

УДК 621.39

Описательная модель сети 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, в части используемых в них технологий. **Целью работы** является разработка описательной модели СС СН на основе качественного анализа технологий и принципов построения СС СН. Для анализа были использованы только открытые источники. **Результаты и их новизна.** Элементом новизны работы являются выявленные общие технологические особенности построения 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 максимально широкое использование в СС СН коммерческих протоколов и технологий из гражданской сферы связи и телекоммуникаций. **Практическая значимость.** Представленная в работе описательная модель будет полезна техническим специалистам для обоснования новых технологических решений в области СС СН. Кроме того, данная модель будет полезна 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.

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 ГИ (Global Information Infrastructure), создает предпосылки для коренного изменения архитек-

Библиографическая ссылка на статью:

Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. URL: <http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf>

Reference for citation:

Makarenko S. I. Descriptive Model of a Special Purpose Communication Network. *Systems of Control, Communication and Security*, 2017, no. 2, pp. 113-164. Available at: <http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf> (in Russian).

туры и принципов построения сетей специального назначения. Так, концепция NGN связана с конвергенцией сетей связи и расширением диапазона предоставляемых связных услуг, а концепция GII – 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, 47], 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, 64], А.Н. Буренина [20, 21, 64], Е.Е. Исакова [22], Р.Л. Михайлова [23, 24], М.А. Шнепс-Шнеппе [25-28, 38], Н.А. Соколова [29, 49, 50, 55], Б.С. Гольдштейна [49, 50, 55], а также других ученых. При этом критический анализ проблемных вопросов, связанных с переходом СС СН на новые информационные технологии представлен в работах М.А. Шнепс-Шнеппе [25-28], Н.А. Соколова [29], В.А. Нетеса [30], а также в предыдущей работе автора [63].

Вместе с тем в данных работах не в полной мере раскрыты эволюционные процессы развития современных СС СН, не сформулирована четкая описательная модель используемых в СС СН современных протоколов и технологических решений. Решению этих задач 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, требования.
 - 2.1. Характеристика сети связи специального назначения как организационно-технической системы.
 - 2.2. Состав и структура сети связи специального назначения.
 - 2.3. Основные требования, предъявляемые к сети связи специального назначения.
3. Основные тенденции развития современных сетей связи специального назначения.
 - 3.1. Многоэшелонированное построение современных сетей связи специального назначения.

- 3.2. Широкое использование в составе сети связи специального назначения арендуемых сетевых ресурсов коммерческих операторов связи.
- 3.3. Массовое использование в современных сетях связи специального назначения технологий коммутации пакетов и коммерческих протоколов связи.
- 3.4. Построение сетей связи специального назначения в соответствии с концепцией NGN.
- 3.5. Переход от сетей связи специального назначения к инфокоммуникационным сетям специального назначения.
4. Описательная модель сети связи специального назначения – основные протоколы и технологии.
 - 4.1. Базовые протоколы технологии IP.
 - 4.2. Маршрутные протоколы.
 - 4.3. Протоколы групповой рассылки.
 - 4.4. Протоколы повышения надежности маршрутизации и доставки пакетов.
 - 4.5. Протоколы и механизмы поддержки качества обслуживания.
 - 4.6. Протоколы безопасности.
 - 4.7. Межсистемные протоколы и интерфейсы.

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, прежде всего, 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, требования

2.1. Характеристика сети связи специального назначения как организационно-технической системы

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

Анализ особенностей построения и функционирования СС СН был проведен в работах А.В. Боговика, В.В. Игнатова [3], К.Е. Легкова, А.Н. Буренина [20, 21], А.Н. Соколова [29], С.М. Одоевского [35], М.А. Шнепс-Шнеппе [38]. В данном подразделе будут обобщены принципы построения СС СН и основные их особенности относительно СС ОП.

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].

Согласно общей классификации систем СС СН может быть отнесена к типу ненаправленных управляемых человеко-машинных систем и, как правило, имеет иерархическую структуру, соответствующую структуре системы управления, в интересах которой она функционирует [3].

Одним из основополагающих принципов исследования сложных организационно-технических систем является принцип декомпозиции, при котором исследуемая система разбивается на ряд более простых составляющих, преследующих локальные цели. При этом успешность решения общей задачи исследования в существенной мере зависит от того, насколько удачно были выбраны признаки, по которым осуществлена декомпозиция. При решении задач информационного обеспечения органов государственного и военного управления, органов обеспечения безопасности и правопорядка для СС СН такими признаками могут быть [3]:

- тип транспортных средств или протоколов, используемых для доставки информации;
- виды обеспечиваемого для абонентов сервиса и услуг связи;
- типы абонентов;
- способы предоставления абонентов сервиса и услуг связи.

Примерная декомпозиция СС СН по некоторым из указанных признаков приведена на рис. 1.

При этом основу современных СС СН как управляемых целенаправленных систем, независимо от их типа и принадлежности, составляют отдельные сети связи (телекоммуникационные системы) и системы управления связью.

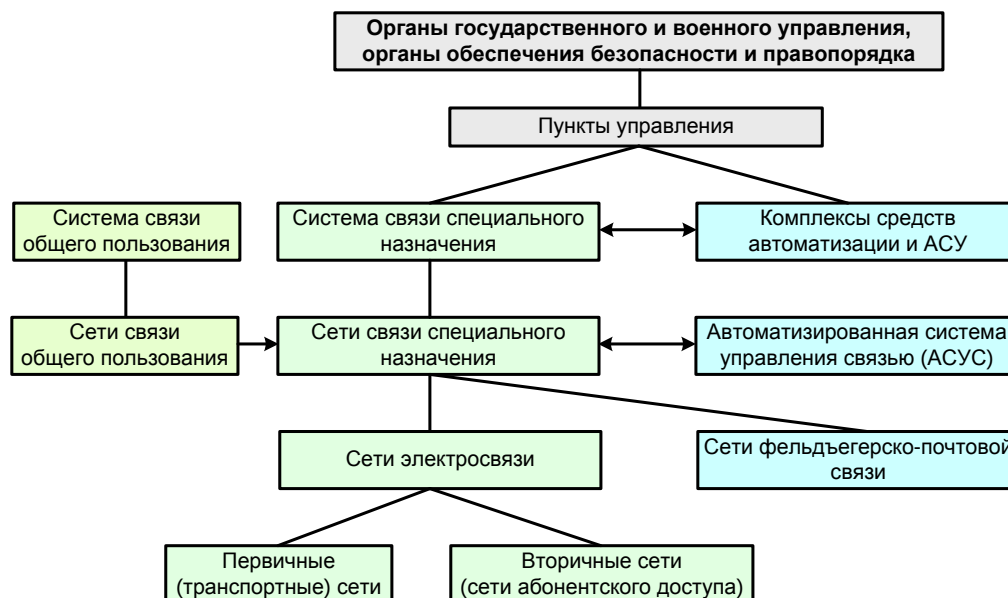


Рис. 1. Вариант декомпозиции СС СН [3]

2.2. Состав и структура сети связи специального назначения

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. При этом под *родом связи* понимается классификационная группировка связи, выделенная по среде распространения сигналов или по применяемым средствам связи.

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. 2.

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.

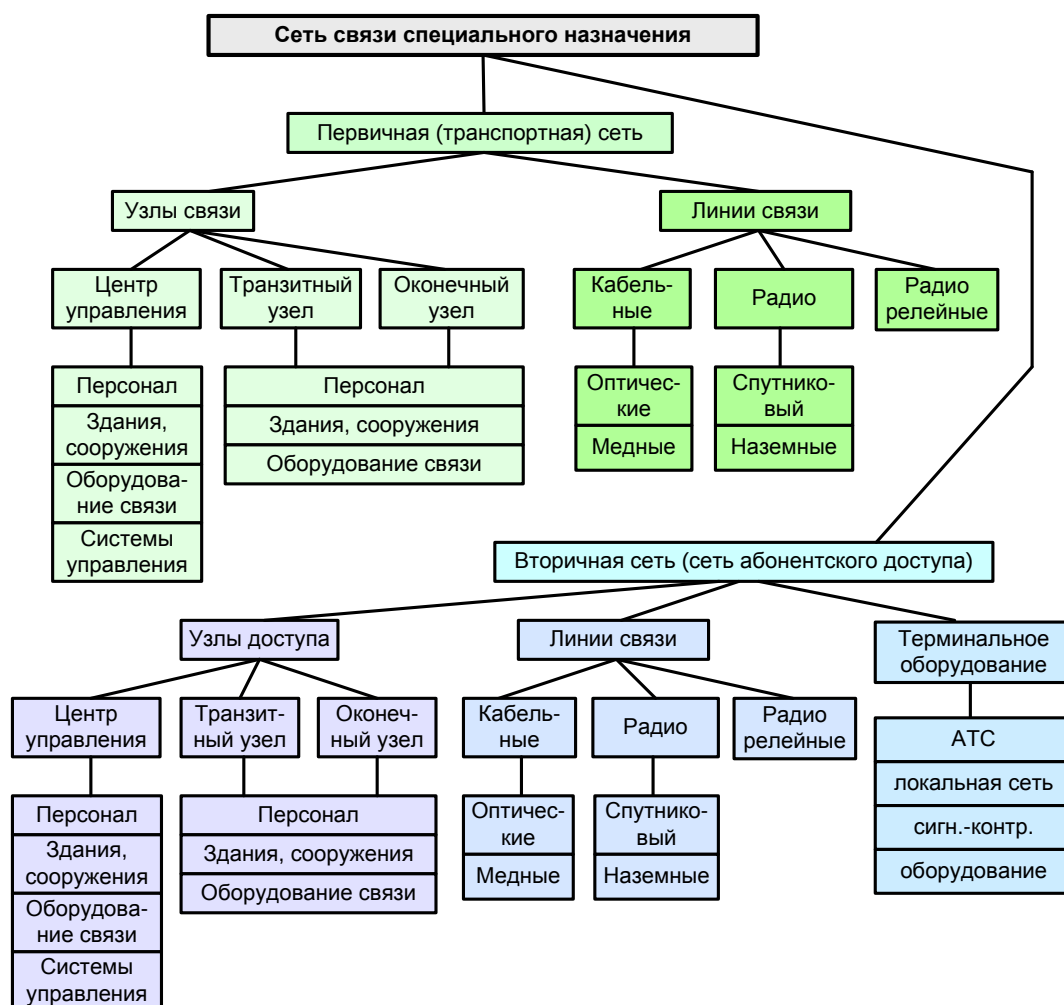


Рис. 2. Классификация элементов СС СН [41]

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

- технологии коммутации каналов – PDH, SDH, OTN;
- 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.

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.

В основу более подробной классификации вторичных сетей (сетей абонентского доступа) может быть положена используемая в ней базовая технология сети – рис. 3.

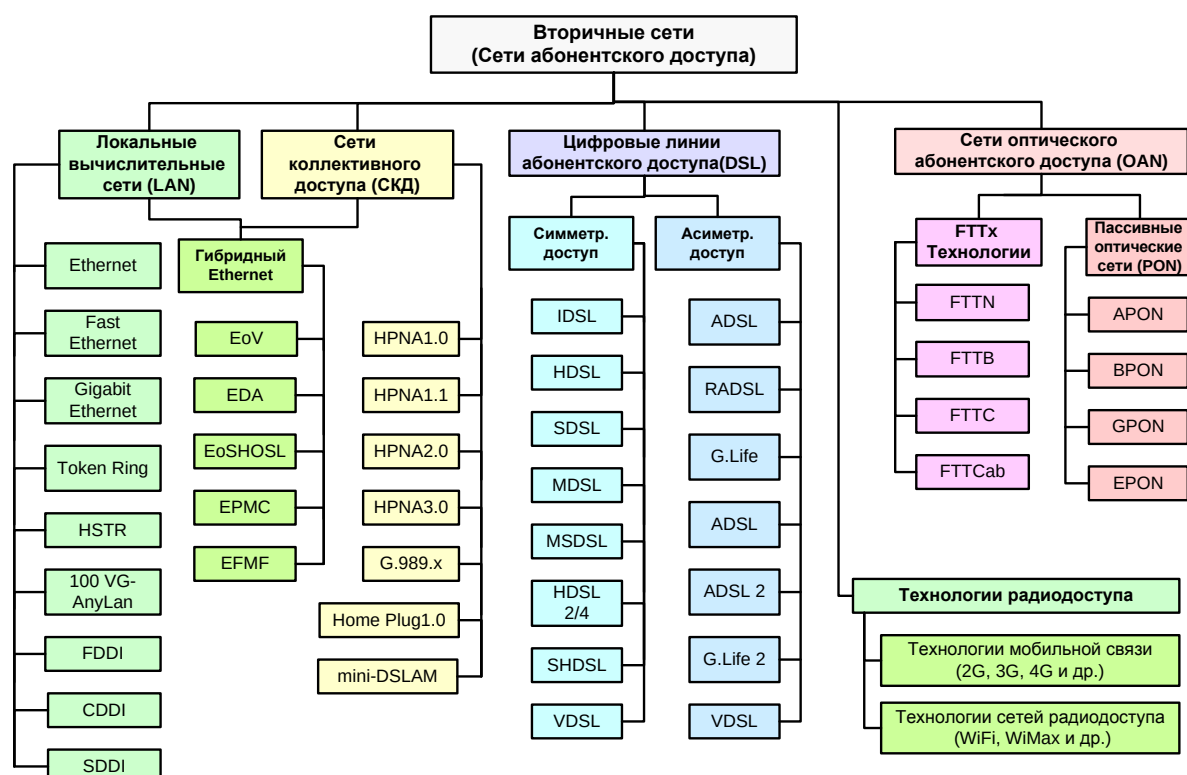


Рис. 3. Классификация вторичных сетей СС СН по используемой технологии связи [33]

По способам предоставления абонентам сервиса и услуг связи в СС СН различают [3]:

- сети с закрепленным ресурсом;
- сети с ресурсом, по требованию;
- сети с адаптивным распределением ресурса.

Под ресурсом, в самом общем случае, понимается пропускная способность сети.

Пропускная способность сети – максимально возможная суммарная скорость передачи сообщений по всем информационным направлениям связи для конкретных условий функционирования. Для СС СН пропускную способность обычно оценивают числом типовых каналов на направлениях связи, которые могут быть предоставлены абонентам [3].

Вместе с тем, обеспечение требуемой пропускной способности однозначно связано с определенными затратами других ресурсов сети – времени, полосы частот и энергии передающих устройств и т. д. В связи с этим можно дать более общее определение ресурсу сети.

Ресурс сети – совокупность канальных, временных, частотных, энергетических и других ресурсов сети связи, затрачиваемых на передачу информации всех абонентов сети [3].

2.3. Основные требования, предъявляемые к сети связи специального назначения

Сеть связи специального назначения 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, поэтому было введено интегральное понятие «качество связи».

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

Для обеспечения указанных требований к связи, в свою очередь СС СН, как организационно-техническая система, должна соответствовать требованиям к определенным ее свойствам. Взаимосвязь этих свойств, требований к связи и требований к системе управления представлена на рис. 4.

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.

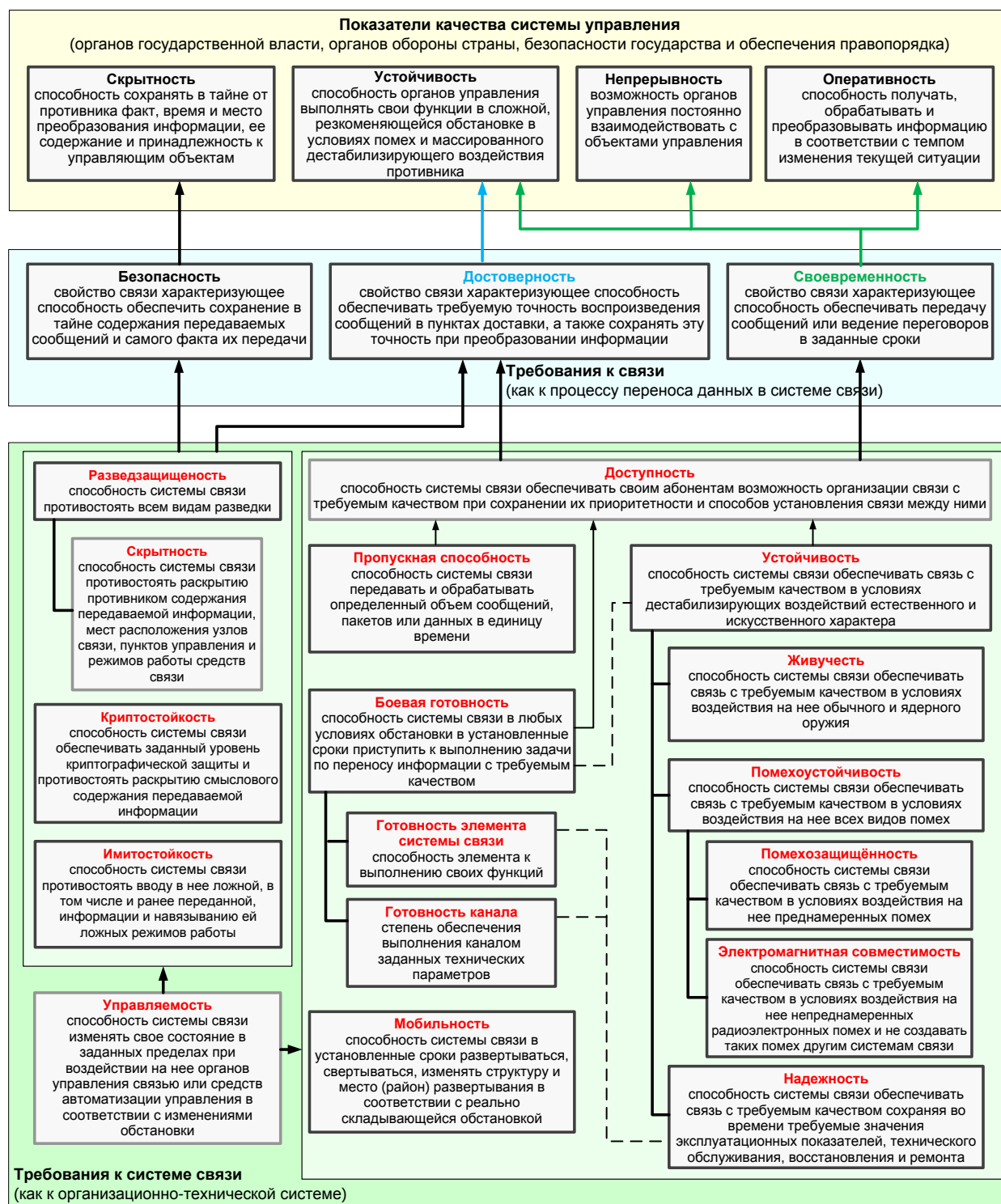


Рис. 4. Требования к связи и к СС СН [3, 33]

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]

Структурно-логическая связь между требованиями к СС СН и категориями информационной безопасности представлены на рис. 5.

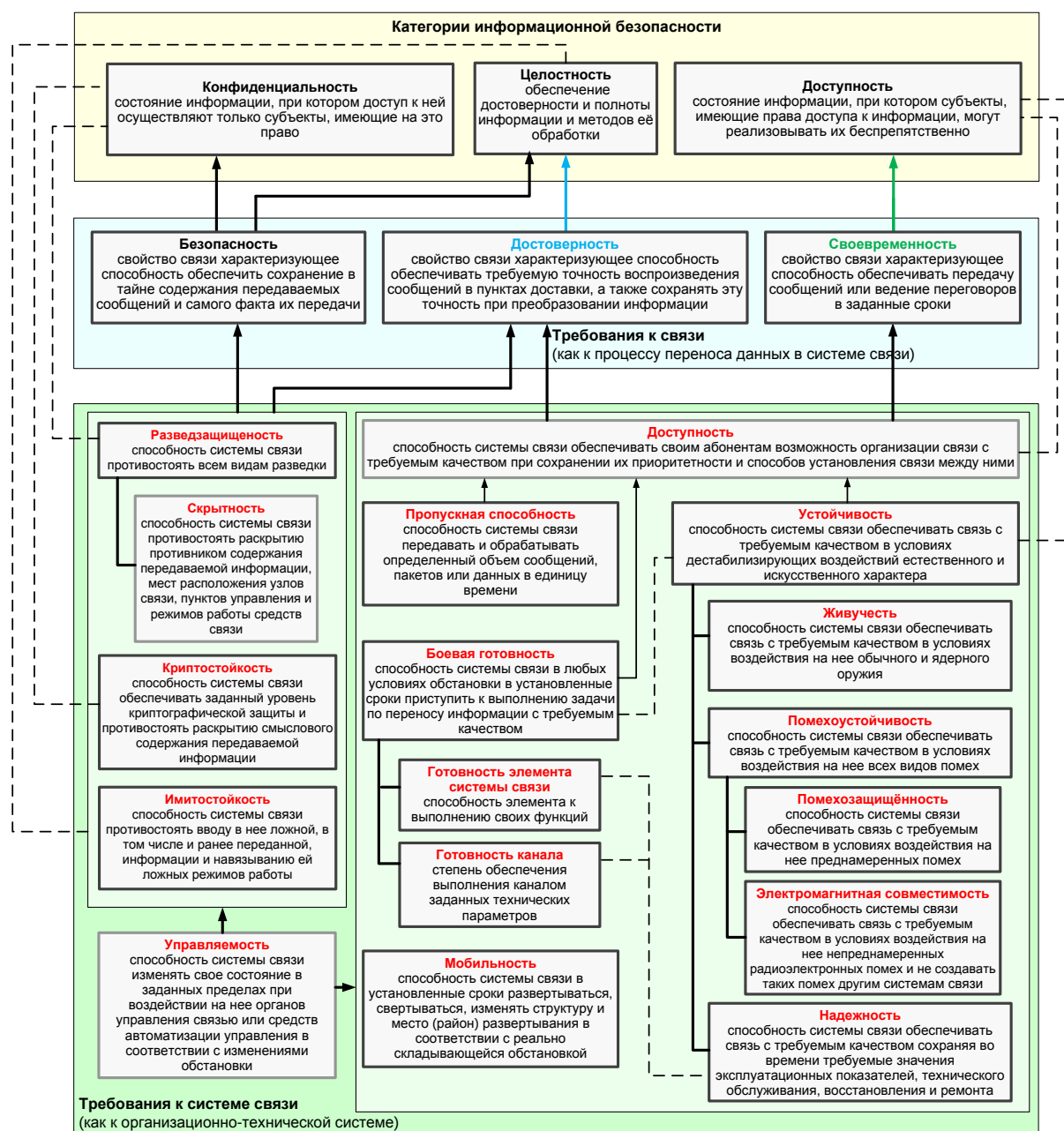


Рис. 5. Связь категорий информационной безопасности с требованиями, предъявляемыми к СС СН

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 особое 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. 6. 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.

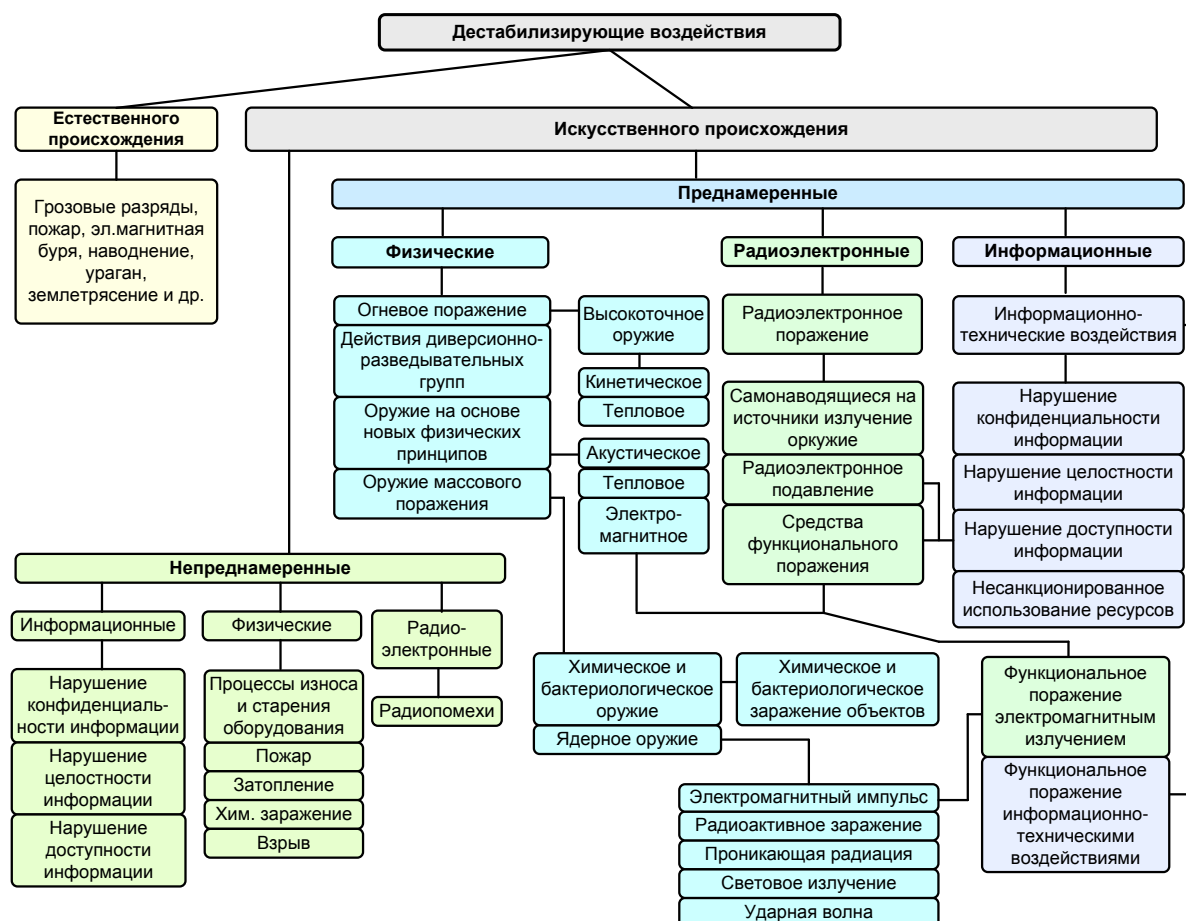


Рис. 6. Классификация дестабилизирующих факторов [41]

3. Основные тенденции развития современных сетей связи специального назначения

Анализ работ в области построения СС СН обеспечивающих информационный обмен в ВС США и НАТО, а также работ в области развития отече-

ственных СС СН [2, 8-11, 25-28, 35, 51-54, 56-60, 63] выявил следующие тенденции развития СС СН:

- переход от сопряжения отдельных СС СН, в различных органах государственного и военного управления к единой СС СН основанной на многоэшелонированном принципе построения (космический, воздушный, наземный и морской эшелоны);
- широкая интеграция в состав СС СН сегментов СС ОП и коммерческих телекоммуникационных ресурсов;
- активное замещение в СС СН технологий коммутации каналов на технологии коммутации пакетов;
- массовое использование коммерческих протоколов и технологий в составе СС 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 СС СН и глобальную управляемость во всех звеньях управления, особенно в военное время, при этом в состав СС СН могут включаться СССР из состава СС ОП в том числе СССР гражданских операторов спутниковой связи;
- использование в сетях СС 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.

3.1. Многоэшелонированное построение современных сетей связи специального назначения

Современные СС СН, как правило, декомпозируются на четыре эшелона (рис. 7):

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

Наземный эшелон СС СН использует сетевые ориентированные, 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 во-

енного управления. Узлы и линии связи наземного эшелона также обеспечивают взаимодействие между техническими средствами других эшелонов.

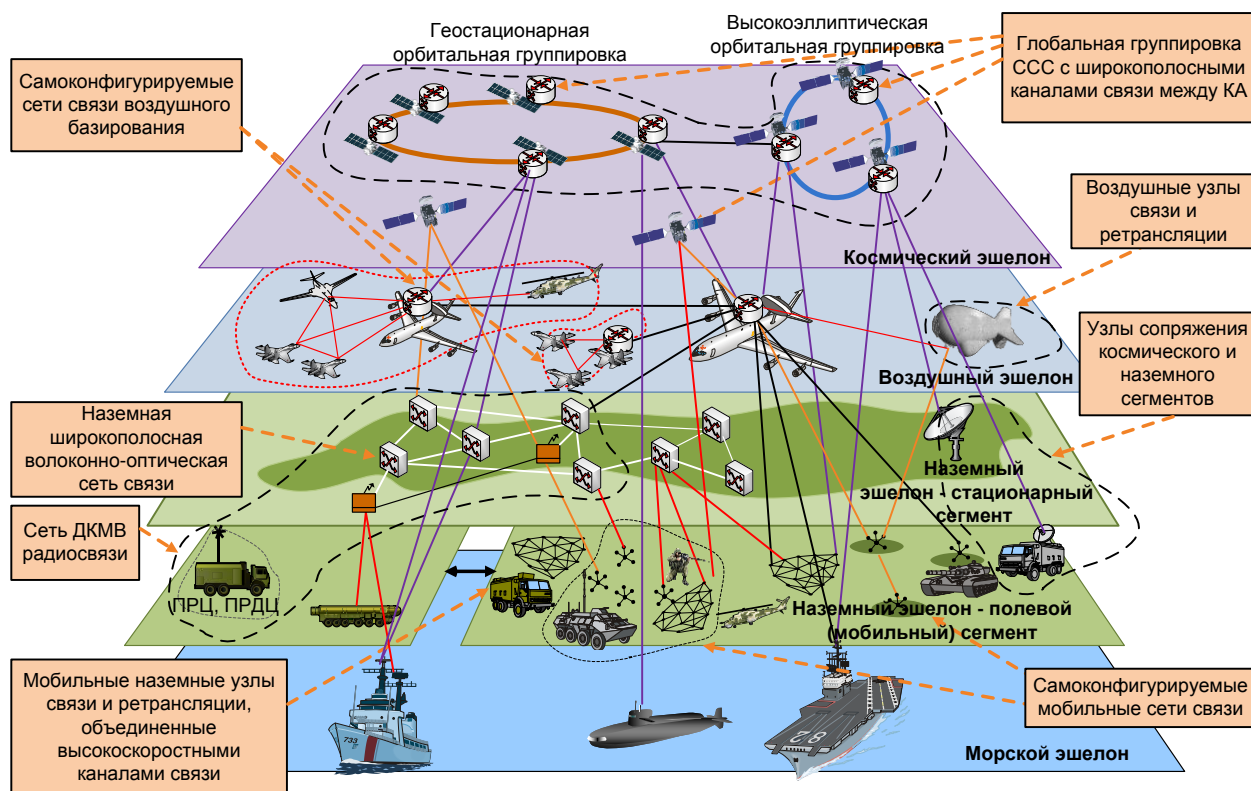


Рис. 7. Общая схема многоэшелонированного построения СС СН [60]

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.

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

Анализ современных СС СН, а также перспектив их развития, представленные в работах [2, 8-11, 25-28, 35, 51-54, 56-60, 63], 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 сетечентрическим 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 построения СС СН как для ВС РФ, так 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 канальные 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 гражданских 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 должны быть использованы решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе СС СН и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются в СС ОП гражданским оператором связи.

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.

3.3. 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.

Принципиальными изменениями, которые происходят в области построения транспортных сетей СС СН является переход к пакетной коммутации, при необходимости обеспечения устойчивого, мультисервисного и интерактивного обслуживания специальных 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 такие технологии транспортных сетей как PDH, SDH и ATM [8-11, 25-28].

Анализ работ [8-11, 25-28, 38, 54, 56, 57, 63], посвященных возможным вариантам технологического построения перспективных СС СН позволил сформировать 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 так же 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);

- АХ.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-RSC) 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/OTN. Это позволяет обеспечить в СС СН следующие эффекты [10]:

- возможность взаимодействия каждого абонента 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.

Обобщенная структурная схема сети СС СН приведена на рис. 8.

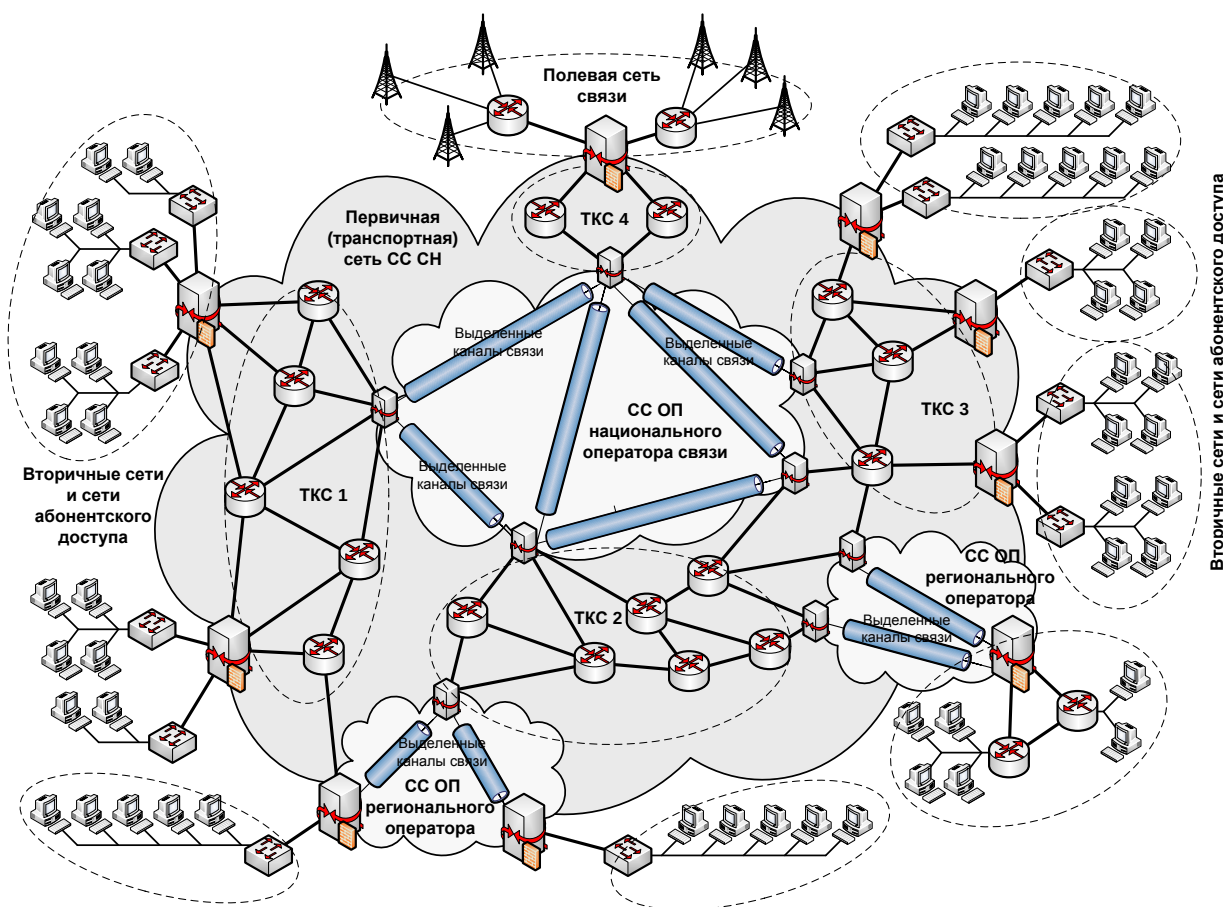


Рис. 8. Обобщенная структурная схема СС СН

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 целесообразно использовать динамические протоколы маршрутизации. При обмене маршрутной 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.

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

- стационарный сегмент транспортной сети СС СН строиться 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, STN-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 строиться 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:

- использовать единую технологию коммутации пакетов для передачи информации 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.

3.4. Построение сетей связи специального назначения в соответствии с концепцией NGN

Анализ работ по глобальным перспективам развития СС СН [8-11, 25-28, 63] 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 [38]. Обзор основных технологических решений концепции NGN представлен в более ранней работе автора [61], 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) уровнем приложений и услуг;
- 2) уровнем коммутации услуг;
- 3) уровнем транспорта, включающего функции управления сетевыми ресурсами и уровень доступа;
- 4) уровнем управления сетью.

Для построения сети NGN необходимо в дальнейшем реализовать каждый из этих уровней в виде соответствующего набора элементов сети NGN (рис. 9). При этом на различных логических уровнях сети могут использоваться различные технологии и протоколы.

Уровень приложений и услуг содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую следующие потребности [61]:

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

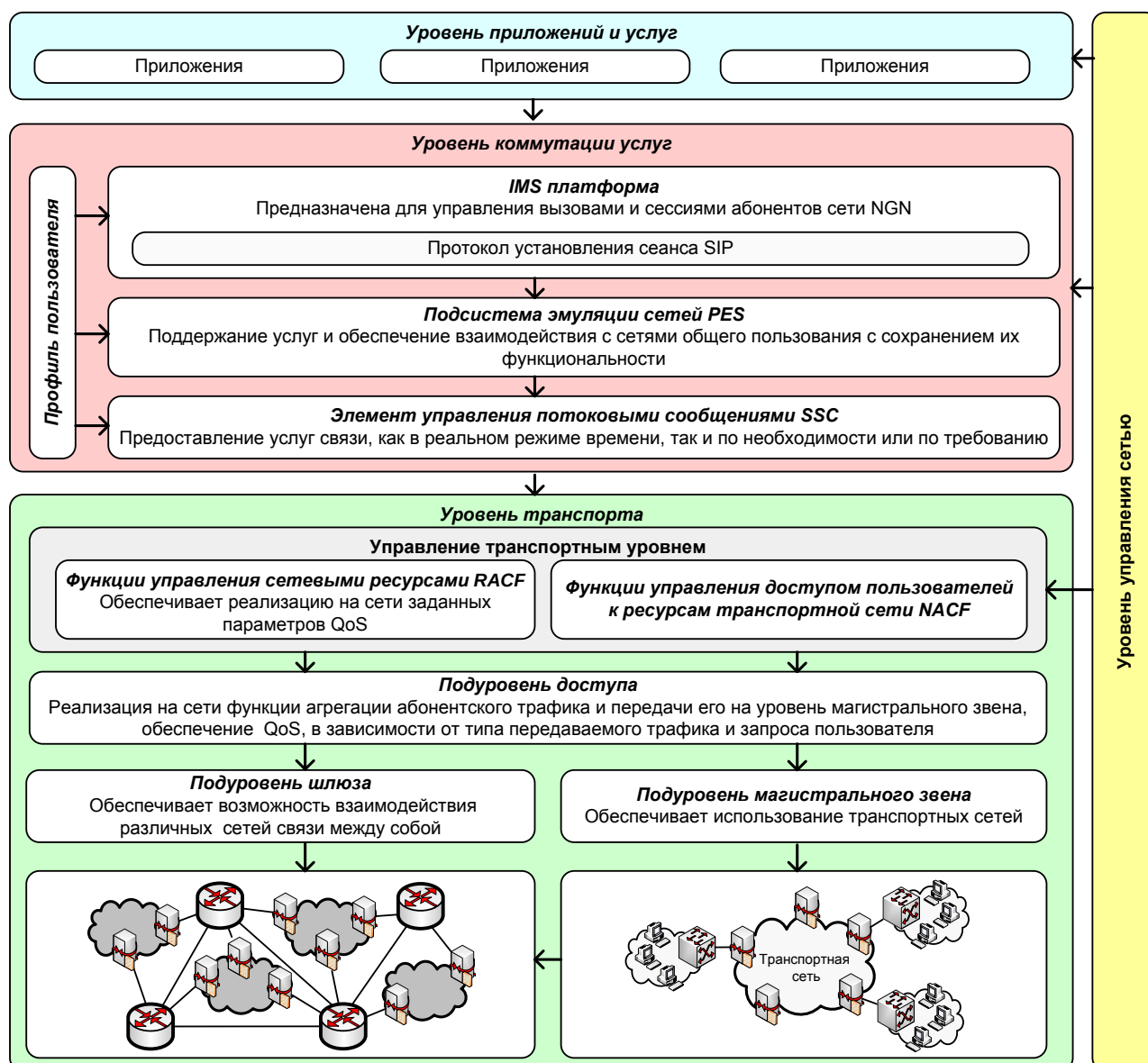


Рис. 9. Схема основных уровней сети NGN [61]

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 [61].

С функциональной точки зрения, данный уровень должен решать основные задачи по установлению соединений и предоставлению услуг в сети NGN.

Основными функциями уровня коммутации услуг являются [61]:

- 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 [61]:

- 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 [61].

- подуровень доступа. На данном уровне реализуются функции агрегации абонентского трафика, которые зависят от типа передаваемого трафика и запросов пользователя, а также обеспечение QoS трафика и передача его на уровень магистрального звена;
- подуровень магистрального звена. Магистральное звено в виде отдельного 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;
- подуровень 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/OTH 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, канально-

го 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 [61].

Система управления должна обеспечивать [61]:

- 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.

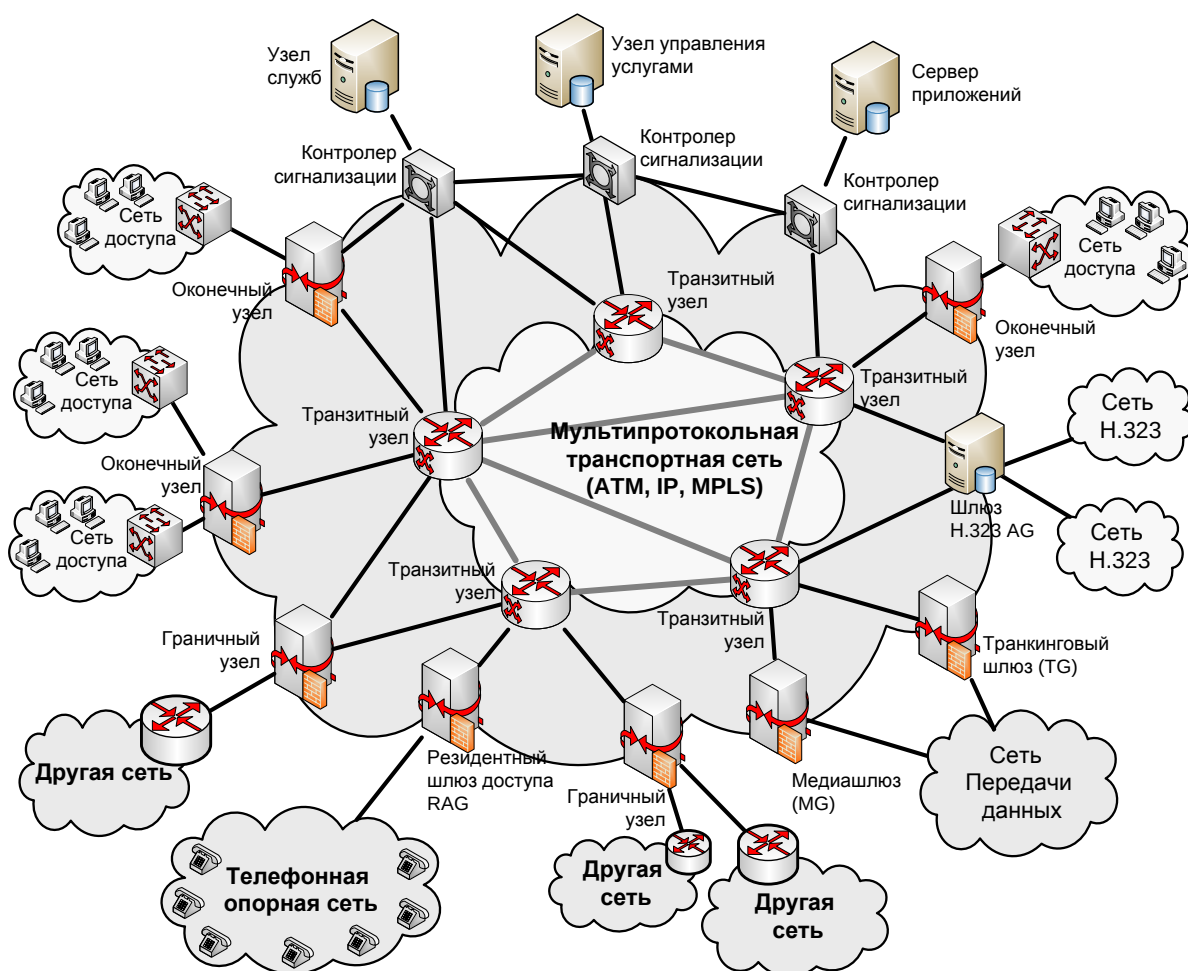


Рис. 10. Мультипротокольная (ATM, IP, MPLS) транспортная сеть NGN [61]

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 обработки информации сигнализации, управления вызовами (запросами) и соединениями, а также управления транспортной сетью NGN;
- 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 CAC (Call Admission Control), управления QoS, концентрации голосового и сигнального трафика;
- 6) 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 конференц-связи.

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. 11. При этом в данной модели для реализации любых сетевых услуг в ТКС предполагается использование IP-технологии.

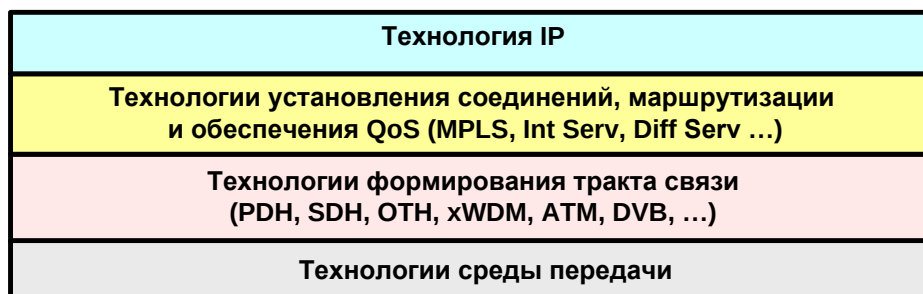


Рис. 11. Модель звена транспортной сети NGN [8]

При организации сети NGN основные функции уровня транспорта из модели NGN реализуются протоколами сетевого и транспортного уровня модели OSI. Именно эти протоколы выполняют в ТКС NGN функции маршрутизации, установления и разрыва соединений, а также обеспечения QoS трафика.

На транспортном уровне OSI в сети NGN для обеспечения QoS передаваемых потоков трафика могут использоваться как известные технологии обеспечения QoS, основанные на моделях Int Serv и Diff Serv, так и механизмы, встроенные в транспортные технологии канального уровня – ATM, MPLS, SDH, DVB и др.

На сетевом уровне OSI для маршрутизации в сети NGN на основе IP могут использоваться протоколы без установления соединения, такие как OSPF, IS-IS, RIP и др. Однако для маршрутизации потоков трафика в мультипротокольном ядре ТКС NGN на основе ATM и IP/MPLS используется протокол маршрутизации с установления соединения PNNI.

На канальном уровне ТКС NGN выполняются функции: формирования цифровых трактов связи – на основе технологий PDH, SDH, WDM, Ethernet (Gigabit Ethernet/10-Gigabit Ethernet), ATM, DVB-S, DVB-S2 и др.

Физический уровень как среда передачи сигналов – реализуется на основе волоконно-оптических, радиорелейных и спутниковых линий связи [8].

В соответствии с этим 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.

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 сетевых ресурсов при передаче разнородного трафика. В перспективе построение транспортной сети CC СН на основе NGN будет эволюционировать к однородной конвергентной структуре на базе связки протоколов IP/MPLS – концепция «все по IP» (рис. 12). 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 CC СН в единую транспортную сеть IP/MPLS, поддерживающую широкий спектр технологий доступа.

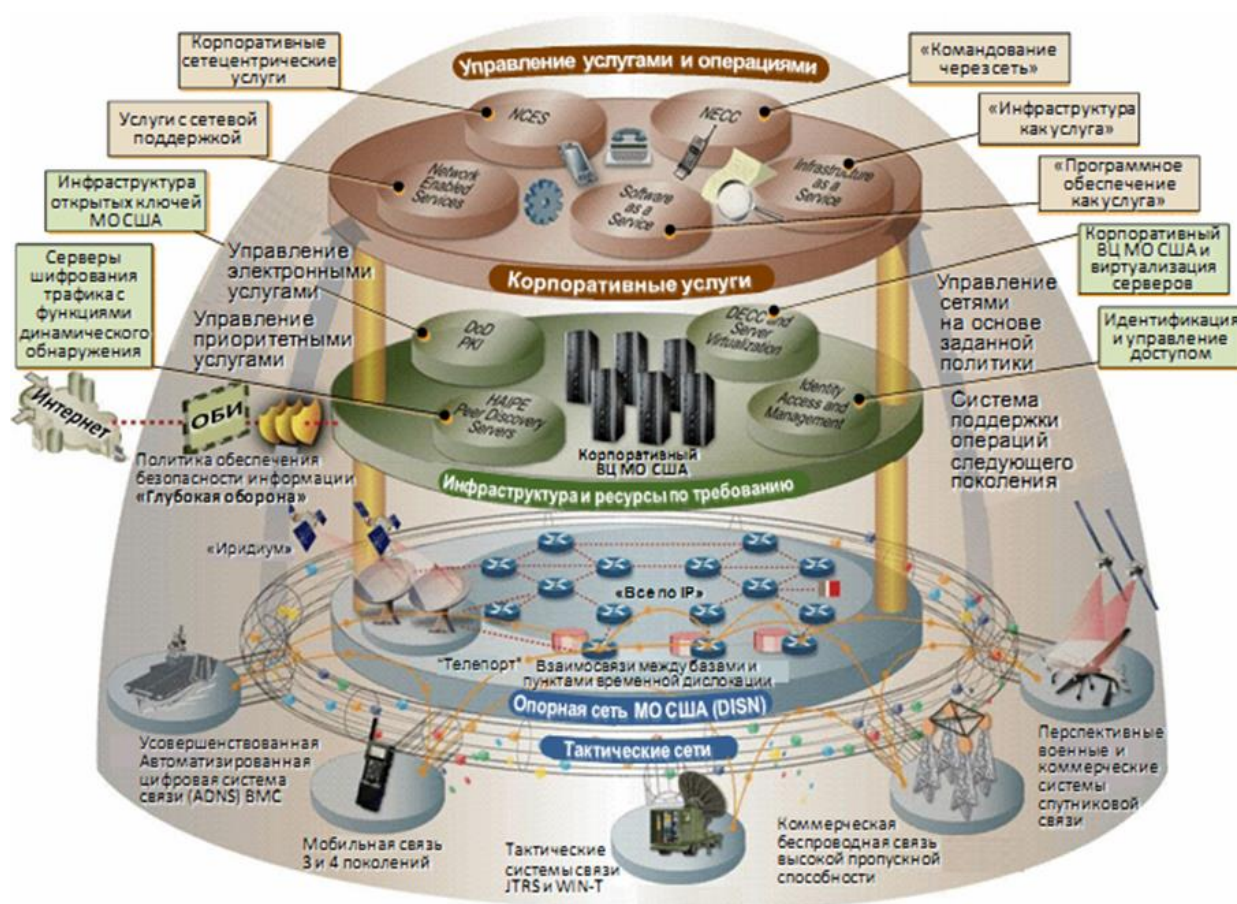


Рис. 12. Общая структура информационного пространства на основе GIG [54]

3.5. Переход 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 представлением 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, с соответствии с концепцией NGN 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 её 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 связанных 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 перспективных ИКС СН 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 части и серверной, при этом 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. 13.

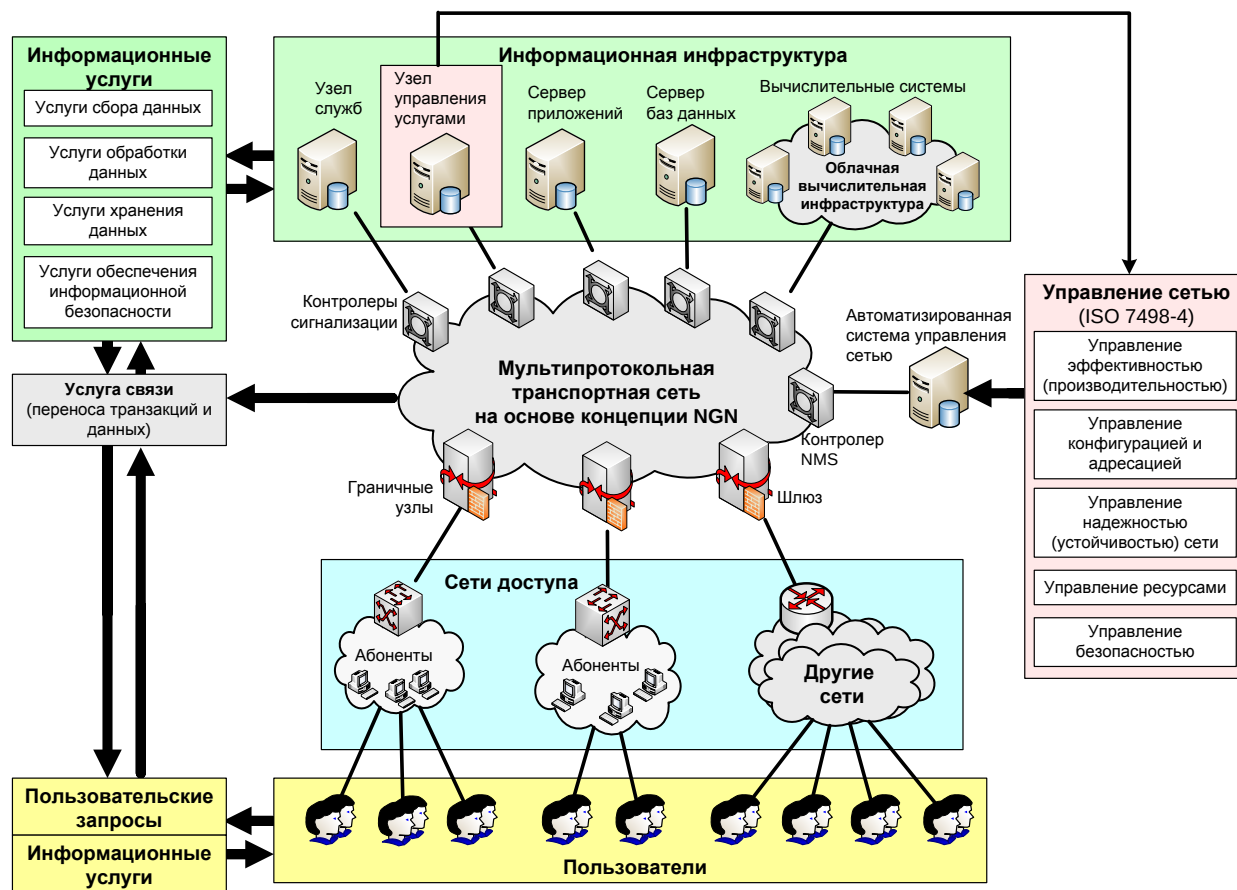


Рис. 13. Обобщенная архитектура перспективной ИКС СН

Особенностью интеграции сервиса оказания информационных услуг пользователя в ИКС СН является то, что существенно возрастет роль систем управления, как услугами, так и сетью. Для реализации функций управления создаются службы MNS (Network Management System), которые обеспечивают оптимальное функционирование сетей, распределенное планирование, управление и контроль сетевых элементов и ресурсов. Функции службы MNS 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.

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].

4. Описательная модель сети связи специального назначения – основные протоколы и технологии

Как было показано выше, одной из основных тенденций развития СС СН является массовое использование в составе СС СН коммерческих протоколов и технологий. Опишем технологии функционирования СС СН и взаимодействие отдельных ТКС в ней более подробно.

При описании сетевого и транспортного уровней СС СН целесообразно протоколы и технологии разбить на несколько основных групп:

- базовые протоколы технологии IP;
- маршрутные протоколы;
- протоколы и механизмы поддержки качества обслуживания;
- протоколы групповой рассылки (multicast);
- протоколы повышения надежности маршрутизации;
- протоколы обеспечения безопасности.

Ниже рассмотрены особенности реализации и функционирования протоколов этих основных групп в ТКС входящих в состав СС СН в соответствии с их применением в коммерческих СС ОП, как это представлено в работах [35, 36, 42-45, 62].

4.1. Базовые протоколы технологии IP

К базовым протоколам технологии IP относятся как собственно протоколы IPv4 или IPv6, так и протоколы, обеспечивающие его работу – Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP). Эти базовые протоколы поддерживаются всеми устройствами сетевого уровня.

Протоколы IPv4 или IPv6 определяют ряд основополагающих параметров и механизмов сетевого уровня. К ним относятся [42]:

- формат IP-пакета;
- сетевую адресацию;
- фрагментацию дейтаграммы на составные части;
- защиту дейтаграммы от заикливания;
- адрес протокола транспортного уровня, которому предназначена дейтаграмма.

Протокол ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче трафика, например, если запрашиваемая услуга связи недоступна, или маршрутизатор не отвечает. Протокол ICMP является самостоятельным для IPv4 и встроен в IPv6 [42].

Протокол ARP используется для получения адреса канального уровня MAC по известному адресу IP. Протокол ARP является самостоятельным для IPv4 и встроен в IPv6 [42].

Протокол DHCP используется для динамической настройки параметров узлов сети. Он наиболее широко используется для получения динамического адреса узла. Данный протокол содержит серверную часть, обслуживающую динамические запросы от узлов и клиентскую часть. При отсылке данных используется сервисом транспортного уровня UDP [42].

В сетях CC CN построенных в соответствии с концепцией NGN на основе технологии IP/MPLS к базовым протоколам также можно отнести протокол MPLS. Этот протокол обеспечивает создание виртуальных каналов в IP-сети, присвоению IP-пакетам специализированных меток и последующей передачей их по виртуальным каналам с использованием технологии быстрой коммутации по меткам. Кроме указанных функций протокол MPLS поддерживает механизмы оптимизации и управления трафиком для обеспечения высокого QoS.

4.2. Маршрутные протоколы

К протоколам маршрутизации в CC CN относят протоколы обмена служебной информацией, обеспечивающие построение сетевыми устройствами таблиц маршрутизации, которые в дальнейшем используются для поиска кратчайших путей передачи трафика между узлами сети.

Различают статическую и динамическую маршрутизацию. Статическая маршрутизация в CC CN используется маршрутизаторами в сетях доступа для тех случаев, когда имеется единственный маршрут доставки пакетов. Статическая маршрутизация используется также для работы в подсетях на основе технологий коммутации каналов (таких как PDH, SDH, OTN), где из-за отсутствия постоянных соединений функционирование протоколов динамической маршрутизации невозможно. Во всех остальных случаях, как правило, в CC CN используется динамическая маршрутизация [51-53].

Протоколы динамической маршрутизации функционально разделяются на [42]:

- протоколы «внутреннего шлюза» (Interior Gateway Protocol – IGP);
- протоколы «наружного шлюза» (Exterior Gateway Protocols – EGP).

Протоколы IGP используются внутри отдельных ТКС, которые с точки зрения сетевого уровня являются автономными системами (областями) маршрутизации в составе CC CN. Основная задача протоколов IGP – автоматическое объединение маршрутизаторов, принадлежащих одной области и связанных каналами связи, в единую сеть. Маршрутизаторы рассылают и используют полученную служебную информацию для построения матриц маршрутов с заданным критерием эффективности. Протоколы IGP характеризуются полным представлением структуры сети, принадлежащей конкретной ТКС.

К протоколам группы IGP относятся следующие протоколы [42]:

- протоколы на основе оценки состояния каналов (OSPF, IS-IS и др.);
- дистанционно-векторные протоколы (RIP, RIPng, IGRP, EIGRP и др.).

В ТКС на основе IP наибольшее распространение получили протоколы RIP, RIPng (для IPv6), OSPF. В составе ТКС, которые построены на оборудовании Cisco, могут использоваться протоколы IGRP или EIGRP. В ТКС на основе технологии IP/MPLS используются протокол установления и поддержания соединений PNNI в котором поиск кратчайших путей реализован через протокол OSPF. В дальнейшем, после установления соединений, передача IP трафика в них производится путем назначения меток и быстрой коммутации по меткам на основе протокола MPLS.

В качестве протоколов IGP также используют сервисные протоколы, обеспечивающие перенос сообщений об изменении топологии сетей от сторонних областей маршрутизации между граничными устройствами своей области маршрутизации. К данным протоколам относятся: IBGP, MP BGP [42].

Протоколы EGP используются при обмене маршрутной информацией между отдельными ТКС внутри СС СН, а также между ТКС отдельного функционального назначения или между ТКС различных уровней государственного или военного управления. Они обеспечивают перенос в СС СН сообщений об изменении топологии сетей отдельных ТКС, а также обмен информацией о достижимости ТКС из других автономных областей маршрутизации. Их задача – автоматическое информирование о достижимых сетях через межсетевой интерфейс. Протоколы EGP еще называют протоколами маршрутизации на основе политик, позволяя определить условия использования сервисов доступа и переноса трафика через транзитные ТКС внутри СС СН. К широко распространенным протоколам EGP относятся протоколы группы BGP (Border Gateway Protocol): IBGP, BGP4, EBGP. Причем наибольшее распространение в СС СН получил протокол BGP4. Протоколы межсетевого взаимодействия ТКС внутри СС СН из группы EGP-протоколов и протокол DNS являются основными протоколами, обеспечивающими объединение отдельных ТКС в единую СС СН (это верно, как для СС СН и СС ОП, так и для глобальной сети Интернет) [42].

4.3. Протоколы групповой рассылки

К протоколам групповой рассылки (multicast) относят протоколы, обеспечивающие эффективную доставку информации до абонентов СС СН, объединенных в группу. Здесь под эффективностью понимают минимизацию трафика, или числа пакетов, которые должны дублировать маршрутизаторы при передаче их через сеть. К данным протоколам в СС СН относятся [42, 51-53]:

- протокол IGMP (Internet Group Management Protocol) – протокол управления групповой передачей данных в сетях, основанных на протоколе IP и сходный по принципам функционирования с протоколом ICMP. Этот протокол используется маршрутизаторами для организации сетевых устройств в группы;
- семейство протоколов PIM (Protocol Independent Multicast) – использует данные функционирующих в IP сети протоколов маршрутизации для построения путей, проведения групповой рассылки пакетов и мно-

гоадресной маршрутизации. Довольно часто протоколы семейства PIM используются совместно с протоколом DVMRP;

- Протокол дистанционно-векторной многоадресной маршрутизации DVMRP (Distance Vector Multicast Routing Protocol) – предназначен для маршрутизации пакетов внутри автономных областей маршрутизации в IP сетях при групповой рассылке сообщений;
- протокол MARS (Multicast Address Resolution Server) – сервер разрешения широковещательных адресов, предназначенный для организации соединений «точка-группа».

Наиболее важным для служебных целей маршрутизации в СС СН являются протоколы семейства PIM (PIM-DM, PIM-SM, PIM-SSM). Они позволяют строить множество кратчайших путей от источника к получателю с определением места каждого маршрутизатора в составе пути и дублированием рассылки пакетов другим маршрутизаторам или группе абонентов, являющихся получателями.

4.4. Протоколы повышения надежности маршрутизации

К данной группе относят протоколы, которые обеспечивают повышение устойчивости и функционирования базовых протоколов СС СН. В своем большинстве, эти протоколы направлены на обеспечение надежности маршрутизации в условиях резко меняющейся интенсивности трафика – так называемым «пульсациям» трафика.

К протоколам повышения надежности маршрутизации и доставки пакетов можно отнести [51-53]:

- протоколы группы STP (Spanning Tree Protocol): RSTP, PVSTP, MSTP – позволяют обнаружить петли в транспортных сетях Ethernet, заблокировать их, а в случае отказа каналов сети использовать эти петли для формирования резервных направлений связи;
- протокол IP-Trunk для объединения отдельных IP-соединений со сходными требованиями к QoS на сетевом уровне в магистрали соединений (так называемые «транки»);
- протокол резервирования сетевых ресурсов RSVP (Resource ReSerVation Protocol) – позволяет зарезервировать сетевые ресурсы маршрутизаторов для обеспечения QoS в соответствии с моделью IntServ;
- протоколы технологий CES (Circuit Emulation Service): TDMoIP и TDMoP – для обеспечения эмуляции типовых каналов цифровой иерархии PDH и SDH при передаче трафика через пакетные сети;
- протоколы виртуализации маршрутизаторов HSRP (Hot Standby Router Protocol) и VRRP (Virtual Router Redundancy Protocol) – предназначены для повышения надежности основного маршрутизатора сети (маршрутизатора по умолчанию) путем объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса;

- протокол резервирования маршрутизаторов в территориально распределенных сетях E-Trunk – обеспечивает резервирование и обмен служебной информацией между граничными маршрутизаторами ТКС, а при выходе из строя одного из них – перенаправление трафика на другой граничный маршрутизатор.

4.5. Протоколы и технологии обеспечения качества обслуживания

Для обеспечения обслуживания трафика, предъявляющего различные требованиям к сетевым характеристикам обмена, на сетевом и транспортном уровнях в СС СН используются стандартные архитектуры обеспечения качества обслуживания QoS.

К основным архитектурам обеспечения QoS в СС СН относятся [62]:

- обслуживание с максимальными усилиями, но без гарантий (Best Effort) – использует механизм выделения дополнительной пропускной способности без использования тонких способов управления трафиком;
- *интегрированное обслуживание* (IntServ – Integrated Service) – использует протокол RSVP для резервирования сетевых ресурсов в каналах и узлах сети на этапе установления соединения, после чего обеспечивает QoS во всем соединении путем контроля соблюдения QoS во всех промежуточных элементах сети;
- *дифференцированное обслуживание* (DiffServ – Differentiated Service) – вводит классификацию трафика по классам обслуживания CoS (Class of Service) на границе сети, определяет требуемое QoS для каждого класса обслуживания, с последующим распределением сетевых ресурсов сети с целью гарантировать QoS допущенного в сеть трафика. Данная архитектура поддерживает управление формированием трафика (классификация пакетов, маркировка, управление интенсивностью и др.) и управления политикой (распределение сетевых ресурсов, политика отбрасывания пакетов и т. д.).

Основной архитектурой обеспечения качества обслуживания в СС СН, как правило, является DiffServ. Для обеспечения высокой эффективности архитектуры DiffServ ее должны поддерживать все сетевые устройства СС СН.

Архитектура DiffServ поддерживает три базовых класса обслуживания трафика [62]:

- трафик «реального времени» (Real Time – RT);
- приоритетный трафик (Priority – P);
- непероритетный трафик (Non priority – NP).

Для трафика класса RT поддерживается 4 приоритета абонентов, для классов P, NP – 3 приоритета абонентов.

Зачастую производители оборудования для СС СН разрабатывают отдельные соответствия маркировок классов обслуживания для трафика специальных абонентов, взяв за основу классы обслуживания, принятые в технологиях DiffServ для MPLS.

Сетевые устройства, поддерживающие DiffServ используют [62]:

- различные выходные очереди для трафика различных классов обслуживания, а также основанную на этих классах приоритетную дисциплину обслуживания этих очередей CQ (Class based Queuing);
- механизмы раннего обнаружения перегрузок RED (Random Early Detection) для контроля за длиной очередей в узлах сети и обнаружения их перегрузок.

Механизм RED важен для обеспечения требуемых показателей QoS в каждой автономной области маршрутизации.

Граничные маршрутизаторы в каждой автономной области маршрутизации (т. е. в каждой ТКС в составе СС СН) должны поддерживать классификацию трафика (traffic classification), а также сопоставление интенсивности поступающего трафика и достаточности доступных сетевых ресурсов для его обслуживания. Для контроля перегрузок и выполнения ограничений по интенсивности и структуре трафика в своей области маршрутизации (в отдельной ТКС) граничные маршрутизаторы могут использовать следующие стандартные технологии [62]:

- технологии формирования трафика (Shaping);
- технологии контроля параметров трафика (Traffic Policing).

При контроле параметров трафика используются технологии:

- «дырявого ведра» (Leaky Bucket);
- «маркерного ведра» (Token Bucket).

При невозможности обслуживания трафика в конкретной области маршрутизации (в отдельной ТКС в составе СС СН) поступающий трафик либо сбрасывается, либо буферизируется с пометкой «Best Effort». Данная пометка означает, что трафик будет обслужен без гарантий обеспечения требований к QoS, но с максимальными усилиями со стороны сетевых устройств по его соблюдению. Для технологии MPLS трафик IP инкапсулируется, а класс MPLS маркируется заново [62].

В СС СН модель DiffServ, может быть реализована совместно с моделями «Best Effort» и IntServ, дополняя друг друга. Например, в отсутствие трафика определенного класса, в отведенной ему полосе обслуживания может передаваться трафик «Best Effort». В сетях с ограниченными ресурсами, дополнительно могут реализоваться функции RSVP протокола, позволяющие выборочно резервировать сетевые ресурсы под соединение для специальных абонентов с высоким приоритетом. Функционал RSVP запросов относится к модели IntServ [62].

4.6. Протоколы безопасности

Для СС СН определены следующие функции безопасности [46]:

- аутентификация (обеспечивает аутентификацию абонентов и пользователей по общению, а также аутентификацию источника данных в СС СН);

- управление доступом (позволяет ограничить режимы взаимодействия сетей и обеспечить сокрытие информации о структуре и особенностях построения как отдельных ТКС, так и СС СН в целом, путем фильтрации пакетов и сообщений на сетевом, транспортном и прикладном уровнях OSI по соответствующим группам служебных атрибутов, извлекаемых из этих сообщений);
- конфиденциальность и целостность трафика в режиме, как с установлением соединения, так и без него (достигается криптографической защитой данных на физическом, канальном, сетевом, транспортном и прикладном уровне);
- целостность соединений с обеспечением и без обеспечения возможности их восстановления (позволяет обнаруживать изменения данных, передаваемых в рамках уже установленных соединений);
- безотказность, или защита от отказа источника или получателя сообщений (основана на использовании криптографических протоколов, которые обеспечивают надежные гарантии отправки и доставки сообщений для их источника/получателя).

К протоколам СС СН, которые обеспечивают эти функции безопасности, относятся [46, 51-53, 64]:

- протоколы фильтрации IP-адресов (IP-filtering);
- протоколы доступа на основе списков (ACL-lists) выполняемые на маршрутизаторах и межсетевых экранах;
- функции авторизации при обмене динамической маршрутной информацией между маршрутизаторами IS-IS authorization, EBGp authorization;
- протоколы виртуальных каналов и сетей;
- другие протоколы.

Кроме того, в состав СС СН, как правило, включаются специализированные закрытые протоколы шифрования, управления ключевой информацией, электронной цифровой подписи, авторизации, а также другие протоколы и технологии, направленные на обеспечение информационной безопасности в СС СН. Более развернутое описание защищаемых ресурсов и требований к протоколам безопасности с учетом специфики СС СН представлено в работе [64].

4.7. Межсистемные протоколы и интерфейсы

Обобщая вышеуказанное, на основе анализа работ [8-11, 25-28, 51-53, 62] возможно сформулировать перечень основных протоколов и интерфейсов которые будут заимствованы из сферы связи гражданского назначения и планируется к использованию в составе элементов СС СН.

К таким коммерческим протоколам, получившим широкое распространение в СС СН, относятся следующие.

1) Базовые протоколы СС СН обеспечивающие передачу данных:

- IP v4;
- IP v6;

- MPLS;
 - ICMP;
 - ARP;
 - DHCP.
- 2) Протоколы маршрутизации:
- а) для внутрисетевой маршрутизации (IGP):
 - OSPF;
 - IS-IS;
 - PNNI;
 - IGRP (EIGRP) – при использовании оборудования Cisco;
 - RIP и другие.
 - а) для межсетевой маршрутизации (EGP):
 - BGP 4;
 - EBGP;
- 3) Протоколы групповой рассылки:
- IGMP;
 - PIM (PIM-DM, PIM-SM, PIM-SSM);
 - DVMRP.
- 4) Протоколы повышения надежности маршрутизации:
- STP, RSTP, PVSTP, MSTP;
 - IP-trunk, E-trunk;
 - RSVP;
 - TDMoIP, TDMoP;
 - HSRP, VRRP.
- 5) Протоколы и технологии обеспечения качества обслуживания:
- архитектуры обеспечения качества обслуживания:
 - o DiffServ;
 - o Best Effort;
 - маркировка трафика – на основе маркировок DiffServ;
 - технологии DiffServ на входных граничных маршрутизаторах:
 - o классификация трафика по классам обслуживания;
 - o технологии контроля параметров трафика (Traffic Policing) при помощи механизмов «дырявого ведра» (Leaky Bucket) и «маркерного ведра» (Token Bucket);
 - o сброс или перемаркировка избыточного трафика;
 - технологии DiffServ на выходных граничных маршрутизаторах:
 - o технологии формирования трафика (shaping) на основе механизма «дырявого ведра» (Leaky Bucket);
 - o управление очередями CQ в маршрутизаторах основанное на классах обслуживания;
 - o раннее обнаружение перегрузок RED;
 - o сброс или перемаркировка избыточного трафика.
- 6) Протоколы обеспечения безопасности:
- IP-фильтрация;
 - листы доступа ACL;

- авторизация маршрутного протокола EBGP;
- другие специализированные протоколы.

К интерфейсам ТКС в составе СС СН, которые также широко заимствуются из сферы гражданской связи, относятся следующие.

1) На физическом уровне модели OSI.

а) Консольные порты:

- RS-232;
- USB 2.0.

б) Интерфейсы пакетной сети:

- Ethernet 100BASE-SX (FX) – многомодовые (одномодовые) ВОЛС;
- Ethernet 100BASE-TX, IEEE 802.3u;
- E1 G.703/G704 (E2, E3, E4);
- STM-1, STM-4, STM-16;
- интерфейсы систем связи предыдущих поколений.

в) Протоколы управления:

- SNMP v.3;
- XML;
- SSH;
- Telnet;
- CLI;
- FTP, TFTP.

2) На канальном уровне модели OSI:

- IEEE 802.3 (Ethernet);
- PPP, MP-PPP;
- кадры Jumbo;
- авторизация и аутентификация (PAP/CHAP, 802.1X, RADIUS);
- L2 VPN;
- резервирование (LAG);
- Ethernet OAM;
- QoS DiffServ;
- STP, RSTP, PVSTP, MSTP.

3) На сетевом уровне модели OSI.

- IPv4, IPv6;
- MPLS;
- BGP4;
- Балансировка трафика IP;
- многоадресные протоколы (PIM, DVMRP);
- авторизация и аутентификация (RADIUS).

4) На транспортном уровне модели OSI:

а) Обеспечение качества обслуживания средствами IntServ:

- RSVP;

б) Обеспечение качества обслуживания средствами DiffServ:

- формирование трафика (Shaping) на входящих и исходящих интерфейсах;

- регулирование трафика на исходящих интерфейсах (буферирование LLQ, WFQ, CB WFQ, WRED и т.д.);
- управление доступом (контроль доступа на базе адресов IP, портов TCP/UDP, полей TOS/DSCP и т. д.);
- как «прозрачный» перенос полей ToS и DSCP, так и их перераспределение;
- ICMP;
- резервирование VRRP.

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.

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.

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 высокодинамичной 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-Сотт: Телекоммуникации и транспорт. 2015. Том 9. № 12. С. 32-36.

17. Легков К. Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения // Т-Сотт: 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_constructing_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. Шнепс-Шнеппе М. А. Телекоммуникации Пентагона: цифровая трансформация и киберзащита. – М.: Горячая линия – Телеком, 2017. – 272 с.

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. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов 4-е изд. – СПб.: Питер, 2010. – 945 с.

43. Гордиенко В. Н., Тверецкий М. С. Многоканальные телекоммуникационные системы: учебник – М.: Горячая линия - Телеком, 2013. – 397 с.

44. Крухмалев В. В., Гордиенко В. Н., Моченов А. Д., Иванов В. И., Бурдин В. А., Крыжановский А. В., Марыкова Л. А. Основы построения телекоммуникационных систем и сетей / Под ред. В.Н. Гордиенко и В.В. Крухмалева. – М.: Горячая линия - Телеком, 2004. – 510 с.

45. Соколов Н. А. Телекоммуникационные сети. Монография в 4-х частях. – М.: Альварес Пабблишинг, 2003, 2004.

46. Агеев С. А., Саенко И. Б. Управление безопасностью защищенных мультисервисных сетей специального назначения // Труды СПИИРАН. 2010. № 2 (13). С. 182-198.

47. Будко П. А., Чихачев А. В., Баринев М. А., Винограденко А. М. Основные направления организации и планирования телекоммуникационной среды сил специального назначения // Научные исследования в космических исследованиях Земли. 2013. Т. 5. № 4. С. 18-23.

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. Гольдштейн Б. С., Соколов Н. А. Потенциальные угрозы для сетей специального назначения // Вестник связи. 2015. № 1. С. 28-31.

50. Гольдштейн Б. С., Пинчук А. В., Соколов Н. А. Минимизация рисков устойчивости функционирования современных ССН // Вестник связи. 2015. № 6. С. 49-51.

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. Гольдштейн Б. С., Пинчук А. В., Соколов Н. А. Минимизация рисков устойчивости функционирования современных ССН // Вестник связи. 2015. № 7. С. 17-18.

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 13.06.2017).

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 «Системпром», 2013. С. 7-9.

61. 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).

62. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. – СПб.: Наука и техника, 2004. – 336 с.

63. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-69. – URL: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf> (дата обращения: 10.10.2017).

64. Буренин А. Н., Легков К. Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Научные технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 46-61.

References

1. Barashkov P. N., Rodimov A. P., Tkachenko K. A., Chudnov A. M. *Model' sistemy svyazi s upravlyaemyimi strukturami v konfliktnykh usloviyakh* [Model of communication system with controlled structures in conflict settings]. Leningrad, Military Communications Academy, 1986. 52 p. (in Russian).
2. Lialyuk I. N. *C4I: sistemy svyazi, 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 svyazi 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., Rismann O. V. *Mnogourovnevnyy sintez informacionno-telekommunikatsionnykh 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 postroyeniya telekommunikatsionnykh setey* [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, identifikatsii i upravleniya transportnymi telekommunikatsionnymi setyami dlya dostizheniya maksimal'noy 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 pokazateley kachestva funkcionirovaniya uzlovogo oborudovaniya i strukturno-setevykh parametrov setey svyazi sleduyushchego pokoleniya* [The Models and the Methods of Measuring of Quality Indicators of Nodal Equipment Functioning and Network Structural Parameters of Next Generation Networks]. Krasnoyarsk, 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 sviazi 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 puppose 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. Kontseptsii 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. *Sovremennye infokommunikatsionnye sistemy i seti spetsial'nogo naznachenii. 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 sviazi 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 sviazi spetsial'nogo naznachenii. 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 sviazi 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 trebovaniiam 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 elektrosviazi 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. Shneps-Shneppe M. A. *Telekommunikatsii Pentagona: tsifrovaia transformatsiia i kiberzashchita* [Telecommunications Pentagon: digital transformation and cyber defence]. Moscow, Goriachaia liniia – Telekom Publ., 2017. 272 p. (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. Olifer V. G., Olifer N. A. *Komp'uternye seti. Printsipy, tekhnologii, protokoly* [Computer network. Principles, technologies, protocols]. Saint-Petersburg, Piter Publ., 2010. 945 p. (in Russian).

43. Gordienko V. N., Tveretskii M. S. *Mnogokanalnye telekommunikatsionnye sistemy* [Multichannel telecommunication systems]. Moscow, Goriachaia Linia – Telekom Publ., 2013. 397 p. (in Russian).

44. Krukhmalev V. V., Gordienko V. N., Mochenov A. D., Ivanov V. I., Burdin V. A., Kryzhanovskii A. V., Marykova L. A. *Osnovy postroeniia telekommunikatsionnykh sistem i setei* [Fundamentals of telecommunication systems and networks]. Moscow, Goriachaia Linia - Telekom, 2004. 510 p. (in Russian).

45. Sokolov N. A. *Telekommunikatsionnye seti. Monografiia v 4-kh chastiakh* [Telecommunication networks. Monograph in 4 volumes]. Moscow, Alvares Publishing, 2003, 2004. (in Russian).

46. Ageev S. A., Saenko I. B. Security management of protected multi-service networks for special purposes. *SPIIRAS Proceedings*, 2010, vol. 13, no. 2, pp. 182-198 (in Russian).

47. Budko P. A., Chikhachev A. V., Barinov M. A., Vinogradenko A. M. Main direction of the organization and planning of strongly connected telecommunication environment of forces of a special purpose. *H&ES Research*, 2013, vol. 5, no. 4, pp. 18-23 (in Russian).

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

49. Goldshtein B. S., Sokolov N. A. Potentsial'nye ugrozy dlia setei spetsial'nogo naznacheniiia [Potential threats to networks of a special purpose]. *Vestnik sviazi*, 2015, no. 1, pp. 28-31 (in Russian).

50. Goldshtein B. S., Pinchuk A. V., Sokolov N. A. Minimizatsiia riskov ustoichivosti funktsionirovaniia sovremennykh SSN [Minimization of risks of stability of functioning of a modern special purpose network]. *Vestnik sviazi*, 2015, no. 6, pp. 49-51 (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, sviaz' 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 svyazi gruppировки 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. Goldshtein B. S., Pinchuk A. V., Sokolov N. A. Minimizatsiia riskov ustoichivosti funktsionirovaniia sovremennykh SSN [Minimization of risks of stability of functioning of a modern special purpose network]. *Vestnik svyazi*, 2015, no. 7, pp. 17-18 (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 sovmestnogo ispol'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. Gavrillov 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 2017) (in Russian).

60. Kobozev Iu. N. Perspektivy razvitiia sistem svyazi 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 naznacheniiia»* [Proceedings of All-Russian Scientific Conference "Telecommunications and Communication in Management Information Systems"], vol. 4, Moscow, JSC "Concern "Sistemprom", 2013, pp. 7-9 (in Russian).

61. 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).

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

63. Makarenko S. I. Prospects and Problems of Development of Communication Networks of Special Purpose. *Systems of Control, Communication and Security*, 2017, no. 2, pp. 18-69. Available at: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf> (accessed 10 October 2017) (in Russian).

64. Burenin A. N., Legkov K. E. Security issues infocommunication systems and networks for special purposes: the main threats, the ways and means of ensuring comprehensive network security. *H&ES Research*, 2015, vol. 7, no. 3, pp. 46-61 (in Russian).

Статья поступила 10 октября 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: сети и системы связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

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

Descriptive Model of Special Communication Network

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. Therefore, the analysis of the current state of CNSP and creation of its descriptive model are relevant. **The aim of this paper** is the development of the descriptive model of CNSP. The descriptive model of CNSP is based only open sources. **Results and their novelty.** New elements of the model of CNSP take into account the main trends of communication evolution, basic protocols, information technologies and network structure. The analysis showed that modern CNSP moving to a decentralized network structure that is more in line with modern requirements to netcentric 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 information technologies widely used in CNSP instead specialized communication protocols too. **Practical significance.** The descriptive model of CNSP is presented in the paper is useful technical professionals for the justification of new technological solutions in the field of CNSP.

Key words: communication system, network communication, communication network of special purpose, network protocols, military communications system, sustainability communications, electronic warfare, information technology, NGN, communication control 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: telecommunication network; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

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