

УДК 621.39

Перспективы и проблемные вопросы развития сетей связи специального назначения

Макаренко С. И.

Актуальность. Ведущие технологически развитые страны активно развивают сети связи специального назначения (СС СН), функционирующие в интересах органов государственной власти, органов обороны страны, безопасности государства и обеспечения правопорядка. Основными мировыми тенденциями развития этих сетей является использование в них ресурсов сетей связи общего пользования (СС ОП), а также коммерческих протоколов связи. Ввиду того, что в коммерческой отрасли связи наблюдается качественный переход к новым сетевым технологиям (концепция NGN, пакетные технологии передачи, использование технологий виртуализации и др.) актуальным является анализ современного состояния СС СН, основных тенденций и проблемных аспектов их развития. **Целью работы** является анализ технологий и принципов построения СС СН, а также перспектив и проблемных вопросов их развития. Для анализа были использованы только открытые источники, а в качестве примеров конкретных СС СН использовались открытые данные о сетях DISN и GIG, используемых в вооруженных силах США. **Результаты и их новизна.** Элементом новизны работы являются выявленные общие тенденции развития и проблемные вопросы СС СН. В частности, анализ показал следующее. Современным СС СН свойственен переход к децентрализованной сетевой структуре, которая в большей степени соответствует современным требованиям к системам государственного и военного управления. Также для современных СС СН характерен переход к гибриднему построению, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН. Кроме того, наблюдается устойчивая тенденция отказа от использования в СС СН закрытых и специализированных протоколов связи и максимальное широкое использование в СС СН коммерческих протоколов и технологий из гражданской сферы связи и телекоммуникаций. Эти тенденции делают современные СС СН уязвимыми к атакам средств радиоэлектронного подавления и информационно-техническим воздействиям. Эти атаки могут проводиться на СС СН через сетевые сегменты общие с СС ОП, которые, как правило, подключены к глобальной информационно-телекоммуникационной сети Интернет. При этом среди коммерческих сетевых протоколов, которые получили широкое распространение в СС СН, не в полной мере отработаны механизмы защиты от таких атак, а также механизмы быстрого восстановления работоспособности. **Практическая значимость.** Представленный анализ будет полезен техническим специалистам для обоснования новых технологических решений в области СС СН. Кроме того, данный анализ будет полезен научным работникам и соискателям, ведущим научные исследования, для прикладного обоснования целесообразности предлагаемых ими улучшений СС СН, а также обоснования защиты СС СН от воздействий со стороны противника.

Ключевые слова: система связи, сеть связи, сеть связи специального назначения, система связи специального назначения, сеть связи общего пользования, сетевые протоколы, система военной связи, устойчивость системы связи, радиоэлектронная борьба, информационно-техническое воздействие, NGN, система управления связью.

Библиографическая ссылка на статью:

Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-68. URL: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf>

Reference for citation:

Makarenko S. I. Prospects and Problems of Development of Communication Networks of Special Purpose. Systems of Control, Communication and Security, 2017, no. 2, pp. 18-68. Available at: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf>

Введение

В настоящее время стремительно развиваются телекоммуникационные технологии. Такое стремительное технологическое развитие, а также внедрение концепции сетей следующего поколения NGN (Next Generation Networks) и концепции глобальной информационной инфраструктуры GI (Global Information Infrastructure), создает предпосылки для коренного изменения архитектуры и принципов построения сетей специального назначения. Так, концепция NGN связана с конвергенцией сетей связи и расширением диапазона предоставляемых связных услуг, а концепция GI – с образованием единого информационного пространства, в котором услуги связи дополнены другими услугами обработки информации, такими как: накопление, хранение, обработка и поиск необходимой информации. При этом отличительной особенностью сетей специального назначения является то, что с одной стороны они традиционно являются наиболее консервативным объектом в отрасли связи, а с другой стороны – они должны быть основаны на новейших достижениях этой отрасли, чтобы обеспечивать высокое качество обслуживания специальных абонентов.

Вопросам анализа функционирования сетей связи специального назначения посвящены работы: П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко, А.М. Чуднова [1], И.Н. Лялюка [2], А.В. Боговика, В.В. Игнатова [3], П.А. Будко [4, 5], Г.И. Линца [6, 7], А.Н. Назарова, К.И. Сычева [8], А.Е. Давыдова [9, 10, 11, 31], Г.В. Сызранцева, К.И. Лукина, Г.В. Иншина [12-15], К.Е. Легкова [16-21], А.Н. Буренина [20, 21], Е.Е. Исакова [22], Р.Л. Михайлова [23, 24], М.А. Шнепс-Шнеппе [25-28], а также других ученых. При этом критический анализ проблемных вопросов, связанных с переходом СС СН на новые пакетные технологии представлен в работах М.А. Шнепс-Шнеппе [25-28], Н.А. Соколова [29], В.А. Нетеса [30].

Вместе с тем в данных работах не в полной мере раскрыты эволюционные процессы развития современных СС СН, а также проблемные аспекты, характерные для этого развития. Решению этой задачи посвящена данная работа.

Цель работы – анализ технологий и принципов построения телекоммуникационных систем и сетей связи специального назначения, а также перспектив и проблемных вопросов их развития.

Ввиду объемности материала работы он был декомпозирован на следующие подразделы.

1. Основные используемые термины и определения.
2. Сеть связи специального назначения – определение, состав, классификация, требования.
3. Анализ вариантов построения современных сетей связи специального назначения (на примере сетей связи вооруженных сил США).
 - 3.1. Сеть DISN.
 - 3.2. Сеть GIG.
4. Анализ основных тенденций развития современных сетей связи специального назначения.

- 4.1. Многоэшелонированный принцип построения современных сетей связи специального назначения.
- 4.2. Широкое использование в составе сети связи специального назначения арендуемых сетевых ресурсов коммерческих операторов связи.
- 4.3. Массовое использование в современных сетях связи специального назначения технологий коммутации пакетов и коммерческих протоколов связи.
- 4.4. Перспективы построения сетей связи специального назначения в соответствии с концепцией NGN.
- 4.5. Перспективы перехода от сетей связи специального назначения к инфокоммуникационным сетям специального назначения.
5. Проблемные вопросы обеспечения эксплуатации и модернизации сетей связи специального назначения.
 - 5.1. Проблемные вопросы обеспечения устойчивости сетей связи специального назначения в условиях перехода от технологий коммутации каналов к технологиям коммутации пакетов.
 - 5.2. Проблемные вопросы обеспечения устойчивости сетей связи специального назначения в условиях внедрения концепции NGN.
 - 5.3. Проблемные вопросы управления сетью связи специального назначения в условиях внедрения концепции NGN.

1. Основные используемые термины и определения

Для конкретизации понятий, рассматриваемых в статье, введем базовые определения.

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [32].

Электросвязь – любое излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам [32].

Сеть электросвязи – сеть связи, обеспечивающая электросвязь при помощи электромагнитных систем. Сеть электросвязи состоит из сетей следующих категорий: сети связи общего пользования; выделенные сети связи; технологические сети связи, присоединенные к сети связи общего пользования; сети связи специального назначения и другие сети связи для передачи информации. Таким образом, сеть электросвязи фактически представляет собой объединение отдельных категорий сетей, которые классифицируются по их назначению [32].

Сеть связи специального назначения (СС СН) – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [32].

При этом для обеспечения функционирования СС СН могут использоваться как ее собственные ресурсы, так и ресурсы сетей связи общего пользования.

Сеть связи общего пользования (СС ОП) – комплекс взаимодействующих сетей связи, обеспечивающих электросвязь, в том числе – трансляцию телеканалов или радиоканалов, предназначенных для возмездного оказания услуг связи любому пользователю. При этом СС ОП могут иметь присоединение к СС ОП иностранных государств [32].

СС СН и СС ОП включают в себя первичные и вторичные сети.

Первичная (транспортная) сеть связи – совокупность технических средств, комплексов, линий связи и обслуживающего персонала, обеспечивающая потребителей стандартными каналами (трактами) передачи первичных электрических сигналов. Основным видом сервиса, предоставляемого абонентам первичных сетей связи, являются типовые каналы и тракты [3].

Вторичная сеть связи (сеть абонентского доступа) – совокупность технических средств и связей между ними, обеспечивающая потребителей различными видами услуг по доставке, хранению и обработке информации. Основным видом сервиса, предоставляемого абонентам вторичных сетей, являются услуги по информационному обмену [3].

Выделенные сети – сети связи, которые организуются в интересах отдельных категорий должностных лиц, пунктов управления (ПУ) и специальных систем управления. К таким выделенным сетям, например, можно отнести сети навигации, государственного опознавания, системы телеметрии в системах непосредственного управления, сети правительственной связи и др.

Кроме того, в современных нормативных актах используется термин «информационно-телекоммуникационная сеть». Причем в подавляющем числе нормативных актов этот термин ассоциируется с сетью Интернет, а содержание этих актов в основном ориентировано на использование информационных ресурсов сети Интернет и, в основном, не касается ее технологических особенностей как сети электросвязи.

Информационно-телекоммуникационной сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [48].

Кроме того, часто используемым является понятие «телекоммуникационная система», которое в большинстве случаев ассоциируется с отдельной первичной (транспортной) сетью, которая соответствует отдельной области маршрутизации в составе СС СН или СС ОП.

Телекоммуникационная система (ТКС) – это совокупность связанных линиями связи сетевых узлов, которая основана на единой транспортной технологии и эксплуатируется в соответствии с едиными принципами маршрутизации, адресации и управления, при этом в ее составе имеются граничные узлы, ответственные за допуск трафика в сеть или направление его в другие смежные телекоммуникационные системы.

2. Сеть связи специального назначения – определение, состав, классификация, требования

СС СН выполняет задачи, в первую очередь, по доставке информации между распределенными в пространстве органами и пунктами системы управления вышестоящего уровня – органов государственной власти, органов обороны страны, безопасности государства и обеспечения правопорядка.

Таким образом, в самом общем виде СС СН может быть определена как совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена в системах государственного и военного управления, а также системах управления обеспечения безопасности и правопорядка [3].

По транспортным средствам, используемым для доставки информации, в составе СС СН различают [3]:

- *сети фельдъегерско-почтовой связи*, в которых доставка информации (в виде карт, схем, посылок, бандеролей, писем и т. д.) осуществляется специальными курьерами (фельдъегерями) с помощью обычных транспортных средств;
- *сети электросвязи*, в которых доставка информации осуществляется с помощью электрических сигналов и электромагнитных волн.

Каналы и тракты транспортных сетей связи в современных СС СН создаются на базе линий и сетей различных родов связи, входящих в состав первичной (транспортной) сети [33, 34].

По видам обеспечиваемого для абонентов сервиса и услуг связи сети электросвязи обычно подразделяют на [3]:

- первичные (транспортные) сети связи;
- вторичные сети связи (сети абонентского доступа).

Классификация элементов сетей первичной и вторичной сетей СС СН представлена на рис. 1.

В составе первичных и вторичных сетей СС СН могут быть организованы *выделенные сети*.

Основой построения первичных (транспортных) сетей в составе СС СН в настоящее время являются [3, 33, 34]:

- линии и сети радиосвязи;
- линии и сети спутниковой связи;
- волоконно-оптические линии связи;
- линии радиорелейной и тропосферной связи;
- кабельные линии электрической связи.

К основным технологиям первичных (транспортных) сетей в составе СС СН можно отнести [33, 35, 36]:

- технологии коммутации каналов – PDH, SDH, OTH;
- технологии коммутации пакетов – IPv4, IPv6;
- технологии коммутации пакетов по виртуальным каналам – X.25, AX.25, Frame Relay, ATM, IP/MPLS, VPN и др.;

- технологии организации, управления и интеграции сетей связи – TMN, ASON/ASTN, NGN, GII и др.;
- специализированные технологии, разработанные для обеспечения связи в условиях преднамеренного воздействия дестабилизирующих факторов на СС СН.

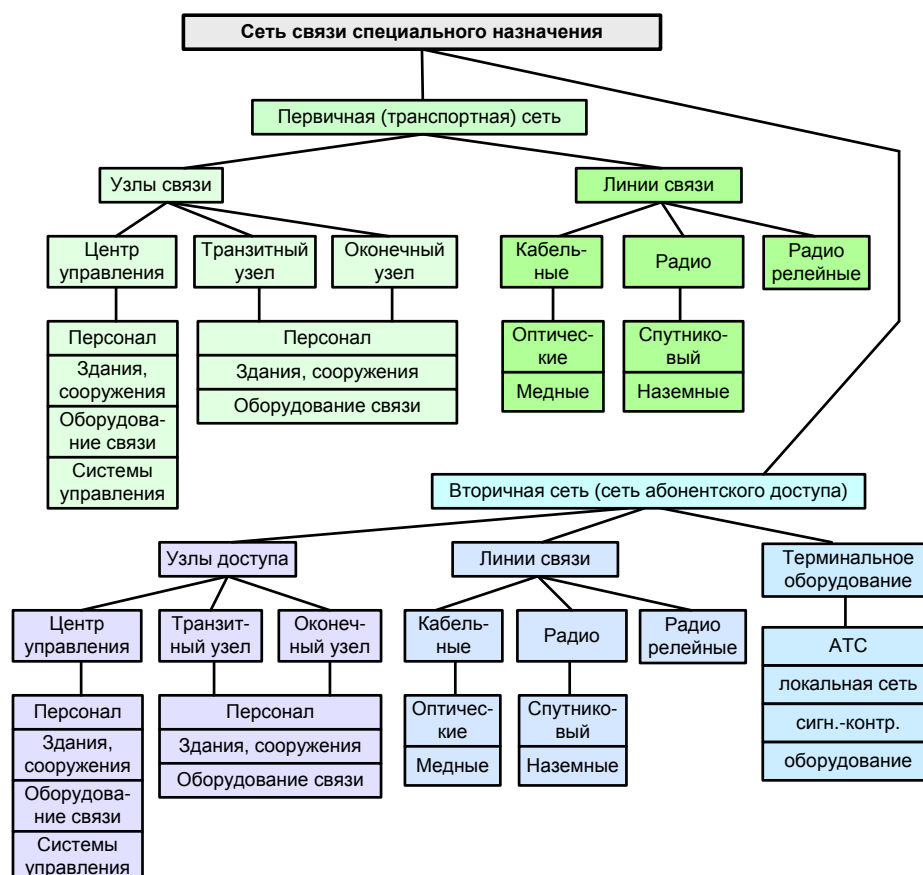


Рис. 1. Классификация элементов СС СН [41]

Вторичные сети СС СН обычно подразделяли по видам предоставляемых ими услуг, однако в настоящее время такая классификация устарела. В соответствии с современными взглядами вторичные сети можно подразделить по типу [33]:

- локальные сети;
- сети коллективного доступа;
- цифровые линии абонентского доступа;
- оптические линии абонентского доступа;
- сети мобильной или транкинговой связи;
- сети радиодоступа.

СС СН функционирует в интересах систем государственного и военного управления, а также систем управления обеспечения безопасности и правопорядка. К данным системам управления предъявляются требования по:

- *устойчивости* – способности органов управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях помех и массированных дестабилизирующих воздействиях противника;

- *непрерывности* – возможности органов управления постоянно взаимодействовать с объектами управления;
- *оперативности* – способности получать, обрабатывать и преобразовывать информацию в соответствии с темпом изменения текущей ситуации;
- *скрытности* – способности сохранять в тайне факт, время и место преобразования информации, ее содержание и принадлежность к управляющим объектам.

Для обеспечения этих требований к управлению, к связи, как к процессу переноса информации от объектов управления к пунктам управления и обратно, предъявляются требования по:

- *своевременности* – свойству связи, которое характеризует ее способность обеспечивать передачу или сообщений или ведение переговоров в заданные сроки;
- *достоверности* – свойству связи, которое характеризует ее способность обеспечивать требуемую точность воспроизведения сообщений в пунктах доставки, а также сохранять эту точность при преобразовании информации;
- *безопасности* – свойству связи, которое характеризует ее способность обеспечить сохранение в тайне содержания передаваемых сообщений и самого факта их передачи.

Соответственно связь, как процесс переноса информации, должна удовлетворять всем этим требованиям. В связи с этим вводится такая интегральная категория как «качество связи».

Качество связи – это свойство связи, характеризующее ее способность обеспечивать своевременную, достоверную и безопасную передачу сообщений.

В СС СН циркулируют информационные потоки системы управления, которые после их обработки и систематизации представляются уполномоченным лицам или органам для принятия решений. В связи с этим в СС СН при передаче этих потоков должны обеспечиваться требования по информационной безопасности.

Информационная безопасность – это состояние, при котором обеспечивается конфиденциальность, целостность и доступность информации [37].

Конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право [39].

Целостность информации – состояние информации, при котором обеспечивается ее достоверность и полнота [37].

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно [39]

Основной особенностью СС СН, которая отличает ее от СС ОП, является то, что СС СН ориентирована на функционирование, как в мирное, так и в военное время, в условиях воздействия противника, а также различного рода дестабилизирующих факторов. В связи с этим для СС СН особенное значение приобретает свойство ее устойчивости.

В ГОСТ Р 53111-2008 даны следующие определения.

Устойчивость сети электросвязи – способность сети электросвязи выполнять свои функции при выходе из строя части ее элементов в результате воздействия дестабилизирующих факторов [40].

Дестабилизирующий фактор – воздействие на сеть электросвязи, источником которых является физический или технологический процесс внутреннего или внешнего характера, приводящее к выходу из строя элементов сети [40].

Таким образом, понятие «фактор», в соответствии с ГОСТ Р 53111-2008, семантически соответствует понятию «воздействие». Уточняя, что основной функцией СС СН является обеспечение требуемого качества связи и, разделяя дестабилизирующие факторы на естественные и искусственные, можно дать следующее определение.

Устойчивость сети связи – способность сети связи обеспечивать требуемое качество связи в условиях воздействия дестабилизирующих факторов естественного и искусственного характера.

Классификация дестабилизирующих воздействий на СС СН представлена на рис. 2. При этом естественные и искусственные непреднамеренные дестабилизирующие воздействия характерны для мирного времени. В военное время и в угрожаемый период эти воздействия дополняются преднамеренными искусственными дестабилизирующими воздействиями.

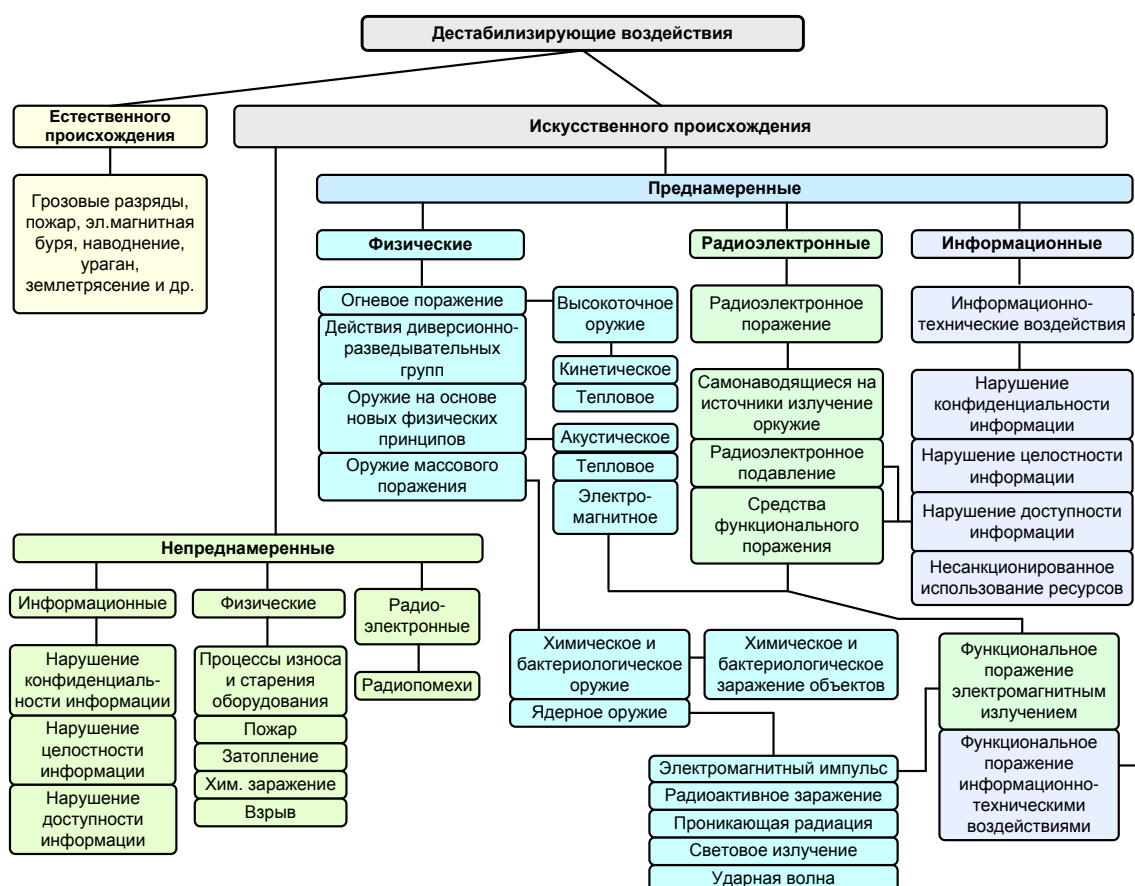


Рис. 2. Классификация дестабилизирующих факторов [41]

3. Анализ вариантов построения современных сетей связи специального назначения (на примере сетей связи Вооруженных сил США)

Рассмотрим структуру и принципы построения современных СС СН на примере систем связи, используемых в интересах силовых ведомств США.

Тенденции развития СС СН США предусматривают разработку концептуальных принципов и плана достижения глобального взаимодействия между органами военного управления и участниками боевых действий, что позволит им выполнять любую задачу в любое время в любом месте, быстро устанавливать надежную и безопасную засекреченную связь и при этом иметь систему, приемлемую по стоимости. Основной задачей построения СС СН является формирование единой информационной среды, которая позволяла бы эффективно поддерживать связь и управление в операциях, проводимых несколькими видами Вооруженных сил (ВС), либо с участием союзных войск с тем, чтобы участники боевых действий имели средства, позволяющие выполнять боевые задачи в любой точке земного шара [54].

Реализацию инициативы создания и развития глобальной единой телекоммуникационной среды, которая должна обеспечить информационные потребности военного командования США в XXI веке рассмотрим на примере сетей DISN и GIG.

При этом необходимо отметить, что одним из основных и важных элементов сетей DISN и GIG является их космический сегмент, образованный сетями спутниковой связи (ССС) DSCS/WGS, MilStar/AEHF, UFO/MUOS. Эти СССР обеспечивают глобальность покрытия сетей DISN и GIG, а также привязку удаленных и мобильных абонентов стратегического, оперативного и тактического звеньев управления к этим сетям. Подробная информация о составе СССР вооруженных сил США, их задачах и технических характеристиках представлена в работе [38].

3.1 Сеть DISN

Сеть DISN (Defense Information Systems Network) – оборонная интегрированная система передачи данных министерства обороны США. Главная цель сети DISN – обеспечение высокой степени интеграции услуг, предоставляемых отдельным пользователям, в локальных и глобальных сетях. Предполагается, что пользователи будут регулярно обмениваться информацией в виде речи, данных и изображений, используя одни и те же терминалы в течение отдельного сеанса. Сеть предоставляет услуги по передаче всех видов информации (речи, данных, видео, мультимедиа) и интегрирует все системы связи министерства обороны США (рис. 3).

В настоящее время основу DISN составляют оптические транспортные сети на основе технологии SONET, использующие коммутацию каналов по стандарту TDM. В сети коммутации каналов сегодня работают следующие основные военные сети связи Министерства обороны США (рис. 3) [25]:

- 1) телефонная сеть DSN (Defense Switched Network);
- 2) закрытая коммутируемая сеть DRSN (Defense Red Switched Network);
- 3) сеть видеоконференцсвязи DVS (DISN VIDEO).

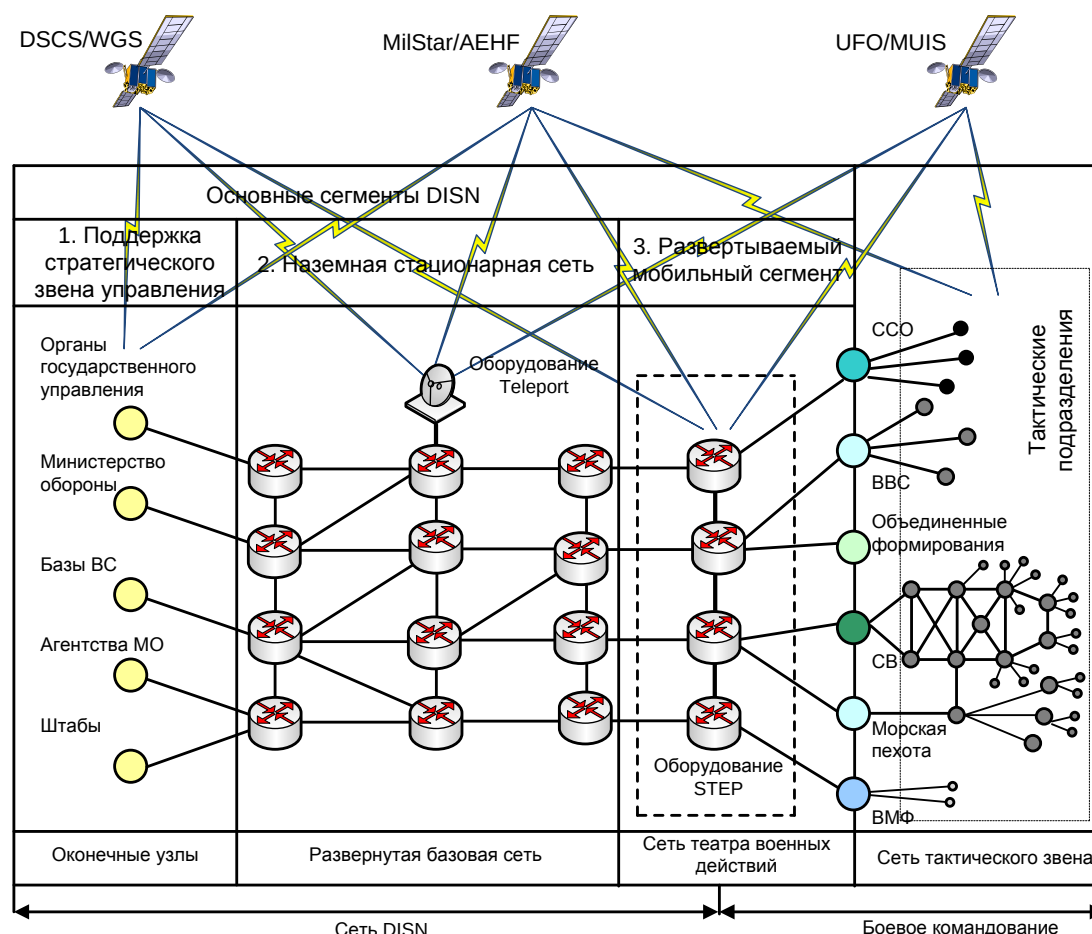


Рис. 3. Сеть DISN [25]

Кроме того, ресурсы DISN используют четыре закрытые сети, которые используют выделенные магистральные каналы [25]:

- объединенная глобальная сеть разведывательных коммуникаций JWICS (Joint Worldwide Intelligence Communications System) – для передачи секретной информации по протоколам TCP/IP;
- сеть управления спутниками AFSCN (Air Force Satellite Control Network);
- NIPRNet (Non-classified Internet Protocol Router Network) – сеть, используемая для обмена незакрытой, но важной служебной информацией между «внутренними» пользователями;
- SIPRNet (Secret Internet Protocol Router Network) – система взаимосвязанных компьютерных сетей, используемых Министерством обороны США для передачи закрытой информации по протоколам TCP/IP;

При этом сети JWICS и AFSCN построены на базе коммутаторов ATM (техника ATM в настоящее время не производится) [25].

В 2006 г. в Министерстве обороны США решили перейти от коммутации каналов к коммутации пакетов. Был принят план Joint Vision 2020, в котором были утверждены перспективы развития DISN в период до 2020 г. В этом плане была объявлена смена принципа построения сети DISN – ее переход к IP протоколу. Предполагалось, что IP протокол станет единственной технологией обме-

на между транспортным уровнем и приложениями (рис. 4), а протоколом сигнализации станет протокол SIP.

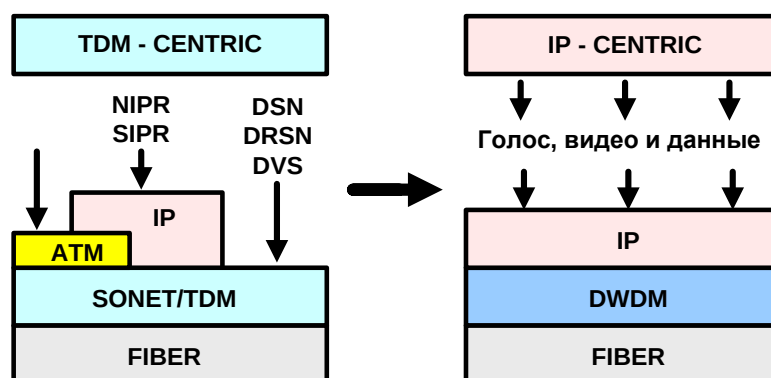


Рис. 4. Эволюция сети DISN [25]

Ввиду того, что у стандартного протокола SIP имеются определенные сложности с обеспечением безопасности связи и обслуживанием приоритетных вызовов, что важно для специальных абонентов, по заказу министерства обороны США был разработан защищенный протокол AS-SIP. Протокол AS-SIP получился очень громоздким. Если стандартный протокол SIP использует 11 стандартов RFC, то AS-SIP требует учета почти 200 стандартов RFC. Кроме того, протокол AS-SIP еще далек от совершенства – в версию AS-SIP, обнародованную в июле 2013 г., внесено более 50 исправлений по сравнению с исходной версией, подготовленной полугодом ранее. Переход от сети SONET с коммутацией каналов, к коммутации IP-пакетов и протоколу SIP (или к AS-SIP) требует использования новых программных коммутаторов Soft Switch, которые будут функционировать в соответствии с концепцией NGN. При этом, в качестве поставщиков этих коммутаторов выступают Avaya, Jupiter и другие производители [25, 26].

Фактически, сеть DISN является базовой телекоммуникационной инфраструктурой, к которой подключаются другие сети (спутниковые, сети тактического звена и др.), а также на основе, которой строятся другие информационно-управляющие сети (такие как GIG) или наложенные сети обмена информацией (такие как NIPRNet, JWICS).

Более полная информация о построении и технологических особенностях функционирования сети DISN приведена в работах [25-27].

3.2 Сеть GIG

Сеть GIG (Global Information Grid) – глобальная информационно-управленческая сеть силовых ведомств США. GIG строится, в том числе, и на основе связных ресурсов DISN и предназначена для информационного обеспечения всех элементов системы национальной безопасности страны, включая вооруженные силы. Она объединяет взаимосвязанные распределенные вычислительные системы коллективного пользования, локальные вычислительные сети, системы связи, базы данных, системы компьютерной и сетевой безопасности, средства обучения пользователей, а также другие элементы, предназна-

ченные для централизованного удовлетворения всех информационно-технических потребностей системы управления войсками и органов государственного управления [56].

GIG поддерживает обработку для обеспечения оперативных задач, действий и функций разведывательных органов Министерства обороны США, АНБ и других разведывательных ведомств. Она предоставляет возможность обмена информацией всем оперативным пунктам дислокации – авиабазам, гарнизонам, военно-морским базам и т. д. Сеть GIG обеспечивает интерфейсы для коалиционных, союзных и не принадлежащих Министерству обороны США пользователей и систем. Информационные технологии в виде автоматизированных и информационных систем, не входящих в GIG, являются автономными, самодостаточными либо информационными системами, которые не предназначены или не могут быть подсоединены к этой информационно-управляющей сети [57].

Сеть обмена данными GIG представляет собой объединенную цифровую сеть на основе протокола IPv6, построенная по принципу «все по IP» и использующая как собственные каналы связи, так и каналы связи региональных и национальных операторов связи. В качестве базового протокола для обмена данными в GIG используется IP/MPLS, а сама сеть строится в соответствии с концепцией NGN с широким использованием программных коммутаторов SoftSwitch производства Avaya, Jupiter и других производителей [26]. При этом ядром GIG является глобальная высокоскоростная опорная сеть GIG-BE (Global Information Grid-Bandwidth Expansion). GIG-BE – это мировая оптическая сеть SONET с каналами 10 Гбит/с, обслуживающая порядка 100 операционных вычислительных центров по всему Земному шару [58, 59].

Первая версия GIG-системы (GIG v. 1), представленная в январе 2000 г., была построена как структура, которая объединяла существовавшие в то время системы с иерархическим принципом построения (platform-centric). В этой связи, формально GIG определялась как множество глобально объединенных по принципу «точка-точка» информационных, а также автоматизированных и коммуникационных систем, связанных с ними процессов сбора, отправки, распределения и управления информацией по требованию участников военных операций, политического руководства и обеспечивающих структур. Она была ориентирована на обслуживание штабов объединенных оперативных формирований и, в основном, ограничивалась стратегическим и оперативным уровнями управления [57].

Разработка архитектуры GIG второй версии (GIG v. 2) была обнародована в ноябре 2002 г. Новая архитектура была ориентирована на создание сетцентрической среды в соответствии с концепцией сетцентрических войн Network-Centric Warfare (NCW). Архитектура GIG v. 2 состоит из 5 блоков для стратегического, оперативного, тактического и комбинированного применения американскими и союзническими ВС в операциях и конфликтах различного масштаба и назначения. Включение тактического уровня в состав GIG v. 2 отражает стремление реализовать то положение, что информационное превосходство становится важным слагаемым на всех уровнях управления и, особенно, по от-

ношению к боевым возможностям перспективных систем тактического звена. Основой этого информационного превосходства становятся Grid-системы, то есть распределенные инфраструктуры для супер-компьютерных приложений.

Вычислительную основу GIG составляют 18 центров корпоративных вычислений министерства обороны США, 5 региональных информационных центров и 10 центров региональной обработки данных сухопутных войск. Создание Grid-системы распределенных вычислений в составе GIG стал возможен за счет использования в качестве ядра GIG высокоскоростной оптической системы связи GIG-BE. Использование Grid-технологий позволило создать управляющую и прикладную инфраструктуру для предоставления широкого класса информационных сервисов в интересах военных пользователей [57].

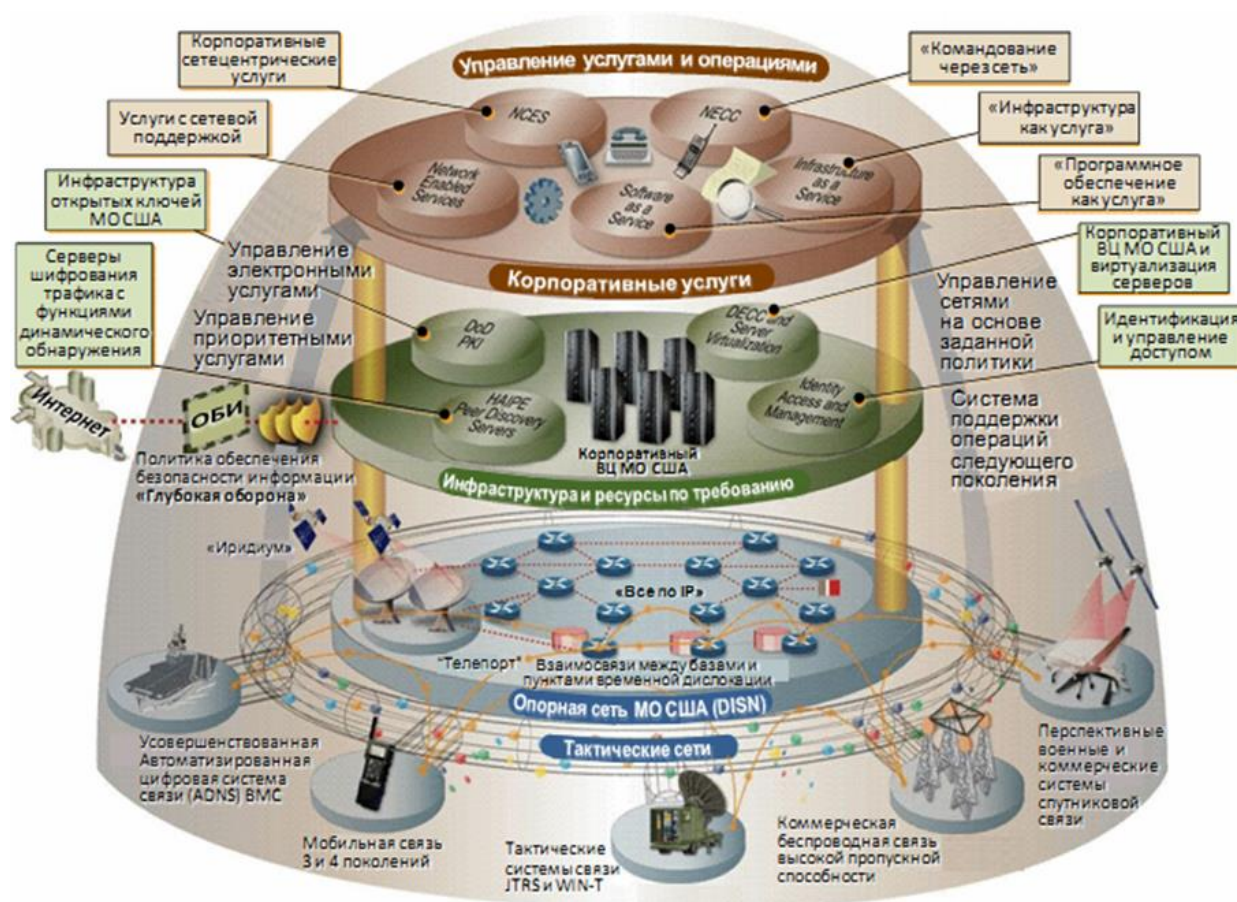


Рис. 5. Общая структура информационного пространства на основе GIG [54]

Глобальная информационная Grid-система в составе GIG – это инфраструктура координированной распределенной обработки информации и хранения гетерогенных информационных ресурсов с гибкой политикой управления, непрерывного доступа к ресурсам и вычислительным мощностям с обеспечением безопасности, распараллеливания обмена данными, эффективного и экономного использования процессорной нагрузки. Она образует так называемую «инфраструктуру базовых возможностей» для своевременного, безопасного и

повсеместного доступа пользователей к информации для выработки, принятия решений и оптимизации их исполнения (рис. 5) [57].

Наличие Grid-инфраструктуры позволило реализовать программу перехода от объединенной глобальной системы оперативного управления GCCS-J (Global Command and Control-Joint) к объединенной системе командования и оперативного управления JC2 (Joint Command and Control System). Переход к последней выполняется посредством переложения программного обеспечения GCCS-J на корпоративные сервисы сетевой связности NCES (Net Centric Enterprise Services), что является одной из основных составляющих корпоративных сервисов GES (GIG Enterprise Services) для GIG в интересах командования и оперативного управления стратегического уровня [57].

С целью расширения диапазона досягаемости и повышения сетевой связности GIG для нее были разработаны дополнительные программы, связанные с включением в сеть спутниковых систем связи через систему телепортов, включения в сеть тактических радиосетей. Кроме того, для повышения качества принятия решений пользователи GIG получили возможность объединяться в виртуальные группы коллегиального сотрудничества [57].

В 2011 г. министерство обороны США приступило к переходу GIG на новую версию – GIG v. 3. Необходимость модернизации обусловлена тем, что основным глобальным связывающим звеном между серверами GIG вне ТВД и участниками боевых действий является спутниковая группировка. Однако, как показали результаты войны в Ираке и Ливии, она зачастую не справляется с передачей больших объемов данных в условиях боевых действий. Развитие сети GIG при переходе к версии GIG v. 3 будет вестись в соответствии с 6-ю ключевыми программами [28].

Программа 1 – формирование высокоскоростного наземного компонента GIG на основе волоконно-оптических линий связи с технологией DWDM, получившая название DISN-Core [28].

Программа 2 – формирование космического сегмента GIG. Эта программа включает строительство перспективной объединенной системы спутниковой связи, базовыми компонентами которой станут несколько орбитальных группировок CCC. К числу таких перспективных группировок CCC относятся WGS, AENF, MUOS [38].

Программа 3 – создание системы «телепортов». Под «телепортом» американские специалисты понимают телекоммуникационный пункт сбора и распределения информации, который объединяет наземный и космический сегменты GIG и обеспечивает боевые подразделения широкополосным, мультимедийным и глобальным доступом к DISN [28].

Программа 4 – разработка тактического радиосегмента GIG. Программа предполагает разработку широкополосных радиостанций нового поколения, структура и функциональные возможности которых реализуются на основе концепции «программируемого радио» SDR (Software Defined Radio) и удовлетворяет новым, повышенным требованиям АНБ США к системам шифрования сигналов [28].

Программа 5 – разработка унифицированного комплекса сетевых сервисов корпоративного информационного обслуживания NCES (Net-Centric Enterprise Service). Комплекс предназначен для обеспечения любого пользователя, имеющего доступ к GIG, стандартным набором информационных услуг по своевременному и безопасному доступу к необходимой информации высокого качества [28].

Программа 6 – обеспечение информационной безопасности в GIG. Ее ключевым элементом является программа модернизации криптографических средств защиты CMP (Crypto Modernization Program), которая предполагает создание новых методов и способов засекречивания, а также защиты информационных ресурсов [28].

Более полная информация о построении и технологических особенностях функционирования сети GIG приведена в работах [25-28, 57, 58].

4. Анализ основных тенденций развития современных сетей связи специального назначения

Анализ представленных выше принципов построения сетей DISN и GIG, анализ работ в области построения CC СН, обеспечивающих информационный обмен в ВС США и НАТО, а также работ в области развития отечественных CC СН [2, 8-11, 25-28, 35, 51-54, 56-60] позволил выявить следующие общие тенденции развития CC СН:

- переход от сопряжения отдельных CC СН в различных органах государственного и военного управления к единой CC СН, основанной на многоэшелонированном принципе построения (космический, воздушный, наземный и морской эшелоны);
- широкая интеграция в состав CC СН сегментов CC ОП и коммерческих телекоммуникационных ресурсов;
- активное замещение в CC СН технологий коммутации каналов на технологии коммутации пакетов;
- массовое использование коммерческих протоколов и технологий в составе CC СН, прежде всего, протоколов IP (Internet Protocol) и MPLS (Internet Protocol and Multiprotocol label switching);
- конвергенция отдельных сетей и систем связи в единое информационное пространство на основе концепции NGN;
- широкое использование спутниковых систем связи (ССС) в качестве основы, обеспечивающей глобальную связность CC СН и глобальную управляемость во всех звеньях управления, особенно в военное время, при этом в состав СН СН могут включаться СССР из состава CC ОП, в том числе СССР гражданских операторов спутниковой связи;
- использование в сетях CC СН тактического звена технологий адаптивных мобильных радиосетей Mesh/MANET-сетей (Mobile Ad hoc Network);

- использование методов обработки Big Data, а также облачных и Grid-технологий для организации распределенного хранения и обработки больших массивов данных.

Рассмотрим основные из этих тенденций более подробно.

4.1. Многоэшелонированный принцип построения современных сетей связи специального назначения

Современные СС СН, как правило, декомпозируются на четыре эшелона (рис. 6):

- наземный эшелон (стационарный и мобильный (полевой) сегменты);
- воздушный эшелон (воздушный и наземный сегменты);
- морской эшелон (морской и наземный сегменты);
- космический (космический и наземный сегменты).

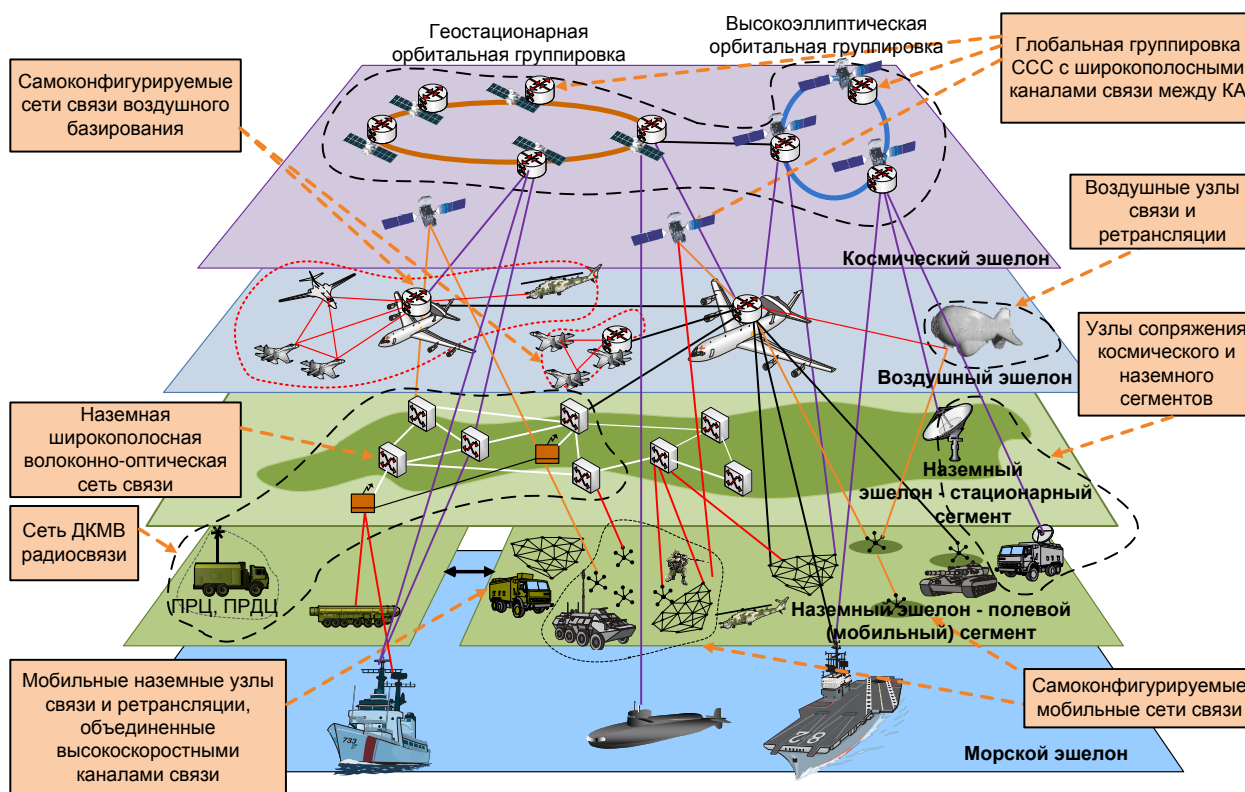


Рис. 6. Общая схема многоэшелонированного построения СС СН [60]

Наземный эшелон СС СН использует сетеориентированные, унифицированные технические и программно-аппаратные решения со стандартной номенклатурой типовых каналов связи. Наземный эшелон является взаимоувязанной совокупностью стационарных и подвижных узлов и линий связи различных родов. Он представляет организационно-техническое объединение средств и комплексов связи, выполняющих задачи по образованию, маршрутизации и коммутации каналов связи в интересах вышестоящей системы государственного и военного управления. Узлы и линии связи наземного эшелона также обеспечивают взаимодействие между техническими средствами других эшелонов.

Наземный эшелон включает в себя:

- стационарный сегмент;
- полевой (мобильный) сегмент;
- автоматизированную систему управления связью.

Стационарный сегмент наземного эшелона представляет собой цифровую стационарную транспортную сеть в составе СС СН. Стационарный сегмент наземного эшелона базируется на основе территориально-распределенных транспортных сетей из состава СС СН, а также на основе арендованных линий связи СС ОП. В качестве основной физической среды передачи стационарного компонента наземного эшелона выступают волоконно-оптические линии связи (ВОЛС).

Полевой сегмент наземного эшелона СС СН представляет собой совокупность самостоятельных, но организационно и технически взаимоувязанных ТКС, объединяющихся по звеньям управления в:

- полевую (мобильную) сеть связи стратегического звена управления;
- полевые (мобильные) сети связи оперативного звена управления;
- полевые (мобильные) сети связи тактического звена управления.

Полевой сегмент СС СН базируется на общих принципах построения самоорганизующихся мультисервисных сетей с максимально возможным использованием унифицированных цифровых средств и комплексов связи. Предполагается, что структура полевого (мобильного) сегмента наземного эшелона СС СН является инвариантной по отношению к структуре системы государственного и военного управления. В состав узлов связи полевого (мобильного) сегмента входит типовый набор радиорелейных, тропосферных, проводных и спутниковых средств связи, комплексы автоматизации связи, аппаратные электропитания и т.д.

Воздушный эшелон СС СН строится на основе средств воздушно-наземной связи и ретрансляторов связи на летно-подъемных средствах различного назначения. Воздушный эшелон СС СН включает в себя:

- наземный сегмент;
- воздушный сегмент;
- автоматизированную систему управления связью с элементами наземного и воздушного базирования.

К воздушному сегменту относится транспортная сеть, включающая в себя бортовые комплексы связи, которыми оснащаются ретрансляторы транспортной сети воздушного эшелона, а также воздушные ПУ летательными аппаратами различных видов авиации, а также средства связи для сопряжения отдельных сетей других эшелонов, базирующихся на летно-подъемных средствах (самолеты, вертолеты, дирижабли, аэростаты, беспилотные дистанционно-управляемые летательные аппараты, летающие платформы).

К наземному сегменту воздушного эшелона относятся комплексы связи, размещаемые на наземных узлах связи, стационарных и подвижных, средства сопряжения с транспортной сетью наземного эшелона.

Технической основой воздушного эшелона являются комплексы радиосвязи ДКМВ, МВ, ДМВ диапазонов и СМВ/ММВ диапазонов спутниковой связи.

Морской эшелон СС СН представляет организационно-техническое объединение стационарно-мобильных узлов связи, радиоцентров, радиостанций, автоматизированных комплексов связи подводных лодок, кораблей, летательных аппаратов, соединенных линиями различных родов связи. Для организации радиосвязи используются различные диапазоны радиоволн – СНЧ, СДВ, ДВ, СВ, КВ, УКВ, а также каналы спутниковой связи. Морской эшелон включает в себя:

- морской сегмент;
- наземный сегмент;
- автоматизированную систему управления связью.

Морской сегмент, как правило, состоит из средств связи и автоматизации, размещаемых на подводных лодках и кораблях, а при организации сетей для ретрансляции сигналов используются радио-ретрансляторы на летно-подъемных средствах и ССС.

Космический эшелон СС СН разворачивается на основе ССС, образованных линиями спутниковой связи и узлами сети – земными станциями и космическими аппаратами связи. Космический эшелон СС СН включает в себя:

- космический сегмент;
- наземный сегмент.

Космический эшелон СС СН предназначен для обеспечения глобальной связности СС СН в стратегическом и оперативно-тактическом звеньях управления, правительственной связи и специальной связи. При этом структура космического эшелона СС СН инвариантна по отношению к структуре системы государственного и военного управления.

Технологии, применяемые в ТКС космического эшелона, обеспечивают интеграцию различных видов трафика, устойчивое и глобальное взаимодействие комплексов и средств, на стационарных, полевых и подвижных узлах связи различных звеньев управления для стационарного наземного, полевого (мобильного) наземного, воздушного и морского эшелонов с целью обеспечения возможности обмена всеми видами информации между всеми абонентами во всех эшелонах СС СН.

4.2. Широкое использование в составе сети связи специального назначения канальных и сетевых ресурсов, арендуемых у коммерческих операторов связи

Анализ принципов построения современных СС СН, а также перспектив их развития, представленные в работах [2, 8-11, 25-28, 35, 51-54, 56-60], позволяет сформулировать следующие основные тенденции по технологическому построению СС СН:

- переход от иерархического принципа построения СС СН, когда ее структура жестко увязывается со структурой организационной подчиненности абонентов к децентрализованной сетевой структуре, которая

не зависит от организации системы подчиненности абонентов, и в большей степени соответствует современным требованиям к сетечетрическим системам государственного и военного управления;

- отказ от построения СС СН на основе отдельной связной инфраструктуры и переход к построению СС СН на основе гибридного подхода, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН;
- максимальное широкое использование для построения СС СН подходов, протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Данные тенденции подтверждаются общими принципами, заложенными в структуру построения СС СН для ВС РФ и для ВС США.

Стационарные и мобильные узлы, на основе которых будут разворачиваться компоненты перспективных СС СН, привязываются к единой транспортной сети СС СН, основу которой составят ВОЛС, а использование ССС обеспечит глобальность информационного обмена и связность отдельных сегментов ВОЛС.

При этом, при недостатке собственных ресурсов СС СН, как правило, необходимые каналные ресурсы из СС ОП арендуются у региональных и национальных операторов связи. Основным подходом к организации такой аренды является использование низкоуровневых ресурсов сети операторов связи, к которым можно отнести [9-11]:

- выделенные каналы связи для передачи потоков E1-E4, STM-n;
- оптические волокна в волоконно-оптическом кабеле;
- отдельные длины волн (в составе ВОЛС с технологией WDM);
- радиоресурсы коммерческих ССС;
- виртуальные и логические соединения на канальном уровне, реализуемые, например, с использованием базовых услуг канального уровня сети передачи данных VLAN, L2 VPN;
- виртуальные частные сети и туннели канального (технологии VLAN, MPLS L2 VPN, VPLS, PPTP, L2TP и др.) и сетевого уровня (технологии IP VPN, MPLS L3 VPN, IPSec и др.).

Необходимо отметить, что используемые структурно-технологические решения по сопряжению транспортных сетей из состава СС СН с сетями в составе СС ОП операторов связи обеспечивают связность на сетевом уровне, как правило, за счет использования единых протокольных решений на основе протоколов IPv4 и IPv6. В целях обеспечения безопасности при сопряжении СС СН с СС ОП оператора связи должны использоваться решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе СС СН и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются оператором связи СС ОП.

Ряд экспертов считает, что в настоящее время развертывание отдельной телекоммуникационной инфраструктуры СС СН является экономически нецелесообразным, и что современные и перспективные СС СН активно используют

и будут использовать ресурсы гражданских операторов СС ОП национального и регионального масштаба. Однако, при таком пути развития СС СН, на нее существенное влияние будут оказывать технологии, на основе которых строится и модернизируется сети гражданских операторов связи [9-11].

Таким образом, из самого факта сопряжения СС СН и СС ОП следует два важных вывода:

- 1) технологии связи СС СН должны быть «обратно совместимыми» с технологиями, используемыми в гражданских СС ОП, для обеспечения использования ресурса СС ОП в интересах СС СН;
- 2) сквозное сопряжение СС СН с СС ОП, а также последней с гражданскими СС ОП других государств, делает СС СН потенциально уязвимой для преднамеренных дестабилизирующих воздействий со стороны других государств.

Эти выводы определяют следующие современные тенденции развития СС СН:

- 1) мировой тенденцией является использование для построения перспективных СС СН современных «гражданских технологий», широко используемых в СС ОП, а не разработка специализированных технологических решений;
- 2) использование в СС СН «гражданских технологий» одновременно с их фактической интеграцией через общие сегменты СС ОП в мировое информационное пространство существенно расширяет спектр уязвимостей СС СН, которые могут быть использованы противником при реализации преднамеренных дестабилизирующих воздействий.

4.3. Массовое использование в современных сетях связи специального назначения технологий коммутации пакетов и коммерческих протоколов связи

В настоящий момент в мире происходит активное замещение специализированных технологий связи на открытые коммуникационные технологии, которые являются общими как для гражданских СС ОП, так и для СС СН. Например, в органах государственного и военного управления США и НАТО эксплуатируется большое количество СС СН, используемых различными ведомствами и базирующихся на использовании как специализированных военных, так и коммерческих телекоммуникационных ресурсов.

Принципиальным изменением, которое происходит в области построения транспортных сетей СС СН является переход к пакетной коммутации с одновременным обеспечением мультисервисного и интерактивного обслуживания абонентов. При этом в качестве базовых технологий в транспортных сетях доступа широко используются технологии коммутации пакетов IPv4 и IPv6, а также технология коммутации по меткам MPLS, которые начинают вытеснять технологии транспортных сетей PDH, SDH и ATM [8-11, 25-28].

Анализ работ [8-11, 25-28, 54, 56, 57], посвященных возможным вариантам технологического построения перспективных СС СН позволил сформиро-

вать основные принципы и технологии, используемые в них для организации связи.

Транспортная сеть СС СН представляет собой совокупность множества объединенных между собой пакетных ТКС, выполняющих задачи по доставке пакетов от абонента-источника к абоненту-потребителю.

Перспективные СС СН, как правило, строятся на основе ТКС, использующих IP протоколы. Кроме того, в них могут использоваться сети на основе технологий MPLS и MPLS-TE (для сетей на основе ресурсов ВОЛС и радиорелейной связи), технологии ATM, протоколов DVB-S/DVB-S2 (для CCC), протоколов на основе открытых стандартов STANAG (для сетей ДКМВ радиосвязи). Для обеспечения работы по каналам низкого качества, в большинстве случаев, в СС СН сохранено использование протоколов X.25 (для проводных аналоговых каналов с вероятностью ошибки 10^{-3}) и AX.25 (для аналоговых радиоканалов с вероятностью ошибки 10^{-2} и $5 \cdot 10^{-2}$) [51-53].

Таким образом, в транспортной сети СС СН используются следующие протокольные решения [2, 10, 22]:

- IP/MPLS самостоятельно или поверх PDH/SDH/OTH/ATM (для построения проводного транспортного сегмента);
- X.25 (для обеспечения работы по проводным аналоговым каналам и каналам связи низкого качества);
- AX.25 (для обеспечения работы по аналоговым радиоканалам и каналам связи низкого качества в условиях мирного времени, а также для построения мобильной (полевой) транспортной сети СС СН в условиях военного времени);
- протоколы семейства DVB (DVB-S/DVB-S2/DVB-RCS) для организации спутниковых каналов связи.

Применение пакетных технологий на основе протоколов IP/MPLS позволяет обеспечить организацию связи в транспортной сети СС СН на сетевых принципах, которые ранее были недоступны для ТКС на основе технологий коммутации каналов PDH/SDH/OTH. Это позволяет обеспечить в СС СН следующие эффекты [10]:

- возможность взаимодействия абонентов по принципу «каждый с каждым» (по схемам «point-to-point» и «multipoint-to-multipoint») в любой момент времени при условии эффективного использования сетевых ресурсов;
- эффект повышения устойчивости транспортной сети и улучшения качества обслуживания (QoS – Quality of Service), несмотря на возможное использование разных операторов связи, в условиях выхода из строя большинства узлов связи, за счет оперативной организации обходных маршрутов в статическом и динамическом режимах.

Объединение отдельных ТКС организуют путем обмена маршрутной информацией, необходимой для правильного выбора маршрута доведения пакетов с учетом отказов и возможной перегрузки элементов СС СН. Для СС СН, состоящей из большого числа ТКС и сетей с высоким числом взаимных связей используются динамические протоколы маршрутизации. При обмене маршрут-

ной информацией между ТКС и сетями в СС СН, как правило, используется маршрутный протокол BGP4 [51-53].

В ТКС и сетях, входящих в состав СС СН, используются известные модели и механизмы обеспечения качества обслуживания (Int Serv, Diff Serv), применяемые в пакетных сетях с целью обеспечения требуемых показателей QoS. С целью исключения случаев перегрузки трафиком в состав каждой ТКС включаются граничные маршрутизаторы. Передаваемый трафик котируется путем соглашения между абонентами и службой администрирования как ТКС, так и всей СС СН в целом. При превышении квот трафик сбрасывается, либо доводится без гарантий по соблюдению требуемых показателей качества обслуживания [50].

Таким образом, транспортная сеть СС СН строится с использованием единых подходов, архитектуры и принципов построения, технологий и средств передачи, защиты данных и управления в части как стационарного, так и мобильного (полевого) сегмента:

- стационарный сегмент транспортной сети СС СН строится с использованием ТКС, основанных на технологии пакетной коммутации IP/MPLS с встроенными функциями динамической маршрутизации, а также с использованием ТКС, основанных на технологиях коммутации каналов PDH/SDH/OTN с каналами типа E1-E4, STM-n. Причем, эти ТКС могут являться как сегментами самой СС СН, так и сегментами СС ОП региональных и национальных операторов связи;
- мобильный (полевой) сегмент СС СН строится с использованием ТКС, основанных на приоритетном использовании пакетных технологий IP/X.25/AX.25;
- унаследованное оборудование СС СН сопрягается с новыми средствами связи и современными ТКС через модули сопряжения, которые инкапсулируют трафик унаследованных средств связи в пакетный трафик, что позволяет обеспечить единый подход к транспортировке всех видов информации с использованием пакетной коммутации.

Вышеуказанные подходы к построению транспортной сети СС СН позволяют:

- организовать единый подход к передаче информации, основанный на технологиях коммутации пакетов, как по проводным (оптическим, медным и др.) и беспроводным (радиорелейным, тропосферным, спутниковым, широкополосного радиодоступа, КВ/УКВ и иным) аналоговым и цифровым каналам связи СС СН, так и по каналам связи СС ОП региональных и национальных операторов связи, включая глобальную сеть Интернет;
- осуществлять оперативное динамическое управление ресурсами СС СН, в том числе адаптивную маршрутизацию потоков трафика с учетом динамики изменения структуры транспортной сети СС СН в результате дестабилизирующих воздействий.
- обеспечить согласованное взаимодействие отдельных ТКС, сетей и унаследованных средств связи, входящих в транспортную сеть СС СН,

- и в итоге – объединить их в единое телекоммуникационное пространство;
- получить ряд технологических преимуществ от внедрения в состав СС СН новых ТКС, основанных на новейших коммерческих технологиях из гражданской отрасли связи.
- Обобщенная структурная схема сети СС СН приведена на рис. 7.

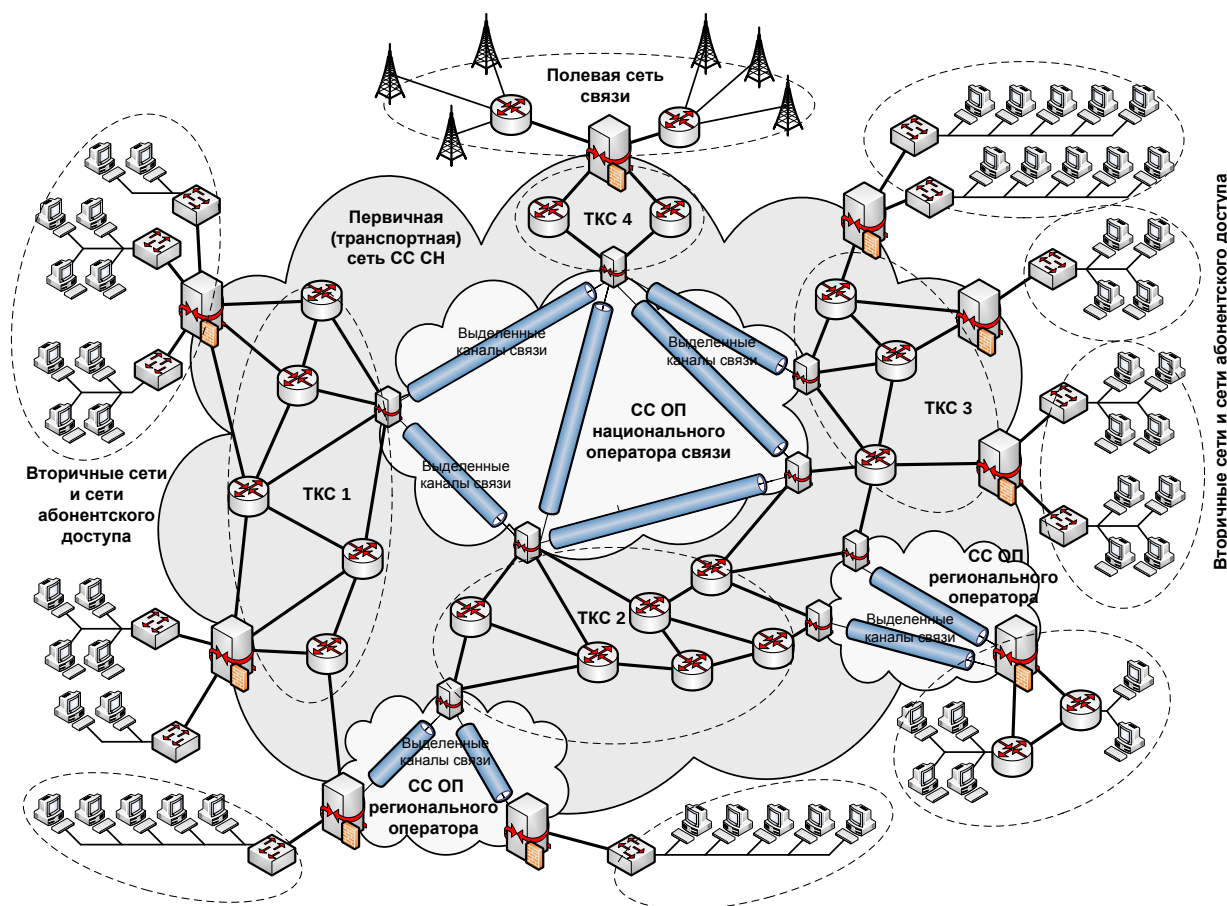


Рис. 7. Обобщенная структурная схема СС СН

4.4. Перспективы построения сетей связи специального назначения в соответствии с концепцией NGN

Анализ работ по глобальным перспективам развития СС СН [8-11, 25-28] позволяет сделать вывод об эволюционном развитии СС СН в направлении перехода к концепции NGN. В частности, в данном направлении эволюционируют СС СН США, в которых приняты концептуальные решения по объединению в единое информационное пространство разнородных сетей и систем связи, с переходом к персонализированным услугам связи для каждого абонента вне зависимости от его географического местонахождения. Обзор основных технологических решений концепции NGN представлен в более ранней работе автора [42], а возможности по использованию концепции NGN для построения СС СН в достаточно полном виде представлены в работе А.Н. Назарова и К.И. Сычева [8].

Базовым принципом построения сети связи следующего поколения является строгое разделение функций переноса и коммутации информационных потоков, управления вызовами и услугами. При этом в соответствии с рекомендацией МСЭ-Т Y.2011 базовая архитектура сети NGN может быть представлена четырьмя функциональными уровнями [8]:

- 1) уровня приложений и услуг;
- 2) уровня коммутации услуг;
- 3) уровня транспорта, включающего функции управления сетевыми ресурсами и уровень доступа;
- 4) уровня управления сетью.

Для построения сети NGN необходимо в дальнейшем реализовать каждый из этих уровней в виде соответствующего набора элементов сети NGN (рис. 8). При этом на различных логических уровнях сети могут использоваться различные технологии и протоколы.

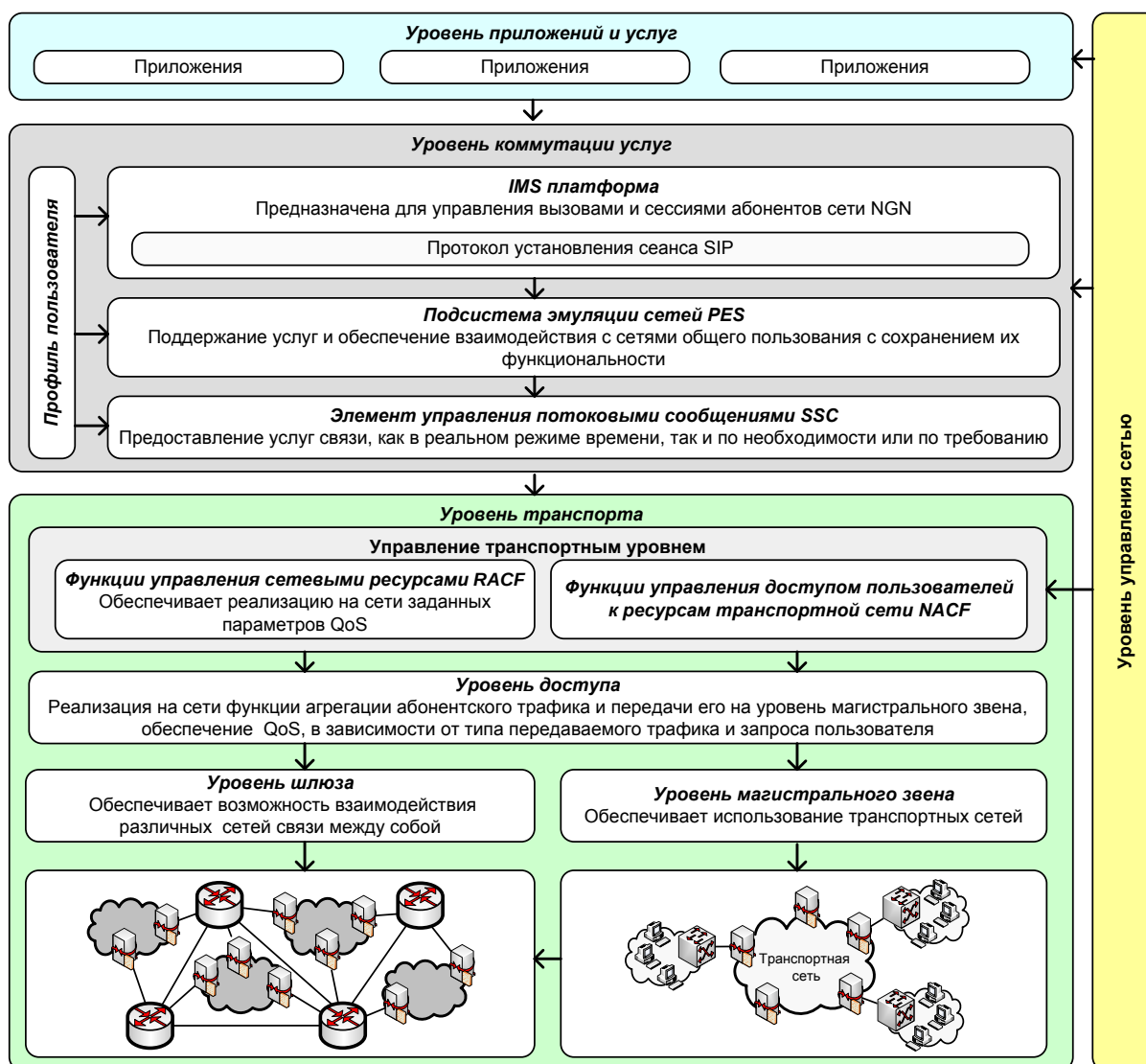


Рис. 8. Схема основных уровней сети NGN [42]

Уровень приложений и услуг содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую следующие потребности [42]:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;
- взаимодействие различных услуг.

Уровень коммутации услуг позволяет реализовать специфику услуг, и применять одну и ту же логику оказания услуги вне зависимости от типа транспортной сети (IP, ATM, FR и т. п.) и способа доступа. Наличие этого уровня также позволяет вводить в сети любые новые услуги без вмешательства в функционирование других уровней. В основе этого уровня лежит взаимодействие с центральными элементами сети NGN – элементами уровня коммутации (IMS, PES и SSC), которое осуществляется по стандартным интерфейсам ANI (Access Network Interface) для доступа в сеть. Данный уровень может включать множество независимых подсистем («сетей услуг»), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации [42].

С функциональной точки зрения, данный уровень должен решать основные задачи по установлению соединений и предоставлению услуг в сети NGN. Основными функциями данного уровня являются [42]:

- регистрация пользователей (аутентификация и авторизация) для предоставления им доступа к определенным услугам NGN;
- управление сессиями, вызовами (установление, разрыв и поддержание соединений);
- управление коммутацией и передачей, обработку информации сигнализации, маршрутизация вызовов и управление потоками;
- управление ресурсами сети, включая шлюзы, установленные на транспортном уровне сети NGN.

Транспортный уровень сети NGN обеспечивает функции коммутации и прозрачной передачи информации пользователя. Данные функции образуются двумя подгруппами [42]:

- функции управления сетевыми ресурсами (RACF – Resource and Admission Control Functions), обеспечивающие реализацию в сети заданных параметров QoS. В их задачи входит резервирование требуемых сетевых ресурсов, управление доступом к ресурсам транспортной сети, управление ресурсами шлюзов и т.д.;
- функции управления доступом пользователей к ресурсам транспортной сети NGN (NACF – Network Attachment and Control Functions), осуществляемые на основе информации авторизации пользователей, соглашений об уровне обслуживания SLA, приоритета предоставляемой услуги, а также доступных сетевых ресурсов на транспортной сети и сети доступа.

Транспортный уровень включает в себя ряд функциональных подуровней [42].

- Уровень доступа. Доступ должен предполагать реализацию в сети функции агрегации абонентского трафика и передачи его на уровень магистрального звена. Данный уровень предполагает наличие функций обеспечения QoS, которые зависят от типа передаваемого трафика и запросов пользователя.
- Уровень магистрального звена. Магистральное звено в виде отдельной ТКС должно обеспечивать передачу агрегированного пользовательского трафика в соответствии с требованиями по QoS. На данном уровне применяются те же механизмы по управлению QoS, что и на уровне доступа.
- Уровень шлюза. Данный уровень обеспечивает возможность взаимодействия различных ТКС, построенных на основе различных технологий, а также взаимодействие с другими сетями NGN;

Технологической основой построения транспортного уровня является транспортная сеть NGN, строящаяся в настоящее время на основе технологий коммутации каналов PDH/SDH/OTN и, преимущественно, коммутации пакетов IP, ATM, MPLS. В дальнейшем планируется, что связка протоколов IP/MPLS и технология построения виртуальных сетей VPN будут базовыми для транспортного уровня NGN. Данные технологии способны обеспечивать управление и мониторинг качества всех уровней магистрального звена: сетевого, канального и физического. Это обеспечивает возможность предоставления абонентам сети услуг с заданным качеством.

Уровень управления сетью отвечает за организацию системы управления сетью NGN. В задачи уровня входят мониторинг и управление инфраструктурой и ресурсами сети, поддержание в сети заданных параметров качества, а также ряда параметров, характеризующих работу сети в целом (безопасность и устойчивость) [42].

Система управления должна обеспечивать [42]:

- управление процедурами устранения ошибок и сбоев;
- управление процедурами конфигурации;
- управление автоматизированной системой расчетов;
- управление сетевыми характеристиками;
- управление безопасностью.

Основу сети NGN составляет мультипротокольная ТКС (как правило, на основе ATM, IP, MPLS), которая предоставляет услуги переноса и реализует функции транспортного уровня и уровня управления вызовами. Целью построения транспортной сети NGN является переход от отдельных сетей предыдущего поколения, предназначенных для отдельных групп пользователей или услуг (телефония, данные и др.) к интегрированной сети с гарантированным качеством обслуживания.

В состав интегрированной транспортной сети NGN могут входить [8]:

- 1) транзитные узлы, выполняющие функции переноса и коммутации;
- 2) оконечные и граничные узлы, обеспечивающие доступ абонентов;
- 3) контроллеры сигнализации или контроллеры медиашлюзов (Media Gateway Controller, MGC/Softswitch), выполняющие функции обработ-

ки информации сигнализации, управления вызовами (запросами) и соединениями, а также управления транспортной сетью NGN;

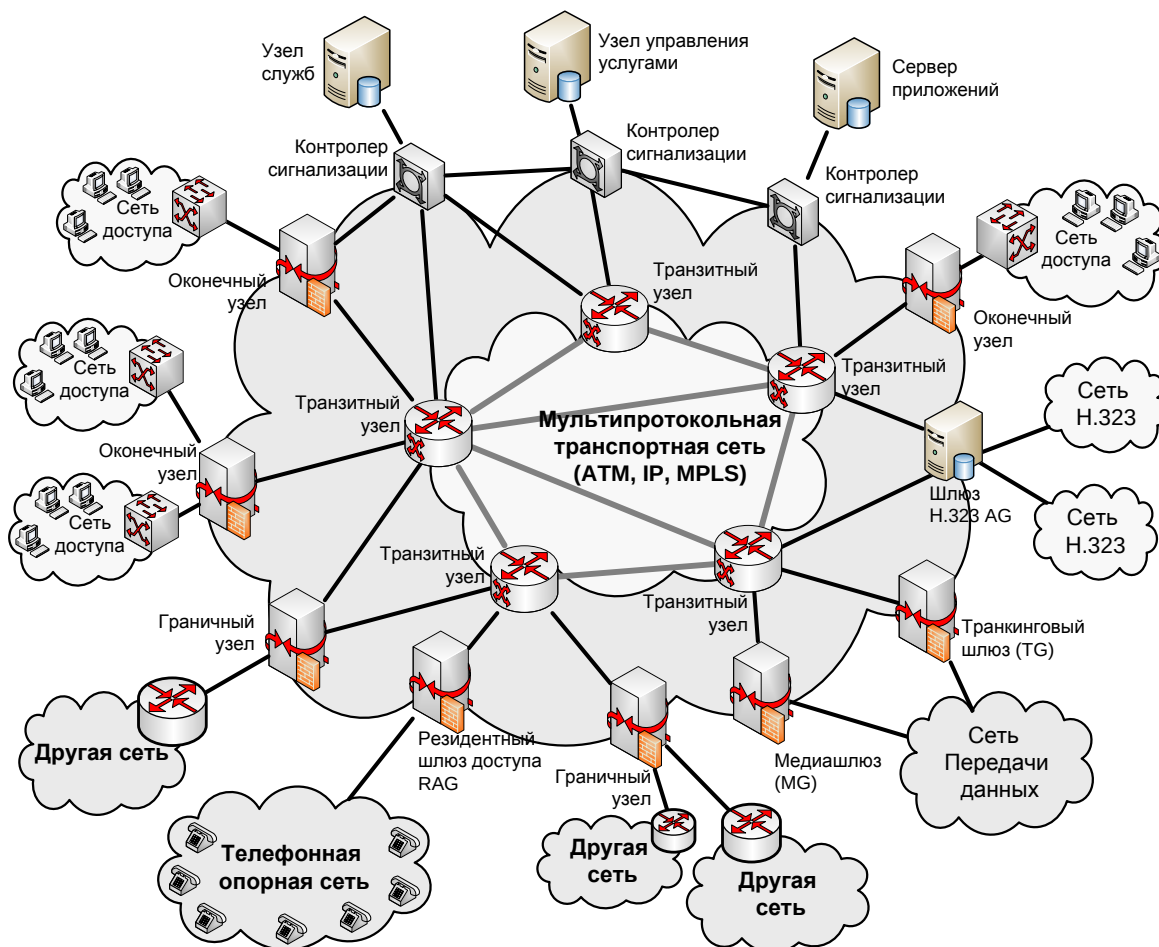


Рис. 9. Мультипротокольная (ATM, IP, MPLS) транспортная сеть NGN [42]

4) шлюзы, осуществляющие подключение сетей связи предыдущих поколений:

- медиашлюз или транспортный шлюз MG (Media Gateway), предназначенный для преобразования речевой информации в IP-пакеты или ATM-ячейки и их маршрутизации;
- сигнальный шлюз SG (Signalling Gateway), предназначенный для преобразования систем межстанционной сигнализации;
- транкинговый шлюз TG (Trunking Gateway), выполняющий функции транспортного и сигнального шлюзов;
- шлюз доступа AG (Access Gateway), выполняющий функции транспортного и сигнального шлюзов при подключении по интерфейсу V.5;
- резидентный шлюз доступа RAG (Residential Access Gateway), предназначенный для подключения пользователей телефонных сетей и сетей ISDN;

5) пограничный контроллер соединений SBC (Session Border Controller), обеспечивающий сопряжение оборудования нескольких производителей и выполняющий функции шлюза сигнализации и медиа-шлюза,

контроля за установлением соединений САС (Call Admission Control), управления QoS, концентрации голосового и сигнального трафика;

б) сетевые устройства на основе стандарта H.323 для реализации узкополосных аудио и видео услуг в комбинированных коммутируемых и пакетных сетях:

- шлюз H.323 AG (Access Gateway), предназначенный для преобразования медиа-потокa между коммутируемыми и пакетными сетями;
- шлюз-привратник (Gatekeeper H.323), предназначенный для преобразования адресации (IP, телефонных номеров) между коммутируемыми и пакетными сетями, а также управления полосой пропускания;
- блок многоточечного управления MCU (Multipoint Control Unit), предназначенный для обеспечения соединений «point-to-multipoint», «multipoint-to-multipoint», а также конференцсвязи.

Концепция NGN предполагает создание регионального и магистрального сегментов сети. При этом на региональном уровне должно обеспечиваться подключение пользователей и предоставление им транспортных услуг, а также взаимодействие с аналогичными региональными транспортными сетями. На магистральном уровне должно обеспечиваться предоставление услуг переноса конвергентного трафика для взаимодействия региональных сетей, а также для передачи трафика всех существующих сетей [8].

Модель звена транспортной сети NGN представлена на рис. 9. При этом в данной модели для реализации любых сетевых услуг в ТКС предполагается использование IP-технологии.

При построении сетей NGN обеспечиваются следующие сочетания транспортных технологий [8]:

- IP/ATM/SDH/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/ATM/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/SDH/ВОЛС, радиорелейные, спутниковые линии связи;
- IP/ВОЛС;
- IP/MPLS/ВОЛС, радиорелейные, спутниковые линии связи.

Технология IP
Технологии установления соединений, маршрутизации и обеспечения QoS (MPLS, Int Serv, Diff Serv ...)
Технологии формирования тракта связи (PDH, SDH, OTH, xWDM, ATM, DVB, ...)
Технологии среды передачи

Рис. 10. Модель звена транспортной сети NGN [8]

Для построения сетей NGN нового поколения могут применяться технологии цифровых транспортных иерархий нового поколения OTN/OTH, а также технологии автоматически коммутируемых транспортных сетей ASON/ASTN, которые будут обеспечивать более высокую эффективность использования се-

тевых ресурсов при передаче разнородного трафика. В перспективе построение транспортной сети NGN будет эволюционировать к однородной конвергентной структуре на базе связки протоколов IP/MPLS – концепция «все по IP» (рис. 5). При этом данная транспортная сеть будет включать две плоскости: сетевой и сервисный [8].

Сетевая плоскость включает [8]:

- транспортную сеть IP/MPLS выполняющую функции канального сетевого и транспортных уровней модели OSI;
- пограничный интеллектуальный слой (шлюзы MG, SG, MGC), предназначенный для объединения, преобразования и передачи трафика по IP/MPLS сети;
- уровень доступа.

В свою очередь сервисный домен включает различные платформы приложений (в том числе IMS) и серверы приложений.

Данный подход обеспечит дальнейшее повышение эффективности использования сетевых ресурсов при внедрении NGN за счёт объединения различных ТКС фиксированной и мобильной связи в составе СС СН в единую транспортную сеть IP/MPLS, поддерживающую широкий спектр технологий доступа.

4.5. Перспективы перехода от сетей связи специального назначения к инфокоммуникационным сетям специального назначения

Дальнейшее развитие концепции NGN в практике построения СС СН привело к эволюционной миграции от СС СН к инфокоммуникационным сетям специального назначения. Ключевым в таком переходе является развитие на основе концепции NGN информационных услуг, связанных не только с передачей информации, но и с ее сбором, обработкой, хранением, а также представлением ее пользователям по их запросам. Переход от СС СН на основе NGN к инфокоммуникационным сетям связан с развитием автоматизированных систем управления связью и интеграцией в них существующего задела в области управления ресурсами связи в СС ОП (прежде всего стандартов концепции TMN), виртуализации сетевых и вычислительных ресурсов, а также использование новых технологических решений по обеспечению устойчивости такой сети в условиях преднамеренных дестабилизирующих воздействий.

Основные принципы формирования инфокоммуникационных сетей достаточно подробно рассмотрены в работах К.Е. Легкова [16-21] и А.Н. Буренина [20, 21].

Инфокоммуникационная сеть специального назначения (ИКС СН) – информационная система, обеспечивающая предоставление набора как связных, так и информационных услуг с гибкими возможностями по управлению ими и их персонализации, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [17].

Главное отличие ИКС СН от СС СН на основе NGN – это дополнительное предоставление пользователям и техническим средствам помимо связных еще и информационных услуг, связанных со сбором, обработкой, хранением и предоставлением информации пользователям. Предоставление этих услуг унифицировано и осуществляется соответствующими программно-аппаратными комплексами услуг, которые поддерживают широкий спектр ТКС в составе ИКС СН. Тем самым обеспечивается предоставления всем пользователям полного спектра услуг, связанных с как обменом информацией и ее передачей, так и с ее обработкой, хранением и накоплением [17].

Как правило, различные ИКС СН существенно отличаются друг от друга потребностями в ресурсах, объемом, структурой, возможностями, реальной пропускной способностью, а также безопасностью и устойчивостью [17].

Создаваемые в настоящее время ИКС СН следуют концепции NGN. Основой архитектурного построения ИКС СН являются транспортная сеть (как правило, двухуровневая), сети доступа, узлы информационных служб, узлы телекоммуникационных служб и узлы управления услугами [17].

В современных ИКС СН двухуровневая транспортная сеть связи, входящая в их состав, является мультипротокольной, и обеспечивает перенос разных видов информации с использованием различных протоколов передачи (PDH, SDH, ATM, FR, IP/MPLS и др.), т. е. реализует универсальную услугу связи, которая заключается в бесшовной передаче информации пользователей между отдельными ТКС в составе ИКС без какого-либо анализа или обработки ее содержания [17].

Средства ИКС СН помимо услуги связи, предоставляют также информационные услуги, основанные на обработке и анализе информации пользователей. В рамках ИКС СН информационные услуги характеризуются транзакциями, которые осуществляются при запросе/активизации услуги. При этом сервис предоставления информационной услуги основан на том, что соответствующие услуги связи для информационных транзакций оказываются с заданным качеством. Пользователи могут воспользоваться информационными услугами ИКС СН напрямую или с помощью пользовательских приложений. При этом компоненты пользовательских услуг обычно объединяются в пакеты, чтобы создать для конкретного пользователя требуемую сложную услугу или предоставить доступ к нескольким приложениям. Спектр информационных и связных услуг, которые обычно обеспечиваются в рамках современных ИКС СН, достаточно широк. При этом он может динамически меняться вместе с изменением доступных ресурсов [17].

В целом ИКС СН составляет совокупность баз данных, средств обработки информации, взаимодействующих ТКС и множество терминалов пользователей. При этом доступ к информационным ресурсам ИКС СН реализуется посредством услуг нового типа – инфокоммуникационных услуг. Предполагается, что именно они будут преобладать в ИКС СН перспективных систем связи уже в ближайшем будущем [17].

К основным технологическим особенностям, отличающим инфокоммуникационные услуги от услуг связи, можно отнести следующие [17]:

- инфокоммуникационные услуги оказываются на прикладном уровне модели OSI, в то время как услуги связи предыдущего поколения предоставляются на транспортном и сетевом уровнях OSI;
- стандартизация инфокоммуникационных услуг ведется на основе стандарта OSE/RM (Open System Environment / Reference Model) и ISO/IEC TR 14252 которые существенно расширяют и дополняют модель OSI в части детализации прикладного уровня [18];
- большинство инфокоммуникационных услуг предполагает наличие клиентской и серверной частей, где клиентская часть реализуется в оборудовании пользователя, а серверная – на специальном выделенном узле ИКС, называемом узлом служб;
- инфокоммуникационные услуги, как правило, предполагают передачу мультимедийной информации, которая характеризуется высокими скоростями передачи и асимметричностью входящего и исходящего информационных потоков;
- для предоставления инфокоммуникационных услуг зачастую необходимы сложные многоточечные топологические конфигурации сетевых соединений;
- для инфокоммуникационных услуг характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;
- для идентификации абонентов инфокоммуникационных услуг, как правило, используется дополнительная адресация в рамках данной инфокоммуникационной услуги.

Обобщенная информационная архитектура перспективной ИКС СН представлена на рис. 11.

Особенностью интеграции сервиса оказания информационных услуг пользователя в ИКС СН является то, что существенно возрастает роль систем управления, как услугами, так и сетью. Для реализации функций управления создаются службы NMS (Network Management System), которые обеспечивают оптимальное функционирование сетей, распределенное планирование, управление и контроль сетевых элементов и ресурсов. Функции службы NMS описываются специальной моделью (рекомендации МСЭ-Т серии X.700, стандарт ISO 7498-4), которая определяет функции управления, виды услуг сетевой службы, предоставляемые для управления, структуру управляющей информации и протоколы, определяющие ее транспортировку по сети [19].

В соответствии с моделью ISO 7498-4 управление сетью обеспечивается локальным управлением всеми элементами, входящими в сеть. Модель охватывает следующие основные функции управления [19]:

- базовые протоколы технологии IP;
- маршрутные протоколы;
- протоколы групповой рассылки;
- протоколы повышения надежности маршрутизации;
- протоколы и технологии обеспечения качества обслуживания;
- протоколы обеспечения безопасности.

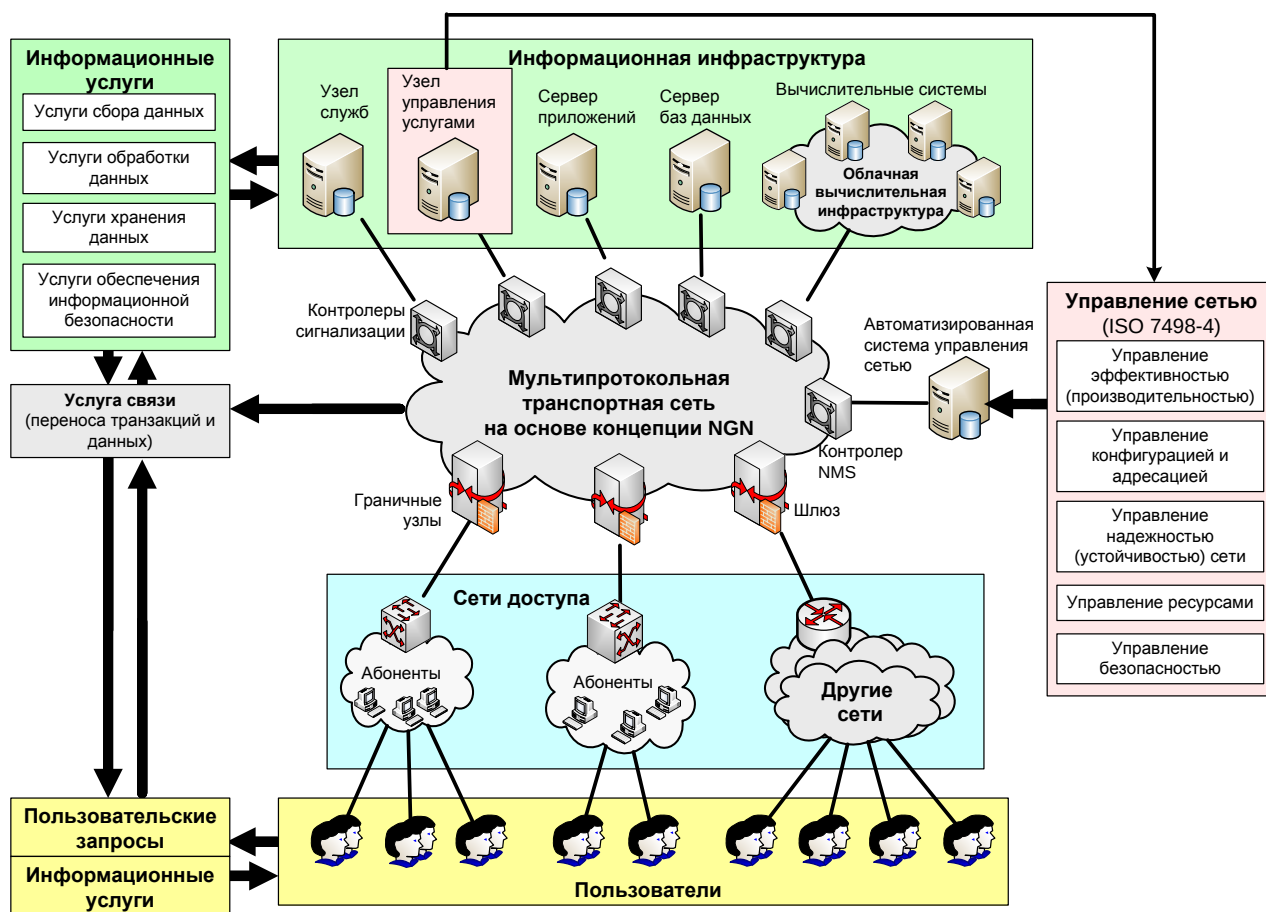


Рис. 11. Обобщенная архитектура перспективной ИКС СН

Подробные сведения о реализации процессов управления в сети в соответствии с моделью ISO 7498-4, а также о современных протоколах мониторинга и управления сетью представлены в работе [19].

Таким образом, наблюдается устойчивая тенденция по все более широкому использованию в сетевом оборудовании СС СН технологий и протоколов из гражданской отрасли связи. Это, с одной стороны, позволяет значительно сократить время и финансовые расходы на разработку и внедрение в СС СН новейших технологий, однако с другой, делает такие СС СН уязвимыми к преднамеренным дестабилизирующим воздействиям, характерным для военного времени.

5. Проблемные вопросы обеспечения эксплуатации и модернизации сетей связи специального назначения

5.1. Проблемные вопросы обеспечения устойчивости сетей связи специального назначения в условиях перехода от технологий коммутации каналов к технологиям коммутации пакетов

Проведенный на основании работ [9-10, 25-28] анализ развития транспортной сети СС СН показал, что модернизация сетей связи, в первую очередь, была направлена на замену устаревших технологий новыми в интересах достижения более высокой пропускной способности и обеспечения абонентам новых

услуг связи. При этом для решения задач повышения пропускной способности транспортной сети используются наработанные подходы и технологии из гражданской сферы связи. Однако при выборе протольно-технологического базиса транспортной сети следует руководствоваться не только необходимостью кардинального повышения пропускной способности и расширения спектра услуг связи, но и специфическими требованиями, предъявляемыми к СС СН, а именно устойчивого функционирования в мирное время, угрожаемый период и военное время. Последнее обуславливает целый ряд дополнительных параметров, вытекающих из необходимости обеспечивать своевременный, скрытный и достоверный обмен информацией между пунктами управления и абонентами СС СН в условиях ведения противником информационной, разведывательно-диверсионной борьбы и РЭБ.

Можно выделить три вида дестабилизирующих воздействий, которые потенциально будут иметь место при функционировании СС СН в угрожаемый период и в военное время:

- 1) информационно-технические воздействия (ИТВ) на узловое телекоммуникационное оборудование и на протоколы связи СС СН;
- 2) воздействия на радиоканалы и радиосети в составе СС СН средствами радиоэлектронного подавления (РЭП), воздействия на узловое оборудование СС СН средствами функционального поражения электромагнитным излучением;
- 3) воздействия на узловое оборудование и проводные линии связи СС СН обычным оружием.

Дестабилизирующие воздействия на объекты физического уровня будут отображаться на сетевом уровне в виде следующих эффектов [3, 24]:

- снижение качества каналов;
- снижение скоростей информационного обмена;
- возникновение одиночных и групповых ошибок приема;
- сбои тактовой синхронизации функционирующего в синхронном режиме оборудования, приводящие к потере данных;
- перерывы в связи;
- сбой или выход из строя телекоммуникационного оборудования сетевых узлов;
- сбой или неправильное функционирование протоколов связи в сети.

Анализ, проведенный в работах [2, 10, 22], показал, что, например, ВС США при построении своей СС СН исходят из того, что в военное время при массированном применении средств РЭП единственным видом связи может остаться передача данных в КВ-диапазоне. Однако информационный обмен по КВ-радиоканалу в режиме пакетной коммутации возможен только с применением протокола AX.25 (так как вероятность ошибки в канале может достигать значений 10^{-3} - 10^{-2} , а в отдельных случаях и $5 \cdot 10^{-2}$). В то время, как стандартные протоколы IP предусматривают работу только по каналам связи среднего качества и выше.

Ранее используемые технологии транспортных сетей, такие как PDH и SDH, так же не способны обеспечить устойчивость связи. Так сети PDH, ввиду

отсутствия возможностей по развитой маршрутизации информационных потоков не способны обеспечить должной оперативности реконфигурации сети. Сети SDH, несмотря на развитый методический аппарат построения устойчивых топологических решений на основе колец и схем резервирования каналов, в результате дестабилизирующего воздействия противника подвержены недопустимо частым сбоям синхронизации, приводящим к непоправимой потере данных.

Недостатки сетей PDH/SDH/OTH следуют из самого принципа их псевдостатического построения, когда все проистекающие в них процессы носят статический характер и фактически не позволяют реконфигурировать транспортную сеть в режиме реального времени. Использование технологии автоматически коммутируемых транспортных сетей ASON/ASTN применительно к существующим сетям PDH/SDH/OTH лишь частично решает вопросы обеспечения структурной устойчивости. По сути технология ASON/ASTN предоставляет только сервис автоматической реконфигурации PDH/SDH/OTH сетей не решая задачи повышения оперативности управления ресурсами сетей.

Однако и пакетные транспортные сети эффективны только при условии, что они поддерживают динамическое равновесие при обеспечении QoS абонентов и приспособляются к быстро изменяющимся условиям. Так, в сетях с использованием пакетных технологий IP/MPLS длительность процессов перемаршрутизации находится в секундном диапазоне [55], что на порядки превышает аналогичные показатели для SDH-сетей, в которых гарантированная длительность переключения на резервную конфигурацию обеспечивается механизмами физического уровня и составляет 50 мс.

Кроме того, сама возможность маршрутизации, порождает специфическую уязвимость пакетных сетей, источником которой является сбой в протоколах маршрутизации [30, 45]. При этом в силу особенностей работы протоколов маршрутизации подобные нарушения могут распространяться по сети лавинообразно. Именно на это обстоятельство обращает внимание в своем отчете [46] Проблемная группа по NGN Консультативного комитета по связи для национальной безопасности при Президенте США. Рекомендация МСЭ-T G.1000 [47] также указывает, что использование сетей и служб на основе IP выдвигает целый ряд проблем, таких, как отсутствие апробированных, надежных и масштабируемых технологий для решения целого ряда задач, в частности, быстрого восстановления связности на сетевом уровне после серьезных сбоев.

Реальным и конкретным примером, показывающим опасность перехода к инфраструктуре на основе IP, является выход из строя значительной части IP сети японского оператора NTT, имевший место 15 мая 2007 г. [49]. При этом от 2 до 4 тыс. маршрутизаторов производства Cisco прекратили работу, и их неработоспособность продолжалась около 7 ч. При этом первопричиной события стало переключение на резервные маршруты, вызвавшее некорректное обновление маршрутных таблиц, что и привело к массовой неработоспособности маршрутизаторов [30].

Еще одной проблемой пакетных сетей является широкий диапазон значений джиттера времени передачи пакетов. Даже если отправитель посылает па-

кеты в сеть через равные интервалы времени, получатель может получать их через промежутки времени, отличающиеся на десятки миллисекунд. Это происходит из-за того, что задержки передачи отдельных пакетов существенно зависят от загруженности маршрутизаторов и каналов связи, от структуры пакетного трафика, а также от длины маршрута, состоящего из разного числа промежуточных приемо-передач. Корректировку джиттера отдельных пакетов, который образуется из-за разности во времени передачи отдельных пакетов по сети, приходится производить в конечном оборудовании данных. При этом сети PDH/SDH/OTN являются детерминированными – задержка распространения сигнала в них мала и постоянна, синхросигнал передается вместе с данными, а на джиттер наложены строгие ограничения, что позволяет добиться передачи информации в режиме времени, близком к реальному. Так для этих сетей изменения задержки должны лежать в пределах от 40 нс до 18 мкс. В то время как в пакетных сетях, в которых данные передаются с использованием таких протоколов как IP и MPLS, изменения задержки передачи пакетов в них могут составлять десятки миллисекунд [10].

В работе [10] указывается, что проблема джиттера пакетов якобы решается путем использования технологий CES (Circuit emulation service) для передачи потоков E1, E3 и STM-1 через пакетные сети при сохранении высоких требований к синхронизации. Технология CES основана на алгоритмах адаптации и инкапсуляции трафика сетей PDH и SDH в пакеты и последующей его передачи через пакетную сеть (технология TDMoIP или TDMoP). Однако технология CES, решая проблемы обеспечения передачи потоков PDH и SDH, а также обеспечивая синхронизацию этих сетей через пакетные сети, не гарантирует постоянный уровень джиттера передачи пакетов, в которые инкапсулируются потоки E1, E3 и STM-1.

Проблемой пакетных сетей также являются гигантские пульсации трафика. Если коэффициент пульсации телефонного трафика имеет значения от 5 до 15, то при передаче данных данный коэффициент составляет значения сотни тысяч [43]. Однако технологии PDH/SDH/OTN в моменты роста трафика вообще не способны динамически предоставить большую полосу пропускания, а в моменты спада не в состоянии использовать свободную полосу.

5.2. Проблемные вопросы обеспечения устойчивости сетей связи специального назначения в условиях внедрения концепции NGN

Одной из основных проблем при построении СС СН в соответствии с концепцией NGN является устойчивость сетевой инфраструктуры. При этом, как отмечается в работе [30], обеспечение устойчивости в сетях NGN является более сложной задачей, чем обеспечение устойчивости сетей предыдущего поколения, основанных на коммутации пакетов или каналов.

Во-первых, в основе сетей NGN лежат IP-сети. В связи с этим все проблемные вопросы, связанные с недостаточно быстрым восстановлением этих сетей, рассмотренные выше, являются актуальными и для сетей NGN.

Во-вторых, для сетей предыдущего поколения, основанных на коммутации каналов, основной нормируемой составляющей надежности является го-

товность узла, требование к которой задавалось в виде $K_T=0,99999$ [44]. При переходе к NGN вместо традиционного узла коммутации используется гибкий коммутатор (Softswitch). Возникает комплекс из большого числа отдельных устройств (контроллеров, шлюзов, серверов). Все они имеют высокую надежность: значение коэффициента готовности каждого из них, как обычно заявляют производители, составляет все те же «пять девяток». Однако для выполнения функций узла коммутации необходима совместная работа нескольких таких устройств, поэтому результирующая надежность будет равняться произведению их коэффициентов готовности, т. е. в итоге она оказывается более низкой [30].

В-третьих, еще более важным фактором, негативно влияющим на надежность сетей NGN, является централизация управления процессами обслуживания вызовов. Критическим элементом сети NGN становится контроллер шлюзов или сервер вызовов (Softswitch в узком понимании этого термина). При этом один такой контроллер или сервер управляет многими шлюзами, поэтому его отказ может привести к прекращению работы сети на большой территории. Подобная ситуация негативно влияет на устойчивость сети. Неслучайно ведущие производители оборудования NGN предусматривают возможность резервирования контроллеров шлюзов, в том числе с географическим разнесением. Однако многие операторы связи подобное резервирование при проектировании своих сетей не используют из соображений экономии [30].

5.3. Проблемные вопросы управления сетью связи специального назначения в условиях внедрения концепции NGN

Вышеуказанные проблемы обеспечения устойчивости СС СН в условиях дестабилизирующих воздействий при ограничениях на качество обслуживания специальных абонентов предъявляют жесткие требования к системе управления связью. Несмотря на то, что концепция NGN предусматривает стандартные подходы к управлению услугами и средствами связи, она не рассматривает условия перманентных дестабилизирующих воздействий как повседневные условия функционирования сети. Таким образом, переход СС СН к концепции NGN требует существенной доработки принципов и подходов NGN в части управления связью применительно к СС СН. Исследование этой тематики проводилось в работах К.Е. Легкова [16-21], А.Н. Буренина [20, 21], Н.А. Соколова [29], А.Е. Давыдова [31].

Система управления связью является важнейшей подсистемой СС СН. В настоящее время практически во всех современных СС СН и СС ОП развитых стран развернуты центры управления связью с той или иной степенью автоматизации, выполняющие необходимые функции, связанные с мониторингом, контролем состояния и изменением конфигурации удаленных сетевых устройств. Большинство этих систем управления строится по иерархическому принципу, позволяющему обеспечивать более гибкое, эффективное и оперативное управление за счет сегментирования СС СН на более мелкие элементы – региональные и местные сети, а также отдельные ТКС. При этом разработка систем централизованного управления связью является довольно сложной

наукоемкой задачей, в рамках которой необходимо объединить разнотипное оборудование различных производителей, которое имеет различный функционал, принципы и возможности управления [31].

Надо отметить, что в этом смысле задачи управления, решаемые в СС СН и в СС ОП, идентичны и в равной степени актуальны. Однако существенные различия в подходах и методах решения задач управления проявляются в уровне наблюдаемости, управляемости, а также в своевременности принятия решений применительно к СС СН. Это обусловлено большим количеством специфичных требований, предъявляемых к СС СН, по сравнению с СС ОП, таких как: устойчивость, боевая готовность, мобильность, управляемость, разведзащищенность и др. Степень выполнения этих специфичных требований зависит от подходов к управлению связью, и, что самое главное, эти требования предъявляют крайне жесткие требования к оперативности управления [31].

Оперативность управления определяет время реакции системы связи на различные виды изменений, вносимые в состав, конфигурацию или режимы функционирования СС СН. В свою очередь характеристики оперативности управления во многом определяются, с одной стороны, уровнем автоматизации процессов управления связью, а с другой – самими принципами организации управления, закладываемыми при разработке телекоммуникационного оборудования [31].

Так, недостаточный уровень автоматизации процессов управления некоторых СС СН уже сегодня стал их ключевой проблемой, решить которую можно только путем перехода от повсеместно применяемого принципа управления отдельно взятым сетевым элементом, предложенного ведущими производителями телекоммуникационного оборудования, к принципу единого сетевого управления, которая рассматривает СС СН как совокупность различных сетевых ресурсов. Такое изменение принципов управления обусловлено не только необходимостью выполнения жестких требований по оперативности управления и автоматизацией связных процессов, но и изменениями самих телекоммуникационных технологий [31].

В большинстве работ под управлением связью понимается настройка оборудования первичной сети с последующим наложением на транспортную сеть различного рода услуг связи. В условиях, когда перечень услуг исчисляется единицами, такой подход подразумевал лишь выделение абоненту номерной емкости и определенного сетевого ресурса. При переходе СС СН к концепции NGN резко увеличивается номенклатура предоставляемых услуг связи и их персонализация. В результате ведущее значение приобретает не настройка отдельных средств связи, а именно персонализация услуг, в зависимости от которых формируется сначала телекоммуникационная инфраструктура СС СН, а затем на ее основе формируется единый пул сетевых ресурсов, который должен использоваться с высокой эффективностью, а также с учетом условий дестабилизирующего воздействия на элементы телекоммуникационной инфраструктуры [31].

Вместе с тем, использование в составе СС СН сегментов СС ОП и коммерческого оборудования связи не позволяет в полной мере реализовать ука-

занные подходы к управлению связью. Разработчики СС СН вынуждены использовать подходы к управлению, принятые ведущим производителями коммерческого сетевого оборудования, ввиду их широкого использования в составе СС СН. В основу управления коммерческим сетевым оборудованием, согласно современным стандартам по NMS, среди прочего включается [19]:

- управление неисправностями;
- управление конфигурацией;
- управление ресурсами.

Как правило, эти функции управления реализуются в отношении одного или группы однотипных устройств в соответствии с моделью «агент – сервер». При этом управление осуществляется с помощью ввода соответствующих команд вручную или с помощью графического интерфейса пользователя и предполагает наличие сервисной инженерной службы, которая в случае отказа или сбоя средства связи диагностирует и конфигурирует его удаленно [31].

Условия функционирования СС СН характеризуются динамическим воздействием преднамеренных дестабилизирующих факторов, выходом из строя элементов СС СН из-за их огневого или радиоэлектронного поражения, динамическим переходом на дополнительные каналы связи, подключением дополнительных сетевых ресурсов в условиях блокировки имеющимися средствами ИТВ. Такие условия функционирования вступают в противоречие с поэлементным автоматизированным управлением СС СН. В таких условиях никакая сервисная инженерная служба не сможет обеспечить требуемый уровень оперативности и эффективности управления. То есть такой подход противоречит современным требованиям к управлению, так как [31]:

- не отвечает требованиям управляемости, оперативности управления, мобильности и боевой готовности;
- требует содержания многочисленной сервисной инженерной службы;
- не отвечает критериям обеспечения информационной безопасности (так как возможен радиоэлектронный и информационный доступ противника к элементам контролируемой зоны СС СН);
- «размывает» функционал и зоны ответственности при предоставлении услуг связи специализированным абонентам (оператор СС СН должен осуществлять полное наблюдение и управление сетью, в то время как сегменты СС ОП в составе СС СН оказываются ограниченно наблюдаемыми и недоступными для управления).

Одним из путей решения задачи создания автоматической системы управления связью СС СН, предложенным в работе [31], является создание единой базы сетевых ресурсов СС СН и автоматической системы управления этими ресурсами. При этом подразумевается, что база сетевых ресурсов и система управления ими будет размещаться в доверенной зоне СС СН и частично реплицироваться в территориальные центры управления отдельных ТКС. Единая база сетевых ресурсов будет содержать агрегированную информацию обо всех сетевых элементах и их конфигурации, в том числе [31]:

- сетевые адреса и параметры;

- профили безопасности и межсетевых экранов (на основе политики безопасности как для уровня должностных лиц, так и для устройств и сетей);
- параметры протоколов обеспечения качества обслуживания, приоритетной обработки трафика и выделения полос пропускания;
- параметры протоколов маршрутизации и протоколов обеспечения функционирования виртуальных наложенных сетей;
- временные параметры и критерии блокировки и разблокировки пользователей, устройств и сетей;
- частоты и режимы работы радиосредств;
- документацию под соответствующую конфигурацию сети и др.

Создание такой базы сетевых ресурсов является одной из подзадач управления связью и осуществляется либо заранее, либо в режиме реального времени при наличии автоматической системы управления связью. Впоследствии каждый сетевой элемент СС СН получает только необходимую ему информацию. При таком централизованном подходе к управлению СС СН конфигурации всех сетевых элементов будут семантически согласованы и централизованно оттестированы на корректность введения тех или иных настроек во избежание конфликтных ситуаций и ошибок, связанных с человеческим фактором, целенаправленными действиями внутреннего нарушителя и др. [31].

Таким образом, задача разработки системы управления связью для СС СН является актуальной научной и технической задачей. При этом, принципы и технологии управления, используемые для СС ОП не приемлемы для управления СС СН ввиду того, что последние функционируют в условиях перманентных дестабилизирующих воздействий. Одним из вариантов решения задачи управления СС СН является создание единой базы сетевых ресурсов СС СН и автоматической системы управления этими ресурсами.

Выводы

СС СН – это сеть связи, функционирующая в интересах государственной и военной систем управления. В условиях перехода этих систем управления к сетевым принципам построения для СС СН становятся характерны следующие основные тенденции по ее технологическому построению:

- переход от иерархического принципа построения СС СН к децентрализованной сетевой структуре, которая в большей степени соответствует современным требованиям к системам государственного и военного управления, а также условиям ведения боевых действий, характеризующимся высокой динамикой развития и мобильностью ее участников;
- отказ от построения СС СН на основе отдельной связной инфраструктуры и переход к построению СС СН на основе гибридного подхода, когда отдельные сегменты СС ОП национальных и региональных операторов связи, а также сегменты глобальных сетей используются в качестве элементов транспортной инфраструктуры СС СН;

- отказ от использования в СС СН закрытых и специализированных протоколов связи и максимальное широкое использование для построения элементов СС СН коммерческих протоколов и технологий, применяемых в гражданской сфере связи и телекоммуникаций.

Использование в качестве сегментов СС СН арендуемых каналов и сетей СС ОП, а также массовое использование в СС СН коммерческих протоколов связи делает СС СН уязвимой к атакам средств РЭП и ИТВ. Эти атаки (особенно атаки ИТВ) могут проводиться на СС СН через сетевые сегменты общие с СС ОП, так как СС ОП, как правило, подключены к глобальной информационно-телекоммуникационной сети Интернет. При этом среди коммерческих сетевых протоколов, которые широко используются в СС СН, не отработаны механизмы защиты от воздействий ИТВ и РЭП, а также механизмы быстрого восстановления после сбоев.

Одним из актуальных направлений снижения негативных эффектов от внедрения в состав СС СН элементов СС ОП и массового использования в СС СН коммерческих протоколов связи может быть создание высокоэффективной централизованной автоматической системы управления сетевыми ресурсами СС СН. Наличие такой системы управления позволит предотвратить ряд негативных эффектов при функционировании СС СН в условиях воздействия перманентных дестабилизирующих факторов, за счет оперативного управления сетевыми ресурсами СС СН.

Литература

1. Барашков П. Н., Родимов А. П., Ткаченко К. А., Чуднов А. М. Модель системы связи с управляемыми структурами в конфликтных условиях. – Л.: ВАС, 1986. – 52 с.
2. Лялюк И. Н. С4I: системы связи, АСУ и разведки вооруженных сил США. – М.: ВАТУ, 2000.
3. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.
4. Будко П. А., Рисман О. В. Многоуровневый синтез информационно-телекоммуникационных систем. Математические модели и методы оптимизации: Монография. – СПб.: ВАС, 2011. – 476 с.
5. Будко П. А., Чихачев А. В., Баринов М. А., Винограденко А. М. Принципы организации и планирования сильносвязной телекоммуникационной среды сил специального назначения // Т-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 6. С. 8-12.
6. Линец Г. И. Системные аспекты теории синтеза и практика построения телекоммуникационных сетей. – Ставрополь: Альфа-Принт, 2010. – 460 с.
7. Линец Г. И. Методы структурно-параметрического синтеза, идентификации и управления транспортными телекоммуникационными сетями для достижения максимальной производительности: Автореф. дис. ... д-ра техн. наук. Ставрополь: Северо-Кавказский федеральный университет, 2013. – 34 с.
8. Назаров А. Н., Сычев К. И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых

параметров сетей связи следующего поколения. – Красноярск: Изд-во ООО «Поликом», 2010. – 389 с.

9. Давыдов А. Е., Хейстонен Д. П. Построение модели системы управления телекоммуникационной сетью специального назначения // Вопросы радиоэлектроники. 2012. Т. 3. № 2. С. 124-130.

10. Давыдов А. Е. Концептуальные подходы к построению адаптивных мультисервисных сетей специального назначения // НИИ Масштаб [Электронный ресурс]. 10.12.2012. – URL: http://mashtab.org/company/massmedia/articles/konceptualnye_podhody_k_postroeniyu_adaptivnyh_multiservisnyh_setej_specialnogo_naznacheniya/ (дата обращения 08.06.2017).

11. Сухотеплый А. П., Давыдов А. Е., Савицкий О. К., Лукьянчик В. Н. К вопросу создания стационарной компоненты наземного эшелона ОАЦСС ВС РФ на территории РФ и сопредельных государств в условиях сетецентрических войн // НИИ Масштаб [Электронный ресурс]. 10.12.2012. – URL: http://mashtab.org/company/massmedia/articles/k_voprosu_sozdaniya_stacionarnoj_komponenty_nazemnogo_eshelona_oacss_vs_rf_na_territorii_rf_i_sopredelnyh_gosudarstv_v_usloviyah/ (дата обращения 08.06.2017).

12. Лебедев С. Ф., Сызранцев Г. В., Добровольский В. С., Лукин К. И., Даниленко А. Н. Базовые положения методики формирования (построения) рационального варианта автоматической полевой сети связи общего пользования специального назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2012. № 1-2. С. 79-84.

13. Сызранцев Г. В., Лукин К. И., Иншин Г. В., Даниленко А. Н. Модель функционирования автоматической сети связи общего пользования полевой системы связи специального назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2012. № 1-2. С. 85-93.

14. Сызранцев Г. В., Лукин К. И., Иншин Г. В., Шмелев А. А., Неверов А. П. Модель функционирования автоматической первичной сети связи высокودинамичной системы связи специального назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2012. № 11-12. С. 65-69.

15. Сызранцев Г. В., Лукин К. И., Иншин Г. В., Лебедев С. Ф. Автоматическая первичная сеть связи на телекоммуникационном оборудовании технологий NGPDH и NGSDH // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2013. № 3-4. С. 63-69.

16. Легков К. Е. Многоуровневые модели инфокоммуникационных сетей специального назначения // Т-Comm: Телекоммуникации и транспорт. 2015. Том 9. № 12. С. 32-36.

17. Легков К. Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения // Т-Comm: Телекоммуникации и транспорт. 2015. Том 9. № 8. С. 14-20.

18. Легков К. Е., Мясникова А. И. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Научные технологии в космических исследованиях Земли. 2012. № 3. С. 20-22.
19. Легков К. Е., Емельянов А. В. Концепция управления сетями в модели взаимодействия открытых систем // Труды Ростовского государственного университета путей сообщения. 2015. № 3. С. 83-92.
20. Буренин А. Н., Легков К. Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Научные технологии в космических исследованиях Земли. 2013. № 3. С. 12-17.
21. Буренин А. Н., Легков К. Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения управления. – М.: Медиа паблишер, 2015. – 348 с.
22. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. – СПб.: Изд-во Политехн. ун-та, 2009. – 400 с.
23. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.
24. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.
25. Шнепс-Шнеппе М.А. «Красный телефон» на DISN сети как родимое пятно в среде AS-SIP // International Journal of Open Information Technologies. 2015. Т. 3. № 6. С. 7-12.
26. Шнепс-Шнеппе М. А., Намиот Д. Е. Об эволюции телекоммуникационных сервисов на примере GIG // International Journal of Open Information Technologies. 2015. Т. 3. № 1. С. 1-13.
27. Шнепс-Шнеппе М. А. От IN к IMS. О сетях связи военного назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 1. С. 1-11.
28. Шнепс-Шнеппе М. А., Намиот Д. Е., Цикунов Ю. В. Телекоммуникации для военных нужд: сеть GIG-3 по требованиям кибервойны // International Journal of Open Information Technologies. 2014. Т. 2. № 10. С. 3-13.
29. Соколов Н. А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. Т. 2. № 9. С. 4-8.
30. Нетес В. А. Надежность сетей связи в период перехода к NGN // Вестник связи. 2007. № 9. С. 1-8.
31. Давыдов А. Е. Концептуальные подходы к построению автоматизированной системы управления связью адаптивных мультисервисных сетей специального назначения // НИИ Масштаб [Электронный ресурс]. 12.11.2012. – URL: http://mashtab.org/company/massmedia/articles/conceptual_approaches_to_construct

ing_an_automated_control_system_for_adaptive_multi-service_special-purpose_networks/ (дата обращения 08.06.2017).

32. О связи. Федеральный закон РФ от 07.07.2003 № 126-ФЗ // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

33. Макаренко С. И., Федосеев В. Е. Системы многоканальной связи. Вторичные сети и сети абонентского доступа: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2014. – 179 с.

34. Макаренко С. И. Вычислительные системы, сети и телекоммуникации: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2008. – 352 с.

35. Новые информационные и сетевые технологии в системах управления военного назначения. Учебник. Часть 1. Новые сетевые технологии в системах управления военного назначения / Под ред. С.М. Одоевского. – СПб.: ВАС, 2010. – 432 с.

36. Коробицин А. А., Кудрявцев А. М., Смирнов А. А. Информационные и сетевые технологии в автоматизированных системах специального назначения: Учебное пособие. – СПб.: ВАС, 2015. – 132 с.

37. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. Национальный стандарт РФ. – М., 2007.

38. Макаренко С. И. Использование космического пространства в военных целях: современное состояние и перспективы развития систем информационно-космического обеспечения и средств вооружения // Системы управления, связи и безопасности. 2016. № 4. С. 161-213. – URL: <http://sccs.intelgr.com/archive/2016-04/09-Makarenko.pdf> (дата обращения 07.06.2017).

39. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. – М., 2006.

40. ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. – М., 2009.

41. Попков В. К., Блукке В. П., Дворкин А. Б. Модели анализа устойчивости и живучести информационных сетей // Проблемы информатики. 2009. № 4. С. 63-78.

42. Макаренко С. И., Чаленко Н. Н., Крылов А. Г. Сети следующего поколения NGN // Системы управления, связи и безопасности. 2016. № 1. С. 81-102. – URL: <http://sccs.intelgr.com/archive/2016-01/05-Makarenko.pdf> (дата обращения 07.06.2017).

43. Кархов А. SDH не умрет, но уже никогда не будет приоритетом. Интервью с директором по перспективному развитию сети Comstar United Telesystems // Connect! Мир связи. 2006. № 6. – URL: <http://www.connect.ru/article.asp?id=4943> (дата обращения 09.06.2017).

44. Гольдштейн Б. С. 10 лет эволюции коммутационной техники // Вестник связи. 2007. № 5. С. 1-6.

45. Norros I. A broad approach to the dependability of IP networks // European CUP Newsletter. 2006. Vol. 2. № 3.
46. Next Generation Networks Task Force Report // The President's National Security Telecommunications Advisory Committee. 2006.
47. ITU-T Recommendation G.1000 (11/2001). Communications Quality of Service: A framework and definitions. 2001.
48. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
49. Duffy J. Cisco routers caused major outage in Japan: report // Network World. 16.05.2007.
50. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. – СПб.: Наука и техника, 2004. – 336 с.
51. Информационные технологии, связь и защита информации в МВД России - 2012 / По ред. М.Л. Тюркина, М.И. Шадаева, А.С. Аджемова, И.П. Иванова, С.В. Дворянкина, А.В. Куц, А.В. Квитко, П.А. Важева, Ю.А. Быстрова. – М.: ООО «Компания «Информационный мост», 2013. 156 с. – URL: www.informost.ru (дата обращения 03.02.2015).
52. Связь в Вооруженных силах Российской Федерации – 2013: тематический сборник. / По ред. А.В. Абрамовича, А.В. Герасимова, С.В. Цибина, К.С. Ометова, Ю.А. Быстрова. М.: ООО «Компания «Информационный мост», 2013. 216 с. URL: www.informost.ru (дата обращения 03.02.2015).
53. Оружие и технологии России. Энциклопедия. XXI век. Системы управления, связи и радиоэлектронной борьбы / Под общ. ред. С. Иванова. – М.: Изд. дом «Оружие и технологии», 2006. – 695 с.
54. Шептура В. Н. Архитектура перспективной системы связи группировки войск (сил) для обеспечения управления адаптивными действиями войск (сил) [Доклад] // Мат. Всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4 «Телекоммуникации и связь в информационно-управляющих системах». Под ред. Ю.В. Бородакия. – М.: ОАО «Концерн «Системпром», 2013. – С. 16-20.
55. Макаренко С. И., Афанасьев О. В., Баранов И. А., Самофалов Д. В. Экспериментальные исследования реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Журнал радиоэлектроники. 2016. № 4. – URL: <http://jre.cplire.ru/jre/apr16/4/text.pdf> (дата обращения 09.06.2017).
56. Паршин С., Кожанов Ю. Современные тенденции в совершенствовании системы управления вооруженными силами ведущих зарубежных стран в информационную эпоху // Зарубежное военное обозрение. 2009. № 7. С. 3-9.

57. Янов О., Ширяев В. Участие Министерства обороны США в федеральной программе создания «Среды совместного использования информации» // Зарубежное военное обозрение. 2011. № 12. С. 15-21.

58. Гаврилов А. Автоматизированная система сбора, обработки и распределения разведывательной информации СВ США DCGS-A // Зарубежное военное обозрение. 2010. № 7. С. 32-40.

59. Военная сеть США будет построена на маршрутизаторах Juniper Networks // Poplar Systems [Электронный ресурс]. 13.01.2004. – URL: <http://www.poplar.ru/view.php3?cls=news&vguid=1256&guid=1256&parent=1255> (дата обращения 13.06.2015).

60. Кобозев Ю. Н. Перспективы развития систем связи и телекоммуникаций в информационно-управляющих системах специального назначения [Доклад] // Мат. Всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». Том 4 «Телекоммуникации и связь в информационно-управляющих системах». Под ред. Ю.В. Бородакия. М.: ОАО «Концерн «Созвездие», 2013. С. 7-9.

References

1. Barashkov P. N., Rodimov A. P., Tkachenko K. A., Chudnov A. M. *Model' sistemy sviazi s upravliaemyimi strukturami v konfliktnykh usloviakh* [Model of communication system with controlled structures in conflict settings]. Leningrad, Military Communications Academy, 1986. 52 p. (in Russian).

2. Lialiuk I. N. *C4I: sistemy sviazi, ASU i razvedki vooruzhennykh sil SShA* [C4I: communications systems, automation and intelligence of the armed forces of the United States.]. Moscow, Military aviation technical University, 2000. (in Russian).

3. Bogovik A. V., Ignatov V. V. *Effektivnost' sistem voennoi sviazi i metody ee otsenki* [The effectiveness of military communications systems and assessment methods]. Saint-Petersburg, Military Communications Academy, 2006. 183 p. (in Russian).

4. Budko P. A., Risman O. V. *Mnogourovnevij sintez informacionno-telekommunikacionnykh sistem. Matematicheskie modeli i metody optimizatsii* [Multi-Level Synthesis of Information Telecommunication Systems. Mathematical Models and Methods of Optimization. Treatise]. Saint-Petersburg, Military Academy of the Signal Corps Publ., 2011. 476 p. (in Russian).

5. Budko P. A., Chikhachev A. V., Barinov M. A., Vinogradenko A. M. Principles of the organization and planning of strongly connected telecommunication environment of forces of a special purpose. *T-Comm*, 2013, vol. 7, no. 6, pp. 8-12 (in Russian).

6. Linets G. I. *Sistemnye aspekty teorii sinteza i praktika postroeniia telekommunikatsionnykh setei* [System aspects of the theory of fusion and practice the design of telecommunication networks]. Stavropol, Alfa-Print Publ., 2010. 460 p. (in Russian).

7. Linec G. I. *Metody strukturno-parametricheskogo sinteza, identifikacii i upravlenija transportnymi telekommunikacionnymi setjain dlja dostizhenija maksimal'noj proizvoditel'nosti*. Diss. dokt. tehn. nauk [The Methods of Structural Parametric Synthesis, Identification and Control of Transport Telecommunication Networks for Achievement of the Maximum Productivity. Extended Abstract of Dr. habil. Thesis]. Stavropol, Northern-Caucasus State University, 2013. 34 p. (In Russian).

8. Nazarov A. N., Sychev K. I. *Modeli i metody rascheta pokazatelej kachestva funkcionirovaniya uzlovogo oborudovaniya i strukturno-setevyh parametrov setej svjazi sledujushhego pokoleniya* [The Models and the Methods of Measuring of Quality Indicators of Nodal Equipment Functioning and Network Structural Parameters of Next Generation Networks]. Krosnoyarsk, Polykom Publ., 2010. 389 p. (In Russian).

9. Davydov A. E., Heystonen D. P. Building the model for controls of a special-purpose telecommunication network. *Questions of radio-electronics*, 2012, vol. 3, no. 2, pp. 124-130.

10. Davydov A. E. Conceptual approaches to constructing adaptive multi-service special-purpose networks. *Research Institute 'Masshtab'*. 10.12.2012. Available at: http://mashtab.org/company/massmedia/articles/konceptualnye_podhody_k_postroeniyu_adaptivnyh_multiservisnyh_setej_specialnogo_naznacheniya/ (accessed 8 June 2017) (in Russian).

11. Suhoteply A. P., Davydov A. E., Savicky O. K., Luk'yanchik V. N. Fixed component of ground echelon of the integrated automatic digital communications network of the armed forces of the Russia and neighbouring states under the conditions of network-centric wars. *Research Institute 'Masshtab'*. 10.12.2012. Available at: http://mashtab.org/company/massmedia/articles/k_voprosu_sozdaniya_stacionarnoj_komponenty_nazemnogo_eshelona_oacss_vs_rf_na_territorii_rf_i_sopredelnyh_gosu_darstv_v_usloviyah/ (accessed 8 June 2017) (in Russian).

12. Lebedev S. F., Syzrantsev G. V., Dobrovol'skii V. S., Lukin K. I., Danilenko A. N. Bazovye polozheniia metodiki formirovaniia (postroeniia) ratsional'nogo varianta avtomaticheskoi polevoi seti sviazi obshchego pol'zovaniia spetsial'nogo naznacheniiia [The basic provisions of a technique of forming (constructing) a reasonable option for automatic field communications network for General use special purpose]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2012, no. 1-2, pp. 79-84 (in Russian).

13. Syzrantsev G. V., Lukin K. I., Inshin G. V., Danilenko A. N. Model funktsionirovaniia avtomaticheskoi seti sviazi obshchego pol'zovaniia polevoi sistemy sviazi spetsial'nogo naznacheniiia [The model of functioning of the automated communication network of General use field communication systems of special purpose]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2012, no. 1-2, pp. 85-93 (in Russian).

14. Syzrantsev G. V., Lukin K. I., Inshin G. V., Shmelev A. A., Neverov A. P. Model funktsionirovaniia avtomaticheskoi pervichnoi seti sviazi vysokodinamichnoi

sistemy svyazi spetsial'nogo naznacheniiia [The model of functioning of the automated primary communications network with highly dynamic communication systems of special purpose]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2012, no. 11-12, pp. 65-69 (in Russian).

15. Sizranchev G., Lukin K., Inshin G., Lebedev S. Automatic primary communication net on telecommunication equipment NGPDH NGSDH technology. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2013, no. 3-4, pp. 63-69 (in Russian).

16. Legkov K. E. A layered model of the special puprose infocommunication networks. *T-Comm*, 2015, vol. 9, no.12, pp. 32-36 (in Russian).

17. Legkov K. E. Organization and models of functioning modern infocommunication networks of a special purpose. *T-Comm*, 2015, vol. 9, no. 8, pp. 14-20 (in Russian).

18. Legkov K. E., Myasnikova A. I. Control of the infocom-munication services on special purpose multiservice networks. *High tech in Earth space research*, 2012, no. 3, pp. 20-22 (in Russian).

19. Legkov K. E., Emelianov A. V. Kontseptsiiia upravleniia setiami v modeli vzaimodeistviia otkrytykh sistem [The concept of governance networks in the model of open systems interconnection]. *Trudy Rostovskogo gosudarstvennogo universiteta putei soobshcheniia*, 2015, no. 3, pp. 83-92 (in Russian).

20. Burenin A. N. Legkov K. E. Features of architecture, functioning, monitoring and control of field components of the modern infocommunication networks of the special purpose. *High tech in Earth space research*, 2013, no. 3, pp. 12-17 (in Russian).

21. Burenin A. N., Legkov K. E. *Sovremennnye infokommunikatsionnye sistemy i seti spetsial'nogo naznacheniiia. Osnovy postroeniia upravleniia* [Modern infocommunication systems and networks for special purposes. Fundamentals of management]. Moscow, Media Publisher, 2015. 348 p. (in Russian).

22. Isakov E. E. *Ustoichivost' voennoi svyazi v usloviakh informatsionnogo protivoborstva* [The stability of military communications in the conditions of information warfare]. Saint-Petersburg, Peter the Great St.Petersburg Polytechnic University, 2009. 400 p. (in Russian).

23. Mikhailov R. L. *Pomekhozashchishchennost' transportnykh setei svyazi spetsial'nogo naznacheniiia. Monografiia* [Noise immunity of transport networks for special purposes. Monograph]. Cherepovets, The Cherepovets higher military engineering school of radio electronics, 2016. 128 p. (in Russian).

24. Antonovich P. I., Makarenko S. I., Mihaylov R. L., Ushanev K. V. New means of destructive effects on network centric military command, control and communication systems in the information space. *Vestnik Akademii voennykh nauk*. 2014, vol. 48, no. 3, pp. 93-101 (in Russian).

25. Shneps-Shneppe M. A. «Krasnyi telefon» na DISN seti kak rodimoe piatno v srede AS-SIP [The "red phone" on DISN network as a birthmark in the environment AS-SIP]. *International Journal of Open Information Technologies*, 2015, vol. 3, no. 6, pp. 7-12 (in Russian).

26. Shneps-Shneppe M. A., Namiot D. E. Ob evoliutsii telekommunikatsionnykh servisov na primere GIG [The evolution of telecommunication services on an example GIG]. *International Journal of Open Information Technologies*, 2015, vol. 3, no. 1, pp. 1-13 (in Russian).
27. Shneps-Shneppe M. A. Ot IN k IMS. O setiakh svyazi voennogo naznacheniiia [About communication networks for military purposes]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 1, pp. 1-11 (in Russian).
28. Shneps-Shneppe M. A., Namiot D. E., Tsikunov Iu. V. Telekommunikatsii dlia voennykh nuzhd: set' GIG-3 po trebovaniyam kibervoiny [Telecommunications for military purposes: the network is GIG-3 according to the requirements of cyberwar]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 10, pp. 3-13 (in Russian).
29. Sokolov N. A. Sistemnye aspekty postroeniia i razvitiia setei elektrosvyazi spetsial'nogo naznacheniiia [The system aspects of the construction and development of telecommunication networks of special purpose]. *International Journal of Open Information Technologies*, 2014, vol. 2, no. 9, pp. 4-8 (in Russian).
30. Netes V. A. Nadezhnost' setei svyazi v period perekhoda k NGN [Reliability of communication networks in the period of transition to NGN]. *Vestnik svyazi*, 2007, no. 9, pp. 1-8 (in Russian).
31. Davydov A. E. Conceptual approaches to constructing an automated control system for adaptive multi-service special-purpose networks. *Research Institute 'Masshtab'*. 12.11.2012. Available at: http://mashtab.org/company/massmedia/articles/conceptual_approaches_to_constructing_an_automated_control_system_for_adaptive_multi-service_special-purpose_networks/ (accessed 8 June 2017) (in Russian).
32. O svyazi [About the connection]. Federal law of Russia. 2003. (in Russian).
33. Makarenko S. I., Fedoseev V. E. *Multichannel communication systems. Secondary networks and subscriber access networks*. Saint-Petersburg, Mozhaisky Military Space Academy Publ., 2014, 179 p. (in Russian).
34. Makarenko S. I. *Computer systems, networks and telecommunication*. Stavropol, Sholokhov Moscow State University for the Humanities (Stavropol Branch) Publ., 2008, 352 p. (in Russian).
35. Odoevskiy S. M. *Novye informatsionnye i setevye tekhnologii v sistemakh upravleniia voennogo naznacheniiia. Chast 1. Novye setevye tekhnologii v sistemakh upravleniia voennogo naznacheniiia* [New information and network technologies in control systems for military use. Part 1. New networking technologies in control systems for military use]. Saint-Petersburg, Military Academy of the Signal Corps Publ., 2010. 432 p. (in Russian).
36. Korobitsin A. A., Kudriavtsev A. M., Smirnov A. A. *Informatsionnye i setevye tekhnologii v avtomatizirovannykh sistemakh spetsial'nogo naznacheniiia* [Information and network technology in automated systems special purpose]. Saint-Petersburg, Military Academy of the Signal Corps Publ., 2015. 132 p. (in Russian).
37. ISO/IEC 17799-2000. Information technology. Code of practice for security management. 2000.

38. Makarenko S. I. Information-Space Systems and Space Weapons – Current State and Prospects of Improvement. *Systems of Control, Communication and Security*, 2016, no. 4, pp. 161-213. Available at: <http://sccs.intelgr.com/archive/2016-04/09-Makarenko.pdf> (accessed 7 June 2017) (in Russian).

39. Recommendations for standardization R 50.1.053-2005. Information technologies. Basic terms and definitions in scope of technical protection of information. Moscow, 2006.

40. GOST R 53111-2008. Stability of functioning of the public communications network. Requirements and check methods. Moscow, 2009. (in Russian).

41. Popkov V. K., Blukke V. P., Dvorkin A. B. Modeli analiza ustoichivosti i zhivuchesti informatsionnykh setei [Model analysis the sustainability and survivability of information networks]. *Problems of informatics*, 2009, no. 4, pp. 63-78 (in Russian).

42. Makarenko S. I., Chalenko N. N., Krylov A. G. Next Generation Networks. *Systems of Control, Communication and Security*, 2016, no. 1, pp. 81-102. Available at: <http://sccs.intelgr.com/archive/2016-01/05-Makarenko.pdf> (accessed 7 June 2017) (in Russian).

43. Karkhov A. SDH ne umret, no uzhe nikogda ne budet prioritom [SDH will not die, but will never be a priority]. *Connect!* 2006, no. 6. Available at: <http://www.connect.ru/article.asp?id=4943> (accessed 9 June 2017) (in Russian).

44. Goldshtein B. S. 10 let evoliutsii kommutatsionnoi tekhniki [10 years of evolution of the switching technology]. *Vestnik sviazi*, 2007, no. 5, pp. 1-6 (in Russian).

45. Norros I. A broad approach to the dependability of IP networks. *European CUP Newsletter*, 2006, vol. 2, no 3.

46. *Next Generation Networks Task Force Report*. The President's National Security Telecommunications Advisory Committee. 2006.

47. ITU-T Recommendation G.1000 (11/2001). Communications Quality of Service: A framework and definitions.

48. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii [About information, information technologies and protection of information]. Federal law of Russia. 2006. (in Russian).

49. Duffy J. Cisco routers caused major outage in Japan: report. *Network World*. 16.05.2007.

50. Kucheryavii E. A. *Upravlenie trafikom i kachestvo obsluzhivaniya v seti Internet* [Traffic Management and the Quality of Service on the Internet]. Saint-Petersburg, Science and Technology Publ., 2004. 336 p. (in Russian).

51. Tiurkin M. L., Shadaev M. I., Adzhemov A. S., Ivanov I. P., Dvoriankin S. V., Kuts A. V., Kvitko A. V., Vazhev P. A., Bystrov Iu. A. *Informatsionnye tekhnologii, svyaz' i zashchita informatsii v MVD Rossii* [Information Technology, Communication and Information Protection in the Ministry of Internal Affairs of Russia]. Moscow, "Company "Information Bridge", 2013, 156 p. Available at: www.informost.ru (accessed 03 February 2015) (in Russian).

52. Abramovich A. V., Gerasimov A. V., Tsibin S. V., Ometov K. S., Bystrov Iu. A. *Sviaz' v Vooruzhennykh silakh Rossiiskoi Federatsii - 2013: tematicheskii sbornik* [Communication in the Armed Forces of the Russian Federation - 2013: Thematic Collection]. Moscow, "Company "Information Bridge" Publ., 2013, 216 p. Available at: www.informost.ru (accessed 03 February 2015) (in Russian).

53. Ivanov S. *Oruzhie i tekhnologii Rossii. Entsiklopediia. XXI vek. Sistemy upravleniia, sviazi i radioelektronnoi bor'by* [Weapons and Technology of Russia. The Encyclopedia. XXI Century. Control Systems, Communications and Electronic Warfare]. Moscow, "Weapons and Technology" Publ., 2006, 695 p. (in Russian).

54. Sheptura V. N. *Arkhitektura perspektivnoi sistemy sviazi gruppirovki voisk (sil) dlia obespecheniia upravleniia adaptivnymi deistviiami voisk (sil)* [Architecture of Advanced Communication Systems Forces to Ensure Adaptive Management Actions of the Troops]. *Vserossiiskaia nauchnaia konferentsiia «Sovremennye tendentsii razvitiia teorii i praktiki upravleniia v sistemakh spetsial'nogo naznacheniiia»* [Proceedings of All-Russian Scientific Conference "Modern Trends in the Theory and Practice of Control Systems for Special Purposes"], vol. 4, Moscow, JSC "Concern "Sistemprom", 2013, pp. 16-20 (in Russian).

55. Makarenko S. I., Afanasev O. V., Baranov I. A., Samofalov D. V. Experimental analysis of the network reaction and the routing effects under conditions of noise-to-signal ratio dynamic changes. *Journal of radio electronics*, 2016, no. 4. Available at: <http://jre.cplire.ru/jre/apr16/4/text.pdf> (accessed 9 June 2017) (in Russian).

56. Parshin S., Kozhanov Iu. *Sovremennye tendentsii v sovershenstvovanii sistemy upravleniia vooruzhennymi silami vedushchikh zarubezhnykh stran v informatsionnoi epokhu* [Modern trends in improving the system of management of the armed forces of the leading countries in the information age]. *Zarubezhnoe voennoe obozrenie*, 2009, no. 7, pp. 3-9 (in Russian).

57. Janov O., Shiriaev V. *Uchastie Ministerstva oborony SShA v federal'noi programme sozdaniia 'Sredy sovместного испол'zovaniia informatsii'* [The participation of the Ministry of defense in the Federal program of creating an "Environment of information sharing"]. *Zarubezhnoe voennoe obozrenie*, 2011, no. 12, pp. 15-21 (in Russian).

58. Gavrilov A. *Avtomatizirovannaia sistema sbora, obrabotki i raspredeleniia razvedyvatel'noi informatsii SV SShA DCGS-A* [Automated system of collection, processing and distribution of intelligence information, US army DCGS-A]. *Zarubezhnoe voennoe obozrenie*, 2010, no. 7, pp. 32-40 (in Russian).

59. *Voennaia set' SShA budet postroena na marshrutizatorakh Juniper Networks* [Military network, the US will be built on Juniper Networks routers]. *Poplar Systems*. 13.01.2004. Available at: <http://www.poplar.ru/view.php3?cls=news&vguid=1256&guid=1256&parent=1255> (accessed 13 June 2015) (in Russian).

60. Kobozev Iu. N. *Perspektivy razvitiia sistem sviazi i telekommunikatsii v informatsionno-upravliaiushchikh sistemakh spetsial'nogo naznacheniiia* [Prospects for the Development of Communication and Telecommunication Systems in

Management Information Systems, Special Purpose]. *Vserossiiskaia nauchnaia konferentsiia «Sovremennye tendentsii razvitiia teorii i praktiki upravleniia v sistemakh spetsial'nogo naznacheniia»* [Proceedings of All-Russian Scientific Conference "Telecommunications and Communication in Management Information Systems], vol. 4, Moscow, JSC "Concern "Sozvezdie", 2013, pp. 7-9 (in Russian).

Статья поступила 15 июня 2017 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей и систем связи к преднамеренным деструктивным воздействиям; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197198, г. Санкт-Петербург, ул. Ждановская д. 13.

Prospects and Problems of Development of Communication Networks of Special Purpose

S. I. Makarenko

Relevance. The leading countries develop communication networks of a special purpose (CNSP) operating for the government, the Ministry of defence, Agency of security etc. Main trends in the development of CNSP are the use of resources of civil networks, as well as the use of commercial communication protocols. New network technologies of civil networks (NGN concept, packet transmission technology etc.) are introduced in CNSP. Consequently, it is important to analyze the current state of CNSP, as well as trends and problems of development their. **The aim of this paper** is to analyze the technologies and principles of CNSP, as well as the prospects and problems of their development. The analysis is based only open sources. DISN and GIG networks are used as examples of CNSP. **Results and their novelty.** Elements of novelty of the paper are main trends and problems of building of CNSP. The analysis showed that modern CNSP moving to a decentralized network structure that is more in line with modern requirements to systems of state and military administration. Also, modern CNSP move to a hybrid structure where the individual segments of civil networks are used as parts of the transport infrastructure of CNSP. Commercial protocols and technologies widely used in CNSP instead specialized communication protocols too. This trends make the modern CNSP more vulnerable. **Practical significance.** The presented analysis is useful for technical professionals in the justification of new technological solutions in the field of CNSP. In addition, this analysis will be useful for researchers to justify as improvements CNSP and protection it.

Key words: communication system, network communication, communication networks of a special purpose, civil network, network protocols, military communications system, sustainability communications, electronic warfare, information technology, NGN, control communication system.

Information about Author

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. Mozhaisky Military Space Academy. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197198, Saint Petersburg, Zhdanovskaya ulica, 13.