# От каналов к пакетам: выполнима ли миссия?

М.А. Шнепс-Шнеппе

***Аннотация*— Противостояние двух технологий – коммутации пакетов и коммутации каналов – имеет давнюю историю и, кажется, в обозримом будущем не прекратится. Эта проблема обсуждается на примерах из двух социально значимых сфер США: экстренной службы и оборонных информационных систем, а также из области микроэлектроники (network-on-a-chip). Изложена история неудачных попыток перехода на пакетную коммутацию в области экстренных служб. Подобные провалы с переходом на пакетную коммутацию в области оборонных информационных систем уже случались, а именно: была сохранена технология ISDN в правительственной сети Defense Red Switch Network и гибридная технология ATM в информационных сетях разведки JWICS и управления спутниками AFSCN; произошел провал программы создания стеков безопасности JRSS в сетях электронной почты NIPRNet и SIPRNet; приостановлена программа Joint Strike Fighter из-за киберуязвимостей в программном обеспечении самолета F-35 Lightning II. Использованы исключительно открытые источники.**

**В итоге можно высказать предположение, что в плане создания сложных систем, основанных на IP-протоколах и к тому же кибернеуязвимых, человечество достигло пределов возможного. Что пришло время осмыслить целесообразность самого лозунга «Everything over Internet Protocol» и искать решения совместной работы двух технологий — коммутации пакетов и коммутации каналов.**

***Ключевые слова*— военные телекоммуникации, интернет-протокол, кибербезопасность, экстренные службы**

*Вавилонская башня осталась недостроенной (Питер Брейгель Старший. 1563)*

## I. Введение

Перед связистами всего мира стоит одна и та же задача – как перейти от коммутации каналов (КК) к коммутации пакетов (КП), как реализовать лозунг «Everything over Internet Protocol». Это означает смену научной парадигмы, то есть принятая научным сообществом новой модели развития телекоммуникаций. Каков будет исход противостояния «КК против КП»? На этот вопрос пока нет окончательного ответа. Пока не ясно – выполнима ли миссия, т.е. удастся ли сменить базовую парадигму телекоммуникаций. Поиску ответа на этот вопрос и посвящена данная статья.

Смена парадигмы – событие революционное, и, дабы понять суть происходящего, бросим взгляд на историю вопроса.

*Как противостояние началось.* Ключевым моментом можно признать создание сети ARPANET и работы профессора Леонарда Клейнрока. В 1961 году он описал технологию разделения файлов на фрагменты (пакеты) и их передачу по сети различными маршрутами. Новую технологию он описал в книге «Communication Nets», 1964 (на русском: Коммуникационные сети, 1970). В ней изложены основные принципы коммутации пакетов, лежащие в основе современных Интернет-технологий. Первое электронное сообщение между двумя компьютерами (между Калифорнийским университетом и Стэнфордским институтом) было отправлено в 1969 году с использованием протокола ARPANET. Пентагон (точнее, Агентство перспективных оборонных исследовательских проектов, DARPA) заинтересовался экспериментом ARPANET и заказал компьютерную сеть для условий ядерной войны. Сеть должна была обеспечивать связь между командными пунктами обороны США во время войны и должна была оставаться в рабочем состоянии, даже если часть командных пунктов будет уничтожена.

Пентагон способствовал стремительному росту средств Интернета. Операторы связи и, что более важно, производители оборудования взяли ориентацию на «Everything over Internet Protocol», тем самым ущемляя развитие традиционных средств коммутации каналов. Закату интереса к КК способствовал также начатый в 1974 году Министерством юстиции США антимонопольный иск против AT&T, ведущей компании в корпорации Bell Systems. После восьмилетнего судебного разбирательства, 8 января 1982 года произошел принудительный распад Bell Systems. Тем самым распался и самый выдающийся в мире институт Bell Laboratories. Заметим, что ученым Bell Laboratories принадлежит ряд самых важных изобретений двадцатого века, включая мобильные сети, цифровые телефонные станции, волоконную оптику, лазеры, транзисторы, солнечные батареи, спутниковую связь, подводные кабели, операционную систему UNIX. За работы, проделанные в Bell Laboratories, присуждено девять Нобелевских премий.

Статья получена 12 мая 2022.

М.А. Шнепс-Шнеппе - Вентспилская Высшая Школа, Латвия (email: manfreds.sneps@gmail.com). ORCID: 0000-0002-0672-8321

.

*Как работает телефонная станция.* Старшее поколение связистов помнит электромеханические автоматические телефонные станции АТС (Crossbar Switch), которые были построены на координатных соединителях или герконовых матрицах. Разговорный канал в таких АТС образовывался из фрагментов в громоздком коммутационном поле (рис. 1), и оборудование больших АТС занимало площадь баскетбольного поля.

С переходом от аналоговой передачи речи на цифровую (8000 отсчетов по одному байту в секунду, т.е. 64 Кб/с) объем оборудования резко сокращается. На входы электронного коммутационного поля поступают потоки цифр 2048 Кб/с, в котором размещены 32 речевых потока по 64 Кб/с каждый. Это называется режимом временного уплотнения (Time Division Multiplexing, TDM), и суть коммутации состоит в перемещения байтов из одной временной позиции в другую.

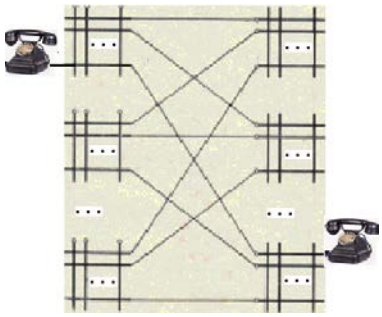

Рис. 1: Пример двухкаскадного координатного коммутатора АТС.

*Сигнализация SS7.* Высшим достижением эпохи коммутации каналов стало внедрение системы сигнализации SS7. Это – своеобразная сеть пакетной коммутации над сетью коммутации каналов, что ускоряет процесс установления соединения, а главное – служит основой построения интеллектуальных сетей связи и предоставления широкого набора дополнительных услуг (рис. 2).

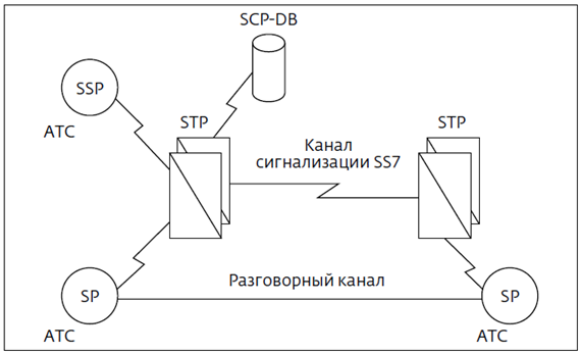


Рис. 2: Базовая архитектура сети SS7. Обозначения: DB = База данных, SSP = Service Switching Point (узел коммутации услуг), SCP = Service Control Point (контроллер услуг), SP = Signaling Point, STP = Signaling Transfer Point (SP и STP относятся к установлению соединения)

Заметим, что, с ликвидацией корпорации Bell Systems и стремительным ростом Интернета, остался незамеченным один важный, как осознается сегодня, вопрос – вопрос живучести сети SS7 (рис. 3). Между АТС имеется множество связей по сети SS7, что обеспечивает высокую живучесть телефонной сети США, и тем самым вряд ли она была бы менее живучей (в случае атомной войны), чем сеть Интернета. Не говоря о киберуязвимости сети коммутации пакетов (большей, чем при коммутации каналов), что становится очевидным только в последние годы.

*Основные особенности КК и КП.* Алгоритм коммутации каналов является более простым, чем коммутации пакетов, но проигрывает в эффективности использования каналов (проигрывает, правда, не всегда). Поясним это. При коммутации каналов физический канал (от входа в сеть до выхода из нее) резервируется перед началом передачи данных, то есть заголовок сообщения (телефонный номер вызываемого абонениа), проходя сеть, резервирует (занимает) путь, по которому будет передано сообщение. Отсюда получаем основную выгоду – низкую задержку передачи сообщения после занятия канала. Но имеются отрицательные свойства: (1) путь продолжает остается недоступным на фазе занятия и на некоторое время после завершения передачи и (2) сеть в режиме КК недостаточно гибка к масштабированию сети.

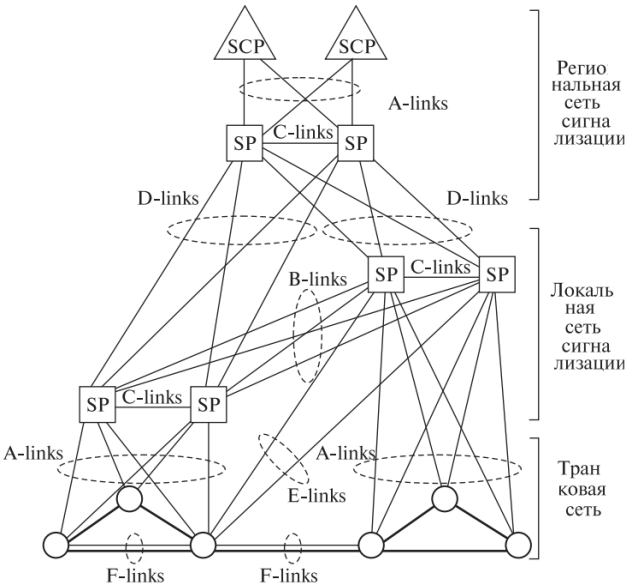


Рис. 3: Полный вариант сети SS7 (Bellcore Notes on the Networks. Bellcore, SR-2275, Dec 1997).

Что происходит в режиме коммутации пакетов? Пакеты могут передаваться разными путями и могут приходить с разными задержками. Из-за нулевого времени начала передачи и меняющейся задержки возникают коллизии в маршрутизаторах, тем самым трудно обеспечить требуемое качество передачи.

*О мировом рынке телекоммуникаций.* В результате анализа стратегии развития телекоммуникаций мы приходим к выводу о целесообразности поиска решений совместной работы двух технологий — коммутации пакетов и коммутации каналов. Но такому повороту событий может препятствовать состояние мирового рынка телекоммуникаций, в том числе отставание США и особенно в производстве традиционных телефонных

станций. На рынке телекоммуникаций создалась странная ситуация.

По мере того, как США переходят на беспроводные сети 5G, американское сообщество видит в китайском телекоммуникационном гиганте Huawei высокий риск своей безопасности. Существует глубокая обеспокоенность тем, что в конечном итоге компания Huawei будет контролировать глобальные рынки, вытеснив других крупных поставщиков 5G, в том числе европейских Ericsson и Nokia (рис. 4). Почему нет американских компаний по производству оборудования связи? В 1970-х двумя крупнейшими производителями телекоммуникационного оборудования были компании США: Western Electric и ITT. Даже в конце 1990-х две крупнейшие компании все еще находились в Северной Америке: Lucent и Nortel (со штаб-квартирой в Канаде). Однако в 2008 году Nortel обанкротилась, а Lucent была продана французской компании Alcatel, которую позже купила финская Nokia. Если будет осознано, что стоит сочетать две технологии — коммутацию пакетов и коммутацию каналов, то возникает сложный вопрос практической реализации, если нет собственной индустрии.

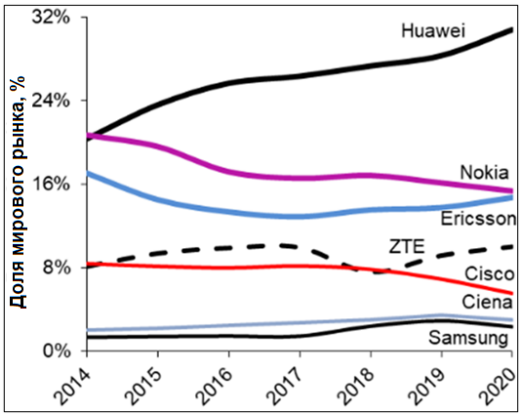


Рис. 4: Мировой рынок телекоммуникационного оборудования, 2020 г. [1]

Далее в настоящей статье на примерах покажем трудности, которые имеются на пути перехода от КК к КП и которые ставят под сомнение саму целесообразность смены парадигмы телекоммуникаций. В Разделе 2 показана аналогия между сетью экстренных вызовов и сетью связи оборонного ведомства США (Global Information Grid, GIG) – крупнейшей в мире ведомственной сети [1]. Эта аналогия предполагает построение этих двух сетей по одним и тем же документам. Но, к сожалению, отсутствует организация, которая бы такие единые документы разработала, и эти сети создаются раздельно.

В разделе 3 изложена история неудачных попыток перехода на пакетную коммутацию в сфере экстренных служб, что, кстати, неудивительно, так как потеря любого экстренного вызова может стать поводом для судебного иска. Только через 18 лет (1999-2017) удалось найти компанию (в данном случае AT&T), которая начала строить пакетную сеть для FirstNet. Но исход дела пока не ясен. Еще менее ясна судьба сети FirstNet как центрального звена в критической инфраструктуре государства.

Раздел 4 посвящен истории создания информационных сетей оборонного ведомства США. В 1996 г. была принята 15-летняя программа развития вооружений «Joint Vision 2010». В части средств связи основной выбор пал на сигнализацию SS7 и интеллектуальные сети (Advanced Intelligent Network, AIN) – высшие достижения техники коммутации каналов. Но в связи со взрывоподобным развитием Интернет-технологий Пентагон поддался модному течению, и в 2006 г. принял новый план «Joint Vision 2020». Этот план объявил смену парадигмы сети DISN – переход от сигнализации SS7 к IP протоколу. Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями. Для перехода между двумя типами сетей изобрели новый коммутатор – многофункциональный софтсвич MFSS, который действует как медиашлюз между TDM каналами и IP-каналами. По заказу МО США разработали протокол AS-SIP (Assured Services for Session Initiation Protocol), который обеспечивает секретность передачи разговора (сообщения) и приоритетность вызовов. Но протокол AS-SIP получился очень громоздким, так как пользуется услугами почти 200 стандартов RFC. Не ясно, есть ли на рынке хотя бы один телефон, реализующий протокол AS-SIP в полном объеме.

Вполне понятно, что реализация плана «Joint Vision 2020» продвигается медленно. В Разделе 5 описана целевая архитектура сети DISN, в которой для сигнализации между MFSS вместо SS7 используется новый протокол высокого уровня ICCS (Intra-Cluster Communication Signaling). Но своеобразным «родимым пятном» на сети DISN, строящейся по единому протоколу AS-SIP для доступа к сети, является сверхсекретная правительственная связь DRSN (Defense RED Switch Network), которая сохраняет технологию коммутацию каналов, точнее, ISDN-каналы. Сохраняется гибридная технология ATM в информационных сетях разведки JWICS и управления спутниками AFSCN.

С развитием микроэлектроники появилась возможность на одном кристалле, помимо процессорного ядра, разместить большое количество сложных функциональных узлов. Появилось новое направление техники – сеть на кристалле (NoC, Network on a Chip), что описано в Разделе 6. Схемы NoC изначально строили для пакетной коммутации, рассматривая коммутацию каналов как побочный вариант. В последнее же время появились работы, говорящие об обратном: изделия коммутации каналов более выгодны или, по райней мере, выгодно сочетать обе технологии.

Разделы 7 и 8 посвящены киберзащите. Киберуязвимость оказалась главным пороком Интернет-технологий. В Разделе 7 изложены основы единой архитектуры безопасности SSA (Single Security Architecture). Единый подход к структуре кибербезопасности обеспечивают объединенные региональные стеки безопасности JRSS (Joint regional security stacks). JRSS, по замыслу, должны обеспечивать

киберзащиту в сетях электронной почты NIPRNet и SIPRNet. Планировалось 48 стеками JRSS заменить около 1000 нестандартных стеков сетевой безопасности, которые в настоящее время разбросаны по всему миру. Программа разработки стеков JRSS длилась более 10 лет и, к сожалению, завершилась полным провалом. В ноябре 2021 г. Министерства обороны объявило о закрытии программы кибербезопасности JRSS стоимостью 2 миллиарда долларов и о переходе на новую технологию киберзащиты - архитектуру нулевого доверия (Zero Trust Architecture).

Раздел 8 начинается сообщением Счетной палаты правительства США (2018 года) о том, что все системы вооружения с программным обеспечением, которые была протестированы в период с 2012 по 2017 год, включая созданные за последние десять лет, имеют киберуязвимости и могут быть взломаны. Особой критике подвергли боевой самолет-невидимку F-35, который управляется программным обеспечением, содержащим 8 млн. строк кода. Несмотря на более чем 20 лет работы и примерно 62,5 потраченных миллиарда долларов, пока не удалось создать надежный самолет. Конгресс США на 2022 финансовый год отказался санкционировать дополнительные новые заказы F-35.

Другой грандиозный проект – это ракетный эсминец USS Zumwalt. Zumwalt имеет колоссальную сложность: 1200 разработчиков программного обеспечения из 30 организаций разработали мозг корабля, управляемый ПО беспрецедентно большого объема – от 14 до 16 миллионов строк компьютерного кода. Пока отсутствуют данные о тестировании киберуязвимостей эсминца Zumwalt (что может таить немало неожиданностей), но появилась крайне важная незадача – отсутствие гиперзвукового оружия. Планы ВМС в настоящее время предусматривают развертывание гиперзвукового оружия на Zumwalt к 2025 финансовому году.

## II. Аналогия между сетью экстренной помощи и военными информационными сетями

### A. *Кардинальные решения 2007 года*

В 2007 г. Министерство транспорта США (Department of Transportation, DoT) опубликовало «Концепцию сети экстренной помощи нового поколения (NG9-1-1)» [2]. Этот документ требовал перехода к IP-протоколу на сетях экстренной помощи. Вслед за этим DoT опубликовало «Описание системы и требования высокого уровня», в котором содержится более подробная информация об архитектуре NG9-1-1 [3].

Примерно в то же время (2007) Министерство обороны США (Department of Defense, DoD) опубликовало «Архитектурное видение глобальной информационной сети Global Information Grid (GIG)» [4]. Этот документ до настоящего времени служит директивой не только для Министерства обороны, но и других ведомств в отношении того, как будут реализованы и развернуты сете-центрические информационные системы, основанные на IP-протоколе.

По замыслу, обе системы NG9-1-1 и GIG имеют несомненное сходство. Оно начинается с архитектуры высокого уровня. Обе архитектуры предполагают наличие потока информации от разнообразных технических устройств к множеству пользователей. Кроме того, эти архитектуры гарантируют наличие некоторой формы взаимодействия между разрозненными системами, которые могут быть подключены к сети. Наконец, архитектура построена так, чтобы быть живучей. В случае модели NG9-1-1 предусмотрена операционная переадресация на разные Центры обслуживания вызовов ЦОВ (Public Safety Answering Points, PSAP), расположенные в одном месте или географически разделены. Для GIG живучесть достигается за счет того, что несколько систем или источников работают параллельно, поэтому, если одна система или источник отключены, информация все еще может передаваться конечному пользователю.

Еще одно подобие заключается в приложениях. Обе концепции NG9-1-1 и GIG требуют возможности передачи голоса, данных и видео. Гарантируется, что приложения могут использовать все эти возможности по первому требованию и с минимально возможной задержкой. Хотя данные двух областей – в экстренной помощи и на войне – могут различаться, в основном же приложения очень похожи. Например, Центру экстренной помощи может потребоваться потоковое видео пожара, чтобы определить потребности в ресурсах. Военному командиру на поле боя может потребоваться потоковое видео перестрелки, чтобы определить тактику боя. Подключение к сети — это, пожалуй, самая трудная задача, с которой сталкиваются обе концепции. Чтобы сотни тысяч конечных пользователей адаптировались к новой сети, обе архитектуры требуют, чтобы сети были достаточно гибкими к выполнению требований конечных пользователей.

### B. *Суть сети нового поколения экстренной помощи*

В США экстренные вызовы обслуживаются по номеру 911. Переход от традиционной сети 911 к сети нового поколения экстренной помощи NG9-1-1 оказался тернистым. Большие трудности возникли при внедрении единого номера для фиксированных и мобильных абонентов, особенно определение номера вызывающего мобильного абонента и его местоположения, что регламентируют требования, объединенные под названием E9-1-1 (рис. 5): требуется определить местоположение мобильного пользователя с точностью до 50 м.

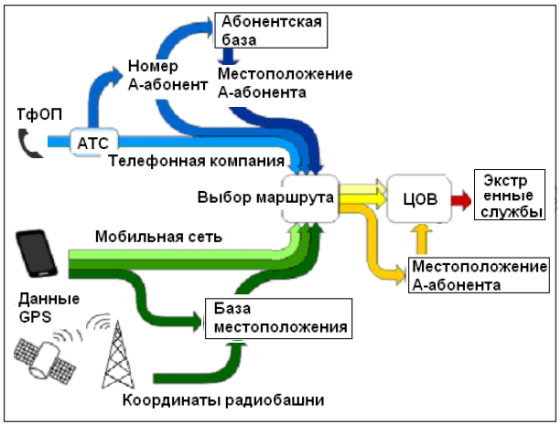


Рис. 5: Экстренный вызов в системе Enhanced 9-1-1

Новое поколение службы экстренных вызовов NG9-1-1 будет реализовано в IP-сети (рис. 6). В этой системе требуется обеспечить возможность любых сообщений реального времени, т.е. не только телефонных вызовов, но и передачу текста, данных, изображений и видео. План NG9-1-1 стартовал в 2000 г. и к 2008 были завершены пилотные проекты. Однако до 2017 года сеть NG9-1-1 не получила никакого внедрения.

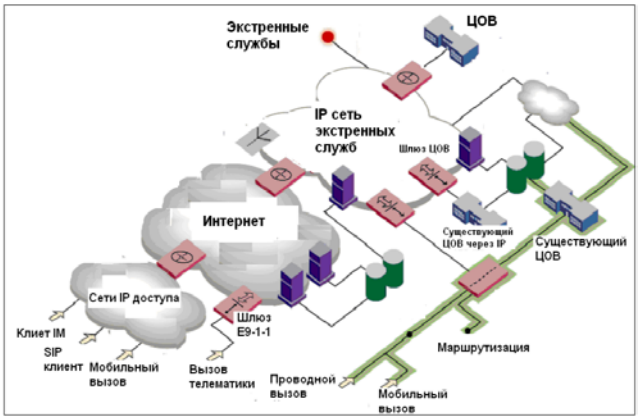


Рис. 6: Новое поколение экстренной службы NG9-1-1 и ее стыковка с существующей службой 911

Обратим внимание на рис. 6 слева внизу: там отдельно указаны телематические вызовы от различных сенсоров. Это могут быть вызовы к противопожарным и охранным службам. Заметим, что такие вызовы могут быть обслужены и существующими средствами E9-1-1.

### *C. Суть перспективной оборонной сети DISN*

Рисунок 7 иллюстрирует главную проблему, которая стоит перед строителями сети GIG, точнее, перед оборонной информационной сетью DISN (Defense Information System Network). Сегодня основу DISN составляет коммутация каналов, а именно: стандарт SONET/SDH, по которому работают оптические кабели, и информация кодируется по телефонному стандарту TDM (Time Division Multiplexing). По сети коммутации каналов сегодня работают три основные военные сети связи Пентагона:

1) телефонная сеть DSN (Defense Switched Network),

2) закрытая коммутируемая сеть DRSN (Defense Red Switched Network),

3) сеть видеоконференцсвязи DVS (DISN VIDEO).

Кроме того, на рис. 7 указаны четыре закрытые сети:

• Объединённая глобальная сеть разведывательных коммуникаций (Joint Worldwide Intelligence Communications System, JWICS) — для передачи секретной информации, которая использует коммутаторы ATM,

• Сеть управления спутниками AFSCN (Air Force Satellite Control Network), которая также использует коммутаторы ATM,

• NIPRNet (Non-classified Internet Protocol Router Network) — сеть, используемая для обмена несекретной, но важной служебной информацией между «внутренними» пользователями по протоколам TCP/IP,

• SIPRNet (Secret Internet Protocol Router Network) — система взаимосвязанных компьютерных сетей, используемых для передачи секретной информации по протоколам TCP/IP.

В настоящее время введена новая классификация сетей DISN: сеть NIPRNet переименована в SBU IP Data, SIPRNet – в Secret IP Data, сеть разведки JWICS - в TS/SCI IP Data и правительственная сеть DRSN – в сеть Multilevel Secure Voice.

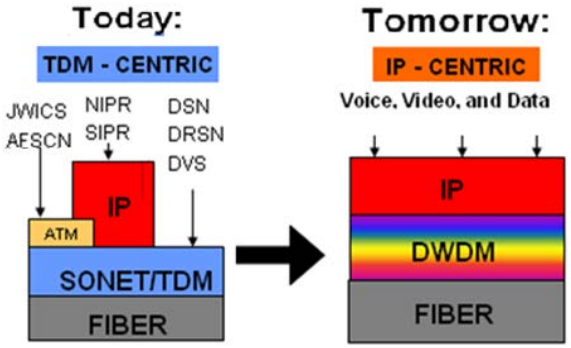


Рис. 7: Иллюстрация текущей проблемы DISN: как перейти полностью от TDM к IP протоколу

Согласно текущей стратегии Пентагона предполагается, что IP-протокол станет единственным средством общения между транспортным уровнем и приложениями (рис. 8).

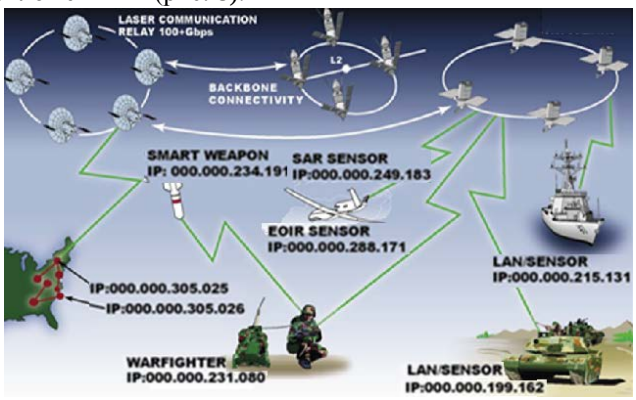


Рис.8: Каждый объект оборонного ведомства имеет свой IP-адрес: солдат, спутник, самолет, даже ракета

С объявленного перехода сети DISN в IP-мир к настоящему времени (2022) прошло уже 15 лет, но ощутимых результатов пока не достигнуто.

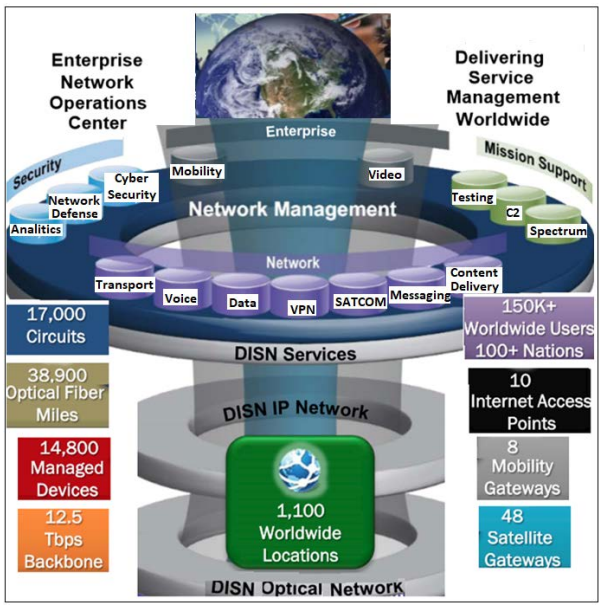


Рис. 9: Сетевая инфраструктура DISN оценивается в 24 миллиарда долларов [5]

Удастся ли модернизировать огромную информационную сеть Министерства обороны США? Эта задача чрезвычайно сложная, так как она состоит из более чем 15 000 секретных и/или открытых отдельных сетей, соединяющих более семи миллионов компьютеров и ИТ-устройств, имеет более 10 000 операционных систем, из которых 20% являются критически важными, 67 000 серверов в более чем 770 центрах обработки данных, расположенных в более чем 6 000 местах в 600 000 зданиях. Систему DISN обслуживают 170 000 ИТ-специалистов в 146 странах (рис. 9). Как это громадное хозяйство перестроить на средства Интернет-технологий?

## III. Как развивается сеть экстренной помощи

### A. *Риски перехода на IP протокол*

В 2014 г. Федеральная комиссия связи (FCC) издала документ о финансовой поддержке операторов, которые будут переходить от коммутации каналов (по технологии TDM) к IP протоколу [6], но эта инициатива успеха не имела. Одновременно FCC обратилась к одной юридической фирме с заказом дать оценку возможных рисков такого перехода. Фирма проанализировала историю нововведений в телефонных сетях, а также перечислила крупнейшие сбои в телефонных сетях от введения новой техники за последние более 20 лет [7]. Сбои появляются в основном из-за ошибок в программном обеспечении, что ведет к крупным авариям на телефонных сетях.

Наиболее известен коллапс сети AT&T, который случился 15 января 1990 г. Тогда одновременно вышли из строя все 114 станций 4ESS сети AT&T. Устранить неполадки удалось только через 9 часов. Дело было в новом программном обеспечении, которое установили месяцем ранее на всех станциях 4ESS. Вкралась всего лишь одна ошибка в работе системы SS7, которая проявилась при перегрузке одной из АТС и по принципу домино «вырубила» почти всю сеть AT&T. Были потеряны 65 млн. вызовов и главное – был нанесен трудно поправимый ущерб репутации компании. Другой подобный коллапс случился через полтора года – 26 июня 1991 г. в Балтиморе. На 6 часов остались без связи 5 млн. абонентов. Тоже из-за ошибки в программах SS7. В докладе указаны также сбои с переносом номера мобильной связи (услуга LNP), с внедрением Бесплатного вызова (по коду 888) и другие. Коллапсы сети связи страны были расследованы Конгрессом США, так как их приравняли к угрозам национальной безопасности. Тем самым был, по крайней мере временно, вынесен «приговор» системе SS7. В частности, в службе экстренных вызовов 911 отказались от применения сигнализации SS7 и интеллектуальной сети и сохранили прежнюю систему многочастотной сигнализации MF.

Заметим, что при многочастотной сигнализации (Multi-Frequency signaling, MF) для передачи адреса (телефонного номера) используют комбинацию звуковых сигналов: каждая цифра набора кодируется двумя частотами из набора шести частот (2 из 6). Эти сигналы передаются по разговорному каналу. Система сигнализации SS7 отличается тем, что сигнализация производится по отдельной сети передачи данных.

Тем самым и переход к IP протоколу практически приостановился на долгие годы. Еще больше, как видится сегодня, повсеместный переход к IP протоколу может и вовсе не состоятся (косвенным свидетельством того является наличие ISDN в сверхсекретной правительственной сети DRSN).

### B. *О критической инфраструктуре государства*

С точки зрения государства сеть экстренной помощи относится к критической инфраструктуре государства, к обеспечению безопасности общества и занимает в ней центральное место. На рис. 10 представлена подробная архитектура безопасности государства с точки зрения приложений. Показаны прикладные области (приложения), которые упорядочены по государственной важности, принятой в США.


Рис. 10: Архитектура безопасности государства

Наивысшую важность имеет служба ПЕРВАЯ ПОМОЩЬ (First Responders), что по российскому законодательству соответствует аппаратно-программному комплексу «Безопасный город», и

включает пожарную охрану, отравляющие материалы (газовая служба), экстренную медицинскую службу, правонарушения (полицию) и службу 911 (в России – 112).

Следующий круг по критичности занимают ЭКСТРЕННЫЕ СЛУЖБЫ. Всего насчитывается 12 разделов жизнедеятельности, которые охвачены экстренными службами - от национальной гвардии до госпиталалей. Внешний круг занимают менее критические разделы инфраструктуры. Это – школы, служба погоды, порты и многое другое. Заметим, что разделение инфраструктуры государства весьма расплывчато, например, во внешний круг вынесены телекоммуникационные компании, в то время как сами сети связи, обслуживающие ПЕРВУЮ ПОМОЩЬ (First Responders) обладают наивысшим приоритетов в обеспечении жизни общества.

### *C. О сети FirstNet*

Подробнее остановимся на центральном звене ПЕРВАЯ ПОМОЩЬ (First Responders). Сама проблема национальной безопасности крайне обострилась после терактов 11 сентября 2001 года. Но прошло долгих 11 лет в обсуждениях, прежде чем в 2012 году было создано Управление сетью первой помощи (First Responder Network Authority, сокращенно – FirstNet) с весьма сложной подчиненностью. Оно является подразделением Министерства транспорта США, а действует как независимый орган в рамках Национального управления по телекоммуникациям и информации (National Telecommunications and Information Administration). Оно отвечает за общенациональную высокоскоростную широкополосную сеть для аварийных служб и, тем самым, за обеспечение общественной безопасности.

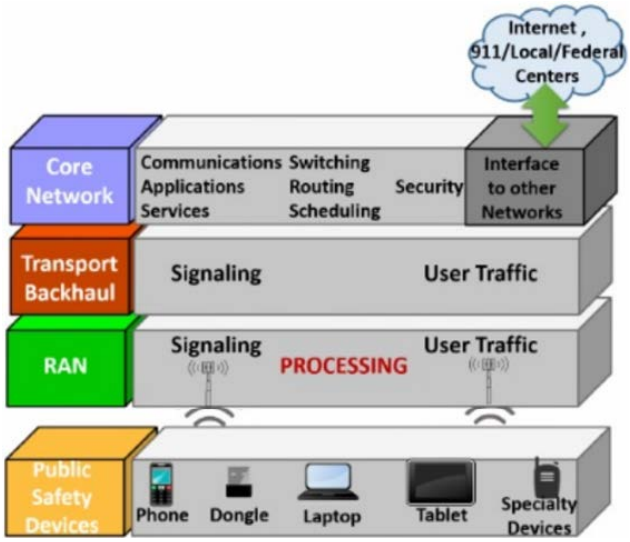


Рис. 11: Инфраструктура FirstNet [8]

Управление FirstNet утверждает, что вновь создаваемая сеть предоставит единую функционально совместимую платформу для передачи экстренных и обычных сообщений, касающихся общественной безопасности.

Следует подчеркнуть, что ключевым компонентом является создание новой сети пакетной коммутации, взаимодействующей с другими государственными, местными и федеральными сетями. По заверениям Управления FirstNet, ядро сети образует гигантский «зонтик», охватывающий все Соединенные Штаты. Ядро этой сети через транзитные узлы будет подключено к сетям радиодоступа в каждом штате. Первоначальное моделирование показало, что для охвата, по меньшей мере, 99% населения и национальной сети автомагистралей необходимы установить десятки тысяч новых базовых радиостанций.

С проблемой создания новой общенациональной сети более-менее все ясно, но, думаю, сложнее обстоит со средствами доступа. Для пользователей FirstNet, по заверениям, будет разработан набор новых мобильных устройств – от смартфонов до ноутбуков, планшетов и других специализированных устройств для работы в сети FirstNet, которые способны передавать голос, данные и видео (нижний слой на рис. 11). Устройства должны удовлетворять множеству весьма противоречивых требований: быть прочными в разнообразных условиях внешней среды, но при этом быть легкими в использовании, удобными и безопасными. Удастся ли эти требования сочетать?

Для нужд общенациональной сети FirstNet в 2012 году был выделен частотный диапазон в области 700 МГц, так называемый Band 14 (рис. 12). Этим был положен конец многолетним спорам о взаимодействии сетей связи при предоставлении экстренных услуг населению. На данный момент для сети FirstNet выделена полоса 20 МГц. Точнее, для широкополосной связи выделены частоты от 758 до 768 МГц и от 788 до 798 МГц, а для узкополосной местной связи (передачи голоса) выделены частоты от 769 до 775 МГц и от 799 до 805 МГц. Предполагается, что сеть FirstNet должна строиться по техническим требованиям LTE.

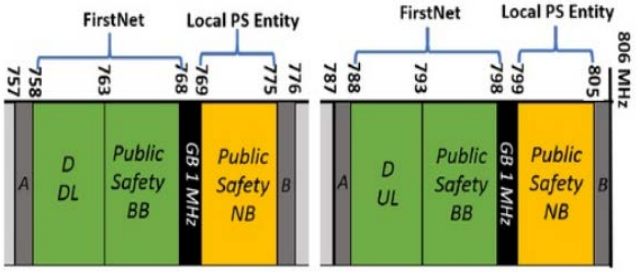


Рис. 12: FirstNet: общенациональный частотный диапазон Band 14 (в области 700 МГц шириной в 20 МГц) [8]

### *D. О трудностях создания сети FirstNet*

В 2016 году в журнале *Atlantic* появилась критическая статья о сети FirstNet под названием «Сеть стоимостью в 47 миллиардов долларов, которая уже устарела» [9]. Статья ссылается на отчет Счетной палаты США (U.S. Government Accountability Office), мол – бесцельно истрачены от 12 до 47 млрд. долларов. Действительно, разработка сети FirstNet и экстренной сети NG9-1-1 продвигалась чрезвычайно медленно. Решение о создании FirstNet начали интенсивно обсуждать сразу

после терактов 2001 года, но технические решения так и не были сформулированы.

Сошлемся на документ Конгресса США [10], в котором перечислены причины медленного прогресса в решении задач FirstNet. Спор шел о возможности создания для нужд FirstNet новой мобильной сети федерального уровня. Необходимо было не только выделить частотный диапазон, но и финансово заинтересовать операторов связи. Предложено было использовать выделенные частоты не только для экстренной помощи, но – в сельских или отдаленных районах – использовать и для других, платных услуг. Мобильная сеть в небольших населенных пунктах может служить оживлению жизни в прямом смысле, например, способствовать улучшению транспортной системы, образованию, управлению сельским и лесным хозяйством, повышению эффективности муниципальных органов власти и услуг, тем самым обеспечить экономический рост сельских территорий.

И вот, наконец, решение по сети FirstNet сдвинулось с мертвой точки – 30 марта 2017 г. объявлено [11], что компания AT&T официально выбрана в качестве коммерческого партнера, который для сети общественной безопасности First Responders будет строить и поддерживать общенациональную мобильную сеть стандарта LTE. Соисполнителями работ AT&T по сети FirstNet названы компании Motorola Solutions, General Dynamics, Sapient Consulting и Inmarsat Government. Единая широкополосная сеть FirstNet охватит все 50 штатов, 5 территорий США и округ Колумбия, включая сельские общины и рассеянные племена в этих штатах и территориях – в общей сложности более 320 миллионов человек в Соединенных Штатах. И главное – всему населению США следует предоставить новые мобильные устройства для работы в выделенных частотах.

Сможет ли AT&T с соисполнителями совершить столь неудачный до сих пор проект сети FirstNet, – покажет будущее. По состоянию на октябрь 2021 года [12] к сети FirstNet были подключены более 18 500 агентств и организаций общественной безопасности с более чем 2,8 миллионами пользователей. Объявлено, что компания AT&T превысила планы FirstNet Authority, обеспечив 95% покрытия частотами Band 14, что каталог приложений FirstNet включает более 315 типов устройств, работающих в сети FirstNet, и более 180 приложений, в том числе вызовов по поддержке психического и физического здоровья в качестве первой помощи. Проект AT&T FirstNet, мол, значительно опережает график. Но следует иметь в виду, что это все еще только само начало проекта AT&T FirstNet.

## IV. О ВОЕННЫХ ИНФОРМАЦИОННЫХ СЕТЯХ

### *A. Стратегический план Joint Vision 2010: ориентация на интеллектуальную сеть AIN*

Use Оборонная информационная сеть DISN (Defense Information Systems Network) разрабатывается с начала 1990-х. Это – глобальная сеть. Ее назначение – предоставлять услуги по передаче различных видов информации (речь, данные, видео, мультимедиа) для эффективного и защищенного управления войсками, связью, разведкой и РЭБ.

Когда стали выполнять план «Joint Vision 2010», проанализировали состояние DISN. И вскрылось множество недостатков [13]. Прежде всего, это – низкий уровень интеграции многих сотен сетей, входящих в состав DISN, что существенно ограничивает взаимодействие в рамках единой сети и препятствует эффективному единому управлению всеми ее ресурсами. В частности, отмечались сложности взаимодействия между стационарной и полевой (мобильной) компонентами базовой сети из-за различия в используемых стандартах, типах каналов связи (аналоговых и цифровых), предоставляемых услугах, пропускной способности (у мобильной компоненты она значительно ниже, чем у стационарной).

Это порождает дополнительные трудности материального обеспечения боевых сил, технического обслуживания и подготовки специалистов. Кроме того, используемые сетевые технологии недостаточно масштабируемы и не в состоянии в должной мере предоставлять пропускную способность по требованию. Из-за отсутствия общей архитектуры и стандартов затруднена передача данных в интересах разведки и РЭБ. Несовместимость оборудования усложняет применение различных средств засекречивания и криптозащиты. В целом базовая архитектура DISN недостаточно гибкая и масштабируемая, особенно для мобильных сил, оперативно развертываемых в различных точках мира.

В условиях технологической неопределенности агентство DISA приняло принципиальное решение – строить военные сети связи США с использованием «открытой архитектуры» и программно-аппаратных средств коммерческого назначения (Commercial-Off-the-Shelf). В результате выбор пал на «старые» разработки Bell Labs, точнее, на протокол телефонной сигнализации SS7 и на интеллектуальную сеть (Advanced Intelligent Network, AIN).

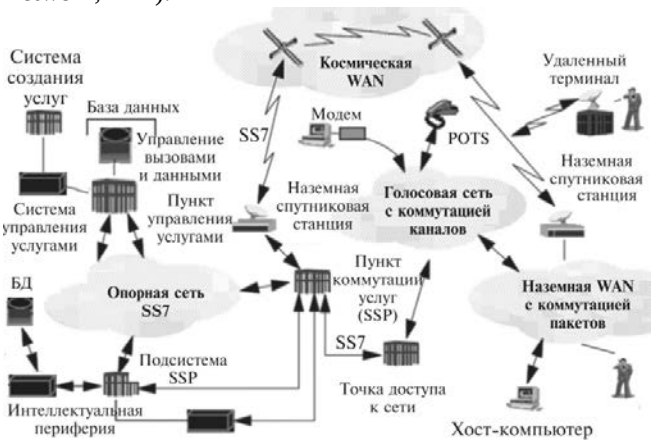

Рис. 13: Архитектура Advanced Intelligent Network [15]

Заметим, что к тому времени институт Bell Labs был давно уж как ликвидирован (корпорацию Bell System расчленили в 1984 г.). Однако разработки Bell Labs по

сигнализации SS7 и интеллектуальной сети AIN были всесторонне апробированы (и живут по сей день).

Представитель агенства DISA в 1999 г. на Международной конференции по военным коммуникациям MILCOM'99 доложил [14]:

*«Будущие сети DISA будут пользоваться преимуществами программных средств IN. Сервисы AIN станут ядром технологии развития, технологии оценки (assessment) и технологии передачи информации МО. Результаты сервисов AIN обеспечат командиров боевых действий способностью собирать, обрабатывать и передавать информацию без перерывов в работе сети. Возможности AIN станут краеугольным камнем информационного превосходства МО».*

На той же конференции MILCOM'99 выступил представитель компании Lockheed Martin Missiles & Space [15], компании, которая является головным разработчиком глобальной информационной сети сил НАТО. В этом докладе подчеркивается, что AIN обеспечивает пользователей любыми сервисами, как-то: голос, данные, e-mail, video, офисные приложения, вызовы «800». А главное, в докладе подробно описывается ключевая роль протокола SS7: он обеспечивает предоставление перечисленных сервисов, включая спутниковую связь. Уже тогда – более 15 лет назад – представитель компании Lockheed Martin отметил, что взрывоподобный рост мощи компьютеров и веб-технологий в 21 веке приведет к чрезвычайным сложностям в управлении боевыми действиями.

Связующим звеном сети AIN служит система сигнализации SS7. Прежде всего, SS7 обеспечивает доступ к базам данных, что лежит в основе организации дополнительных услуг (в частности, Бесплатного вызова по коду 800). Пользователями AIN могут быть как абоненты сети коммутации каналов, так и коммутации пакетов. Важная роль отводится интеллектуальной периферии, в ее функции входит генерация тонов, распознавание голоса, сжатие речи и данных, распознавание набора номера и многое другое, включая тактические и стратегические сервисы по идентификации персонала. Обратим внимание на Подсистему SSP в нижнем левом углу схемы (рис. 13). Это, например, в случае войны в Афганистане представляло собой контейнерную электронную АТС, которую доставили самолетом и по наземному кабелю подключили к общей сети DISN.

Рисунок 14 показывает практическую реализацию сети DISN. Она использует разные протоколы и устройства: 4-проводной (4W); секретную локальную сеть (ASLAN); ISDN BRI; Интернет-телефонию (VoIP); видеоконференцсвязь (VTC); нестартизованные (proprietary) протоколы. Несмотря на то, что новое терминальное оборудование, в основном, является IP-типа, сеть SS7, тем не менее, сохраняет свое центральное место. Отсюда делаем важный вывод: наличие сети SS7 (ОКС7) не препятствует переходу на протоколы IP, а скорее наоборот - облегчает переход на пакетную коммутацию, делает его поэтапным. Сеть SS7 является, образно говоря, нервной системой коммутируемой сети DSN.

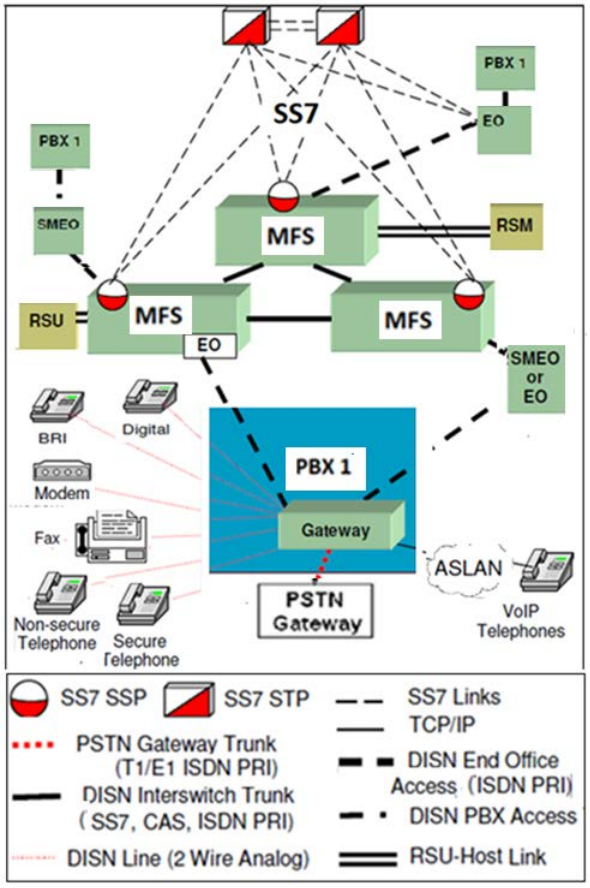


Рис. 14: Упрощенная схема DISN [16]

### *B. Стратегический план Joint Vision 2020: ориентация на IP протокол*

*MFSS — основа перехода от TDM к IP.* К сожалению, полномасштабное внедрение сетей AIN затормозило появление Интернет-технологий. Пентагон поддался модному течению, и в 2006 г. принял новый план «Joint Vision 2020» – на следующие 15 лет. Этот план объявил смену парадигмы сети DISN – переход от сигнализации SS7 к IP протоколу. Предполагается, что IP протокол станет единственным средством общения между транспортным уровнем и приложениями. План «Joint Vision 2020» был принят без должного анализа последствий (в том числе кибербезопасности, что, правда, трудно было предвидеть).

Отрицательные последствия столь поспешного решения очень скоро выявились. Приводим яркое высказывание одного генерала в 2009 г. – в адрес производителей военного оборудования: «Нам ящиков больше не нужно», и напоминает, что в Вооруженных силах имеется 40 различных систем связи: «Ящиков у нас хватает. Помогите нам, чтобы эти ящики умели говорить друг с другом.»

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 нового оборудования – многофункциональных программируемых коммутаторов

MFSS (MultiFunction SoftSwitch) как своеобразных шлюзов между миром PCM и миром IP [17].

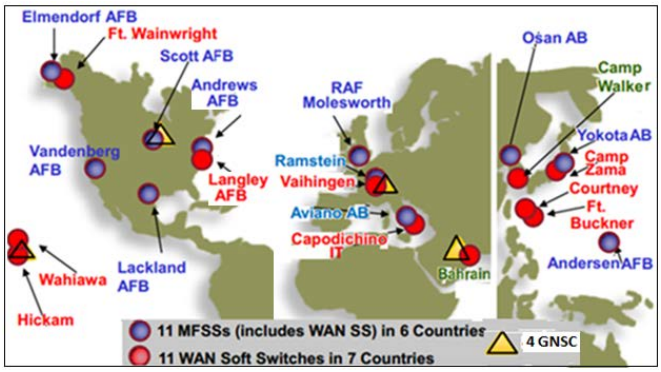


Fig. 15: Планы CISCO по установке 22 крупных программируемых коммутаторов (Softswitch) [18]

Компания CISCO — крупнейшей подрядчик Пентагона – установила 22 крупных программируемых коммутаторов (Softswitch) на военных базах по всему миру (рис. 15): 11 WAN SS (Wide Area Network SoftSwitch), действуют в среде IP, и 11 MFSS (действуют в среде PCM и IP). Там же указаны четыре центра управления сетью (Global Network Support Center, GNSC) — два в США (на авиабазе Scott и на Гавайях), по одному в Германии и Бахрейне.

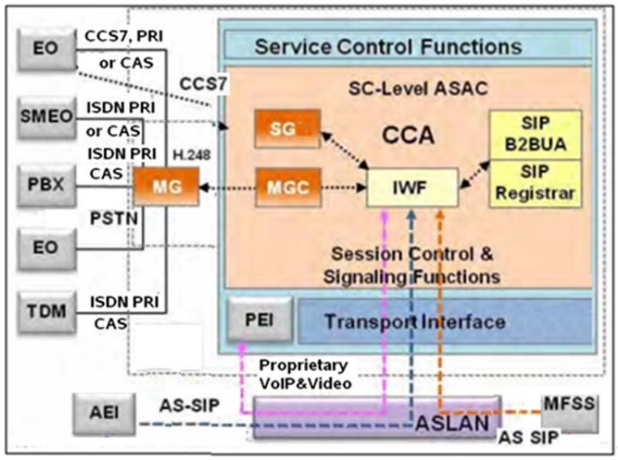


Fig. 16: Многофункциональный программный коммутатор (софтсвич) MFSS [19]

Объясним, как многофункциональный софтсвич MFSS управляет вызовами (рис. 16):

• в сторону внешней публичной сети ТфОП или сети ISDN (Integrated Services Digital Network) используется функция IWF (ISUP-SIP-interworking function);

• контроллер MFSS обеспечивает «старые» сигнализации ТфОП/ ISDN, включая ISUP, SS7 и CAS (Channel Associated Signaling);

• 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 SS7 и AS-SIP.

В окружении MFSS имеются еще (1) оконечные усройства EI (End Instrument) — в сети коммутации каналов и (2) два типа устройств в IP сети: AEI (Assured Services End Instrument), работающие по про□токолу AS-SIP, а также нестандартные устройства PIE (Proprietary Internet Protocol Voice End Instrument).

Заметим, что со времени установки первых MFSS прошло уже более десяти лет, но до сих пор отсутствует информация об успешном запуске хотя бы одного из 22 MFSS, т.е. о замене хотя бы одной электронной телефонной станции на MFSS. И это понятно: MFSS – весьма сложное оборудование. Вряд ли командиры связи, отвечающие своей должностью за надежные коммуникации, без большего принуждения откажутся от проверенных решений коммутации каналов и перейдут на Интернет-технологии.

В состав MFSS входит сложнейший узел – функция контроля сессии SCF, ее описание см. Приложение 1, а описание сигнализации AS-SIP см. Приложение 2.

*Унифицированные армейские коммуникации.* Целью концепции «Joint Vision 2020» является внедрение унифицированных армейских коммуникаций, так называемых унифицированных возможностей UC (Unified Capabilities) [19]. Унифицированные армейские коммуникации UC определяются как пакет услуг передачи голоса, видео и/или данных, предоставляемых через безопасную и доступную сетевую инфраструктуру (рис. 21).

Ниже приведены основные голосовые функции и возможности:

• переадресация вызовов (выборочная, по занятой линии и др.),

• многоуровневый приоритет и прерывание вызова (взаимодействие с переадресацией вызовов, сигнал «отсутствие вызываемого абонента» и др.),

• ожидание приоритетного вызова (занято вызовом с более высоким приоритетом, занято вызовом с равным приоритетом и др.),

• переадресация вызова (с разными уровнями приоритета, с одинаковыми уровнями приоритета),

• удержание вызова и трехсторонний вызов.

Архитектура унифицированных армейских коммуникаций (рис. 21) использует протокол AS-SIP для доступа к глобальной магистральной сети IP/MPLS. Всемирная магистральная базовая транспортная сеть DISN будет состоять из проводных (например, оптоволоконных) и беспроводных (например, спутниковых) сетей. Сети доступа могут быть разного рода, такие как IP, LAN, PSTN/ISDN/TDM, Wi-Fi, DSL, кабельное и оптоволокно, беспроводная связь 3G, WiMAX и беспроводная связь LTE/4G. Технологии доступа IP/LAN будут беспрепятственно работать с сетью IP/MPLS, а сети PSTN/ISDN/TDM нуждаются в соответствующих шлюзах для взаимодействия с сетью IP/MPLS.

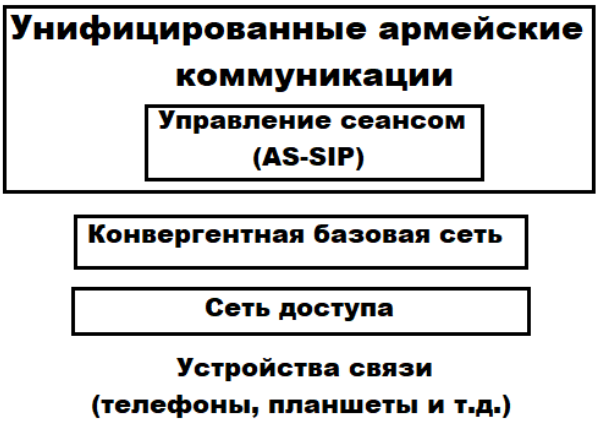


Рис. 21: Концептуальный вид эталонной архитектуры унифицированных армейских коммуникаций (рисунки 17-20 – см. приложение)

Унифицированные армейские коммуникации охватывают множество возможностей связи: от точки к точке, от точки к нескольким точкам, голосом к мультимедиа, от проводных к беспроводным, в реальном времени или по расписанию и т.д. [18]. Набор коммуникаций включает электронную почту и ведение календаря, обмен мгновенными сообщениями и чат, унифицированный обмен сообщениями, видеоконференции, голосовые конференции, веб-конференции и другое (рис. 22).

Солдат имеет богатый набор коммуникаций, но возникает множество резонных вопросов. Не слишком ли их много? Сможет ли солдат и даже командир воспользоваться этим набором услуг в условиях боя? Даже еще важнее – можно ли любого солдата научить пользоваться столь сложным переносным устройством? На эти и другие подобные вопросы пока нет ответа. Не останутся ли только на бумаге планы создания унифицированных армейских коммуникаций. Если еще выполнять требования кибернеуязвимости, то даже голосовую беспроводную связь в условиях боя трудно обеспечить. Таковы вот дела!


Рис. 22: Богатый набор информационных сервисов вокруг солдата: не слишком ли много?

## V. Целевая архитектура сети DISN

### A. *Основная схема*

Целевая архитектура сети DISN содержит два уровня: Tier 0 и Tier 1. (Fig. 23). Кластер Tier 0 отвечает за неуязвимость всей сети DISN. Кластер содержит три софтсвича уровня Tier 0, соединенных протоколом ICCS (Intra-Cluster Communication Signaling), по которому автоматически обновляются их базы данных. Такой кластер, по существу, представляет собой 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 6600 км. 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 речи и видео по протоколу IP. Своеобразным «родимым пятном» на сети DISN является сверхсекретная правительственная связь DRSN (Defense Red Switch Network), которая сохраняет технологию коммутации каналов, точнее, ISDN-каналы и протоколы сигнализации ISDN PRI и CAS (Channel Associated Signaling). Следует подчеркнуть, что в методических материалах по DISN [24] не предусмотрен перевод сети DRSN на коммутацию пакетов, что служит ярким подтверждением неверия в киберзащищенность Интернет-технологий. И сама целевая архитектура сети DISN весьма замысловата. Будет ли она реализована в ближайшее десятилетие? Она ведь, по концепции, охватывает все базы NATO, практически весь мир.

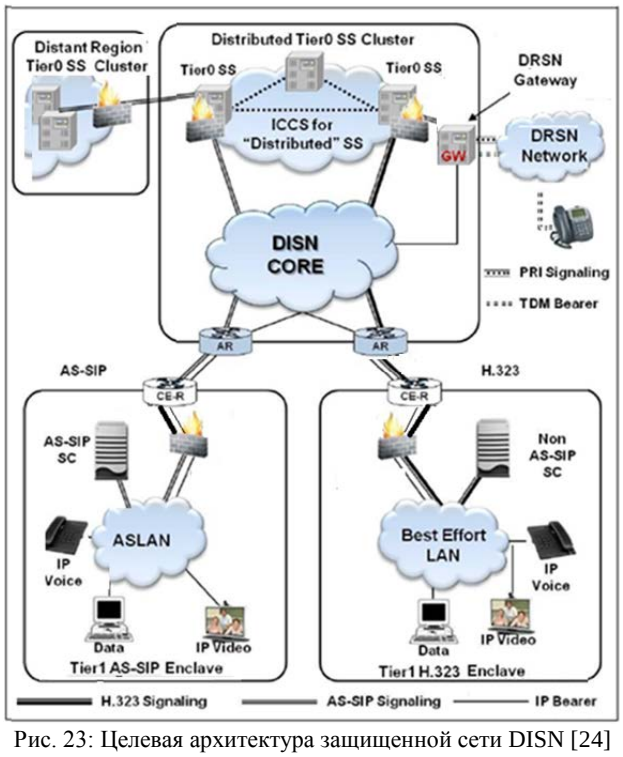


Рис. 23: Целевая архитектура защищенной сети DISN [24]

### *B. Правительственная сеть DRSN как «родимое пятно» в среде IP*

В период Кубинского ракетного кризиса в октябре 1962 года, когда мир был на грани ядерной войны, выяснилось, что существующие способы связи между Вашингтоном и Москвой слишком медленны для принятия решений в кризисных ситуациях. Вашингтону потребовалось почти 12 часов, чтобы получить и расшифровать сообщение Хрущева об урегулировании кризиса, которое состояло из 3000 слов. Чтобы предотвратить риск в будущем, Соединенные Штаты и Советский Союз установили прямую линию связи между двумя столицами в августе 1963 года. В общении политиков горячую линию Вашингтон-Москва прозвали Красным телефоном.

Горячая линия Вашингтон-Москва использовалась в основном для информирования другой стороны о внезапных перемещениях флота или войск, чтобы другая сторона не восприняла это как провокацию или подготовку к агрессии. Как сообщается, горячей линией впервые воспользовались американцы в день убийства президента Кеннеди, 22 ноября 1963 года. Это происходило всего лишь через несколько месяцев после того, как связь была установлена.

Сеть DRSN (Defense Red Switch Network) — это выделенная телефонная сеть, которая обеспечивает управление вооруженными силами США [25]. «Красный телефон» (Secure Terminal Equipment, STE) подключается к сети по ISDN линии и работает на скорости 128 кбит/с (рис. 24). Для передачи данных и факсимиле встроен порт RS-232. Вся криптографическая информация хранится на карте (щель для карты — слева внизу на изображении телефона). Обратите внимание на 4 кнопки наверху телефона — для выбора приоритетности разговора (рис. 25).

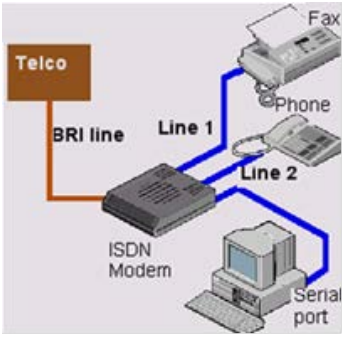


Рис. 24: Схема ISDN

Рис. 25: Телефон секретной связи STE (производитель L-3 COMMUNICATIONS)

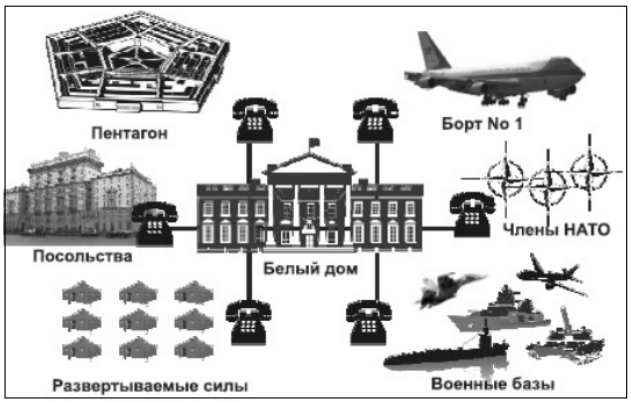


Рис. 26: Схема правительственной сети DRSN

«Красные телефоны» общаются по протоколу SCIP (Secure Communications Interoperability Protocol). Это — межнациональный протокол сил НАТО для обеспечения закрытой передачи речи и данных по множеству сетей: наземная телефонная сеть, радио военного назначения, спутниковая связь, Интернет-телефония, разные стандарты мобильных сетей (рис. 26). Протокол взаимодействия безопасных коммуникаций SCIP разработан в США. Он обеспечивает защищенную передачу голоса и данных по предварительно установленному сквозному каналу (т.е. работает в сети коммутации каналов, а не коммутации пакетов). SCIP поддерживает ряд различных режимов, включая национальные и многонациональные режимы, в которых используются разные методы криптографии. Стандарт SCIP состоит из нескольких компонентов: управление ключами, сжатие голоса, шифрование и планы сигнализации для передачи голоса, данных и для мультимедийных приложений.

*Управление ключами.* Чтобы установить безопасный вызов, необходимо согласовать новый ключ шифрования трафика (Traffic Encryption Key, TEK). Для обеспечения безопасности секретного вызова сигнализация SCIP использует усовершенствованную систему обмена сообщениями FIREFLY. FIREFLY — это система управления ключами, разработанная в АНБ (NSA), основанная на криптографии с открытым ключом.

*Сжатие голоса* происходит с помощью вокодеров (Voice Coders). SCIP может работать с различными вокодерами. Стандарт требует, как минимум, поддержку кодера линейного предсказания со смешанным возбуждением (mixed-excitation linear prediction, MELP). MELP работает на скорости 2400 бит/с, отправляя 54-битный кадр данных каждые 22,5 миллисекунды.

*Шифрование.* Безопасность, используемая многонациональным и национальным режимами SCIP, определяется семейством документов SCIP 23x. Протокол SCIP 231 определяет криптографию на основе стандарта AES, который можно использовать на международном уровне. SCIP 232 определяет альтернативные многонациональные криптографические решения.

Терминал STE стоит дорого – более 3000 долларов (по ценам 2008 г.), не считая криптокарты, а его

эксплуатации требует высокой квалификации, поэтому ведомства не спешат с отказом от прежней версии «красного» телефона STE-III со «старой» версией криптозащиты (несовместимой с STE). Специалисты службы секретной связи весьма консервативны и придерживаются проверенных решений, поэтому неудивительно, что в защищенных (классифицированных) сетях по-прежнему используются не только цифровые решения TDM и ISDN, но и более дешевые телефоны, подключаемые по аналоговой линии. Например, Агентство национальной безопасности только в начале 2019 года объявило о прекращении поддержки проводного терминала Sectéra (Sectera Wireline Terminal SWT), производимого компанией General Dynamics, поскольку SWT не отвечает новейшим криптографическим требованиям АНБ [26].

### *C. Регулятор армии США борется за IP-технологии: Выполнима ли миссия?*

По мнению экспертов AT&T [27], Министерство обороны (DoD) сегодня все еще имеет много устаревшей техники связи: аналоговую инфраструктуру, мультиплексирование с временным разделением (TDM) и даже инфраструктуру с асинхронным режимом передачи (ATM), содержание и ремонт которой требует миллиарды долларов из годового бюджета Министерства обороны США, при этом, по мнению AT&T, излишне подвергая Министерство обороны рискам кибербезопасности. Устаревшая сетевая архитектура основана на двухточечных схемах соединений коммутации каналов и требует постоянного обслуживания и обновления оборудования. Нынешняя ситуация частично является результатом организации оборонных контрактов, а не виной сетевых провайдеров. Примерно 15 000 отдельных сетей, составляющих общую сеть Министерства обороны США, были построены сотнями различных компаний, которые сами не занимаются сетевым бизнесом. Почему министерство обороны должно отдавать создание сетей сторонним подрядчикам, чьими сетями затем управляет AT&T? «Существующая среда TDM отстает от нынешних коммерческих технологий на 30 лет», — таков резкий упрек AT&T [27].

Аналогичный суровый приговор деятельности Министерства обороны в неявной форме содержится в Постановлении армии AR 25-13 [28] от 2017 года, касающегося телекоммуникационных систем и услуг. Армейский регулирующий орган признает, что в сети имеется «старое» оборудование: TDM, ISDN, средствами коммутации каналов предоставляются также видео услуги. Все эти услуги обязаны использовать IP-технологии. Назовем несколько характерных положений из документа AR 25-13:

*4–2. d. Команды, которым необходимо приобрести или заменить существующие коммутаторы Multilevel Secure Voice (ранее известные как Defense Red Switched Network, DRSN), для получения разрешения должны предоставить подробное обоснование и заявление в контрольный орган CIO/G-6.*

*4–2. e. Вводится мораторий на инвестиции в устаревшее оборудование коммутации каналов [..] Армия должна как можно скорее перейти на архитектуру «Everything-over-Internet Protocol», включая унифицированные коммуникации (Unified Capabilities, UC).*

*4–4. Все армейские организации прекратят инвестиции в (неэкстренные) цифровые сети ISDN [..]. Все армейские организации перейдут с ISDN на предоставление всех услуг по IP технологии, включая, помимо прочего, видео-, факсимильные, голосовые и другие сетевые услуги.*

*7–4. Секретная IP-голосовая связь является предпочтительным для армии способом обеспечения секретности. Новейший документ по унифицированным коммуникациям UCR является руководством по реализации секретной IP-голосовой связи. UCR требует, чтобы средства секретной IP-голосовой связи мигрировали на оборудование с использованием протокола AS-SIP.*

Сделаем комментарий к перечисленным требованиям. Заметим, что в Статье 4-2.d отсутствует категорическое требование на переход к Интернет-техногогиям в правительственной сети DRSN, а в Статье 4-4 отказ от ISDN упомянут только для неэкстренных вызовов.

Требования документа AR 25-13 (2017 года) к модернизации армейских сетей связи и услуг (данные, видео и голос) более подробно изложены в документе AR 25-1-1 (2019 года) и в весьма категорической форме [29], а именно:

1) запрет на инвестиции в оборудование ISDN,

2) непременная миграция «Everything over Internet Protocol»,

3) запрет на дальнейшие инвестиции в оборудование коммутаторы асинхронного транспортного режима (ATM).

Благие намерения!

### *D. Технология ATM*

Явное упоминание технологии ATM в открытом документе AR 25-1-1 требует комментариев. Заметим, что коммутаторы ATM установлены на двух важнейших сетях:

(1) на объединённой глобальной сети разведывательных коммуникаций (Joint Worldwide Intelligence Communications System, JWICS) и

(2) на сети управления спутниками AFSCN (Air Force Satellite Control Network).

Упоминание ATM означает, что эта технология сохранилась по крайней мере с начала 1990-х, то есть около 30 лет. Вряд ли офицеры, отвечающие за киберзащиту этих важнейших для национальной безопасности сетей, так легко согласятся на переход от проверенного ATM оборудования к заведомо более уязвимому IP оборудованию.

Для читателей молодого поколения напомним в двух словах суть ATM (Asynchronous Transfer Mode). В

коммутаторах ATM реализована своеобразная коммутация каналов в сочетании с коммутацией пакетов (рис. 27). По технологии ATM передаваемая информация делится на ячейки фиксированной длины. Ячейка ATM имеет длину в 53 байта и состоит из «заголовка» и «полезной нагрузки». Полезная нагрузка (48 байтов) содержит информацию для передачи (голос, данные или видео), а заголовок (5 байтов) используется для механизма адресации и указания пути передачи данной ячейки через коммутатор. Технология ATM была изобретена в начале 1980-х годов. Стандарт ATM был принят в ITU в 1988 году. Технология коммутации ATM вместе с средсвами транспорта синхронной цифровой иерархии SONET/SDH должен был стать основой общедоступной широкополосной сети ISDN (B-ISDN).

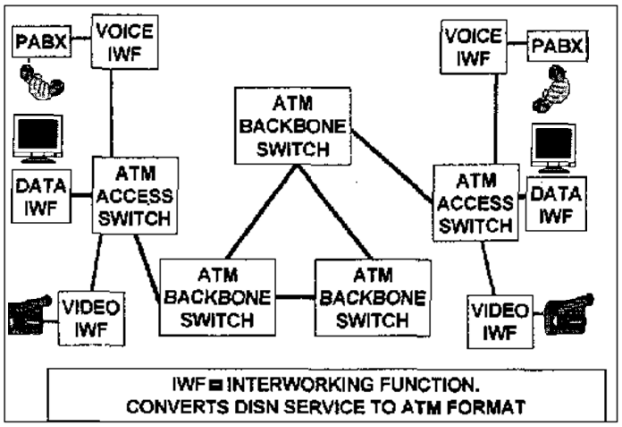


Рис. 27: Архитектура ATM

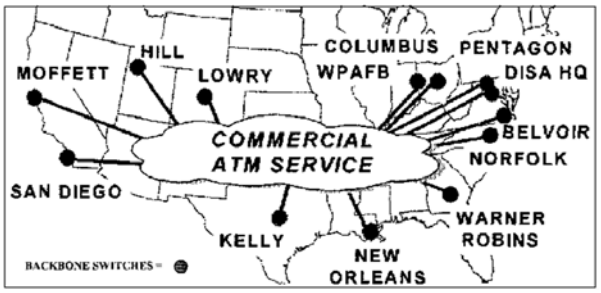


Рис. 28: Базовая сеть DISN ATM, 1996 [30]

В начале 1990-х технология ATM стала самой популярной. Была создана базовая сеть ATM коммутаторов на всей территории США (рис. 28). Агентство DISA в 1993-1994 годах на базе ATM создало широкополосную сеть передачи информации на Гавайских островах. К концу 1998 г. сеть DISN ATM охватывала 125 военных баз, в 1999 г. планировалось расширение сети ATM до 200 объектов. Однако дальнейшие планы установки коммутаторов ATM на сети DISN приостановило принятие в 1995 году стратегии «Joint Vision 2010» [31], что привело к переходу на ранее апробированную технологию коммутации каналов, точнее, на протокол сигнализации SS7 и интеллектуальную сеть AIN.

Новую доктрину «Joint Vision 2010» издал генералом Дж. Шаликашвили, и она вплоть до настоящего времени является краеугольным документом для систем управления, контроля, связи и компьютеров (C4 - Command, Control, Communications, Computers). «Развитие DISN будет эволюционным процессом, который поддержит движение вооруженных сил в информационную эпоху 21-го века и заменит отдельные унаследованные системы связи бесшовным транспортом», — приказал генерал Шаликашвили в начале своей службы в качестве председатель Объединенного комитета начальников штабов США[1].

Немалую роль в отказе от коммутаторов ATM сыграл и Интернет: продукция коммутации пакетов оказалась более дешевой (ее киберуязвимость тогда не смогла быть осознана). Ключевым моментом стало появление веб-технологий, а именно, в 1993 году появился веб-браузер Mosaic, который начал молниеносно захватывать рынок. Началась борьба между сторонниками «старой» технологии коммутации каналов и новой технологии коммутации пакетов. Началась борьба, которая продолжается и по сей день.

### *E. Почему не удается перестроить DISN*

Существенным тормозом внедрения новой техники на информационных сетях является все усложняющееся программное обеспечение. Приведем два примера.

С самого начала принятия программы «Joint Vision 2010» за интеллектуальную сеть AIN в составе глобальной оборонной сети DISN отвечает компания Lockheed Martin [32]. Появление все новых вооружений и новых сервисов требует непрерывного совершенствования средств AIN. Об этом свидетельствуют приглашения на работу в Lockheed Martin, например, на сайте для ветеранов: *lockheedmartin-veterans.jobs.* Там названы требования к набору аналитиков информационных систем для работы в оборонном агентстве DISA (Форт Мид, штат Мэриленд):

- необходимо понимать оборонную доктрину США и как эффективно использовать тактические и стратегические телекоммуникационные системы,
- применять специальные знания военных свойств, встроенных в аппаратную и программную часть сети, для обеспечения боевых действий,
- внедрять и расширять возможности AIN,
- обеспечить выполнение требований криптографических систем, используемых в сети,
- иметь опыт работы с одной или более системами: IP маршрутизация; QoS/MPLS;

[1] Джон Шаликашвили (1936 – 2011) – человек чрезвычайно удивительной судьбы. Он служил на всех уровнях командования от взвода до дивизии. С 1992 по 1993 год служил верховным главнокомандующим объединенными силами США в Европе. Шаликашвили был первым человеком иностранного происхождения, который стал председателем Объединенного комитета начальников штабов (с 1993 по 1997 год). Он родился в Варшаве, Польша, в семье грузинского офицера-эмигранта Дмитрия Шаликашвили и его жены русского происхождения графини Марии Рюдигер-Беляевой. Оба родителя имеют аристократическую родословную.

расчеты трафика; расчеты каналов сети; DNS; ATM коммутация; VPN; TDM коммутация; волоконная техника; Crypto; сетевые применения (WAN ускорители и др.); голосовые и видеосервисы.

И самое важное – приглашаются на работу *ветераны с 28-летним работы,* т.е. имеющие опыт работы с сетями коммутации каналов. Молодые специалисты, выросшие в среде веб-программирования, по-видимому, не в силах поддержать и развивать существующие сети AIN, построенные на технике коммутации каналов.

Второй пример относится к рассмотренному ниже скандалу с провалом грандиозного плана Пентагона по установке стеков кибербезопасности JRSS. Сложность задачи, в частности, характеризует набор требований к потенциальным разработчикам JRSS, указанных в приглашениях на работу в компанию Leidos. Требуется опыт работы от 12 до 14 лет и знание как минимум двух или более продуктов 11 компаний, которые разрабатывают средства киберзащиты, а именно: ArcSight, TippingPoint, Sourcefire, Argus, Bro, Fidelis XPS, Niksun FPCAP, Lancope, NetCool, InfoVista и Riverbed. Отметим, что каждая из этих компаний предоставляет свой сложный комплекс программного обеспечения для киберзащиты. Как их совместить в составе JRSS? Как нанять столь высококлассных разработчиков программного обеспечения, к тому же для работы в сверхсекретной среде? Не удивительно, что программа JRSS провалилась.

## VI. Сеть на кристалле NoC: КК против КП

### A. *Как устроена сеть NoC*

С развитием микроэлектроники появилась возможность на одном кристалле, помимо процессорного ядра, разместить большое количество сложных функциональных узлов. Появилось новое направление техники – сеть на кристалле (NoC, Network on a Chip). Схемы NoC изначально строили для пакетной коммутации, рассматривая коммутацию каналов как побочный вариант. В последнее же время появились работы, говорящие об обратном: на рынке NoC изделия КК (CS, Circuit Switching) могут взять верх над КП (PS, Packet Switching).

На рис. 29 показан пример сложной схемы: так называемая сеть на кристалле (NoC) [33]. В монокристалле много знакомых элементов: центральный процессор (CPU); память (MEM); ввод/вывод (I/O); интерфейс USB, Ethernet и другие. В основном, они общаются с помощью шин, но вопрос, относящийся к данному разделу, заключается в том, как построить центральную часть — коммутационную сеть между шинами.

На рис. 30 показана сеть NoC для пакетной коммутации (PS NoC). Каждый узел S имеет некоторый ресурс (процессор CPU, память MEM, устройство ввода/вывода IO и другие узлы), который общается с узлом S по интерфейсу RNI (Resource-Network-Interface).

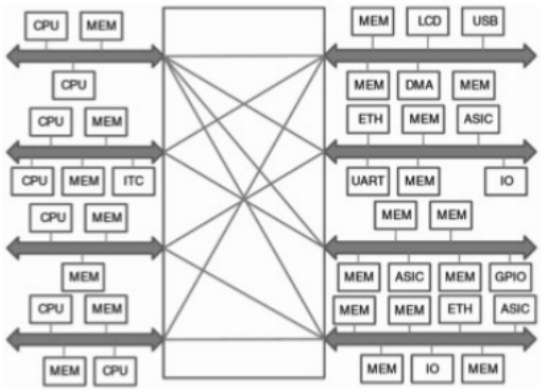


Рис. 29: Пример монокристальной микросхемы (NoC) [33]

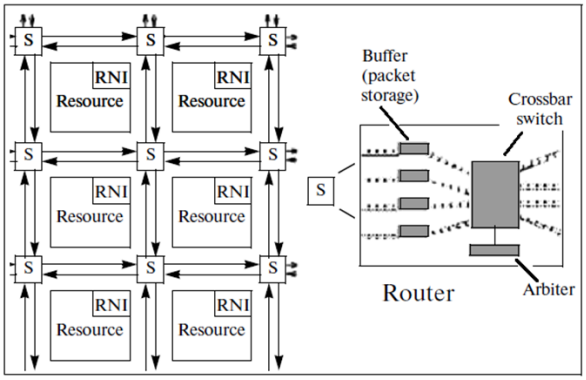


Рис. 30: Сеть на кристалле из 9-ти узлов (слева), каждый узел S представляет собой маршрутизатор с 4-мя входами и выходами (справа) [33]

Сравним два режима коммутации PS-NoC и CS-NoC.

*Коммутация пакетов в сети PS-NoC.* На рис. 31 показан механизм передачи сообщений, поступающих на вход микросхемы. Сообщение разбивается на более мелкие части в зависимости от разрядности устройств (обычно это определяет количество параллельных проводов между блоками). Сообщения разбиваются на пакеты, а те, в свою очередь, на более мелкие блоки: Flit и Phit (часто длины Flit и Phit совпадают). Phit — это единица данных, передаваемых между узлами за один цикл работы чипа.

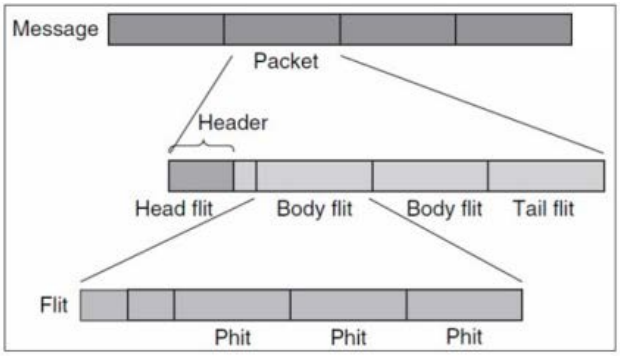


Рис. 31: Разделение сообщений на более короткие фрагменты при передаче сообщения чипом [34]

Обычно маршрутизатор использует адрес получателя, указанный в заголовке пакета, и по таблице маршрутизации определяет путь, по которому следует

пересылать пакеты данных. Таблица маршрутизации состоит из некоторого числа записей — маршрутов, в каждой из которых содержится:

• идентификатор сети получателя (состоящий из адреса и маски сети);

• адрес следующего узла, которому следует передавать пакеты;

• административное расстояние — степень доверия к источнику маршрута;

• некоторый «вес» записи — метрика. Метрики записей в таблице играют роль в вычислении кратчайших маршрутов к различным получателям.

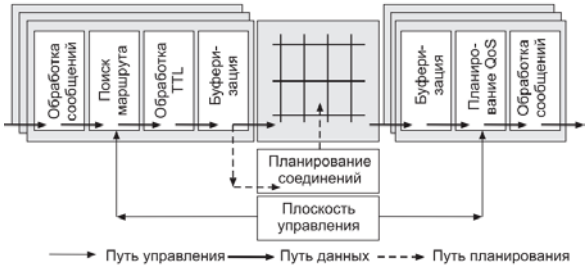


Рис.32: Функциональные блоки маршрутизатора [34]

Проследим алгоритм маршрутизатора (рис. 32):

• модуль обработки сообщений (framing) извлекает входящий пакет из кадра канального уровня;

• модуль поиска маршрута (route lookup) определяет его следующий шаг и выходной порт;

• после поиска маршрута выполняется несколько операций: уменьшается Time-To-Live поле, обновляется контрольная сумма пакета и т. д.;

• затем пакет посылается в выходной порт с помощью коммутатора (router's interconnect);

• конфликтующие пакеты должны быть поставлены в очередь во входном порту и/или выходном порту;

• в выходной линейной карте маршрутизатор планирует передачу согласно требованиям QoS;

• наконец, пакет помещают в выходной кадр и отправляют на следующий узел.

*Коммутация каналов в сети CS-NoC.* Коммутация каналов, по своей сути, значительно проще пакетной коммутации, требует меньше работы для передачи данных и, следовательно, будет стоить меньше. А в результате будет потреблять меньше энергии, будет занимать меньше места.

Основное различие между маршрутизатором и коммутатором каналов заключается в организации выхода. В маршрутизаторе пакеты могут поступать в любое время, поэтому приходится решать конфликты между пакетами путем их буферизации. Напротив, при коммутации каналов информация, принадлежащая данному потоку, может поступать только по заранее определенному каналу, который заранее резервирован для этого конкретного потока. Никаких конфликтов или незапланированных поступлений не происходит, что позволяет коммутаторам каналов избавиться от буферизации, оперативного планирования межсоединений и большей части обработки данных по пути передачи. На рис. 33 показаны функциональные блоки NoC в режиме коммутации каналов. Как видите, путь данных намного проще.

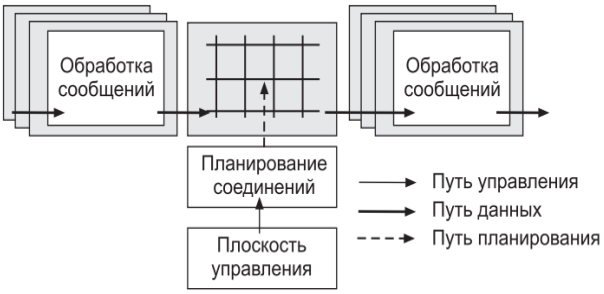


Рис. 33: Функциональные блоки NoC в режиме КК [34]

Коммутация каналов, по своей сути, значительно проще пакетной коммутации, требует меньше действий для передачи данных, потребляет меньше энергии, следовательно, будет стоить дешевле. Правды ради следует отметить, что плоскость управления в режиме коммутации каналов становится более сложной: она требует новой сигнализации для управления каналами. Но это сказывается лишь в тех случаях, когда в потоке сообщений преобладают короткие пакеты.

### *B. Примеры сравнения технологий КК и КП*

*MPEG-4 декодер, Тайвань [35].* Начнем с конкретного массового изделия. MPEG-4 – это широкоприменяемый международный стандарт (с 1998), используемый преимущественно для сжатия цифрового аудио и видео. Инженеры университета в Тайване в 2006 г. представили прототипы MPEG-4 декодера с использованием технологии 0.18 μm, реализованные в двух вариантах: коммутации каналов CS NoC и пакетов PS NoC. Результаты испытаний убедительно показали преимущество коммутации каналов. Вариант CS NoC оказался выгоднее варианта PS NoC по всем показателям (Таблица 1), особенно выделяется показатель потребляемой электроэнергии – в 45 раз.

*Таблица 1.* Сравнение решений MPEG-4 декодера в вариантах CS NoC и PS NoC.

| | CS NoC | PS NoC |
|---|---|---|
| Площадь (μм$^2$) | 56.26 x 10$^3$ | 649.27 x10$^3$ |
| Потребление (μW) | 260.6 | 11793.69 |
| Задержка (ns)/switch | 3.48 | 29.66 |
| Пропускная способность (10$^6$ ns) | 2.16 | 12.04 |

*Эксперимент Королевского технологического института, Швеция [36].* Шведские инженеры в 2013 г. представили результаты сравнения трех решений NoC:

CS-NoC с полем 4 x 4 коммутатора,

PS-NoC с таким же полем: 4 виртуальных канала и 4 буфера (ps_v4_b4),

PS-NoC: 16 виртуальных каналов и 16 буферов (ps_v16_b16).

Измерения показали, что в подавляющем диапазоне

нагрузок выгоднее пользоваться коммутацией каналов CS-NoC (рис. 34). Первый вариант коммутации пакетов PS-NoC (ps_v4_b4) имеет преимущество только для пакетов длиною всего 500 байтов, второй вариант PS-NoC (ps_v16_b16) сохраняет преимущество до пакетов длиною в 800 байтов. При длине пакетов в 5120 байтов пропускная способность обоих вариантов PS-NoC выравнивается. Если же пакеты имеют длину более 500-800 байтов, то выгоднее пользоваться коммутацией каналов CS-NoC.

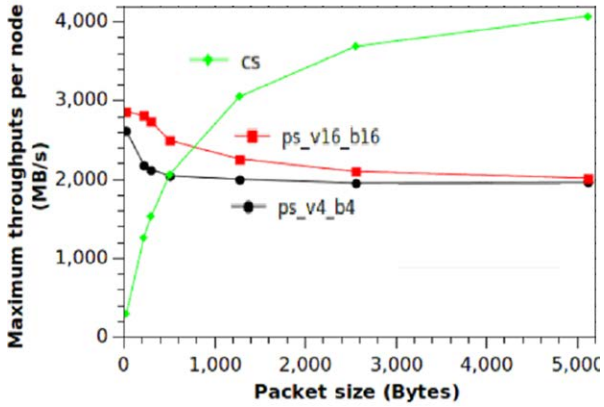


Рис. 34: Сравнение пропускной способности CS-NoC и PS-NoC в зависимости от длины пакета

*Феноменальный успех Intel [37, 38].* В феврале 2014 г. компания Intel объявила о разработке микросхемы (рис. 35), которая содержит сеть, состоящей из матрицы в 256 узлов (16 x 16). Эта сеть является мощнейшим синхронным гибридным коммутатором с общей пропускной способностью до 20,2 Тбит/с (при условиях: 0,9 В, 25°C). Микросхема разработана по технологии 22 nm tri-gate CMOS при параллельной передаче 112 битов и длине соединений 855 µm. Микросхема коммутирует как пакеты (что сейчас общепринято), так и каналы, и наибольшая производительность достигнута при сочетании обоих режимов.

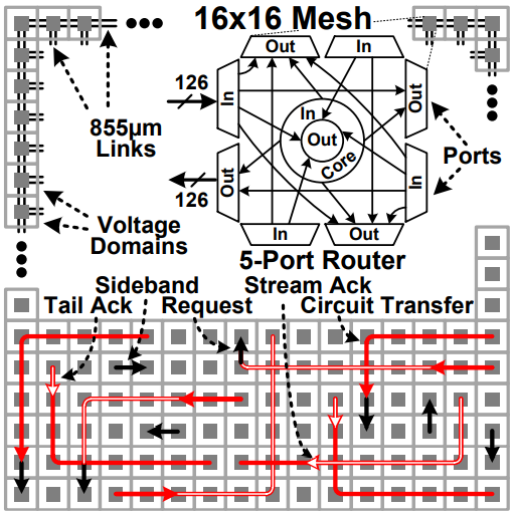


Рис. 35: Общий вид микросхемы 16×16 узлов [37]

Математические модели изучения пропускной способности NoC см. [38].

## VII. Киберуязвимость – главный порок Интернет-технологий

### A. *Единая архитектура безопасности SSA*

В октябре 2010 года было создано Киберкомандование армии США (U.S. Army Cyber Command). USCYBERCOM теперь входит в состав Стратегического командования вместе со стратегическими ядерными силами, противоракетной обороной и космическими силами [39].

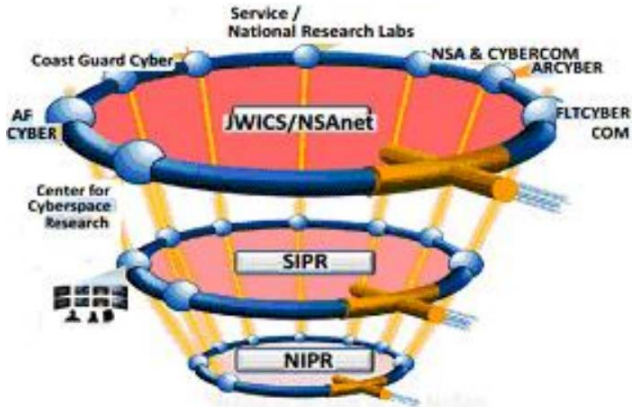


Рис. 36: Три уровня единой архитектуры безопасности – по мере роста секретности [40]

Одной из ключевых задач Киберкомандования является создание Единой информационной среды (Joint Information Environment) на основе единой архитектуры безопасности Single Security Architecture (рис. 36).

Стоит отметить, что действия Киберкомандования США значительно замедляют переход к IP-технологиям, так как Киберкомандование требует сбора ситуационной информации от множества элементов сети. Решение задач киберзащиты кардинально меняет все планы развития сети DISN.

Сама концепция Единой информационной среды (Joint Information Environment, JIE) чрезвычайно сложная. Суть концепции JIE заключается в создании общей военной кибербезопасной инфраструктуры. В соотетствии с требованиями SSA, основными компонентами среды JIE являются объединенные региональные стеки безопасности JRSS (Joint regional security stacks). Они обеспечивают единый подход к структуре кибербезопасности, к защите компьютеров и сетей во всех военных организациях.

### B. *Региональные стеки безопасности JRSS*

JRSS представляет собой чрезвычайно сложный вычислительный комплекс, который выполняет функции брандмауэра, обнаружения и предотвращения вторжений, управления предприятием, виртуальной маршрутизации и переадресации, обеспечивает множество других требований сетевой безопасности. Оборудование JRSS, по сути своей, представляет собой громадных размеров IP-маршрутизатор со сложным набором программного обеспечения для киберзащиты. Например, типичный физический стек NIPR JRSS состоит из 20 стоек (рис. 37).

Рис. 37: Оборудование стека NIPR JRSS – 20 стоек

Первый стек JRSS был установлен и успешно работает на военной базе Сан-Антонио, штат Техас. В 2014 г. было установлено 11 стеков JRSS в США, 3 стека на Ближнем Востоке и один в Германии. Общий объем работ включает установку 23 стеков JRSS в сервисной сети NIPRNet и 25 стеков JRSS в секретной сети SIPRNet (рис. 38). К 2019 году планируется перевести на эти стеки программы кибербезопасности, которые сейчас развернуты более чем в 400 локациях [39].

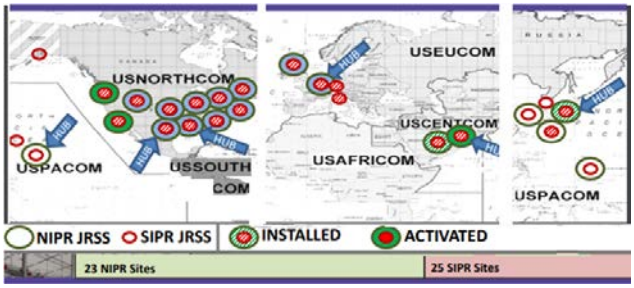


Рис. 38: Текущие/планируемые стеки JRSS в силах НАТО (2019 г.) [42]

Стеки JRSS контролируют безопасность корневой сети DISN. На рис. 39 показаны трое ключевых позиций JRSS.

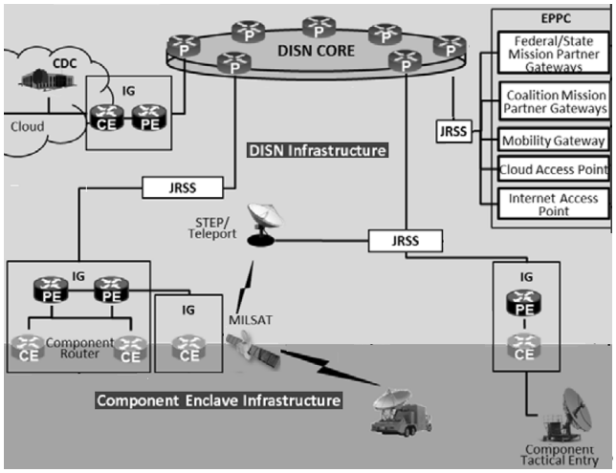


Рис. 39: Схема сети DISN и ключевая роль JRSS [43]

### *C. Провал программы JRSS*

По программе JRSS, этому оборудованию предстояло заменить около 1000 нестандартных стеков сетевой безопасности, которые в настоящее время разбросаны по всему миру [44]. Предстояло установить 48 новых стандартизированных стеков в 25 местах, «уменьшив количество возможностей для кибератак» [45]. Реализация полной программы JRSS обошлось бы налогоплательщикам в несколько миллиардов долларов. Счетная палата США уделяла особое внимание обоснованности бюджетных трат по программе JRSS. Проследим хронологию реализации программы JRSS до ее провала.

Июль 2016 г. Отчет GAO-16-593 [46] требует большего контроля за расходованием средств по программе JRSS и на создание информационной среды JIE в целом. В отчете ГАО говорится:

*«Министерство обороны (DOD) планирует потратить к концу этого финансового года почти 1 миллиард долларов на внедрение только одного элемента JIE. Однако ведомство не полностью определило объем JIE или его ожидаемую стоимость. Оценка затрат на JIE затруднена из-за размера и сложности инфраструктуры ведомства и подхода к реализации JIE, однако без информации об ожидаемых затратах на JIE возможности чиновников контролировать и принимать эффективные решения о ресурсах ограничены».*

Ноябрь 2016. Директор по информационным технологиям Министерства обороны Терри Халворсен (Terry Halvorsen) нападает на GAO [47], они, мол, не понимают, что такое Единая информационная среда: *«Мы пытались сказать GAO, что в данном случае не следует измерять JIE — вы должны измерять ее компоненты».* JIE состоит из различных программ, таких как стеки безопасности JRSS и компьютерные сети стран-партнеров. JRSS, например, стремится объединить 1000 устаревших стеков сетевой безопасности в 48 стандартизированных стеков в 25 точках по всему миру. По мнению Халворсена, там есть конкретные показатели для измерения.

Февраль 2017 г. Министерство обороны к результатам аудита GAO отнеслась серьезно, заверило, что предпримет шаги для выполнения всех рекомендаций GAO относительно JIE. Однако Директор по информационным технологиям Халворсен подал в отставку.

Январь 2018 г. Под давлением критики GAO Глава управления по приему новых вооружений Пентагона заявил, что Министерству обороны следует прекратить развертывание программы стеков сетевой безопасности JRSS. Он заявил, что во время испытаний в ВВС текущая версия оборудования JRSS не смогла предотвратить кибернападение на сеть [48].

Февраль 2018 г. Несмотря на критику GAO, Министерство обороны объявило о продолжении программы JRSS. Министерство обороны уже установило 14 из 23 стеков NIPR JRSS, запланированных для сети в США, Европе,

Тихоокеанском регионе и юго-западных регионах Азии; установку последнего стека безопасности планируется завершить к концу 2019 года [49].

В это время в прессе уже стали появляться рассуждения о целесообразности проекта JRSS в целом. Как приговор судьбе проекта JRSS звучало утверждение [50], что JRSS действует слишком медленно (too S-L-O-W).

17 мая 2018 г. Во время пресс-конференции официальные лица DISA признали некоторые проблемы с производительностью программ JRSS. В оправдании было сказано, что текущая версия JRSS является ранним этапом запланированного компьютерного облака для всего Министерства обороны, но признали, что передача данных из облака к пользователю занимает слишком много времени, а именно - JRSS работает слишком медленно [51].

Ноябрь 2021 г. Директор по информационным технологиям Министерства обороны объявил о закрытии программы Joint Regional Security Stacks [52]. Таким образом, Пентагон приостановил проект кибербезопасности, на который истратили 2 миллиарда долларов.

12 мая 2021 г. Предидент США Дж. Байден издал распоряжение об обеспечении национальной кибербезопасности, в котором содежится требование к Федеральному правительству о повсеместном внедрении архитектуры нулевого доверия (Zero Trust Architecture) [53]. Министерство обороны объявило о переходе на новую технологию киберзащиты под названием Thunderdome. В результате вся программа JIE подвергается «капитальному ремонту». Время покажет, будет ли проект Thunderdom более успешным, так как переход на облачные вычисления предполагает использование не менее сложного программного обеспечения.

### *D. Что такое архитектура нулевого доверия*

«Архитектура нулевого доверия» (Zero Trust Architecture, ZTA) – новый метод проектирования инфраструктуры кибербезопасности сети (рис. 40). Этот метод соответствует русской поговорке «доверяй, но проверяй». По своей сути Zero Trust работает по принципу отсутствия неявного доверия к любой части сети, то есть организация не должна доверять никаким запросам без проверки, независимо от того, исходит ли запрос изнутри или за пределами ее периметра [54].

Напомним, что сетевая безопасность в целом связана с доступом. Чтобы получить доступ к ресурсу, любой пользователь должен подтвердить свою личность, указав учетные данные, и тем самым завоевать доверие сети. Традиционный подход к обеспечению безопасности «замок и ров» основан на защите периметра. При входе в охраняемую область проверяются учетные данные и после их подтверждения доступ предоставляется. Однако такая практика таит в себе потенциальные угрозы безопасности. Достаточно одной точки взлома, например, наличие сервера с устаревшим программным обеспечением, что может стать лазейкой для всей сети. Так произошло во время недавней атаки на *Colonial Pipeline* [55].


Рис. 40: Схема *Colonial Pipeline*

*Colonial Pipeline* — крупнейшая трубопроводная система для нефтепродуктов в США. Трубопровод, состоящий из двух труб, имеет длину 8 850 км и может транспортировать 3 миллиона баррелей топлива в день между Техасом и Нью-Йорком (рис. 40).

7 мая 2021 года произошла кибератака, которая была самой крупной из известных атак программ-вымогателей на инфраструктуру в Соединенных Штатах. Был остановлен один из двух нефтепроводов *Colonial Pipeline* и прекращена поставка половины нефти к восточному побережью, что вызвало скачок цен и волну панических покупок. Компания через несколько часов выплатила запрошенную хакерской группой сумму (4,4 миллиона долларов); после получения выкупа компьютерная сеть *Colonial Pipeline* была восстановлена.

Кибератаку рассматривал Комитет Сената США. Генеральный директор компании *Colonial Pipeline* признался, что взлом произошел по недосмотру, что хакеры получили доступ через старую виртуальную частную сеть, которая, по мнению компании, вышла из строя. Расследование показало, что для доступа к сети требовался взломать только один пароль.

Как только злоумышленник проникает через защиту периметра, он может свободно перемещаться внутри сети, как ему заблагорассудится. В модели Zero Trust же каждый сетевой запрос следует рассматривать так, как если бы сеть уже была взломана, и даже простые запросы следует рассматривать как потенциальную угрозу. Многофакторная аутентификация и авторизация требуются до начала сеанса или предоставления любого доступа. Более того, всякий раз, когда аутентифицированный пользователь запрашивает доступ к новому ресурсу, его учетные данные необходимо проверять заново.

Трудно утверждать, что новая модель киберзащиты Zero Trust будет более успешной, чем JRSS. Проект JRSS потерпел неудачу из-за медленной работы, что противоречило требованиям сети. В модели Zero Trust число проверок неизбежно возрастает, и на первый взгляд кажется, что работа сети еще больше замедлится. Так ли это?

## VIII. Проклятие киберугроз

### A. *Критика Счетной палаты правительства США*

Проблема кибербезопасности очень сложная, и по мере роста объемов программного обеспечения (ПО) угрозы кибербезопасности постоянно растут. Это особенно актуально в вооруженных силах, где крайне важно разрабатывать системы, которые должны удовлетворять многим требованиям, частично взаимно противоречивым, а именно: обеспечивать ожидаемый уровень конфиденциальности, безотказности, аутентификации, целостности и доступности [56].

В октябре 2018 года Счетная палата правительства США (Government Accounting Office, GAO) сенсационно сообщила [57], что все системы вооружения с программным обеспечением, которые была протестированы в период с 2012 по 2017 год, включая созданные за последние десять лет, имеют киберуязвимости и могут быть взломаны. В ответ на упрек GAO, Генеральный инспектор Министерства обороны в январе 2019 года представил отчет с объемами бедствия, а именно, было обнаружено 266 киберуязвимостей.

При обсуждении ситуации с киберугрозами нельзя игнорировать и фактор стоимости борьбы с киберугрозами, что создает своего рода порочный круг. Пентагон за новые цифровые системы с программным обеспечением платит больше денег, чем стоили их аналоговые предшественники. К тому же каждая из этих более дорогих систем повышает уязвимость для взлома, а это означает, что Пентагону нужно тратить все больше средств на их защиту. В 2019 финансовом году Минобороны потратили почти 8,5 млрд. долларов на усилия по обеспечению кибербезопасности.

В борьбе с киберугрозами можно выделить три положения [58].

*Сложность ПО.* Отчеты по тестировании кибербезопасности показали, что испытательные группы (состоящие, как правило, из опытных хакеров) смогли получить несанкционированный доступ и полный или частичный контроль над системами оружия за сравнительно короткий промежуток времени, используя при этом относительно простые инструменты и методы. Возникла угрожающая ситуация.

Системы вооружения Министерства обороны США сегодня больше, чем когда-либо прежде, зависят от программного обеспечения. Объем программного обеспечения в современных системах вооружения растет в геометрической прогрессии, ПО встроено в многочисленные технологически сложные подсистемы, как показано на рис. 41. Любые виды вооружения, начиная от кораблей и самолетов, становятся все более технологичными, используя больше программного обеспечения и меньше аппаратуры для управления всеми функциями [59].


Рис. 41: Встроенное программное обеспечение и системы информационных технологий в системах вооружения (условное изображение для иллюстрации) [57]

*Взаимодействие систем вооружения.* Существующие программы тестирования слишком ограничены, чтобы позволить Министерству обороны получить полное представление об уязвимостях систем вооружения, что усугубляется нехваткой квалифицированных специалистов по тестированию киберугроз. К тому же оружейные платформы на самом деле работают не изолированно друг от друга. Скорее, большинство современных оружейных снаряжений состоят из сложного набора систем, а подразумевают «совместное использование нескольких платформ и систем для выполнения военных задач». Примером может служить система вооружения Aegis[2], которая содержит множество интегрированных подсистем, включая обнаружение, командование и управление, целеуказание и другие возможности. Поэтому оценки уязвимостей, которые определены на отдельных платформах, не могут выявить потенциальные уязвимости, которые могут возникнуть при взаимодействии этих платформ в более широкой сети [59].

Оружейные системы имеют широкий набор интерфейсов, часть из которых не очевидны и могут быть использованы злоумышленниками для доступа к системам, как показано на рис. 42.

Следует также отметить, что оружейные системы подключаются не только к чрезвычайно сложной информационной сети Министерства обороны США, но и к внешним сетям, например к сетям оборонных подрядчиков. Технологические системы, логистика, персонал и системы, связанные с бизнесом, иногда подключаются к тем же сетям, что и системы вооружения. Кроме того, некоторые системы вооружения к сети могут подключаться не напрямую, а опосредованно, например, к системам электроснабжения, которые связаны с общедоступной

[2] Aegis Combat System — американская интегрированная система противоракетной обороны. Она использует мощные компьютерные и радиолокационные технологии для отслеживания и наведения оружия для уничтожения вражеских целей. Первоначально использовался ВМС США, в настоящее время также является частью европейской системы противоракетной обороны НАТО.

сетью Интернета. Если злоумышленникам удается получить доступ к одной из этих систем, они могут получить доступ к любой другой через их соединения.

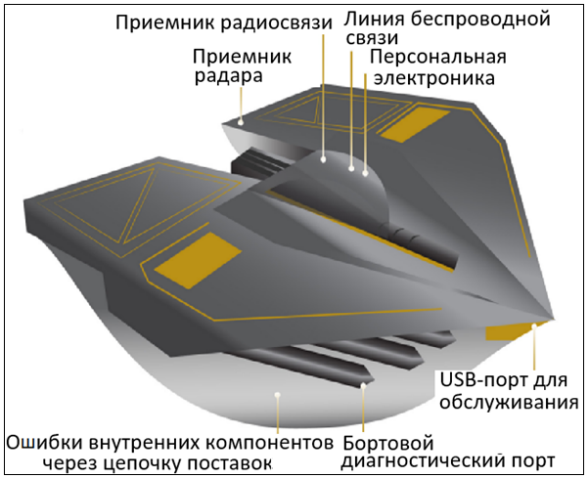


Рис. 42: Вооружение включает в себя многочисленные интерфейсы (условное изображение для иллюстрации) [57]

*Стоимость устранения киберуязвимостей.* Удастся ли кардинально изменить положение с киберзащитой? При анализе угрожающего положения возникает болезненный вопрос оплаты труда. Согласно исследованию RAND [60], проведенному в 2014 году, специалисты, способные обнаруживать наличие сложных угроз или находить скрытые уязвимости в программном обеспечении и в системах, получают от 200 000 до 250 000 долларов в год, что значительно превышает шкалу оплаты Министерства обороны США. Ограниченные ресурсы не позволяют вовремя устранить недостатки. Как показала практика тестирования (рис. 43), программисты уже заранее знали о некоторых уязвимостях систем вооружения, поскольку они были выявлены в ходе предыдущих оценок кибербезопасности. Например, в одном отчете по тестированию указано, что только 1 из 20 киберуязвимостей, выявленных в ходе предыдущей проверки, была устранена.

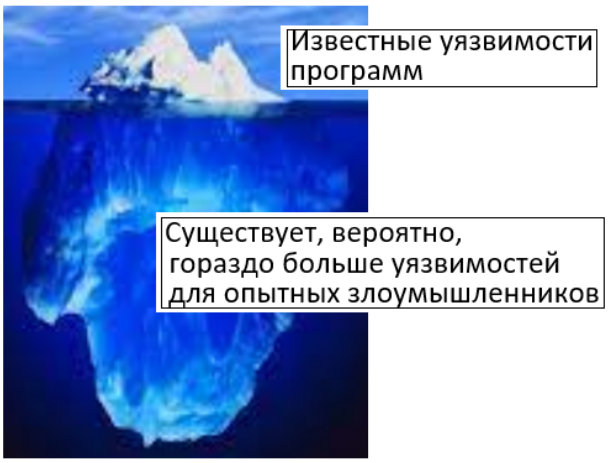


Рис. 43: Айсберг киберуязвимостей

*B. Боевой самолет F-35 – 8 млн. строк программного кода*

Lockheed Martin F-35 Lightning II — семейство удивительных боевых самолетов будущего: одноместных, одномоторных, построенных по технологии *stealth*, всепогодных, многоцелевых, предназначенных как для завоевания господства в воздухе, так и для нанесения ударов [61].

Самолет разрабатывает Lockheed Martin с 2001 года – после победы над Boeing в схватке за программу Joint Strike Fighter. Первый самолет F-35B поступил на вооружение Корпуса морской пехоты США в июле 2015 года, за ним последовали F-35A для ВВС США в августе 2016 года и F-35C для ВМС США в феврале 2019 года. США планировало закупить 2456 самолетов F-35 до 2044 года. Предполагается, что самолет будет на вооружении до 2070 года (рис. 44).

Программное обеспечение самолета было разработано в виде шести выпусков или блоков:

- Первые два блока, 1A и 1B, обеспечили обучение пилотов F-35 и тестирование многоуровневой безопасности.
- Block 2A улучшил возможности обучения пилотов и обслуживающего персонала.
- 2B был первым боеспособным выпуском, запланированным для морской пехоты США.
- Окончательная версия – Block 3F – имеет все базовые боевые возможности.

Наряду с выпусками программного обеспечения каждый блок сопровождало обновление аппаратного обеспечения авионики и усовершенствование летательных аппаратов – по результатам летных и структурных испытаний. После завершения 17 000 часов летных испытаний в апреле 2018 года компания Lockheed Martin уже считала, что программа Joint Strike Fighter успешно завершена. Но не тут-то было.

Рис. 44: Эскадрилья F-35

Хакерами уже разработаны различные способы удаленного нарушения работы транспортных средств, подключенных к сети. Это является реальной угрозой для такой программы, как F-35 [62]. Недаром Пентагон рекламировал его, пусть и в виде шутки, как «компьютер, которому довелось летать», а подрядчик Lockheed Martin гордился (на своем веб-сайте) 8 миллионами строк программного кода, встроенного в

самолет, который управляет большинством его функций, включая управление полетом, радаром, связью и нацеливанием оружия. Но большой объем ПО неизбежно имеет не только ошибки, но и неустраненные уязвимости. К тому же самолет F-35 работает в сети других авиационных и наземных систем, что дает дополнительные возможности хакерам. Любое из соединений между подсистемами в самолете и/или с другими частями внешней сети вражеские кибервоины могут использовать для проникновения и разрушения или вывода из строя самолета.

Самолет F-35, напомним, как ожидается, будет центральным звеном вооруженных сил США в течение десятилетий, поэтому его уязвимости, выявленные экспертами GAO, воспринимаются как национальное бедствие. В настоящее время программа F-35 Joint Strike Fighter, по-видимому, находится в состоянии приостановленной разработки. Последний отчет (за 2021 год) Дирекции Пентагона по эксплуатационным испытаниям и оценке (DOT&E) указывает на стагнацию, и даже откат в некоторых показателях надежности самолета. Несмотря на более чем 20 лет и примерно 62,5 миллиарда долларов, потраченных только на исследования и разработки, руководители программы до сих пор не смогли создать самолет, который мог бы летать так часто, как это необходимо, и полностью продемонстрировать свои боевые качества. Это ставит военных в невыгодное положение, а персонал подвергает опасности. В общедоступной открытой версии отчета доступны некоторые ключевые выводы [63]:

• Показатели надежности F-35 в течение большей части 2021 года «стояли на месте», а в последние месяцы года даже снизились.

• Руководители программы отказались от усилий по завершению Автономной информационной системы логистики (Autonomic Logistics Information System, ALIS) стоимостью 16,7 миллиарда долларов, так как в процессе тестирования обнаружилось, что нет ни одного раздела программы F-35, защищенного от кибератаки. В 2020 году руководители Пентагона вынуждены были отказаться от всего проекта ALIS и заменить его новой облачной системой под названием Интегрированная сеть оперативных данных (Operational Data Integrated Network, ODIN). Новая система, предназначенная для прогнозирования проблем с техническим обслуживанием и отслеживания деталей и процессов ремонта, работает быстрее и проще в развертывании, чем ALIS, но уже отстает от графика и имеет некоторые из тех же киберуязвимостей. В качестве положительной новости DOT&E сообщает, что базовый комплект ODIN весит всего 202 фунта, версия ALIS весила 891 фунт.

• Среда имитации самолета, призванная стать высокоточным и полностью проверенным имитатором для проверки всех возможностей F-35, в настоящее время отстает от графика более чем на четыре года. Решение о полном производстве не может быть принято до тех пор, пока не будут завершены запланированные 64 испытания модели самолета.

В итоге следует отметить, что, спустя более двадцати лет разработки, самолет F-35 остается, во всех практических и юридических смыслах, не более чем очень дорогим прототипом. Тот простой факт, что подрядчики и Управление программой Joint Strike Fighter не смогли поставить самолет, эффективность которого была бы доказана в ходе полной программы эксплуатационных испытаний, наводит на мысль, что первоначальная концепция истребителя Joint Strike Fighter была ошибочной и выходила за рамки практической технологической реальности. Программа F-35, похоже, останется в своем нынешнем застойном состоянии в обозримом будущем. Конгресс США во время дебатов по бюджету на 2022 финансовый год придерживался твердой позиции и отказался санкционировать дополнительные новые заказы F-35 помимо уже утвержденных запросов Пентагона.

Обратите внимание на роковые слова «концепция Joint Strike Fighter выходила за рамки технологической реальности» [63], т.е., программа F-35 не реализуема при существующем уровне технологического развития. Это очень суровое утверждение. Отнести ли его к уровню технологического развития США? Вполне допустимо, что столь сложные проекты, как F-35 и Zumwalt, использующие чрезвычайно объемное программное обеспечение, в создании которого участвует до сотни организаций, неизбежно сохраняют киберуязвимости. Образно говоря, миссия невыполнима.

### *C. Ракетный эсминец Zumwalt – 6 млн. строк программного кода*

USS Zumwalt (DDG-1000) — ракетный эсминец ВМС США (рис. 45). Корабль назван в честь адмирала Элмо Зумвальта. Это головной корабль класса Zumwalt в серии. Zumwalt построен по технологии *stealth,* имеет исключительную незаметность: несмотря на большие размеры, имеет радиолокационное сечение, подобное рыбацкой лодке. Система вертикального пуска ракет (компания Raytheon) может нести противокорабельные, зенитные и наземные крылатые ракеты; имеет 80 ячеек вертикального запуска ракет (рис. 46).


Рис. 45: USS Zumwalt. Параметры: вес 15 тыс. т, длина 183 м, осадка 25 м, скорость 62 км/ч

Решение о постройке эсминца приняли в июле 2008 г. с графиком завершения строительства в 2013 г. Корабль был сдан в эксплуатацию в Балтиморе 15 октября 2016 г. С течением времени (из-за срыва сроков постройки) ВМС сократили закупку эсминцев класса Zumwalt с 32

до трех [64].

Рис. 46: USS Zumwalt. Система вертикального пуска ракет

USS Zumwalt, как образно выразился репортер [65], будет плавучим центром обработки данных (рис. 47), вооруженным ракетами и роботизированными пушками стоимостью почти 4 миллиарда долларов. ЦОД Zumwalt построен из готового оборудования (commercial-of-the-shelf, COTS) — в основном блейд-серверов IBM под управлением Red Hat Linux, размещенных в защищенной серверной комнате EME. Серверные комнаты представляют собой шестнадцать автономных мини-центров обработки данных, построенных Raytheon. Имея длину 35 футов, высоту 8 футов и ширину 12 футов, эти 16 серверных комнат имеют в общей сложности более 235 стоек оборудования.

Рис. 47: ЦОД Zumwalt в «коробке»

EME подключаются к бортовому Интернету Zumwalt. Сетевая система с резервной коммутацией, управляющая несколькими секционированными сетями, сочетающими оптоволокно и медь, соединяет все системы корабля — внутреннюю и внешнюю связь, вооружение, технику, датчики и т. д. — по Интернет-протоколам, включая TCP и UDP. Почти все внутренние коммуникации корабля основаны на передаче голоса по IP (за исключением нескольких аналоговых телефонов для экстренных случаев). На борту Zumwalt также есть собственная беспроводная сеть для нужд технического обслуживания и чрезвычайных ситуаций.

Системы, которые не предназначены для подключения к IP-сети, объединены с помощью адаптеров на основе одноплатных компьютеров и операционной системы Lynx OS. Вычислительная сеть соединяет все инженерные системы корабля, системы пожаротушения, ракетные пусковые установки, а также средства радио- и спутниковой связи.

Рабочие станции с тремя экранами в Операционном центре, получившие название Common Display System (CDS), оснащены набором материнских плат Intel с четырьмя процессорами в бронированном корпусе. Даже кресла командира и старшего офицера на мостике имеют встроенные рабочие станции CDS.

Zumwalt еще не отправился в плавание, но его программное обеспечение уже обновлялось шесть раз. Когда версия 5 была завершена, компания Raytheon привлекла моряков для тестирования системы, соединив их с имитатором различных боевых сценариев. Извлеченные уроки были учтены в версии 6, а версия 7, как предусмотрено графиком, будет установлена на корабле перед испытательным круизом корабля.

В статье под громким названием «Титановая «жестяная банка» ВМС США» высказана суровая критика нового ракетного эсминца. По мнению репортера [66], «USS Zumwalt стоимостью 8 миллиардов долларов выглядит устрашающе, пока вы не поймете, что в его пушках нет снарядов». Zumwalt представляет собой колосс сложности: 1200 разработчиков программного обеспечения из 30 организаций разработали мозг корабля, управляемый беспрецедентным числом от 14 до 16 миллионов строк компьютерного кода. Более 35 000 сигналов, отслеживающих все, от открывающихся дверей до силовых установок корабля, проходят через 16 «корпусов электронных модулей» размером с железнодорожный вагон, каждый из которых весит 18 тонн и содержит в общей сложности 235 шкафов, заполненных электроникой. Вместо шкипера с жирным карандашом, определяющего курс, скорость и другие важные решения с помощью нескольких вахтенных, большую часть работы выполняет кремний. Он предназначен для облегчения 18 000 задач, выполняемых экипажем, а это означает, что на борту находится меньше моряков, что теоретически снижает стоимость эксплуатации корабля, но усложняет программное обеспечение и, к сожалению, увеличивает киберуязвимость. Репортер заключает [66]: «Пристрастие Пентагона к выбору излишне сложного и дорогого оружия не только угрожает обанкротить национальную казну, но и ставит под угрозу национальную оборону, создавая сокращающуюся и гораздо более хрупкую военную силу».

Пока отсутствуют данные о тестировании киберуязвимостей эсминца Zumwalt (что может таить немало неожиданностей), появилась также крайне важная нерешенная задача – переоснастить корабль гиперзвуковым оружием и научиться перехватывать и

уничтожать нападающее гиперзвуковые ракеты. Дирекция приема вооружений Пентагона отмечает, что служба имеет «ограниченные возможности летных испытаний» для поддержки гиперзвукового оружия на борту кораблей класса Zumwalt [67]. Планы ВМС в настоящее время предусматривают развертывание гиперзвукового оружия на Zumwalt к 2025 финансовому году, а интеграция с подводной лодкой класса Virginia последует в 2028 финансовом году. Задержка с завершением программы гиперзвукового оружия угрожает сохранению превосходству США в мире.

*Справка о гиперзвуковом оружии.* Это ракета, способная осуществлять полёт в атмосфере с гиперзвуковой скоростью (большей или равной 6000 км/ч, т.е. в пять раз выше скорости звука, 5М) и маневрировать с использованием аэродинамических сил (рис. 48). Границы гиперзвуковой скорости обычно связаны с началом процессов ионизации и диссоциации молекул в пограничном слое около ракеты, что начинает происходить примерно при 6000 км/ч.

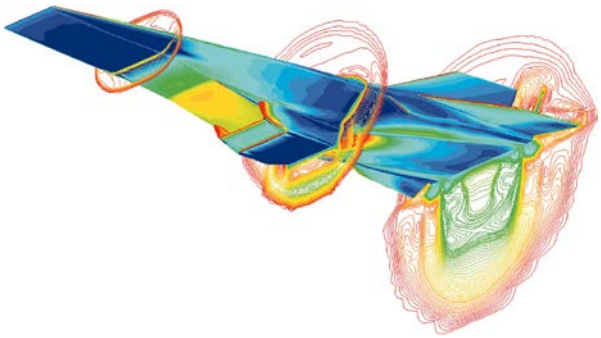

Рис. 48: Моделирование воздушного потока вокруг гиперзвуковой ракеты «X-43» (Боинг) при 7М [68]

Гиперзвуковая ракета «X-43» разрабатывалась в течение долгого времени. В 2004 год прошли успешные испытания X-43A. Начиная с 2006 проект «X-43» сменила новая программа X-51. Первые испытания гиперзвуковой крылатой ракеты X-51 были проведены в 2009 году. Принятие на вооружение было запланировано на 2017 год, однако, на начало 2022 года ракета X-51 на вооружение еще принята не была.

### *D. Ностальгия по вещам простым и надежным*

Оружие, которое нередко считается устаревшим, так как не оснащено новейшими гаджетами, не означает, что этому больше нет места на поле боя. Многие знаковые виды оружия и транспортных средств в американской военной истории достигли своего статуса не потому, что имели передовой дизайн, а потому что были востребованы. Солдаты склонны уважать простое оружие и технологии, на которые можно положиться в боевых условиях. Простые торговые суда (которыми перевозили солдат во время Второй мировой войны), пистолеты M1911 (известные как Colt 1911), которые находились на вооружении армии в течение 75 лет, и джипы (рис. 49) — примеры простых изделий, которые делали именно то, что нужно было делать. Американцы до сих пор видят джипы на дорогах, потому что солдаты полюбили их..

Рис. 49: Джип

Джипы можно было использовать как пулеметные платформы, импровизированные машины скорой помощи или для транспорта пушек. При цене 650 долларов за штуку (около 9000 долларов сегодня) джип был дешевым, достаточно прочным для любой местности и простым в обслуживании. Джип создан по запросу армии США в 1940 году как автомобиль общего назначения, имел полный привод для передвижения по пересеченной местности. Всего с 1940 по 1945 год было построено 647 925 джипов.

Известна крылатая фраза программистов «Don’t touch what works!». Вряд ли ее можно отнести к столь сложным объектам, как самолет F-35 и эсминец Zumwalt, но вполне допустимо, что и в таких колоссах умопомрачительной сложности придется кое-где отказаться от применения программируемых и/или киберуязвимых IP-решений в пользу более простых, но более надежных средств коммутации каналов или даже аппаратных изделий. К сожалению, это будут весьма болезненные решения.

Пока еще эйфория всесилия программируемых средств не прошла, все еще звучат заклинания в пользу облачных вычислений, искусственного интелекта. Несомненно, эти программируемые средства могут предоставить богатые возможности и новые услуги, но вместе с тем они множат киберуязвимости, устранение которых, по-видимому, выходит уже за пределы возможностей современного технологического развития. Что же делать? Придется остепениться, подобно тому, как современное индустриальное развитие осознает необходимость ограничения выбросов пыли в атмосферу или выбросов мусора в мировой океан.

## IX. Заключение

В статье рассмотрено противостояние двух телекоммуникационных технологий – коммутации пакетов и коммутации каналов, что длится уже более 50 лет и, кажется, в обозримом будущем не прекратится. Эта проблема обсуждается на примерах из двух социально значимых сфер: экстренной службы и оборонных информационных систем, а также из области микроэлектроники (network-on-a-chip).

Показана аналогия между сетью экстренных вызовов и сетью связи оборонного ведомства США – крупнейшей в мире ведомственной сети. Эта аналогия предполагает построение этих двух сетей по одним и тем же документам. Но, к сожалению, отсутствует организация, которая бы такие единые документы разработала, и эти сети создаются раздельно. Сам переход на Интернет-технологии в этих двух сферах встречает большие препятствия.

В сфере экстренных служб только через 18 лет (1999-2017) удалось найти компанию (в данном случае AT&T), которая начала строить пакетную сеть для FirstNet; но исход дела пока не ясен. В оборонном ведомстве США в 1996 г. была принята 15-летняя программа развития вооружений «Joint Vision 2010». В части средств связи основной выбор пал на сигнализацию SS7 и интеллектуальные сети (Advanced Intelligent Network) – высшие достижения техники коммутации каналов. Но в связи со взрывоподобным развитием Интернет-технологий Пентагон поддался модному течению, и в 2006 г. принял новый план «Joint Vision 2020». Этот план объявил переход от сигнализации SS7 к IP протоколу. Для перехода между двумя типами сетей изобрели новый коммутатор - многофункциональный софтсвич MFSS, который действует как медиашлюз между TDM каналами и IP-каналами, разработали протокол AS-SIP (Assured Services for Session Initiation Protocol), который обеспечивает секретность передачи разговора (сообщения) и приоритетность вызовов. Но протокол AS-SIP получился очень громоздким, так как пользуется услугами почти 200 стандартов RFC. Вполне понятно, что реализация плана «Joint Vision 2020» продвигается медленно.

Своеобразным «родимым пятном» на сети связи оборонного ведомства, строящейся по единому протоколу AS-SIP для доступа к сети, является сверхсекретная правительственная связь DRSN (Defense RED Switch Network), которая сохраняет технологию коммутацию каналов, точнее, ISDN-каналы. Сохраняется также «устаревшая» технология ATM в информационных сетях разведки и управления спутниками.

С развитием микроэлектроники появилась возможность на одном кристалле, помимо процессорного ядра, разместить большое количество сложных функциональных узлов. Появилось новое направление техники – сеть на кристалле (NoC, Network on a Chip). Схемы NoC изначально строили для пакетной коммутации, рассматривая коммутацию каналов как побочный вариант. В последнее же время появились работы, говорящие об обратном: изделия коммутации каналов более выгодны или, по райней мере, выгодно сочетать обе технологии.

Киберуязвимость оказалась главным пороком Интернет-технологий. Накапливается все больше примеров о невозможности этот порок устранить. Потерпела полную неудачу попытка создания объединенных региональных стеков безопасности JRSS (Joint regional security stacks). JRSS, по замыслу, должны обеспечивать киберзащиту в сетях электронной почты NIPRNet и SIPRNet. Планировалось 48 стеками JRSS заменить около 1000 нестандартных стеков сетевой безопасности, которые в настоящее время разбросаны по всему миру. Программа разработки стеков JRSS длилась более 10 лет и, к сожалению, завершилась полным провалом. В ноябре 2021 г. Министерство обороны объявило о закрытии программы кибербезопасности JRSS стоимостью 2 миллиарда долларов и о переходе на новую технологию киберзащиты – архитектуру нулевого доверия (Zero Trust Architecture). Будет ли она более успешной?

Исторически важным является заключение Счетной палаты правительства США (2018), что все системы вооружения с программным обеспечением, которые была протестированы в период с 2012 по 2017 год, включая созданные за последние десять лет, имеют киберуязвимости и могут быть взломаны. Особой критике подвергли боевой самолет-невидимку F-35, который управляется программным обеспечением, содержащим 8 млн. строк кода. Несмотря на более чем 20 лет работы и примерно 62,5 потраченных миллиарда долларов, пока не удалось создать надежный самолет. Конгресс США на 2022 финансовый год отказался санкционировать дополнительные новые заказы F-35. Сомнения вызывает и киберзащита ракетного эсминца USS Zumwalt. Zumwalt использует программное обеспечение беспрецедентно большого объема – от 14 до 16 миллионов строк компьютерного кода. Пока отсутствуют данные о тестировании киберуязвимостей эсминца Zumwalt (что может таить немало неожиданностей).

В результате анализа мы приходим к важному предположению, – что человечество достигло пределов возможного в плане создания сложных систем, основанных на IP-протоколах, в том числе и в плане кибернеуязвимости. Что пришло время осмыслить саму целесообразность лозунга «Everything over Internet Protocol» и искать решения совместной работы двух технологий — коммутации пакетов и коммутации каналов.

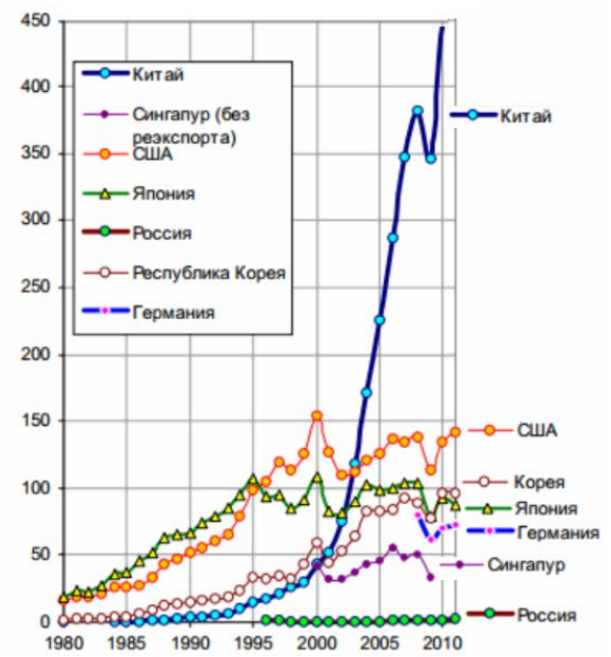


Рис. 50. Объемы экспорта офисного и телекоммуникационного оборудования в мире, млрд. долл. [70]

Напоследок хочу высказать пожелание: пора возродить производство средств связи. Без этого не может быть суверенной России. В настоящее время подавляющее большинство средств связи в России имеют иностранное происхождение. Например, сети «Ростелекома» до недавнего времени были ареной борьбы американских компаний Cisco и Juniper. В последнее время с ними конкурирует Huawei. Рисунок 50 раскрывает состояние мирового рынка телекоммуникационного оборудования; печально, что участие России тут близко к нулю. В последнее десятилетие лидирует Китай – и в большой мере за счет того, что США и другие страны производство перенесли в Китай. А ведь в советское время было мощное Министерство промышленности средств связи. Изложенный выше опыт США, в том числе просчеты с Интернет-технологиями, надеюсь, поможет выбрать успешную стратегию возрождения исследований и производства средств связи.


## Благодарности

Настоящая статья имеет обзорный характер, так как большая часть материалов были опубликована ранее – в течение длительного периода (2014-2021). Перечень работ приведен в Приложении 3. Они частично выполнены в соавторстве. Выражаю благодарность соавторам за возможность общения и за плодотворную совместную работу.


## Приложение 1

*Функция контроля сессии SCF*

В состав MFSS входит сложнейший узел – функция контроля сессии SCF (рис. 16 выше), его состав показывает рис. 17.

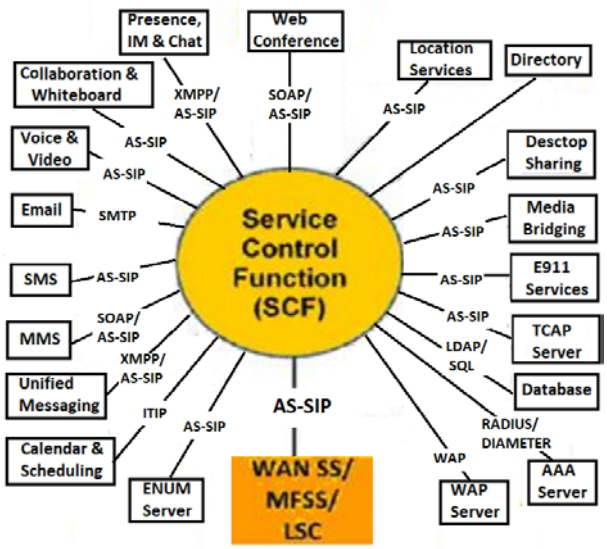


Fig. 17. Базовая модель функции контроля сессии SCF [19]

Для общения с контроллерами WAN SS, MFSS или LSC (Local Session Controller) узел SCF использует единый протокол AS-SIP, а для общения с серверами разных сервисов пользуется множеством других протоколов:

SOAP — Simple Object Access Protocol;
HTTP — HyperText Transport Protocol;
LDAP — Lightweight Directory Access Protocol;
SQL — Structured Query Language;
RADIUS — Remote Authentication Dial in User Service;
DIAMETER — расширенная версия RADIUS;
WAP — Wireless Access Protocol;
ITIP — iCalendar Transport Independent Interoperability Protocol;
SMTP — Simple Mail Transfer Protocol;
AAA — Authentication; Authorization; and Accounting;
TCAP — Transaction Capabilities Application Part;
ENUM — E.164 Number;
IM — Instant Messaging;
MMS — Multimedia Messaging Service;
SMS — Short Message Service.

В базовой модели функции контроля сессии SCF имеются 19 серверов. Это могут быть 19 программ в составе софтсвича MFSS как физического объекта, а могут быть и 19 удаленных объектов. Среди них имеются 16 серверов, которые представляют 16 сервисов реального времени (Real-Time Communications, RTC), и еще три выделенных сервера: TCAP сервер — обеспечивает выход на базы данных интеллектуальной сети AIN для маршрутизации TDM и беспроводных вызовов. Как отмечено в методических материалах по DISN [7], детальная проработка архитектуры TCAP сервисов оставлена на будущее; AAA сервер — обеспечивает услуги Authentication, Authorization и Accounting и пользуется протоколами RADIUS и DIAMETER; Database сервер — содержит данные, которые доступны по протоколам LDAP и SQL.

Приводим список 16 сервисов реального времени:

- Voice & Video;
- Web Conferencing;
- Conferencing, Collaboration & Whiteboard;
- Media Bridging;

• Presence, Instant Messaging (IM) & Chat;
• Unified Messaging;
• Calendaring & Scheduling;
• E.164 Number Mapping (ENUM);
• E.911 (Emergency Call);
• Transaction Capabilities Application Part (TCAP);
• Desktop Sharing; • Short Message Service (SMS);
• Multimedia Message Service (MMS);
• E-mail;
• Wireless Application Protocol (WAP);
• Location Services (Fixed/Mobile).

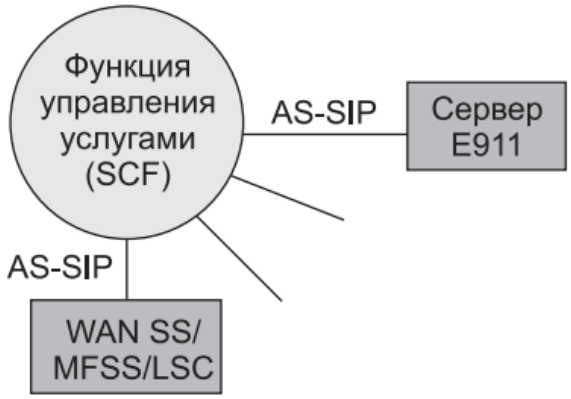


Рис. 18: Фрагмент узла Service Control Function с сервером E911

Обратим внимание на E911 сервер, обслуживающий экстренные вызовы (рис. 18). В нормативном документе по армейским сервисам [19] о сервере E.911 сказано следующее:

*«Армейский набор унифицированных сервисов UC по чрезвычайным ситуациям (E-911) предполагает гибридную архитектуру, которая использует возможности как IP-, так и TDM-сети, потому что архитектура вызова E-911 с помощью внедряемого нового протокола AS-SIP только начинается. Существующая ныне система доступа к узлам экстренных вызовов PSAP в настоящее время работает на сети TDM, является довольно стабильной и будет удовлетворять потребности в течение длительного времени. В настоящее же время объявлена интеграция архитектуры E-911 над обеими сетями IP и TDM, что названо архитектурой нового поколения NG-911. Несмотря на достигнутый значительный прогресс в этом направлении, стандарты по архитектуре NG-911 еще только отрабатываются, а создание инфраструктуры NG-911 потребует немало лет».*

Следовательно, в части обслуживания экстренных вызовов военное ведомство [20] полностью полагается на успехи гражданских институтов.

**Приложение 2**

*Сигнализация AS-SIP*

Главными недостатками протокола SIP являются трудности с обеспечением секретности (в условиях кибервойны) и с обслуживанием приоритетных вызовов, что важно как для военных применений, так и для экстренной службы. Поэтому по заказу МО США разработали защищенный протокол AS-SIP [21]. К сожалению, ввиду множества новых требований протокол AS-SIP (Assured Services for Session Initiation Protocol) получился очень громоздким. Если обыкновенный SIP использует 11 других стандартов RFC, то AS-SIP пользуется услугами почти 200 стандартов RFC. (RFC – технические спецификации Интернета.) Сам протокол AS-SIP еще далек от совершенства: в версии протокола AS-SIP, обнародованной в июле 2013 г., внесено более 50 исправлений по сравнению с исходной версией, обнародованной полугодом ранее [22]. Не ясно, есть ли на рынке хотя бы один телефон, реализующий протокол AS-SIP в полном объеме.

*Приоритеты.* Поясним правила установления приоритетных вызовов методом «Многоуровневые приоритеты и прерывание» (Multilevel Precedence and Preemption, MLPP). Этот метод обеспечивает выполнение трех требований:

(а) присваивает один из нескольких уровней приоритетности конкретным вызовам или сообщениям, обрабатывает их в заранее определенном порядке и в заданные сроки,

(б) обеспечивает контролируемый доступ к сетевым ресурсам, в которых вызовы и сообщения могут быть вытеснены только более высокими по приоритетности вызовами и сообщениями,

(в) обеспечивает распознавание приоритетности только в заранее определенном домене.

При поступлении вызова более высокого приоритета, чем любой из обслуживаемых вызовов, и занятости всех ресурсов, вызов более низкого приоритета прерывается. Прерванный вызов переводится в состояние ожидания, и соединение восстанавливается после обслуживания приоритетного вызова.

В основе протокола AS-SIP лежит стандарт RFC 4542 [23], в котором изложена архитектура метода MLPP. В соответствии с нуждами оборонного ведомства и экстренных служб предусмотрены шесть классов приоритетов (в порядке убывания):

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

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

3. Flash: этот уровень резервирован для телефонных звонков, относящихся к командованию и контролю военных сил, к важным действиям разведки, для ведения дипломатических переговоров, для оповещения граждан о событиях, важных для национального выживания, для выполнения федеральных государственных функций, важных для национального выживания и обеспечения

внутренней безопасности, для сообщений о катастрофических событиях национального или международного значения.

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

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

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

Для предоставления связи с учетом класса приоритета в протоколе AS-SIP сформулированы четкие правила прерывания и ожидания прерванных разговоров (рис. 19).

*Секретность.* Протокол сигнализации AS-SIP имеет развитую систему обеспечения секретности. Укажем три протокола: SRTP, TLS и SSL.

*Безопасный транспортный протокол реального времени SRTP* (Secure Real Time Transport Protocol) изложен в документе RFC 3711. SRTP определяет структуру, которая обеспечивает конфиденциальность, аутентификацию сообщений и защиту от воспроизведения, как для одноадресных, так и для многоадресных потоков RTP и RTCP. Безопасный RTP может обеспечить высокую пропускную способность и низкое расширение пакета даже в средах, которые представляют собой смесь проводных и беспроводных сетей.

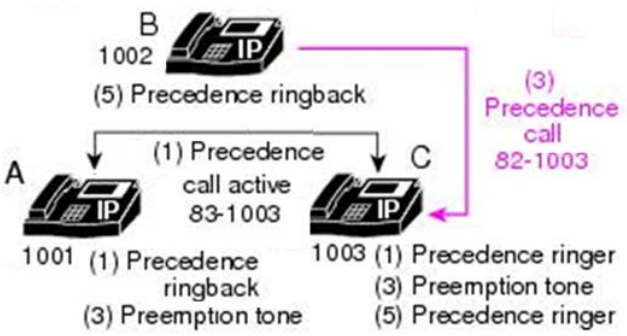


Рис. 19: Пример установки соединения высокого приоритета 82-1003 и прерывание менее приритетного 83-1003

В схеме OSI протокол SRTP располагается между прикладным уровнем RTP/RTCP и транспортным уровнем. Он генерирует безопасные пакеты Secure RTP из потока RTP/RTCP и передает на транспортный уровень. Точно так же он преобразовывает входящие пакеты Secure RTP в пакеты RTP/RTCP и передает их вверх по стеку. Информация о криптографическом состоянии, связанная с каждым безопасным потоком RTP, называется криптографическим контекстом. Он должен поддерживаться как отправителем, так и получателем этих потоков. Криптографический контекст включает в себя ключ сеанса (используемый непосредственно в шифровании/аутентификации сообщения) и мастер-ключ (случайная битовая строка, используемая для получения ключей сеанса, которой обмениваются безопасным образом), а также другие рабочие параметры сеанса.

Объясним два остальных протокола TLS и SSL. Безопасность транспортного уровня (Transport Layer Security, TLS) и уровень защищенных сокетов (Secure Socket Layer, SSL) — это криптографические методы шифрования данных на транспортном уровне от начала до конца. Эти протоколы безопасности используются для защиты протоколов приложений, таких как HTTP, FTP, SIP, SMTP, NNTP и XMPP.

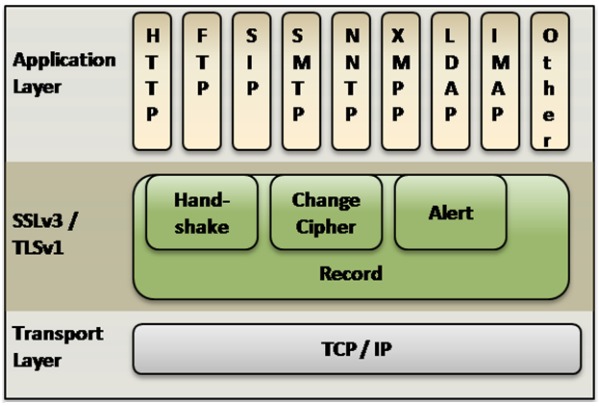


Рис. 20: Протоколы TLSv1 и SSLv3 шифруют данные на транспортном уровне

Протоколы TLSv1 и SSLv3 размещены между транспортным и прикладным уровнями (рис. 20). Они поддерживают несколько протоколов прикладного уровня, защищая данные приложений перед их отправкой на транспортный уровень.

Уровень TLSv1 и SSLv3 состоит из четырех подпротоколов:

• Протокол рукопожатия (Handshake Protocol) – отвечает за согласование сеанса.

• Протокол изменения спецификации шифра (Change Cipher Spec Protocol).

• Протокол оповещения (Alert Protocol) – сообщает суть оповещения, а также его серьезность.

• Протокол записи (Record Protocol) — этот протокол использует информацию о наборе шифров, шифрует данные приложений перед их передачей на транспортный уровень.

Из изложенного видно, что обеспечение секретности – очень сложная область программирования и

математических методов криптографии, и упомянутые три протокола составляют только часть системы обеспечение секретности.

**Приложение 3**

*Публикации по данному обзору*


1. M. Sneps-Sneppe, “On Telecommunications Thorn Path to the IP World: From Cybersecurity to Artificial Intelligence”, January 2021. DOI: 10.5772/intechopen.94575. In book: Cybersecurity Threats with New Perspectives ISBN:978-1-83968-852-2.
2. M. Sneps-Sneppe, D. Namiot, “On Paradigm Shift in Telecommunication Technologies: Review of Pentagon's Approach” // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 9, no.1, 2021.
3. M. Sneps-Sneppe, D. Namiot, R. Pauliks, “Information System Cyber Threats and Telecommunications Engineering Courses” // Latvian Journal of Physics and Technical Sciences, 2020, 57(1-2), pp. 52–61.
4. M. Sneps-Sneppe, D. Namiot, “The curse of software: Pentagon telecommunications case”. In ISSE 2019 - 5th IEEE International Symposium on Systems Engineering, Proceedings, 2019, 8984557.
5. M. Sneps-Sneppe, V. Sukhomlin, D. Namiot, “On Enterprise Information Systems and Cyber Threats: Some Pentagon's Shortcomings and Newer Initiatives.” In International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 2019, 2019-October, 8970991.
6. M. Sneps-Sneppe, D. Namiot, “On emergency and military telecom services: A thorns road to IP world.” In ConTEL 2019 - 15th International Conference on Telecommunications, Proceedings, 2019, 8848528.
7. M. Sneps-Sneppe, D. Namiot,.M. Alberts, “Channel Switching Protocols Hinder the Transition to IP World: The Pentagon Story.” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, 11660 LNCS, pp. 185–195.
8. M. Sneps-Sneppe, D. Namiot, “Time to Rethink the Power of Packet Switching.” In Conference of Open Innovation Association, FRUCT, 2018, 2018-November, pp. 369–374, 8588104.
9. M. Sneps-Sneppe, V. Sukhomlin, D. Namiot, “On Cyber-Security of Information Systems.” In Distributed Computer and Communication Networks. 21st International Conference, DCCN 2018, Moscow, Russia, September 17–21, 2018. Proceedings
10. M. Sneps-Sneppe, V. Sukhomlin, D. Namiot, “On cyber-security of information systems.” // Communications in Computer and Information Science, 2018, 919, pp. 201–211.
11. M. Sneps-Sneppe, “On telecommunications evolution: Pentagon case and some challenges.” In International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 2017, 2017-November, pp. 370–375.
12. M.A. Sneps-Sneppe, V.A. Sukhomlin, D. Namiot, “On information models of the digital economy.” In CEUR Workshop Proceedings, 2017, 2064, pp. 367–379.
13. И.А. Соколов, М.А. Шнепс-Шнеппе, В.П. Куприяновский, Д.Е. Намиот, С.П. Селезнев, “Телекоммуникации как решающее звено цифровой экономики. Опыт России” // International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 6 - 76-93.
14. M. Sneps-Sneppe, D. Namiot, “On telecommunication architectures: From Intelligent Network to Network Functions Virtualization.” In International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 2016, 2016-December, pp. 251–256, 7765366.
15. М.А. Шнепс-Шнеппе, “О эволюции сети DISN с учетом кибербезопасности”// International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 4.- 38-50.
16. M.A. Schneps-Schneppe, “Circuit switching is coming back?” // Automatic Control and Computer Sciences, 2015, 49(1), pp. 57–65.
17. М.А. Шнепс-Шнеппе, “Развитие телекоммуникаций и наследие Bell Labs: 30 лет блужданий”// International Journal of Open Information Technologies. – 2015. – Т. 3. – №. 11.
18. М. А. Шнепс-Шнеппе, “Телекоммуникации для экстренных и военных нужд: параллели” //International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 7. – С. 25-36.
19. М. А. Шнепс-Шнеппе, “От IN к IMS. О сетях связи военного назначения” // International Journal of Open Information Technologies. – 2014. – Т. 2. – №. 2. – С. 1-11.


БИБЛИОГРАФИЯ


[1] Total Telecom Equipment Market 2020. https://www.delloro.com/key-takeaways-total-telecom-equipment-market-2020/ Retrieved: May,2022.
[2] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative Concept of Operations, Version 2.0. April 6, 2007.
[3] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative System Description and High-Level Requirements Document, Version 1.1. July 31, 2007.
[4] U.S. Department of Defense, Global Information Grid Architectural Vision, Version 1.0. June 1997.
[5] Ch. Osborn. *Defense Information Systems Network (DISN) An Essential Weapon for the Nation’s Defense*. 16 May 2018/ file:///G:/Pentagon-book+/Osborn_%20DISN%20An%20Essential%20Weapon2018.pdf Retrieved: May,2022.
[6] FCC. Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13-5, FCC 14-5 (rel. Jan. 31, 2014).
[7] FCC. In the Matter of Technology Transitions GN Docket No. 13-5, March 19, 2014. http://apps.fcc.gov/ecfs/document/view?id=7521093879 Retrieved: May,2022.
[8] Ph. Tracy, “Understanding FirstNet, the post-9/11 public safety initiative,” August 31, 2016. http://www.rcrwireless.com/20160831/fundamentals/firstnet-tag31- tag99/ Retrieved: May,2022.
[9] 47 billion network https://www.theatlantic.com/magazine/archive/2016/09/the-47- billion-network-thats-already-obsolete/492764/ Retrieved: May,2022.
[10] L.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 http://www.crs.gov Retrieved: May,2022.
[11] AT&T wins FirstNet network contract, March 30, 2017. https://forums.radioreference.com/community-announcements-news/350888-t-wins-firstnet-network-contract.html/ Retrieved: May,2022.
[12] FirstNet Surpasses 2.8 Million Connections and Establishes Market Leadership with Law Enforcement. October 27, 2021. https://about.att.com/story/2021/momentous-public-safety-expansion.html/ Retrieved: May,2022.
[13] В. Жигадло, “Телекоммуникационные сети военного назначения США и стран НАТО. Особенности и тенденции развития”//Электроника НТБ. Выпуск #4/1999.
[14] B.T. Bennet, “Information Dissemination Management/ Advanced intelligent Network services for department of Defense”// MILCOM, 1999.
[15] W.W. Chao, “Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters”// MILCOM, 1999.
[16] Special Interoperability Test Certification of Avaya S8300D with Gateway 450 (G450). Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), 17 Apr 2012
[17] Department of Defense. Unified Capabilities Master Plan. October 2011
[18] Local Session Controller: Cisco’s Solution for the U.S. Department of Defense Network of the Future. White Paper. 2011. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/white_paper_c11_686977.pdf Retrieved: May,2022.
[19] U.S. Army Unified Capabilities Reference Architecture Version 1.0; October 2013
[20] Department of Defense Unified Capabilities Requirements 2013 (UCR 2013) January 2013.
[21] Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) January 2013
[22] Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1, July 2013.
[23] F. Baker, J. Polk (Cisco Systems), “Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite”, RFC 4542, May 2006.
[24] Department of Defense. Unified Capabilities Framework 2013. January 2013.
[25] W.E. Burr. *Security in ISDN*. NIST Special Publication 500-189. September 1991

[26] End of Support for Sectéra Wireline Terminal. May 17, 2019 https://www.redcom.com/sectera-wireline-terminal-eos/ Retrieved: May,2022.
[27] The Defense Network of Tomorrow—Today. AT&T White paper. 2018.
[28] AR 25–13. Information Management. Army Telecommunications and Unified Capabilities. Headquarters Department of the Army. Washington, DC. 11 May 2017
[29] AR 25–1–1. Army Information Technology Implementation Instructions. Headquarters Department of the Army. Washington, DC. 15 July 2019
[30] L. Bowman, R. Riehl, and S. Shah, "Defense Information System Network (DISN) asynchronous transfer mode (ATM) goal architecture and transition strategy," in IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201), 19-21 Oct, 1998, Boston, USA. DOI: 10.1109/MILCOM.1998.722548.
[31] "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," 30 May 1995. http://waffenexporte.de/NRANEU/others/jp_doctrine/jp6_0(95).pdf/ Retrieved: May,2022.
[32] "DARPA names Lockheed Martin to build intelligent network," March 24, 2005. http://www.militaryaerospace.com/articles/2005/03/darpanames-lockheed-martin-to-build-intelligent-network.html/ Retrieved: May,2022.
[33] S. Pasricha, and N. Dutt, *On-Chip Communication Architectures*, Elsevier, 2008.
[34] P.M. Fernandez, "Circuit switching in the internet," Dissertation, Stanford University, June 2003.
[35] Kuei-chung Chang, Jih-sheng Shen, and Tien-fu Chen, "Evaluation and design trade-offs between circuit-switched and packet-switched NoCs for application-specific SoCs," Proc. Design Autom. Conf., San Francisco, 2006, pp. 143--148.
[36] Shaoteng Liu et al, "Analysis and evaluation of circuit switched NoC and packet switched NoC" // Digital System Design (DSD), 2013 Euromicro Conference on, 4-6 Sept. 2013.
[37] G. Chen et al, "A 340mV-to-0.9V 20.2Tb/s source-synchronous hybrid packet/circuit-switched 16@x16 network-on-chip in 22 nm tri-gate CMOS," Proc. Solid-State Circuits Conf. Digest of Technical Papers (ISSCC), IEEE International, 2014, pp. 276--277.
[38] A.E. Kiasari et al, *Mathematical Formalisms for Performance Evaluation of Networks-on-Chip*. 2013. DOI: http://dx.doi.org/10.1145/2480741.2480755
[39] D. Metz, "Joint Information Environment Single Security Architecture (JIE SSA)," DISA, 12 May, 2014. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ Retrieved: May,2022.
[40] "Cyber Situational Awareness - Big Data Solution." https://docplayer.net/2357634-Cyber-situational-awareness-big-data-solution.html/ Retrieved: May,2022.
[41] 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,2022.
[42] "JRSS Deployments." https://c.ymcdn.com/sites/alamoace.site-ym.com/resource/resmgr/2017_ace/2017_speakers/2017_AACE_Keynote_Presentations/doc_keynote_Yee.pdf / Retrieved: May,2022.
[43] DoD Instruction 8010.01. "Department of Defense Information Network (DODIN) Transport," September 10, 2018. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ Retrieved: May,2022.
[44] Sneps-Sneppe, Manfred, Vladimir Sukhomlin, and Dmitry Namiot. "On Enterprise Information Systems and Cyber Threats: Some Pentagon's Shortcomings and Newer Initiatives." 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2019.
[45] "Cyberscoop." https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/ Retrieved: May,2022.
[46] GAO-16-593, "Joint Information Environment: DOD Needs to Strengthen Governance and Management," Jul 14, 2016.
[47] "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,2022.
[48] M. Gruss, "The debate about whether DISA's new security system is ready for primetime", Febr 7, 2018, Web Link https://www.c4isrnet.com/show-reporter/afceawest/2018/02/08/the-debate-about-whether-disas-new-securitysystem-is-ready-for-primetime/ Retrieved: May,2022.
[49] L.C. Williams, "DOD CIO: JRSS set for 2019 completion," Mar 05, 2018. https://fcw.com/articles/2018/03/05/jrss-completionmiller. aspx/ Retrieved: May,2022.
[50] L. C. Williams, "Is it time to rethink JRSS?" Feb 01, 2019. https://defensesystems.com/articles/2019/02/01/jrss-pause-report-williams.aspx/" Retrieved: May,2022.
[51] J. Marks, "The Pentagon Has a Big Plan to Solve Identity Verification in Two Years," in NEXTGOV, May 17, 2018. https://www.defenseone.com/technology/2018/05/pentagon-has-big-plan-solve-identity-verification-two-years/148280/ Retrieved: May,2022.
[52] M. Pomerleau, "The Pentagon is moving away from the Joint Regional Security Stacks," Nov 1, 2021. https://www.c4isrnet.com/it-networks/2021/11/01/the-pentagon-is-moving-away-from-the-joint-regional-security-stacks/ Retrieved: May,2022.
[53] Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ Retrieved: May,2022.
[54] S. W. Rose et al, *Zero Trust Architecture.* Special Publication (NIST SP) - 800-207. August 10, 2020. https://doi.org/10.6028/NIST.SP.800-207
[55] Colonial Pipeline ransomware attack. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack/ Retrieved: May,2022.
[56] G. Sawyer, and B. Emmett, "A Review of the Cybersecurity Programs in the United States Army," *Journal of Information and Technology*, 2021, *5*(1), 22 - 30. https://doi.org/https://doi.org/10.53819/81018102t2017
[57] GAO-19-128, "Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities," Report to the Committee on Armed Services, U.S. Senate, US Government Accountability Office, October 2018.
[58] D. Grazier. "What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks? An Obvious Solution Being Ignored," January 31, 2019. https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a generation-of-weapons-vulnerable-to-cyberattacks/ Retrieved: May,2022.
[59] M. Montgomery, and E. Borghard, "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence." https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-102/jfq-102_79-89_Features-Cyber_Threats.pdf/ Retrieved: May,2022.
[60] RAND Corporation, Hackers Wanted: An Examination of the Cybersecurity Labor Market, (2014).
[61] D. Grazier, "F-35: Still No Finish Line in Sight." March 19, 2018. https://www.pogo.org/investigation/2018/03/f-35-still-no-finish-line-in-sight/ Retrieved: May,2022.
[62] D. Grazier, "What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks? An Obvious Solution Being Ignored," January 31, 2019. https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a-generation-of-weapons-vulnerable-to-cyberattacks/ Retrieved: May,2022.
[63] F-35 program stagnated in 2021. https://www.pogo.org/analysis/2022/03/f-35-program-stagnated-in-2021-but-dod-testing-office-hiding-full-extent-of-problem/ Retrieved: May,2022.
[64] Zumwalt-class destroyer - Wikipedia Retrieved: May,2022.
[65] S. Gallagher, "The Navy's newest warship is powered by Linux." 10/18/2013. The Navy's newest warship is powered by Linux | Ars Technica Retrieved: May,2022.
[66] M. Thompson, "The U.S. Navy's Titanium "Tin Can""// Analysis. January 10, 2019.
[67] J. Katz, and A. Eversden, "Navy's problems with the Zumwalt may be hurting its hypersonic weapon efforts" // Breaking Defense. January 27, 2022
[68] NASA X-43. https://en.wikipedia.org/wiki/NASA_X-43/ Retrieved: May,2022.
[69] Boeing X-51 Waverider - Wikipedia Retrieved: May,2022.
[70] Анализ внешнеторговой деятельности России. http://kaivg.narod.ru/exp.pdf/ Retrieved: May, 2022.

# From Channels to Packets: Is the Mission Possible?

Manfred Schneps-Schneppe

***Abstract*— The confrontation between two telecommunications technologies – packet switching and circuit switching – has a long history and, it seems, will not stop in the foreseeable future. This problem is discussed using examples from two socially significant areas of the United States: emergency services and defense information systems, as well as from the field of microelectronics (network-on-a-chip). The history of unsuccessful attempts to switch to packet switching in the field of emergency services is outlined. Similar failures with the transition to packet switching in the field of defense information systems have already happened, namely: the ISDN technology was retained in government Defense Red Switch Network and hybrid ATM technology in intelligence information network JWICS and satellite control network AFSCN; the failure of the JRSS security stack program on the NIPRNet and SIPRNet email networks; The Joint Strike Fighter program was suspended due to cyber vulnerabilities in the software of the F-35 Lightning II aircraft.**

**As a result, we can assume that in terms of creating complex systems based on IP protocols and, moreover, cyber-invulnerable, humanity has reached the limits of what is possible. That the time has come to reflect on the feasibility of the very slogan "Everything over Internet Protocol" and look for solutions for the joint work of two technologies – packet switching and circuit switching.**

***Keywords*— circuit switching, cybersecurity, DRSN network, emergency services, F-35 aircraft, Internet protocol, packet switching, SS7 protocol**

REFERENCES

[1] Total Telecom Equipment Market 2020. https://www.delloro.com/key-takeaways-total-telecom-equipment-market-2020/ Retrieved: May,2022.

[2] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative Concept of Operations, Version 2.0. April 6, 2007.

[3] U.S. Department of Transportation, Next Generation 9-1-1 (NG9-1-1) System Initiative System Description and High-Level Requirements Document, Version 1.1. July 31, 2007.

[4] U.S. Department of Defense, Global Information Grid Architectural Vision, Version 1.0. June 1997.

[5] Ch. Osborn. *Defense Information Systems Network (DISN) An Essential Weapon for the Nation's Defense*. 16 May 2018/ file:///G:/Pentagon-book+/Osborn_%20DISN%20An%20Essential%20Weapon2018.pdf Retrieved: May,2022.

[6] FCC. Technology Transitions, Order, Report & Order and Further Notice of Proposed Rulemaking, Report Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, GN Docket No. 13-5, FCC 14-5 (rel. Jan. 31, 2014).

[7] FCC. In the Matter of Technology Transitions GN Docket No. 13-5, March 19, 2014. http://apps.fcc.gov/ecfs/document/view?id=7521093879 Retrieved: May,2022.

[8] Ph. Tracy, "Understanding FirstNet, the post-9/11 public safety initiative," August 31, 2016. http://www.rcrwireless.com/20160831/fundamentals/firstnet-tag31- tag99/ Retrieved: May,2022.

[9] 47 billion network https://www.theatlantic.com/magazine/archive/2016/09/the-47- billion-network-thats-already-obsolete/492764/ Retrieved: May,2022.

[10] L.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 http://www.crs.gov Retrieved: May,2022.

[11] AT&T wins FirstNet network contract, March 30, 2017. https://forums.radioreference.com/community-announcements-news/350888-t-wins-firstnet-network-contract.html/ Retrieved: May,2022.

[12] FirstNet Surpasses 2.8 Million Connections and Establishes Market Leadership with Law Enforcement. October 27, 2021. https://about.att.com/story/2021/momentous-public-safety-expansion.html/ Retrieved: May,2022.

[13] V. Zhigadlo, "Telekommunikacionnye seti voennogo naznachenija SShA i stran NATO. Osobennosti i tendencii razvitija"//Jelektronika NTB. Vypusk #4/1999.

[14] B.T. Bennet, "Information Dissemination Management/ Advanced intelligent Network services for department of Defense"// MILCOM, 1999.

[15] W.W. Chao, "Emerging Advanced Intelligent Network (AIN) For 21st Century Warfighters"// MILCOM, 1999.

[16] Special Interoperability Test Certification of Avaya S8300D with Gateway 450 (G450). Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), 17 Apr 2012

[17] Department of Defense. Unified Capabilities Master Plan. October 2011

[18] Local Session Controller: Cisco's Solution for the U.S. Department of Defense Network of the Future. White Paper. 2011. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/white_paper_c11_686977.pdf Retrieved: May,2022.

[19] U.S. Army Unified Capabilities Reference Architecture Version 1.0; October 2013

[20] Department of Defense Unified Capabilities Requirements 2013 (UCR 2013) January 2013.

[21] Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) January 2013

[22] Department of Defense. Assured Services (AS) Session Initiation Protocol (SIP) 2013 (AS-SIP 2013) Errata-1, July 2013.

[23] F. Baker, J. Polk (Cisco Systems), "Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite", RFC 4542, May 2006.

[24] Department of Defense. Unified Capabilities Framework 2013. January 2013.

[25] W.E. Burr. *Security in ISDN*. NIST Special Publication 500-189. September 1991

[26] End of Support for Sectéra Wireline Terminal. May 17, 2019 https://www.redcom.com/sectera-wireline-terminal-eos/ Retrieved: May,2022.

[27] The Defense Network of Tomorrow—Today. AT&T White paper. 2018.

[28] AR 25–13. Information Management. Army Telecommunications and Unified Capabilities. Headquarters Department of the Army. Washington, DC. 11 May 2017

[29] AR 25–1–1. Army Information Technology Implementation Instructions. Headquarters Department of the Army. Washington, DC. 15 July 2019

[30] L. Bowman, R. Riehl, and S. Shah, "Defense Information System Network (DISN) asynchronous transfer mode (ATM) goal architecture and transition strategy," in IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201), 19-21 Oct, 1998, Boston, USA. DOI: 10.1109/MILCOM.1998.722548.

[31] "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations," 30 May 1995. http://waffenexporte.de/NRANEU/others/jp_doctrine/jp6_0(95).pdf/ Retrieved: May,2022.

[32] "DARPA names Lockheed Martin to build intelligent network," March 24, 2005. http://www.militaryaerospace.com/articles/2005/03/darpanames-lockheed-martin-to-build-intelligent-network.html/ Retrieved: May,2022.

[33] S. Pasricha, and N. Dutt, *On-Chip Communication Architectures*, Elsevier, 2008.

[34] P.M. Fernandez, "Circuit switching in the internet," Dissertation, Stanford University, June 2003.

[35] Kuei-chung Chang, Jih-sheng Shen, and Tien-fu Chen, "Evaluation and design trade-offs between circuit-switched and packet-switched NoCs for application-specific SoCs," Proc. Design Autom. Conf., San Francisco, 2006, pp. 143--148.

[36] Shaoteng Liu et al, "Analysis and evaluation of circuit switched NoC and packet switched NoC" // Digital System Design (DSD), 2013 Euromicro Conference on, 4-6 Sept. 2013.

[37] G. Chen et al, "A 340mV-to-0.9V 20.2Tb/s source-synchronous hybrid packet/circuit-switched 16@x16 network-on-chip in 22 nm tri-gate

CMOS," Proc. Solid-State Circuits Conf. Digest of Technical Papers (ISSCC), IEEE International, 2014, pp. 276--277.
[38] A.E. Kiasari et al, *Mathematical Formalisms for Performance Evaluation of Networks-on-Chip*. 2013. DOI: http://dx.doi.org/10.1145/2480741.2480755
[39] D. Metz, "Joint Information Environment Single Security Architecture (JIE SSA)," DISA, 12 May, 2014. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ Retrieved: May,2022.
[40] "Cyber Situational Awareness - Big Data Solution." https://docplayer.net/2357634-Cyber-situational-awareness-big-data-solution.html/ Retrieved: May,2022.
[41] 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,2022.
[42] "JRSS Deployments." https://c.ymcdn.com/sites/alamoace.site-ym.com/resource/resmgr/2017_ace/2017_speakers/2017_AACE_Keynote_Presentations/doc_keynote_Yee.pdf / Retrieved: May,2022.
[43] DoD Instruction 8010.01. "Department of Defense Information Network (DODIN) Transport," September 10, 2018. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/801001p.pdf?ver=2018-09-10-082254-477/ Retrieved: May,2022.
[44] Sneps-Sneppe, Manfred, Vladimir Sukhomlin, and Dmitry Namiot. "On Enterprise Information Systems and Cyber Threats: Some Pentagon's Shortcomings and Newer Initiatives." 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). IEEE, 2019.
[45] "Cyberscoop." https://www.cyberscoop.com/audit-warns-of-poor-planning-onvast-pentagon-it-plan/ Retrieved: May,2022.
[46] GAO-16-593, "Joint Information Environment: DOD Needs to Strengthen Governance and Management," Jul 14, 2016.
[47] "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,2022.
[48] M. Gruss, "The debate about whether DISA's new security system is ready for primetime", Febr 7, 2018, Web Link https://www.c4isrnet.com/show-reporter/afceawest/2018/02/08/the-debate-about-whether-disas-new-securitysystem-is-ready-for-primetime/ Retrieved: May,2022.
[49] L.C. Williams, "DOD CIO: JRSS set for 2019 completion," Mar 05, 2018. https://fcw.com/articles/2018/03/05/jrss-completionmiller. aspx/ Retrieved: May,2022.
[50] L. C. Williams, "Is it time to rethink JRSS?" Feb 01, 2019. https://defensesystems.com/articles/2019/02/01/jrss-pause-report-williams.aspx/" Retrieved: May,2022.
[51] J. Marks, "The Pentagon Has a Big Plan to Solve Identity Verification in Two Years," in NEXTGOV, May 17, 2018. https://www.defenseone.com/technology/2018/05/pentagon-has-big-plan-solve-identity-verification-two-years/148280/ Retrieved: May,2022.
[52] M. Pomerleau, "The Pentagon is moving away from the Joint Regional Security Stacks," Nov 1, 2021. https://www.c4isrnet.com/it-networks/2021/11/01/the-pentagon-is-moving-away-from-the-joint-regional-security-stacks/ Retrieved: May,2022.
[53] Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ Retrieved: May,2022.
[54] S. W. Rose et al, *Zero Trust Architecture*. Special Publication (NIST SP) - 800-207. August 10, 2020. https://doi.org/10.6028/NIST.SP.800-207
[55] Colonial Pipeline ransomware attack. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack/ Retrieved: May,2022.
[56] G. Sawyer, and B. Emmett, "A Review of the Cybersecurity Programs in the United States Army," *Journal of Information and Technology*, 2021, *5*(1), 22 - 30. https://doi.org/https://doi.org/10.53819/81018102t2017
[57] GAO-19-128, "Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities," Report to the Committee on Armed Services, U.S. Senate, US Government Accountability Office, October 2018.
[58] D. Grazier. "What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks? An Obvious Solution Being Ignored," January 31, 2019. https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a generation-of-weapons-vulnerable-to-cyberattacks/ Retrieved: May,2022.
[59] M. Montgomery, and E. Borghard, "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence." https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-102/jfq-102_79-89_Features-Cyber_Threats.pdf/ Retrieved: May,2022.
[60] RAND Corporation, Hackers Wanted: An Examination of the Cybersecurity Labor Market, (2014).
[61] D. Grazier, "F-35: Still No Finish Line in Sight." March 19, 2018. https://www.pogo.org/investigation/2018/03/f-35-still-no-finish-line-in-sight/ Retrieved: May,2022.
[62] D. Grazier, "What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks? An Obvious Solution Being Ignored," January 31, 2019. https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a-generation-of-weapons-vulnerable-to-cyberattacks/ Retrieved: May,2022.
[63] F-35 program stagnated in 2021. https://www.pogo.org/analysis/2022/03/f-35-program-stagnated-in-2021-but-dod-testing-office-hiding-full-extent-of-problem/ Retrieved: May,2022.
[64] Zumwalt-class destroyer - Wikipedia Retrieved: May,2022.
[65] S. Gallagher, "The Navy's newest warship is powered by Linux." 10/18/2013. The Navy's newest warship is powered by Linux | Ars Technica Retrieved: May,2022.
[66] M. Thompson, "The U.S. Navy's Titanium "Tin Can""// Analysis. January 10, 2019.
[67] J. Katz, and A. Eversden, "Navy's problems with the Zumwalt may be hurting its hypersonic weapon efforts" // Breaking Defense. January 27, 2022
[68] NASA X-43. https://en.wikipedia.org/wiki/NASA_X-43/ Retrieved: May,2022.
[69] Boeing X-51 Waverider - Wikipedia Retrieved: May,2022.
[70] Analiz vneshnetorgovoj dejatel'nosti Rossii. http://kaivg.narod.ru/exp.pdf/ Retrieved: May, 2022.