УДК 623.618.5

© Горбатюк О.С., Зенуков Б.В.
Gorbatyuk O., Zenukov B.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЦИФРОВОЙ СВЯЗИ ДЛЯ ОБЪЕКТОВ, ЗАЩИЩАЕМЫХ КОМПЛЕКСАМИ СРЕДСТВ ЗАЩИТЫ В СЕТЕЦЕНТРИЧНОМ КОНТУРЕ ВОЗДУШНО-КОСМИЧЕСКОЙ ОБОРОНЫ

COMPARATIVE ANALYSIS OF DIGITAL COMMUNICATION OBJECTS PROTECTED BY THE COMPLEXES OF PROTECTION IN THE NETWORK-CENTRIC CIRCUIT AEROSPACE DEFENSE

Аннотация. *Приведен обзор и сравнительный анализ сетевых средств связи для объектов, защищенных комплексами средств защиты в сетецентричном контуре воздушно-космической обороны. Показано, что на сегодняшний день наиболее подходящей является ISDN-связь, как наиболее полно удовлетворяющая требования действующих руководящих документов. Однако перспективы развития связываются не с ней, а с IP-связью. Сделан вывод о том, что ближайшая тенденция развития сетевой связи будет определяться увеличением плотности каналов и повышением общей пропускной способности сети, ростом её защищённости и криптостойкости, улучшением качества сигнала при уменьшении затрат на аппаратуру. С этим сможет справиться только IP- сеть.*

Annotation. *An overview and comparative analysis of network communications for the objects that are protected by complexes of remedies in network-centric circuit of air and space defense. It is shown that by far the most suitable is the ISDN-connection, as most fully satisfies the requirements of the guidelines. However, prospects did not communicate with her, and with IP-connection. It is concluded that the immediate trend of networking will be determined by an increase in channel density and an increase in total network capacity, increase its security and the reliability, improved signal quality while reducing the cost of the equipment. With that can handle only IP-based network.*

Ключевые слова. *Сетецентричность, сеть, воздушно-космическая оборона, канал связи, контур управления, пакет данных, протокол передачи данных.*

Key words. *Network-centric, network, aerospace defense, communications channel, kennels control, a package of data, data transfer protocol.*

Актуальной проблемой современной России является проблема организации воздушно-космической обороны (ВКО) [1]. ВКО представляет собой комплекс общегосударственных и военных мероприятий, включая боевое применение войск, направленных по единому замыслу, плану и под единым руководством на борьбу со средствами воздушно-космического нападения противника для защиты населения, группировок Вооруженных сил, экономических и других объектов от ударов с воздуха и космоса. Исследования показали [2], что наиболее актуальной задачей для решения проблемы ВКО является разработка и внедрение в войска комплексов средств защиты (КСЗ) объектов. Они, как и традиционные средства ПВО и ПРО, должны быть встроены в управляющий контур ВКО.

Основным организационным принципом системы ВКО является сетецентричность [3]. Под этим принципом понимается такая сетевая организация системы, которая:

- реализует наиболее полный учет системных и внесистемных факторов для эффективного управления в реальном масштабе времени;
- обеспечивает прогноз с заданной достоверностью последствий управления;
- позволяет переводить систему из начального состояния в конечное состояние по принятому ситуационному или другому экстремально-эффективному показателю.

Горбатюк Олег Святославович – старший научный сотрудник, 4ЦНИИ Минобороны России;
Зенуков Богдан Вадимович – старший инженер, центр связи Минобороны России, тел. (495)910-37-66.

Gorbatyuk Oleg – senior fellow, 4CSRI Russian Defense Ministry;
Zenukov Bogdan – senior engineer, Russian Defense Ministry communications center, tel. (495) 910-37-66.

Понятие сетецентричности (в англоязычной литературе – NCW[1]) не ново. Оно появилось 5-10 лет назад в США в результате выработки ими системы взглядов на военно-техническое обеспечение и бесконтактное ведение боевых действий в условиях тотальной компьютеризации сил и средств вооруженной борьбы последнего десятилетия XX века. Операция США «Буря в пустыне» в Ираке 1991 г., боевые действия в Сомали 1992 г., в Боснии 1993 г., в Югославии 1999 г. ознаменовали появление новой природы войны – сетецентричной, основанной на компьютерных сетях.

По своему глубинному существу и содержанию это действительно революционный принцип ведения будущих войн любого уровня и масштаба. Он опирается на применение в управлении войсками в боевых операциях компьютеризованной, автоматизированной и централизованной сети систем наблюдения, разведки, связи, боевого управления, интегрированной в единую командно-управленческую систему С4 ISR[2] .

Эта многофункциональная система боевого управления оснащается разветвленной сетью боевых постов управления в штабах, командно-управленческих пунктах, в разведывательно-информационных структурах, в войсках, на боевых платформах оружия.

В ней для театра военных действий (ТВД) широко используется стратегическая и видовая разведка (агентура, космические аппараты, беспилотные аппараты и обычные средства воздушной, морской и наземной разведки уровня поля боя и целеуказания, и т.д.). Вся развединформация рассосредоточенно компьютерно обрабатывается и по сетям передаётся в Центр. Он из полученной информации формирует виртуальную реальность ТВД в виде единого киберпространства. В нём для каждой единицы активных сил и средств назначается зона ответственности. В её рамках в реальном масштабе времени, опять же через сеть, осуществляется централизованно-децентрализованное ситуационное боевое управление. В итоге получается упреждение действий по отношению к противнику и исключение его огневого сопротивления. Война становится практически бесконтактной.

Дальнейшая ближайшая перспектива - переход к сетецентричной боевой робототехнике, которая позволит сократить потери живой силы за счет формирования массовых боевых робототехнических группировок. Если сейчас к роботам относятся как к средству, которое нужно использовать там, где невозможно использовать людей, то в перспективе будет всё наоборот: использовать людей только там, где невозможно использовать роботов.

Полная реализация описанной выше концепции запланирована Пентагоном на ближайшее десятилетие (к 2020 году). В боле отдаленной перспективе – сетевые информационные войны. В них делается упор на достижение политических целей не силовыми средствами, а с помощью сетевого избирательного информационно – управленческого воздействия на социальные слои населения и отдельные личности, являющиеся ключевыми фигурами в стране или в блоке стран, относимых к категории стороны противника. Речь идет не о простых информационных войнах, осуществляемых через СМИ и Интернет в рамках принципа сетецентричности, а о специальном оружии, воздействующем на человеческий мозг, организм в целом и среду обитания. Здесь уже имеется в виду оружие на новых физических принципах (ОНФП)[3]: инфразвуковые пушки, психотронные генераторы, лучевое, кинетическое, генетическое, климатическое и другие виды оружия [4].

Что же мы противопоставляем этим угрозам?

Во-первых, мы начали реформирование ВПК и Вооруженных сил. Первым шагом на этом пути стала организация ВКО. Толчком к ней послужила угроза со стороны США по созданию ПРО в Европе и расширение НАТО на Восток вплотную к нашим границам.

Во-вторых, мы активизировали дипломатическую работу по формированию системы коллективной безопасности СНГ и предотвращению международного терроризма.

В-третьих, ведется работа в области фундаментальных и прикладных научных исследований в системе РАН и военной науки, направленных на несимметричное парирование обозначенных выше угроз.

Однако надо отметить, что работа эта продвигается с трудом. Человеческая инерция и незрелость сознания в несовершенной правовой системе молодой страны, коей является РФ, всё ещё препятствуют на пути полного осознания всей глубины нависшей над нами смертельной опасности от этих угроз. До сих пор наши военачальники готовятся к прошлым войнам, а ВПК навязывает

[1]NCW – Network Centric Warfare, – сетецентричная война.

[2]C4 ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

[3]ОНФП – это средства вооруженной борьбы, действие которых основывается на нетрадиционных способах полного или частичного поражения живой силы, боевой техники и объектов гражданской и военной инфраструктуры противника. Они основаны на использовании направленных высокоэнергетических искусственных или естественных излучений и полей нейтральных или заряженных частиц, воздействующих на живые организмы и растения на территории противника.

оружие вчерашнего дня. Сетецентричность всё ещё воспринимается многими как некая научно-фантастическая абстракция, а предпринимаемые военно-политическим руководством шаги – как надуманные, далекие от жизни усилия, направленные на решение коньюктурных интересов в подковёрной борьбе за власть и контроль финансовых потоков для личной наживы. Недостаточное внимание обозначенным угрозам уделяет и отечественная наука, особенно её прикладная часть. Всё это послужило причиной появления настоящей статьи.

Цель работы – сориентировать заинтересованного читателя на возможность уже сейчас создать сетецентричный контур управления ВКО.

Такой контур управления, на примере армии США, полностью основан на цифровых сетях. Такие сети есть и у нас. Они подразделяются на две технологии передачи информации: асинхронную, использующую протокол передачи данных TCP/IP[1], и синхронную, использующую протокол передачи данных PDH[2] или SDH[3]. В сетецентричном контуре циркулирует разнообразная информация. Для каждого его вида характерны свои особенности и в рамках статьи их описание не представляется возможным. Поэтому сосредоточимся на одном каком-то виде информации, например, на передаче речевых сообщений – телефонной связи.

Сама по себе цифровая связь характеризуется широким применением компьютерных средств, которые имеются у каждого обычного пользователя. Доступность использования связи в гражданском секторе определяется стоимостью и возможностями услуг, предоставляемых компаниями - провайдерами.

Наиболее доступным для обычного российского пользователя является VoIP-связь[4], а не ISDN[5], которая, главным образом, используется крупными компаниями в качестве корпоративной связи.

В первом виде цифровой связи используется пакетная синхронизация, а во втором – цикловая синхронизация.

Пакетная синхронизация (синхронизация пакетов) – определение начала и конца поступающих пакетов с целью построения правильной последовательности пакетов на приеме, что особенно важно при передаче по пакетной сети сигналов реального времени (телефонии, медиаресурсов и т.д.).

Цикловая синхронизация (синхронизация каналов) – определение в потоке битов с цикловой структурой начала и конца информации от различных источников для ее правильного распределения на приеме.

Цикловой и пакетный виды синхронизации занимают ключевые места в определении двух основных режимов (способов организации) передачи сигналов в транспортной сети - синхронного и асинхронного. Для них выполним сравнительный анализ на примере VoIP и ISDN связи.

Пакетная синхронизация

В войсковой части IP-телефония используется тогда, когда уже существует локальная сеть LAN[6] между распределенными структурными подразделениями, заведенных в персональный домен или хост, а также между пользователями этих доменов и хостами в рамках следующих групп: между персональными компьютерами (ПК) различных отделов и управлений; между автоматизированными рабочими местами (АРМ) операторов дежурных смен, суточных нарядов и вышеприведенными ПК; между конкретными АРМ, ПК и АРМ, ПК других войсковых частей, сторонних организаций и госучреждений для ежедневной оперативной работы с документами (рапортами, заявками, графиками, планами, ОКРами, НИОКРами, НИРами, техзаданиями, предписаниями, приказами, требованиями и т.д.) в единой системе документооборота (ЕСД). Примером ЕСД является уже готовый программный продукт (OTRS, или Docs Vision), прошедший проверку в ЦБС ФСБ России, для работы по закрытым каналам обмена информацией Ethernet-VPN (Virtual Private Network) с различными вышеприведенными группами по протоколу DNS[7].

---

[1]TCP/IP (Transmission Control Protocol/Internet Protocol)— протокол управления передачей/ Интернет-протокол. Это набор из четырех сетевых протоколов разных уровней модели сетевого взаимодействия, разработанной Министерством обороны США – US DoD (Department of Defense): 1) прикладного уровня (приложения); 2) транспортного; 3) межсетевого и 4) уровня сетевого доступа.

[2]PDH (Plesiochronous Digital Hierarchy) — цифровой метод передачи данных и голоса, основанный на временном разделении канала и технологии представления сигнала с помощью импульсно-кодовой модуляции.

[3]SDH (Synchronous Digital Hierarchy) — цифровой метод передачи данных, основанный на синхронизации по времени передающего и принимающего устройства.

[4]VoIP (Voice over IP) — система телефонной связи через Интернет по IP-протоколу.

[5]ISDN (Integrated Services Digital Network) — цифровая сеть с интеграцией услуг.

[6]LAN (Local Area Network)— компьютерная сеть локальной области или сеть с относительно небольшим числом пользователей.

[7]DNS (Domain Name System)— система доменных имён для формирования IP адресов, основанная на иерархической древовидной адресации, в которой доменом называется узел, вместе со всеми подчинёнными ему узлами. Структура доменного имени отражает порядок следования узлов в иерархии.

Плюсы пакетной синхронизации определяются:

• объединением гетерогенных локальных и глобальных сетей PTP[1], а также базовых служб поверх такого взаимодействия;

• удобной технической поддержкой типа клиент/сервер по криптографическим защищённым протоколам SSL, HTTPS, SSH[2];

• централизованной биллинговой системой контроля предоставляемых ip-услуг и своего оборудования, размещённого в Дата-центре: BSS, NGOSS-системы[3];

• эффективным администрированием своего оборудования, используя правильное выделение памяти и сетевых ресурсов по протоколу управляющих сообщений ICMP[4];

• надёжным отслеживанием маршрутизации локальной сети по протоколам RD, RIP, IGRP и EIGRP[5] ;

• терминальным доступом к любому хосту посредствам telnet, remote control, terminal access, WMWare, VirtualPC[6];

• возможностью копирования файлов с одного хоста на другой по протоколу FTP[7];

• обменом сообщениями и электронной почтой между любыми пользователями по протоколам POP3, IMAP, SMTP, интернет-Messenger'a (ICQ, Miranda, QIP....и т.д.)[8];

• печатью на удаленном принтере: Remote Printing;

• управлением средствами ip-телефонии по MAC-адресу;

• работой с сетевой файловой системой NFS и сетевыми новостями Network News;

• работой в Gopher и его средствами WAIS для индексации и поиска текстовых файлов;

• работой в распределённой сети WAN по запросам www, http, https, URL;

• работой с сетевым оборудованием по протоколу динамического конфигурирования хоста DHCP;

• работой с доменными именами и их алиасами (alias) по средствам службы Whois;

• объединением телефонных сетей и сетей передачи данных средствами сервиса gateway;

• простотой организации хостинг-услуг (hosting collocation) на виртуальной платформе;

• простотой создания корпоративной ip-телефонной сети со следующими функциями: 1) обеспечение мобильности внутренних пользователей, в том числе, в пределах зон Wi-Fi (находясь вне расположения своих кабинетов, их номера перемещаются вместе с ними); 2) организация связи между географически отдалёнными филиалами (H.323); 3) Объединение телефонной ёмкости филиалов в единый номерной план; 4) организация видео - и аудио-конференций (SIP-телефония); 5) построение центров обработки вызовов (call-центров) с использованием виртуальных телефонных аппаратов-кодеков: X-Lite, SJPhone; 6) интеллектуальная обработка входящих и исходящих вызовов; 7) автосекретарь и автоинформатор при постановке в очередь входящего вызова; 8) Прямой доступ к ресурсам системы связи без помощи оператора (DISA); 9) переадресация вызовов (находясь вне расположения кабинета, ваш номер переадресует входящий звонок на ваш другой телефонный аппарат, трубку или гарнитуру); 10) возможность использования голосовой почты: IVR и CRM системы; 11) записи разговоров; 12) AOH'a: Caller ID; 13) детализации и тарификации вызовов; 14) факс-сервера; 15) получить возможность совершить звонок прямо с веб-сайта организации: функция: Click2Dial;

• небольшой стоимостью затрат на предоставляемые ip-услуги пользователям нежели по другим цифровым протоколам (ISDN BRI, PRI) вследствие более низкой стоимости трафика. При этом один и тот же канал свя-

[1]PTP (peer-to-peer) – одноранговый.

[2]SSL (Secure Socket Layer) - протокол защищенных сокетов; HTTPS (Hypertext Transfer Protocol Secure) - протокол безопасной передачи гипертекстовых данных; SSH (Secure SHell — «безопасная оболочка») — сетевой протокол удалённого управления операционной системой и туннелирования TCP-соединений (например, для передачи файлов).

[3]BSS (Base Station Subsystem) – подсистема базовых станций, NGOSS (New Generation Operations Support System) — поддержка эффективных операций нового поколения.

[4]ICMP (Internet Control Message Protocol) — протокол семейства TCP/IP для межсетевых управляющих сообщений.

[5]RD (Router Discovery) – протокол обнаруженияе маршрутизаторов. RIP (Routing Information Protocol) - протокол маршрутной информации. IGRP (Interior Gateway Routing Protocol.) — протокол маршрутизации внутреннего шлюза. EIGRP (Enhanced Interior Gateway Routing Protocol) — расширенный протокол маршрутизации на основе протокола IGRP.

[6]TELNET (TErminaL NETwork) — сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола; remote control — программа для удаленного управления компьютером. terminal access – программное обеспечение терминала; VirtualPC — программная система виртуальных машин.

[7]FTP (File Transfer Protocol) — протокол передачи файлов.

[8]POP3 (Post Office Protocol) протокол электронной почты; IMAP (Internet Message Access Protocol) — протокол доступа к электронной почте (альтернатива POP3); SMTP (Simple Mail Transfer Protocol) — простой протокол для пересылки почты.

зи одновременно используется для передачи голоса, данных, факсимильных сообщений и медиаконтента, что очень удобно для оконечного пользователя.

Вышеперечисленные возможности обеспечивает сама архитектура сетевого уровня IP, что и сделало его основным сетевым протоколом для правительственных агентств, университетов и коммерческих организаций всего мира.

Следует отметить, что прародителем сети TCP\IP стало Министерство обороны США в конце 70-х годов, для: реализации основных мероприятий в вооружённых силах при переводе их с мирного на военное время; для объявления в стране чрезвычайного положения по сети объявления тревог ОСК ПАС (PAS – Primary Alerting System); для административного управления по сети АСУ стратегическими силами САККС (SACCS – Strategic Automated Command Control System). Данное военное ведомство в основу создания сети положило единообразие доступа к любому компьютеру PAS, SACCS или US DoD по протоколу терминального доступа (TELNET). С течением времени TELNET расширил свои возможности по работе с самыми разнообразными моделями терминалов и операционными системами. В настоящее время одним из активных пользователей сети WAN является Агентство национальной безопасности США (US NSA - National Security Agency-Central Security Service) — разведывательная организация Соединённых Штатов. Оно считается крупнейшим государственным агентством по сбору разведывательной информации в сетях Internet посредством криптоанализа.

Минусы пакетной синхронизации

Качество связи сильно зависит от следующих основных характеристик:

• уровня искажения голоса;

• частоты "пропадания" голосовых пакетов;

• времени задержки (между произнесением фразы первого абонента и моментом, когда она будет услышана вторым абонентом).

Цикловая синхронизация

В войсковой части ISDN-телефония используется тогда, когда уже существует обычная телефонная сеть между распределенными структурными подразделениями, а также между всеми пользователями этой организации.

Плюсы цикловой синхронизации

• наличие специального заголовка (циклового синхросигнала) обеспечивает высокую защиту от ложного синхронизма или потерю циклового сигнала под воздействием помех;

• обеспечение высоконадежного качества сетевой структуры;

• высокая отказоустойчивость технологии SDH (используют магистральные провайдеры ТТК, РТК, сотовые операторы)[1];

• обеспечение гарантированной передачи интегрированной информации различной природы по стандартным аналоговым телефонным линиям;

• широкий набор функций для телефонии, высокое качество звука;

• быстрый набор номера (менее 1 с);

• широкая доступность и распространенность в Европе.

Минусы цикловой синхронизации (по сравнению с IP-телефонией):

• низкая помехоустойчивость при высокой помехозащищенности волоконно-оптической среды передачи;

• постоянная длина заголовка, вследствие чего нерационально используются кадры PDH из-за его формата, что отражается на скорости передачи данных (от 64Кбит/с до 155,52 Мбит/с), в частности, при передаче данных по оптике (все телефонные операторы в нашей стране для стыков друг с другом используют N-е количество потоков E1);

• неудобные возможности кроссовых переключений;

• ограниченная скорость обработки сигналов;

• отсутствие развитых встроенных процедур контроля и администрирования сетью;

• недоступность данной технологии для частных пользователей по экономическим причинам (дорогой трафик и предоставляемые услуги связи, высокая стоимость сетевого оборудования, небольшой выбор программного обеспечения, отсутствие единой национальной, региональной и общегородской ISDN-сети, очень узкий круг корреспондентов);

• слабая гибкость транспортных сетей, а именно:

а) строго иерархическая система мультиплексирования, ограничивающая структуры сигналов стандартными размерами (STM-0,1, 4, 16) и со стандартными временными интервалами;

б) внутриканальная система сигнализации разрабатывалась для управления с центральной системой

[1]SDH (Synchronous digital hierarchy) — синхронизация цифровой иерархии. Это технология организации сетей, использующих различные среды для образования каналов связи; ТТК — федеральная Телекоммуникационная компания, РТК — ЗАО "Русская телефонная компания". Они входят в пятерку ведущих российских операторов связи.

управления, обеспечивающей как задачи поддержки работоспособности, так и контроля. Резервирование трактов гарантируется байтами сигнализации низкого уровня, вставленными в поток данных. Сигнализация обеспечивается набором байтов, сжатых в канал 576 Кбит/с, которого недостаточно для поддержки полосы передачи и требований задержки таких современных средств управления, как, например, GMPLS;

в) топология традиционных сетей ограничивается линейной и кольцевой конфигурациями с фиксированными схемами резервирования. Первичной задачей при разработке схемы резервирования была как минимум поддержка внутри элементной сигнализации при отсутствии стандарта на поддержку сигнализации как таковой. Так, первые кольца с низкой скоростью (STM-1/4), изначально были созданы с однонаправленным резервированием UPSR[1], при котором не требовалось никакой сигнализации, а резервирование осуществлялось исключительно на основе тракта. Это крайне неэффективное использование полосы передачи в кольце. По мере роста колец и числа элементов в них была добавлена двунаправленная схема резервирования BLSR[2]. Это требовало четкой сложной схемы сигнализации, сравнимой с UPSR/SNCR. Такая сигнализация была усовершенствована очень простым байт-ориентированным протоколом, использующим байты К1 и К2, размещенные в заголовке. Однако для поддержки требований по переключению для BLSR на каждом узле была необходима запасная коммутационная емкость.

Из вышеизложенного следует, что цикловая синхронизация в настоящий момент удовлетворяет предъявляемым требованиям руководящих документов [5-6] к качеству связи. В частности выполняется обеспечение:

• надежности, бесперебойности и информационной безопасности в сетях связи общего пользования (сети электросвязи РФ, сети связи иностранных государств), в сетях связи специального назначения (для нужд государственного управления, обороны страны, безопасности государства и правопорядка);

• первоочередного и оперативного предоставления абонентам президентской связи в независимости от формы собственности операторов связи, федерального органа исполнительной власти в области связи, органа связи иных федеральных органов исполнительной власти, услуг связи.

Кроме того, сети ISDN, которые сейчас лучше развиты в Европе, чем в США и РФ, для реалий российской действительности имеют некоторые преимущества над сетями TCP\IP:

• в сетях ISDN намного меньше как физических лиц (абонентов-пользователей), так и юридических, чем в сетях TCP\IP, ввиду дороговизны трафика и, как следствие, нераспространённость использования медиаконтента или услуг хостинга;

• всеми возможностями сети ISDN, как правило, пользуются очень крупные компании в своих корпоративных интересах. Поэтому здесь исключены Fishing, Flood и DDoS-атаки;

• сети ISDN менее подвержены технической разведке противника, добывающей информацию посредством криптоанализа, так как в ней не используется протокол терминального доступа TELNET, управляющих сообщений ICMP, маршрутизации локальной сети Router Discovery, динамического конфигурирования хоста DHCP, запроса www, http, https, URL и сервиса gateway.

Однако сети с коммутируемыми каналами имеют принципиальное ограничение, фактически сводящее на нет все их преимущества – ограниченную пропускную способность. В момент связи двух абонентов устанавливается временный выделенный канал, который существует в течение всего времени передачи данных. Абоненты обладают этим каналом монопольно – то есть не разделяют его ни с кем другим, пока не разорвут соединение. Это обстоятельство, как раз, и сдерживает пропускную способность сети. Для сетецентричного контура управления ВКО это неприемлемо.

VoIP-связь лишена этого недостатка. В сетях с коммутацией пакетов данные разделяются на пакеты и пересылаются по каналам, разделяемым множеством пользователей. Каждый пакет снабжается адресами источника и приемника. По мере перемещения пакета по сети коммутирующие устройства читают эти адреса и направляют пакет по нужному маршруту к адресу назначения. Весь этот процесс похож на процесс выделения канала, только канал получается виртуальный. Такие сети наилучшим образом соответствуют трафику локальных сетей, который является асинхронным и неравномерным во времени. А так как в сетецентричном контуре одновременно циркулирует плотный поток самой разнообразной информации от различных источников, прежде всего от сенсорного слоя, формирующего виртуальное киберпространство ТВД, то такие сети как раз и нужны. Конечно, не все проблемы решены для IP-связи, но они решаются. Будущее за этими сетями.

[1]UPSR (Unidirectional Path Switched Ring) - однонаправленный путь коммутируемого кольца.
[2]BLSR (Bi-directional Line Switched Ring) - двунаправленная линия коммутируемого кольца.

Выводы

1. Логика развития средств вооруженной борьбы выдвигает на первый план сетецентричный принцип управления войсками и информационно-управляющее оружие как средство, которое способно в условиях региональных войн обеспечить решающее превосходство над противником.

2. Адекватным ответом РФ усилиям США получить такое превосходство является организация ВКО страны. Она должна быть построена по тем же принципам сетецентричности, что и у американцев, тем более что все необходимые технологии для этого у нас имеются.

3. Выполненный в работе сравнительный анализ различных подходов к передаче данных показал, что основной технологией в контуре управления ВКО должна стать асинхронная технология передачи информации на основе протокола TCP/IP.

Литература

1. Указ Президента Российской Федерации от 5 февраля 2010 г. N 146 "О Военной доктрине Российской Федерации" // Российская газета. Федеральный выпуск № 5106 от 10 февраля 2010 г.

2. Горбатюк О.С., Зенуков Б.В. Способы и перспективы защиты объектов в воздушно-космической обороне / Проблемы эффективности и безопасности функционирования сложных технических и информационных систем: материалы XXX Всероссийской НТК филиала ВА им. Петра Великого (Серпуховской ВИ РВ), п8. Проблемы развития специального вооружения. – Серпухов, 2012. - с. 298-303.

3. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию. - М.: Евраз. Движение, 2011. - 130 с.

4. Самардак В.А. Вооруженная борьба и ее развитие в XXI в. часть 2 // Электронный Альманах: "Войны, история, факты". – 2009, №13.

5. "Положение о президентской связи" N 759 от 8 июля 2003 // Собрание законодательства Российской Федерации от 14 июля 2003 г. N 28 ст. 2899.

6. Федеральный закон N 126-ФЗ "О связи" от 25 июня 2003 // Российская газета. Федеральный выпуск № 3249 от 10 июля 2003 г.

Материал поступил в редакцию 18. 06. 2012 г.