А.Ю. Гребешков

Управление сетями электросвязи по стандарту TMN

Рекомендовано
Пленумом совета учебно-методического объединения
по образованию в области телекоммуникаций
в качестве учебного пособия для студентов,
обучающихся по специальности 200900
«Сети связи и системы коммутации»

МОСКВА
РАДИО И СВЯЗЬ
2004

УДК 621.395

Рецензент : *зам. директора Самарского филиала ОАО «ВолгаТелеком» – директор Технического центра электросвязи Сазер А.И.*

Гребешков А.Ю. Управление сетями электросвязи по стандарту TMN: Учеб. пособие.– М.: Радио и связь, 2004 г. – 155 с.: ил.
ISBN 5-256-01730-6.

В книге рассматриваются вопросы управления современными сетями связи на основе построения сети управления электросвязью TMN (Telecommunication Management Network), стандартизованной в рекомендациях МСЭ-Т серии М.3000. В книге приводится базовая информация по структуре и особенностям протокола CMIP. Дополнительно рассмотрены основные функции, структура и особенности применения протокола SNMP. Приведён обзор платформ и продуктов сетевого управления производства компаний Siemens, Compaq, Hewlett-Packard. Дан список литературы для углублённого изучения основ управления сетями связи.

Пособие предназначено для студентов специальности 200900, аспирантов, работников отрасли «Связь», интересующихся вопросами управления телекоммуникациями.

Таб. 16. Ил.37. 2 прил. Библиогр.: 43 назв.

ISBN 5-256-01730-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Оказание услуг электросвязи неразрывно связано с вопросами комплексного управления сетями связи. Цель управления – обеспечение заданного уровня качества оказания услуг и функционирования сетей связи. Основная задача управления сетью состоит в реализации целенаправленного воздействия (мониторинг, контроль, администрирование) на оборудование связи с помощью средств автоматизации и информатизации. Наиболее эффективно задачу управления сетями электросвязи можно решить, основываясь на концепции *сети управления электросвязью* (telecommunication management network, TMN).

Актуальность применения TMN обусловлена внедрением новых, мультимедийных услуг связи, возросшей интенсивностью трафика на сетях, усложнением архитектуры и топологий сетей. В этих условиях требуется инструментарий, позволяющий контролировать работу любых сетевых средств и систем в реальном масштабе времени. Необходимо применять системы и платформы TMN, которые позволяют управлять сетями связи по единым принципам, вне зависимости от технологических особенностей оборудования и систем связи различных типов.

Предметом данного учебного пособия является рассмотрение вопросов, связанных с современными подходами к управлению сетями электросвязи. Рассматриваются основные принципы управления сетями электросвязи, стандарты управления, используемые информационные технологии и протоколы. Приводятся примеры практической реализации систем и платформ управления сетями связи.

1. ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ СЕТЯМИ ЭЛЕКТРОСВЯЗИ

1.1 Характеристика предмета изучения

В настоящее время мировая телекоммуникационная индустрия претерпевает революционные изменения. Постоянное развитие телекоммуникационных технологий, появление новых средств связи ставит перед операторами сетей и провайдерами телекоммуникационных услуг сложные задачи в части поддержания нормативного качества оказания услуг связи и функционирования сетей.

За последние годы структура телекоммуникационных сетей стала более сложной и многоплановой. Наряду с традиционными аналогово-цифровыми телефонными сетями связи бурно развиваются новые цифровые сети связи с коммутацией пакетов на основе технологий Frame Relay, ATM, MPLS. Повсеместное применение протокола IP и развитие сети Интернет сделало возможным появление на рынке IP-телефонии и других телематических служб. Развитие транспортных сетей со скоростью передачи данных от 2 Мбит/сек до 256 Гбит/сек повлекло за собой развитие сетей высокоскоростного абонентского доступа как на базе традиционной технологии ЦСИС, так и с использованием технологий семейства DSL (ADSL, XDSL, SDSL, HDSL). В подвижной радиосвязи начинается переход к сетям связи 3-го поколения на базе стандартов UMTS и CDMA.

В итоге, сети связи становятся *гетерогенными* т.е. включающими множество типов оборудования связи, поддерживающих различные стандарты и протоколы передачи информации. Требуется поддерживать заданный уровень качества связи для различных категорий пользователей. Неизбежно возникает необходимость автоматизации контроля, мониторинга и управления разнородным оборудованием и системами связи на основе единых принципов. Для выполнения указанной задачи оператор связи должен иметь центр управления сетями и/или услугами связи, который позволяет ему реализовывать следующие функции :

- быстро внедрять новые услуги связи для приобретения новых клиентов и получения дополнительных источников доходов;

- поддерживать нормативное качество обслуживания клиентов, включая минимизацию времени восстановления оборудования после сбоев или отказов;
- обеспечивать круглосуточную техническую поддержку пользователей;
- снижать затраты на эксплуатацию сети при разумном соотношении «стоимость/производительность/надёжность».

Для решения задачи интегрированного управления Международный союз электросвязи предлагает использовать концепцию сети управления электросвязью TMN. Сеть TMN есть «… специальная сеть, обеспечивающая управление сетями электросвязи и их услугами путём организации взаимосвязи с компонентами различных сетей электросвязи на основе единых интерфейсов и протоколов, стандартизованных МСЭ-Т» [18,19]. Применение TMN предполагает комплексный подход к управлению сетями связи, начиная с управления бизнесом оператора и услугами связи (верхний уровень управления) и заканчивая управлением отдельным устройством или элементом сети (нижний уровень управления). В совокупности с организационно–техническими решениями и современными информационными технологиями на базе TMN появляется возможность контролировать процесс оказания услуг связи, воздействовать на рабочие характеристики оборудования и систем связи. Для этого используются функциональные элементы TMN со стандартизованными интерфейсами взаимодействия и подключения.

Под *функциональным элементом* понимается компонент TMN, который выполняет определённую функцию, например функцию мониторинга характеристик коммутационного оборудования, функцию сети передачи данных, функцию отображения информации управления для администрации связи. В рамках TMN предусматривается техническая возможность целенаправленного воздействия на характеристики оборудования, например установка порога перегрузок, изменение характеристик абонента, блокировка направления связи, перенаправление нагрузки и т.п.

Согласно рекомендациям МСЭ-Т серии М.3ххх (см. Приложение 1), TMN имеет интерфейсы с телекоммуникационной сетью в обусловленных точках стыка. Эти интерфейсы используются для обмена информацией

управления, предоставления услуг управления, а также для приёма-передачи управляющих команд между системой управления и оборудованием связи [13,15,24].

В сферу управления TMN попадают практически все существующие в настоящее время виды сетей и систем связи, разнообразные типы телекоммуникационного оборудования:

- сети связи общего пользования и выделенные сети;
- оборудование систем передачи (мультиплексоры, кросс-коннекторы, каналообразующее оборудование и т.д.);
- линии связи (медные и волоконно-оптические кабельные системы, радиорелейное оборудование, спутниковое каналообразующее оборудование);
- программное обеспечение оборудования связи;
- аппаратное обеспечение вычислительных комплексов;
- цифровые и аналоговые коммутаторы ТФОП и других сетей связи;
- сети передачи данных, сети связи с коммутацией пакетов, включая информационно-вычислительные сети (локальные и глобальные);
- сама сеть TMN (т.е. управление сетью TMN);
- системы сигнализации, в т.ч. ОКС№7 [4];
- телематические службы и телесервисы;
- учрежденческие АТС (УАТС),
- учрежденческо–производственные АТС (УПАТС);
- пользовательские терминалы ЦСИС;
- программное обеспечение, необходимое для предоставления телекоммуникационных услуг (например услуги интеллектуальных сетей);
- прикладное программное обеспечение (ПО) вычислительных систем;
- системы электропитания, инженерного обеспечения (системы безопасности, пожаротушения, системы кондиционирования воздуха и т.д.).

Управление Взаимоувязанной сетью связи Российской Федерации также основано на концепции TMN [3]. Основы организации управления ВСС РФ изложены в следующем разделе.

1.2 Организация управления ВСС Российской Федерации

В определении понятия Взаимоувязанной сети связи, ВСС указано, что «Взаимоувязанная сеть связи Российской Федерации - это комплекс технологически сопряжённых сетей электросвязи на территории Российской Федерации, обеспеченный общим централизованным управлением». Применительно к ВСС РФ, управление сетями связи на практике реализуется с помощью создания автоматизированной системы управления согласно руководящего документа *РД 45.174-2001 «Построение систем управления сетями связи операторов ВСС РФ»* [20]. Управление электросвязью является одной из важнейших организационно-технических задач, согласно «Концепции развития Взаимоувязанной сети связи Российской Федерации» [3,18,19].

Внедрение централизованного сетевого управления в России, как и во всём мире, сегодня затруднено. Сложности внедрения единого сетевого управления в рамках национальной сети России определяются следующими факторами [7]:

- разнообразие типов телекоммуникационного оборудования, эксплуатируемого на сетях операторов связи,
- использование различных средств технической эксплуатации и обслуживания;
- применение на сетях связи значительного числа устаревших электромеханических систем коммутации, изначально не приспособленных для стандартного подключения к сети TMN;
- отсутствие на узлах связи встроенных средств контроля, мониторинга и удаленного взаимодействия с системой управления;
- отсутствие у операторов связи достаточных финансовых средств на приобретение дорогостоящих программно-аппаратных платформ сетевого управления.

Тем не менее, при внедрении современного комплекса сетевого управления TMN, даже при наличии «трудно управляемого» устаревшего оборудования, оператор связи получает следующие преимущества:

- повышается качество услуг связи и уровень технического обслуживания сети;
- оперативно обнаруживаются и устраняются неисправности и отказы;
- снижаются эксплуатационные расходы и появляются дополнительные доходы за счёт предоставления качественно новых услуг [14], а это создает предпосылки для дальнейшего расширения и модернизации сети;
- оператор связи может контролировать альтернативных операторов, пользующихся той же сетью связи на правах присоединения;
- оператор связи может контролировать техническое состояние и работоспособность как отдельных узлов, так и всей сети в режиме реального времени;
- оператор связи получает возможность контролировать абонентские линии и управлять потоками вызовов, анализировать трафик, а также принимать обоснованные решения по вопросу номенклатуры услуг, ценообразования, обслуживания сети.

Некоторые из перечисленных возможностей были частично реализованы при создании в 1980-1990-х *годах центров технической эксплуатации оборудования* (ЦТЭ) сетей связи. Создание ЦТЭ позволило накопить достаточный практический опыт и усовершенствовать технологию удалённого контроля и управления телекоммуникационным оборудованием [10,11,21]. Однако ЦТЭ позволяют решить только часть задач TMN, например централизованный контроль неисправностей и обновление программного обеспечения узлов связи.

В основе организации управления ВСС РФ лежат следующие принципы:

- интеграция функциональных, физических и информационных структур управления;
- создание гибкой архитектуры управления на основе методологии открытых систем, обеспечивающей возможность реконфигурации и

развития автоматизированной системы управления (АСУ) сетями электросвязи;

- стандартизация компонентов системы управления;
- повышение уровня автоматизации процессов управления;
- применение новейших информационных технологий.

Как уже говорилось, в качестве теоретической базы для построения системы управления ВСС принята концепция построения сети управления электросвязью TMN, которая в общем виде изложена в Рек. МСЭ-Т М.3010 [26]. Этот подход представляет методологическую основу для реализации интегрированного управления сетями электросвязи, различающимися по структуре, составу и объему передаваемой информации.

В целом под *системой управления сетью электросвязи* понимается «система, выполняющая функции по управлению сетью на основе комплекса информационных технологий по планированию, техническому обслуживанию, эксплуатации, оперативному и административному управлению сетями и предоставляемыми услугами» [18].

Организационно каждая *система управления сетями* (СУС) оператора представляет собой территориально-разнесенную иерархическую структуру, построенную в соответствии с принципами TMN. Топология сетей управления в пределах зоны ответственности оператора, размещение *центров управления* (ЦУ), число уровней иерархии совокупно определяется в соответствии с особенностями управляемых сетей, их назначением**,** размерами, разветвленностью, организацией технических средств.

Минимальное число уровней иерархии управления – два:

- на нижнем уровне находятся *центры управления элементами сети* (ЦУ-ЭС), осуществляющие контроль и непосредственное взаимодействие с оборудованием связи;
- на верхнем уровне создаётся *центр управления сетью* (ЦУС) в целом, с возможностью управления сетями, услугами связи.

На разветвленных сетях связи, охватывающих большие территории, существуют промежуточные уровни управления. В частности, кроме центра управления сетью и услугами связи оператора на верхнем уровне и центра управления элементами на нижнем уровне иерархии, создаются еще два промежуточных уровня управления сетями (см. рис. 1.1):

- *территориальный центр управления* (ТЦУ), осуществляющий функции по управлению сетью и услугами связи в зоне, определенной администрацией связи под контролем ЦУС;
- *узловой центр управления* (УЦУ), осуществляющий управление на части выделенной территории ТЦУ в непосредственном взаимодействии с ТЦУ.

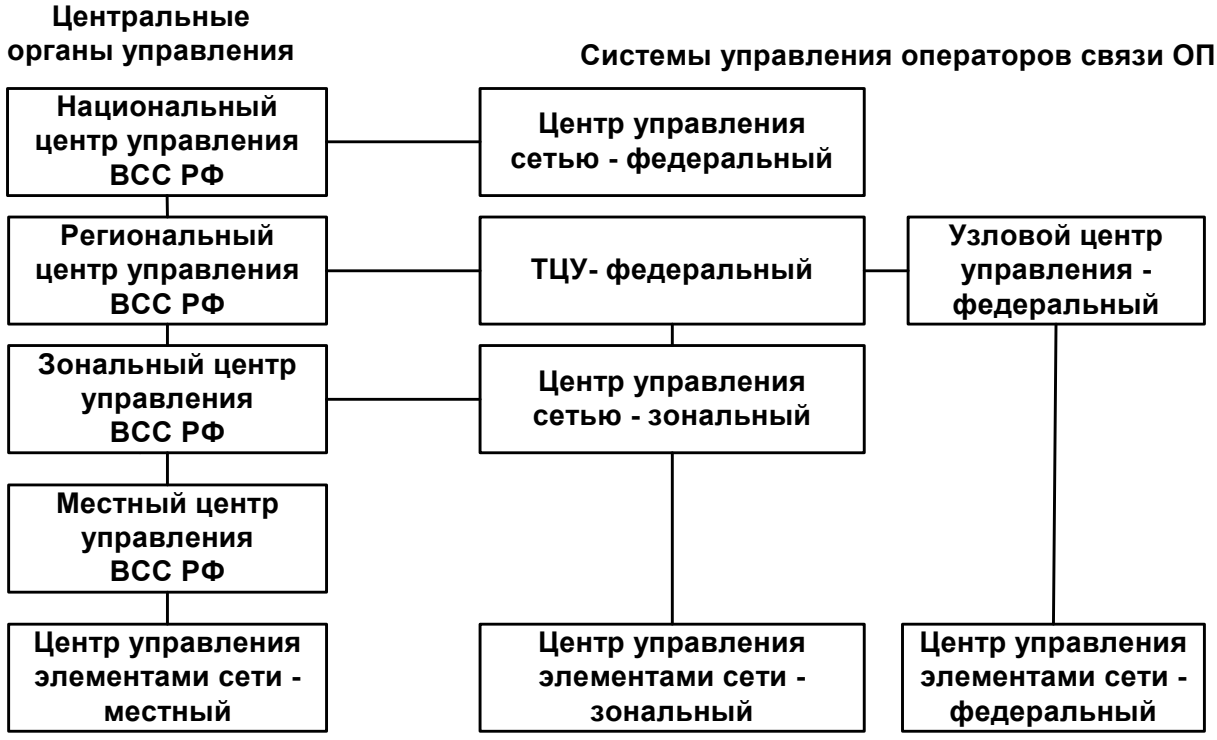


Рисунок 1.1 – Структурно-функциональная схема управления для операторов сетей общего пользования (ОП)

Системы управления зоновыми сетями должны иметь трех- или двухуровневую структуру Системы управления местными сетями, как правило, должны иметь двухуровневую структуру управления. Системы управления сетями оператора могут включать ряд подсистем управления различными видами сетей связи в зоне ответственности данного оператора. Центральные органы управления интегрируют все подчинённые системы управления в единую АСУ ВСС РФ.

В каждой СУС оператора должен быть организован многофункциональный головной ЦУС, который осуществляет контроль за состоянием сетей зоны оператора в целом, планирует развитие и предоставление услуг и сетей связи, осуществляет взаимодействие с центрами управления других операторов и центральными органами управления ВСС РФ.

Итак, структура управления ВСС РФ и операторов связи представляет собой сложную многоуровневую структуру с разнообразными функциональными связями. Создание и обеспечение работоспособности рассмотренной структуры управления требует не только организационно-технических, но управленческих решений по реорганизации управления предприятием связи (оператором) в целом. Это более высокий уровень управления, обсуждение которого выходит за рамки настоящего учебного пособия. Далее рассматриваются в основном технические аспекты организации системы управления сетями связи.

1.3 Управление в информационной инфраструктуре GII

Глобальная информационная инфраструктура (Global Information Infrastructure, GII) по своему назначению и функциям аналогична ВСС РФ [32]. Основой GII являются существующие и строящиеся телекоммуникационные системы и сети. Для предоставления услуг телекоммуникаций в GII используются многочисленные программно-аппаратные средства, которые позволяют пользователям обмениваться разными видами сообщений (речь, видео, данные) в любое время по приемлемой цене и с заданным качеством. Средства GII позволяют унифицировать процедуры предоставления доступа к услугам связи для жителей различных государств, а также организовать межсетевое взаимодействие сетей связи различных стран. Концептуально ВСС РФ является частью GII.

Инфраструктура GII включает в себя 4 основных элемента :

- *Люди*, которые являются источниками и получателями сообщений, а также используют полученную информацию.

- *Информационные устройства* (information appliances), которые используются для хранения, обработки данных и позволяют получать доступ к информации.

- *Коммуникационная инфраструктура*, которая осуществляет передачу информации между географически удалёнными информационными устройствами. Информационная инфраструктура

может быть представлена в виде транспортной сети и сети доступа.

- *Информация*, которая включает в себя видео, речь, данные, а также прикладное программное обеспечение (пользовательские приложения), которое позволяет конвертировать сообщения из оригинальной формы (голос, изображение, компьютерная графика) в электронную форму.

Взаимодействие перечисленных элементов показано на рис. 1.2.

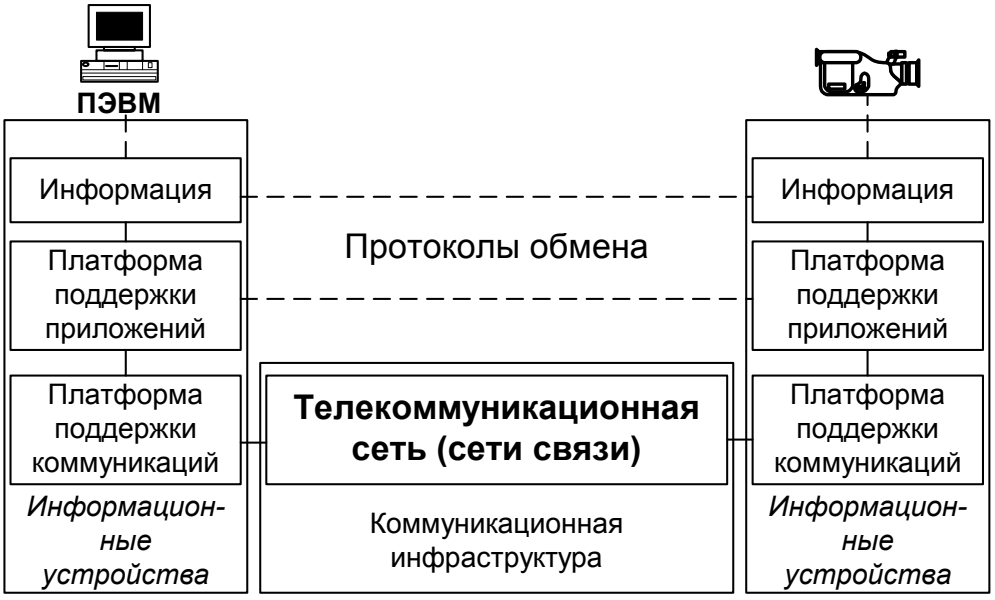


Рисунок 1.2 – Взаимодействие основных элементов GII

Примеры информационных устройств – персональный компьютер, рабочая станция в ЛВС, телефонный аппарат, телевизионный приёмник, факсимильный аппарат. В качестве *платформы поддержки приложений* могут использоваться вычислительные средства в совокупности с операционными системами, микропрограммное обеспечение информационных устройств, прикладное программное обеспечение, специализированные процессоры, кодеки.

Платформы поддержки коммуникаций – это оконечное оборудование данных, модемы, устройства и средства доступа различного назначения. Примеры средств доступа – абонентская линия связи до АТС, линия DSL-доступа, сеть кабельного телевидения, оптическая линия доступа, канал радиосвязи, спутниковый канал, линия радиодоступа. Примеры те-

лекоммуникационной сети – телефонная сеть связи общего пользования, первичная сеть связи, сеть передачи данных различных стандартов (X.25, Frame Relay, ATM, MPLS), сеть Интернет. Все перечисленные программные и аппаратные компоненты GII, а также услуги, оказываемые на их основе, являются объектами сетевого управления.

Структура GII связывает между собой в единое целое сетевые ресурсы, устройства хранения и обработки данных, а также ресурсы *промежуточного уровня* (middleware) с тем, чтобы предложить пользователям стандартные услуги и поддержать индивидуальные пользовательские приложения. К средствам middleware в рамках GII можно отнести средствам обеспечения информационной безопасности, биллинг, а также средства сетевого управления и администрирования. Общая структура услуг GII показана на рис. 1.3.

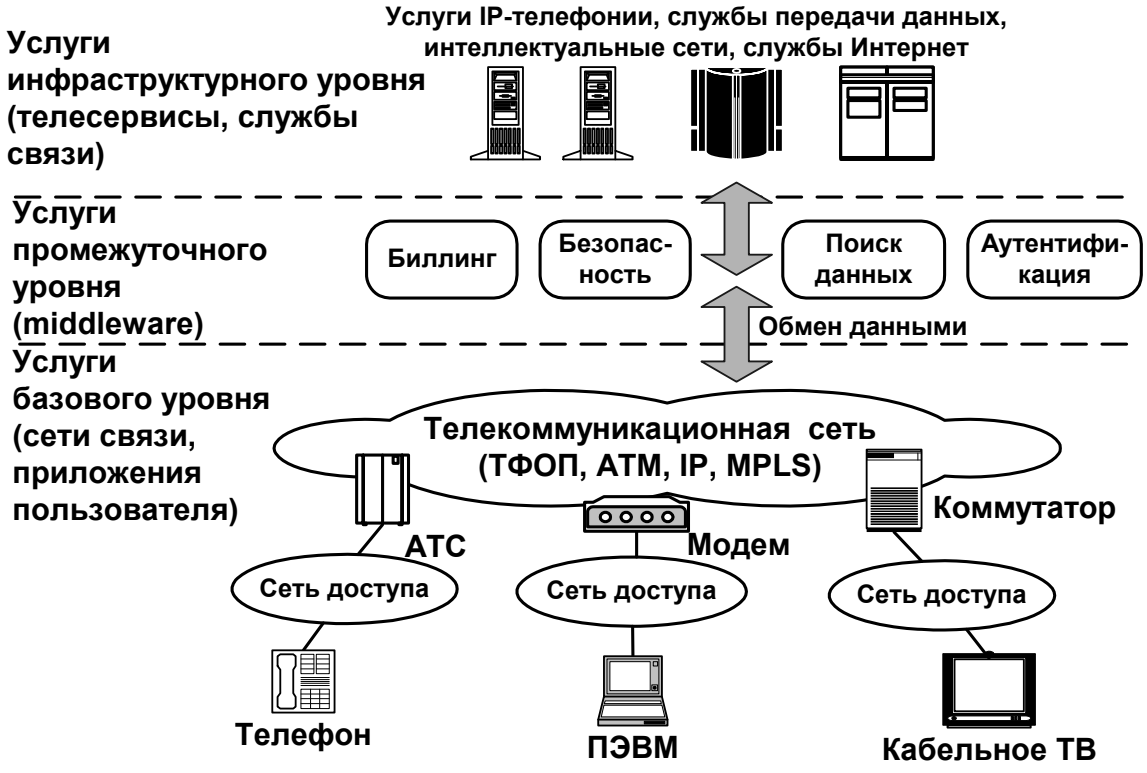


Рисунок 1.3 – Уровни услуг GII

Спектр услуг, которые предлагаются GII, достаточно широк и может динамический изменяться вместе с изменением доступных сетевых и информационных ресурсов. Поэтому целесообразно классифицировать компоненты услуг. При этом каждый компонент услуги зависит от ресурса,

необходимого для поддержки услуги. Различают следующие компоненты услуги :

Инфраструктурные компоненты услуги (infrastructural service components) – предоставляют возможности доступа к конечным информационным услугам (службам, телесервисам) для передачи речи через телефонную сеть, пересылки файлов через Интернет и т.п. Инфраструктурные компоненты могут также включать услуги компонент промежуточного и *базового (baseware)* уровня программного управления.

Компоненты услуг промежуточного (middleware) уровня – используются для обеспечения межсетевого взаимодействия и совместного функционирования нескольких приложений. Компоненты услуг промежуточного уровня позволяют объединять компоненты услуг базового уровня и добавлять функциональность, которая необходима для предоставления всего набора инфраструктурных услуг.

Существует 4 категории услуг промежуточного уровня; в рамках настоящего пособия интерес представляют категории M1 и M2.

Категория M1 – компоненты взаимодействия услуг. Обеспечивают возможность объединения в пакет ряда инфраструктурных услуг; поддерживают взаимодействие между различными элементами GII.

Категория M2 – компоненты поддержки услуг промежуточного ПО. Применяются для обеспечения коммуникационной функции GII и включают :

- Компоненты услуг человеко-машинного интерфейса.
- Компоненты услуг регистрации (пользователя).
- Компоненты услуг аутентификации.
- Компоненты услуг обеспечения информационной безопасности.
- Компоненты услуг поиска информации.
- Компоненты услуг биллинга.
- Компоненты услуг управления услугами.

Компоненты услуг базового уровня поделены между компонентами услуг сетей связи и компонентами услуг обработки и хранения данных. Соответственно, компоненты услуг связи используют сетевые ресурсы; компоненты услуг сбора и хранения информации используют ресурсы систем хранения и обработки данных.

Для базового уровня характерно функционирование услуг в реальном времени, т.е. оперативно-техническое управление оборудованием связи : установление оконечного соединения, маршрутизация вызова, коммутация каналов или пакетов, поддержка систем сигнализации. Следует отметить, что услуги базового уровня реализуются с помощью программного обеспечения управления оборудования электросвязи и не относятся к TMN. Логика управления на промежуточном уровне носит более общий характер, работает не в реальном времени, затрагивает вопросы контроля качества услуг связи, обеспечение информационной безопасности и межсетевого взаимодействия. Далее рассматриваются интерфейсы взаимодействия между функциями управления и другими функциями GII.

Под *функцией* понимается логический элемент, который выполняет заранее определённое задание в ответ на появление входного сигнала; в результате выполнения задания появляется определённый выходной сигнал или информация. Функции реализуются устройствами или компонентами устройств. Одна и та же функция, например установление исходящего соединения, может осуществляться телекоммуникационными устройствами различных видов и типов.

Логический интерфейс – это описание процедуры взаимодействия между двумя функциями, включая формат информации, которая передаётся между функциями и описание отклика на передачу информации. С точки зрения технического устройства, реализующего ту или иную функцию, отклик означает срабатывание этого устройства.

В описание логического интерфейса включается описание *протокола взаимодействия* и описание *функциональной опорной точки* (functional reference point) обмена информацией.

Функциональная опорная точка описывает требования к интерфейсу т.е. указывает, какие точно действия или операции должны быть доступны при внешнем обращении или вызове функции через интерфейс.

Протокол содержит описание входных/выходных сигналов и последовательности обмена ими. В более широком смысле под *протоколом* понимается набор правил и форматов (семантических и синтаксических), который определяет взаимосвязанное поведение логических объектов при выполнении определённых функций.

Логический интерфейс является реализацией функциональной опорной точки, т.е. логический интерфейс описывает, как именно реализуется взаимодействие с данной функцией на уровне обмена информацией.

Стык между функциями свидетельствует о наличии информационного взаимодействия на уровне протокола через соответствующий интерфейс.

Функции, функциональные опорные точки, логические интерфейсы (стыки) в совокупности составляют *функциональную модель GII*.

Разработка функциональных моделей позволяют разработчикам определить, как будет функционировать тот или иной элемент GII и какие функции этот элемент будет выполнять.

На рис. 1.4 показаны основные составляющие функциональной модели. Подразумевается, что функции взаимодействуют через логический интерфейс.

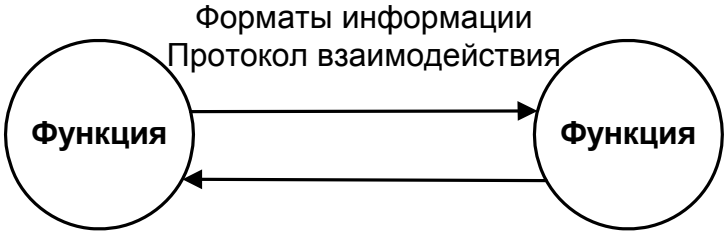


Рисунок 1.4 – Функциональная модель

По *форматом информации* на рис. 1.4 понимается способ кодировки данных в том или ином протоколе, например CORBA IDL, HyperText Markup Language (HTML), способы цифрового кодирования речи и сжатия/оцифровки видеоизображения.

В GII существуют следующие виды функций :

Функции приложений (applications functions, AF) – описание прикладных задач пользователя, в частности, прикладных задач управления.

Функции промежуточного уровня (middleware functions, MF) – описание задач, которые решаются следующими функциями прикладного уровня:

- *Функции контроля услуг* (service control functions, SCF) – функции промежуточного уровня, которые позволяют создавать услуги из

отдельных компонент и сетевых ресурсов; здесь же присутствуют функции контроля за взаимодействием пользователя и услуги.

- *Функция управления* (management functions, ManF) – эта функция реализует задачи управления всеми другими функциями.

Функции базового уровня (baseware functions, BF) позволяют функционировать прикладным функциям и функциям промежуточного уровня, обмениваться сообщениями с другими функциями, используя для этого сетевые функции и создавать интерфейс (точки взаимодействия) с пользователями.

Существует различные типы логических интерфейсов и протоколов для организации взаимодействия между функциями (см. таблицу 1.1).

Таблица 1.1 – Назначение интерфейсов и стыков

Тип интерфейса или протокола	Назначение стыка или интерфейса
Прикладной протокол AP (Application Protocol)	Логический стык между прикладными функциями.
Прикладной программный интерфейс API (Application Programming Interface)	Логический интерфейс между прикладными функциями и функциями промежуточного уровня, которые поддерживают прикладные функции.
Протокол промежуточного уровня MP (Middleware Protocol)	Логический стык между функциями прикладного уровня.
Базовый программный интерфейс BPI (Basic Programming Interface)	Логический интерфейс между функциями промежуточного уровня и функциями базового уровня, которые поддерживают функции промежуточного уровня (часто эти интерфейсы относятся к API).
Интерфейс человек–компьютер или человеко–машинный интерфейс HCI (Human-Computer Interface)	Логический интерфейс между пользователем и, главным образом, функциями базового уровня; это не исключает возможности человеко–машинного интерфейса к функциям промежуточного уровня и к прикладным функциям.
Опорная точка сетей связи TRP (Telecommunications Reference Point)	Логический интерфейс между функциями базового уровня и функциями сети связи.

На рис. 1.5 на следующей странице показаны функции управления различного уровня GII, взаимодействующие через соответствующие интерфейсы.

Интерфейсы 1,9 – соответствуют опорным точкам транспортных функций, которые «прозрачны» для других элементов, включая прикладные протоколы, протоколы промежуточного уровня, средства контроля (оперативного управления) функциями базового уровня и *функциями сетевого контроля* (network control functions).

Интерфейс 2 – соответствует опорным точкам транспортных функций, которые обеспечивают обмен информацией между функциями сетевого контроля и функциями базового уровня.

Интерфейс 3 – соответствует опорным точкам транспортных функций, которые «прозрачны» для всех типов протоколов.

Интерфейс 4 – опорная точка между функцией базового уровня и функциями оперативного управления сетью (контроль сети). Интерфейс 4 позволяет предоставлять услуги связи и независимо от технических средств реализации транспортной функции.

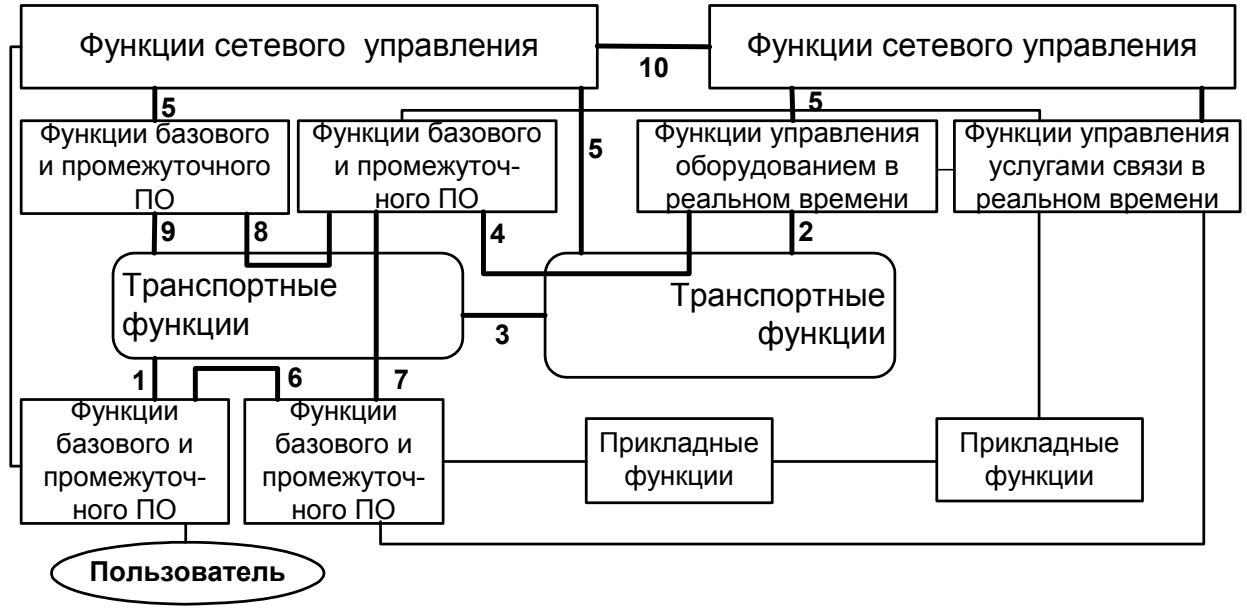


Рисунок 1.5 – Примеры функций и логических интерфейсов в GII

Интерфейс 5 – опорная точка сетевого управления. Имеет множество реализаций, осуществляет управление в целом всеми функциями, не зависит от транспортной функции.

Интерфейсы 6,7,8 – реализуются с помощью протоколов промежуточного уровня, которые передаются с помощью сетевой функции.

Интерфейс 10 – протокол *сетевого управления* (management protocol), который осуществляет обмен данными между функциями сетевого управления.

В функциональной модели GII обозначены опорные точки и соответствующие интерфейсы управления. При этом функции управления распределены между функциями базового и промежуточного программного обеспечения. В то же время необходимо организовать взаимодействие между функциями управления и транспортными функциями, т.к. в противном случае будет потеряна управляемость транспортной (телекоммуникационной) сетью связи. Для реализации задач сетевого управления в рамках ВСС, как составной части GII, необходимы опорные точки и интерфейсы различного назначения, которые позволяют реализовать следующие виды взаимодействия :

- взаимодействие между функциями GII;
- взаимодействие пользователя и GII;
- взаимодействие между различными функциями управления.

Описание реализации перечисленных функций, опорных точек и интерфейсов в рамках концепции TMN приводится в главах 2 и 3.

Контрольные вопросы к главе 1.

1. Какие функции реализует центр управления сетями связи?
2. Дайте определение сети управления электросвязью TMN.
3. Какое оборудование связи управляется с помощью TMN?
4. Какие преимущества получает оператор связи при реализации TMN?
5. Что понимается под «системой управления сетью электросвязи»?
6. Какую организационную структуру имеет система управления сетью электросвязи ВСС РФ?
7. В чём основное назначение Глобальной информационной инфраструктуры?
8. Дайте определение понятиям «функция», «логический интерфейс».

2. СЕТЕВОЕ УПРАВЛЕНИЕ ПО СТАНДАРТУ TMN

2.1 Состав и назначение основных элементов TMN

Термин «Сеть управления электросвязью» (Telecommunication Management Network, TMN) введен МСЭ-Т с 1992 г. Общие положения концепции TMN определены в Рек. МСЭ-Т М.3010. Концепция TMN основана на базовых принципах управления открытыми системами. Согласно Рек. МСЭ–Т М.3010, TMN является самостоятельной сетью, «надстройкой» над традиционной сетью электросвязи. Сеть TMN обеспечивает управление, оперативный контроль (мониторинг) и автоматизированную эксплуатацию телекоммуникационного оборудования (см. рис. 2.1). Сеть TMN используется для управления услугами сетей связи, для администрирования сетевыми устройствами в целях обеспечения нормативного качества оказания услуг связи и безопасности связи [7,13,15,24].

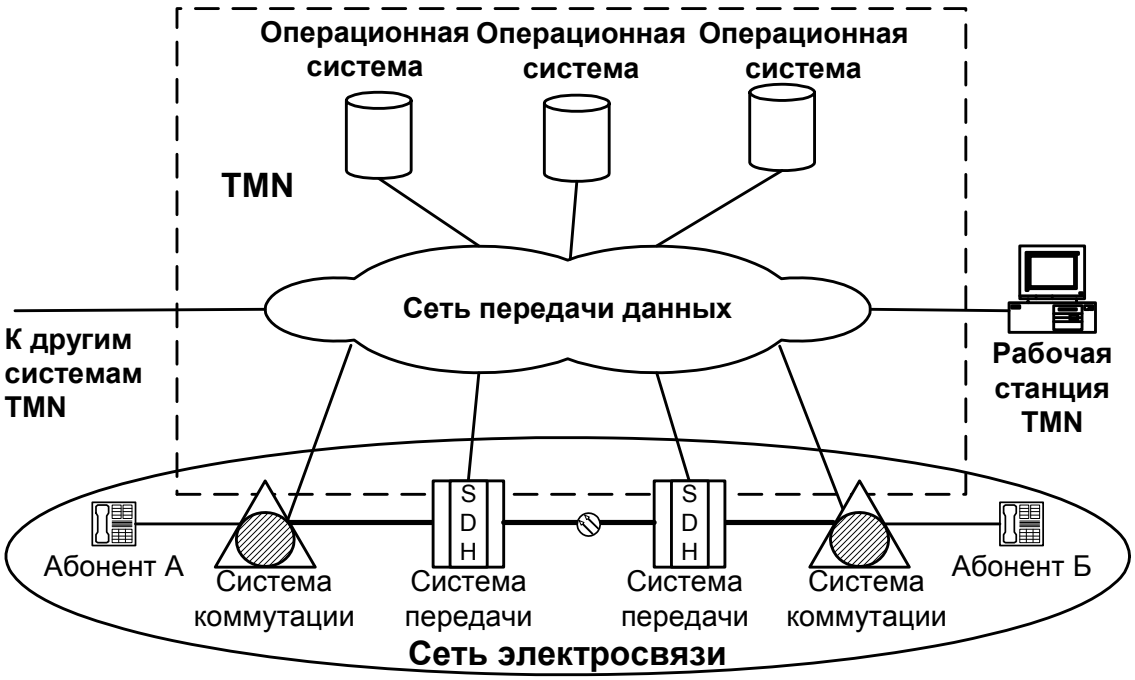


Рисунок 2.1 – TMN и сеть электросвязи (согласно Рек. МСЭ-Т М.3010)

Объектом управления сети TMN являются *телекоммуникационные или сетевые ресурсы*. Телекоммуникационные ресурсы управления физически представляют собой оборудование связи – стативы, функцио-

нальные блоки, модули, программное обеспечение управления – на определённые свойства и характеристики которых можно осуществлять целенаправленное управляющее воздействие. Например, можно с помощью изменения станционных данных запрещать организацию обходных направлений связи через определённый узел, повышать уровень допустимых потерь в направлении, административно блокировать доступ абонента к услугам связи. При управлении по стандартам TMN оборудование связи обычно называется *элементом сети* (network element, NE*)* или *сетевым элементом*.

Сеть TMN предоставляет оператору связи *услуги управления сетями электросвязи* (management service). Услуги управления определяются как решения, предлагаемые TMN для удовлетворения потребностей оператора в сетевом управлении. Услуга управления в TMN состоит из множества компонентов, причём самая элементарная из этих компонентов, например генерация сообщения о неисправности (отказе), определяется как *функция управления* (management function). Сеть TMN предоставляет оператору связи множество функций управления телекоммуникационными сетями и услугами, обеспечивая обмен информацией в процессе управления. Обмен *информацией управления* (management information) предусматривает прежде всего выдачу команды управления, выполнение команды, передачу в систему управления результатов выполнения команды.

Обмен командами управления и иной информацией между TMN и оборудованием связи осуществляется через опорные точки, которые реализуются в виде стандартизованных или нестандартизованных МСЭ-Т интерфейсов TMN.

Для передачи сигналов и команд управления, TMN подключается к оборудованию электросвязи по *сети передачи данных* (data communication network, DCN). Сеть DCN реализует транспортные уровни сети TMN согласно семиуровневой эталонной модели взаимосвязи открытых систем (ВОС). Функции прикладного уровня TMN реализуются с помощью одной или нескольких *операционных или управляющих систем* (operations systems, OS).

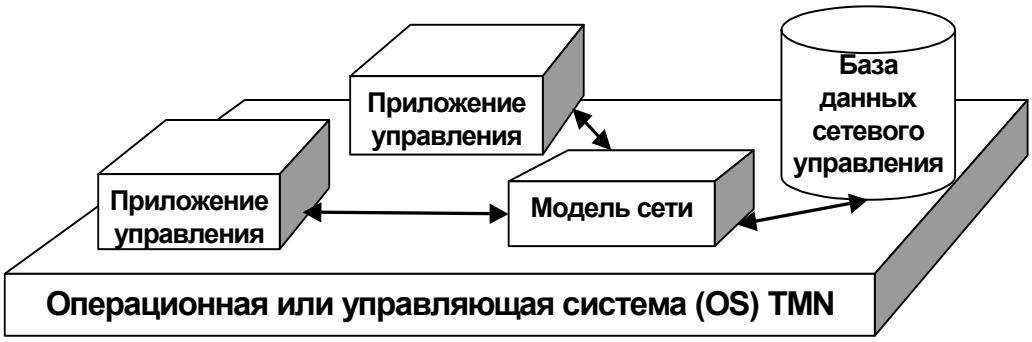


Рисунок 2.2 – Операционная система в TMN

В первую очередь, операционные системы (см. рис. 2.2) обеспечивают поддержку обработки данных, поступающих от управляемой сети электросвязи. Эта обработка осуществляется в целях мониторинга и контроля функционирования телекоммуникационного оборудования, а также для обеспечения работы собственно сети TMN. Операционная система поддерживает информационную модель сети электросвязи.

Информационная модель сети электросвязи представляет собой логическое описание физических объектов электросвязи с использованием принятой информационной технологии и специальных программных средств, например систем управления базами данных (СУБД). База данных сетевого управления – совокупность определённым образом организованных данных системы управления и связей между данными. Операционные системы обеспечивают управление вычислительными программами и функционирование прикладных программных средств управления (*приложений управления*), которые, собственно, и реализуют большинство услуг и функций управления. Функции управления могут выполняться непосредственно человеком-оператором или осуществляться приложением управления в автоматическом режиме. Кроме того, OS обеспечивает поддержку терминалов пользователя, форматирование данных, распределение машинных ресурсов между приложениями управления.

Выполнение некоторых функций управления может обеспечиваться несколькими операционными системами. В этом случае сеть передачи DCN используется для обмена информацией между различными OS. С помощью DCN данная система сетевого управления может взаимодействовать с другими TMN. Сеть DCN также используется для соединения между *рабочими станциями* (work stations, WS) и операционными систе-

мами, что позволяет операторам и администраторам получать и интерпретировать информацию по управлению с помощью человеко-машинных интерфейсов. Рабочие станции имеют графические человеко-машинные интерфейсы, чьи характеристики соответствуют требованиям рекомендаций МСЭ–Т Z.300; детальное определение такого интерфейса находится вне рамок рекомендаций МСЭ–Т по TMN. Рабочая станция WS поддерживает язык общения «человек-машина» и обладает возможностями обработки данных, средствами ручного и автоматического ввода-вывода информации.

Основные положения концепции TMN стали результатом длительного исследовательского процесса. Исследования по TMN были начаты в 1985 г. IV исследовательской группой МККТТ (ныне – МСЭ-Т). Первая рекомендация TMN имела код M.30 и была издана в 1988 г. В 1992 г. появилась полностью пересмотренная версия данной рекомендации, и её номер был изменен на M.3010. Эта версия вновь претерпела изменения в 1996–2000 г.г. Большое количество рекомендаций TMN было разработано МСЭ-Т для управления цифровыми сетями с интеграцией служб ЦСИС (ISDN). Европейский институт по стандартизации телекоммуникаций (European Telecommunication Standards Institute, ETSI), в свою очередь, разработал ряд спецификаций отдельных элементов TMN, в частности интерфейса Q.3 для управления первичными сетями синхронной цифровой иерархии SDH.

2.2 Функции и архитектуры TMN

2.2.1 Функциональные возможности TMN

Сеть TMN обладает следующими функциональными возможностями [26,28]:

- способность производить обмен информацией управления между сетями связи и TMN;
- способность преобразовывать информацию управления для различных систем связи в единый формат с целью обеспечения совместимости и согласованности данных в сети TMN;

- способность передавать информацию управления между различными компонентами сети TMN;
- способность анализировать и предсказуемо реагировать на поступающую информацию управления;
- способность преобразовывать информацию управления в форму, которая понятна пользователю системы управления – оператору или администратору, что достигается с помощью дружественного взаимодействия с пользователями посредством графического отображения информации;
- возможность обеспечения защищённого доступа к информации управления.

Сеть TMN обеспечивает возможности по управлению в 5 функциональных областях, которые рассматриваются далее.

Управление конфигурацией (configuration management), включает следующие функции управления :

- планирование и проектирование сетей, управление установкой оборудования, ввод в эксплуатацию;
- контроль наличия и функционирования оборудования систем и сетей связи (соответствие паспортным данным, доступность оборудования для эксплуатации);
- обеспечение запасными частями и резервными комплектами оборудования.

Управление неисправностями или последствиями отказов (fault management) включает следующие функции управления ::

- сбор и обработка сообщений о неисправностях;
- локализация неисправности.
- устранение повреждения или неисправности;
- тестирование и повторный ввод в эксплуатацию;
- проведение планово-предупредительных мероприятий.

Управление расчетами за услуги связи (account management), включает следующие функции управления :

- сбор сведений об оказанных услугах связи (файлы с данными о соединениях, импульсные счетчики);
- поддержание и сохранение протарифицированных данных.

Управление надежностью и безопасностью (security management) включает следующие функции управления :

- разграничение и контроль доступа к элементам сети и компонентам TMN;
- аудит действий операторов;
- генерация и обработка сообщений о повреждениях (неисправностях) системы TMN;
- восстановление (программное и аппаратное) оборудования сетей и систем связи.

Управление возможностями (рабочими характеристиками) сетей связи (performance management) включает следующие функции управления

- отслеживание и сбор данных о функционировании сети;
- перемаршрутизация трафика, динамическое управление;
- анализ показателей функционирования сети во времени (trend analysis).

Существует несколько способов описания свойств сети TMN. Каждый способ описания соответствует определённым свойствам сети. В терминах TMN это соответствует описанию архитектуры сети TMN. Под *архитектурой TMN* понимается совокупное обозначение состава и структуры сети TMN, описание взаимного расположения компонентов сети TMN, определение способов взаимодействия компонентов TMN между собой и с внешней средой.

Рекомендация МСЭ–Т М.3010 определяет общие понятия концепции управления TMN и представляет несколько видов архитектуры управления :

функциональная архитектура TMN, которая описывает функции управления;

физическая архитектура TMN, которая определяет технические и программные средства реализации функций управления;

информационная архитектура TMN, которая описывает понятия TMN на основе стандартов управления ISO в рамках объектно–ориентированного подхода;

логическая многоуровневая архитектура TMN (logical layered architecture, LLA) – показывает, как управление сетью может быть структурировано в соответствии с различными потребностями администрации связи.

Архитектуры TMN далее рассматриваются более подробно.

2.2.2 Функциональная архитектура TMN

Функциональная архитектура TMN состоит из следующих основных компонентов :

Функциональные блоки (functional blocks) или блоки функций – элементарная единица функциональности TMN, которая может быть стандартизирована.

- *Функции приложений управления* (management application functions, MAF) - функции, с помощью которых предоставляются одна или несколько услуг управления. Функции MAF могут обозначаться с помощью тех функциональных блоков, в рамках которых они применяются. Как правило, в одном функциональном блоке реализуется одна функция MAF. Функции MAF являются основой для формирования услуг управления.
- *Функция управления TMN* (TMN management function, TMN MF) и *множество* функций управления TMN (TMN management function sets). Функция TMN MF обеспечивает взаимодействие между парами MAF в управляющей и управляемой системах. Функции TMN MF группируются в набор функций управления и обеспечивают взаимодействие с другой функцией MAF.
- *Опорные точки (*reference point*)* представляют собой описание требований к интерфейсам TMN. Опорные точки отражают суть взаимодействия между функциональными блоками; опорная точка позволяет определить все возможные функции, которые данный функциональный блок запрашивает у других блоков.

Функциональные блоки являются описанием функций TMN, а именно:

- функции сети передачи данных;

- функции рабочей станции;
- функции интерфейса «человек-машина»;
- функции базы данных сетевого управления;
- функции безопасности сети TMN;
- функции обмена сообщениями.

В функциональной архитектуре TMN определено четыре типа функциональных блоков. Нет необходимости, чтобы все 4 типа присутствовали в каждой возможной реализации TMN.

Существуют следующие типы функциональных блоков (см. рис. 2.3)**:**

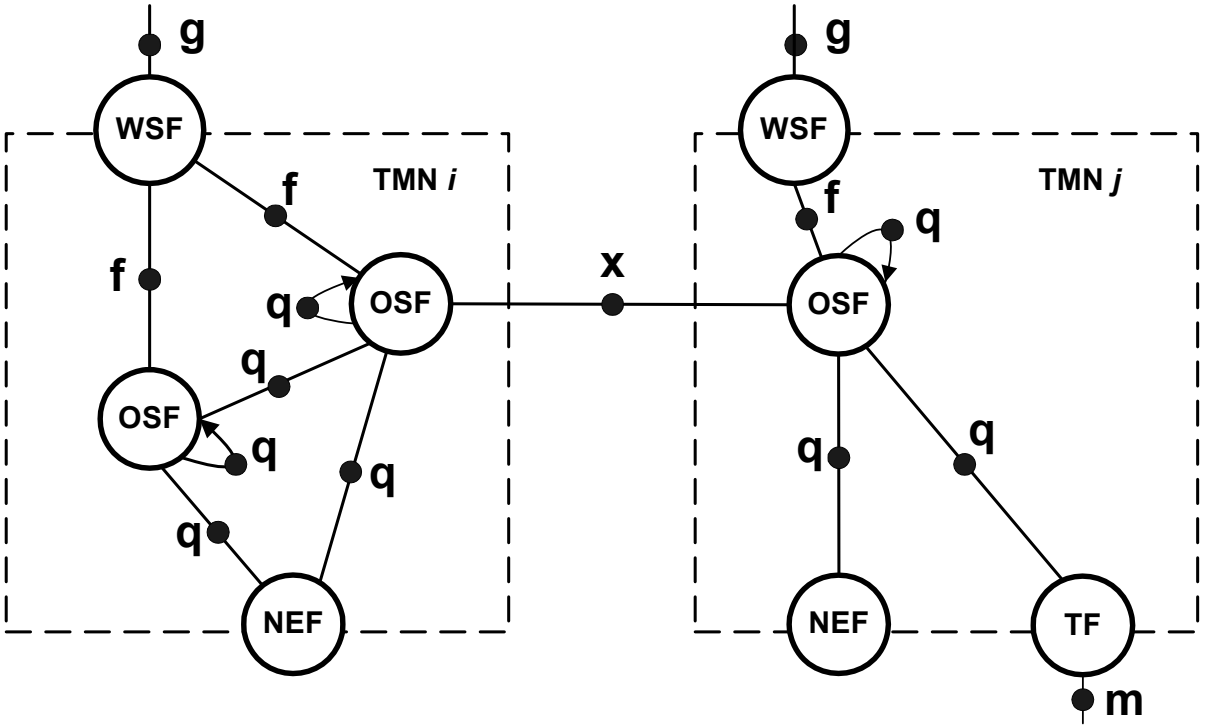


Рисунок 2.3 – Опорные точки и функциональные блоки TMN

- *Функциональный блок операционной системы* (operations systems function block, *OSF*).
- *Функциональный блок элемента сети* (network element function block, NEF).
- *Функциональный блок рабочей станции* (workstation function block, WSF).
- *Функциональный блок преобразования* (transformation function block, TF).

Блоки, которые полностью находятся внутри области, помеченной как «TMN» означает, что эти функциональные блоки полностью описаны в рекомендациях TMN. Оставшиеся функциональные блоки (WSF, NEF и TF) указаны на граничной линии. Это указывает на то, что только часть этих функциональных блоков описана в рекомендациях TMN. Аналогично, три класса опорных точек (q, f и x) полностью описаны в рекомендациях TMN; другие классы (g и m) располагаются вне систем TMN и описаны рекомендациями МСЭ–Т лишь частично.

Функциональный блок элемента сети, NEF. Как уже говорилось, в терминах TMN управляемое оборудование обозначается как элементы сети (network element, NE). Функция NEF описывает функции оборудования электросвязи, доступные для управления TMN. NEF поддерживает обмен информацией с TMN для обеспечения передачи управляющих команд и информации управления. Эта часть NEF, доступная TMN, изображена на рис. 2.3 внутри границ TMN.

Функциональный блок управляющей системы, OSF инициализирует операции управления и получают сообщения/уведомления о выполнении операций управления. OSF устанавливает связь и взаимодействует с NEF через опорную точку q (см. Рек. МСЭ–Т М.3010). Рисунок 2.4 показывает отношение между OSF, NEF и q. Услуги, предоставляемые в опорной точке q в основном относятся к услугам протокола CMIP (см. главу 4).

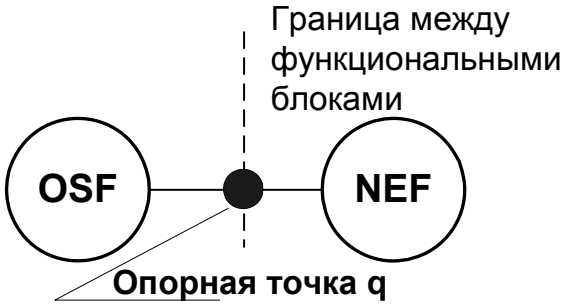


Рисунок 2.4 – Взаимосвязь между OSF, NEF и опорной точкой q

Как видно из рис. 2.3, на отдельно взятой сети TMN (эксплуатируемой одной администрацией связи) обмен между несколькими OSF осуществляется через опорную точку q. Обмен между OSF в различных сетях TMN (эксплуатируемых различными администрациями связи) осуществляется через опорную точку x.

Функциональный блок рабочей станции, WSF обеспечивает представление информации управления для пользователя в наиболее доступной и ясной форме. Функция WSF включает поддержку интерфейса пользователю через опорную точку g. Этот аспект WSF не являются частью стандартов TMN. Поэтому на рисунке 2.3 WSF расположена на краю оболочки TMN, а опорная точка g расположена вне рамок TMN.

Функциональный блок преобразования, TF используется для организации связи между двумя элементами, которые имеют несовместимый механизм информационного обмена. Несовместимыми могут оказаться информационные модели, протоколы обмена. Функции TF могут использоваться как для связи функциональных блоков внутри сети TMN, так и для организации взаимодействия с внешними системами. В частности, на границе TMN, функциональный блок TF обеспечивает взаимодействие с окружением, которое не соответствует стандартам TMN, с помощью опорной точки m. Функция TF преобразовывает информацию на участке от опорных точек q (которые являются стандартными опорными точками TMN) до опорных точек m. Так как опорная точка m не является целиком стандартной с точки зрения TMN, то часть функции TF показана на краю оболочки TMN. Кроме того, TF осуществляет хранение и фильтрацию информации по управлению; преобразование информации из некоторой локальной или частной формы в стандартизированную форму. Взаимосвязь между функциональными блоками и опорными точками приведена в таблице 2.1 :

Таблица 2.1 – Функциональные блоки и опорные точки TMN

	NEF	OSF	TF	WSF	He TMN
NEF		**q**	**q**		
OSF	**q**	**q, x**[1]	**q**	**f**	
TF	**q**	**q**	**q**	**f**	**m**
WSF		**f**	**f**		**g**
He TMN			**m**	**g**	

Примечания.

[1]x интерфейс применяется когда OSF находятся в разных функциональных блоках
Опорная точка g находится между WSF и персоналом, управляющим сетью.

Функциональный блок в заголовке столбца таблицы 2.1 может обмениваться информацией управления с функциональным блоком в крайней левой графе через опорную точку, которая указана на пересечении столбца и строки. В случае, если пересечение пусто, функциональные блоки не могут обмениваться информацией управления.

Кроме перечисленных элементов, до 2000 г. описание функциональной архитектуры TMN включало некоторые дополнительные функции. В частности, это была *функция передачи данных TMN* (data communication function, DCF). Несмотря на то, что описание указанных функций исключено из текущей версии рекомендации М.3010, на практике функции передачи данных DCF, реализованные сейчас в DCN, обеспечивается уровнями с 1 по 3 (транспортные уровни) TMN согласно семиуровневой модели ВОС.

2.2.3 Физическая архитектура TMN

После функциональной архитектуры определяется физическая архитектура TMN. В физической архитектуре TMN функциональные блоки реализовываются с помощью *физических блоков* (phisical blocks).

Физическим блокам соответствует оборудование связи, ЭВМ, системное или прикладное программное обеспечение. Физическая архитектура TMN состоит из следующих физических блоков:

- *Элемент сети (или сетевой элемент)*, NE.
- *Устройство медиатора* (Mediation Device, MD).
- *Q-Адаптер* (QA).
- *Операционная система*, OS.
- *Рабочая станция*, WS.
- *Сеть передачи данных*, DCN.

Физические блоки являются реализацией одноименных функциональных блоков. К примеру, блок «Элементы сети» выполняет функции элемента сети т.е. оборудования связи.

Функции преобразования TF в данном случае разделяются на две составляющие:

- функции адаптации, которую реализуют устройства адаптации;

- функции медиации, которую выполняют устройства медиатора.

Как уже отмечалось, интерфейсы TMN реализуют соответствующие им опорные точки.

В более широком смысле, под интерфейсом понимается граница между взаимодействующими системами, которая определяется общими функциональными и конструктивными характеристиками, а также требованиями к протоколам обмена.

Рассмотрим далее элементы физической архитектуры TMN более подробно.

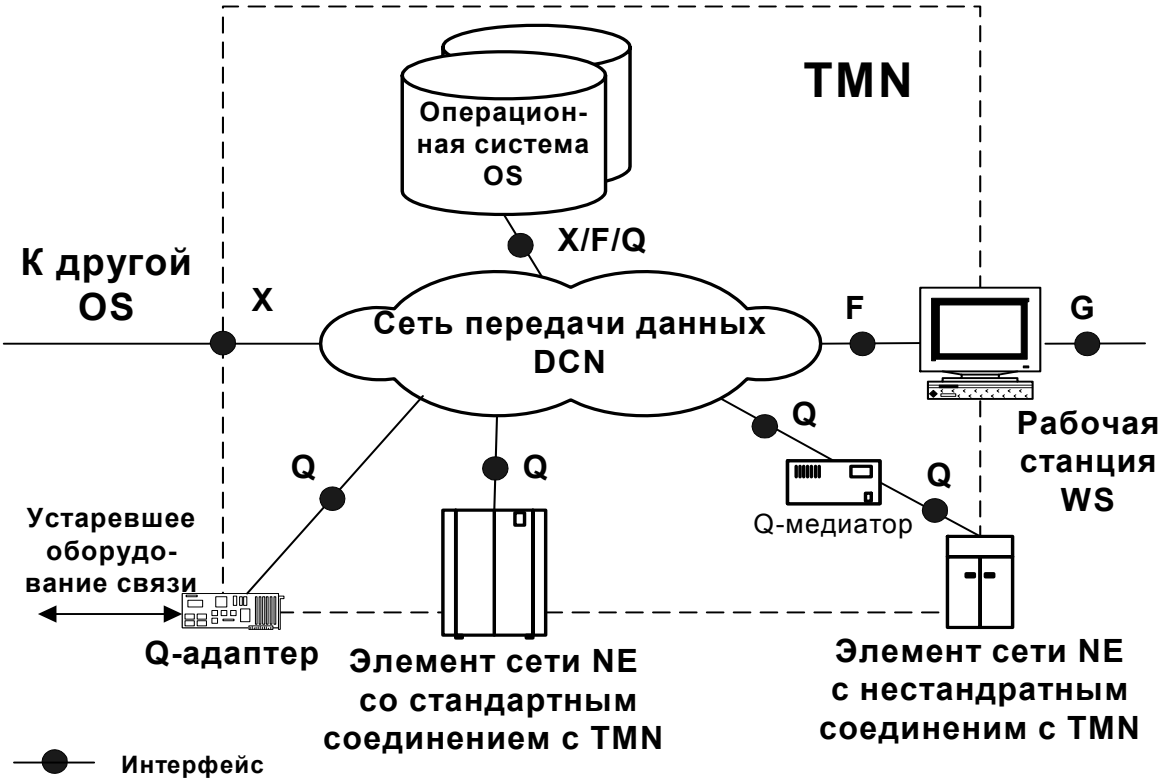


Рисунок 2.5 – Физическая архитектура TMN

Элементы физической архитектуры TMN представлены на рис. 2.5.

Функция адаптации и *устройство адаптации* (adaptation device, AD), реализующее данную функцию, обеспечивает информационный обмен между физическими элементами, не поддерживающими стандарты TMN и элементами сети (операционной системой), которые соответствуют принципам TMN. В этом случае, как видно на рис. 2.5. применяется устройство, которое называется *Q-адаптером* (Q-adapter, QA). Q-адаптер обеспечивает подключение элемента сети с несовместимым с TMN интерфейсом к Q-интерфейсу TMN. Характерным примером такого взаимо-

действия может быть подключение устаревшей электромеханической или квазиэлектронной АТС к сети TMN. Адаптер поддерживает интерфейсы TMN, интерфейс к «не-TMNовской» системе, а при необходимости и внешние интерфейсы для вывода информации, например аварийной.

Выделяют также *X-адаптер* (X-adapter, XA), который позволяет организовать обмен информацией управления между операционной системой TMN и несовместимой с TMN управляющей системой, которая не поддерживает стандартный коммуникационный механизм TMN. Скажем, унаследованная автоматизированная система технической эксплуатации с устаревшим типом программного управления может взаимодействовать с операционной системой TMN через X-адаптер.

Устройства медиатора MD осуществляют трансформацию данных при обмене между физическими блоками TMN, которые поддерживают несовместимый механизм обмена информацией. Здесь опять различают *Q-медиатор* (Q-Mediator, QM) и *X-медиатор* (X-mediator, XM). Q-медиатор поддерживает соединения внутри TMN, а X-медиатор поддерживает соединения между операционными системами различных сетей TMN. Адаптеры и медиаторы могут выполнять преобразование форматов данных.

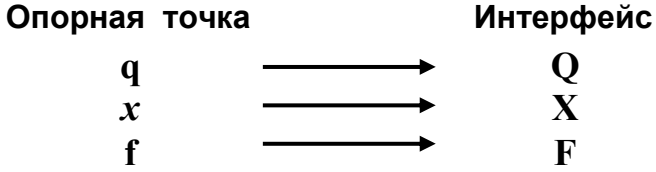
Существует техническая возможность реализовать в виде единого физического блока несколько функциональных блоков одного или различных типов. Например, операционная система может быть использована для выполнения нескольких OSF, а также может применяться для реализации OSF, MF и WSF. В случае, если физический блок реализует несколько функциональных блоков различных типов, выбор наименования блока определяется его преобладающим использованием.

2.2.4 Интерфейсы TMN

Как отмечалось в подразделе 2.2.3, интерфейсы могут рассматриваться как физическая реализации опорных точек TMN [26,28,29]. Интерфейсы можно сравнить со шлюзами, с помощью которых услуги управления становятся доступны пользователю. Через интерфейсы реализуется взаимодействие между различными элементами (физическими

блоками) TMN или взаимодействие сети TMN и внешнего окружения. С точки зрения модели ВОС, интерфейсы обеспечивают *интероперабельность* т.е. позволяют сохранять взаимосвязь между различными открытыми системами или между уровнями открытых систем. Для сетей TMN это означает взаимодействие между физическими блоками безотносительно к типу устройств и фирме-производителю. При этом стандартный интерфейс TMN получает то же самое имя (но записывается заглавными буквами !), что и соответствующая опорная точка.

Взаимосвязь опорных точек и соответствующих им интерфейсов выглядит следующим образом :



Спецификации интерфейсов TMN осуществляются различными организациями, в том числе МСЭ-Т, ETSI, TMF. Спецификации интерфейсов, как правило, содержат формальное описание управляемого объекта с помощью выбранного метода описания и сценарий использования интерфейса. Иногда сценарий использования интерфейса TMN не входит в состав рекомендаций TMN. В спецификациях интерфейсов TMN указываются все ресурсы, доступные для управления и способы доступа к информации управления. Спецификация интерфейса TMN определяет функциональность интерфейса; в спецификации не содержится описание протоколов, которые используются для обмена информацией через интерфейс. Методология, которую нужно применять при проектировании и разработке интерфейсов TMN, описана в Рек. МСЭ-Т М.3020 [27].

Согласно этой методологии, проектирование интерфейса TMN начинается с определения услуги управления, доступ к которой желательно получить с помощью интерфейса. Далее услуги управления декомпозируются (разбиваются) на отдельные компоненты; компоненты услуг управления, в свою очередь, декомпозируются на функции управления. Функции управления описываются с помощью объектно-ориентированного подхода в виде классов управляемых объектов. Примерами различных классов управляемых объектов является элемент сети (NE), *файл журналирования* (logfile) данных управления и *отдельная*

журнальная запись (logRecord) о сетевом событии. При этом возможно использование средств моделирования, например UML.

После моделирования осуществляется фаза консолидации и объединения разработанных классов объектов в единую информационную модель интерфейса. На этапе консолидации подтверждается, что первоначально спланированные услуги управления поддерживаются классом объектов управления, который создан разработчиком. На всех этапах разработки безусловно учитываются содержание процесса управления, правила управления и цели управления.

Услуги управления и функции, необходимые для разработки информационной модели управления документированы в Рек. МСЭ-Т M.3200 и M.3400. Эти рекомендации в большей степени носят информативный чем нормативный характер. Поскольку интерфейсы TMN созданы на базе объектно-ориентированного подхода, новые разработки интерфейсов должны учитывать основную сетевую информационную модель согласно Рек. МСЭ-Т M.3100 (см. Приложение А).

Существует три стандартных интерфейса TMN : интерфейс Q, интерфейс F и интерфейс X.

Интерфейс Q указывает, какая часть информации об объекте управления совместно используется и операционной системой и элементом сети. Другими словами, интерфейс Q определяет, какие телекоммуникационные ресурсы и операции элемента сети будут «видны» сети TMN в процессе управления, а какие ресурсы «не видны». Тот же интерфейс Q применяется на стыке OS – NE и на стыке OS – OS.

Интерфейс F позволяет соединить рабочую станцию WS и физические блоки TMN, которые поддерживают реализацию OSF и TF. Соединение осуществляется через сеть передачи данных DCN.

Интерфейс X поддерживает взаимосвязь TMN и других внешних систем, включая другие сети TMN. Интерфейс X используется для управления оказанием коммерческих услуг. Это возможно при наличии в корреспондирующих системах интерфейсов, взаимодействующих с TMN. С учётом факта передачи информации во внешнее окружение, уровень информационной безопасности для интерфейса X должен быть выше, чем для интерфейса Q. По аналогии с интерфейсом Q, интерфейс X опреде-

ляет для внешних систем видимую часть «айсберга» сети TMN и порядок доступа к ресурсам сети TMN [24].

2.2.5 Информационная архитектура TMN

Информационная архитектура TMN, в рамках которой осуществляется описание объектов управления и обмен данными по управлению, основана на стандартной модели, предложенной ISO (Рек. МСЭ-Т X.720) и использует объектно-ориентированный подход. Информационная архитектура TMN оказывает непосредственное влияние на спецификацию интерфейсов TMN. Ключевыми элементами информационной архитектуры являются информационные элементы, модель взаимодействия элементов и структура информационной модели.

Информационные элементы TMN с точки зрения объектно-ориентированного подхода и принципов ВОС делятся на управляющие и управляемые объекты. В дальнейшем рассматривается описание управляемого объекта, как наиболее существенной части информационной архитектуры TMN. Описание управляемого объекта осуществляется с помощью *контура управляемого объекта* (managed object boundary). В контуре указываются характеристики объекта, доступные для управления. Общая структура описания управляемого объекта приведена на рис. 2.6.

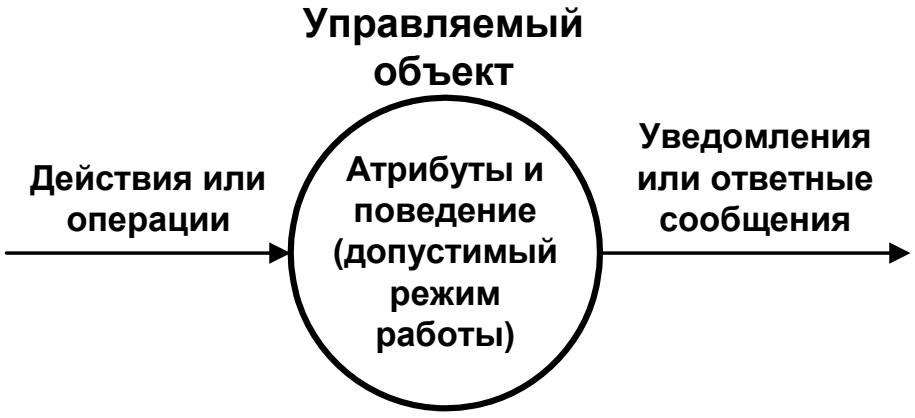


Рисунок 2.6 – Описание управляемого объекта

В состав описания управляемого объекта входят :

- *атрибуты (attributes)*, которые описывают свойства управляемого объекта;

- *действия или операции (actions)*, которые могут выполняться на объекте по команде;
- *поведение или режим работы (behavior)* объекта, который предусмотрен в ответ на поступившую команду;
- *уведомления или ответные сообщения (replays)*, которые выдаются объектом в ответ на действия или операции.

Атрибут управляемого объекта – информация, относящаяся к управляемому объекту, используемая для описания (частично или полностью) управляемого объекта. Атрибут включает тип атрибута и значение атрибута.

В атрибутах представлены характеристики, которые характеризуют свойства управляемого объекта; доступ к атрибутам можно получить с помощью операций/действий по команде управляющего объекта.

При описании управляемого объекта определяется набор *уведомлений* (notifications), *ответных сообщений* или *подтверждений* (acknowledgement), которые посылает управляемый объект для оповещения управляющей системы о произошедших событиях на объекте, включая результаты выполнения требуемых действий/операций.

Описание управляемых объектов достаточно абстрактно и реализуется по единым принципам для разных типов элементов сети. Для описания структуры и поведения управляемых объектов следует использовать «Общее определение управляемых объектов» (Guidelines for the Definition of Managed Objects, GDMO) по Рек. МСЭ-Т X.722. Управление в TMN осуществляется с помощью информационной модели взаимодействия типа «менеджер – агент» (см. рис. 2.7 на следующей странице).

Считается, что программно-аппаратный комплекс, который выдаёт команды управления и принимает уведомления / сообщения / подтверждения об исполнении команды, является *менеджером*.

Программно-аппаратный комплекс или программное приложение, установленное на элементе сети (управляемом объекте), которое выполняет команды и посылает сообщения о результатах операций, называется *агентом*.

Менеджер устанавливает сеанс связи с агентом для осуществления управляющего воздействия. Возможное нарушение такой связи может быть обнаружено обеими сторонами.

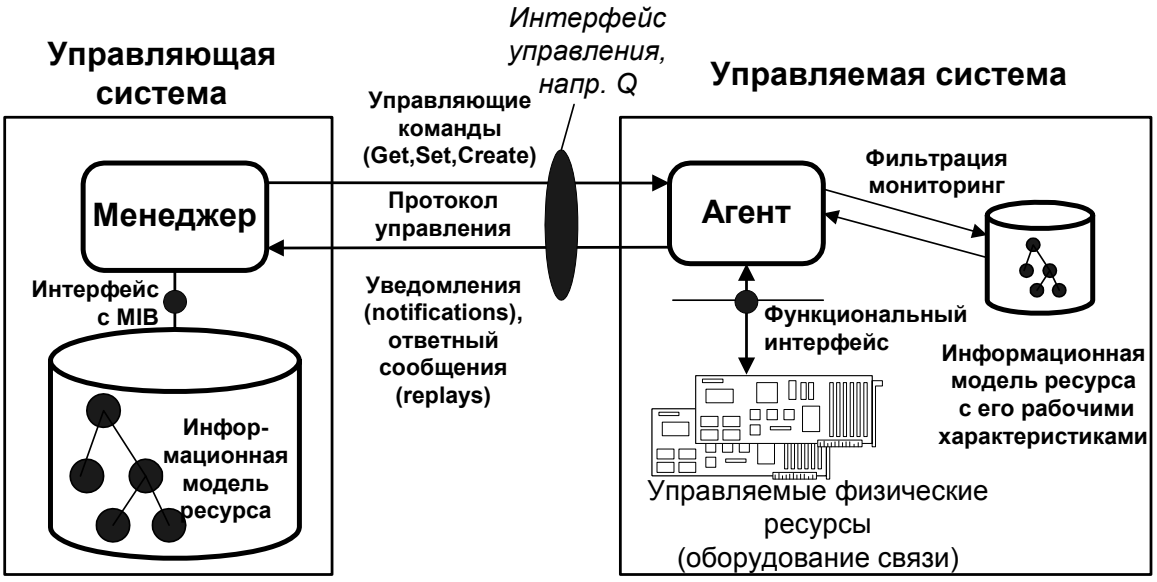


Рисунок 2.7 – Взаимодействие менеджера и агента в информационной архитектуре TMN

Менеджер и агент могут быть физически реализованы в виде отдельного модуля, платы, процессора с соответствующим программным обеспечением или в виде специальной компьютерной программы.

Как только связь между менеджером и агентом установлена, может осуществляться обмен информацией. С помощью управляющих команд, которые оформляются в виде запросов, менеджер может потребовать у агента выполнить процедуры «Создать» (Create), «Удалить» (Delete), «Выполнить» (Action) в отношении управляемых объектов в целом, а также процедуры «Получить» (Get) и «Установить» (Set) в отношении атрибутов управляемых объектов. Процедура описывает последовательность выполнения требуемой операции, включая последовательность обмена необходимыми запросами. Получив запрос на осуществлении той или иной процедуры, агент сначала на информационной модели ресурса, а затем – через функциональный интерфейс – непосредственно на оборудовании связи (телекоммуникационном ресурсе), выполняет необходимую операцию управления. Как правило, имена операций и процедур управления совпадают. Операция представляет собой описание требуемого действия.

После завершения операции агент изменяет содержимое информационной базы управления и посылает сообщение о результатах менеджеру. Агент выступает своего рода посредником между менеджером и

управляемым оборудованием связи. При этом агент через функциональный интерфейс непосредственно взаимодействует с управляемыми телекоммуникационными ресурсами (ТЭЗ, процессор, аппаратный модуль). Логическое описание ресурсов агент поддерживает с помощью информационной модели ресурса. В информационной модели ресурса содержатся данные о рабочих характеристиках, на которые можно воздействовать или контролировать в процессе управления. С другой стороны, менеджер также поддерживает информационную модель управляемого ресурса. Поэтому информационные модели агента и менеджера в основном одинаковы. Однако информационная модель менеджера включает модели нескольких ресурсов, например нескольких узлов или всех узлов сети связи. Кроме того, информация менеджера является «очищенной», нормализованной, упорядоченной. Это происходит благодаря действиям агента, который фильтрует поток данных в сторону менеджера, удаляя сведения о незначительных ошибках, искажения, повторах.

Сведения информационной модели, которую поддерживает агент, хранятся в *базе данных информации управления* (management information base, MIB). Менеджер также поддерживает MIB, но база данных менеджера вторична по отношению к базе данных агента по причинам, которые были перечислены выше. Для обновления своей базы данных менеджер всегда запрашивает агента. В базе данных MIB информация управления логически упорядочена с помощью *классов управляемых объектов* и их атрибутов.

Под *классом* понимается множество управляемых объектов с идентичными атрибутами, допустимыми операциями, поведением. База MIB позволяет хранить описание действий (операций управления) которые можно осуществлять над классами управляемыми объектами и описания реакции на эти действия т.е. допустимые режимы работы. Другими словами, база MIB позволяет программным приложениям управления (в первую очередь агентам, затем менеджерам), поддерживать в упорядоченном виде информацию об управляемых объектах. Передача управляющих команд чаще основана на модели асинхронной передачи сообщений, чем на модели синхронной передачи сообщений.

Все операции управления, осуществляемые в рамках модели «менеджер-агент», могут быть представлены в виде 4 примитивов –

элементарных сообщений пользователей услуг управления т.е. агентов и менеджеров. Примитивы имеют соответствующие имена. Например, услуга по установлению соединения описывается примитивом с именем CONNECT, примитив услуги по передаче данных между менеджером и агентом имеет имя DATA. Примитивы используются следующим образом:

1. Для выполнения операции на агенте, менеджер посылает управляющую команду в виде сообщения-запроса в виде *примитива запроса* (Request Primitive).
2. Когда сообщение-запрос поступает агенту, запрос принимается как указание и инициирует на агенте *примитив индикации* (Indication Primitive), указывающий на необходимость вызова агентом необходимой процедуры.
3. Агент выполняет действие, необходимое в рамках вызванной процедуры, посылает сообщение-ответ в виде *примитива ответа* (Response Primitive) в сторону менеджера.
4. Сообщение-*ответ* принимается менеджером как сообщение-подтверждение в виде *примитива подтверждения* (Confirm Primitive).

Функциональная архитектура TMN с учётом менеджеров и агентов имеет вид, представленный на рис. 2.8.

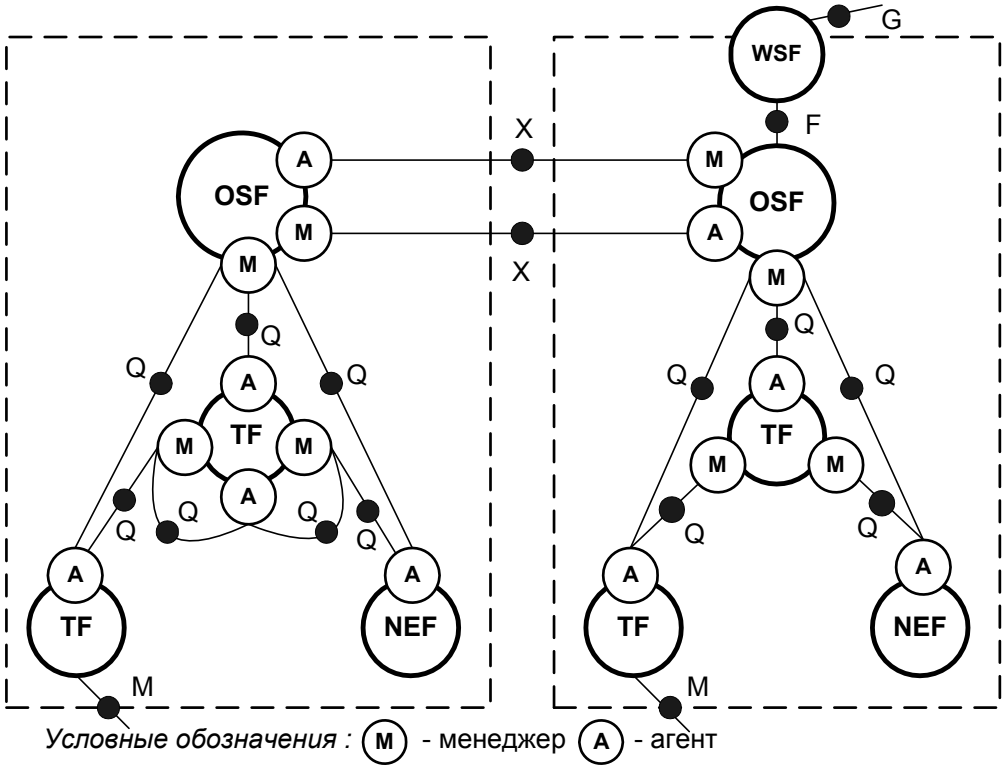


Рисунок 2.8 – Функциональная архитектура TMN

Информационная модель управления TMN представляет собой упорядоченную конструкцию, которая включает информационную модель, технологию менеджер-агент и базы данных *с общими (совместными) знаниями по управлению* (shared management knowledge, SMK). Знания SMK могут быть разделены по нескольким узлам или операционным системам TMN.

Выполнение операций Get, Cancel-Get (отменить получение), Create и Delete подтверждаются всегда; выполнение операций Set, Event-Report (сообщение о событии) и Action могут подтверждаться или не подтверждаться.

В целом, информационная модель управления представляет собой абстрактное описание сетевых ресурсов, доступных для управления, а также допустимых операций управления. Информационная модель содержит развёрнутое описание классов объектов управления, информация о которых хранится в упорядоченном виде в MIB. Модель определяет стандарты для содержания информационного массив, который появляется в ходе сетевого управления. Следовательно, информационная модель и поддерживающая её MIB относятся к прикладному уровню семиуровневой модели ВОС. Поэтому при разработке модели и MIB требуется организовать взаимодействие с другими приложениями 7-го уровня и нижестоящих уровней модели ВОС, которые используются для хранения, поиска и обработки информации управления. Это взаимодействие будет рассмотрено в главе 4.

2.2.6 Логическая многоуровневая архитектура TMN

В рамках концепции TMN признается, что существует определенная иерархия «обязанностей», связанных с управлением теми или иными объектами. Такая иерархия может быть описана с помощью термина «уровень управления»; соответственно архитектура которая описывается с мощью уровней называется *логической многоуровневой архитектурой* (logical layered architecture, LLA) TMN.

Концепция уровней управления стала наиболее важным и наиболее упоминаемым видом архитектуры TMN.

Впервые описание этого вида архитектуры появилось в 1992 г., как приложение к Рек. МСЭ-Т М.3010. Далее описание данной архитектуры перешло в основной текст рекомендации версии 1996 г. и сохранилось в версии 2000 г.

Появление LLA обусловлено тем, что задачи сетевого управления достаточно сложны и многоплановы.

Для упрощения управления и разграничения полномочий между различными участниками процесса управления, функциональные возможности TMN вместе с необходимой информацией декомпозированы (разбиты) на ряд логических уровней. Общий принцип такого иерархического разбиения показан на рис. 2.9 [34].

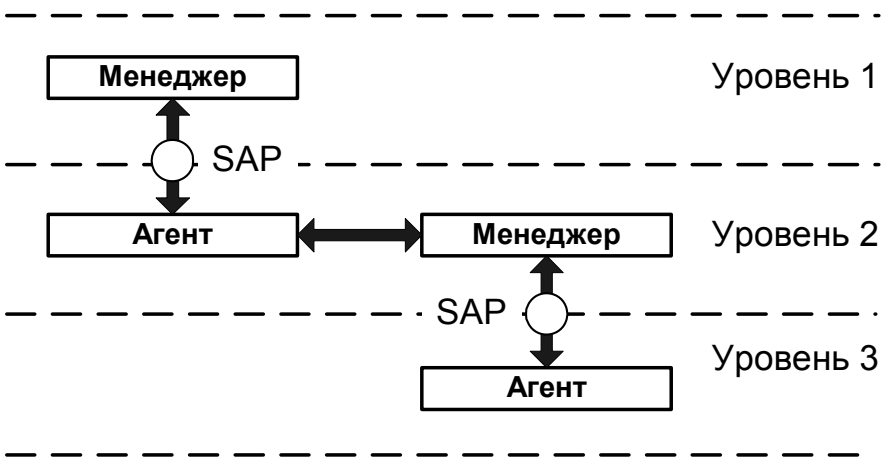


Рисунок 2.9 – Декомпозиция функциональности управления

На рис. 2.9 уровень 2 на границе между уровнем 1 и 2 предоставляет услуги по управлению уровню 1 через *опорную точку доступа к услугам* (service access point, SAP). Предоставление услуг реализовано с помощью передачи на вышестоящий уровень 1 информации по управлению, которая формируется с помощью программы-агента уровня 2. Управление, которое осуществляется на уровне 1 не требует детальной и подробной информации о состоянии уровня 2; программа–агент на уровне 2 будет обеспечивать только ту информацию по управлению, которая является жизненно необходимой для принятия решений на уровне 1. Здесь действует принцип «знать только то, что нужно для работы».

Описанный принцип иерархического представления можно применять рекурсивным способом – предоставление информации управления с

уровня 3 обеспечивается для уровня 2 с помощью программы–агента уровня 3. Важно отметить, что по аналогии с моделью ВОС, уровень 1 не может напрямую управлять уровнем 3; для этого уровень 1 получает услуги управления от уровня 2, а уровень 2 в свою очередь получает услуги управления от уровня 3. Другими словами, уровень 1 управляет уровнем 3 только через уровень 2. Применительно к TMN, логическая декомпозиция уровней управления может быть выражена с помощью следующего разбиения с учётом функциональности (см. рис. 2.10):

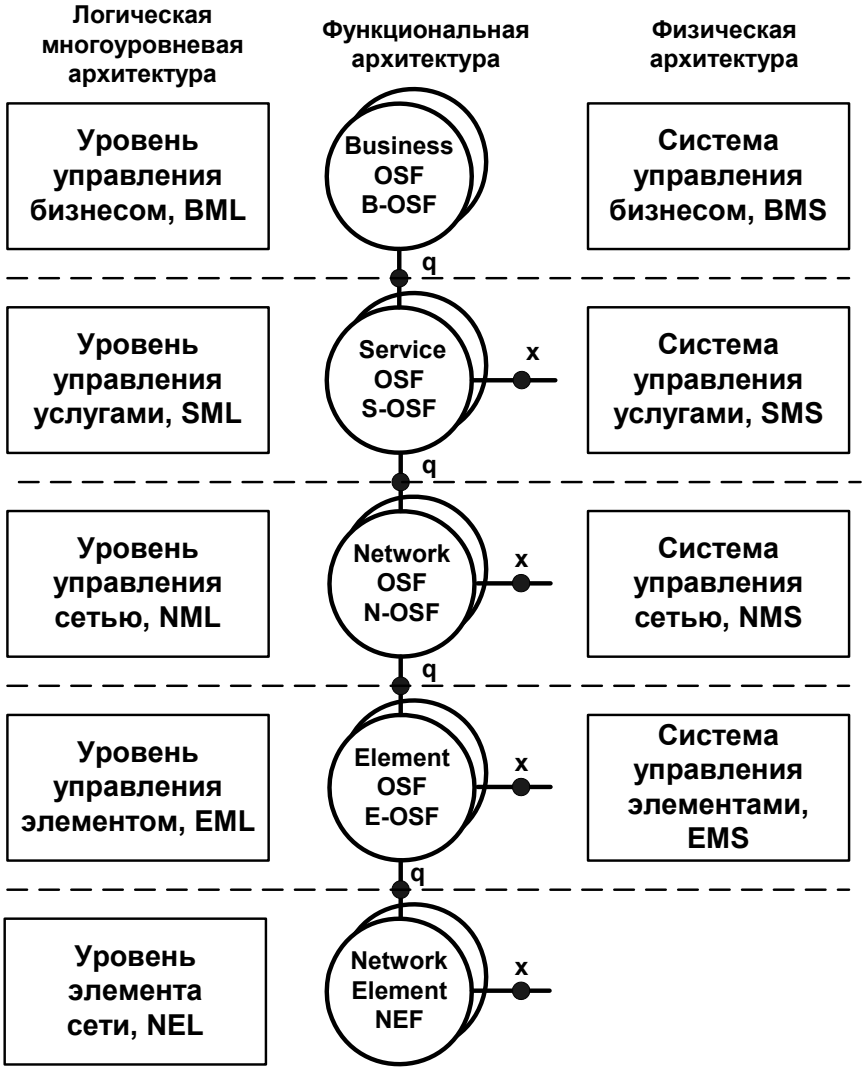


Рисунок 2.10 – Логическая многоуровневая архитектура TMN и её связь с другими архитектурами

- *Уровень элемента сети* (network element layer, NEL).
- *Уровень управления элементом* (element management layer, EML).

- *Уровень управления сетью* (network management layer, NML);
- *Уровень управления услугами* (service management layer, SML).
- *Уровень управления бизнесом* (business management layer, BML).

Реализация многоуровневой архитектуры TMN включает *бизнес-функции операционной системы* (business operation system function, B-OSF), которые имеют отношение ко всем управляемым сетям/системам связи и осуществляют общую координацию управления бизнесом оператора связи.

Функции операционной системы по управлению услугами (service operation system function, S-OSF) имеют отношение к услугам связи, предоставляемых с помощью технических средств сетей электросвязи. Сервисные S-OSF на уровне управления услугами обеспечивают интерфейс с абонентом или клиентом.

Функции операционной системы по управления сетями (network operation system function, N-OSF) охватывают различные реализации функции управления сетями связи. При этом сетевые N-OSF взаимодействуют с OSF элементов сети E-OSF.

Функции операционной системы по управления элементами сети (element operation system function, E-OSF) обеспечивают управление отдельными элементами сети. Сетевые N-OSF и E-OSF элементов сети обеспечивают управление сетью электросвязи на уровне телекоммуникационного оборудования и предоставляют информацию о сети по запросам сервисных S-OSF. *Функции элемента сети* (network element function, NEF) входят в состав уровня EML и управляются со стороны уровня элемента сети.

В рамках LLA предполагается, что программы-менеджеры OSF любого уровня могут управлять OSF-агентами, находящимися на том же уровне, либо на нижнем уровне. Это управление, как в пределах данной сети TMN так и между разными сетями TMN, осуществляется через опорные точки q или x соответственно. Управление агентами NEF осуществляется с помощью E-OSF. Далее уровни LLA рассматриваются более подробно.

Уровень элемента сети (network element layer, NEL)**.** Уровень элемента сети – это телекоммуникационное оборудование с функционирую-

щей программой-агентом для сбора информации и обработки управляющих воздействий, поступающих от уровня управления элементом.

Уровень управления элементом сети (element manager layer, EML)**.** Элементы сети управляются с помощью функций E-OSF на уровне управления элементом. На этом уровне осуществляется взаимодействие со специфическими функциями данного оборудования, реализация которых зависит от поставщика оборудования. В результате специфические функции оборудования «скрываются» от других уровней LLA на уровне управления элементом. В качестве примера можно привести следующие функции управления, выполняемые на уровне управления элементом сети:

- обнаружение ошибок и неисправностей телекоммуникационного оборудования и систем связи;
- измерение мощности, потребляемой оборудованием;
- измерение задействованных ресурсов оборудования связи, например загрузка центрального процессора, наличие свободного места в буфере передачи/приема, длина очереди и т.п;
- регистрация статистических данных.

Следует отметить, что OSF (на уровне управления элементом) и NEF могут быть выполнены в виде единого или различных аппаратно-программных модулей.

Уровень управления сетью (network management layer, NML)**.** Уровень управления сетью осуществляет функции управления, касающиеся взаимодействия между многими видами телекоммуникационного оборудования. На уровне управления сетью внутренняя структура элемента сети «невидима», это означает, к примеру что состояние буфера устройства приема/передачи, температура оборудования и т.п. не могут напрямую контролироваться и управляться этим уровнем. С другой стороны, здесь доступны сведения о состоянии внешних портов, соединительных линий, загрузке процессоров элементов сети.

Примеры функций, выполняемых на уровне управления сетью:

- создание полного представления о сети (информационная модель сети);
- поддержка QoS для конечных пользователей;
- модификация и обновление таблиц маршрутизации;

- мониторинг загрузки линий и каналов связи;
- динамическое управление трафиком;
- обнаружение неисправностей и ошибок программного обеспечения.

Функции OSF на уровне управления сетью используют информацию по управлению, которая не зависит от производителей систем. Эта информация предоставляется с уровня управления элементом сети.

Уровень управления услугами связи (service management layer, SML)**.** Уровень управления услугами (сервисами) затрагивает вопросы управления, которые непосредственно касаются потребительской ценности услуг электросвязи. Пользователями данного уровня могут быть клиенты оператора, абоненты сетей связи, а также администрации операторов связи или провайдеры услуг. Управление услугами осуществляется на основе информации, которая обеспечивается уровнем управления сетью; при этом уровень управления услугами «не видит» детальную внутреннюю структуру сети. Это весьма полезное свойство с учётом обеспечения информационной безопасности и коммерческой тайны оператора связи. Маршрутизаторы IP-сетей, традиционные АТС, системы передачи, базовые станции и центры коммутации систем подвижной связи не могут непосредственно управляться с уровня управления услугами.

Примеры функций управления, которые выполняются на уровне управления услугами :

- контроль качества услуг связи (задержки, потери, и т.д.);
- учет объема использования услуг связи;
- тарификация (расчёты) за услуги связи;
- назначение сетевых адресов и номеров абонентских устройств;
- сопровождение группы адресов или номеров, например номеров присоединенного оператора.

Управление услугами может осуществляться различными способами. К примеру, пусть два оператора обмениваются информацией по управлению для того, чтобы управлять своими взаимосвязанными сетями (межоператорское управление). Из соображений безопасности и с учётом конкуренции на рынке связи каждый из этих операторов будет скрывать внутреннюю структуру своей сети от другого оператора. Обмен

будет осуществляться только в той части информации управления, которая является жизненно необходимой для обеспечения качества предоставления услуг связи. К примеру, это могут быть данные о приоритетах абонента, профиль услуг абонента, данные об интенсивности принимаемой-передаваемой нагрузки (трафика).

Второй случай – оператор сети связи обменивается информацией по управлению с системой управления, которая принадлежит одному из клиентов оператора или присоединенному оператору связи. Основной оператор вновь скрывает внутреннюю структуру сети от клиента и обеспечивает доступ только к общей информации о количестве и качестве предоставленных услуг, например о количестве и продолжительности телефонных разговоров [34].

Уровень управления бизнесом (business management layer, BML)**.** Уровень управления бизнесом отвечает за управлением предприятием связи или компанией связи. Этот уровень управления следует рассматривать в самом широком контексте, при этом управление сетью и услугами связи – только часть управления бизнесом. Управление бизнесом непосредственно связано со стратегией управления сетями электросвязи в экономическом аспекте и не затрагивает оперативно–техническое управление сетью электросвязи.

На основании логической многоуровневой архитектуры TMN можно осуществлять логическое разбиение *систем управления* (management system, MS). Как правило, системы управления рассматриваются в рамках физической архитектуры TMN. Это позволяет упростить схемы функциональных архитектур. Для описания принадлежности систем управления к уровням LLA применяются следующие обозначения (см. рис. 2.10) :

- *Система управления бизнесом* (business management system, BMS).
- *Система управления услугами* (service management system, SMS).
- *Система управления сетью* (network management system, NMS).
- *Система управления элементами сети* (element management system, EMS).

Физически MS представляют собой распределенную или централизованную вычислительную систему, которая состоит из серверных ЭВМ,

специализированных устройств-адаптеров или медиаторов и персональных компьютеров, которые связаны между собой с помощью сети передачи данных DCN. На серверах и компьютерах пользователей MS установлено разнообразное программное обеспечение (ПО): операционные системы, ПО удаленного доступа, системы управления базами данных (СУБД), управляющие системы OS, приложения управления электросвязью и средства администрирования этими приложениями.

Администрации связи пользуются услугами управления сетями связи с помощью программных приложений управления , которые поддерживаются OS. Эти приложения осуществляют аналитическую обработку данных и взаимодействуют с пользователями. Например, пользователь может вывести на экран графики ежедневной нагрузки в направлении связи, сведения об отказах оборудования, проанализировать качество предоставления услуг связи и т.п. Кроме того, программные приложения управления осуществляют сбор, обработку данных от оборудования и систем электросвязи, генерацию и передачу управляющего воздействия (команды) на элемент сети и получение отклика элемента с результатом операции.

Система управления любого уровня может включать OS как своего, так и нижележащих уровней. Поставщики систем управления предлагают, как правило, определенный выбор приложений управления, который приводится в условиях заказа. Выбор тех или иных приложений управления может привести к изменению исходного типа системы управления с точки зрения функциональных возможностей

Контрольные вопросы к главе 2.

1. Для чего предназначена сеть TMN ?
2. Перечислите основные компоненты и функциональные возможности TMN.
3. Какие функции выполняет управляющая система OS TMN?
4. Может ли сеть TMN осуществлять оперативное управление процессом внутристанционного соединения?
5. Что такое информационная модель сети электросвязи?
6. Какие уровни описания (виды архитектуры) используются в TMN?
7. В чём разница между функциональным и физическим блоком TMN?
8. Для чего в TMN применяется рабочая станция?
9. Может ли сеть передачи данных DCN использовать стандарт X.25?
10. Какие функции выполняет агент, а какие функции выполняет менеджер?
11. Какие операции осуществляет менеджер?
12. Можно ли создать агента для декадно-шаговой АТС?
13. Для чего создаётся база данных информации управления MIB?
14. Какие существуют логические уровни управления?
15. Какие задачи решаются на уровне управления услугами связи?
16. Как взаимосвязаны различные архитектуры управления?

3. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ И ИНТЕРФЕЙСЫ

3.1 Услуги, функции управления и интерфейсы TMN

Под *функций управления* TMN понимается логический элемент, который обеспечивает реализацию задачи управления в любой её части. Совокупность функций управления образует услуги управления. Доступ к услугам управления на уровне функций, а также взаимодействие различных функций между собой осуществляется через интерфейсы управления.

Базовые функции управления TMN описаны в рекомендации МСЭ–Т М.3200 [20]. В последующих рекомендациях серии МСЭ–Т М.32хх для некоторых видов и служб связи описаны индивидуальные услуги управления. Услуги управления TMN могут быть детализированы с точностью до элементарной функции. Базовое множество функций TMN, соответствующее функциональным областям управления для семиуровневой модели ISO, описано в рекомендации МСЭ–Т М.3400 [30].

Функция управления отражает заключительный этап в определении требований к сетевому управлению. Выбор существующей или разработка новой функции управления обусловлены необходимостью реализовать те или иные задачи управления.

Функции управления реализуются в рамках информационной модели управления и допускают многократное использование в различных услугах управления.

Перечень услуг управления TMN содержится в Рек. МСЭ–Т М.3020. Рекомендация М.3200 предусматривает для описания услуги управления *шаблон*.

Согласно шаблону каждая услуга управления должна быть описана в общем виде по схеме согласно таблицы 3.1 на основании Рек. МСЭ-Т М.3200, 1997 г. :

Таблица 3.1 – Услуги и области управления

Области управления **Услуга управления**	**ТФОП**	**Системы подвижной связи**	**Интеллектуальные сети**	**ОКС №7**	**ЦСИО**	**Первичные сети связи**	**TMN**	**Сети передачи данных**
Администрирование данными пользователей	+	+	+		+		+	+
Управление тарифами.	+	+	+	+	+			+
Администрирование качеством услуг связи и рабочими характеристиками сети	+	+	+	+	+	+	+	+
Измерение нагрузки и анализ результатов измерения	+	+	+	+	+	+	+	+
Администрирование маршрутизацией и системой нумерации	+	+	+	+	+		+	+
Техническая эксплуатация и управление неисправностями (последствиями отказов)	+	+	+	+	+	+	+	+
Управление безопасностью	+	+	+	+	+	+	+	+

Примечание : символ «**+**» означает, что область управления нуждается в данной услуге управления.

Например, в Рек. МСЭ–Т М.3200 содержится услуга управления «Техническая эксплуатация и управление неисправностями (последствиями отказов)». Эта услуга требуется для всех видов областей управления. Управление техэксплуатацией и управление неисправностями обеспечивается следующими группами функций управления: «Наблюдение за

неисправностями (отказами)», «Тестирование», «Администрирование в условиях аварийной ситуации».

Группа функций управления «Наблюдение за неисправностями (отказами)», в свою очередь, включает в себя множество функций (Management Functions Set, MFS) :

- «Сообщение о неисправности».
- «Обобщение данных о неисправности» (alarm summary).
- «Критерий выбора состояния неисправности» (alarm event criteria).
- Контроль журналирования сообщения о неисправностях.
- Корреляция и фильтрация аварийных сообщений.

В свою очередь, группа функций «Сообщение о неисправности» включает в себя такие функции TMN, как «Сообщение о неисправности», «Маршрутизация сообщения о неисправности» (route alarm report), «Запрос истории повреждения» (request alarm history).

В итоге, создаётся следующая иерархия услуг и функций управления (от верхнего уровня 1 к нижнему уровню 4):

1. Услуга управления – «Управление техническим обслуживанием».
2. Группа функций управления – «Наблюдение за неисправностями» (в составе услуги).
3. Множество функций управления – «Сообщения о неисправности» (в составе группы функций).
4. Функция управления – «Маршрутизация сообщения о неисправности» (в составе множества функций).

Функции управления доступны через интерфейсы. Для интерфейсов TMN можно сформулировать следующие общие требования по функциональности :

- Поддержка нескольких одновременно работающих систем управления т.е. данный объект может управляться различными OS. Управляемый объект должен генерировать соответствующие уведомления для каждого приложения управления.
- Обеспечение коммуникативности – поддержка операций управления должна осуществляться как в асинхронном так и в синхронном режиме. Синхронный режим операций предусматривает, что

управляемые объекты предварительно проверяются на предмет осуществления той или иной операции. Если хотя бы один объект не может выполнить операцию, то она не осуществляется.

- Подтверждения о результатах операции – интерфейс должен обеспечить передачу положительных или отрицательных подтверждений о завершении операции.

Более подробный перечень требований к интерфейсам можно найти в документе [20]. В документе [27] рассматриваются общие требования к интерфейсам TMN. Эти требования затрагивают вопросы проектирования, построения, проверки системы управления на соответствие стандартам TMN. Основной целью проверки системы управления является оценка степени взаимодействия различных элементов систем сетевого управления через используемые интерфейсы. Взаимодействие элементов должно обеспечить единство системы управления в той мере, в какой это требуется для оператора связи и для реализации функций управления. Детально проформа (методика) проверки интерфейсов на соответствие требованиям TMN описана в Рек. МСЭ–Т Q.823.1 «Management Conformance Statement Proforma», 1997 [Проформа утверждения о соответствии управлению]. Далее рассмотрим основные интерфейсы TMN.

3.2 Описание интерфейса Q

Интерфейс Q (ранее интерфейс Q.3) является стандартным интерфейсом управления между элементом сети (адаптером, медиатором) и OS. Интерфейс Q включает все уровни модели взаимосвязи открытых систем с использованием отдельных протоколов на каждом уровне реализации. Общий вид стека протоколов модели ВОС, используемых при реализации интерфейса Q представлен на рис. 3.1 [33].

Подробно реализация транспортного уровня интерфейса Q представлена в Рек. МСЭ–Т Q.811, реализация верхних уровней интерфейса Q в рамках модели ВОС представлена в Рек. МСЭ–Т Q.812. Дополнительно в рекомендации МСЭ–Т G.784 представлено описание интерфейса Q для управления сетью первичной цифровой иерархии SDH.

Прикладной уровень управления (уровень приложений) предлагает две услуги: услуги CMISE для управления и услуги протокола FTAM для передачи файлов с целью загрузки программного обеспечения.

Рисунок 3.1 – Реализация интерфейса Q

Протокол FTAM использует услуги ASCE, в то время как CMISE использует услуги как ACSE так и ROSE. Подробнее ASE, CMISE, ACSE, ROSE описаны в главе 4. Уровень представления в стеке интерфейса Q обеспечивает кодирование данных в обусловленном формате.

Сессионный уровень обеспечивает управление сессией, т.е. открытие и закрытие сеансов обмена информацией между взаимодействующими приложениями. В случае прерывания сеанса, сессионный уровень пы-

тается восстановить обмен информацией. Если сеанс прерывается на долгое время, сессионный уровень может завершить данный сеанс и создать новый. Перечисленные действия прозрачны для уровня представления и прикладного уровня. Сессионный уровень в стеке интерфейса Q обеспечивает синхронизацию при обмене блоками данных протокола (protocol data unit, PDU).

Транспортный уровень обеспечивает оконечные соединения. Транспортный уровень осуществляет контроль потока данных т.е. информация передаётся только в том случае, когда адресат позволяет передачу источнику сообщения. Это предупреждает ситуацию, при которой информация посылается быстрее, чем она может быть обработана получателем. Транспортный уровень осуществляет выявление ошибок и их коррекцию в пакетах данных, например в случае если данные были повреждены при передаче или переприёме. Если поле данных в протокольном блоке слишком велико, то транспортный уровень осуществляет разбиение на блоки (пакеты) меньшей длины при передаче и обратную процедуру сборки протокольного блока на приёме.

На физическом, канальном и сетевом уровнях обеспечивается маршрутизация информации управления в DCN, которая передаётся через интерфейс Q. Передача данных по управлению может осуществляться средствами протокола FTAM на прикладной уровень. Средства интерфейса управления Q обеспечивают шлюз к программному обеспечению менеджера или агента. Это программное обеспечение, по сути, выполняет функции интерфейса Q т.к. поддерживает описание характеристик и режима функционирования управляемого объекта, обеспечивает доступ к функциям и услугам управления.

Сетевой уровень обеспечивает маршрутизацию пакетов и доставку пакетов данных к любому узлу в сети. Основная часть доставки пакета данных сводится с передаче пакета от одного узла к другому на основании локальной таблица маршрутизации узла. Эта часть процесса передача определяется с помощью сетевого *протокола передачи без установления соединения* (connectionless network protocol, CLNP). Усовершенствование CLNP состоит в автоматическом создании и обновлении локальной таблицы маршрутизации. Эта часть описывается протоколом обмена *ES-IS* между *оконечной открытой системой* (end system, ES) и *проме-*

жуточной открытой системой (intermediate system, IS) или протоколом обмена IS–IS. Формат пакетов данных, например кодировка адреса и данных, определены в протоколе CLNP.

На сетевом уровне данные интерфейса Q, могут передаваться, например, через канальный временной интервал в первичном групповом тракте E1 по принципу «из конца - в конец». Этот способ применяется при организации управления удалёнными элементами сети. При расположении управляемых объектов и рабочей станции управления на одном объекте для передачи данных интерфейса Q используется локальная вычислительная сеть.

Канальный уровень обеспечивает определение ошибок и коррекцию данных на уровне бита. Оконечное соединение организуется с помощью протокола LapD (Link Access Procedure D-channel, процедура доступа к линии D–канала), описанного в Рек. МСЭ-Т Q.921.

Преобразование данных протокола LapD с помощью услуг канального уровня описано в Рек. МСЭ-Т G.784. Соединение через Ethernet использует *протокол управления логическим каналом* (logical link control, LLC).

Семейство протоколов X.25 использует *протокол высокого уровня для управления каналом данных* (high-level data link control protocol, LapB), который определён в стандарте ISO 7776.

В итоге, интерфейс Q охватывает все уровни модели ВОС. Важной задачей является правильная спецификация интерфейса Q на верхних уровнях этой модели. Спецификации для программно-аппаратной реализации интерфейса Q в основном разрабатываются с помощью объектно–ориентированного подхода различными международными институтами по стандартизации, такими как ETSI, МСЭ-Т, ISO и производственными консорциумами, подобно АТМ Форуму (ATM Forum). В частности, АТМ Форум разрабатывает спецификации для интерфейсов управления оборудованием, использующим асинхронный режим переноса АТМ.

Для одного и того же типа телекоммуникационного оборудования с помощью объектно–ориентированного подхода может быть разработано несколько информационных моделей интерфейса Q, причём каждая модель затрагивает одну из функциональных областей управления. Это

подтверждается анализом многочисленных рекомендаций ETSI и аналогичных рекомендаций МСЭ-Т, которые описывают модель интерфейса Q для управления конфигурацией и неисправностями сетью доступа и портами пользователя на базе интерфейса V.5.1, V.5.2.

По адресу в Интернете www.etsi.org в свободном доступе можно найти множество спецификаций интерфейса Q для управления различными сетями и оборудованием связи. С учётом предполагаемого повсеместного перехода к повременному учёту местных телефонных соединений безусловно актуально ознакомление с Рек. МСЭ-Т Q.825 «Спецификация приложений управления на интерфейсе Q.3 : Подробная запись о состоявшемся соединении» (введено в действие с 06.1998 г.) – см. перечень в Приложении А.

Функциональные возможности интерфейса Q определяются тем, насколько проведённая работа по спецификации интерфейса соответствует реальным характеристикам и возможностям оборудования.

К примеру, пусть создаётся спецификация интерфейса Q для управления абонентским комплектом (АК). В информационной модели управления отсутствует описание состояний абонентского комплекта с атрибутами «комплект административно заблокирован» и «комплект разблокирован» и допустимыми операциями («изменить состояние комплекта»). Следовательно, администрация связи лишена возможности заблокировать доступ к услугам связи для злостного неплательщика за услуги связи т.к. соответствующий раздел модели отсутствует и требуемая операция не может быть запрошена и реализован через функциональный интерфейс. Проблема состоит в том, что программа-менеджер попросту не «увидит» в программе-агенте и, соответственно, в базе MIB требуемых возможностей по блокировке – ведь их не описали в информационной модели.

Услуги управления абонентскими данными, которые доступны через интерфейс Q, включают, например, определение вида информации, которая доступна абоненту (телефония, факсимильная связь или телеконференции), контроль использования дополнительных услуг (переадресация входящего вызова, конференц-связь, телематические услуги) и т.п.

Модель интерфейса Q для управления телефонной нагрузкой описывает функции управления трафиком, связанные с обработкой вызова в

телефонной сети общего пользования ТФОП и ЦСИО. Цель управления телефонной нагрузкой состоит в обеспечении требуемого оконечного соединения для максимально возможного числа поступивших вызовов при различных условиях эксплуатации АТС, т.е. при нормальном режиме и перегрузке.

В целом функциональность интерфейса Q, который применяется для управления АТС [33] может выглядеть следующим образом (см. таблицу 3.2) :

Таблица 3.2 – Функции управления АТС, доступные через интерфейс Q

№ № п/п	Управляемая область	Функции управления
1	Управление абонентскими и станционными данными	Обеспечение предоставления услуг ТФОП Обеспечение предоставления услуг ЦСИС Управление услугами Centrex Тестирование и мониторинг абонентских и соединительных линий
2	Управление нагрузкой	Маршрутизация потоков вызовов (для данной АТС) Управление телефонной нагрузкой (для данной АТС) Управление ОКС№7 Измерение нагрузки АТС
3	Управление системными ресурсами	Обеспечение живучести при повреждениях Обработка событий Журналирование Управление интерфейсом V.5x Сбор данных об использовании оборудования Управление безопасностью Управление программным обеспечением АТС.

Управление маршрутизацией вызовов связано с функциями анализа цифр набора номера для направления вызова по оптимальному, к примеру по наименее загруженному пути.

В настоящее время большинство спецификаций интерфейса Q основаны на базовых принципах управления, определенных в рекомендации МСЭ-Т серии X.700 и M.3100.

3.3 Описание интерфейса X

Для примера возможностей интерфейса X рассмотрим управление установлением, поддержкой и разъединением тракта между первичной

сетью операторов А и Б через первичную цифровую сеть SDH оператора В на основании документов [22,25].

Как известно, сети SDH разделяются на транспортные слои. Слой каналов обеспечивает передачу пользовательской информации из конца в конец; слой трактов, поддерживает транспорт виртуальных контейнеров (virtual container, VC) и делится на тракты низшего и высшего порядков.

Слой секций гарантирует передачу модулей SDH (STM-n) между сетевыми узлами. Сеть может быть разбита на подсети которые связываются между собой промежуточными трактами или звеньевыми соединениями [22]. Иерархическая модель сети SDH в соответствии с европейской схемой приведена в документе ETSI EN 300 147 V1.4.1. «Transmission and Multiplexing; Synchronous Digital Hierarchy (SDH); Multiplexing structure», 2001. [Передача и мультиплексирование; Синхронная цифровая иерархия; Структура мультиплексирования]).

Общая схема данной модели представлена на рис. 3.2 :

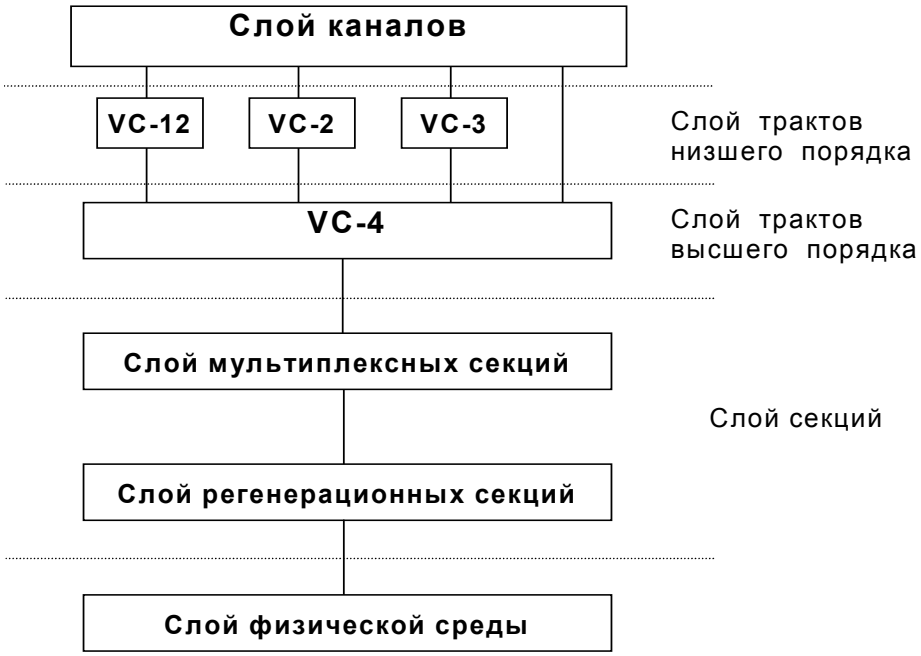


Рисунок 3.2 – Иерархическая модель структуры сети SDH

Управляемыми объектами здесь являются элементы сети (мультиплексоры или кросс-коннекторы), линии связи между ними и тракты VC. Тракты VC соединяются через промежуточные тракты с помощью оконечных элементов первичной сети. В результате создаётся трасса или путь. Тракты могут создаваться ручным или автоматическим выбором трактов

VC-n на каждом участке пути между требуемыми элементами сети. Основные функции уровня управления сетью SDH связаны с обслуживанием трактов VC-12, VC-2, VC-3, VC-4 по принципу «из конца в конец». Тракты VC-n образуются на свободных позициях синхронного транспортного модуля STM-n между двумя оконечными узлами передачи. Функциональные возможности интерфейса X рассматриваются далее на примере двух составляющих процесса управления сетью SDH, а именно управление организацией пути (path provisioning) и управление неисправностями (fault management). Для описания интерфейса управления X между OS оператора А, OS оператора Б и OS оператора В (см. рис. 3.3) предполагается, что в каждой OS есть менеджеры и агенты [25].

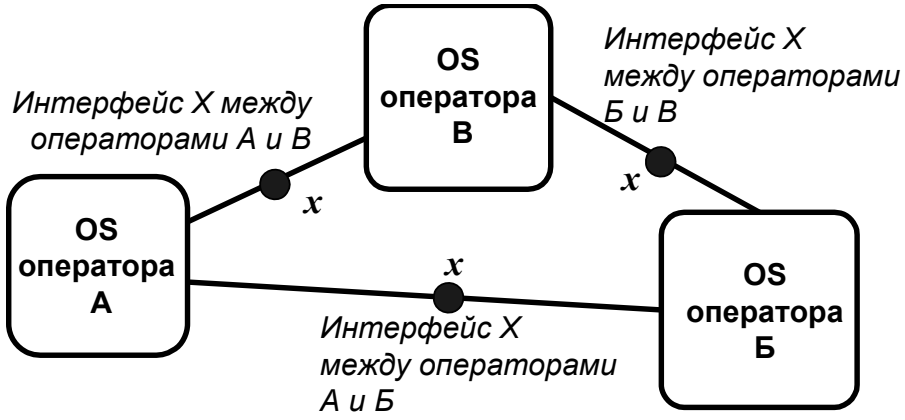


Рисунок 3.3 – Интерфейс X при межоператорском взаимодействии

Техническая сторона задачи выглядит следующим образом. Имеется сеть SDH условно–исходящего оператора А, сеть SDH оператора назначения Б и транзитная сеть SDH оператора В (см. рис. 3.4).

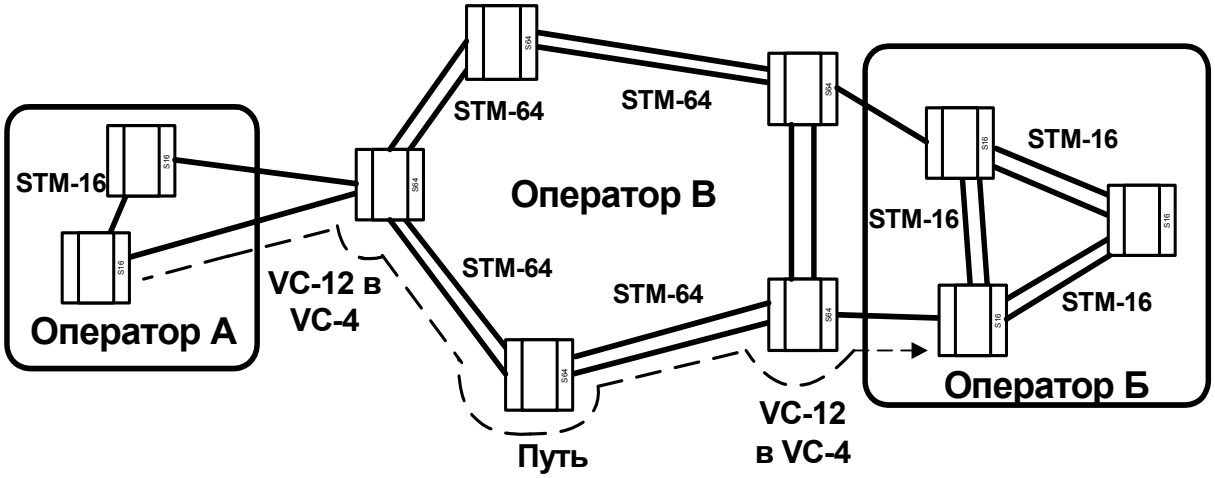


Рисунок 3.4 – Организация связи между операторами первичной сети

Основной целью межоператорского управления первичной цифровой сетью SDH в рассматриваемом примере является автоматизация управления трактом VC–12, который мультиплексирован в тракт VC–4. Управляемые ресурсы состоят из соединений трактов (link connections, LC), отдельных трактов VC–4 и сетей оператора А, Б и В. При этом точкой пересечения LC и условной границы сети операторов управляет только один из оконечных операторов. Каждый из операторов А, Б или В может уведомить других операторов о тех сетевых ресурсах, которые он желает сделать доступными для использования третьей стороной. Сети, где тракт VC–12 начинается и заканчивается, называются *шлюзами*.

Для рассматриваемого случая не существует центральной базы данных с информацией по управлению. Каждый оператор имеет собственные сведения о своей сети и сетях, с которыми он взаимодействует с использованием технологии распределённой базы знаний SMK. Операторы должны распространять данные об изменении характеристик своей сети, прежде всего аварийные сообщения. Аварийное сообщение в первую очередь получает именно тот оператор, который использует неисправный ресурс. Далее рассмотрим отдельно группу услуг управления предоставлением пути (path provisioning) и группу услуг управления неисправностями.

Когда оператор А желает задействовать для передачи тракт VC–12 через транзитную сеть оператора В, этот тракт VC–12 и *предоставляемое соединение тракта* (deliverablerable link connection, DLC) должны быть предварительно зарезервированы. Соединение тракта VC-12 осуществляется в слое трактов низшего порядка.

Запрос на резервирование посылается условно исходящим оператором А ко всем операторам вдоль предполагаемого пути. Получаемые оператором А ответы на запросы содержат *идентификаторы* (identificators, ID) оконечных точек пути по каждому оператору и ID зарезервированных DLC.

Когда запрос на резервирование удовлетворен, оператор А может активировать (задействовать) путь, посылая следующие сигналы операторам Б и В :

- запрос на активизацию DLC;

- запрос на установление соединений трактов в сетях между DLC, которые начинаются и заканчиваются известными оконечными точками с идентификатором ID.

Предусмотрена возможность частичного освобождения пути, который ещё не был задействован. Процедура отмены резервирования запускается автоматически в том случае, если DLC не был активизирован в течении оговоренного периода времени.

Множество функций управления MFS, которые используются для организации предоставления пути, состоит из следующих функций :

- *Резервирование DLC* – резервирование множества DLC внутри требуемого пути.
- *Отмена резервирования DLC* – отмена резервирования множества DLC внутри требуемого пути.
- *Отмена резервирования по истечении времени* – отмена резервирования DLC в связи с несостоявшейся активизацией за указанное время.
- *Активизация пути* – активизация множества DLC или соединения *подсети SNC* (SubNetwork Connections, соединение через подсеть между окончаниями пути, в данном случае подсетью является сеть B). Активизация, как правило, осуществляется сразу после резервирования.
- *Разъединение пути* – деактивизация и отмена резервирования множества DLC или SNC внутри пути.
- *Обновление доступных соединений* – обусловленное внутренними причинами изменения доступных соединений DLC внутри пути.
- *Возможность обновления соединения* – уведомление, которое обозначает техническую возможность подсети поддерживать установление новых соединений.

Множество функций управления MFS, как показано ранее в разделе 3.1, декомпозируются на отдельные функции управления. Результат декомпозиции показан в таблице 3.3.

Реализация каждой функции управления из таблицы 3.3 состоит из примитива запроса и примитива ответа на запрос.

Таблица 3.3 – Функции управления для организации пути в сети SDH

Наименование множества функций управления MFS	Функции управления
Резервирование DLC	Резервирование DLC (DLC Reservation)
	Распространение по сети изменений в данных о доступных соединениях (Available Connections Change Dissemination, ACCD).
Отмена резервирования DLC	Отмена резервирования DLC
	ACCD
Отмена резервирования по истечении времени	ACCD
Активизация пути	Активизация DLC
	Установка SNC
Разъединение пути	Разъединение DLC
	Разъединение SNC
Обновление доступных соединений	ACCD
	Чтение данных о доступных соединениях
Возможность обновления соединения	Способность распространять по сети информацию об изменении соединений, ATCCD (ability to connect change dissemination)
	Способность к чтению данных о доступных соединениях

Группа услуг управления неисправностями обеспечивает передачу сообщений о неисправностях только операторам, которые используют данные тракты и подсети. Операторы на рис. 3.4 должны поддерживать журналирование в специальный файл всех аварийных сообщений, которые посылаются корреспондирующим операторам. Этот файл журналирования должен быть частично доступен и другим операторам для того, чтобы сохранить возможность отслеживания (трассировки) всех случайно потерянных сообщений о неисправностях. Наличие и доступность файла журналирования позволяет, например, оператору А в любое время получить доступ к файлам журналирования другого оператора для ознакомления и проверки. Доступ осуществляется только в части аварийных сигналов, посланных оператору А (к примеру, те сообщения, которые могли быть посланы или те сообщения, которые были потеряны).

Когда появляется сообщение о неисправности соединений трактов LC или об изменениях в отношении существующих соединений LC, то менеджеру, который управляет предоставлением пути, посылается специальное межгрупповое сообщение. Менеджер распространяет это сооб-

щение всем операторам для обновления данных о существующей сетевой ситуации.

Множество функций MFS, которые входят в состав группы управления неисправностями, состоит из следующих функций :

- *Обработка сообщения о неисправности* (alarm processing) – получение сообщения о неисправности, распространение сообщения о неисправности по другим получателям и обновление сведений о состоянии сети;
- *Журналирование аварийных событий* (alarm event logging) – включает контроль файлов журналирования.

Множество функций управления неисправностями, доступные через интерфейс X, состоят из отдельных функций управления, как это показано, к примеру, в таблице 3.4 на следующей странице. Каждая функция управления из таблицы 3.4 состоит из примитива запроса и примитива ответа.

Таблица 3.4 – Функции управления для обработки аварийных сообщений

Наименование множества функций управления	Функции управления
Обработка аварийного сообщения	Распространение по сети аварийных сообщений
Журналирование аварийных событий	Проверка файла журналирования

Итак, на примере первичной сети связи SDH показано, какого рода информацией обмениваются различные операционные системы управления сетью через интерфейс X.

3.4 Описание интерфейсов F и G

Интерфейс F соединяет рабочие станции WS с операционной системой OS или с устройствами медиации MD. Интерфейс F предназначен для обеспечения доступа пользователя к системе управления электросвязью. Через интерфейс F происходит обмен данными, которые могут использоваться как для внутренней обработки в системе сетевого управления, так и для обмена информации между системами. Здесь могут

применяться средства описания данных GDMO/ASN.1 или IDL. Опорная точка f осуществляют адаптацию информации OS для функции рабочей станции WSF; через соответствующий интерфейс F данные поступают на рабочую станцию WS. Через интерфейс F реализуется трансляция информации OS для дальнейшего представления на дисплее оператора; выполняется и обратная трансляция – данные, введённые оператором преобразуются в информацию, понятную OS.

Информационная модель интерфейса F может включать данные, которые недоступны элементу сети, но необходимы для обмена между пользователями системы управления и OS. К такой информации относятся списки выполняемых заданий системы управления, расписание запуска этих заданий и т.п. Соответственно на интерфейсе F определены следующие функции управления (см. таблицу 3.5) [29,30]:

Таблица 3.5 – Функции управления, доступные через интерфейс F

Область управления	Функции управления
Управление рабочими характеристиками	Предоставление информации об измерении трафика
	Создание нового графика для обработки сообщений об измерениях трафика
	Запрос данных об измерении трафика
	Список всех запрошенных сообщений
	Отмена запроса об измерении трафика
Управление неисправностями (последствиями отказами)	Генерация аварийного сообщения
	Регистрация (журналирование) неисправности
	Выбор файла регистрации неисправности
	Подтверждение факта неисправности
	Испытание оборудования (множество функций)
	Планирование испытаний (множество функций)
Управление конфигураций	Получение подробной информации относительно уровня обслуживания абонентов или элементов сети.
	Проверка состояния, модернизация, отмена уровня обслуживания абонентов или элементов сети.
	Конфигурация управляемого ресурса
Управление расчётами за услуги связи	Получение информации по выставлению счёта за оказанные услуги связи.
	Согласование счёта
	Информация пользователя об поступлении оплаты по счёту
Управление безопасностью	Обеспечение безопасности доступа пользователей в систему управления.

Непосредственный доступ пользователя к функциям, указанным в таблице 3.5 осуществляется через интерфейс G рабочей станции. Интерфейс G пользователя в TMN можно рассматривать как практическую реализацию средств интерактивного взаимодействия между системой управления и внешним агентом. Агентом может являться пользователь системы, физическое устройство, прикладная программа.

Существует несколько стандартов и значительное число рекомендаций, посвященных описанию интерфейса G. Стандарт ISO 9241 «Эргономические требования к работе с пультом визуального отображения информации в учреждении» включает в себя много разделов, посвящённых различным аспектам работы с дисплеями. Только некоторые части этого документа имеют статус международного стандарта. Достоинством данного документа можно считать ориентацию на «человеческий фактор», а не на описание возможностей программного обеспечения. Для описания интерфейса G важны следующие части стандарта ISO 9241 : часть 10 «Принципы диалогового режима», часть 11 «Руководство по использованию», часть 13 «Руководство пользователя», часть 16 «Непосредственное манипулирование объектами в режиме диалога». Организация МСЭ–Т разработала стандарты на интерфейсы пользователя в рамках рекомендаций серии МСЭ–Т Рек. Z.300 и Z.350.

Из коммерческих стандартов в наибольшей степени отвечает задачам TMN интерфейс OSF/Motif а также руководство по разработке приложений для платформы управления Hewlett-Packard Open View. Аналогичные руководства имеют компании IBM (США) под названием *общий интерфейс пользователя* (common user access, CUA) и компания Microsoft Corporation (США).

Основное меню интерфейса пользователя системы сетевого управления должно соответствовать функциональности системы управления. Например, пусть система сетевого управления состоит из нескольких OS : OS для управления сетью SDH, OS для управления сетью PDH, OS для управления сетью ATM. Тогда главное меню интерфейса каждой OS соответствует общему назначению OS, а второй уровень экранного меню должен отражает функциональность, которая специфична для каждой OS.

Заполнение в процессе диалога полей данных в экранных формах – ещё один важный аспект работы интерфейса пользователя. Экранные формы применяются для отображения сообщений о неисправностях, для ввода параметров при техническом обслуживании и эксплуатации, для ввода имени и пароля пользователя при начале работы с системой управления.

Манипулирование объектами управления предусматривает графическое выделение символов на экране, перемещение символов, соответствующих объектам управления, по дисплею. Символы (пиктограммы) на экране условно отображают управляемые объекты.

Выделение цветом может означать, к примеру, изменение административного статуса атрибутов объекта с «Доступен» на «Недоступен», что влечёт за собой невозможность вмешиваться в работу элемента сети для администрации связи.

Цвета играют особую роль при отображении информации управления на экране рабочей станции. Целесообразно одновременно использовать четыре различных цвета. В таблице 3.6 показаны возможные цвета для кодирования состояния управляемых объектов:

Таблица 3.6 – Цветовое решение графического интерфейса пользователя

Назначение	Цвет	Применение цветовой кодировки
Общее обозначение	Серый	Базовые символы, нет индикации состояния объекта (например, технически исправные объекты)
Обозначение неисправности (отказа)	Красный	Критическая неисправность или нештатное состояние услуги управления
	Жёлтый	Неисправность, состояние услуг управления штатное
	Зелёный	Неисправность устранена или прекратила своё действие
	Синий	Предупреждение или неопределённое состояние (т.е. неисправность не обнаружена, рабочий режим нештатный)

Графическое представление сети важно как для управления неисправностями, так и для контроля и управления маршрутами установления соединений. Одна и та же графическая схема сети на экране может быть использована для реализации многих услуг управления. Схема сети должна генерироваться автоматически, на основании сведений о составе, состоянии и размещении управляемых объектов. Схема сети и её эле-

менты периодически обновляются в соответствии с сетевой ситуацией и в связи с изменением состояния управляемых объектов.

На экран рекомендуется вывод не более трёх уровней отображения сети: фоновый рисунок (географическая карта), средний уровень, который включает объекты с которыми работает оператор и передний план, на который выводятся основные сигналы или данные по управлению. Эти уровни должны различаться по цвету, яркости, насыщенности и по используемым цветовым решениям.

Помимо графических изображений в интерфейсе G для взаимодействия с пользователем используются сообщения. Сообщения могут выдаваться в следующих формах :

- короткий и ясный текст;
- речевое сообщение (автоинформатор);
- звуковые сигналы.

Пользователь должен однозначно воспринимать и интерпретировать сообщение. Особый раздел сообщений представляют собой инструкции по пользованию программой в виде «Help» (меню «Помощь») или в виде контекстной подсказки. Эти сообщения должны, например, указывать пользователю на то, ввода каких данных ожидает система. Сообщения системы (системная информация) генерируется системой управления для того, чтобы пользователь имел представление о текущих заданиях и действиях системы. Среди сообщений системы можно выделить следующие :

- уведомления и сообщения о состоянии системы;
- информация о выполняемых заданиях;
- предупреждения т.е. извещение пользователя о потенциальных или появившихся неисправностях и отказах;
- требование вмешательство пользователя – сообщение о ситуации , в которой для продолжения действий системы управления требуется вмешательство оператора системы;
- запросы системы – предложение пользователю провести выбор одного из разделов (пунктов) меню.

Интерфейс G – это основной интерфейс для обмена между пользователем и системой сетевого управления. Персонал оператора связи

оценивает функциональность системы сетевого управления по тем возможностям, которые предоставляет пользователю интерфейс G. Поэтому разработка интерфейса G должна проводиться не менее тщательно, чем других интерфейсов TMN.

3.5 Методология разработки интерфейсов TMN

Методология разработки интерфейсов TMN называется UTRAD (Unified TMN Requirements, Analysis and Design) [27]. Эта методология описывает процесс разработки описаний (спецификаций) интерфейсов TMN. При разработке описаний интерфейсов, а также других объектов TMN, необходимо учитывать следующие факторы :

- требования к интерфейсу со стороны пользователя;
- анализ проблемы и постановка задачи;
- технология разработки.

Совокупно перечисленные факторы обозначаются как RAD (user Requirements, Analysis and Design). В настоящее время правила для реализации RAD рекомендуют использовать способ записи данных об интерфейсе с помощью графического *языка унифицированного моделирования* (unified modelling language, UML). Детальная проработка применения UML для описания интерфейсов TMN находится в стадии разработки исследовательских групп МСЭ-Т. Поэтому допускается пользоваться и другими методологиями для спецификаций интерфейсов TMN, например GDMO.

Спецификация интерфейсов TMN с точки зрения услуг (сервисов) управления определена в Рек. МСЭ-Т М.3200. Услуги управления реализуются с помощью несколько функций управления. Приведённые в Рек. МСЭ-Т М.3400 стандартные функции управления могут удовлетворить условиям большинства вариантов сетевого управления и являются основой для создания новых функций управления.

Методология UTRAD включает три стадии итеративного процесса разработки спецификаций интерфейсов, причём существуют средства для отслеживания отдельных этапов разработки интерфейсов (трассирование).

Три стадии UTRAD выглядят следующим образом :

1. Формирование требований пользователя (как правило, это общие требования).
2. Анализ требований и учёт возможностей функций управления.
3. Разработка описания интерфейса или управляемого объекта.

Все три стадии разработки описания интерфейсов TMN в рамках UTRAD используют современные информационные технологии, в частности объектно-ориентированный подход к анализу и разработке описания интерфейсов.

При завершении каждой из трёх перечисленных стадий формируются следующие документы (данные):

- *Стадия формирования требований к интерфейсу* – в результате формируются и документируются требования к интерфейсу.
- *Стадия анализа* – в результате формируются отдельные описания или спецификации для внедрения интерфейса.
- *Стадия разработки* – разрабатывается технологическое описание интерфейса; описание не зависит от программно-аппаратных средств реализации интерфейса.

На стадии разработки создаётся детальное описание интерфейса или объекта TMN. В контексте использования в TMN семиуровневой модели ВОС, разработка описаний интерфейса представляет собой описание информационной модели управления с использованием шаблонов GDMO для классов управляемых объектов, атрибутов, поведения объектов, уведомлений, действий, ошибок и исключений из правил. Синтаксис записи использует специальный язык ASN.1 или UML. На стадии разработки рекомендуется, чтобы описания UML, выполненные на стадии требований и анализа, были дополнены описаниями режима работы управляемого объекта

При использовании в TMN технологии CORBA, информационная модель разрабатывается с помощью языка IDL. Описание технологии CORBA можно найти в учебнике «Конструирование распределённых объектов», В. Эммерих Пер. с английского. – М.: Мир, 2002 г. (серия «Лучший зарубежный учебник»).

Контрольные вопросы к главе 3.

1. Дайте определение функции управления TMN.
2. В чём различие между опорной точкой и интерфейсом TMN?
3. Можно ли с помощью TMN управлять сетью ОКС №7?
4. Для управления какими характеристиками АТС используется интерфейс Q?
5. Какие задачи управления решаются с помощью интерфейса X?
6. Применяется ли к интерфейсу G графический стандарт интерфейсов пользователя?
7. Какие стадии включает разработка описания интерфейса TMN?

4. ОБЩИЙ ПРОТОКОЛ ИНФОРМАЦИИ УПРАВЛЕНИЯ CMIP

4.1 Реализация управления в модели ВОС

Управление в рамках эталонной семиуровневой модели взаимосвязи открытых систем ВОС (предложена Международной организацией по стандартизации, ISO) можно рассматривать как взаимодействие между объектами с помощью *коммуникационных протоколов* для обеспечения функций и услуг управления [31]. Объектом управления является информация управления, которой обмениваются взаимосвязанные открытые системы. Стандарты ISO определяют коммуникационные протоколы как обобщенные функции, необходимые для успешного обмена информацией управления между программами прикладного уровня различных открытых систем. Соответствующий стандарт ISO 9595 содержит описание услуг управления с помощью *элемента общей услуги информации управления* (Common Management Information Services Element, CMISE). В рамках объектно-ориентированного подхода *элемент CMISE* рассматривается как *элемент услуги приложения* (application service element, ASE), разработанный для поддержки управления системами [23,35].

Элемент услуги приложения ASE – это логический объект, который обеспечивает взаимодействие между различными приложениями управления. Предметом управления ASE может являться контроль взаимодействия между элементами услуги управления. К услугам ASE относится управление передачей файлов, управление доступом, удаленное управление директориями. При реализации ASE предусматривается возможность многократного использование этого элемента несколькими приложениями управления.

Определение CMISE, как и определения любого стандарта ВОС, осуществляется в терминах услуг или сервисов, которые обеспечиваются пользователю с помощью т.н. *машины протоколов* (protocol machine). Машина протоколов позволяет формировать *блоки данных протокола* PDU, которыми обмениваются равноправные или одноуровневые, с точки зрения модели ВОС, приложения управления. Услуги управления информацией используются приложениями управления для обмена инфор-

мацией и необходимыми командами. Существуют следующие услуги управления ВОС :

1. *Услуги управления ассоциацией* (management association services, MAS) – это услуги, которые обеспечивают организацию обмена информацией между управляемым объектом и управляющим объектом. Услуги MAS реализуется с помощью трёх услуг :
    - Услуга M-Associate – позволяет данной функции CMISE инициализировать взаимодействие с равной по уровню (с точки зрения модели ВОС) функцией CMISE другой открытой системы.
    - Услуга M-Release – штатно прерывает взаимодействие между равными, с точки зрения ВОС, функциями CMISE.
    - Услуга M-Abort – используется, когда взаимодействие между функциями прерывается нештатно.
2. *Услуга передачи уведомлений в процессе управления* (management notification service, MNS) – это одиночный сервисный элемент, который используется, чтобы передать прикладной программе уведомление/подтверждение о получении информации по управлению.
3. *Услуги управления операциями* (management operation services, MOS) состоят из шести операций, с помощью которых оказываются услуги по передаче и обработке информации, которой обмениваются программные приложения управления :
    - операция M-GET – получение информации об управляемом объекте (открытой системе);
    - операция M-SET – установка значения атрибута (параметра); операция M-CREATE – создание описания управляемого объекта;
    - операция M-DELETE – удаление описания управляемого объекта; операция M-ACTION – инициализация действия/процедуры/ операции;
    - операция M-EVENT-REPORT – генерация сообщения о сетевом событии;
    - операция M-CANCEL–GET – отмена операции получения информации об управляемом объекте.

Услуги управления в процессе взаимодействия с пользователями (приложениями управления) показаны на рис. 4.1.

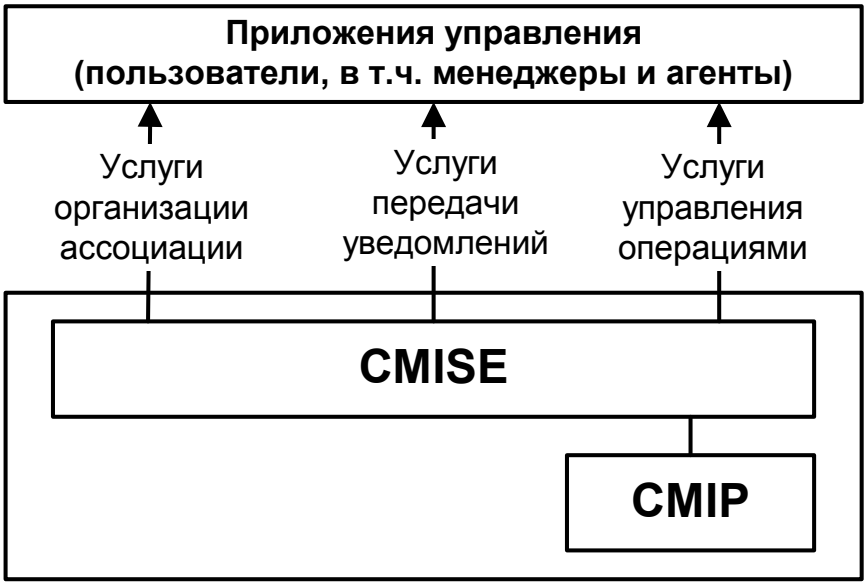


Рисунок 4.1 – Взаимодействие между приложениями управления и CMISE

Услуга общей информации управления, использующая CMISE, предоставляет дополнительные возможности по структурированию информации управления. В частности, операции управления могут выполняться на нескольких управляемых объектах, которые выделяются по определённым критериям.

Элементы, формирующие структуру управления ВОС и относящиеся к ASE, следующие:

- *Элемент услуги управления системой* (system management application service element, SMASE).
- *Элемент услуги общей информации управления* (common management information service element, CMISE).
- *Элемент услуги управления ассоциацией* (association control service element, ACSE).
- *Элемент услуги удаленного выполнения операции* (remote operations service element, ROSE).
- *Функция координации* (co-ordination function).

Взаимодействие между элементами структуры управления реализуется с помощью *прикладного программного интерфейса* (application program interface, API).

Элемент SMASE при физической реализации представляет собой программное приложение или аппаратно-программный комплекс, который в автоматическом режиме или с помощью оператора инициирует выполнение той или иной операции управления. Основные из перечисленных элементов в их взаимосвязи показаны на рис. 4.2.

Элемент ACSE используется, чтобы установить *ассоциативные связи или ассоциации* (application associations) между программными приложениями, т.е. между программой-менеджером и программой-агентом. Приложения управления, разумеется, должны поддерживать правила, которые необходимы для координации обмена информацией между различным ASE. Эти правила записываются с помощью параметров услуг пользователя ASCE.

Элемент ACSE включает два необязательных функциональных блока. Один функциональный блок поддерживает информационный обмен данными по аутентификации при создании ассоциативной связи; второй блок поддерживает согласование контекста обмена при установлении ассоциации.

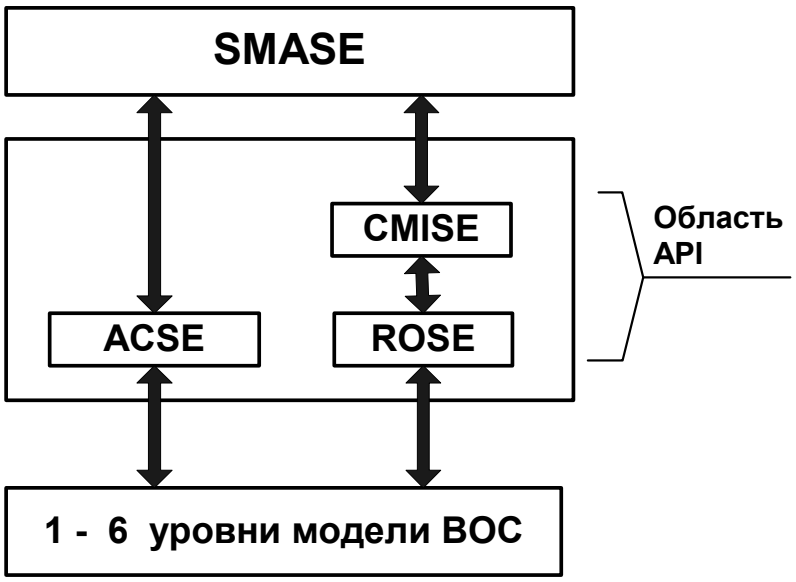


Рисунок 4.2 – Элементы ASE в модели управления ВОС

Элемент ROSE используется для оформления информационных запросов и их передачи с помощью механизма *удаленного вызова процедур* (remote procedure calls, RPC) используемого в разных системах. В рамках международных стандартов, как правило, рассматриваются эле-

менты и услуги модели ВОС, имеющие отношение к обмену информацией управления, а внутренняя логика процесса управления не затрагивается. Следует отметить, что в книге [4] ASE рассматривается в рамках описания подсистемы INAP системы общеканальной сигнализации ОКС №7.

Всего в CMISE имеются два вида средств управления системами, удовлетворяющих стандартам ВОС. Это *общие услуги информации управления* (common management information services, CMIS) и *общий протокол информации управления* (common management information protocol, CMIP), определяемые стандартом ISO 9696.

Услуги CMIS определяют функции для контроля и управления сетью, обеспечивают интерфейс пользователя услуг управления. Протокол CMIP используется для поддержки обмена информацией управления между открытыми системами. Протокол CMIP обеспечивает взаимодействие открытых систем на прикладном уровне ВОС. В итоге, CMIS и CMIP являются частью большого и достаточно сложного набора стандартов для управления системами на основе модели ВОС.

CMIS определяет услуги, которые могут поддерживать программы-менеджеры и программы-агенты. CMIS также определяет набор *функциональных модулей*, благодаря которым поддерживаются услуги управления. Функциональные модули включают описание возможных услуг управления и предназначены для поддержки параметров услуг. Когда менеджер и агент устанавливают связь друг с другом, они «договариваются» о том, какие услуги (т.е. какие функциональные модули) будут использоваться при взаимодействии. Функциональный модуль является компонентом программного приложения управления.

Протокол обмена информацией CMIP основан на парадигме ответа на запрос, где менеджер с помощью запроса инициирует операции управления на одном или большем количестве управляемых объектов. Услуги и протоколы определены посредством :

- описания различных операций, которые осуществляются системой управления на управляемых объектах;
- с помощью ответных сообщений/уведомлений, которые выдаются управляемыми объектами по направлению к управляющей системе.

Описываемая архитектура требует, чтобы была чётко определена логическая и информационная структура управляемого объекта. В данном случае управляемый объект является абстрактным представлением управляемого физического ресурса и содержит информацию управления, требуемую для успешного осуществления процесса управления. При каждом информационном обмене программа–менеджер посылает программе–агенту запрос на выполнение операции управления с помощью протокола CMIP (см. рис. 4.3).

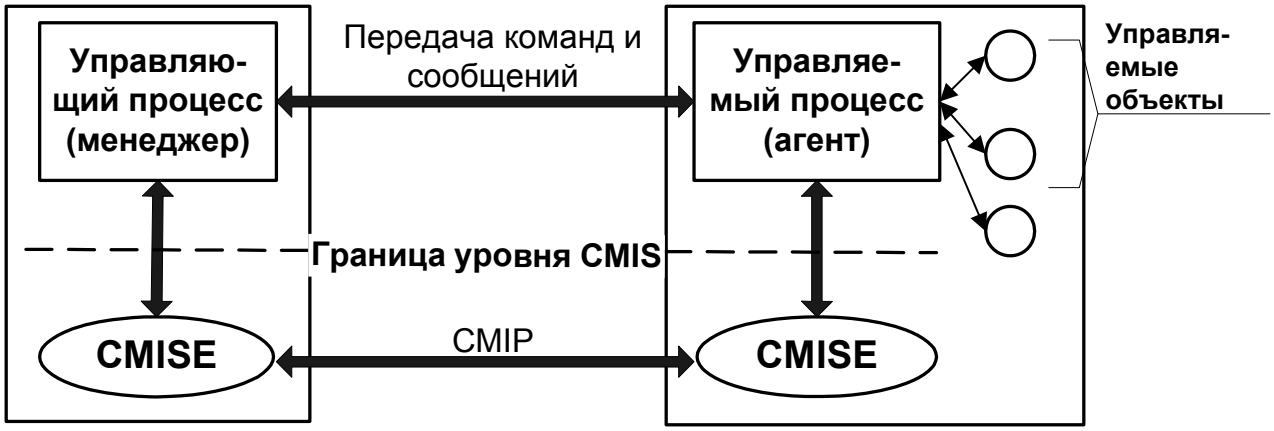


Рисунок 4.3 – Управление открытыми системами в рамках модели «менеджер-агент»

Операции управления подразумевают наличие протокола информационного обмена для создания, удаления, чтения данных и изменения информация управления. Термин «Информация управления» (management information) используется здесь для описания свойств управляемых объектов. В дополнение к вышеупомянутым операциям, CMISE поддерживает сообщения, которые генерируются на управляемых объектах и содержат информацию о происшедших на объекте событиях.

В данном случае протокол CMIP применяется как протокол информационного обмена для поддержки операций создания, удаления объектов в MIB, считывания данных об управляемом объекте и изменения информация управления.

Если управляемым объектом является аппаратная часть элемента сети – например абонентский комплект, то такой управляемый ресурс как процесс приёма и трансляции цифр набора номера в CMISE не рассматривается т.к. в данном случае операции по обработке принятых цифр

абонентского номера осуществляются в реальном масштабе времени и поддерживаются встроенным программным обеспечением управления АТС, которое не относится к TMN.

Протокол CMIP поддерживает доступ к базам данных управления MIB т.е. доступ к упорядоченной совокупности данных об управляемых объектах. Управляемые объекты на уровне базы данных имеют заданные имена, им присваиваются атрибуты, описывается допустимое поведение (режим работы) объектов. Данные об управляемых объектах могут быть созданы, удалены, модифицированы.

Сведения MIB позволяют прикладной программе управления осуществлять действия над объектами, которые инициированы сетевым менеджером. Описание поведения объекта в MIB обусловлено ресурсом управления, который этот объект представляет. Например, функционирование терминального окончания соединительной линии или канала связи может зависеть от функционирования (поведения) других компонентов системы, например системы синхронизации или типа физической среды переноса сигнала электросвязи.

Как уже говорилось, атрибуты управляемого объекта описывают состояние и поведение данного объекта. Продолжая рассматривать в качестве примера терминальное окончание (например, сетевое окончание типа NT1, NT2 в ЦСИС) можно сказать, что атрибуты включают ссылки на другие объекты, с которыми взаимодействует терминальное окончание. Например в модели сети ЦСИС допустимы ссылки на описание в MIB интерфейсов типа S или типа U.

По аналогии, *действия* (actions) рассматриваются здесь как услуги, которые объект может обеспечивать при запросе со стороны системы управления. Типовые примеры или *шаблоны* (templates) для описания поведения управляемых объектов определяются в TMN средствами GDMO и ASN.1.

Тип услуги или сервиса CMISE определяет набор элементарных операций или *примитивов*, с помощью которых пользователь услуг CMIS получает доступ к услугам управления. К таким примитивам относится, например, примитив «Запрос» (*request*), который указывает на требование предоставления услуги CMIS (см. раздел 2.2.5).

В CMIS существует механизм выдачи подтверждений о выполнении request, а некоторые услуги CMIS также поддерживает неподтверждаемые операции т.е. операции, выполнение которых не требует специального подтверждения о выполнении. Кроме примитива *request* существуют следующие примитивы :

- *indication* [индикация] – свидетельствует о наступлении какого–то события, например поступление запроса request;
- *response* [ответ, отклик] – ответная реакция на событие, например выполнение запроса;
- *confirmation* [подтверждение] – сообщение о поступлении ответа на направленный запрос.

Соответственно, примитив запроса услуги Get для пользователя CMISE буден записан как M-GET request, а примитив ответа на запрос Get будет записан как M-GET response.

Операции запроса с подтверждением (confirmed request operations) всегда требуют ответа, независимо от успеха или отказа в совершении операции. Операции *запроса, не требующие подтверждения* (unconfirmed request operations), не получают подтверждения о выполнении.

Услуги с подтверждением требуют, чтобы агент, который выполняет операции на управляемом объекте, послал с помощью CMIS управляющей системе т.н. *«квитанцию» о приёме* или *ответ* (receipt, responce) со сведениями о том, осуществлялась ли требуемая операция управления успешно или произошла ошибка. При услугах без подтверждения такой механизм отсутствует.

Далее рассматривается протокол CMIP.

4.2 Общий протокол информации управления CMIP

Как отмечалось в разделе 4.1, протокол CMIP используется CMISE для обмена информацией управления. Этот протокол позволяет осуществлять управление элементами всех уровней модели ВОС т.к. обеспечивает обмен информацией управления. Протокол CMIP формирует блоки данных протокола PDU и осуществляет обмен PDU между одноуровне-

выми приложениями управления. В дополнение к ACSE, обмен PDU зависит от ROSE. Протокол CMIP используется для обеспечения услуг управления операциями и услуг передачи уведомлений CMISE. В совокупности CMISE, ASCE и ROSE представляют собой стек протокола CMIP. Каждая услуга CMISE определяется с помощью нескольких CMIS-примитивов, которые отображаются в виде соответствующих PDU. Список примитивов и форматов сообщений CMIP приведён в рекомендации МСЭ-Т X.710 (аналог рекомендации ISO/IEC 9595) и МСЭ-Т Рек.X.711 (аналог рекомендации ISO/IEC 9596-1).

Важное значение в понимании функционирования протокола CMIP имеет понятие *протокольной машины CMIP* (common management information protocol machine, CMIPM). Протокольная машина является логическим представление основных функций протокола CMIP. На стороне менеджера, который выдаёт управляющие команды, протокольная машина принимает запросы пользователя CMIS на предоставление услуг управления. На основании запросов в CMIPM инициализируются те или иные примитивы. В результате CMIPM выдаёт ответы (подтверждения) на запросы услуг, а также генерирует блоки данных CMIP PDU, которые передаются на нижестоящий уровень ROSE для осуществления операций, необходимых пользователю услуг CMISE (см. рис. 4.4).

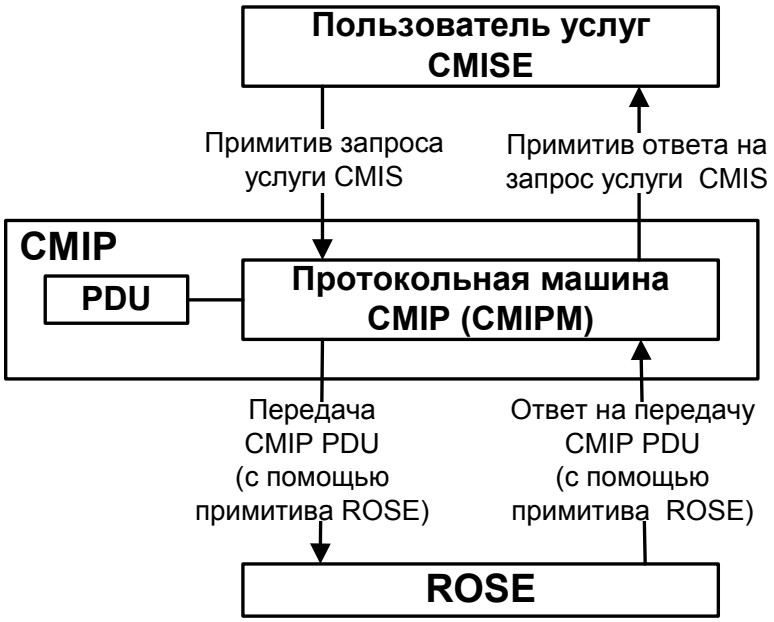


Рисунок 4.4 – Протокольная машина CMIPM

На стороне агента, т.е. при выполнении управляющей команды, машина CMIPM принимает с нижестоящих уровней корректные PDU и передаёт информацию о требуемых услугах управления на уровень CMISE. Если PDU не корректен, то такой PDU отбрасывается, о чём выдаётся соответствующее уведомление в сторону менеджера.

Важно, что машина CMIPM осуществляет только обработку данных PDU, не затрагивая вопроса о том, что происходит с данными на уровне CMIS или, к примеру, как инициализируются услуги CMIS со стороны пользователя.

Согласно Рек. МСЭ–Т X.638, перед наименованием услуг и соответствующий операций CMISE указываются специальные буквенные идентификаторы :

- Символ R указывает на принадлежность услуги или примитива к ROSE согласно стандарту ISO/IEC 9072-4.
- Символ A указывает на принадлежность услуги или примитива к ACSE согласно Рек. МСЭ–Т X.247 или аналогичному стандарту ISO/IEC 8650-2.
- Символ P указывает на принадлежность услуги или примитива к уровню представления согласно Рек. МСЭ–Т X.246 или аналогичному стандарту ISO/IEC 8823-2.
- Символ S указывает на принадлежность услуги или примитива к сессионному уровню согласно Рек. МСЭ–Т X.245 или аналогичному стандарту ISO/IEC 8327-2.

Система с подтверждением должна использовать по крайней мере одну из приведенных услуг. При этом система может выполнять функции как управляемой системы так и управляющей. В данный момент времени система либо сама является управляющей, либо управляется другой системой. Далее рассмотрим некоторые услуги, доступные с помощью CMIP.

В процессе обмена информацией услуга A-ASSOCIATE и соответствующие примитивы используются для установления взаимодействия между двумя приложениями.

Услуга A-RELEASE используется в том случае, когда пользователь, пославший запрос, не согласен с ранее организованным взаимодействи-

ем между приложениями. При этом в случае прекращения ранее установленной связи между приложениями не происходит потери информации.

Услуга A-ABORT используется в случае ошибок при передаче информации или при аварии. При использовании услуги A-ABORT с целью аварийного обрыва сеанса обмена информацией между двумя приложениями существует потенциальная возможность потери информации. Услуга A-ABORT используется в случае, когда обнаружено нарушение коммуникационного протокола или когда сеанс связи между приложениями еще не установлена.

Услуга A-P-ABORT используется для обнаружения аварийного прекращения операции на уровне представления с возможной потерей информации при обмене информацией.

С помощью протокола CMIP доступны следующие услуги ROSE :

- услуга RO-INVOKE;
- услуга RO-RESULT;
- услуга RO-ERROR;
- услуга RO-REJECT.

Услуги ROSE и их описание сведены в таблицу 4.1.

Таблица 4.1 –Услуги ROSE

Услуги ROSE	Определение услуги ROSE
RO-INVOKE	Позволяет программе управления (инициатору) запросить другую программу (получатель запроса) о выполнении получателем некоторой операции. Получателем может быть программа, установленная на удалённом управляемом объекте.
RO-RESULT	Позволяет получателю запроса RO-INVOKE передать (возвратить) инициатору результат выполнения запрошенной операции.
RO-ERROR	Позволяет получателю запроса RO-INVOKE передать отрицательный ответ на запрос или передать сообщение об ошибке.
RO-REJECT-U	Позволяет отказаться выполнять запрошенную операцию, если получатель запроса обнаружил ошибку.
RO-REJECT-P	Позволяет инициатору запроса информировать получателя запроса ROSE об ошибке.

Схема взаимодействия перечисленных услуг приведена далее на рис. 4.5.

Следует отметить, что на схеме рис. 4.5 не указан уровень SMASE, взаимодействие с которым осуществляется с уровня CMISE через прикладной программный интерфейс API CMISE. Подробнее этот вопрос рассмотрен в книгах [7,9].

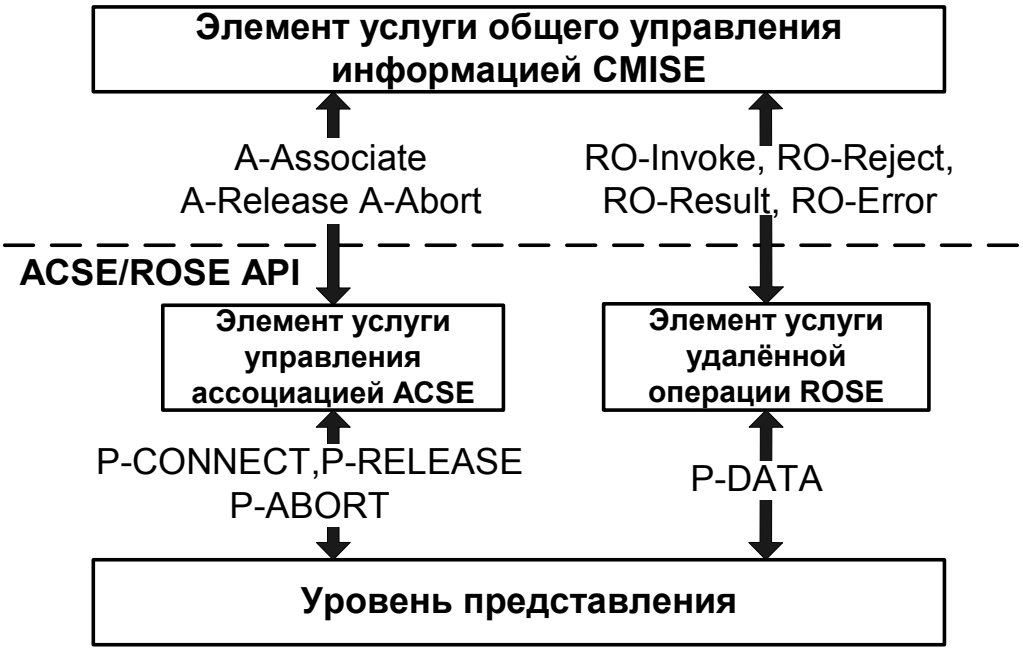


Рисунок 4.5 – Стек протокола CMIP : ACSE и ROSE

Согласно Рек. МСЭ-Т X.711 и разделу 2.2.5, каждой услуге, например A–ASSOCIATE, соответствует свой примитив запроса на предоставление данной услуги. Этот примитив обозначается как A–Associate.

Аналогично, услуге RO-INVOKE соответствует примитив RO-Invoke. Примитив запроса формируется в виде соответствующего PDU приложения (Application PDU, APDU) и обозначается как RO-INVOKE request, где RO указывает на принадлежность к ROSE, INVOKE – имя примитива, request – тип примитива. После обозначения примитива могут указываться пароли, данные, которые передаются с помощью примитива.

В качестве примера функционирование CMIS и ROSE с помощью протокола CMIP рассмотрим услугу установления IP-адреса удалённого компьютерного устройства с помощью услуги и соответствующей ей процедуры Get

Процесс обмена примитивами и соответствующими им PDU при выполнении рассматриваемой процедуры приведён на рис. 4.6 на следующей странице. Здесь показано, как система управления (инициатор за-

проса) SMISE выполняет процедуру M-Get. Обработка примитива M-GET[1] request на CMIPM приводит к инициализации машины протокола CMIP для формирования соответствующего APDU.

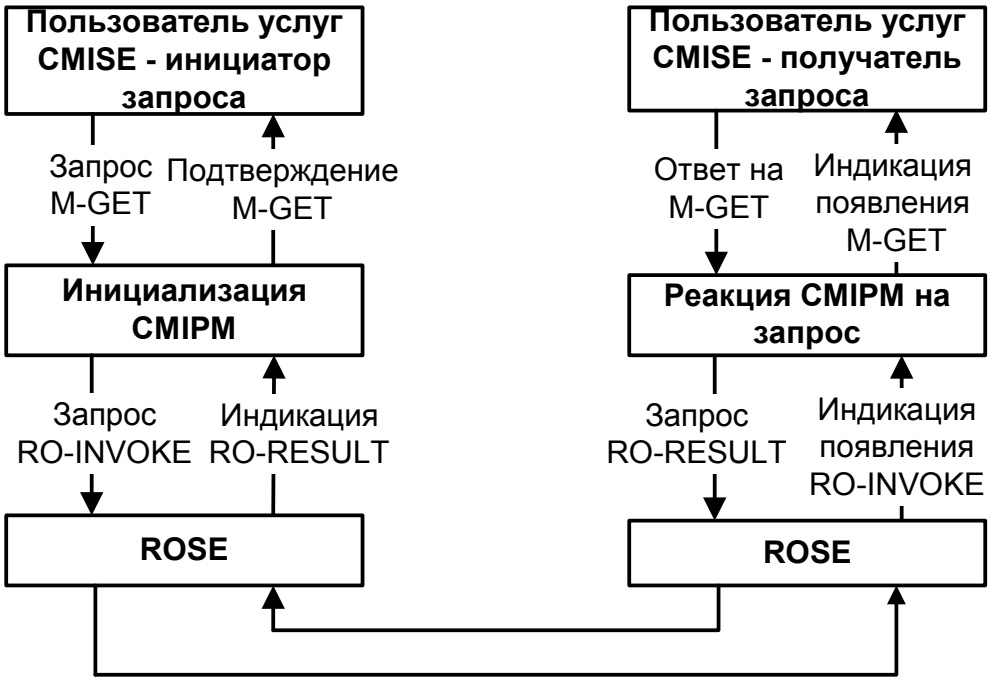


Рисунок 4.6 – Схема обмена PDU при выполнении процедуры Get с помощью ROSE (случай обмена без ошибок)

Запрос на оказание услуги M-GET с помощью CMIP передаётся на удалённый объект (получателю запроса) через ROSE. Как уже говорилось, запрос на выполнение процедуры Get осуществляется с помощью примитива M–GET request. После получения M–GET request, протокольная машина CMIPM инициатора запроса осуществит следующие операции:

- Протокольная машина сформирует блок PDU протокола CMIP, который обозначается APDU, для инициализации (т.е. выполнения) операции M–GET у получателя запроса.

[1] Согласно Рек. МСЭ–Т X.711, через M–GET request обозначен примитив запроса CMIS, который инициирует выполнение процедуры Get на CMIPM инициатора запроса. В свою очередь, через с помощью M–GET request будет затребовано выполнение операции m–Get протокола CMIP на удалённом объекте – получателе запроса. Операция m-Get осуществляется с помощью услуг ROSE с помощью передачи APDU и сервиса P-DATA [7,24].

- Протокольная машина CMIPM инициатора запроса передаст сформированный APDU получателю запроса с помощью услуг ROSE с использованием RO-INVOKE.

Протокольный блок APDU будет передан через 1–6 уровни модели ВОС. Услуги этих уровней здесь детально не рассматриваются.

Протокольная машина CMIPM получателя запроса (управляемый объект, который принимает запрос M–GET) в случае, если полученный APDU корректен, выдаёт в сторону получателя примитив индикации M–GET (M-GET indication), который указывает на появление запроса M–GET. Если поступивший от инициатора запроса PDU некорректен, то протокольная машина на приёме сформирует PDU с уведомлением об ошибке и направит этот PDU через ROSE в сторону инициатора запроса с помощью процедуры RO-REJECT-U.

При формировании ответа на M–GET, протокольная машина получателя запроса осуществит следующие операции :

- Примет ответ от получателя запроса – пользователя услуг CMISE – в виде примитива M-GET responce. Запрашиваемый IP-адрес устройства содержится в поле данных примитива.
- Сформирует блок данных протокола APDU, подтверждающий выполнение операции M–GET.
- Передаст сформированный APDU с искомым IP-адресом в сторону инициатора запроса с помощью процедуры RO–RESULT; в случае ошибки ответ передаётся с помощью процедуры RO–ERROR.

При получении PDU от получателя запроса, протокольная машина CMIPM инициатора запроса выполнит следующие операции :

- В случае, если полученный APDU с искомым IP-адресом корректен, выдаёт в сторону инициатора запроса примитив индикации RO-RESULT (RO-RESULT indication),
- Выдаст уведомление (подтверждение) о выполнении запроса в виде примитива M–GET confirmation и требуемые данные об IP-адресе в сторону инициатора запроса.
- Для некорректного APDU сформирует специальный блок данных протокола, содержащий сообщение об ошибке; этот блок данных

будет передан в сторону получателя запроса с помощью процедуры RO-REJECT-U.

Итак, протокол CMIP осуществляет передачу информации управления между различными открытыми системами, тем самым обеспечивая взаимосвязь и управляемость открытых систем. Однако протокол CMIP имеет достаточно сложное и абстрактное описание, в связи с чем затруднена его практическая реализация. В связи с вышеизложенным протокол CMIP не получил широкого распространения и практического применения, хотя и является официальным протоколом МСЭ. Альтернативой протоколу CMIP в настоящее время является протокол SNMP, который рассматривается в главе 5.

Контрольные вопросы к главе 4.

1. Какие услуги управления являются стандартными для семиуровневой модели ВОС?
2. Приведите примеры реализации элемента услуги приложения ASE.
3. С помощью каких компонентов реализуется взаимодействие между элементами структуры управления в модели ВОС?
4. Для каких целей используется элементы ROSE и ACSE?
5. Использует ли протокол CMIP концепцию «менеджер-агент»?
6. Какие функции осуществляет протокольная машина CMIPM?
7. Возможно ли создание описания объекта управления с помощью CMIPM?
8. Какие операции выполняются с помощью ROSE?

5. ПРОТОКОЛ SNMP ДЛЯ УПРАВЛЕНИЯ СЕТЯМИ СВЯЗИ

5.1 Общие сведения о протоколе SNMP

Протокол управления SNMP относятся к протоколам прикладного уровня семиуровневой модели взаимодействия открытых систем. Основное назначение данного протокола состоит в передаче управляющего воздействия от менеджера к агенту, а также передача уведомления/подтверждения о результатах, к которым привело управляющее воздействие. Таким образом, протокол SNMP поддерживает информационную модель TMN, но не является официально признанным протоколом управления в рамках стандартов МСЭ-Т по TMN. По своей структуре и принципам организации протокол SNMP проще для реализации и практического использования, чем протокол CMIP [17,43].

Исторически в создание протокола SNMP внесли свой вклад разработки 1980-х годов по трем направлениям :

- *Система управления объектами высшего уровня* (High-level Entity Management System, HEMS), которая использовалась локально, что в конечном итоге привело к прекращению работ по HEMS.
- *Простой протокол мониторинга шлюза* (Simple Gateway Monitoring Protocol, SGMP). Разработка SGMP была начата группой инженеров для решения проблем, связанных с управлением быстрорастущей сети Интернет; результатом работ стал протокол, предназначенный для управления IP–маршрутизаторами. SGMP был реализован во многих региональных доменах сети Интернет.
- Протокол *CMIP через TCP* (Common Management over TCP, CMOT) – реализует сетевое управление, базирующееся на стандартах ВОС [36]. Вариант CMOT был призван облегчить применение сложного протокола CMIP для управления объединенными информационно – вычислительными сетями, базирующимися на протоколе TCP.

Достоинства и недостатки HEMS, SGMP и CMOT особенно интенсивно обсуждались с 1987 г. В начале 1988 г. был образован комитет Internet Activities Board, IAB. Это неправительственный комитет стал ответственным за техническую разработку протоколов для сети Интернет, в том числе решал вопросы в части протокола сетевого управления.

В конечном счёте улучшенная версия протокола SGMP была переименована в *простой протокол управления сетью* (Simple Network Management Protocol, SNMP). Протокол SNMP получил статус временного решения. Для долгосрочного применения планировалось проанализировать один из протоколов, базирующихся на семиуровневой модели ВОС : CMOT или CMIP. Но в итоге протокол SNMP стал постоянным техническим решением.

Начиная с 1990 г. протокол SNMP версии 1 (SNMPv1) становится базовым протоколом управления в сети Интернет. Основным нормативным документом, определяющим концепцию управления и администрирования сетями, использующими стек протоколов TCP/IP, является документ RFC 1157 «Simple Network Management Protocol (SNMP)», который разработан специалистами IETF.

Деятельность по стандартизации SNMP продолжается постоянно. Как альтернатива более масштабным, но зато и более дорогим решениям CMIP, протокол SNMP получил особенно широкое распространение начиная с 1993 года в качестве базового протокола управления сетями, использующими стек протоколов TCP/IP. С помощью SNMP реализовано управление как одиночными устройствами, так и группами сетевых средств, в том числе крупными сетями связи (информационно-вычислительными сетями).

На протяжении 1990-х годов протокол SNMP неоднократно рассматривался и дорабатывался неправительственной международной организацией *Инженерная группа по развитию Интернета* (Internet Engineering Task Force, IETF). В настоящее время протокол SNMP применяется на сетях, использующих стек протоколов TCP/IP, и на сетях, использующих другие телекоммуникационные протоколы.

Сеть связи в рамках протокола SNMP представляется как совокупность сетевых управляющих станций и элементов сети (шлюзы, маршрутизаторы, коммутаторы); на элементах сети поддерживается программы-

агенты, с помощью протокола передачи дейтаграмм пользователя (user datagram protocol, UDP) обеспечивается обмен информацией управления между сетевыми управляющими станциями и агентами.

Сейчас на сетях связи практически применяются две версии протокола SNMP: SNMP версии 1 (SNMPv1) и SNMP версии 2 (SNMPv2) [37, 39]. Обе версии имеют много общего, однако версия SNMPv2 предоставляет некоторые преимущества, например дополнительные операционные возможности протокола, поддержку средств аутентификации. Стандартизация SNMP версии 3 (SNMPv3) завершается. В настоящей главе в качестве основной версии протокола SNMP рассматривается версия 2.

Учитывая существенный объём источников информации по протоколу SNMP и их доступность, обсуждение протокола SNMP будет проведено в сжатой форме. В качестве источников информации здесь и далее использовались сведения с Интернет-сайтов www.simpleweb.org, www.citforum.ru, www.laes.ru/list/pve/SNMP/.

5.2 Модель управления, используемая в протоколе SNMP

Как уже говорилось, при использовании протокола SNMP программа пользователя (менеджер сети) осуществляет виртуальные соединения с SNMP-агентами. Программа SNMP-агента установлена на элементе сети, и предоставляет менеджеру сети информацию о состоянии данного элемента. Этот процесс осуществляется в рамках *системы управления сетью* (network management systems, NMS), см. рис 5.1 [42,43] на следующей странице.

Существуют некоторые отличия понятия «управляемый объект» в протоколах CMIP и SNMP. Управляемый объект в протоколе CMIP – это законченное и подробное описание управляемого ресурса; управляемым объектом в протоколе SNMP является чаще всего некоторый атрибут объекта, например число отказов или сбоев.

Как уже отмечалось, управляемое устройство, на котором функционирует программа-агент, может быть любым – сервер доступа в Интернет, УПАТС, принтер, маршрутизатор, концентратор ЛВС и т.п. В данной ситуации программы управления должны быть построены таким образом,

чтобы минимизировать воздействие программы-агента на управляемое устройство; другими словами, функционирование агента не должно влиять на выполнение основных функций средств связи.

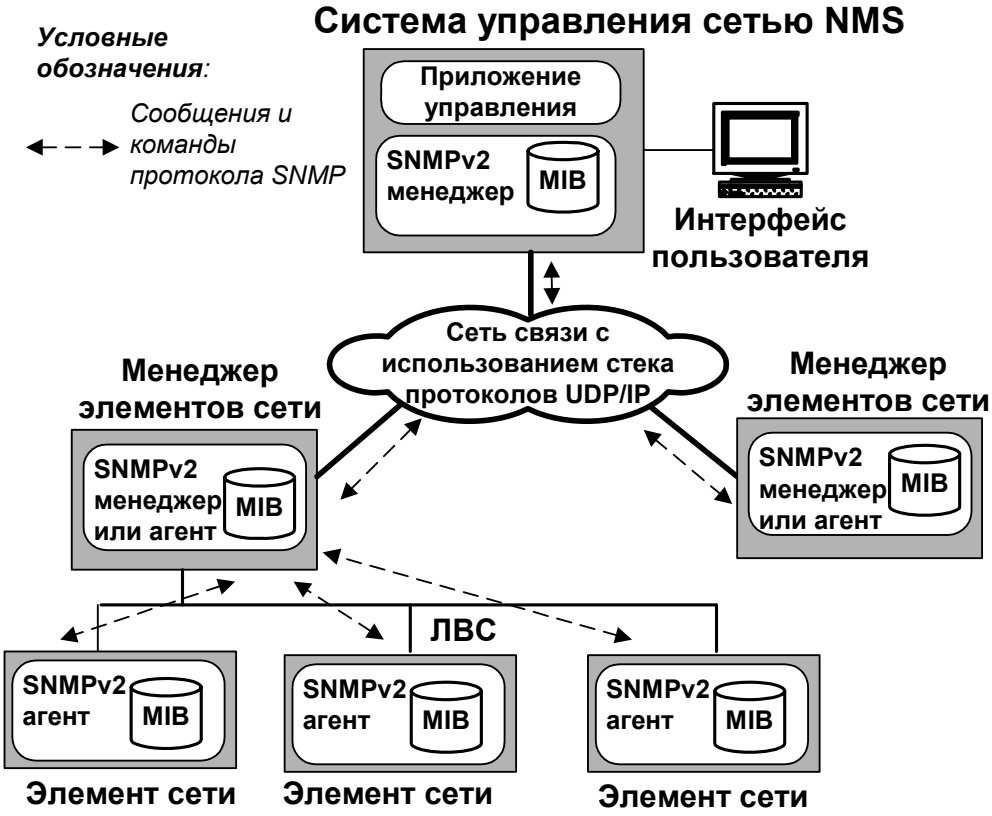


Рисунок 5.1 – Использование протокола SNMPv2

Агенты по заданию менеджера или автоматически (по расписанию) могут отслеживать следующие показатели работы оборудования:

- Число и состояние виртуальных каналов.
- Число определенных видов сообщений о неисправностях/отказах.
- Число входящих и исходящих байтов (пакетов) для данного устройства.
- Максимальная длина очереди на входе/выходе (для маршрутизаторов и других устройств).
- Отправленные и принятые широковещательные сообщения.
- Отказавшие и вновь запущенные в эксплуатацию сетевые и абонентские интерфейсы.

База данных с информацией о состоянии элементов сети Интернет определена ISO и называется *Интернет-информационной базой управления* (Internet management information base, IMIB) [38]. База IMIB является виртуальным информационным массивом, который подобно базе данных MIB, содержит в формализованном и упорядоченном виде информацию, связанную с сетью связи и с сетевым оборудованием. В протоколе SNMP база IMIB также является информационной моделью управляемого объекта, однако уровень её подробности ниже, чем в протоколе CMIP. Стандартная IMIB протокола SNMP включает различные объекты/элементы, создаваемые с целью измерения, мониторинга и контроля функционирования протоколов IP,TCP,UDP, контроля IP-маршрутов, TCP-соединений, состояния сетевых интерфейсов элементов сети в целом. При управлении протокол SNMP обращается за информацией именно к IMIB.

Существует два стандарта IMIB, применяемых в протоколе SNMP, а именно стандарт MIB-I и стандарт MIB-II. Кроме того, существует версия MIB для удалённого управления с помощью агентов *протокола удалённого мониторинга сетей* (Remote Monitoring, RMON). Протокол RMON в данном пособии детально не рассматривается.

В стандарте MIB-I (см. нормативный документ RFC 1156) определены только операции чтения из базы. В этой версии существует всего 114 управляемых объектов, разделённые на 8 групп. Например, группа «System» содержит атрибуты, которые позволяют описать общие данные об устройстве – обозначение поставщика, время последнего включения/активизации устройства; группа «IP» включает данные протокола IP: адрес IP-шлюза, статистика IP-пакетов.

Каждый из управляемых объектов связан (ассоциирован) с именем и со специальным *объектным идентификатором*. Объектный идентификатор представляет собой формальный регистрационный признак (номер) объекта управления, под которым управляемый объект занесён в IMIB. Совокупность объектных идентификаторов образуют т.н. «дерево регистрации» управляемых объектов, основные «ветви» которого контролируются и поддерживаются Международной организацией по стандартизации (идентификатор iso), МСЭ (ccitt или itu), организациями, сотрудничающими с МСЭ (идентификатор joint–to–ccitt).

Пример рассматриваемого «дерева регистрации» управляемых объектов приведён далее на рис.5.2. На практике для записи данных об управляемых объектах используется специальный язык *абстрактной записи синтаксиса №1* (Abstract Syntax Notation No1). Язык ASN.1 является универсальным способом записи данных об управляемом объекте т.к. не зависит от языка программирования, который применяется для разработки программных приложений управления.

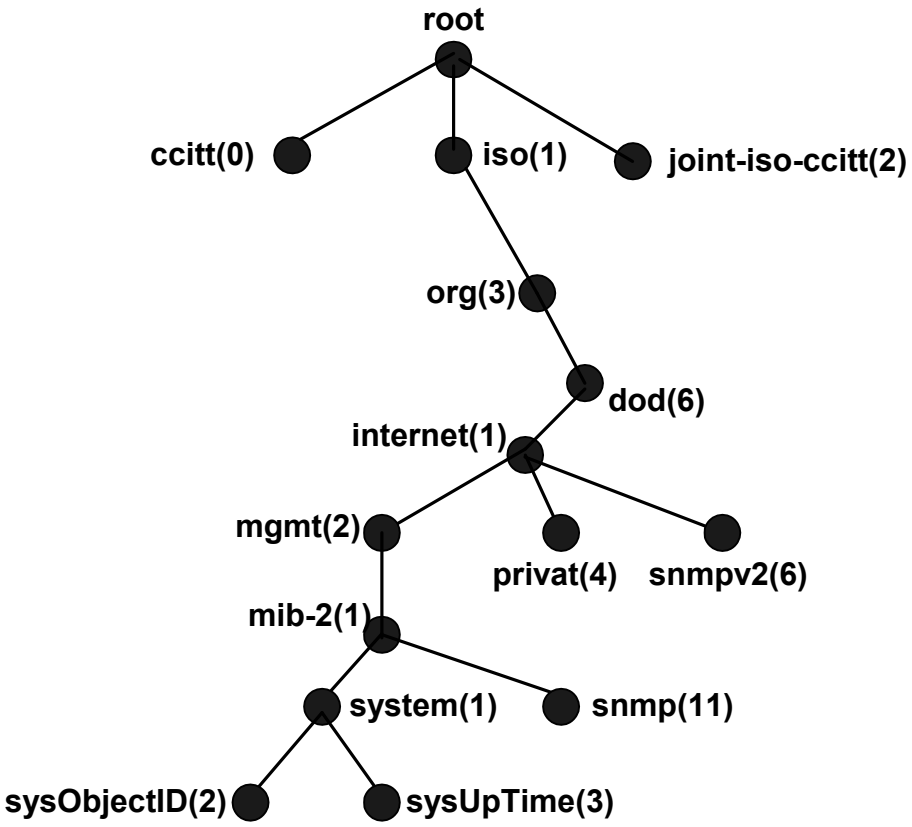
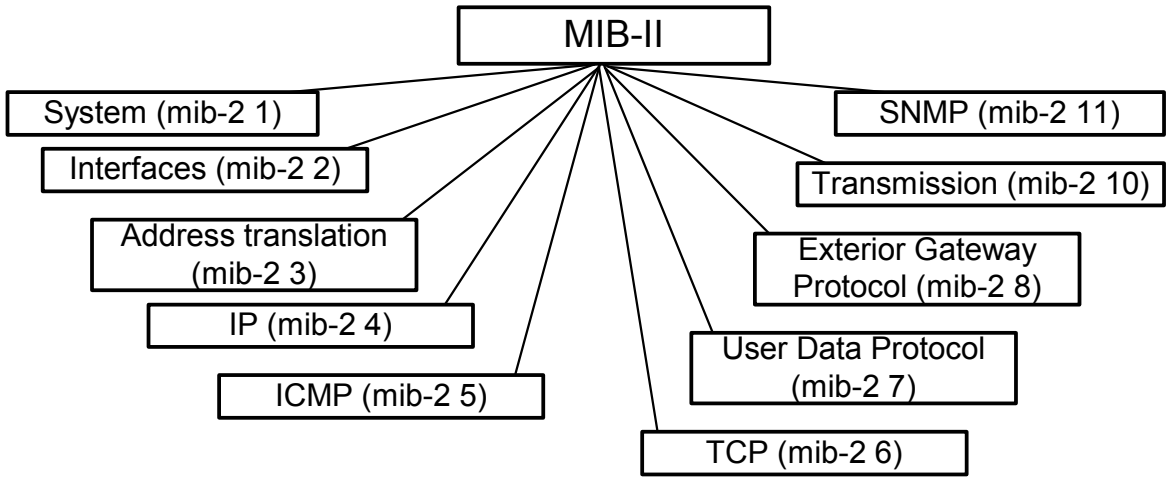


Рисунок 5.2 – Схема «дерева» регистрации объектных идентификаторов управляемых объектов в сети Интернет

Например, объект с именем «sysUpTime», значение которое указывает время в сотнях секунд, истекшее с момента перезагрузки/ управляемого устройства, связан с объектным идентификатором OID system 1.3, а также с регистрационным номером 1.3.6.1.2.1.1.3.0, который соответствует «узлам» на «ветви» дерева идентификаторов (сверху вниз): iso(1) $\rightarrow$ org(3) $\rightarrow$ dod(6) $\rightarrow$internet(1) $\rightarrow$ mgmt(2)$\rightarrow$ mib-2(1) $\rightarrow$ system(1) $\rightarrow$ sysUpTime(3) $\rightarrow$ 0.

Эту запись следует понимать так : объект зарегистрирован в «ветви» дерева идентификаторов, которое поддерживается ISO, находится в домене, относящимся к организациям (org) поддерживается Министерством обороны США (department of defense, dod), относится к сети Интернет (internet), применяется для решения задач управления (mgmt), зарегистрирован в базе данных MIB-II (mib-2), относится к группе системы (system), обозначается sysUpTyme (3) и является дискретным (0) Вершина **root** является глобальной ссылкой (точкой отсчёта) и содержательного смысла не имеет. В стандарте MIB-II (см. нормативный RFC 1213), который действует с 1992 г., количество управляемых объектов увеличено до 185, а количество групп – до 10 (см. рис 5.3).



Условные обозначения :

mib-2 x – объектный идентификатор
System – группа системы (содержит имя домена, физическое расположение узла, описание сервисов узла)
Interfaces – группа сетевых интерфейсов (содержит описание вида интерфейса, данные о скорости передачи, сведения о рабочем состоянии)
Address translations – отображение IP-адресов в физические адреса
IP (Internet Protocol) – группа протокола межсетевого взаимодействия
ICMP (Internet Control Message Protocol) – группа сообщений межсетевого протокола управляющих сообщения
TCP (Transaction Control Protocol) – группа протокола управления передачей
UDP (User Data Protocol) – группа протокола дейтаграмм пользователя
Exterior Gateway Protocol – группа протоколов для взаимодействия маршрутизаторов
Transmission – данные о среде передачи информации
SNMP – данные статистической информации протокола SNMP

Рисунок 5.3 – Структура MIB-II

Регистрационный номер объектов уникальным образом обозначают управляемые объекты в IMIB и похож на телефонные номера тем, что организован иерархически; отдельные части регистрационного номера назначаются различными организациями.

Основные группы объектов IMIB, по аналогии с приведённым примером, можно изобразить в виде абстрактного дерева, «ветвями» которого являются отдельные группы управляемых объектов (см. рис. 5.3.). Каждая группа в MIB-II на практике представлена в виде одной или нескольких таблиц. Таблица соответствует управляемому объекту и может включать скалярные величины, соответствующий конкретному значению атрибута управляемого объекта, имя атрибутов указано в заголовке таблицы. Например, таблица tcpConnTable, регистрационный номер 1.3.6.1.2.1.6.13.1, которая содержит данные о TCP–соединениях элемента сети (группа TCP mib2-6), предложенная компанией Cisco Systems, имеет вид (см. рис. 5.4):

TcpConnState	**tcpConnLocalAddress**	**TcpConnLocalPort**	**…**
(значение 1)	(значение 3)	(значение 5)	**…**
(значение 2)	(значение 4)	(значение 6)	**…**
…	**…**	**…**	**…**
(значение I)	(значение J)	(значение K)	…

Условные обозначения :
TcpConnState – обозначает состояние TCP–соединения, значение - целое число (INTEGER).
TcpConnLocalAddress – обозначает IP–адрес инициатора соединения, его значение соответствует IP–адресу (IpAddress).
TcpConnLocalPort – обозначает номер порта, через который осуществляется соединения, целое число (INTEGER).

Рисунок 5.4 – Пример таблицы SNMP, отображающей состояние TCP–соединения

Директивы или управляющие команды, выданные сетевым менеджером агенту, наряду с собственно командами состоят из идентификаторов объектов MIB, значение которых следует получить. Поэтому команды управления в SNMP используются в первую очередь для получения текущего значения или установки нового значения атрибута объекта управления с соответствующим идентификатором.

В тоже время существует возможность с помощью добавления в IMIB новых элементов – таблиц, столбцов в существующую таблицу – расширять описания существующих или создавать новые управляемые объекты. Рассмотрим далее элементы протокола SNMP.

5.3 Элементы протокола SNMP

В протоколе SNMP можно выделить следующие основные стандартизованные элементы [39,40].

1. *Стандартный формат сообщения* (standard message format), который определяется форматом сообщения UDP.
2. *Стандартный набор управляемых объектов* (standard set of managed objects) представляет собой набор стандартных объектов и значений (values) их атрибутов в IMIB. Эти значения можно получить в ответ на запросы станции управления. Значение, получаемое в ответ на запрос (т.н. возвращаемое значение) позволяет сделать вывод о состоянии управляемого объекта. Стандартный набор включает величины для контроля протоколов TCP, IP, UDP, сетевых интерфейсов устройств. Каждая величина ассоциирована с объектом, имеющим уникальный объектный идентификатор. Идентификатор записывается в форме в форме «записи-через-точку» (dot-notation), см. раздел 5.2.
3. *Стандартный способ добавления объектов* (standard way of adding objects). Наличие этого элемента – одна из причин того, почему протокол SNMP стал широко известным и приобрел статус de–facto промышленного стандарта управления. Этот метод позволяет фирмам-производителям расширять стандартный набор управляемых объектов посредством спецификации новых управляемых объектов и добавления их в IMIB.

Начиная с протокола SNMP версии 1 (SNMPv1) были определены четыре типа стандартных SNMP-операций для управления объектами :

- Операция *Get* [получить] применяется чтобы возвратить (получить) значение атрибутов управляемого объекта из группы IMIB.

- Операция *GetNex*t [получить следующий] существует, чтобы возвратить имя (и значение атрибутов) следующего по порядку управляемого объекта в IMIB.
- Операция *Set* [установить] применяется, чтобы установить на управляемых объектах значения атрибутов (изменить содержание ячейки таблицы на рис. 5.4).
- Операция *Trap* [прерывание] используется сетевыми устройствами асинхронно; с помощью прерывания, остановив выполнение других программ управления, элементы сети могут самостоятельно, без специального запроса, сообщить менеджеру сети о возникших отказах, перегрузках и т.п.

В протоколе SNMP версии 2 (SNMPv2) помимо перечисленных, были добавлены новые SNMP-операции, а именно :

- Операция *GetBulk* [получить перечень] используется для извлечения большого числа значений из таблиц, а не единичных значений атрибутов.
- Операция *Inform* [информировать] позволяет одной NMS выполнять операцию Trap на другой NMS и, соответственно, получать ответ на асинхронный запрос.
- Операция *Report* [рапорт] позволяет агенту сообщить о состоянии управляемого ресурса; сообщение выдаётся без запроса.

Каждой перечисленной операции соответствует PDU определённого формата. Используя перечисленные операции (команды) можно сформировать соответствующие примитивы запросов для обмена между менеджером и агентом.

В результате выполнения операции менеджером или агентом будет сгенерирован один из следующих запросов :

- Запрос *«Получить»* (GetRequest) – используется чтобы определить технические характеристики и состояние устройства с помощью операции Get. В результате из базы данных IMIB могут быть получены требуемые значения атрибутов управляемых объектов.
- Запрос *«Получить следующий»* (GetNextRequest) –используется в стандарте SNMP сетевыми менеджерами для «просмотра» всех

имен управляемых объектов и их атрибутов, которые поддерживаются агентом на данном сетевом устройстве. Эта процедура выполняется начиная с первого объекта так, чтобы после выборки информации о первом объекте перейти к выборке данных по следующему объекту в IMIB (с использованием *GetNext*). Данная процедура может повторяться до тех пор, не будет обнаружена ошибка сетевого устройства или до конца перечня объектов IMIB.

- Запрос *«Установить»* (SetRequest) – позволяет осуществлять действия, связанные с изменением значения атрибута с помощью операции «Set»; например, отключение интерфейса, разъединение пользователей, сброс в 0 содержимого буфера ввода–вывода и т.д. Этот запрос обеспечивает возможность конфигурирования и управления устройствами сети с помощью протокола SNMP.
- Запрос *«Прерывание»* (Trap). Протокол SNMP предоставляет механизм, посредством которого сетевые устройства могут «выдавать наружу» (reach out) или самим себе (через Trap) прерывание, обозначающее наличие проблемы.

Кроме перечисленных, имеются запросы типа InformRequest [информировать] и GetBulkRequest [получить перечень]. Сообщение Response [ответ] включает информацию, передаваемую в ответ на запрос. Последовательность обмена перечисленными запросами (сообщениями) представлена на рис. 5.5.

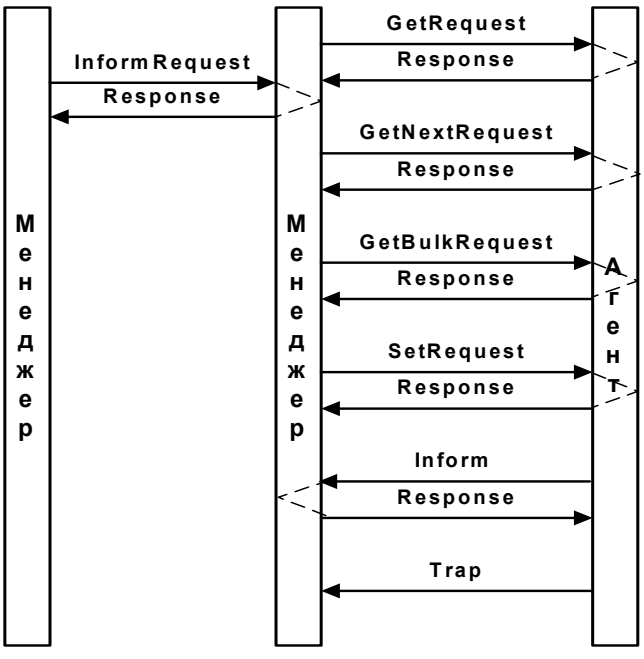


Рисунок 5.5 – Обмен запросами и ответами (response) в SNMPv2

Все вышеупомянутые типы операций и запросов закодированы в виде PDU, которыми обмениваются устройства, поддерживающие протокол SNMP (см. рис.5.6 и таблицу 5.1) :

Рисунок 5.6 – Форматы PDU в SNMP (v1 и v2)

Таблица 5.1 – Назначение полей PDU протокола SNMP

Наименование поля	**Назначение**
Версия SNMP	Номер версии протокола SNMP
Сообщество	Строка символов для обмена между агентом и менеджером
Название и тип PDU	**Get (тип 0), Set (тип 2), GetNext (тип 1), Responce (тип 3)**
Идентификатор запроса *(Request-ID).*	Устанавливает связь между командами и ответами на команды.
Статус ошибки *(Error-status)*	Указывает ошибку и ее тип.
Индекс ошибки *(Error-index)*	Устанавливает связь между ошибкой и конкретной реализацией управляемого объекта.
Имя, значение переменных *(Variable bindings*)	Данные SNMP PDU, которые содержат значения атрибутов, которые записаны с помощью переменных и текущих значений переменных.
Название и тип PDU	**Trap (тип 4)**
Сообщество, область *(Enterprise)*	Идентифицирует тип объекта, генерирующего данное прерывание.
Адрес агента (*Agent address)*	Содержит сетевой адрес объекта, генерирующего данное прерывание
Общий тип прерывания *(Generic trap type)*	Содержит общие данные об типе прерывания.
Спецкод прерывания *(Specific trap code)*	Содержит специфический код прерывания.
Временнáя отметка *(Time stamp)*	Содержит величину времени, прошедшего между последней повторной инициализацией сети и генерацией данного прерывания.
Имя, значение переменных *(Variable bindings*)	Содержит перечень значений атрибутов в виде переменных и их значений с информацией о прерываниях.

Форматы PDU, которые соответствуют GetBulkRequest и Inform несколько отличаются от вышеперечисленных. На практике форматы приведённых на рис.5.6 сообщений протокола SNMP не всегда удобны. В рамках объектно-ориентированного подхода протокол SNMP не поддерживает некоторые отношения наследования, поэтому, чтобы получить данные о нескольких взаимосвязанных управляемых объектах, необходимо использовать механизм многократных запросов. Здесь же следует отметить, что запрос в протоколе SNMP либо выполняется полностью, либо совсем не выполняется. Перечисленные недостатки протокола SNMP не влияют на его распространение для контроля и управления сетями электросвязи.

5.4 Функции управления SNMP

Самый убедительный довод в пользу применения протокола SNMP заключается в том, что SNMP разрабатывался как протокол, поддерживающий единый способ доступа к сетевому устройству на основе стека протоколов TCP/IP. Коль скоро стек протоколов TCP/IP достаточно универсален, следовательно универсален и протокол SNMP. SNMP является своего рода прикладным программным интерфейсом API к сети управления. При этом сохраняется универсальность интерфейса в части доступа к сетевым устройствам различных видов. При отсутствии протокола SNMP, безусловно, было бы создано большое число специальных, написанных «под заказ» протоколов, действующих только с оборудованием определенного поставщика.

Дополнительный аргумент в пользу применения SNMP состоит в том, что данный протокол определяет состояние устройства без организации сложного удаленного доступа или без потребности в сложных процедурах аутентификации. В результате появляется возможность получения большого числа данных о состоянии элементов крупномасштабной сети. Однако отсутствие надёжных средств обеспечения информационной безопасности нецелесообразно с точки зрения живучести и надёжности системы управления. Поэтому в версии 3 протокола SNMP аутентификации и криптозащите уделено особое внимание.

Большинство программ-менеджеров в SNMP обеспечивают следующие функции управления :

Функции сбора информации о неисправностях (alarm polling functions). SNMP-менеджеры обеспечивают возможность установить *пороги чувствительности* (thresholds) на управляемых объектах (например, максимально допустимое число ошибок), и своевременно выдавать аварийное сообщение, когда эти пороги превышены. Реализация данной функции позволяет постоянно контролировать техническую исправность сети и её отдельных элементов. Функция сбора информации о неисправностях определяет, какие устройства отвечают на управляющее воздействие, а какие устройства не отвечают на запросы (то есть, какие устройства условно можно считать поврежденными).

Функции контроля тренда (trend monitoring functions). На протяжении определенного времени SNMP-менеджеры обеспечивают возможность непрерывного наблюдения за некоторыми значениями атрибутов управляемых объектов; эти объекты и значения атрибутов зафиксированы в IMIB. Периодически производится считывание значений атрибутов, что позволяет оценить рабочие характеристики сети в динамике т.е. построить тренд сети по тому или иному признаку. В частности, описанная функция может использоваться для определения графика (профиля) нагрузки сети на заданном интервале времени.

Функции прерывания при приеме (trap reception functions). SNMP-менеджеры обеспечивают возможность приёма и фильтрации SNMP-прерываний, которые выдаются сетевыми устройствами. SNMP-прерывания являются важной частью протокола SNMP; прерывания позволяют сетевым устройствам самостоятельно, не дожидаясь запроса, сообщать о проблемах, отказах и т.п. Допустимые типы прерываний обычно регистрируются сетевым менеджером. Прерывания управляют уведомлениями о происшествиях/сетевых событиях. Поскольку прерывания выдаются в асинхронном режиме, SNMP-менеджеры поддерживают фильтрацию прерываний, чтобы устранить сообщения о прерывании, которые являются несущественными или вторичными (повторными).

Для реализации описанных выше функций управления используются следующие средства, применяемые совместно с аппаратно-программной реализацией протокола SNMP :

Набор инструментов/средств управления (management tool set). Все SNMP-менеджеры обеспечивают набор инструментальных программных средств для решения задачи управления. Наиболее традиционный тип инструмента управления – программа просмотра IMIB, которая позволяет пользователю ознакомится с объектами IMIB для определенного устройства. Набор инструментов позволяет реализовать сетевой интерфейс администратора для установки значений SNMP-агента и, следовательно, применяется для внесения изменений в конфигурацию сети через SNMP.

IMIB Компилятор (compiler). Это средство поддерживает функцию добавления новых объектов в IMIB, например при появлении нового сетевого оборудования. Описание нового управляемого объекта добавляется в базу данных IMIB, после чего с помощью компилятора осуществляется кодирование и формирование исполняемого программного кода для менеджера и агента.

Вышеупомянутая функциональность SNMP приводит к появлению существенной нагрузки, вызванной «мониторинговым» аспектом управления сетью связи. В протоколе SNMP достаточно велико число управляемых объектов, которые поддерживают режим доступа «только для чтения». Тем не менее, общепризнанным достоинством SNMP является возможность с помощью относительно простых средств получать информацию о состоянии сети и тем самым определять техническое состояние сети.

Теоретически возможности SNMP менее мощные по сравнению с протоколом CMIP, особенно когда возникает необходимость в модификации данных об управляемом оборудовании. В частности, SNMP не поддерживает динамическое создание управляемых объектов с помощью операции Create и удаление описания объектов с помощью операции Delete. Поэтому протокол SNMP не может работать с динамическими объектами, в отличии от протокола CMIP, который динамику поддерживает. Тем не менее, использование операции Set позволяет администратору осуществлять некоторые формы корректирующего воздействия и модификации атрибутов.

5.5 Особенности протокола SNMP версии 3

Основные спецификации протокола SNMP версии 3 (SNMPv3) содержатся в документах IETF :

- документ **RFC 2570. Introduction to SNMP v3** [Введение в SNMP версии 3], опубликован в апреле 1999 г.
- документ **RFC 2571. An Architecture for Describing SNMP Management Frameworks** [Архитектура для описания структуры SNMP], опубликован в мае 1999 г.
- документ **RFC 2572. Message processing and Dispatching** [Обработка и диспетчеризация сообщений], опубликован в мае 1999 г.
- документ **RFC 2573. SNMP Applications** [Приложения SNMP], опубликован в апреле 1999 г.
- документ **RFC 2574. User-Based Security Model** [Модель безопасности пользователя], опубликован в апреле 1999 г.

Согласно данным документам, протокол SNMP версии 3 имеет следующие особенности :

- Модульность архитектуры как программных решений, так и спецификаций SNMPv3. Модульность позволяет сочетать в рамках одной системы управления NMS компоненты от разных поставщиков, проводить модернизацию протокола и развивать его. Это гарантирует сохранность инвестиций в систему сетевого управления и способность протокола SNMP к развитию.
- Поддержка режима распределённой обработки данных.
- Возможность работать в режиме агента, менеджера или в совмещённом режиме.
- Масштабируемость т.е. поддержание конфигурации сети произвольного масштаба и состава.
- Механизмы обеспечения информационной безопасности для защиты управляющих сообщений и разграничения доступа к информации управления.

На следующей странице, на рис. 5.7а и 5.7б представлены основные компоненты архитектуры SNMPv3 для конфигурации агента и менеджера.

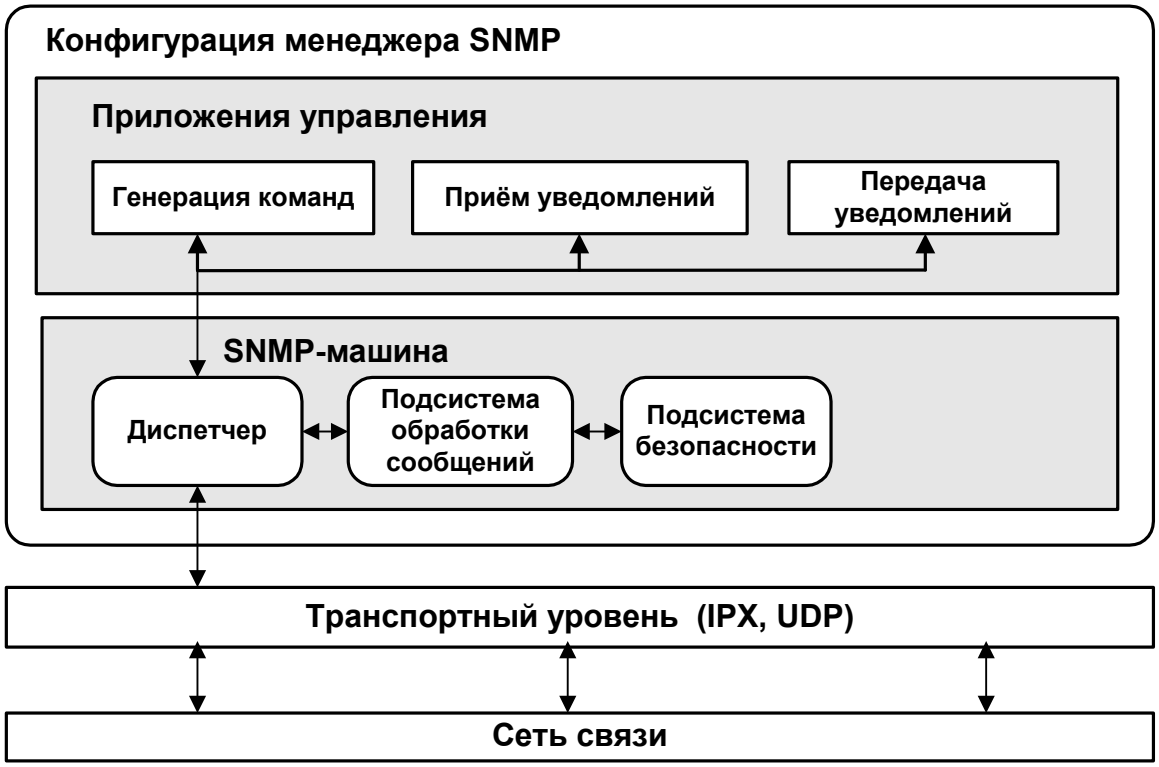


Рисунок 5.7а – Конфигурация менеджера в SNMPv3

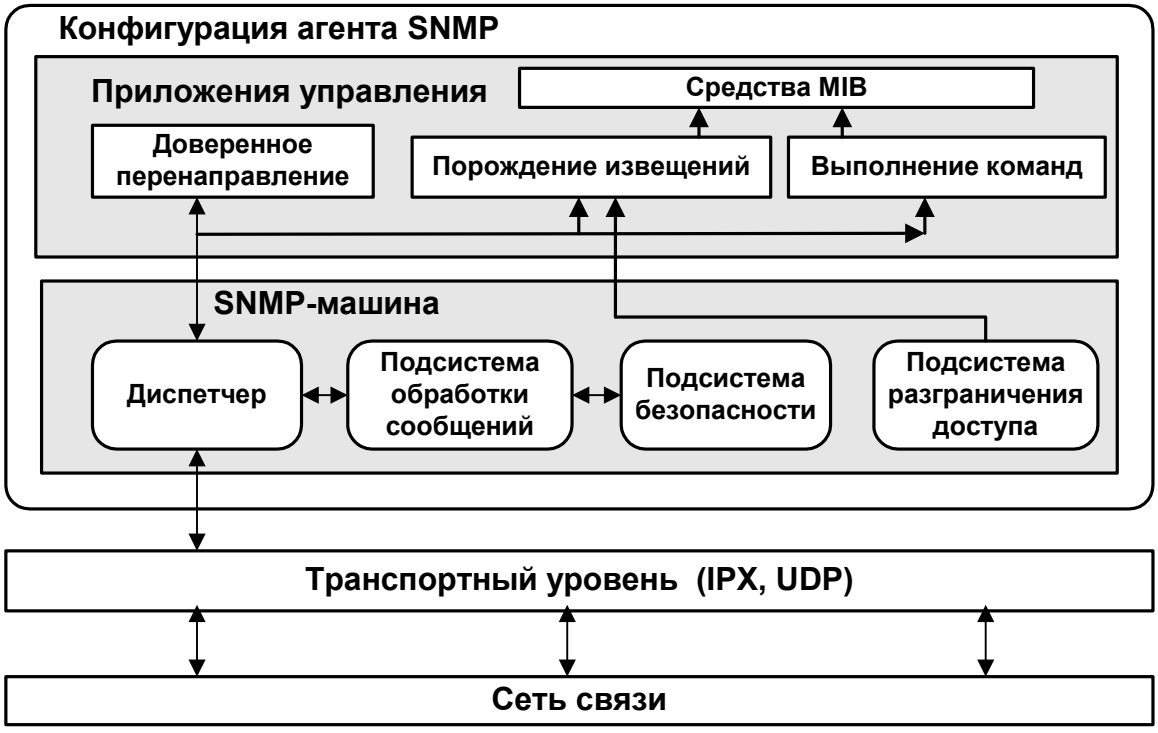


Рисунок 5.7б – Конфигурация агента в SNMPv3

Основных компонентов два:

- *машина* протокола SNMP, SNMP-машина (SNMP engine);
- *приложения управления* SNMP (SNMP application).

Машина протокола SNMP присутствует во всех управляемых и управляющих системах т.е. и в менеджерах и в агентах. Машина протокола SNMP осуществляет функции посылки и приёма PDU, функции аутентификации с помощью вставки специальных кодов, шифрование и дешифрование SNMP-сообщений, функции контроля доступа к управляемым объектам.

Машина протокола SNMP по отношению к приложению управления функционирует как в режиме приёма так и в режиме передачи. Машина протокола SNMP имеет модульную структуру и включает четыре компонента:

- *диспетчер* (dispatcher);
- *подсистема обработки сообщений* (message processing system);
- *подсистема информационной безопасности* (security subsystem);
- *подсистема разграничения доступа* (access control subsystem).

Диспетчер занимается приемом и отправкой SNMP-сообщений. Подсистема обработки сообщений поддерживает несколько моделей обработки сообщений, соответствующих протоколу SNMP версии 1 и версии 2. Это ключевое свойство позволяет обеспечить преемственность между различными версиями протокола SNMP. Диспетчер выполняет функции управления нагрузкой. Диспетчер по номеру версии в заголовке PDU определяет, какой тип обработки сообщений необходим для данного SNMP-сообщения.

Подсистема обработки сообщений принимает/передаёт сообщения диспетчеру. На передаче данная подсистема добавляет необходимый заголовок для передачи через сеть передачи данных; на приёме эта подсистема извлекает PDU протокола SNMP из пакета, полученного по сети передачи данных.

Подсистема информационной безопасности (security subsystem) протокола SNMP обеспечивает функции аутентификации и шифрования. В протоколах SNMPv1 и SNMPv2 особого внимания вопросам информационной безопасности управления не уделялось. В противоположность прежним версиям, протокол SNMPv3 включает модель обеспечения безопасности, которая предусматривает меры защиты против следующих потенциальных угроз :

- модификация информации управления при передаче;
- подмена данных, как средство неавторизованного выполнения операций управления на объекте;
- резкое увеличение потока сообщений до уровня, превышающего обычные отклонения, возможные при использовании транспортных протоколов TCP/IP;
- несанкционированное ознакомление с сообщениями.

При передаче подсистема безопасности получает SNMP-сообщение от подсистемы обработки сообщений. В зависимости от требуемой услуги управления, подсистема безопасности может шифровать PDU и часть полей в заголовке сообщения SNMP.

Защищённое сообщение возвращается в подсистему обработки сообщений. На приёме происходит обработка сообщения в обратном порядке (дешифровка), однако дополнительно может выполняться проверка аутентификационного кода для определения подлинности источника сообщений.

Для контроля целостности и аутентификации источника предусматриваются хэш-функции, вычисляемые на основании алгоритма *криптозащиты цифрового сообщения* MD5 (message digest, MD) или алгоритма *безопасного хэширования* (secure hash algorithm, SHA). Стандартным средством шифрования в SNMPv3 является *стандартный алгоритм шифрования DES* (data encryption standard, DES).

Протокол SNMPv3 не предусматривает специальных средств защиты против атак на доступность, поскольку во многих случаях атаки на дос-

тупность неотличимы от потока сообщений о массовых отказах в сети, с которыми должен работать любой протокол управления.

Модель безопасности включает подсистему разграничения доступа к информации управления. Эта подсистема обеспечивает услуги авторизации для контроля доступа к IMIB в случае чтения или установки новых значений атрибутов управляемых объектов.

Модель доступа описана в документе RFC 2275. Согласно данной рекомендации, каждый субъект управления получает т.н. *представление* (view) о данных системы, а также о подмножестве информации управления, задаваемой спецификациями IMIB. Это позволяет сделать доступными только те функции, которые включены в представление.

Для операций чтения, записи и выдачи уведомлений могут использоваться отдельные представления, что повышает надёжность механизма информационной защиты SNMPv3.

В SNMPv3 предусмотрено пять стандартных модулей приложений управления :

- Генерация команд (command generator applications) – осуществляет мониторинг и манипуляции с данными управления на удалённых агентах. Использует стандартные PDU из таблицы 5.1

- Прием уведомлений/извещений (notification receiver application) – обрабатывает входящие асинхронные сообщения типа InformRequest, Trap, Response.

- Создание уведомлений/извещений (notification originator application) – инициирует асинхронные сообщения. Использует запросы InformRequest.

- Доверенное перенаправление (proxy forwarded applications) – использует возможности диспетчера для перенаправления сообщений SNMP, например, по направлению к инициатору запроса или уведомления.

С учётом вышеизложенного формат сообщения SNMP v3 изменяется (см. рис. 5.8) :

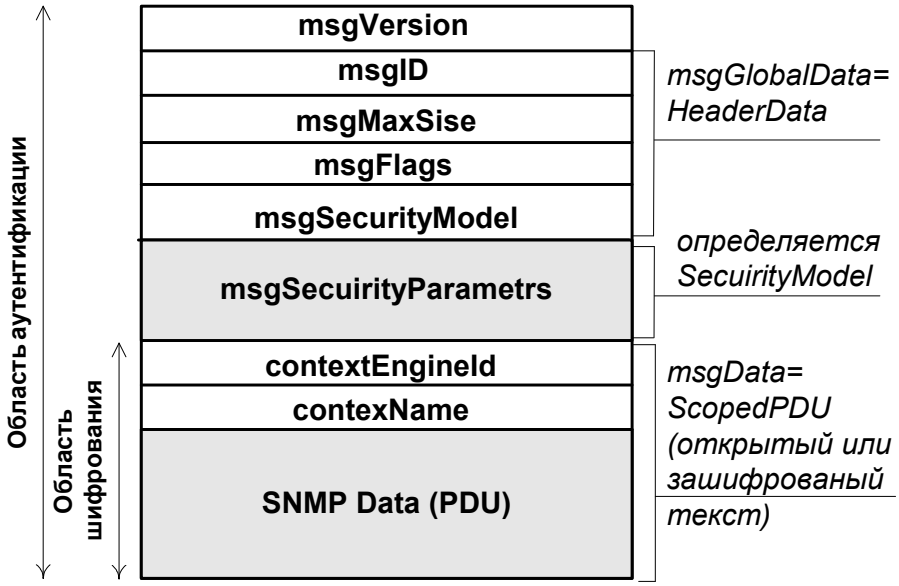


Рисунок 5.8 – Формат сообщений SNMP v3

Расшифровка полей формата приведена в таблице 5.2 :

Таблица 5.2 – Назначение полей PDU протокола SNMP v3

Наименование поля	Назначение
msgVersion	Версия SNMP, устанавливается в snmpv3 (3)
Header data – Данные заголовка сообщения	
msgID	Уникальный идентификатор, используется для обмена между объектами SNMP для координации запроса и ответного сообщения а также для координации обработки сообщений различными подсистемами SNMP на данном объекте. Принимает значение от 0 до 2^{31}-1
msgMaxSize	Содержит значение максимальной длины сообщения в байтах в диапазоне от 484 до 2^{31}-1, которое может обрабатываться отправителем (источником) сообщения.
MsgFlags	Байт данных, который поддерживает три флага, использующих три бита. Флаги указывают на тип сообщения (Get, Set, Inform), устанавливают порядок обмена PDU, указывают на уровень защищённости сообщения. Флаги принимают значения 0 или 1.
MsgSecurityModel	Этот идентификатор принимает значение от 0 до 2^{31}-1 и указывает на тип модели безопасности, которая используется источником сообщения. Зарезервированные значения : 1 – для протоколов SNMPv1; 2 – для протокола SNMPv2; 3 – для протокола SNMPv3,

Наименование поля	Назначение
msgSecurityParame-tersl	Байт данных, используется для коммуникации (информационного обмена) между машиной протокола SNMP отправителя и машиной протокола SNMP получателя сообщений. Данные в этом поле используются только подсистемой безопасности.
ContextEngineId	На приёме обозначает, совместно с полем типа в PDU, какому приложению управления данное сообщение должно быть направлено на обработку. При передаче указывает на приложение, которое сформировало запрос.
ContextName	Совместно с полем contextEngineId идентифицирует конкретное содержание, которое связно с информацией управления в PDU
SNMP Data (PDU) – данные протокола SNMP	

Как уже отмечалось, протокол SNMP имеет несколько преимуществ по сравнению с протоколом CMIP. Самая большое преимущество – универсальность и простота протокола SNMP. SNMP-агенты существуют для широкого класса устройств, начиная от коммутаторов, IP-маршрутизаторов, принтеров, ПЭВМ, источниками электропитания и жизнеобеспечения и заканчивая АТСЭ. В результате протокол SNMP de-facto стал основным промышленным протоколом управления для различных средств и устройств.

Протокол SNMP является достаточно гибким и расширяемым протоколом управления. Агенты SNMP могут выполнять многочисленные задания, специфические для различных классов устройства, обеспечивая стандартный механизм сетевого управления и мониторинга.

К недостаткам SNMP, помимо уже перечисленных, можно отнести то, что протокол SNMP не является особенно эффективным с точки зрения сети передачи данных, нередко сетевой ресурс используется для передачи малосущественной для целей управления информации, например версия SNMP (передается в каждом сообщении SNMP), описание данных различной длины, которые содержатся в каждом сообщении.

Проблемы с обеспечением информационной безопасности широко используемых в настоящее время SNMP версии 1 и версии 2, существенны, о чём имеется специальное предупреждение неправительственной *организации по компьютерной безопасности CERT* (Computer emer-

gency response team, CERT) CA-2002-03 «Отчет CERT о множестве уязвимостей в некоторых реализациях SNMP» от 12.02.2002. Однако в данном извещении речь идёт преимущественно о недостатках SNMPv1. В версии 3 протокола SNMP проблемы, имевшиеся в версиях 1 и 2 с информационной безопасностью, вероятно, решены.

В целом, завершая обсуждение протокола SNMP, следует отметить, что этот протокол всё решительнее заменяет собой протокол CMIP, в том числе в традиционных системах связи. Об этом свидетельствует, например, использование протокола SNMP в системе NetManager производства компании Siemens (Германия) для управления коммутационной системой EWSD, версия 15.

Контрольные вопросы к главе 5.

1. Какие технические характеристики оборудования можно контролировать помощью протокола SNMP?
2. Каково назначение Интернет-базы данных IMIB?
3. Приведите описание стандартных операций управления в протоколе SNMPv2.
4. Можно ли реализовать агента SNMP в виде отдельной ПЭВМ со специальным программным обеспечением?
5. Для каких целей в протоколе SNMP используются прерывания?
6. Опишите основные функции и средства управления протокола SNMP.
7. В чём особенности PDU протокола SNMPv3?
8. Какие достоинства и недостатки имеются у протокола SNMP по сравнению с протоколом CMIP?

6. РЕАЛИЗАЦИЯ СЕТЕВОГО УПРАВЛЕНИЯ

6.1 Системы и платформы управления

До недавнего прошлого системы управления телекоммуникационными сетями, использующие принципы TMN, строились, в основном, на индивидуальной основе, без использования интегрированных платформ. Сейчас ситуация изменилась. В настоящее время на рынке продуктов сетевого управления появились многофункциональные платформы TMN для приложений, реализующих интегрированное управление разнородными телекоммуникационными сетями. К таким универсальным аппаратно–программным средствам управления относятся HP Open View Telecom, Digital TeMIP, Vertel TMN Manager Platform и Agent Platform, Siemens S&MNS, Tivoli NetView, Harris Network Management. Далее ряд этих решений рассматривается более подробно [8,9,11,12,14,15,16].

Под *платформой сетевого управления* понимается программно–аппаратный комплекс, предназначенный для реализации задач управления сетями и/или услугами электросвязи. Платформа предлагает потенциальному пользователю системы управления готовые решения – приложения управления, реализующие стандартные услуги управления; интерфейсы управления; программно-аппаратный комплекс поддержки. Оператор связи или сервис–провайдер, который приобрёл платформу, может воспользоваться существующей структурой MIB, имеющимися программами–менеджерами и, возможно, агентами, чтобы создать полноценную автоматизированную систему управления сетью электросвязи. Таким образом, платформа управления предлагает тиражируемые решения по управлению. На основе платформы управления оператор связи или сервис–провайдер может создавать законченные решения по системе управления с использованием продуктов разработки третьей стороны.

Следует отметить, что система управления, помимо собственно платформы управления, включает такие элементы, как:

- организационно-функциональную структуру управления;
- регламент сетевого управления;

- сформированные соглашения об уровне обслуживания SLA;
- распределение задач управления по уровням LLA TMN;
- распределение функций и обязанностей персонала;
- описание технологических процедур взаимодействия между уровнями управления;
- формы документооборота и порядок формирования и подачи отчётности о работе сети оператора связи.

Система управления может быть реализована как на единой, так и на нескольких платформах управления. Вне зависимости от того, с каким вариантом построения системы управления работает оператор, каждая система управления должна пройти стандартный цикл внедрения, соответствующей циклу внедрения автоматизированной системы управления по ГОСТ 34.601–90 «Информационная технология. Автоматизированные системы. Стадии создания» (введён с 01.01.1992).

При создании масштабной или ограниченной системы управления разнородным телекоммуникационным оборудованием, как правило, существует два основных варианта, на которые указывается в [15]:

- применение отдельных программных приложений управления для конфигурирования технических средств, мониторинга, диагностики или тестирования ряда элементов сети или сети связи одного вида (например, только сети SDH, только сети ATM);
- использование комплексной платформы управления, которая позволяет осуществлять комплексное управление различными видами сетей и служб связи из единого центра управления (см. главу 1) .

Оба варианта предусматривают, что внедряется система производства стороннего разработчика. Это не исключает возможности производства средств сетевого управления собственными силами, что сделано в таких крупных компаниях как MCI (США), Sprint (США), AT&T (США), Deutsche Telekom (Германия).

Каждый из вариантов создания системы сетевого управления имеет сильные и слабые стороны. Приобретение и создание системы «по частям» создаёт иллюзию относительно невысоких единовременных затрат. Действительно, продукт для решения одной задачи сетевого управления стоит существенно дешевле нежели платформа управления в целом.

Внедрение одного продукта занимает относительно небольшое время (4..6 месяцев). Проблемы начинаются с момента ввода в эксплуатацию нескольких продуктов, особенно от разных поставщиков. Здесь неизбежно возникают вопросы увязки и интеграции многих продуктов. Сказанное не означает, что решения сетевого управления на базе отдельных продуктов или совокупности отдельных продуктов не имеют право на существование. В частности, если продукты производятся одной компанией, то это снижает трудности интеграции. Например, корпорация Lucent Technologies (США) в 2001 г. объединила несколько приложений управления собственной разработки в программный продукт управления Navis iOperations Software (источник – www.lucent.ru/products/application/oss/soft/soft.html).

Приложения управления в составе iOperations Software реализуют «ролевую» концепцию управления, при которой те или иные приложения используются в зависимости от текущей потребности оператора. Приложение управления Navis iEngineer обеспечивает, в первую очередь, средства проектирования сети, внедрение новых сервисов и технологий, интегрированное планирование емкости сети, пуско-наладочные работы, развертывание и эксплуатация оборудования электросвязи. Другое приложение управление Navis iProvision в составе iOperations Software рассчитано на операторов, которые располагают действующей сетевой инфраструктурой, однако активно ее расширяют за счет включения новых сегментов или присоединения сетей других компаний (в качестве примера можно привести сотовых операторов). Приложение Navis iProvision обеспечивает «сквозное» конфигурирование подключаемых услуг и ускоренную активацию новых абонентов. С его помощью можно включать в эксплуатацию новые узлы связи, осуществлять синхронизацию данных о сетевых ресурсах и визуальное представление сети на дисплее рабочей станции.

Приложение Navis iAssure позволяет обеспечить контроль качества обслуживания (QoS) с помощью интегрированных средств устранения отказов, управления производительностью и услугами в гетерогенной среде, где используются различные телекоммуникационные технологии. Данное приложение проводит анализ корреляции отказов, сбор и анализ статистики о функционировании сети, выдает отчетность по выполнению

соглашений об уровне обслуживания (SLA), автоматически оповещает администрацию связи о возникновении сетевых проблем. Московская городская телефонная сеть (МГТС) использует iNavis Access в составе Navis iProvision для управления 90 узлами в широкополосной сети передачи данных общего пользования в части регистрации, активации абонентов, администрирования доступом к новым услугам связи. Также МГТС использует продукт iNavis NFM (Network Fault Manager), входящий в состав приложения Navis iAssure, для контроля трех коммутационных станций Lucent, а также ряда АТС других производителей (оборудование коммутации NEC, Siemens, Alcatel). Стоимость описанной системы, рассчитанной на 25 узлов, приближается к 500 тыс. долларов США.

Аналогично, по данным компании Hewlett Packard начальная цена решения на базе платформы управления телекоммуникационными сетями голосовой связи Compaq TeMIP составляет 350 000 долларов, а для крупных сетей связи она может достичь от 1 до 3 миллионов долларов США. Поэтому стоимостной показатель является существенным при принятии решения о способе реализации и конфигурации платформы сетевого управления.

На отечественных сетях связи помимо ОАО «Ростелеком» и МГТС, заслуживают внимания планы Петербургской телефонной сети (ПТС) по созданию системы управления сетью связи [1]. На ПТС установлено 5 основных типов цифрового коммутационного оборудования, 4 основных типа аналогового коммутационного оборудования и более 10 типов систем передачи. С 1999 г. на сети проводятся работы по созданию *информационно–технологической системы управления* (ИТСУ). Разработке планов создания ИТСУ предшествовал анализ существующей ситуации по управлению. В процессе анализа было отмечено, что в наименьшей степени подготовлена к современному управлению коммутационная телефонная сеть, в частности здесь отсутствует постоянное измерение нагрузки на межстанционной соединительной сети и управление трафиком. Поэтому на первом этапе создания ИТСУ предусматривается внедрение системы управления трафиком ПТС с организацией центра управления нагрузкой.

На сетях связи широко используются «фирменные» системы управления элементами сети или системы управления сетью, в частности :

- система управления Cisco Works производства компании Cisco Systems для управления средствами связи производства Cisco Systems;
- система управления Optivity Network Management System (NMS) производства компании Nortel;
- система управления 46020 MainStreet для управления оборудованием компании Newbridge, которая ныне приобретена компанией Alcatel;
- платформа управления Ericsson Packet Backbone Network (Ericsson PBN) и Element Management Access, EMA производство компании Ericsson.

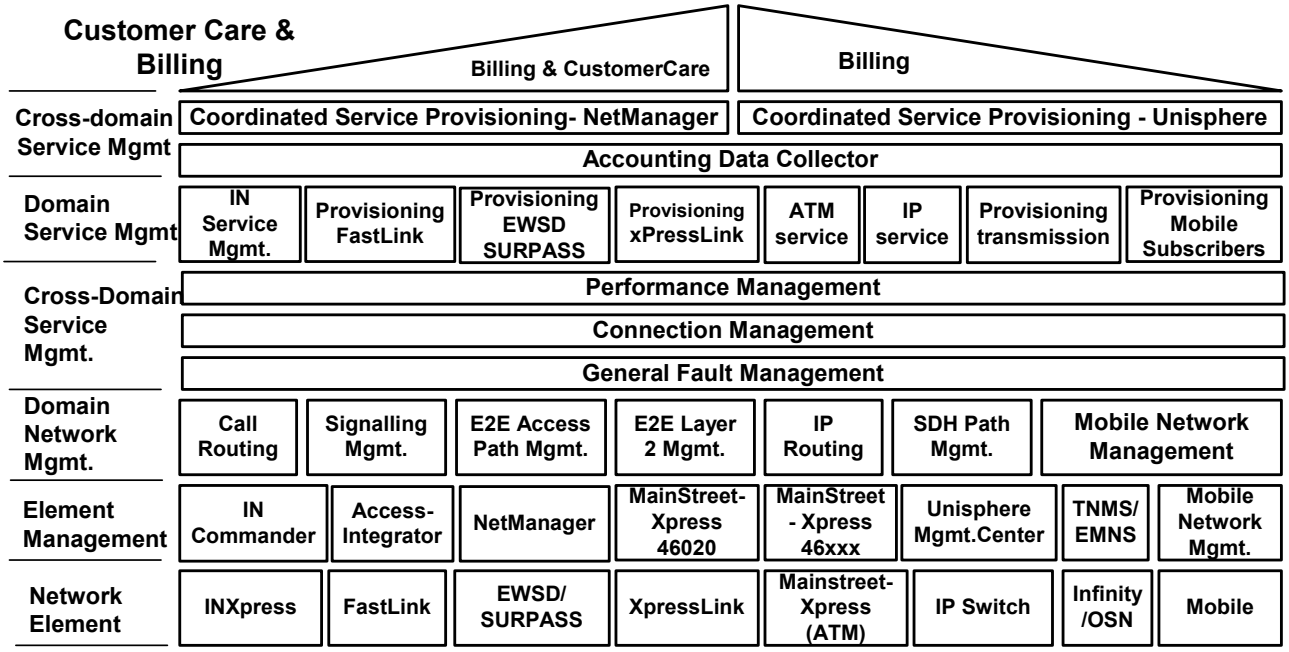
Итак, любой крупный производитель телекоммуникационного оборудования предлагает заказчикам систему управления оборудованием собственного производства. Однако фирменные решения не всегда способны включить в систему управления оборудование сторонних производителей. Для решения этой задачи необходимо наличие открытых и доступных пользователю интерфейсов взаимодействия с внешними системами.

6.2 Система управления S&NMS компании Siemens

Система управления услугами и сетями связи компании Siemens (Service & Network Management System, SNMS), построена по модульному принципу. В системе имеются стандартные области или домены управления: домен управления элементами сети (Domain Element Management), домен управления сетью связи (Domain Network Management), домен управление услугами (Domain Service Management). В решении Siemens также используются области межуровневого взаимодействия : междоменное управления сетью связи (Cross–Domain Network Management), междоменное управление услугами (Cross–Domain Service Management) [2]. В междоменных уровнях реализуются общие функции управления для всех видов сетей или элементов сети – основное управление неисправностями (General Fault Management), управление соединениями (Connection Management), управление техническими характеристиками сети (Per-

formance Management), сбор данных для расчёта стоимости услуг (Accounting Data Collector). Обращает на себя внимание, что на верхнем уровне, между межуровневой областью управления сетью и уровнем управления бизнесом находится область биллинга и подсистемы работы с клиентом (Billing & Customer Care), см. рис. 6.1.

Интегрированная система сетевого управления S&NMS компании Siemens предназначена для управления конвергентными сетями с передачей голоса, данных, в том числе для управления сетями подвижной связи, сетями доступа, первичными сетями SDH, сетями IP и интеллектуальными сетями. Обращает на себя внимание, что начиная с уровня управления элементами рассматриваемая система S&NMS управляет в основном оборудованием связи производства компании Siemens или компаний, приобретённых Siemens.



Сокращения и обозначения :
Mgmt. - управление
Coordinated Service Provisioning - скоординированное обеспечение услуги

Рисунок 6.1 – Архитектура системы управления S&NMS

Система S&NMS построена на основе отдельных прикладных продуктов (приложений) для сетевого управления:

- продукт NetManager – для управления коммутационной системой EWSD;

- продукт AcessIntegrator – для управления оборудованием доступа FastLink;
- продукт IMNS – для управления неисправностями сетей связи;
- продукт SPOTS/SPOTSXpress – для управления рабочими характеристиками сети.

Вся функциональность системы S&NMS доступна персоналу администрации связи через пользовательские приложения на базе IP–протокола и с применением технологии Интранет. Программными средствами администрирования устанавливаются различные уровни доступа пользователей к различным функциям системы. Для обмена данными используются следующие протоколы:

- для передачи аварийных сообщений – протокол SNMP;
- для передачи файлов – протокол FTAM/FTP;
- для интерфейсов приложений управления – Java/CORBA.

Далее перечисленные особенности S&NMS рассматриваются подробно.

Маршрутизация вызовов (call routing) и *управление системой сигнализации* (signaling management) в рассматриваемой схеме осуществляется с помощью продукта NetManager. Этот продукт позволяет оптимизировать использование каналов связи, осуществить функции администрирования, распределить сетевые ресурсы каналов связи, каналов передачи данных и сигнальных звеньев, которые подключены к оборудованию АТСЭ типа EWSD, оборудованию *SURPASS*™, и к оборудованию мобильных сетей связи (mobile Network). Имеется возможность поддержки профилей услуг управления для различных категорий пользователей.

В процессе сквозного управления по принципу *«из конца в конец»* на канальном уровне (End–to–End Layer 2 Management, E2E Layer 2 Management) с помощью продукта InterXpress MNS 7000 осуществляется обработка и управление сетевыми ресурсами и соединениями, а именно : физические линии связи, управление путями в ATM (ATM Path Management), администрирование сигнализацией Q.SIG. Аналогично, *сквозное управление мультисервисным доступом* (End–to–End Multi–Service Access Management, E2E Access Management) осуществляет управление

обычными и xDSL линиями доступа (решение по доступу FastLink) для передачи голоса и других служб в рамках продукта AccessIntegrator.

Управление IP–маршрутизацией (IP–Routing Management) осуществляется с помощью центра сетевого управления *Unisphere* (Unisphere Network Management Center). Этот модуль генерирует графическую схему сети с легко воспринимаемым оператором отображением топологии сети.

Управление путями в сети SDH и оптических сетях осуществляется с помощью *системы управления элементами сети* (Element Network Management System, ENMS) и *системы управления сетью передачи* (Transmission Network Management System, TNMS). Перечисленные продукты позволяют осуществлять управление оборудованием передачи семейства TransXpress, выполняются требования касающиеся сохранения управления при расширения сети, а также существуют возможности по маршрутизации, зависящей от стоимости маршрута и тарифов за передачу трафика.

Управление сетями подвижной радиосвязи (mobile network management) осуществляется с помощью модуля Mobile Integrator. Этот модуль представляет собой распределённую систему управления для сетей подвижной связи, которая обеспечивает необходимый баланс между требуемым качеством связи и оптимальным использованием радиочастотного спектра.

Общее управление неисправностями (general fault management) осуществляется с помощью *системы интегрированного управления сетью* (Integrated Network Management System, IMNS). Эта система разработана для следующих областей применения:

- Мониторинг мультисервисных сетей связи для интегрированной передачи голоса, данных.
- Мониторинг распределенных услуг.

Распределенные услуги – это услуги, которые обеспечиваются группой распределенных сетевых ресурсов с интегрированной поддержкой различных сетевых и информационных технологий. Используя INMS оператор может вводить в эксплуатацию услуги связи без учета технических особенностей компонентов сети (например, элементов сети, портов, линий). Эти услуги связи затем могут быть предоставлены заказчикам через *сетевой интерфейс обслуживания пользователей* (service user network

interface, SUNI). Система INMS способна интегрировать управление всеми видами сетевых протоколов и оборудованием связи, такими как WDM/SDH/PDH, ATM, Frame Relay, X.25, маршрутизаторы, концентраторы, коммутаторы, серверы доступа, АТСЭ и УПАТС.

Модуль *управления сетевыми соединениями* (Network Connection Management) осуществляет управление междоменными функциями. Основной задачей является обеспечение междоменного оконечного соединения с заданным качеством через гетерогенные сетевые домены. Для этого используется продукт InterXpress MNS 7000. Управление рабочими характеристиками (производительностью) сети осуществляется с помощью модуля SPOTS XDMS. Этот продукт осуществляет междоменное управление рабочими характеристиками сетей связи для обеспечения совместной передачи голоса и данных с заданным качеством.

Домен приложений управления услугами (Domain Service Management Application) состоит из следующих модулей :

- Управление услугами интеллектуальных сетей (IN Service Management) с многофункциональным пользовательским приложением INXpress.
- Управление услугами IP (IP Service Management) с помощью центра управления услугами Unisphere (Unisphere Service Management Center, SMC).
- Управление услугами ATM (ATM Service Management) с помощью продукта MainStreetXpress 46020.
- Обеспечение услуг для пользователей EWSD и SURPASS (Service Provisioning for EWSD and SURPASS hiA) с помощью модуля NetManager.
- Обеспечение услуг для пользователей скоростного доступа (Service Provisioning for FastLink subscribers) с помощью модуля AccessIntegrator.
- Обеспечение услуг для пользователей XpressLink (Service Provisioning for XpressLink subscribers) с помощью модулей MainStreetXpress Network и Service Management System.
- Обеспечение услуг передачи (Transmission Service Provisioning) с помощью системы ENMS и TNMS.

- Обеспечение услуг для пользователей подвижных систем связи (Service Provisioning for mobile subscribers) с помощью модуля SwitchCommander.

Компоненты *междоменного уровня управления услугами* (Cross Domain Service Management) используются для обработки данных с целью координации обеспечения услуг для бизнес–абонентов, которым доступны IP–сервисы. Сюда относятся услуги передачи речи и данных в IP–сетях, включая дополнительные IP–услуги в сетях IP–VPN. Здесь же решается задача интеграции управления xDSL и администрирования IP–маршрутизации. Междоменное управление услугами осуществляется с помощью модулей NetManager и Unisphere Management Center (UMC). На этом уровне управления, с учётом бизнес–процессов оператора и характеристик сети, может быть изменена последовательность этапов введения или обеспечения услуги. Здесь же поддерживается функциональный профиль услуг, который основан на профиле сетевых ресурсов. Профиль сетевых ресурсов обусловлен пакетом услуг, который продаётся конечному пользователю.

Сбор и конвертация данных для расчёта стоимости услуги (Accounting data collection and conversion, ADC) осуществляется с помощью модуля NetManager. Это приложение позволяет осуществить сбор детальных записей о состоявшихся сеансах связи, провести их предобработку, консолидацию и привести к единой форме (не зависящей от поставщиков оборудования связи) для тарификации.

Для обеспечения услуг уровня управления в структуре системы S&NMS используется система управления взаимоотношениями с клиентами (Customer Care System) и биллинговая система Arbor/BP производства компании Kenan System (США) для расчётов за услуги связи.

6.3 Платформа сетевого управления TeMIP фирмы Compaq

Платформа TeMIP (Telecom Management Information Platform) фирмы Compaq - решение для управления сетью и услугами для мультисер-

висных сетей связи. Платформа позволяет реализовать следующие функции управления сетью:

- контроль за телефонной нагрузкой;
- управление услугами связи;
- управление рабочими характеристиками сети;
- управление обнаружением неисправностей и отказами;
- управление последовательностью выполняемых действий при устранении неисправностей;
- ведение электронного журнала неисправностей (trouble ticketing).

Допускается интеграция с внешними приложениями управления, такими как управление нагрузкой, управление соглашениями об уровне обслуживания SLA.

Платформа TeMIP обеспечивает интегрированное представление телекоммуникационной сети для оператора связи в реальном масштабе времени, охватывает сетевой уровень и уровень услуг. Платформа TeMIP осуществляет управление следующими видами сетей связи :

- Сети подвижной связи стандарта GSM.
- Первичная сеть передачи SDH.
- Коммутационное оборудование АТСЭ, УПАТС.
- Корпоративные сети связи с интегрированной передачей речи и данных.
- Сеть ATM.
- Сети радиодоступа и беспроводные сети передачи.
- Сеть ОКС№7.

Платформа TeMIP включает в себя:

- Объектно-ориентированную распределенную информационную модель, которая поддерживает архитектуру «менеджер – агент».
- Набор программных приложений, которые управляют конфигурацией сети и последствиями неисправностей (отказов). Приложения управления разработаны таким образом, чтобы поддерживать развитие сети и изменение телекоммуникационных технологий без дополнительного изменения кодов программы.

Платформа TeMIP основана на открытых прикладных программных интерфейсах API и включает ряд инструментальных средств для обеспечения развёртывания системы, её расширения и развития.

Платформа TeMIP состоит из следующих компонентов :

- оболочка TeMIP (TeMIP Framework);
- управление неисправностями и проблемами (TeMIP Fault and Trouble Management);
- программное обеспечение клиента TeMIP на платформе Microsoft Windows NT;
- библиотека доступа TeMIP для операционной системы Windows NT и UNIX (TeMIP Access Library), которая обеспечивает разработку приложений и интерфейсов пользователей.

Кроме того, в состав TeMIP входят средства разработки :

- средства разработки приложений (TeMIP Application Developer's Toolkit) с визуальными средствами проектирования Visual TeMIP;
- экспертная система Expert System Access;
- средства разработки для протокола SNMP;
- средства разработки для доступа к стеку протоколов BOC.

Следует отметить наличие в составе TeMIP специального модуля доступа к *генератору неисправностей* (Alarm Generator Access Module). Этот модуль используется для имитации отказов элементов сети и применяется для тестирования приложений TeMIP.

Платформа TeMIP поддерживает развитый графический интерфейс G пользователя системы сетевого управления с возможностью вывода информации как в командной строке, так и в виде карт, графиков, условных обозначений. Интерфейс G, а также интерфейс F поддерживаются модулем представления.

Функциональные модули TeMIP поддерживают обработку сообщений о неисправностях с помощью специальных правил описания аварийной ситуации, на основании которых программное обеспечение генерирует аварийное сообщение.

Аварийное сообщение может быть сохранено в журнальном файле, отослано по электронной почте и способно автоматически запустить приложение управления для обработки аварийной ситуации.

Модуль услуг уведомления обеспечивает передачу сообщений о неисправностях или сетевых события к другим функциональным модулям системы.

Модуль автоконфигурации помогает пользователю конфигурировать, управлять и осуществлять мониторинг оборудованием, которое поддерживает IP–протокол. Этот модуль позволяет определить схему и структур сети.

Модуль управления доменом осуществляет менеджмент группы элементов сети а модуль графики осуществляет вывод графических карт, схем на экран рабочей станции.

Модуль регистрации (журналирования) фиксирует данные о каждом элементе сети, управляет группами общих атрибутов для классов управляемых объектов.

Модуль IP Poller осуществляет мониторинг и изменение состояния объектов SNMP.

Модуль фильтрации событий и корреляций позволяет пользователю TeMIP разделять общий поток информации управления на уровне источников, определять временные характеристики получения сообщений, устанавливать моменты превышения пороговых значений тех или иных характеристик сети и элементов сети. Здесь же осуществляется сбор статистической информации о работе сети.

Платформа TeMIP имеет следующие технические характеристики:

- полностью распределенная архитектура, включая высокоскоростную подсистему обработки событий на сети;
- мультипротокольная интеграция и поддержка протоколов OSI/CMIP Q3, SNMP;
- выбор графических интерфейсов, включая интерфейсы X Windows, OSF/Motif, Microsoft Windows NT;
- управление безопасным доступом;
- согласованная эффективность, позволяющая более чем сотни одновременных активных рабочих мест управлять миллионами объектов;
- фильтрация сообщений об отказах;

- использование интерфейса Q, который дает возможность TeMIP поддерживать функции TMN-агента;
- клиент-серверные среды, использующие технологии типа CORBA, Java и Microsoft.

Открытость платформы TeMIP позволяет реализовать взаимосвязь с внешними приложениями, такими как электронные таблицы, для эффективного и качественного анализа процесса обслуживания сети.

Схема платформы TeMIP показана на рис. 6.2 на следующей странице.

На рис. 6.2. модуль представления поддерживает вывод данных для администратора сети, репозиторий информации управления поддерживает информационную модель управляемых телекоммуникационных ресурсов и базу данных MIB. Модули доступа позволяют осуществлять связь TeMIP с агентом или медиатором.

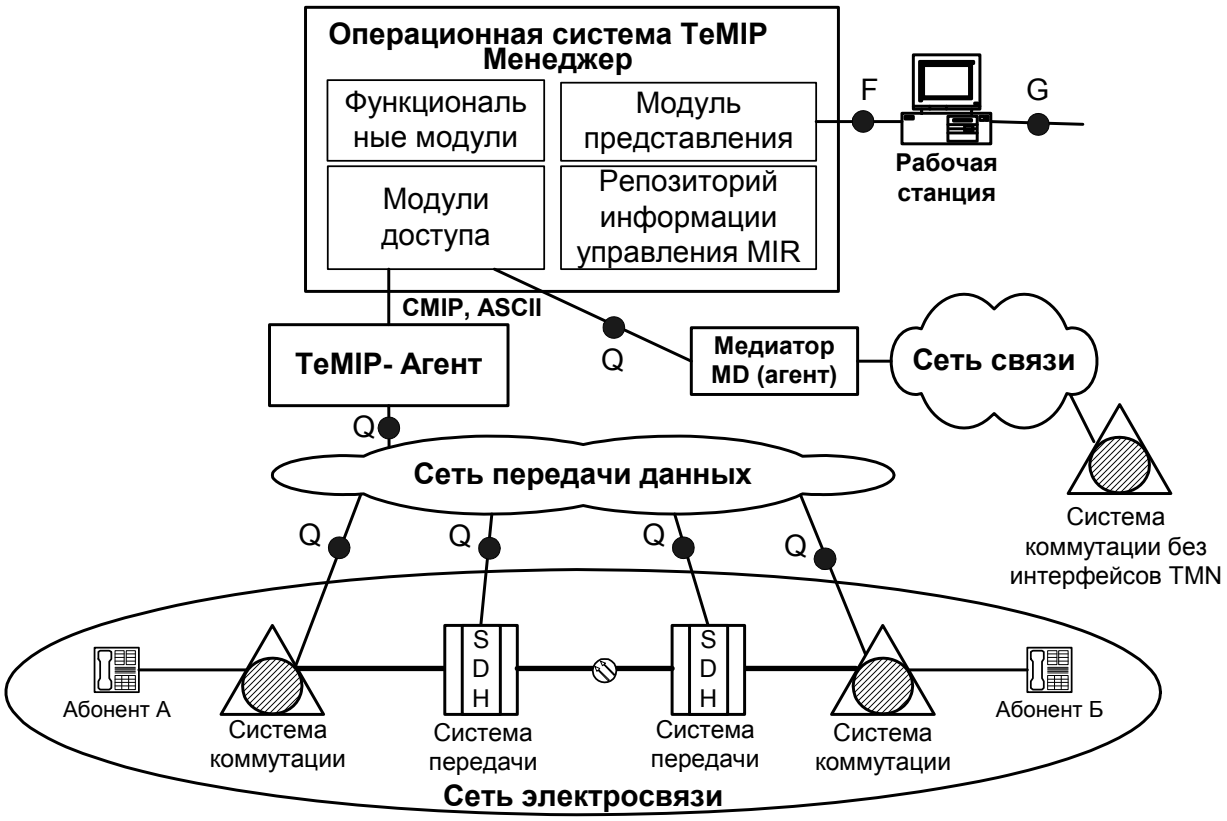


Рисунок 6.2 – Платформа управления TeMIP в рамках концепции TMN

В связи с объединением компаний Hewlett–Packard и Compaq в настоящее время решения TeMIP включены в состав платформы управления производства компании Hewlett–Packard; совокупно данные продукты обозначены как hp Open View TeMIP solutions (данные по состоянию на 1.09.2002 от источника информации по адресу www.openview.hp.com).

В рамках данного решения предлагаются следующие продукты в составе платформы TeMIP :

- Для управления сетью связи «из конца в конец» – продукт TeMIP Real–Time Network Operations.
- Для анализа маршрутов пропуска нагрузки для TeMIP – продукт TeMIP Expert.
- Для обработки сообщений о неисправностях – продукт TeMIP Fault Management.
- Анализ воздействия услуг связи на сетевую инфраструктуру – продукт TeMIP Service Monitor.

Для обеспечения повсеместной поддержки различных сетевых технологий предлагаются следующие решения :

- Активизация (запуск в эксплуатацию и оперативный контроль) сетей ATM, Frame Relay и DSL – продукт TeMIP Broadband Service Controller.
- Активизация сетей SDH – продукт TeMIP Broadband Service Controller.

Платформа TeMIP применяется для управления сетью связи компании British Telecom (Великобритания), где контролирует более 1000 коммутаторов, в том числе оборудование связи следующего поколения.

6.4 Платформа управления HP OpenView Telecom DM TMN

Платформа распределенного управления компании Hewlett-Packard (HP) OpenView Telecom Distributed Management (DM) TMN – это программная платформа, на которой строятся переносимые системы управления для телекоммуникаций, удовлетворяющие открытым стандартам. Работы по данной системе были начаты в 1985 г.

В 2000 г. платформа переименована в OpenView Communications/Service Assurance (HP OVC/SA), причём функциональные возможности управления были расширены с учётом необходимости поддержания заданного качества услуг пользователя в гетерогенных сетях [6].

При разработке HP OpenView Telecom DM TMN особое внимание уделялось требованиям производителей оборудования, поставщиков услуг и компаний системных интеграторов к надежности, производительности и возможности распределенного функционирования.

Компоненты HP OpenView Telecom DM TMN удовлетворяют спецификациям протоколов, объектов и услуг, определенных МСЭ–Т, ISO и IETF в части SNMP. Обеспечивается полная поддержка протоколов сетевого управления CMIP и SNMP. Платформа HP OpenView Telecom DM TMN построена в соответствии с принципами архитектуры открытых систем, позволяющей получать аппаратно-независимые решения.

Поддержка обеспечивается для рабочих станций и серверов HP типа 9000, работающих с операционной системой HP-UX версий 10.20, 11.0 и выше, а также рабочих станций Sun SPARC с операционной системой Solaris 2.6, 7, 8 и выше. Допускается применение компьютерных средств на базе микропроцессоров производства компании Intel с операционными системами MS Windows NT версия 4.0 и MS Windows 2000.

Платформа HP OpenView Telecom DM TMN предоставляет набор служб и услуг управления, которые могут использоваться для управления обработкой событий и сообщений от элементов сети и систем связи. Этот набор включает посредническую службу, которая осуществляет сбор, сохранение, фильтрацию и разбор сообщений, а также службу управления обработкой событий, отображающую и коррелирующую взаимосвязанные события и активизирующую внешние приложения на основе данных об аварийных ситуациях.

Платформа HP OpenView Communications (ранее – Telecom) DM TMN включает два базовых продукта :

Платформа DM TMN Agent – включает необходимую коммуникационную инфраструктуру (аппаратно-программное обеспечение), которое позволяет осуществлять маршрутизацию сообщений, оказывать услуги автоматического контроля информационного обмена между приложения-

ми управления, предоставлять услуги регистрации объектов в базе данных агента и услуги обработки событий.

Эта же платформа позволяет осуществлять развёртывание программы-агента для элементов сети или разработку приложений управления с графическим интерфейсом пользователя.

Платформа DM TMN Manager – объединяет платформу сетевого менеджера и *инструменты разработчика менеджеров* (Manager's Developer's Kit).

Данная составляющая платформы сетевого управления включает DM TMN Agent вместе с продуктом Network Node Manager. Платформа DM TMN Manager поддерживает разработку сетевых менеджеров и комбинированных приложений менеджер–агент. Имеется графический интерфейс с поддержкой географических карт OpenView Windows GUI.

Продукт Network Node Manager [Менеджер сетевых узлов] обеспечивает интеллектуальное, ориентированное на пользователя управление сетевого окружения для провайдеров услуг сети Интернет, пользователей услуг аутсорсинга (outsourcing) и провайдеров услуг связи в промышленном масштабе (Enterprise service providers).

Согласно рекламным материалам компании Hewlett-Packard, решения HP OpenView Network Node Manager в настоящий момент являются «краеугольным камнем» семейства HP OpenView и основой для разработки решений третьей стороной на базе Network Node Manager.

Продукт Network Node Manager поддерживает централизованной хранилище данных системы и *обработку данных управления*, что позволяет администраторам сетей выполнять сложный анализ тенденций развития сетевой ситуации.

При этом используется технология *интеллектуальной корреляции событий* (event correlation technology), позволяющая устанавливать взаимосвязь между сигналами о неисправности.

В результате администратору сети с помощью функции *маршрутизации* поступает единый высокоуровневый сигнал о главном источнике возникшего сбоя.

Данный продукт позволяет автоматически создавать и поддерживать карту TCP/IP и IPX сетей, поддерживается «тонкий» клиент на основе Java и WEB-интерфейс пользователя.

Графический пользовательский интерфейс GUI обеспечивает пользователей представлением об управляемой среде и позволяет интегрировать функции управления, независимо от поставщика или типа управляемого объекта.

Общая схема платформы HP OpenView Telecom DM TMN представлена на рис. 6.3.

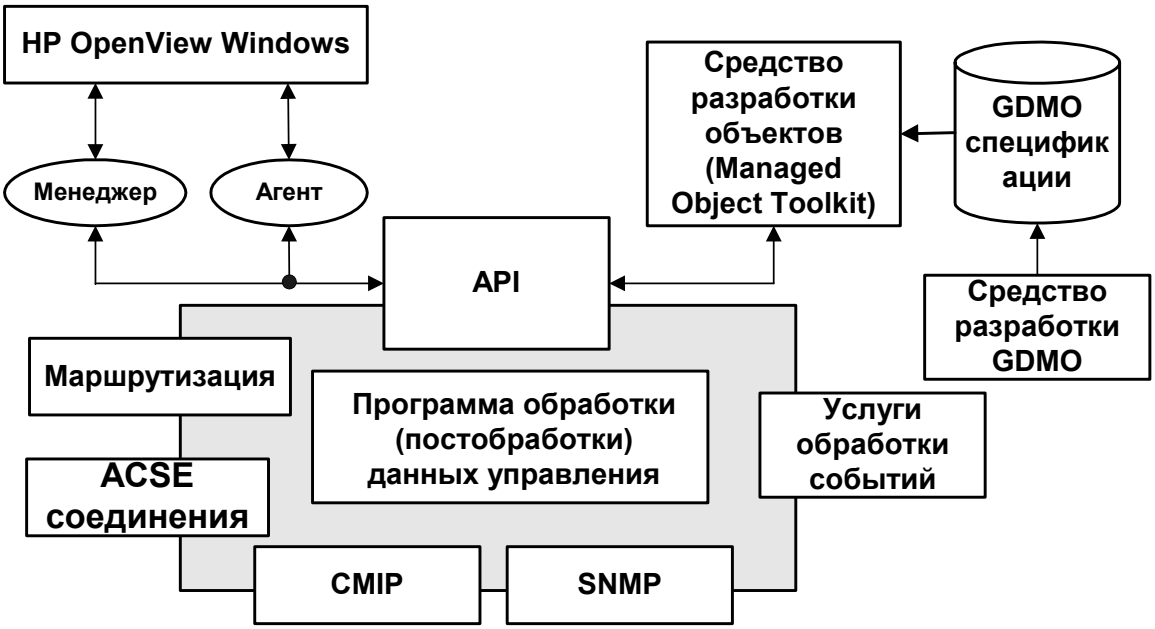


Рисунок 6.3 – Основные компоненты платформы HP OpenView Telecom

Решения по интегрированному управлению услугами предлагаются компанией Hewlett-Packard в виде компонента HP ISM (Integrated Service Management). Основные компоненты HP ISM:

Компонент HP OpenView – позволяет отслеживать и контролировать ресурсы и телекоммуникационную инфраструктуру, а также управлять ими.

Компонент HP Process Manager – предоставляет возможность оперативно определять, отслеживать и детализировать операционные/сетевые процессы на всем протяжении жизненного цикла услуг.

Компонент HP Internet Usage Manager – предоставляет возможности для биллинга т.е. расчётов за услуги связи, реализуемые с помощью информации об использовании услуг.

В составе HP ISM применяется несколько программных продуктов. Продукт HP Service Delivery позволяет быстро, эффективно и с минимальными затратами внедрять новые услуги связи. HP Service Delivery управляет процессом активации услуг, а также осуществляет контроль за ходом их предоставления.

Контроль обеспечения качества обслуживания осуществляется с помощью продукта HP Service Assurance. Этот продукт управляет соглашениями об уровне обслуживания SLA и поддерживает для предоставляемых услуг такой уровень качества, который установлен для клиентов согласно SLA. Это решение позволяет управлять всеми компонентами, составляющими процесс проверки качества обслуживания : управление последствиями отказов, создание нарядов на выполнение работ и управление производительностью (техническими характеристиками) сети. С помощью HP Service Assurance можно обеспечить высокое качество обслуживания и добиться оперативного разрешения проблем при минимальном времени простоя сети электросвязи.

В составе набора продуктов для управления услугами имеются решения по управлению услугами IP–телефонии. Основные компоненты решений HP для управления услугами IP-телефонии нового поколения выглядят следующим образом:

- платформа HP OpenCall – программное средство организации сеансов, контроля услуг и оборудования IP–телефонии;
- программные коммутаторы Softswitch, шлюзов и серверов приложений от партнеров Hewlett-Packard;
- интегрированное управление услугами HP VoIP (voice over IP, голос по сетям IP);
- серверы и устройства хранения данных HP, оптимизированные для работы у операторов связи.

Помимо управления услугами проводных средств связи, в составе HP ISM имеется ряд продуктов для управления услугами подвижных сетей связи.

По утверждению компании Hewlett-Packard, 67% американских компаний, провайдеров Интернет-услуг используют программное обеспечение HP Open View. В настоящее время объединённое решение HP Open

View TeMIP solutions применяется на 170 телекоммуникационных сетях, в том числе на 8 крупнейших международных сетях из 10 (по рекламным данным). Лицензиями на право использования этой платформы OpenView DM Telecom TMN обладают ведущие зарубежные компании Siemens, Alcatel, Nortel, Lucent, Nokia, Fujitsu. Платформа HP Open View TeMIP интегрирована с продуктами и устройствами таких фирм, как Motorola, Siemens, Marconi, Tellabs, Ericsson. В частности, крупнейшая компания British Telecom использует HP Open View TeMIP в качестве контроллера услуг широкополосной сети для обеспечения услуг ATM, FrameRelay, ADSL.

В России решения HP OpenView OEMF в виде комплекса мониторинга телекоммуникационных сетей были сертифицированы Минсвязи России в 2000 г. В качестве пилотного проекта был выполнен Центр технической эксплуатации и мониторинга в ОАО «Тулателеком» на ГТС г. Тула, где осуществлялось управление АТСЭ типа DX200 производства компании Nokia и АТСЭ Alcatel 1000 S12. Также HP OpenView OEMF с 1998 года применяется в филиале ОАО «Ростелеком» – «Московский междугородный и международный телефон».

В настоящее время компания Hewlett-Packard также предлагает средства HP OpenView ServiceCenter/SLM для полного управления качеством услуг связи. Данное приложение позволяет осуществлять мониторинг и генерацию сообщений о предоставлении услуг связи в реальном времени.

6.5 Развитие систем сетевого управления

Одной из главных причин бурного развития систем и платформ управления в 1990-х – 2000-х г.г является постоянная конкуренция в сфере телекоммуникаций. Причём конкуренция идёт не на уровне телекоммуникационного оборудования – парк технических средств связи практически одинаков у конкурирующих операторов или сервис-провайдеров.

В условиях конкурентной борьбы и развития рынков новых и базовых услуг связи на передний план выходит обеспечение гарантированного качества услуг связи. Решение этой задачи требует от оператора как вертикальной так и горизонтальной интеграции имеющейся телекоммуникационной инфраструктуры.

Если требуется обеспечить качество услуги по принципу «из конца в конец», то здесь необходимо осуществлять не только технический контроль и управление элементами сети и сетью связи, но и постоянно сравнивать получаемые статистические данные с условиями соглашения об уровне обслуживания SLA, заключенного с пользователем. В этом случае серьёзное влияние приобретают технологические процедуры, мероприятия и программно-аппаратные средства по обеспечению *гарантии качества услуг* (Service Assurance).

Для поддержки гарантии качества услуг осуществляется оптимизация бизнес-процессов операторов и сервис-провайдеров, что предусматривает применение новых методов исследования и моделирования бизнес-процессов как на содержательном уровне (уровень описания), так и на уровне реализации. Продолжается совершенствование средств и методов анализа/синтеза технологических цепочек производственных процессов с целью снижения эксплуатационных затрат на предоставление услуг связи и повышения эффективности использование оборудования.

На нижних уровнях управления (управление элементами сети и управление сетью) происходит дальнейшее развитие систем управления «от производителей». Проблема состоит в том, чтобы в программном обеспечении управления систем и оборудования связи были предусмотрены стандартные интерфейсы управления Q и необходимые средства для создания MIB. Функции управления и протоколы управления, доступные с помощью интерфейса Q, должны быть одинаковы для различных систем управления. В противном случае существенно возрастают затраты на создание интегрированной системы управления сетью и услугами. В этой связи для семи межрегиональных компаний связи (МРК) и ОАО «Ростелеком» актуальной является задача создание интегрированной («зонтичной») системы управления транспортной сетью SDH (рис. 6.4на следующей странице), которая будет взаимодействовать с «фирменными» системами управления сетью и/или сетевыми элементами, развернутыми на территории филиалов МРК.

Особое значение приобретают методы интеграции управления различными видами электросвязи. Принципиальной задачей является унификация информации управления внутри системы. В системе управления существуют самые разнообразные данные – сведения об объёме пере-

данной/принятой информации, сведения о продолжительности сеансов связи, которые далее используются для расчётов за услуги связи, многообразная технологическая информация. Необходимо привести описанные данные к единой форме представления так, чтобы при расчёте за услуги связи принималось во внимание не только фактическое время пользования услугой но и качество связи. Это особенно важно для систем IP-телефонии, других телематических служб.

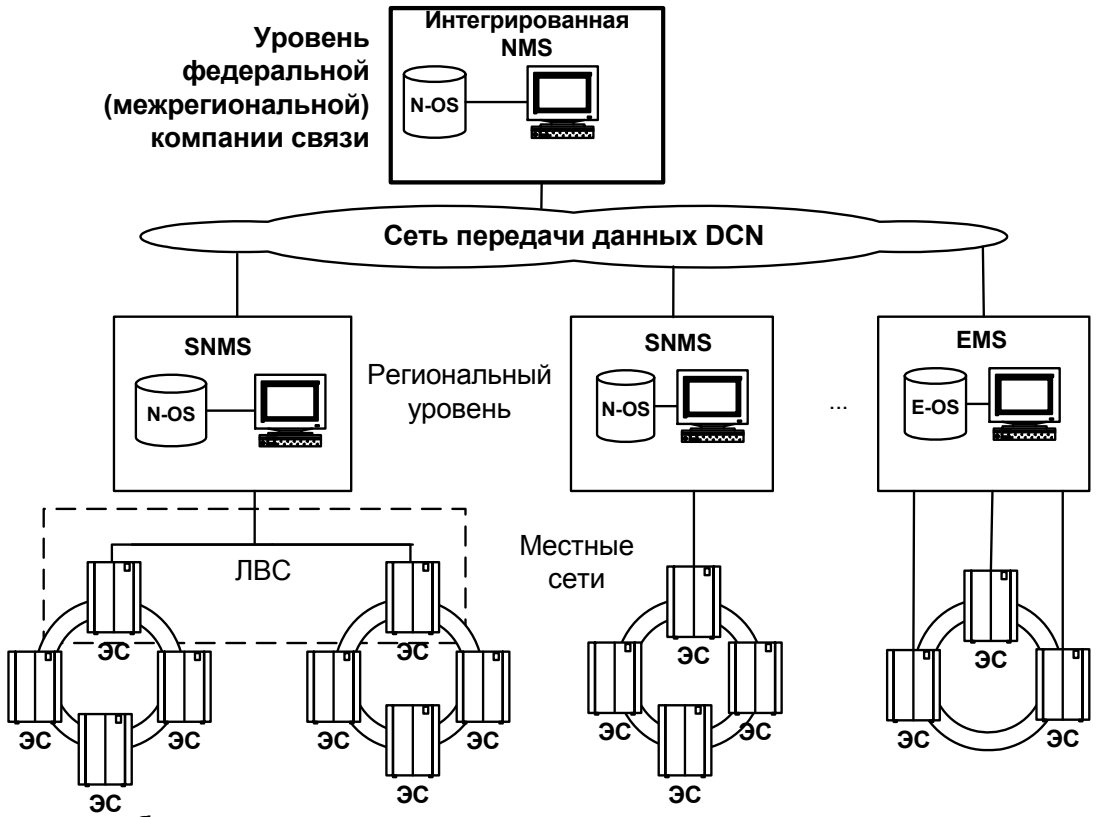


Рисунок 6.4 – Интегрированная система управления транспортной сетью SDH для МРК (по данным ЦНИИС, ЛОНИИС)

Важным является направление, связанное с предоставлением части полномочий, по управлению услугами и оборудованием связи пользователю. Эти мероприятия позволят разгрузить оператора от многих рутинных функций по управлению, обеспечивают источник доходов за счёт администрирования профиля услуг клиента, платного доступу к подроб-

ным сведениям о состоянии лицевого счёта пользователя [14]. Здесь необходимо чётко разграничить доступ к информации управления, обеспечить информационную безопасность доступа.

Для решения задач управления услугами и сетями связи важным является уровень развития новых информационных технологий [5]. Учитывая совершенствование технологий промежуточного уровня (middleware), перспективные программные приложения управления будут поддерживать распределённую обработку информации управления. Это приведёт к применению децентрализованной схемы обработки данных при сохранении принципов централизованного управления. Использование технологий распределённой обработки может привести к уменьшению числа уровней управления. Не исключено, что на начальном этапе развёртывания современной системы сетевого управления, центры управления будут создаваться по видам сетей связи (ЦУ первичной сети связи и ЦУ коммутируемой телефонной сеть), а с течением времени эти центры будут преобразованы в центры объединённого управления сетями электросвязи.

Контрольные вопросы к главе 6.

1. Дайте определение понятию «платформа TMN».
2. В чём различие между системой и платформой сетевого управления?
3. В чём особенность решения компании Siemens для управления сетями связи ?
4. Какими средствами связи можно управлять с помощью платформы Compaq TeMIP ?
5. Каковы основные направления развития систем управления ?

ИСТОЧНИКИ ИНФОРМАЦИИ

1. Берлин Б.З, Ларичев И.И, Ревелова З.Б. Разработка и внедрение системы управления на принципах TMN// Вестник связи.– 1999.– №12.

2. Боро Б. Междоменное взаимодействие – необходимое звено управления сетью будущего// Вестник связи.– 2000.– №4.– с.86–92.

3. Булгак В.Б., Варакин Л.Е и др. Концепция развития связи Российской Федерации. – М.: Радио и связь, 1995.

4. Гольдштейн Б.С. Сигнализация в сетях связи. – М.: Радио и связь.– 1997.

5. Гордеев Э.Н. Новые технологии в системах управления сетями связи // Вестник связи– №1.–2000.– с. 29–32; №2–2000. – с.79–83.

6. Гордеев Э.Н. Использование современных технологий в системах управления сетями связи. // Электросвязь.–№7.–1998.–с.8–18.

7. Гребешков А.Ю. Стандарты и технологии управления сетями электросвязи. – М.: Эко–Трендз, 2003 г.

8. Гриднев С.А, Коновалов Г.В. Управление сетью синхронизации в сетях на основе СЦИ // Мир связи. Connect.–1998.–№12; 1999.–№1–с.138-141.

9. Дымарский Я.С, Крутякова Н.П, Яновский Г.Г. Управление сетями связи : стандарты, протоколы, прикладные задачи. Серия изданий «Связь и бизнес», М.: ИТЦ «Мобильные коммуникации», 2003.

10. Даленбах Д., Мирошников Д.Г. Единая система технической эксплуатации сети связи// Вестник связи – 1996. – №12 – с.23-27.

11. Дубенсков П.О. TMN в конце туннеля// Системы и сети связи.– 1998.– №5.

12. Закумбаева З.А. Современные системы управления сетями связи //Вестник связи – 2000.–№1– с.33-34.

13. Иванов П.И. Управление сетями связи. – М.: Радио и связь, 1999 г.

14. Князев К.Г. Система управления сетью как источник новых доходов // Вестник связи. – 2001. – №1. – с. 26–29.

15. Нетес В.А, Гриднев С.А, Дорф И.Г. Зарубежный опыт развития систем управления сетями связи и перспективы их развития : обзор // Электросвязь. – 1994. – с.3 –17.

16. Нетес В.А., Трубникова Н.В. Управление сетями : стандарты, проблемы и перспективы // Вестник связи. – 2000. – №2. – с.83 – 87.

17. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – Изд-во Питер: С-Пб. – 2000 г. – 672 с.

18. Основные положения развития Взаимоувязанной сети связи Российской федерации на перспективу до 2005 г. Руководящий документ. Книга 1,8 – М., ЦНТИ «Информсвязь», 1996 г.

19. Основы управления связью Российской Федерации/ В.Б. Булгак, Л.Е. Варакин, А.Е. Крупнов и др.; Под ред. А.Е. Крупнова и Л.Е. Варакина. – М.: Радио и связь, 1998.

20. Построение систем управления сетями связи операторов ВСС РФ. Руководящий документ. – М.: Минсвязи России, 2001.

21. Проектирование системы централизованного технического обслуживания оборудования ГТС : Учебное пособие / Росляков А.В, Карташкин А.Н., Харченко Ю.Ю. – Самара.: ПИИРС, 1997.

22. Шмалько А.В. Цифровые сети связи : основы планирования и построения. – М.: Эко-Трендз, 2001 г.

23. CMIP Services and Topology Agent Programming Guide. Document Number: SC31-6544-00. Режим доступа : [http://publib.boulder.ibm.com/cgi-bin/bookmgr/BOOKS/ISTP7000/CCONTENTS 25.03.2002]

24. Divakara K. Udupa TMN: Telecommunications Management Network. - McGraw-Hill. – 1999. – 420 p.

25. ES 201 654. Telecommunications Management Network (TMN); X interface; SDH path provisioning and fault management. – June, 1999 – V1.1.1.

26. ITU–T Recommendation M.3010. Principles for a telecommunications management network. – 2000.

27. ITU–T Recommendation M.3020. TMN interface specification methodology. – 2000.

28. ITU–T Recommendation M.3200. TMN management services and telecommunications managed areas: overview. – 1997.

29. ITU–T (Prepublished recommendation) M.3300. TMN F interface requirements. – 1998.

30. ITU–T Recommendation M.3400. TMN management functions. – 2000.

31. ITU-T: Recommendation X.711**.** Information technology – Open Systems Interconnection – Common management information protocol. **–** 1997.

32. ITU–T Recommendation Y.110. Global Information Infrastructure principles and framework architecture. – 1998.

33. Petermueller W. J. Q3 Object Models for the Management of Exchanges.//IEEE Communications Magazine. – March, 1996. – Volume 34, Number 3.

34. Pras Aiko Network Management Architectures. – CTIT Ph. D-thesis series No. 95-02. – Thesis University of Twente, Enschede. – With ref. ISBN 90-365-0728-6. – 1995. Режим доступа : [http://www.simpleweb.org/nm/research/results/publications/pras/thesis.html 17.10.01]

35. Raman L. CMISE Functions and Services/IEEE Communications Magazine. – May 1993. – Volume 31, Number 5. Режим доступа [http://www.comsoc.org/livepubs/surveys/public/raman/raman.html 4.04.01]

36. RFC 1095. The Common Management Information Services and Protocols for the Internet (CMOT and CMIP). – October, 1990.

37. RFC 1441. Introduction to version 2 of the Internet-standard Network Management Framework. – IETF. – April 1993.

38. RFC 1442. Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2). – IETF. – April 1993.

39. RFC 1444. Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2). – IETF. – April 1993.

40. RFC 1446 Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2). – IETF. – April, 1993.

41. RFC 1448. Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2).– IETF. – April 1993.

42. RFC 1450. Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2). – IETF. – April 1993.

43. Stallings W. SNMP, SNMPv2, SNMPv3, and RMON1 and 2, Third edition. – Addisson-Wesley. – 1998.

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ

A – Agent – Агент
ACCD – Available Connections Change Dissemination – Распространение по сети изменений в данных о доступных соединениях
ACSE – Association Control Service Element – Элемент услуги управления ассоциациями
AD – Adaptation device – Устройства адаптации
ADC – Accounting data collection and conversion – Сбор и трансформация данных для расчёта стоимости услуг связи
ADSL – Asymmetrical Digital Subscriber Line – асимметричная цифровая абонентская линия
AF – Application Function – Функции приложения
AIS – Alarm Identification Signal – Сигнал индикации аварийного состояния
ANSI – American National Standard Institute – Американский национальный институт стандартов
AP – Application Process – Прикладной процесс
AP – Application Protocol – Прикладной протокол в GII
API – Application Programming Interface – Прикладной программный интерфейс
APDU – Application PDU – PDU приложения
ASE –Application Service Element – Элемент услуги приложения
ASN.1 – Abstract Syntax Notation no 1 – Абстрактная запись синтаксиса № 1
ATCCD – Ability To Connect Change Dissemination – Способность распространять по сети информацию об изменении соединений
ATM – Asynchronous Transfer Mode – Асинхронный режим переноса
BER – Basic Encoding Rules – Базовые правила кодирования (данных)
BMF – Basic management functions – Базовая функция управления
BML – Business Management Layer – Уровень управления бизнесом
BML – Business Management System – Система управления бизнесом
BPI – Basic Programme Interrface – Базовый программный интерфейс
CASE – Computer-aided software engineering – Автоматизированное проектирование и создание программ
CERT – Computer Emergency Response Team – Группа реагирования на угрозы безопасности компьютерных систем
CDMA – Code division multiplexing access –Технология мультидоступа с кодовым разделением каналов
CF – Control Function – Функция контроля в GII

CLNS – Connectionless-Mode Services – Услуги протокола без установления соединения

CMIP – Common Management Information Protocol – Общий протокол информации управления

CMIS – Common Management Information Service – Услуга общей информации управления (услуга информационного протокола общего управления)

COM – Component Object Model –Компонентная модель объектов

CONS – Connection-Mode Services – Услуги протокола с установлением соединения

CORBA – Common Object Request Broker Architecture – Общая архитектура брокера запросов объектов

CORBA IDL – CORBA Interface Description Language – Язык описания интерфейсов CORBA

CCS №7 – Common Channel Signaling no 7 – Общеканальная система сигнализации №7

CUA – Common User Access – Общий доступ пользователя

DCF – Data Communication Function – Функция передачи данных

DCC – Data Communications Channel – Служебный канал передачи данных

DCE – Distributed Computing Environment – Распределённая компьютерная обработка

DCN – Data Communication Network – Сеть передачи данных

DLC – Deliverablerable Link Connection – Предоставляемое соединение звена

DPT - Danamic Transport Data – протокол динамической передач пакетов

DSL – Digital Subscriber Loop – Цифровая абонентская линия

DWDM – Dense Wavelength Division Multiplexing – Мультиплексирование с разделением по длине волны

ECC – Embedded Communication Channel – Встроенный канал передачи данных

EEI – Environment External Interface – Интерфейс внешней среды

EML – Element Management Layer – Уровень управления элементом

EMS – Element Management System – Система управления элементом

ETSI – European Telecommunication Standard Institute – Европейский институт стандартов в области связи (телекоммуникаций)

ES – End System – Оконечная открытая система

FTAM – File Transfer Access Methode – Управление доступом передачи файлов

FTP – File Transfer Path – Протокол передачи файлов

GDMO – Guidelines for Definition of Managed Objects – Общее опреде-

ление объектов управления

GII - Global Information Infrastructure – Глобальная информационная инфраструктура

GPRS - General Packet Radio Service – Общая радиослужба передачи данных

HCIF – Human-Computer Interfacing – Интерфейс «человек-машина»

HCIF – Human-Computer Interfacing Function – Функция интерфейса «человек-машина»

HDLC – High-level data link control protocol – Протокол высокого уровня для управления каналом передачи данных

HDSL - High Bit Rate Digital Subscriber Line – Цифровая абонентская линия с высокой скоростью передачи данных

HMI – Human-machine interface – Интерфейс «человек – машина»

HTTP – Hypertext Transfer Protocol – Протокол передачи гипертекстовой информации

HTML – HyperText Markup Language – Язык гипертекстовой разметки (в сети Интернет)

IEEE – Institute of Electrical and Electronics Engineers – Институт инженеров по электротехнике и электронике

IETF – Internet Engineering Task Force – Рабочая группа по инженерным проблемам Интернета

IMIB - Internet Management Information Base – Интернет-база информации управления

INAP – Intelligent Network Application Part – Прикладная подсистема пользователя интеллектуальной сети в ОКС №7

IP Internet Protocol –Протокол межсетевого взаимодействия

IS Intermediate system – Промежуточная открытая система

IS-IS Intermediate system to IS – Протокол взаимодействия промежуточных систем

ISDN – Integrated Service Digital Network– Цифровая сеть с интеграцией служб, ЦСИС.

ISO – International Standard Organization – Международная организация по стандартизации

ITU – International Telecommunication Unit – Международный союз электросвязи

ITU-T – International Telecommunication Unit – Standardization Sector – Международный союз электросвязи – сектор стандартизации

LAPB(D) – Link Access Procedure B (D) – channel – Процедура доступа к линии B(D)–канала

LC – Link Connection – Соединение звена

LCC – Logical Link Control – Протокол управления логической линией

LCS – Leased Circuit Services – Услуга аренды линии

LLA – Logical Layer Architecture – Логическая многоуровневая архитектура
LT – Line Terminal – Линейное окончание в ISDN
M – Manager – Менеджер, программная логика
MAF Manager Application Function – Функция приложения управления
ManF Management Function – Функция управления в GII
MAS Management Association Services – Услуги управления связями (между приложениями)
MCF – Management Communication Function – Функция передачи сообщений
MD – Management Device – Устройство медиации, медиатор
MESA – Mobile e-Services Architecture – Архитектура мобильных электронных услуг
MF – Mediation Function – Функция медиации
MF – Middleware Function – Функции промежуточного слоя (промежуточного ПО) в GII
MFS – Management function sets – Множество функций управления
MIB – Management Information Base – База информации управления
MIS – Management Information Service – Услуга информации по управлению
MNS – Management Notification Service – Услуга управления уведомлениями
MO – Management Object – Управляемые объекты, объекты управления
MP – Middleware Protocol – Протокол промежуточного уровня в GII
MPLS – Multi-Protocol Label Switch – Многопротокольная коммутация на основе меток
NE – Network Element –Элемент сети, сетевой элемент
NEF – Network Element Function – Функция элемента сети
NEL – Network element layer – Уровень элемента сети
NIC – Network Interface Card – Сетевая интерфейсная карта
NF - Network Function – Функция сети
NIST – National Institute of Standards and Technology – Национальный институт США по стандартам и технологиям
NMF – Network Management Forum – Форум сетевого управления, ныне TMF.
NML – Network Management Layer – Уровень управления сетью
NMS – Network Management System – Система управления сетью
NPDU – Network Protocol Data Unit – Сетевой блок данных протокола

NT – Network Terminal – Сетевое окончание в ISDN

ODP – Open distributed processing – Открытая распределённая обработка [данных]
OMG – Object Management Group – Группа по управлению объектами, неправительственная организация
OS – Operation System – Управляющая система (операционная система)
OSF – Operation System Function – Функция управляющей системы
OSI – Open System Interaction – Взаимосвязь открытых систем
OSIE – Open System Interaction Environment – Среда взаимосвязи открытых систем
PDU – Protocol Data Unit – Блок данных протокола
RPC – Remote Procedure Call – Удалённый вызов процедуры
P&SF – Processing and Storage Function – Функция обработки и хранения информации.
PCI – Protocol control information – Управляющая информация протокола
Q – Q-interface – Q-интерфейс
QA – Q-adapter – Q-адаптер
QAF – Q-adapter Function – Функция Q-адаптера
QoS – Quality of Service – Качество обслуживания
RAD – [user] Requirements, Analysis and Design – требования пользователя, анализ и разработка
RDSL – Rate Adaptive Digital Subscriber Line – Цифровая абонентская линия с адаптивной скоростью передачи
RFC – Request For Comments – обозначение документа IETF
RMON – Remote Monitoring – Дистанционный мониторинг
ROSE – Remote Operations Service Element – Элемент услуги удалённого выполнения операций
RPC – Remote Procedure Call – Удалённый (дистанционный) запрос процедуры.
SAP – Service Access Points – Точка доступа к услуге
SCF – Service Control Function – Функция контроля услуг
SDH – Synchronous Digital Hierarchy – Синхронная цифровая иерархия
SDL – Specification and Description Language – Язык спецификаций и описаний
SDU – Service data unit – Блок данных услуги
SDSL – Symmetrical Digital Subscriber Line – Симметричная цифровая абонентская линия
SLA – Service Level Agreement – Соглашение об уровне обслуживания
SMAE Service Management Application Element – Прикладной объект управления системой
SMASE Service Management Application Service Element – Элемент

прикладной услуги управления системой

SMC Service Management Center–Центр управления услугами

SMI Structure of Management Information – Структура информации управления (управляющей информации)

SMF Systems Management Function – Функция управления системой

SML Service Management Layer – Уровень управления услугами

SMK – Shared Management Knowledge – Управление знаниями об объекте управления

SML – Service management layer – Уровень управления услугами

SMS – Service management system – Уровень управления услугами

SNC – SubNetwork Connections – Соединение подсети

SNMP – Simple Network Management Protocol – Простой протокол сетевого управления

STM –Synchronous Transport Module – Синхронный транспортный модуль.

SUNI – Service user network interface– Сетевой интерфейс обслуживания пользователя

SQL – Server-Client Language – Язык запросов Сервер-клиент (архитектура «клиент-сервер»)

TF – Transformation function – Функция преобразования

TF – Transport Function – Транспортная функция в GII

TCP – Transmission Control Protocol – Протокол контроля передачи (входит в стек протоколов TCP/IP)

TMF – TeleManagement Forum – Форум по управлению телекоммуникациями, неправительственная организация

TMN – Telecommunications Management Network – Сеть управления электросвязью

TRP –Telecommunications Reference Point – Опорная точка сети электросвязи

UDP – User Datagram Protocol –Протокол передачи дейтаграмм пользователя

UML – Unified Modelling Language – Язык унифицированного моделирования

UMTS – Universal Mobile Telecommunications System – Универсальная система мобильной связи

UNI – User-Network Interface – Интерфейс «пользователь – сеть».

UCD – User Centered Design – Дизайн интерфейса, ориентированный на пользователя

UTRAD – Unified TMN Requirements, Analysis and Design – Единые требования TMN, анализ и разработка [интерфейсов]

VC – Virtual Container – Виртуальный контейнер

VC-n – Virtual Container of level n – Виртуальный контейнер уровня n (n=12, 2,3,4)

VDSL – Very High Bit Rate Digital Subscriber Line – Цифровая абонентская линия с очень высокой скоростью передачи битов
VoIP – Voice over IP – передача голоса по протоколу IP
VPN – Virtual Privet Network – виртуальная частная (выделенная) сеть
X.25 – Сеть передачи данных по протоколу X.25
X-adapter – X-adapter – Адаптер интерфейса X
WAN - Wide Area Network – глобальная вычислительная сеть (или сеть связи)
WS – Working Station – Рабочая станция
WSF – Working Station Function – Функция рабочей станция
АК – Абонентский комплект
АМТСЭ – Автоматическая междугородная телефонная станция электронная
АСУ – Автоматизированная система управления (сетью связи)
АТС – Автоматическая телефонная станция
АТСЭ – Автоматическая телефонная станция электронная
БД – База данных
ВСС РФ – Взаимоувязанная сеть связи Российской Федерации
ЗИП – Запасные инструменты и приборы
ИТСУ – Информационно–технологическая система управления
ИСО – Международная организация по стандартизации
ГОСТ – Государственный стандарт
ГОСТ Р – Государственный стандарт России
ЛВС – Локальная вычислительная сеть (LAN)
ЛОНИИС – ФГУП «Ленинградский отраслевой научно-исследовательсткий институт связи»
МРК – Межрегиональная компания связи (укрупнённый оператор связи, всего на момент подготовки учебного пособия имеется 7 МРК)
МСЭ – Международный союз электросвязи
МСЭ-Т – Сектор стандартизации электросвязи МСЭ
МЭК – Международная электротехническая комиссия, IEC
НСД – Несанкционированный доступ (к данным, к оборудованию)
ПО – Программное обеспечение
ПЭВМ – Персональная электронно-вычислительная машина
РД – Руководящий документ
СУБД – Система управления базами данных
СУЭС – Сеть управления электросвязью
СУС – Система управления сетями (связи)
ТЦУ – Территориальный центр управления
ТФОП –Телефонная сеть связи общего пользования (также ТфСОП).

ТЭЗ - Типовой элемент замены
УПАТС – Учрежденческо-производственная АТС
УС – Устройства сопряжения
УЦУ – Узловой центр управления
ЦСИС – Цифровая сеть с интеграцией служб
ЦНИИС – Центральный научно-исследовательский институт связи
ЦТЭ – Центр технической эксплуатации
ЦУ, ЦУС – Центр управления (сетями) электросвязи
ЦУ-З – Центр управления оператора зонового уровня
ЦУ-М – Центр управления оператора местного уровня
ЦУ-Ф – Центр управления оператора федерального уровня
ЦУ-ЭС – Центр управления элементами сети
ЧС – Чрезвычайная ситуация
ЭВМ – Электронно-вычислительная машина

ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ МСЭ ПО СЕТЕВОМУ УПРАВЛЕНИЮ И ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ

Список составлен по данным официального сайта МСЭ http://www.itu.int/rec/recommendation. В список не включены технические коррекции рекомендаций с момента публикации

Рекомендации серии M

ITU–T Recommendation M.3010. Principles for a telecommunications management network. – 2000. [Принципы сети управления электросвязью]

ITU–T Recommendation M.3016. TMN security overview. – 1998. [Обзор безопасности сети TMN]

ITU–T Recommendation M.3020. TMN interface specification methodology. – 2000. [Методология спецификации интерфейсов TMN]

ITU–T Recommendation M.3030. Telecommunications Markup Language (tML) Framework. – 2002. [Общие правила языка разметок для телекоммуникаций]

ITU–T Recommendation M.3100. Generic network information model. – 1995. [Основная информационная модель сети]

ITU–T Recommendation M.3120. CORBA generic network and network element level information model. – 2001. [Основы сети CORBA и уровень информационной модели элемента сети]

ITU–T Recommendation M.3200. TMN management services and telecommunications managed areas: overview. – 1997. [Обзор услуг управления TMN и областей/сфер управления]

ITU-T Recommendation M.3207.1 TMN management service: maintenance aspects of B-ISDN management. – 1996. [Управление широкополосной ЦСИС]

ITU-T Recommendation M.3208.1 TMN management services for dedicated and reconfigurable circuits network : Leased circuit services. – 1997. [Услуги управления TMN для сетей из физических цепей с возможностью переключения. Услуги аренды выделенных линий]

ITU-T Recommendation M.3208.2 TMN management services for dedicated and reconfigurable circuits network : Connection management of pre-provisioned service link connections to form a leased circuit service. - 1999 [Услуги управления TMN для сетей из физических цепей с возможностью переключения. Управление соединением для услуг, предоставляемых с помощью линий подключения в форме аренды выделенных линий]

ITU-T Recommendation M.3208.3 TMN management services for dedicated and reconfigurable circuits network : Virtual private network. – 2000. [Услуги управления TMN для сетей из физических цепей с возможностью переключения. Виртуальные частные сети]

ITU-T Recommendation M.3210.1 TMN management services for IMT-2000 security management. – 2001. [Услуги управления TMN для управления безопасностью сетей IMT–2000]

ITU-T Recommendation M.3211.1 TMN management service: Fault and performance management of the ISDN access. – 1996. [Услуги управления TMN. Управление последствиями отказов и управление рабочими характеристиками доступа ЦСИС]

ITU–T Recommendation M.3320. Management requirements framework for the TMN X-Interface. – 1997. [Общая схема требований к управлению для X–интерфейса TMN]

ITU–T Recommendation M.3300. TMN F–interface requirements. – 1998.[Требования к F–интерфейсу TMN]

ITU–T Recommendation M.3400. TMN management functions. – 2000. [Функции управления TMN]

ITU–T Recommendation M.3600. Principles for the management of ISDNs. – 1992. [Принципы управления ЦСИС]

ITU–T Recommendation M.4100. Maintenance of common channel Signalling System No. 7. – 1996. [Техническое обслуживание ОКС№7]

Рекомендации серии Q

ITU-T Recommendation Q.811. Lower layer protocol profiles for the Q3 and X interfaces. – 1997. [Профиль протокола низкого уровня для интерфейсов Q3 и X интерфейса]

ITU-T Recommendation Q.812. Upper layer protocol profiles for the Q3 and X interfaces – 1997. [Профиль протокола высокого уровня для интерфейсов Q3 и X интерфейса]

ITU-T Recommendation Q.816 CORBA-based TMN services. – 2001. [Услуги управления TMN, основанные на CORBA].

ITU-T Recommendation Q.821. Stage 2 and Stage 3 description for the Q3 interface - Alarm Surveillance. – 2000. [Стадия 2 и стадия 3 описания интерфейса Q3. Контроль неисправностей/отказов]

ITU-T Recommendation Q.821.1 CORBA-based TMN alarm surveillance service. – 2001. [Услуги TMN по контролю за неисправностями, основанные на CORBA]

ITU-T Recommendation Q.825 Specification of TMN applications at the Q3 interface: Call detail recording. – 1998. [Спецификации приложений TMN на интерфейсе Q3. Детальная запись о соединении]

Рекомендации серии X.

ITU–T Recommendation X.200. Information technology – Open systems interconnection – Basic reference model: The basic model. – 1994. [Информационные технологии. Взаимосвязь открытых систем. Базовая модель]

ITU–T Recommendation X.650. Information technology - Open Systems Interconnection - Basic Reference Model: Naming and addressing. – 1996. [Информационные технологии. Взаимосвязь открытых систем. Базовая модель взаимосвязи : именование и адресация]

ITU–T Recommendation X.680. Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation. – 2002. (pre-published) [Информационные технологии. Абстрактная запись синтаксиса №1.Спецификация базовых обозначений].

ITU–T Recommendation X.700. Management framework for open system interconnection (OSI) for CCITT applications. – 1992. [Правила управления взаимосвязанных открытых систем для телекоммуникационных приложений]

ITU–T Recommendation X.701. Information technology. Open systems interconnection. Systems Management overview. – 1992. [Информационные технологии. Взаимосвязь открытых систем. Обзор управления системами]

ITU–T Recommendation X.710. Information technology - Open Systems Interconnection - Common Management Information Service. – 1997. [Информационные технологии. Взаимосвязь открытых систем. Услуги общей информации управления]

ITU–T Recommendation X.711. Information technology - Open Systems Interconnection - Common Management Information Protocol: Specification. – 1997. [Информационные технологии. Взаимосвязь открытых систем. Спецификации общего протокола информации управления]

ITU-T Recommendation X.720. Information technology - Open Systems Interconnection - Structure of management information: Management information model. – 1992. [Информационные технологии. Взаимосвязь открытых систем. Структура информации управления: информационная модель управления]

ITU-T Recommendation X.722. Information technology - Open Systems Interconnection - Structure of Management Information: Guidelines for the definition of managed objects. – 1996. Информационные технологии. Взаимосвязь открытых систем. Структура информации управления: руководство по определению объектов управления]

ITU–T Recommendation X.901. Information technology - Open distributed processing - Reference Model: Overview. – 1997. [Информационные технологии. Открытая распределённая обработка. Обзор модели взаимодействия]

Рекомендации серии Y

ITU–T Recommendation Y.110. Global Information Infrastructure principles and framework architecture. – 1998. [Принципы и правила архитектуры Глобальной информационной инфраструктуры]

ПРИЛОЖЕНИЕ Б. ОЦЕНКА ПОКАЗАТЕЛЕЙ НАДЁЖНОСТИ ФУНКЦИОНИРОВАНИЯ ОБОРУДОВАНИЯ АТСЭ (АМТСЭ)

Материалы приложения Б подготовлены на основании монографии «Надёжность и техническое обслуживание АМТС с программным управлением» Справ. пособие/Р.Р. Вегенер и др.; Под ред. В.Г. Дедоборща и Н.Б. Суторихина. – М.: Радио и связь, 1989. – 320 с.: ил.

Для решения задачи управление неисправностями принципиально важным является своевременное выявление неисправных устройств и средств связи, что связано с общими вопросами надёжности АТСЭ (АМТСЭ).

Под *надёжностью АТСЭ* понимается свойство системы коммутации при заданной интенсивности поступающей телефонной нагрузки и условиях эксплуатации сохранять определённое время значения рабочих характеристик, обеспечивающих выполнение требуемых (паспортных) функций.

К таким функциям можно отнести число установленных соединений, потери при обслуживании вызовов, число отказов при установлении соединения, точность фиксации продолжительности телефонных переговоров и т.п. Основными свойствами, характеризующими надёжность АТСЭ, являются безотказность, ремонтопригодность и материально-техническое обеспечение технического обслуживания, которые составляют комплексное свойство оперативной готовности и долговечность. При оценке влияния отказов коммутационного оборудования на качество обслуживания вызовов выделяют следующую ситуацию. Пусть в результате отказа устройство сразу же блокируется и до момента окончания восстановления оно не доступно для поступающих вызовов. Это возможно только в случае, если отказ обнаруживается сразу после его возникновения, т.е. при непрерывном контроле технического состояния оборудования.

К непрерывному контролю приближенно можно также отнести периодический контроль с малым периодом (длительность интервала между моментами контроля не превосходит нескольких секунд). Периодический контроль может осуществляться через равные промежутки времени (постоянный период) и через случайные промежутки времени. Если ин-

тервалы между моментами контроля случайны, то предполагается, что они независимы и распределены экспоненциально. Соответствующие формулы для расчёта показателей надёжности устройств сведены в таблицы Б.1 – Б.3. Используются следующие обозначения:

$T_о$ – среднее время пребывания устройства в неработоспособном состоянии;

$T_н$ – среднее время пребывания неработоспособного устройства в незаблокированном состоянии;

$T_б$ – среднее время пребывания устройства в заблокированном состоянии;

β – доля отказов, не обнаруживаемых непрерывным контролем;

$\beta_н$ – условная вероятность ошибки второго рода (пропуск ошибки) непрерывного контроля при условии отказа объекта контроля;

ω – параметр потока отказов устройства;

μ^{-1} – среднее время восстановления;

η^{-1} – средняя длительность периода для достоверного контроля;

τ - длительность постоянного периода контроля;

$\tau_о$ - интервал между моментами сигнала таймера;

N - общее число основных устройств данного вида;

$N_{зип}$ - объём ЗИП для устройств данного вида оборудования;

$P\{D\}$ - вероятность того, что в ЗИП имеется хотя бы одно устройство данного вида;

$t_{зам}$ - среднее время замены отказавшего устройства.

Таблица Б.1 – Формулы для расчёта показателей надёжности одиночного нерезервированного устройства при достоверном периодическом контроле с экспоненциально распределённым периодом

Функциональное состояние объекта контроля во время проверки	Показатель надёжности	Формула для расчёта
Объект функционирует	$T_о$	$1/\omega$
Объект функционирует	$T_н$	$1/\eta$
Объект функционирует	$T_б$	$1/\mu$
Объект функционирует	$P\{\xi \geq t\}$ – вероятность простоя больше t	$\frac{\eta e^{-\mu t} - \mu e^{-\eta t}}{\eta - \mu}$, если $\eta \neq \mu$ $(1+\mu t)\cdot e^{-\mu t}$, если $\eta = \mu$

Таблица Б.2 – Формулы для расчёта показателей надёжности одиночного нерезервированного устройства при различных видах контроля (периодического) с постоянным периодом (объект контроля во время проверки функционирует)

Вид контроля	Формулы для расчёта			Приближённые формулы	Условия применения формул
	$T_о$	$T_н$	$T_б$		
Достоверный	$1/\omega$	$\frac{A(\omega\tau) - (\omega/\mu)^2 A(\mu\tau)}{\omega(1-\omega/\mu)}$	$1/\mu$	$T_н \approx \tau/2$	$\omega\tau << 1$ $\mu\tau << 1$
Достоверный (момент контроля равномерно распределён в интервале между соседними сигналами таймера)	$1/\omega$	–	$1/\mu$	$T_н \approx \frac{7}{12}\tau_0$	$\omega\tau << 1$ $\mu\tau << 1$

Таблица Б.3 – Формулы для расчёта показателей надёжности одиночного

нерезервированного устройства при различных видах комбинированного контроля с экспоненциально распределённым периодом

Вид комбинированного контроля	Функциональное состояние объекта контроля во время периодической проверки	Формулы для расчёта			
		$T_о$	$T_н$	$T_б$	$\eta_{опт}$
Сочетание неполного непрерывного контроля и достоверного периодического контроля	Функционирует	$\frac{1}{\omega}$	$\frac{\beta}{\eta + (1-\beta)\cdot\omega}$	$\frac{1}{\mu}$	–

Среднее время восстановления $T_в=1/\mu$ зависит от принятого способа технического обслуживания, объёма ЗИП и способа восстановления отказавшего устройства. Если требуемое устройство отсутствует в ЗИП, то отказавшее устройство восстанавливается на месте; время восстановления имеет экспоненциальное распределение с параметром μ_1.

Формулы, по которым вычисляются $T_в$ и $P\{D\}$ для перечисленных двух случаев восстановления оборудования с учётом объёма ЗИП, приведены в таблицах Б.4 – Б.5.

Таблица Б.4 – Формула для расчёта среднего времени восстановления $T_в$ нерезервированного устройства с учётом объёма ЗИП

Условие применения формулы	Формула для расчёта $T_в$
ТЭЗ восстанавливаются на месте (для рабочей АТС)	$\frac{1}{\mu_1} - \left(\frac{1}{\mu_1} - t_{зам}\right) P\{D\}$

Таблица Б.5 – Формула для расчёта вероятности $P\{D\}$ наличия в ЗИП хотя бы одного устройства данного вида

Условия применения	Точная формула	Приближённая формула	Условия применения приближённых формул
–	$\sum_{k=0}^{N_{зип}-1} \frac{N^k}{k!}\left(\frac{\omega}{\mu_2}\right)^k$ $\sum_{k=0}^{N_{зип}} \frac{N^k}{k!}\left(\frac{\omega}{\mu_2}\right)^k + \sum_{s=1}^{N} \frac{N! N^{N_{зип}}}{(N-s)!(N_{зип}+s)!}\left(\frac{\omega}{\mu_2}\right)^{N_{зип}+s}$	–	–
$N_{зип}=1$	$\left[\frac{1}{N+1} + \frac{N}{N+1}\left(1+\frac{\omega}{\mu_2}\right)^{N+1}\right]^{-1}$	$1-N\omega/\mu$	$\frac{N\omega}{\mu} << 1$
$N_{зип}=2$	$\frac{1+\frac{N\omega}{\mu_2}}{1+\frac{N\omega}{(N+1)\mu} + \frac{N^2}{(N+1)(N+2)}\left[\left(1+\frac{\omega}{\mu_2}\right)^{N+2}-1\right]}$	$1-\frac{1}{2}\left(\frac{N\omega}{\mu}\right)^2$	$\left(\frac{N\omega}{\mu}\right)^2 << 1$

Для применения формул в таблицах Б.1 – Б.5 требуются паспортные или статистические данные по отказам на оборудовании связи.

Гребешков Александр Юрьевич

Управление сетями электросвязи по стандарту TMN

Учебное пособие

Издательская лицензия №010164 от 29.01.97 г.
Издательство «Радио и связь»
127473, Москва, 2-й Щемиловский пер., д. 4/5, стр. 1

ИБ № 3140

Подписано в печать 11.02.2004.
Формат 60x84/16 Бумага офсетная. Печать оперативная.
Объём 9,06 усл. печ.л. Тираж 200 экз. Заказ 282.

Отпечатано в типографии ООО «Офорт»,
443068, Самара, ул. Межевая 7.
Лицензия ПД 7-0050 от 30.08.2000 г.