take the Hit' for GAO Criticism of JIE. Nov 02, 2016 http://www.nextgov.com/cio-briefing/2016/11/pentagon-tech-chief-says-hell-take-hit-gao-criticism-jie/132882/ Retrieved: May, 2018

[6] DOD CIO: JRSS set for 2019 completion. Mar 05, 2018 https://fcw.com/articles/2018/03/05/jrss-completion-miller.aspx Retrieved: May, 2018

[7] The Department of Defense. Strategy for Implementing the Joint Information Environment. Sept 18, 2013.

[8] С. Карпенко. Применение модели Захмана для проектирования ИТ-архитектуры предприятия. http://www.management.com.ua/ims/ims177.html
[9] D. DeVries. DoD Joint Information Enterprise. http://c4i.gmu.edu/eventsInfo/reviews/2013/pdfs/AFCEA2013-DeVries.pdf Retrieved: May, 2018
[10] Department of Defense. Information Enterprise Architecture (DoD IEA). Version 2.0. Volume II – IEA Description, July 2012.
[11] DODAF http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf Retrieved: May, 2018
[12] Department of Defense. Unified Capabilities Framework 2013. January 2013.
[13] Department of Defense. Unified Capabilities Master Plan. October 2011.
[14] Cisco LSC https://www.cisco.com/web/strategy/docs/gov/Cisco_LSC_Overview_Jan2011.pdf Retrieved: May, 2018
[15] S. Meloni. The Future of the Joint Information Environment (JIE), SEPT 24, 2014 http://blog.immixgroup.com/2014/09/24/the-futureof-the-joint-information-environment-jie Retrieved: May, 2018
[16] The JRSS program is underway, Oct. 1, 2014 http://archive.c4isrnet.com/article/20141001/C4ISRNET12/310010005/The-JRSS-program-underway Retrieved: May, 2018
[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 Retrieved: May, 2018
[18] D. Metz. Joint Information Environment Single Security Architecture (JIE SSA), 12 May 2014.
[19] Cyber Systems Training Support Engineer – JRSS https://www.energyjobline.com/job/571137/cyber-systems-training-support-engineer-jrss/ Retrieved: May, 2018
[20] Николаев А., Зыль С. Визуальное проектирование на основе SysML//Открытые системы. – 2006. – № 05.
[21] DISA. Global Information Grid (GIG) Convergence Master Plan (GCMP), Vol. 1, 02 August 2012

On the complexities of cyberprotection of information systems

Manfred Sneps-Sneppe, Vladimir Sukhomlin, Dmitry Namiot

***Abstract*— The article deals with issues related to cybersecurity for information systems. In this paper, information systems are considered, which are built, basically, according to the Zachman model. The main idea of the model is to provide the possibility of sequential description of each individual aspect of the system in coordination with all the others. For any sufficiently complex system, the total number of links, conditions, and rules usually exceeds the possibilities for simultaneous consideration. At the same time, separate, in isolation from others, consideration of each aspect of the system often leads to suboptimal decisions, both in terms of productivity and the cost of implementation. According to this model, many attempts have been made in the world to create complex information systems - from the largest corporations to electronic governments. In this article, as an example, the project of modernization of the management of cyber defense of the DISN network (Defense Information System Network) of the US Defense Ministry was chosen. Also in the work, the language SysML is considered. It is a clone of the UML language, which allows designing hardware and software systems. Consideration concerns new diagrams from the specification of this language: requirements, external and internal blocks, time, parametric.**

***Keywords*— digital economy, cybersecurity, information systems.**