Макаренко С.И.

ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ И ТЕЛЕКОММУНИКАЦИЙ

Учебное пособие

Санкт-Петербург
Наукоемкие технологии
2024

Макаренко С. И.

ЗАЩИТА КОМПЬЮТЕРНЫХ СЕТЕЙ И ТЕЛЕКОММУНИКАЦИЙ

Учебное пособие

Санкт-Петербург
Наукоемкие технологии
2024

УДК 004.7
ББК 32.973
М15

Рецензенты:

***Михаил Викторович Буйневич**, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета Государственной противопожарной службы Министерства чрезвычайных ситуаций России;*

***Роман Леонидович Михайлов**, доктор технических наук, доцент, научно-педагогический сотрудник Военного университета радиоэлектроники.*

М15 Макаренко С. И.
Защита компьютерных сетей и телекоммуникаций. Учебное пособие. – СПб.: Наукоемкие технологии, 2024. – 311 с.

ISBN 978-5-907618-79-4

Учебное пособие, содержит материал по дисциплине «Защита компьютерных сетей и телекоммуникаций», преподаваемой по специальности «Компьютерная безопасность» со специализацией «Информационная безопасность объектов информации на базе компьютерных систем». Учебное пособие учитывает требования государственного образовательного стандарта, и содержательно соответствует отдельным лекциям и темам, изучаемым в рамках вышеуказанной дисциплины.

В первой части пособия подробно рассматриваются организация систем связи, компьютерные и телекоммуникационные сети. Особое внимание уделено сетевым протоколам и современным технологиям транспортных сетей, сетей абонентского доступа и технологиям мобильной связи. Вторая часть пособия посвящена обеспечению информационной безопасности в телекоммуникационных сетях. Подробно рассмотрены типовые средства и способы атак на компьютерные сети, варианты защиты и обеспечения информационной безопасности.

Учебное пособие обсуждено и одобрено на заседании кафедры «Информационная безопасность» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина).
Протокол заседания кафедры № 8 от 05.10.2023 г.

ISBN 978-5-907618-79-4

Оглавление

Предисловие

Учебное пособие, содержит материал по дисциплине «Защита компьютерных сетей и телекоммуникаций», преподаваемой в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» имени В.И. Ульянова (Ленина) по специальности «Компьютерная безопасность» со специализацией «Информационная безопасность объектов информации на базе компьютерных систем». Учебное пособие учитывает требования государственного образовательного стандарта и содержательно соответствует отдельным лекциям и темам, изучаемым в рамках вышеуказанной дисциплины.

Учебное пособие является развитием ранее изданных учебных работ автора [1-7, 69] по системам связи и информационной безопасности (ИБ), изданных по итогам ведения автором соответствующих дисциплин в Ставропольском высшем военном авиационном инженерном училище, в Ставропольском филиале Московского государственного гуманитарного университета имени М.А. Шолохова, в ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», в Военно-космической академии имени А.Ф. Можайского.

В части I пособия (главы 1-9) подробно рассматриваются организация систем связи, компьютерные и телекоммуникационные сети. Особое внимание уделено сетевым протоколам и современным технологиям транспортных сетей, сетей абонентского доступа и технологиям мобильной связи.

В части II (главы 10-13) рассматривается обеспечение ИБ в телекоммуникационных системах (ТКС). Подробно рассмотрены типовые средства и способы атак на компьютерные сети, варианты защиты и обеспечения информационной безопасности.

В основу глав учебного пособия положен материал следующих источников:

- глава 1 «Основные понятия и определения теории систем связи» – работы [1, 3, 5, 8];
- глава 2 «Построение компьютерных сетей и телекоммуникационных систем в соответствии с моделью OSI» – работы [1, 5, 12];
- глава 3 «Физические среды и каналы связи» – работы [1, 14];
- глава 4 «Технологии проводных компьютерных сетей» – работы [1, 12, 14];
- глава 5 «Технологии беспроводных сетей передачи данных» – работа [1, 14, 15];
- глава 6 «Организация информационного обмена между сетями» – работы [12, 14, 16];
- глава 7 «Обеспечение качества обслуживания при межсетевом обмене» – работы [14, 17, 18];
- глава 8 «Транспортные телекоммуникационные сети» – работы [1, 14, 19-23];

– глава 9 «Сети и системы абонентского доступа» – работы [1, 5, 24-47];
– глава 10 «Типовые информационно-технические воздействия на телекоммуникационные сети» – работы [48-53, 55, 69];
– глава 11 «Механизмы реализации удаленных атак в глобальной сети Интернет» – работы [51-55, 69];
– глава 12 «Обеспечение безопасности систем, входящих в состав телекоммуникационных сетей» – работы [52, 55-62, 69].

Следует отметить, что в материалах учебного пособия нашли отражение некоторые отдельные результаты научно-исследовательской работы автора по исследованию качества функционирования систем связи в условиях преднамеренных дестабилизирующих воздействий, а также вопросов обеспечения ИБ ТКС [63-68, 70-74].

Автор признателен рецензентам за их кропотливый труд и доброжелательный критичный подход к оценке содержания учебного пособия, за ценные замечания и предложения по формированию его структуры, способствовавшие выработке единого подхода к рассмотрению вопросов рассматриваемой предметной области.

Предложения и замечания по учебному пособию автор просит направлять Макаренко С.И. на email: mak-serg@yandex.ru.

ЧАСТЬ I. КОМПЬЮТЕРНЫЕ СЕТИ И ТЕЛЕКОММУНИКАЦИИ

1. Основные понятия и определения теории систем связи

1.1. Основные термины и определения в области систем связи

Для конкретизации понятий, рассматриваемых в данной работе, введем базовые определения.

В настоящее время в нормативно-правовых документах введены следующие термины.

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи [9].

Электросвязь – любое излучение, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам [9].

Сеть электросвязи – сеть связи, обеспечивающая электросвязь при помощи электромагнитных систем. Сеть электросвязи состоит из сетей следующих категорий: сети связи общего пользования; выделенные сети связи; технологические сети связи, присоединенные к сети связи общего пользования; сети связи специального назначения и другие сети связи для передачи информации. Таким образом, сеть электросвязи фактически представляет собой объединение отдельных категорий сетей, которые классифицируются по их предназначению [9].

Сеть связи специального назначения (СС СН) – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [9].

При этом для обеспечения функционирования сети связи специального назначения могут использоваться как ее собственные ресурсы, так и ресурсы сетей связи общего пользования.

Сеть связи общего пользования (СС ОП) – комплекс взаимодействующих сетей связи, обеспечивающих электросвязь, в том числе – трансляцию телеканалов или радиоканалов, предназначенных для возмездного оказания услуг связи любому пользователю. При этом сети связи общего пользования могут иметь присоединение к аналогичным системам связи иностранных государств [9].

Сети связи включают в себя первичные и вторичные сети.

Первичная (*транспортная*) *сеть связи* – совокупность технических средств, комплексов, линий связи и обслуживающего персонала, обеспечивающая потребителей стандартными каналами (трактами) передачи первичных электрических сигналов. Основным видом сервиса, предоставляе-

мого абонентам первичных сетей связи, являются типовые каналы и тракты [2].

Вторичная сеть связи (*сеть абонентского доступа*) – совокупность технических средств и связей между ними, обеспечивающая потребителей различными видами услуг по доставке, хранению и обработке информации. Основным видом сервиса, предоставляемого абонентам вторичных сетей, являются услуги по информационному обмену [2].

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

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

Информационно-телекоммуникационной сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [10].

Как видно из вышеуказанных определений, существующие документы делают основной упор на сети, как физико-логические территориально-распределенные структуры, объединяющие узлы и каналы связи. Данный подход соответствует восприятию функций системы связи преимущественно на сетевом уровне, а когда речь идет об услугах связи – на прикладном уровне модели OSI (модель OSI будет подробно изложена в следующей главе). Трактовка понятия «система связи» является более широким и подразумевает включение в себя не только технических объектов и функций на всех уровнях модели OSI, но и организационных структур, осуществляющих проектирование, развертывание, сопряжение со смежными системами (системами управления, навигации, единого времени и т.д.), а также эксплуатацию технических средств связи.

Таким образом, в самом общем, виде термин «система связи» может быть определен следующим образом.

Система связи (СС) – это совокупность распределенных в пространстве взаимосвязанных технических средств и обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена.

С точки зрения теории систем СС может быть отнесена к типу ненаправленных управляемых человеко-машинных систем, которая, как правило, функционирует в интересах одной или нескольких систем управления.

По отношению к системам связи, довольно часто используют понятия «телекоммуникационная система» и «компьютерная сеть». Телеком-

муникационная система в большинстве случаев ассоциируется с отдельной первичной (транспортной) сетью, которая соответствует отдельной области маршрутизации в составе системы связи. А компьютерная сеть – с отдельной изолированной локальной сетью или сетью абонентского доступа с отдельным подключением к транспортной сети. Таким образом, можно утверждать, что термины «телекоммуникационная система» и «компьютерная сеть» относится к понятию «система связи», как частое к общему.

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

Компьютерная сеть – совокупность компьютерных систем, объединенных каналами передачи данных, обеспечивающие эффективное предоставление различных информационно-вычислительных услуг пользователям.

1.2. Состав системы связи

По транспортным средствам, используемым для доставки информации в составе СС, различают [2]:

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

Каналы и тракты транспортных сетей связи в современных СС создаются на базе линий и сетей различных родов связи, входящих в состав первичной (транспортной) сети. При этом под *родом связи* понимается классификационная группировка связи, выделенная по среде распространения сигналов или по применяемым средствам связи.

По видам обеспечиваемого для абонентов сервиса и услуг связи сети электросвязи обычно подразделяют на [8]:

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

Классификация элементов сетей первичной и вторичной сетей СС СН представлена на рис. 1.1.

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

Основой построения первичных (транспортных) сетей в составе СС в настоящее время являются [8]:

- линии и сети радиосвязи;

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

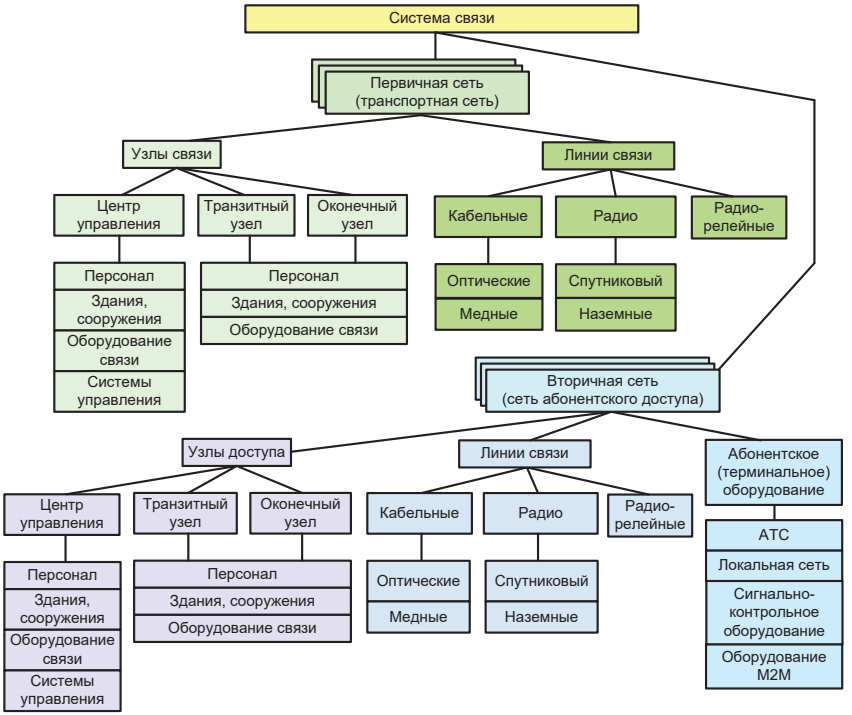


Рис. 1.1. Классификация элементов СС [8]

К основным технологиям первичных (транспортных) сетей в составе современных СС можно отнести [8]:

– технологии коммутации каналов – PDH, SDH, OTH;
– технологии коммутации пакетов – IPv4, IPv6;
– технологии коммутации пакетов по виртуальным каналам – X.25, AX.25, ATM, IP/MPLS, VPN и др.;
– технологии организации, управления и интеграции сетей связи – TMN, ASON/ASTN, NGN и др.;
– специализированные технологии, разработанные для обеспечения связи в условиях преднамеренного воздействия дестабилизирующих факторов на СС.

Вторичные сети СС обычно подразделяли по видам предоставляемых ими услуг, однако в настоящее время такая классификация устарела.

В соответствии со современными взглядами, вторичные сети можно подразделить по типу [5]:

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

В основу более подробной классификации вторичных сетей (сетей абонентского доступа) может быть положена используемая в ней базовая технология сети – рис. 1.2.

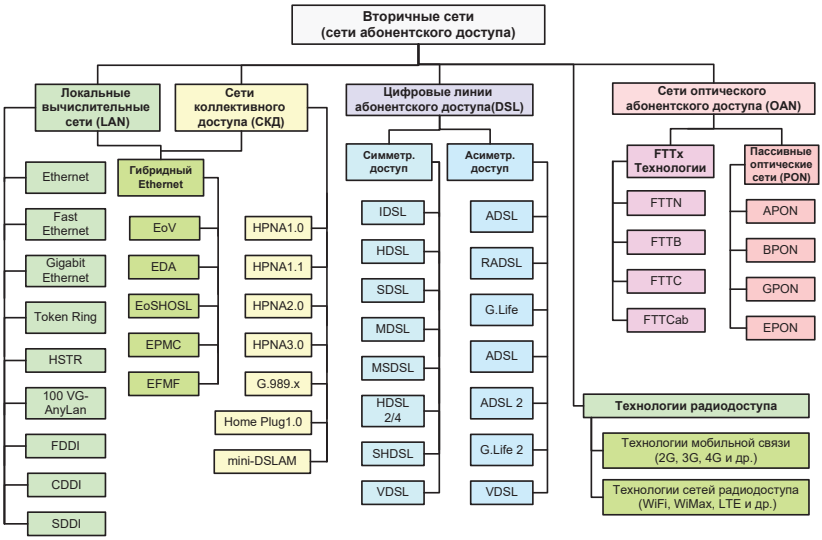


Рис. 1.2. Классификация вторичных СС
по используемой технологии связи [5]

По способам предоставления абонентам сервисов и услуг связи в СС различают [2]:

– сети с закрепленным ресурсом;
– сети с ресурсом по требованию;
– сети с адаптивным распределением ресурса.

Под ресурсом, как правило, если не указывается иное, понимается пропускная способность сети.

Пропускная способность сети – максимально возможная суммарная скорость передачи сообщений по всем информационным направлениям связи для конкретных условий функционирования. Довольно часто пропускную способность сети оценивают числом типовых каналов на направлениях связи, которые могут быть предоставлены абонентам [8].

При этом под типовым каналом, как правило, понимают *основной цифровой канал* (ОЦК) – цифровой канал связи со скоростью 64 кбит/с, позволяющий передавать оцифрованные с достаточным качеством голосовые сообщения в диапазоне 0,3-3,4 кГц.

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

Ресурс сети – совокупность канальных, временных, частотных, энергетических и других ресурсов сети связи, затрачиваемых на передачу информации всех абонентов сети [8].

1.3. Основные требования, предъявляемые к системе связи

1.3.1. Основные понятия теории эффективности

Предъявление требований к связи, системам, сетям, комплексам и средствам связи является сложным процессом и основывается на теории эффективности. Объектом исследования теории эффективности являются системы и процессы оценки эффективности, а предметом исследования – закономерности создания, функционирования и развития систем и процессов оценки эффективности. Оценка эффективности связи и системы связи связана с такими понятиями как: свойство, характеристика, показатель, критерий, требование. Рассмотрим эти понятия.

Свойство – та сторона предмета (объекта, процесса), которая обуславливает его различие или общность с другими предметами (объектами, процессами) или обнаруживается в его отношении с ними. Каждый предмет, объект или процесс имеет основные и второстепенные свойства.

Характеристика – описание отличительных качественных свойств чего-либо или кого-либо. Характеристика может быть качественной или количественной. Для качественной характеристики систем и процессов используют понятия «лучше» или «хуже». Количественные характеристики часто называют *параметрами*. Для оценки эффективности процесса связи чаще пользуются понятием показателя эффективности.

Показатель эффективности (или просто *показатель*) – характеристика, функция характеристик или правило, выбранное для оценки некоторого свойства объекта или совокупности его свойств. Показатели разделяют на количественные и качественные. Пример: своевременность связи может оцениваться такими показателями как вероятность своевременной передачи сообщений и среднее время пребывания сообщения в канале связи.

Количественные показатели выражаются в виде функции от параметров объекта и определяют абсолютную или относительную (доля, часть) числовую меру проявления свойства или совокупности свойств.

Качественные или порядковые показатели оперируют понятиями какой-либо установленной шкалы суждений, отражающей количественные предпочтения (типа: хуже, лучше, больше, меньше и т. п.), либо бальной шкалы или шкалы весовых коэффициентов.

Оценка эффективности процесса связи напрямую связана с ответом на вопрос: «в какой степени достигнута требуемая эффективность?» Для ответа на этот вопрос используют понятие критерия.

Критерий (*эффективности*) – это признак, правило, мера суждения, на основании которых проводится оценка или классификация чего-либо. Критерий может быть абсолютным или относительным.

Абсолютный критерий выражает предельную меру достигаемого эффекта для сравнительной оценки возможных альтернативных решений.

Относительный критерий – норма оценки показателя для достижения требуемой эффективности. Практика показывает, что не всегда экономически целесообразно достигать максимальных или оптимальных критериальных значений. В таких случаях устанавливают целесообразную величину требований к показателям.

Требование – это установленный количественный уровень значения характеристики или показателя оцениваемого объекта, либо высказывательная форма, устанавливающая его качественное соответствие поставленным целям или решаемым задачам.

1.3.2. Требования к вышестоящим информационно-управляющим системам

Как правило СС функционируют не сами по себе, а в интересах вышестоящих систем управления, информационно-управляющих систем (ИУС) или пользователей. При этом к вышестоящим ИУС предъявляются требования по [8]:

- *устойчивости* – способности органов управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях помех и массированных дестабилизирующих воздействиях противника;
- *непрерывности* – возможности органов управления постоянно взаимодействовать с объектами управления;
- *оперативности* – способности органов управления получать, обрабатывать и преобразовывать информацию, а также формировать управляющие воздействия и доводить их до управляемых объектов в соответствии с темпом изменения текущей ситуации;
- *скрытности* – способности сохранять в тайне информацию о процессах управления, конечной цели и решаемых задачах, имеющихся силах и средствах, а также их возможностях; факт, время и место передачи управляющей информации, ее содержание и принадлежность к конкретным объектам системы управления.

1.3.3. Требования к связи и системе связи

Для обеспечения вышеуказанных требований к управлению, к связи, как к процессу переноса информации между органами и объектами управления, предъявляются требования по [8]:

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

Соответственно связь, как процесс переноса информации, должна удовлетворять всем этим требованиям, поэтому было введено интегральное понятие «качество связи».

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

Сообщение – конечный набор данных, содержащий информацию о каком-либо отдельном факте, явлении или событии, который является базовой семантически-неделимой частью процесса передачи информации.

Для обеспечения указанных требований к связи, в свою очередь СС, как организационно-техническая система, должна соответствовать требованиям к определенным ее свойствам. К таким свойствам СС относятся [8]:

- *пропускная способность* – способность системы связи передавать и обрабатывать определенный объем сообщений, пакетов или данных в единицу времени.
- *разведзащищенность* – способность системы связи противостоять всем видам разведки;
- *скрытность* – способность системы связи противостоять раскрытию злоумышленникам факта передачи, содержания передаваемой информации, мест расположения узлов связи, пунктов управления и режимов работы средств связи;
- *криптостойкость* – способность системы связи обеспечивать заданный уровень криптографической защиты и противостоять раскрытию смыслового содержания передаваемой информации;
- *имитостойкость* – способность системы связи противостоять вводу в нее ложной, в том числе и ранее переданной информации и навязыванию ей ложных режимов работы;
- *имитоустойчивость* – способность системы связи обеспечивать требуемый уровень имитостойкости в условиях ввода в нее лож-

ной, в том числе и ранее переданной информации, а также навязыванию ей ложных режимов работы;
- *управляемость* – способность системы связи изменять свое состояние в заданных пределах при воздействии на нее органов управления связью или средств автоматизации управления, в соответствии с изменениями обстановки;
- *готовность* – способность системы связи в любых условиях обстановки в установленные сроки приступить к выполнению задачи по переносу информации с требуемым качеством;
- *мобильность* – способность системы связи в установленные сроки развертываться, свертываться, изменять структуру и место (район) развертывания в соответствии с реально складывающейся обстановкой;
- *устойчивость* – способность системы связи обеспечивать связь с требуемым качеством в условиях дестабилизирующих воздействий естественного и искусственного характера;
- *живучесть* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее обычного и ядерного оружия;
- *помехоустойчивость* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее всех видов помех;
- *помехозащищенность* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее преднамеренных помех;
- *электромагнитная совместимость* – способность системы связи обеспечивать связь с требуемым качеством в условиях воздействия на нее непреднамеренных радиоэлектронных помех и не создавать таких помех другим системам;
- *надежность* – способность системы связи обеспечивать связь с требуемым качеством, сохраняя во времени требуемые значения эксплуатационных показателей, технического обслуживания, восстановления и ремонта;
- *доступность* – способность системы связи обеспечивать своим абонентам возможность организации связи с требуемым качеством при сохранении их приоритетности и способов установления связи между ними.

1.3.4. Требования к системе связи по обеспечению информационной безопасности

В СС при передаче информационных потоков и сообщений должны обеспечиваться требования по информационной безопасности.

Информационная безопасность (ИБ) – это состояние, при котором обеспечивается конфиденциальность, целостность и доступность информации [8].

Конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право [8].

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа к информации, могут реализовывать их беспрепятственно [8].

Целостность информации – состояние информации, при котором обеспечивается ее достоверность и полнота [8].

Полнота информации – состав и объем информации достаточный для правильного понимания какого-либо явления или принятия решения.

Достоверность информации – истинность и точность информации в описании какого-либо факта, события или явления.

Структурно-логическая связь между требованиями к СС и свойствами ИБ представлены на рис. 1.3.

Основной особенностью СС, если ее рассматривать в контексте ИБ, является то, что СС функционирует в условиях воздействия нарушителей (злоумышленников), которые проявляются в виде различного рода дестабилизирующих факторов (рис. 1.4). В связи с этим для СС особенное значение приобретает свойство ее устойчивости.

В стандарте [11] даны следующие определения.

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

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

Таким образом, понятие «фактор», в соответствии со стандартом [11], семантически соответствует понятию «воздействие». Уточняя, что основной функцией СС является обеспечение требуемого качества связи, а также разделяя дестабилизирующие факторы на естественные и искусственные, можно дать следующее определение.

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

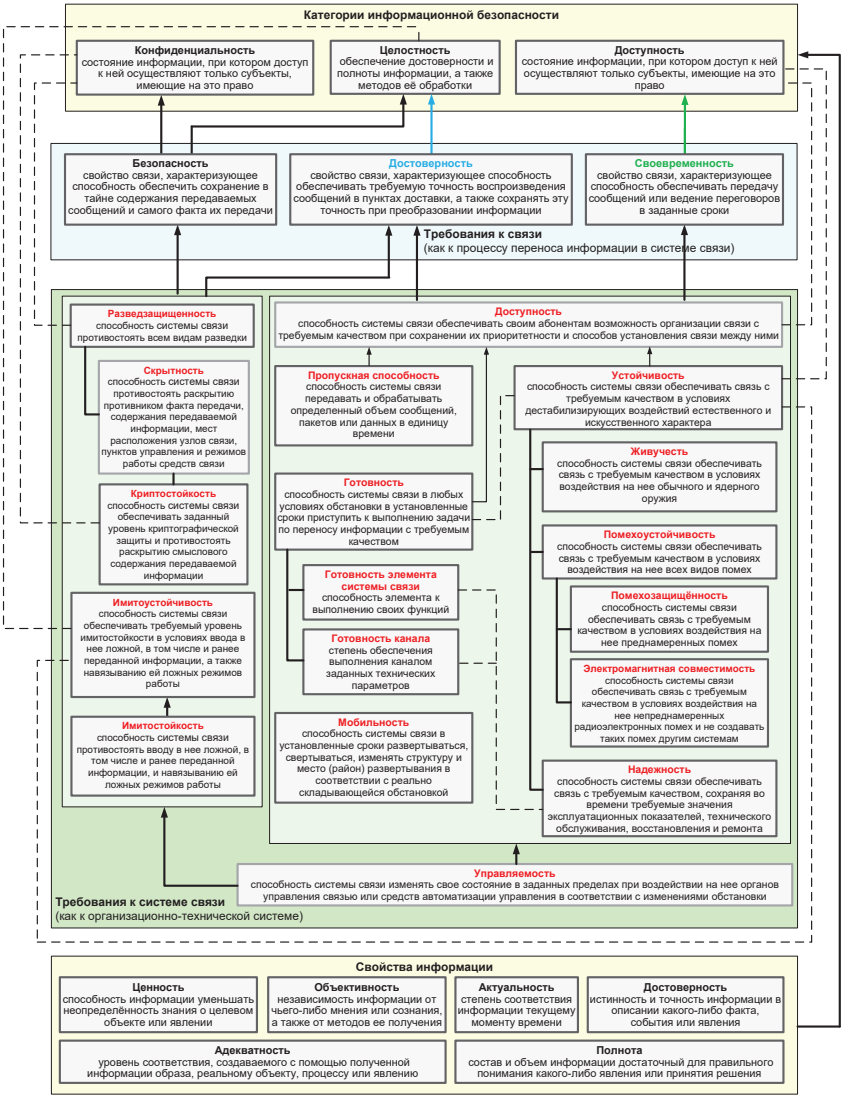


Рис. 1.3. Связь категорий ИБ со свойствами информации и с требованиями, предъявляемыми к СС [8]

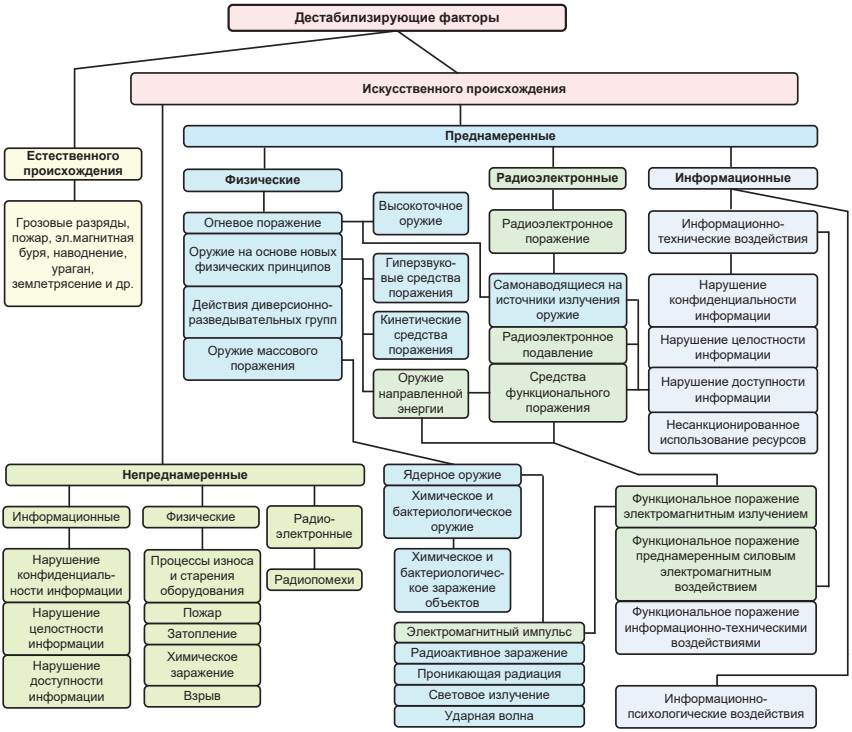


Рис. 1.4. Классификация дестабилизирующих факторов, влияющих на СС [8]

1.4. Канал связи, рода и виды связи

1.4.1. Основные понятия о канале связи

Обобщенная структурная схема одноканальной системы связи представлена на рис. 1.5. Отправителем и получателем сообщения могут выступать как человек, так и различного рода технические устройства, обеспечивающие формирование, регистрацию, хранение и использование сообщений. При этом по своему характеру сообщения могут иметь различную структуру. Сообщения могут быть в виде речи, буквенно-цифрового текста, изображения, цифровых данных и т. д.

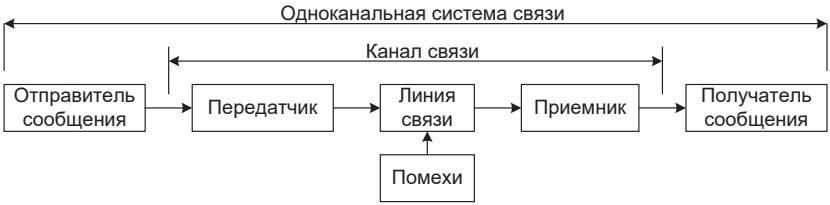


Рис. 1.5. Обобщенная структурная схема
одноканальной системы связи [3]

Совокупность передающего устройства, линии связи и приемного устройства принято называть каналом связи. Отправитель сообщений, канал связи и получатель сообщений образуют систему связи.

Канал связи – совокупность средств связи и среды распространения, обеспечивающая передачу сигналов электросвязи между узлами связи в определенной полосе частот или с определенной скоростью.

Канал связи обеспечивает соединение передатчика и приёмника. Классификация каналов по различным основаниям приведена на рис. 1.6. В настоящее время основными используемыми каналами связи являются цифровые двухсторонние каналы связи для передачи данных.

Рис. 1.6. Классификация каналов связи [3]

Физически канал может быть, как проводной линией, которая пропускает электрический сигнал, так и стекловолокном, которое переносит информацию посредством модулированного светового луча, или радиоэфиром. Данные каналы имеют различные частотные характеристики и полосы рабочих частот (рис. 1.7).

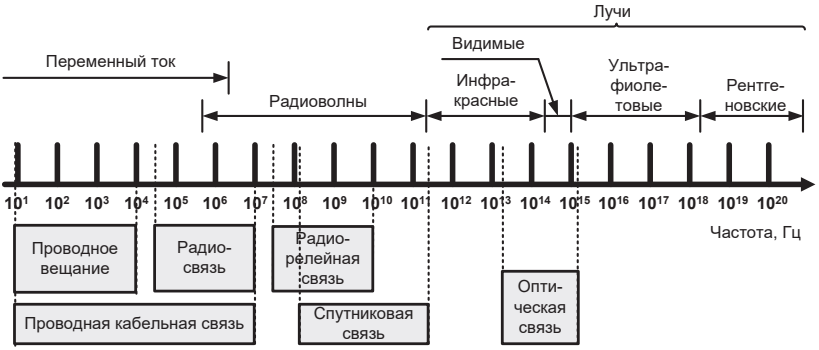


Рис. 1.7. Частотный диапазон различных каналов связи

Общая проблема при передаче сигнала через любой канал – аддитивный шум. Вообще говоря, аддитивный шум часто создаётся внутри различных электронных компонентов, таких как резисторы и твердотельные устройства, используемые в системах связи. Эти шумы часто называют *тепловым шумом.* Другие источники шума и интерференции (наложения) могут возникать вне системы, например, переходные помехи от других пользователей канала. Когда такой шум и переходные помехи занимают тот же самый диапазон частот, что и полезный сигнал, их влияние может быть минимизировано путем соответствующего выбора передаваемого сигнала и демодулятора в приемнике.

Еще одним видом сигнальных искажений, которые могут встречаться при передаче сигнала по каналу являются затухание сигнала, амплитудные и фазовые искажения сигнала и искажения сигнала, обусловленные многопутевым распространением волн. Влияние шума может быть уменьшено увеличением мощности передаваемого сигнала. Однако конструктивные и другие практические соображения ограничивают уровень мощности передаваемого сигнала.

Другое базовое ограничение при передаче сигналов – ограниченная доступная ширина полосы частот канала. Ограничение ширины полосы обычно обусловлено физическими ограничениями среды и электрических компонентов, используемых в передатчике и приемнике (рис. 1.5). Эти два обстоятельства приводят к ограничению количества данных, которые могут быть переданы надёжно по любому каналу связи.

1.4.2. Рода связи

Род связи – классификационная группировка связи, выделенная по среде распространения сигналов или по применяемым средствам связи.

Классификация по родам связи приведена на рис. 1.8.

Все рода связи реализуются конкретными средствами связи: радиостанциями, радиорелейными, тропосферными станциями, станциями спутниковой связи, проводными средствами связи, волоконно-оптическими

средствами связи. Эти средства образуют каналы связи: радио-, радиорелейные, тропосферные и т.д. Для каналообразующих средств каждого рода связи установлены условные обозначения, применяемые при разработке документов по связи.

Рассмотрим отдельные рода связи более подробно.

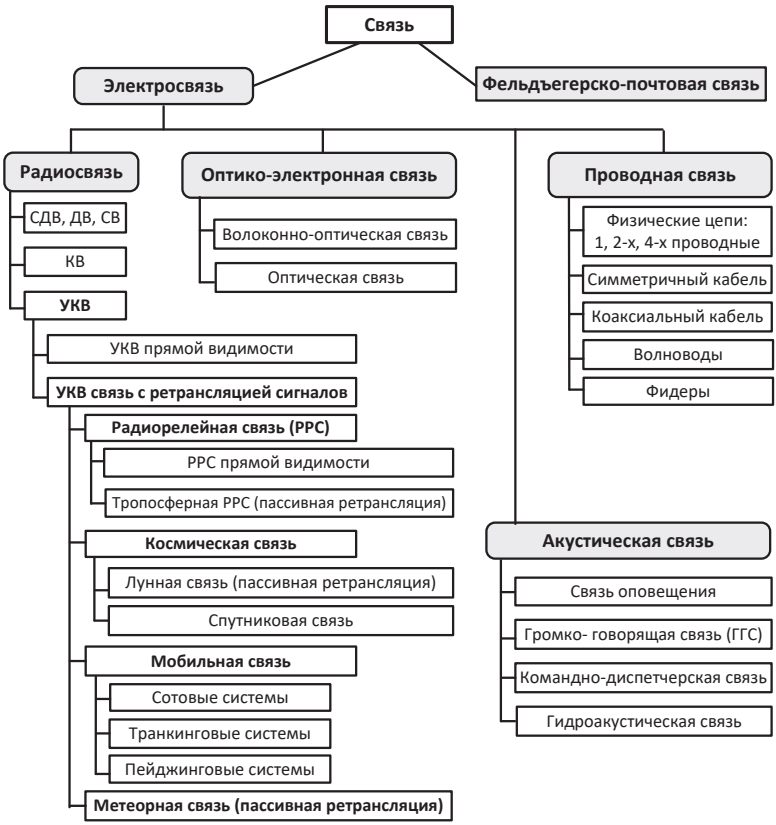


Рис. 1.8. Классификация родов связи [3]

1.4.2.1. Радиосвязь

Радиосвязь – род связи, который реализуется с использованием радиосредств, земных и ионосферных радиоволн [3].

Частными случаями радиосвязи являются радиорелейная и космическая рода связи.

Радиорелейная связь – род связи, который реализуется с использованием радиорелейных средств связи и радиоволн в ультракоротковолновом диапазоне [3].

Частным случаем радиорелейной связи являются тропосферная и спутниковая связь.

Тропосферная связь – это род связи, который реализуется с использованием тропосферных средств связи и физического явления дальнего тропосферного распространения ультракоротких волн (УКВ) [3].

Космическая связь – радиосвязь в интересах абонентов наземного, воздушного и морского базирования, имеющая общие участки распространения радиоволн за пределами ионосферы [3].

Спутниковая связь – частный случай космической связи, когда между абонентами наземного, воздушного или морского базирования связь осуществляется с использованием ретранслятора, размещенного на искусственном спутнике Земли [3].

Рассмотрим особенности радиосвязи при различных вариантах ее организации и при использовании различных диапазонов.

В системах радиосвязи (беспроводной связи) электромагнитная энергия передается в среду распространения антенной, которая служит излучателем. Физические размеры и структура антенны зависят, прежде всего, от рабочей частоты. Чтобы получить эффективное излучение электромагнитной энергии, размеры антенны должны быть больше чем 1/10 длины волны.

Способы распространения электромагнитных волн в атмосфере и в свободном пространстве можно разделить на три категории, а именно:

– распространение поверхностной волной;
– распространение пространственной волной;
– распространение прямой волной.

В диапазоне очень низких частот (ОНЧ) и звуковом диапазоне, в которых длины волн превышают 10 км, Земля и ионосфера образуют волновод для распространения электромагнитных волн.

В этих частотных диапазонах сигналы связи фактически распространяются вокруг всего земного шара. По этой причине эти диапазоны частот во всём мире используются прежде всего для решения навигационных задач при управлении удаленными объектами. Ширина полосы частот канала, доступной в этих диапазонах, относительно мала (обычно составляет 1...10% центральной частоты), и, следовательно, информация, которая передается через эти каналы, имеет относительно низкую скорость передачи и обычно неприемлема для цифровой передачи.

Доминирующий тип шума на этих частотах обусловлен грозовой деятельностью вокруг земного шара, особенно в тропических областях. Интерференция возникает из-за большого числа станций в этих диапазонах частот.

Распространение земной волной, как иллюстрируется на рис. 1.9, является основным видом распространения для сигналов в полосе средних частот (0,3…3 МГц). Это диапазон частот, используемый для радиовещания с амплитудной модуляцией (АМ) и морского радиовещания.

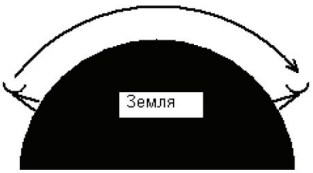


Рис. 1.9. Распространение поверхностной волны

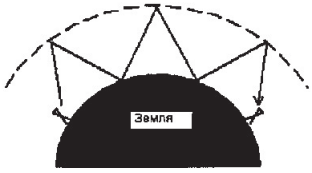


Рис. 1.10. Ионосферное распространение пространственной волны

При радиовещании с использованием амплитудной модуляции и распространении земной волной дальность связи даже при использовании мощных радиостанций ограничена 150 км. Атмосферные шумы, промышленные шумы и тепловые шумы от электронных компонентов приёмника являются основными причинами искажений сигналов, передаваемых в диапазоне средних частот.

Частным случаем распространения пространственной волны является ионосферное распространение, иллюстрируемое рис. 1.10. Оно сводится к отражению (отклонение или рефракция волны) передаваемого сигнала от ионосферы, которая состоит из нескольких слоев заряженных частиц, расположенных на высоте 50...400 км от поверхности Земли. В дневное время суток разогрев нижних слоев атмосферы солнцем обусловливает появление нижнего слоя на высоте ниже 120 км. Эти нижние слои, особенно D-слой, вызывают поглощение частот ниже 2 МГц, таким образом, ограничивая распространение ионосферной волной радиопередач АМ радиовещания.

1.4.2.2. Проводная связь

Проводная связь – связь, осуществляемая по проводным (кабельным) линиям связи [3].

В системах проводной связи электрический сигнал передается по кабельной линии. Средства проводной связи обеспечивают высокое качество каналов, простоту организации связи, относительно большую скрытность по сравнению с радиосвязью, почти не подвержены воздействию преднамеренных помех.

Витые проводные пары и коаксиальный кабель образуют электромагнитный канал, который обеспечивает прохождение электрических сигналов относительно умеренной ширины полосы частот. Так телефонный провод, обычно используемый для соединения абонента с центральной станцией, имеет ширину полосы несколько сотен килогерц. С другой стороны, коаксиальный кабель обычно имеет используемую ширину полосы частот порядка несколько мегагерц.

Сигналы, передаваемые через такие каналы, искажаются по амплитуде и фазе, кроме этого на них накладывается аддитивный шум. Проводная линия связи в виде витой пары также склонна к интерференции переходных

помех от рядом расположенных пар. Поскольку проводные каналы составляют большой процент всех каналов связи, широкие исследования были направлены на определение их свойств передачи и на уменьшение амплитудных и фазовых искажений в канале.

1.4.2.3. Волоконно-оптическая связь

Волоконно-оптическая связь – связь, осуществляемая по волоконно-оптическому кабелю с использованием специальной аппаратуры преобразования электрических сигналов в оптические [3].

Стекловолокно предоставляет проектировщику системы связи ширину полосы частот, которая на несколько порядков больше, чем у кабельных каналов. В течение последнего времени были разработаны оптические кабели, которые имеют относительно низкое затухание для сигнала, и высоконадёжные оптические устройства для генерирования и детектирования сигнала. Эти технологические достижения привели к быстрому освоению таких каналов как для внутренних, так и для трансатлантических и мировых систем связи. С учётом большой ширины полосы частот, доступной на волоконно-оптических каналах, стало возможным предложить абонентам широкий диапазон услуг связи, включая передачу речи, данных, факсимильных и видеосигналов.

Передатчиком или модулятором в волоконно-оптической системе связи является источник света, светоизлучающий диод или лазер. Информация передается путем изменения (модуляции) интенсивности источника света посредством сигнала сообщения. Свет распространяется через волокно как световая волна, которая для компенсации затухания сигнала периодически усиливается (в случае цифровой передачи детектируется и восстанавливается ретрансляторами) вдоль тракта передачи.

В приемнике интенсивность света детектируется фотодиодом, чей выход является электрическим сигналом, который изменяется пропорционально мощности света на входе фотодиода. Источники шума в волоконно-оптических каналах – это фотодиоды и электронные усилители. Предполагается, что в ближайшее время волоконно-оптические каналы вытеснят почти все каналы проводных линий связи в ТКС.

1.4.2.4. Подводные гидроакустические каналы

Электромагнитные волны не распространяются на большие расстояния под водой, за исключением крайне низких частот. Однако организация передачи сигналов на таких низких частот имеет очень высокую стоимость из-за чрезвычайно больших и мощных передатчиков. Затухание электромагнитных волн в воде может быть выражено *глубиной поверхностного слоя* – расстояния, на котором сигнал ослабляется в *e* раз.

Например, для частоты 10 кГц глубина поверхностного слоя 2,5 м. Напротив, акустические сигналы распространяются на расстояния порядка десятков и даже сотен километров.

Подводный акустический канал ведет себя как многопутевой канал благодаря сигнальным отражениям от поверхности и дна моря. Из-за случайного движения волны сигнальные продукты многопутевого (многолучевого) распространения приводят к случайным во времени задержкам распространения и в итоге к замираниям сигнала. Кроме того, имеется частотнозависимое затухание, которое приблизительно пропорционально квадрату частоты сигнала. Глубинная скорость номинально равна приблизительно 1500 м/с, но реальное значение выше или ниже номинального значения в зависимости от глубины, на которой сигнал распространяется. Окружающий океанский акустический шум вызван рыбой. Ближние гавани добавляют к окружающему шуму промышленный шум. Несмотря на эту помеховую окружающую среду, возможно проектировать и выполнять эффективные и безопасные подводные акустические системы связи для передачи цифровых сигналов на большие расстояния.

1.4.3. Виды связи

Одна и та же по содержанию информация может быть представлена сообщениями различного вида: текстом, данными, изображением или речью. В зависимости от способа представления сообщений к удобному для восприятия виду различают виды связи.

Вид связи – это классификационная группировка связи, выделенная по виду передаваемого сообщения, оконечного оборудования или средства связи [3].

При использовании соответствующей оконечной аппаратуры по каналам радио-, радиорелейных, тропосферных, спутниковых, проводных (кабельных) линий связи обеспечиваются следующие *виды связи* [3]:

- сигнальная связь;
- телефонная связь;
- телеграфная связь;
- факсимильная связь;
- передача данных;
- видеотелефонная связь;
- телевизионная связь.

Сигнальная связь – это связь, осуществляемая с помощью заранее определенных зрительных и звуковых сигналов [3].

В настоящее время сигнальная связь используется для управления автомобильным и железнодорожным движением путем применения зрительных (световые ракеты, цветные дымы и др.) и звуковых средств (сирены, свистки и др.).

Телефонная связь – это вид связи, обеспечивающий передачу (прием) речевой информации, переговоры пользователей [3].

Телефонная связь создает условия, близкие к личному общению, поэтому является наиболее удобной в различных звеньях управления. С целью скрытия от содержания телефонных переговоров в каналах связи при-

меняется аппаратура шифрования, засекречивания или устройства технического маскирования речи. В зависимости от применяемой оконечной и специальной аппаратуры телефонная связь может быть открытой, маскированной, засекреченной временной или гарантированной стойкости [3].

Телеграфная связь – вид связи, обеспечивающий обмен телеграммами (краткими текстовыми сообщениями). Кроме того, она предназначается для передачи документальных сообщений в виде шифрограмм, кодограмм [3].

Телеграфная связь может быть буквопечатающей или слуховой, засекреченной или открытой (с применением аппаратуры засекречивания или без ее применения). Телеграммы, несущие важную информацию, могут предварительно шифроваться или кодироваться.

Факсимильная связь – это вид связи, обеспечивающий обмен документальной информацией в цветном и черно-белом изображении. Она предназначается для передачи документов в виде карт, схем, чертежей, рисунков и буквенно-цифровых текстов в черно-белом или цветном изображении [3].

Факсимильная связь представляет большое удобство должностным лицам органов управления, так как на приемном устройстве получается готовый для дальнейшей работы документ с соответствующими подписями и печатями.

Передача данных – это вид связи, обеспечивающий обмен формализованными и неформализованными сообщениями между электронно-вычислительными машинами (ЭВМ), автоматизированными рабочими местами (АРМ) должностных лиц, компьютерными системами [3].

Данные – поддающееся многократной интерпретации представление информации в формализованном знаково-символьном виде, пригодном для формирования, сбора, хранения, передачи, обработки или представления в информационных системах [3].

Телеграфную связь, передачу данных и факсимильную связь принято объединять понятием «*документальная связь*».

Видеотелефонная связь – это вид электросвязи, обеспечивающий переговоры пользователей с одновременной передачей видео и звука в режиме реального времени [3]. Данный вид связи в настоящее время находит широкое применение, не только в различных информационных системах, но и при личном общении.

Телевизионная связь – это вид связи, обеспечивающий передачу видеоинформации в реальном масштабе времени [3].

Подробная информация об особенностях организации телефонной, телевизионной и телеграфной связи изложена в работе [5]. Далее эти типы связи в учебном пособии не рассматриваются, а основное содержание материала будет посвящено основному используемому в настоящее время виду связи – передаче данных.

1.5. Структура сети связи

Система связи представляет собой достаточно сложную совокупность технических и программных средств передачи и распределения информации. Относясь по уровню организации к классу технических систем, она может быть охарактеризована с принятых системологических принципов морфологического и функционального описаний.

Под морфологическим описанием СС понимается описание с точки зрения ее структуры и состава ее элементов [5].

Под функциональным описанием СС понимается описание процессов изменения параметров системы [5].

Если не учитывать взаимодействие элементов СС, ее структуру можно представить как совокупность телекоммуникационных сетей и системы управления.

При этом в узком морфологическом смысле *сеть* есть совокупность *узлов*, в которых происходит распределение информации, ввод/вывод ее в сеть (пользователем или средствами вышестоящей ИУС), и *каналов связи*, обеспечивающих перенос информации между узлами [5].

Структура сети задается графом сети $G(V, U)$, где V – вершины графа, соответствующие узлам, U – дуги (ребра), соответствующие линиям связи между узлами.

Говоря о структуре сети, как правило имеют в виду топологию размещения узлов и абонентов сети, а также характер их взаимосвязи, при этом, отождествляют группу абонентов узла с абонентскими линиями, служащими для ввода-вывода информации, с данным узлом, полагая, что сам узел является источником и потребителем информации. Хотя на самом деле такое упрощение зачастую слишком грубое, о чем свидетельствуют проблемы так называемой «последней мили».

Различают следующие основные топологические структуры сетей (рис. 1.11): полносвязная сеть, радиальная, радиально-узловая, кольцевая. На основе базовых топологических структур может быть построена сеть произвольной структуры.

На основании изложенного выше можно перечислить основные характеристики сети:

- первичность, вторичность сети связи;
- число и структуру уровней иерархии сети;
- число узлов сети;
- число сетевых узлов;
- число коммутационных узлов;
- число линий связи;
- матрица пропускных способностей линий связи;
- матрица емкостей линий связи;
- матрица длин линий связи;
- матрица стоимостей линий связи;
- матрица прямых каналов сети;

– матрица надежности линий связи;
– число и структура зон обслуживания (управления) сети;
– число и структура уровней иерархии системы управления со своими структурными параметрами и др.

В обобщенном виде структурная схема отдельной ТКС приведена на рис. 1.12.

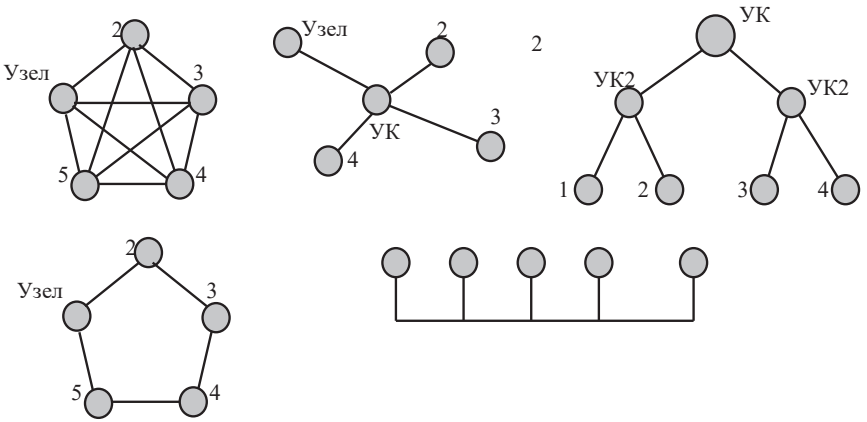


Рис. 1.11. Топологические структуры сетей:
а) полносвязная, б) узловая, в) радиально-узловая, г) кольцевая, д) шина

Рис. 1.12. Структурная схема отдельной ТКС [5]

В сетях с коммутацией каналов различают два вида соединений:
– долговременные – кроссировка каналов;
– оперативные – коммутация каналов.

В зависимости от применяемого на узлах типа коммутации различают:
– некоммутируемые сети;
– коммутируемые сети.

Коммутируемые сети в свою очередь делятся на сети:
– с коммутацией каналов;
– с коммутацией сообщений;
– с коммутацией пакетов.

Линии и каналы связи, инцидентные некоторому узлу, делятся на:

– оконечные (к абонентам данного узла);
– транзитные (образованные с помощью кроссировки);
– коммутируемые.

Для передачи потоков информации между различными парами узлов телекоммуникационной сети образуются *пути*, являющиеся последовательностью узлов и линий, в которых ни один узел не встречается дважды.

Путь характеризуется:

– суммарной длиной составляющих его линий;
– пропускной способностью, равной минимальной пропускной способности составляющих линий;
– надежностными характеристиками.

1.5.1. Узлы связи

Узел связи – организационно-техническое объединение средств и комплексов связи (канального, коммутационного, абонентского и др. оборудования), характеризуемого определенными структурными свойствами и предназначенного для ввода, вывода информации, каналообразования, коммутации каналов связи (сообщений, пакетов) в соответствии с потребностью пользователей (абонентов) сети [5].

В узлах осуществляется формирование путей передачи информации между оконечными пунктами сети. С этой целью на узле предусматривается возможность непосредственного (для сетей с коммутацией каналов) или косвенного, через промежуточную буферную память (для сетей коммутации сообщений или пакетов), соединения между каналами линий связи, инцидентных (смежных) данному узлу.

Основными параметрами узла коммутации, которые влияют на параметры сети в целом, являются [5]:

– пропускная способность $c(i)$, определяющая возможности коммутации в узле i (она зависит от объема коммутационного поля и от процедур управления узлом);
– кроссировочная способность, определяющая максимальный объем кросса через узел;
– надежностные характеристики (вероятность отказа, средняя частота отказа, среднее время восстановления и др.);
– объем буферной памяти (при коммутации сообщений и пакетов);
– стоимость узла;
– параметры системы управления узлом.

1.5.2. Каналы связи в сети

Канал связи в сети – комплекс устройств, обеспечивающих перенос сигналов (передачу информации) из одной точки пространства в другую,

причем полюсами (концами) канала будем считать устройства ввода и вывода информации, либо вход и выход коммутационных систем [5].

Направление связи (пучок каналов) – совокупность каналов между двумя узлами в сети.

Направления и каналы связи в зависимости от того, возможна передача информации в обоих направлениях или только в одном могут быть:

– двусторонними;
– односторонними.

Основными характеристиками канала связи являются [5]:

– *пропускная способность* – максимально возможная скорость передачи информации по каналу (либо полоса пропускания канала);
– *достоверность* – вероятность ошибочного приема элементарного символа (при помехоустойчивом кодировании – вероятность ошибочного приема кодограммы или сообщения);
– *надежность* – вероятность того, что достоверность приема не будет хуже заданной; надежностные характеристики аналогичны характеристикам узла;
– *коэффициент использования оборудования канала*.

Заметим, что в случае составных каналов на их характеристики существенно влияние оказывают характеристики элементов узла.

Основными характеристиками направления связи, как совокупности каналов, являются [5]:

– пропускная способность;
– длина линии;
– стоимость эксплуатации или аренды;
– надежностные характеристики.

Возвращаясь к графовой модели сети, отметим, что вершинам графа приписываются числовые значения характеристик соответствующего узла, а каждому ребру – числовые значения характеристик соответствующего канала.

1.5.3. Управление в сети

Сеть связи предполагает наличие системы управления. Говоря о функциональных характеристиках сети, последнюю нужно рассматривать как сложную систему, функционирующую в двух случайных, взаимозависимых средах, одна из которой определяется поступающей нагрузкой, другая – потоком отказов/восстановлений на элементы сети, формирующим состояние сети.

Описание системы управления можно рассматривать на двух уровнях:

1. уровень средств контроля и управления;
2. уровень функций управления.

Элементами описания первого уровня являются программные и технические средства контроля и управления телекоммуникационной системы

и сеть служебных каналов передачи информации контроля и управления (например, сеть общих каналов сигнализации – ОКС). Первый уровень описания системы представляется в виде взвешенного графа управления $G(У)$, вершинам которого соответствуют средства контроля и управления сети, ребрам – служебные каналы, а веса вершин и ребер определяются техническими и стоимостными характеристиками системы управления. Элементами описания второго уровня являются конкретные функции управления сети.

Основным назначением любой сети связи является обеспечение требуемого качества обслуживания ее абонентов. Обслуживание заключается в реализации их требований на передачу и получение информации. Требования абонентов (потребность в телекоммуникационных услугах) характеризуют потоком заявок на обслуживание. Показатель качества обслуживания выражается либо через интенсивность отказов (частоту отказа в обслуживании поступающих вызовов), либо через среднюю задержку в обслуживании. Отказы и задержка в обслуживании обусловлены ограниченностью ресурсов телекоммуникационной системы. В этом случае особая роль в телекоммуникационных системах отводится управлению.

Управление системой – это процесс формирования эффективного (с точки зрения принятого критерия эффективности) функционирования системы.

Под изменением характера нагрузки обычно понимается как изменение абсолютной величины нагрузки (увеличение или уменьшение среднего числа заявок на обслуживание), так и изменение относительных величин требований на передачу по отдельным направлениям. Как правило, существует детерминированная и случайная составляющие изменения нагрузки. Из общего характера предъявляемой к обслуживанию нагрузки следуют две функции управления телекоммуникационной сетью (рис. 1.13):

– управление нагрузкой, поступающей в сеть;
– управление потоками нагрузки в сети.

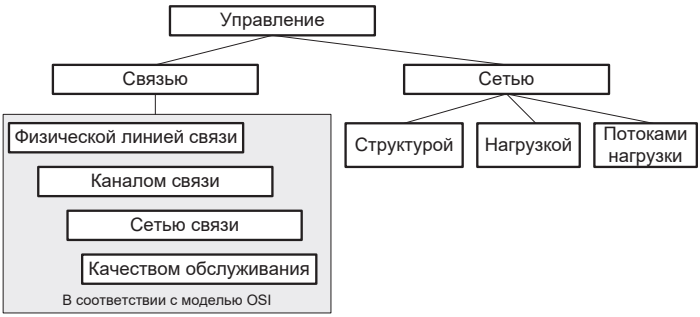


Рис. 1.13. Структура системы управления связью в сети

Следует отметить, что способность сети пропускать предъявляемую нагрузку несущественно зависит от характера распределения потоков информации по сети и определяется лишь общим объемом предъявляемой нагрузки. Из этого факта следует, что первоочередной задачей управления сетью является поддержание величины пропускаемой нагрузки в пределах допустимого уровня, и управление потоками нагрузки эффективно выполняется только при выполнении этого условия. Управление потоками нагрузки в сети осуществляется протоколами маршрутизации.

Возможность поражения или отказа отдельных элементов телекоммуникационной системы и существенного возрастания нагрузок в линиях связи вызывает необходимость в управлении структурой сети.

Управление структурой сети – переход от структуры пораженной или перегруженной сети, не обеспечивающей заданных требований на качество связи, к некоторой другой структуре, удовлетворяющей этим требованиям. Сущность перехода может заключаться в добавлении резервных комплектов канального, коммутационного и абонентского оборудования, в организации транзитов на некоторых узлах для отдельных потоков и др.

Материал главы 1 подготовлен на основе материалов [1, 3, 5, 8].

2. Построение компьютерных сетей и телекоммуникационных систем в соответствии с моделью OSI

2.1. Модель OSI как основа описания взаимодействия абонентов компьютерных сетей и телекоммуникационных систем

На рис. 2.1 показана модель взаимодействия двух узлов ТКС. Процедура взаимодействия узлов может быть описана в виде набора правил взаимодействия каждой пары соответствующих уровней обеих участвующих сторон.

Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются *протоколом* [12].

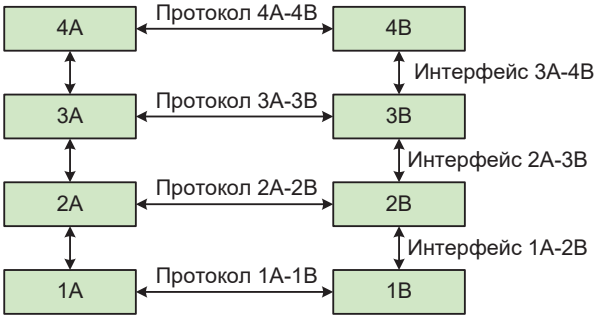


Рис. 2.1. Взаимодействие двух узлов

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *интерфейсом* [12].

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов* [12].

В начале 1980-х годов ряд международных организаций по стандартизации – ISO, ITU-T и некоторые другие – разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется *моделью взаимодействия открытых систем – OSI* (*Open System Interconnection*) [12]. В модели OSI средства взаимодействия делятся на 7 уровней – рис. 2.2. При этом каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой (ОС), системными утилитами, системными аппаратными средствами. Однако при этом модель не включает средства взаимодействия приложений конечных пользователей.

Рис. 2.2. Функции уровней модели OSI, представление данных на различных уровнях, а также соответствие уровням функций различных устройств вычислительной системы

Рассмотрим пример. Пусть приложение обращается с запросом к прикладному уровню, например к файловой службе. На основании этого запроса программное обеспечение (ПО) прикладного уровня формирует сообщение стандартного формата.

Обычное сообщение состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладному уровню машины-адресата, чтобы сообщить ему, какую работу надо выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные, например те, которые необходимо записать в удаленный файл.

После формирования сообщения прикладной уровень направляет его вниз по стеку *представительному уровню*. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию – заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата. Полученное в результате сообщение передается вниз *сеансовому уровню*, который в свою очередь добавляет свой заголовок, и т. д. Наконец, сообщение достигает нижнего, *физического уровня*, который собственно и передает его по линиям связи машине-адресату. К этому моменту сообщение «обрастает» заголовками всех уровней (рис. 2.3).

Когда сообщение по сети поступает на машину-адресат, оно принимается ее физическим уровнем и последовательно перемещается вверх с уровня на уровень.

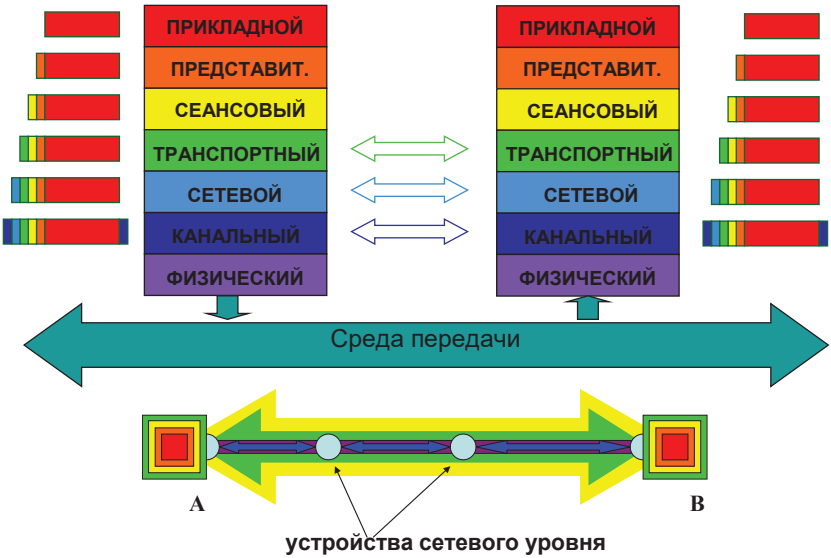


Рис. 2.3. Модель взаимодействия ISO/OSI
в процессе передачи сообщений

Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

Наряду с термином *сообщение* (*message*) существуют и другие термины, применяемые сетевыми специалистами для обозначения единиц данных в процедурах обмена. Для обозначения блоков данных определенных уровней часто используются специальные названия: кадр (frame), пакет (packet), дейтаграмма (datagram), сегмент (segment).

В модели OSI различаются два основных типа протоколов [12]:

1. *протоколы* с *установлением соединения* перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать некоторые параметры протокола, которые они будут использовать при обмене данными. После завершения диалога они должны разорвать это соединение. Телефон – это пример взаимодействия, основанного на установлении соединения;
2. *протоколы без предварительного установления соединения*. Отправитель просто передает сообщение, когда оно готово. Опускание письма в почтовый ящик – это пример связи без предвари-

тельного установления соединения. При взаимодействии компьютеров используются протоколы обоих типов.

2.2. Уровни модели OSI

Рассмотрим подробно функции отдельных уровней модели OSI в процессе организации информационного обмена между абонентами в компьютерных сетях и в ТКС.

2.2.1. Физический уровень

Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизуются типы разъемов и назначение каждого контакта [12].

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

2.2.2. Канальный уровень

Одной из задач канального уровня является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые *кадрами* (*frames*). Канальный уровень обеспечивает корректность передачи каждого кадра, добавляя контрольную сумму к кадру. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров [12].

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Хотя канальный уровень и обеспечивает доставку кадра между любыми двумя узлами локальной сети, он это делает только в сети с совершенно определенной топологией связей, именно той топологией, для которой он был разработан

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи.

2.2.3. Сетевой уровень

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей [12].

Протоколы канального уровня локальных сетей обеспечивают доставку данных между любыми узлами только в сети с соответствующей типовой топологией, например топологией иерархической звезды. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами. Можно было бы усложнять протоколы канального уровня для поддержания петлевидных избыточных связей, но принцип разделения обязанностей между уровнями приводит к другому решению. Чтобы с одной стороны сохранить простоту процедур передачи данных для типовых топологий, а с другой допустить использование произвольных топологий, вводится дополнительный сетевой уровень.

На сетевом уровне сам термин «сеть» наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня. Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.

Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или *хопов* (от hop – прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Проблема выбора наилучшего пути называется *маршрутизацией*, и ее решение является одной из главных задач сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изме-

нению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например, надежности передачи.

На рис. 2.4 показаны 4 сети, связанные 3 маршрутизаторами.

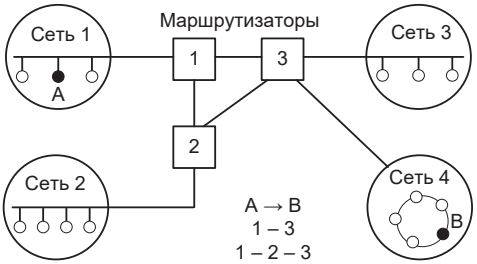


Рис. 2.4. Пример составной сети

Между узлами A и B данной сети пролегают два маршрута: первый через маршрутизаторы 1 и 3, а второй через маршрутизаторы 1, 2 и 3.

В общем случае функции сетевого уровня шире, чем функции передачи сообщений по связям с нестандартной структурой, которые мы сейчас рассмотрели на примере объединения нескольких локальных сетей. Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Сообщения сетевого уровня принято называть *пакетами* (packets). При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части – номера сети и младшей – номера узла в этой сети. Все узлы одной сети должны иметь одну и ту же старшую часть адреса, поэтому термину «сеть» на сетевом уровне можно дать и другое, более формальное определение: *сеть* – это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

На сетевом уровне определяются два вида протоколов [11]:

1) *сетевые протоколы* (*routed protocols*) – реализуют продвижение пакетов через сеть;
2) *протоколы маршрутизации* (*routing protocols*). С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют *протоколами разрешения адресов – ARP* (Address Resolution Protocol). Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути. Примером протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP.

2.2.4. Транспортный уровень

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется [12]. Модель OSI определяет различные классы сервисов по поддержанию качества обслуживания, предоставляемых транспортным уровнем [12]:

- время доставки сообщения;
- возможность восстановления прерванной связи;
- наличие средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол;
- способность к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней, а с другой стороны, этот выбор зависит от того, насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенными ниже транспортного – сетевым, канальным и физическим.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем. Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы (рис. 2.5).

2.2.5. Сеансовый уровень

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала [12].

2.2.6. Представительный уровень

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является прото-

кол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP [12].

2.2.7. Прикладной уровень

Прикладной уровень содержит набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Приведем в качестве примера несколько наиболее распространенных реализации файловых служб: HTTP, FTP и TFTP, входящие в стек TCP/IP [12].

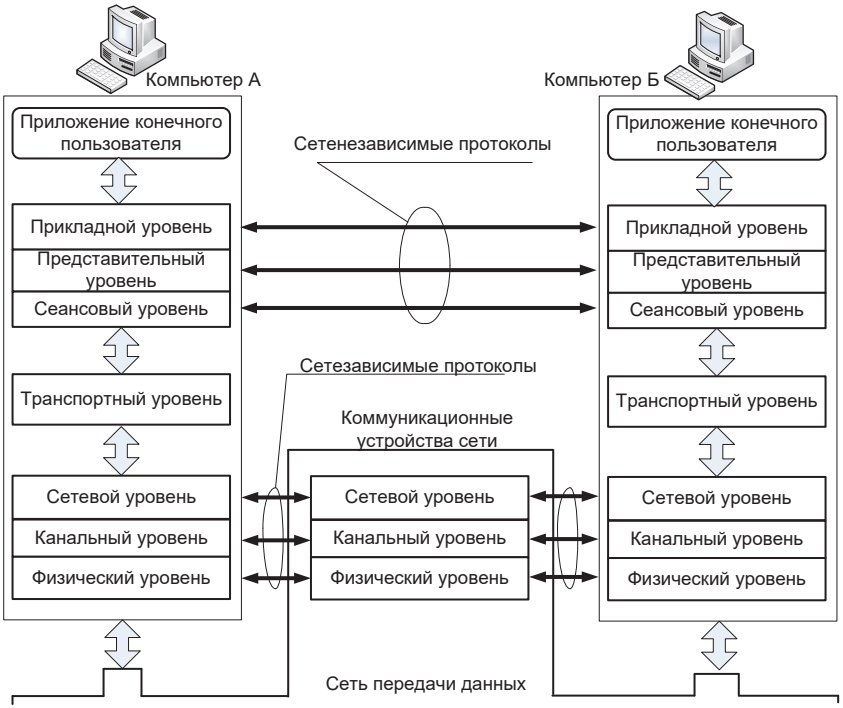


Рис. 2.5. Соответствие функций устройств сети уровням модели OSI

2.3. Особенности функционирования протоколов передачи данных в рамках модели OSI

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форма-

тами сообщений, службами, поддерживаемыми на верхних уровнях, и прочими параметрами. Соответствие популярных стеков протоколов модели OSI показано в таблице 2.1.

Таблица 2.1 – Соответствие популярных стеков протоколов модели OSI

<table>
<tr><th rowspan="2">Уровень модели OSI</th><th colspan="3">Стек протоколов</th></tr>
<tr><th>IBM/Microsoft</th><th>TCP/IP</th><th>OSI</th></tr>
<tr><td>Прикладной</td><td rowspan="2">SMB</td><td rowspan="2">Telnet, FTP, TFTP, SNMP, SMTP, WWW</td><td rowspan="3">X.400, X.500, FTAM
Протокол представления OSI
Сеансовый протокол OSI</td></tr>
<tr><td>Представительный</td></tr>
<tr><td>Сеансовый</td><td rowspan="2">NetBIOS</td><td rowspan="2">TCP, UDP</td></tr>
<tr><td>Транспортный</td><td>Транспортный протокол OSI</td></tr>
<tr><td>Сетевой</td><td></td><td>IP, RIP, OSPF, BGP, IGRP</td><td>ES-ES, IS-IS</td></tr>
<tr><td>Канальный</td><td colspan="3">Ethernet, Token Ring, FDDI, X.25, ATM PPP</td></tr>
<tr><td>Физический</td><td colspan="3">Медный кабель, оптическое волокно, радиолиния</td></tr>
</table>

Модель OSI описывает концепцию организации информационной связи компьютеров, но не конкретный способ обмена данными. Реальная последовательность действий компьютеров определяется используемыми *протоколами обмена*. В рассматриваемом контексте протокол определяется как набор правил и соглашений, предписывающих компьютерам последовательность действий для осуществления обмена через среду передачи данных.

Существует довольно большое разнообразие протоколов обмена – протоколы локальных и глобальных сетей, межсетевого взаимодействия, маршрутизации. Протоколы локальных сетей выполняют функции физического и канального уровня. Протоколы глобальных сетей работают на трех низших уровнях модели. Протоколы межсетевого взаимодействия, как очевидно из названия, являются протоколами сетевого уровня. И, наконец, протоколы маршрутизации также являются протоколами сетевого уровня, поскольку отвечают за обмен информацией между маршрутизаторами, выбирающими сетевой маршрут. Многие протоколы при выполнении своих функций основываются на результатах работы других протоколов. Например, протоколы маршрутизации используют протоколы межсетевого взаимодействия для обмена данными между маршрутизаторами. Концепция построения протоколов, опирающихся на другие существующие протоколы, является фундаментальной для OSI модели и служит основой создания стеков взаимодействующих протоколов.

Соответствие реальных протоколов сетевого обмена уровням модели OSI приведено в таблице 2.2.

Таблица 2.2 – Соответствие протоколов ТКС уровням модели OSI

Уровень OSI	Протоколы
Прикладной	HTTP, Telnet, DNS, DHCP, SMTP, SNMP, CMIP, FTP, TFTP, SSH, IRC, AIM, NFS, NNTP, NTP, SNTP, X.400, X.500, AFP, SIP, Modbus TCP, BACnet IP, IMAP, POP3, SMB, MFTP, BitTorrent, eD2k, NCP
Представительный	XML-RPC, TDI, XDR, SNMP, Telnet, NCP, AFP, ICA
Сеансовый	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, NWLink, Printer Access Protocol, Zone Information Protocol, SSL, TLS, RPC
Транспортный	TCP, UDP, SOCKS, NetBEUI, AEP, ATP, IL, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP, TFTP
Сетевой	IP, IPv6, ICMP, IGMP, NetBEUI, DDP, IPSec, RARP, BOOTP, SKIP, RIP
Канальный	STP, ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token ring, StarLan, L2F, L2TP, PPTP, PPP, PPPoE, PROFIBUS, CSMA/CD, CSMA/CA, ARP
Физический	xDSL, ISDN (T1, E1), Ethernet, Fast Ethernet, Gigabit Ethernet

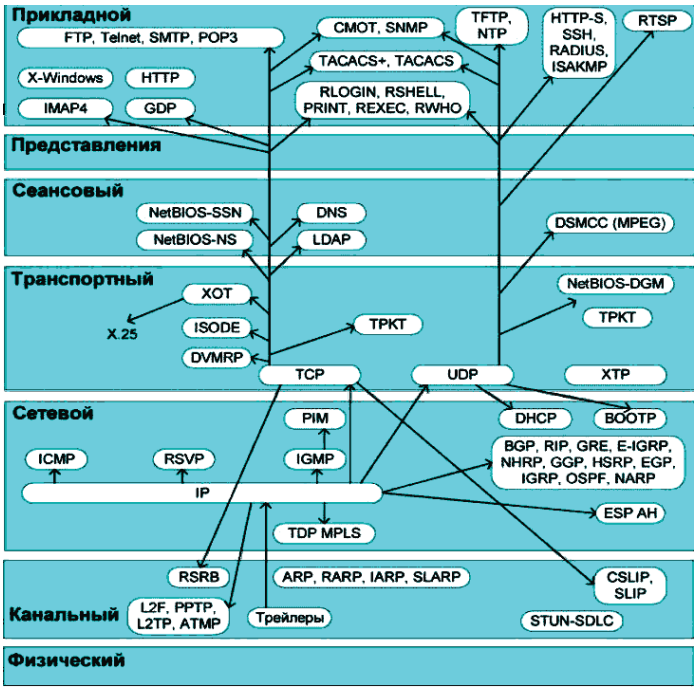


Рис. 2.6. Взаимосвязь отдельных протоколов внутри стека TCP/IP

Глава 2 основана на материале работы [12] с дополнениями из работ [1, 5].

3. Физические среды и каналы связи

3.1. Общая характеристика каналов связи телекоммуникационных систем

Физический уровень OSI отвечает за транспортировку информации в виде сигналов непосредственно через физическую среду передачи.

Среда передачи – физическая субстанция, по которой происходит передача (перенос) той или иной информации от источника (передатчика, отправителя) к приёмнику (получателю). Информация переносится с помощью сигналов.

Сигнал – код (символ, знак), созданный и переданный в пространство (по каналу связи) передатчиком, либо возникший в процессе взаимодействия нескольких систем. Смысл и значение сигнала проявляются после его регистрации и интерпретации в приемнике (принимающей системе).

Сигналы могут иметь различную природу:

- электрическую (электроны по меди, заряженные ионы);
- механическую (звуковые волны по воздуху, сейсмические волны в грунте);
- электромеханическую;
- электромагнитную (радиоволны по воздуху, в безвоздушном пространстве или в грунте);
- оптическую (свет лазера по оптоволокну).

Для стационарных ТКС можно указать приблизительные типовые варианты использования физических сред, сигналов, информационного и помехоустойчивого кодирования, протоколов доступа к среде передачи для базовых транспортных технологий: PDH, SDH, OTH и Gigabit Ethernet (см. таблицу 3.1).

В подавляющем большинстве телекоммуникационных сетей используются проводные или *кабельные каналы связи*, хотя существуют и *беспроводные сети*, которые сейчас находят все более широкое применение.

Промышленностью выпускается огромное количество типов кабелей которые можно разделить на 3 большие группы [1]:

1) электрические (медные) кабели на основе витых пар проводов (twisted pair), которые делятся на:
   - экранированные (shielded twisted pair, STP);
   - неэкранированные (unshielded twisted pair, UTP);
2) электрические (медные) коаксиальные кабели (coaxial cable);
3) оптоволоконные кабели (fiber optic).

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать, как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Таблица 3.1 – Типовые среды, сигналы, коды и технологии доступа, используемые в стационарных ТКС [8]

Технология	Физическая среда	Используемые сигналы	Линейное кодирование	Помехоустойчивое кодирование	Технология доступа / мультиплексирования
PDH (E1)	Радио (ТРРЛ)	2FSK, 4FSK	По стандарту G.703	код Витерби, FEC, РС, БЧХ	TDM, FDM
PDH (E1…E4)	Радио (РРЛ)	BPSK, QPSK, 8PSK, 2FSK, 4FSK, 4QAM…1024QAM	По стандарту G.703	код Витерби, FEC, РС, БЧХ	TDM, FDM, CDMA, OFDM, COFDM
PDH (E1…E4)	Проводные линии связи (UTP, STP)	PCM (по стандарту G.703)	AMI, B8ZS, B6ZS, HDB3, CMI (по стандарту G.703)	FEC	TDM
SDH (STM-1)	Проводные линии связи (UTP, STP)	PCM (по стандарту G.703)	CMI	BPI	TDM
SDH (STM-1, STM-4)	Радио (РРЛ)	BPSK, QPSK, 8PSK, 2FSK, 4FSK, 4QAM…1024QAM	NRZ	код Витерби, FEC, BPI	TDM, OFDM, COFDM
SDH (STM-1…STM-256)	ВОЛС (SMF, MMF)	PCM	NRZ	BPI	TDM, WDM, CWDM, DWDM, HDWDM
OTH	ВОЛС (SMF, MMF)	PCM	–	FEC, PC	TDM, WDM, CWDM, DWDM, HDWDM
Gigabit Ethernet	ВОЛС (SMF, MMF)	PCM	NRZ	CRC	CSMA/CD, MPCP, EoT, PON

Можно выделить следующие основные параметры кабельных каналов связи, принципиально важные для использования в сетях [1]:

- *полоса пропускания кабеля* (частотный диапазон сигналов, пропускаемых кабелем) и *затухание сигнала в кабеле*. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. Надо выбирать кабель, который на заданной частоте сигнала имеет приемлемое затухание;
- *помехозащищенность* кабеля и обеспечиваемая им *безопасность* передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние помехи, и насколько просто прослушать информацию, передаваемую по кабелю;

– *скорость распространения сигнала* по кабелю или, обратный параметр – *задержка сигнала* на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины задержек – от 4 до 5 нс/м;
– для электрических кабелей очень важна величина *волнового сопротивления* кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

Таблица 3.2 – Характеристики основных каналов связи

Типовой канал связи	Расстояние	Скорость
Неэкранированная витая пара	до 90 м	10-155 Мбит/с
Коаксиальный кабель	до 2 км	2-44 Мбит/с
Телефонная линия	-	56,6 кбит/с
Оптоволоконный	до 10 км	до 10 Гбит/с
Радиоканал	до 70 км	до 400 кбит/с
Экранированная витая пара	до 300 м	16 Мбит/с

3.2. Кабельные каналы связи на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке (рис. 3.1-3.5). Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Неэкранированные витые пары – UTP (unshielded twisted pair**)** характеризуются слабой защищенностью от внешних электромагнитных помех, а также от утечки побочных электромагнитных излучений и наводок (ПЭМИН).

В случае экранированной витой пары STP (shielded twisted pair) каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (crosstalk – перекрестные наводки). Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов.

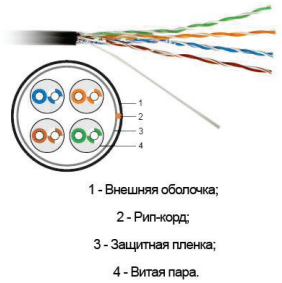


Рис. 3.1. Структура кабеля UTP

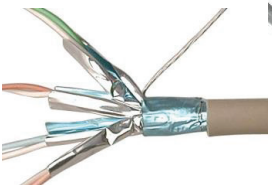


Рис. 3.2. Кабель STP

Рис. 3.3. Кабель UTP 5 с разъемом RJ-45

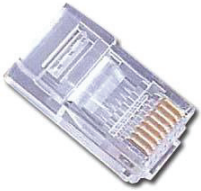


Рис. 3.4. Вилка RJ-45

Рис. 3.5. Гнездо RJ-45

3.3. Коаксиальные кабельные каналы

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (экрана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку.

Коаксиальный кабель до 2000-х гг. был очень популярен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), более широкими, чем в случае витой пары, полосами пропускания (свыше 1 ГГц), а также большими допустимыми расстояниями передачи (до километра). К нему труднее механически несанкционированно подключиться, он дает также заметно меньше ПЭМИН во вне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5–3 раза). Сложнее и установка разъемов на концах кабеля. Сейчас его применяют существенно реже, чем витую пару. Волновое сопротивление кабеля указывается в сопроводительной документации. Чаще всего в локальных сетях применяются 50-омные (RG-58, RG-11, RG-8) и 93-омные кабели (RG-62). Распространенные в телевизионной технике 75-омные кабели в локальных сетях не используются.

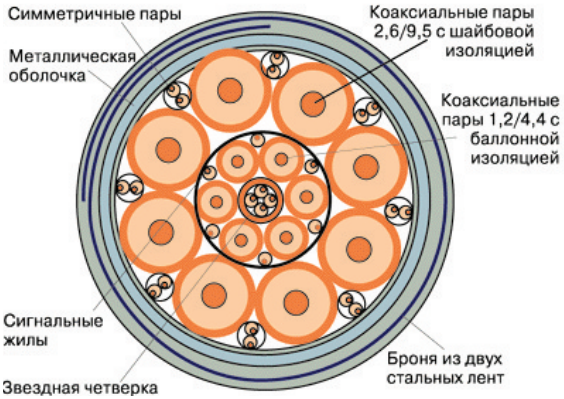


Рис. 3.6. Комбинированный коаксиальный кабель для прокладки в земле

Рис. 3.7. Разъем подключения коаксиального кабеля

Рис. 3.8. Коаксиальный кабель

3.4. Оптико-волоконные кабельные каналы

3.4.1. Общая характеристика оптико-волоконных каналов

Оптико-волоконный кабель (часто встречается сокращение соответствующей линии связи – ВОЛС (волоконно-оптическая линия связи)) – это принципиально иной тип кабеля, информация по которому передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.

Структура оптико-волоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля. Только вместо центрального медного провода здесь используется тонкое (диаметром около 1–10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или

пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна.

Оптико-волоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля. Теоретически возможная полоса пропускания такого кабеля достигает величины 10–12 Гц, то есть 1000 ГГц, что несравнимо выше, чем у электрических кабелей. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля. В случае оптико-волоконного кабеля при росте частоты передаваемого сигнала затухание увеличивается очень незначительно, и на больших частотах (особенно свыше 200 МГц) его преимущества перед электрическим кабелем неоспоримы.

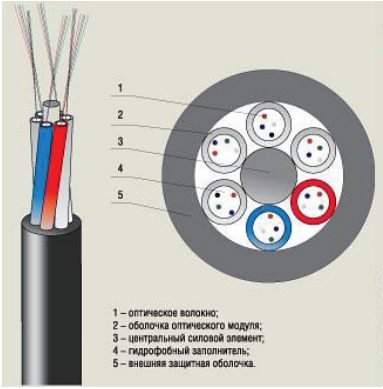


Рис. 3.9. Оптический кабель с профилированным сердечником

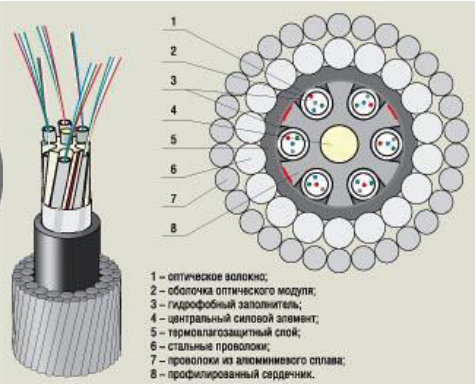


Рис. 3.10. Оптический кабель, со свободной укладкой оптических модулей

Однако оптико-волоконный кабель имеет и некоторые недостатки. Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. В любом случае для этого нужна высокая квалификация персонала и специальные инструменты.

Также надо помнить, что использование оптико-волоконного кабеля требует специальных оптических приемников и передатчиков, преобразу-

ющих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

3.4.2. Многомодовые и одномодовые кабели

Существуют два различных типа оптико-волоконного кабеля [1]:

- *многомодовый* кабель, более дешевый, но менее качественный;
- *одномодовый* кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.

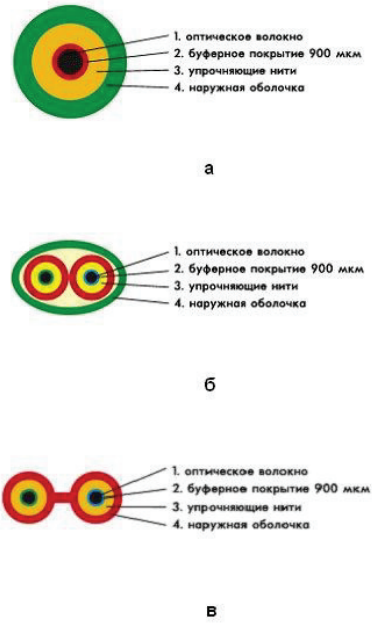


Рис. 3.11. Структура оптико-волоконного кабеля для внутриобъектовой прокладки (а – Simplex, б – Duplex Zipcord, в – Duplex Heavy Duty)

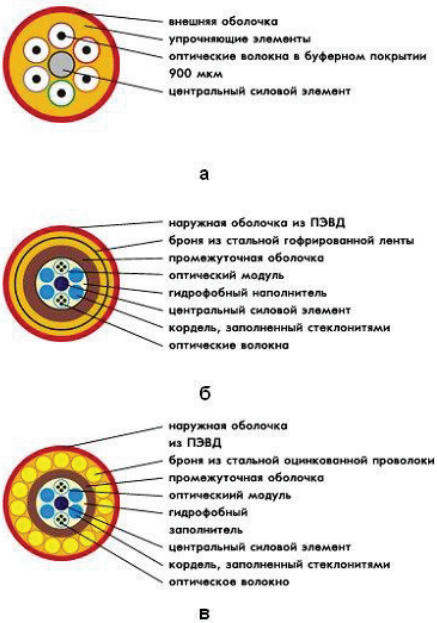


Рис. 3.12. Структура оптико-волоконного кабеля для наружных работ (а – Distribution, б – ДПЛ, в – ДПС)

Рис. 3.13. Коннектор и соединитель для оптического волокна

В *одномодовом кабеле* практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны.

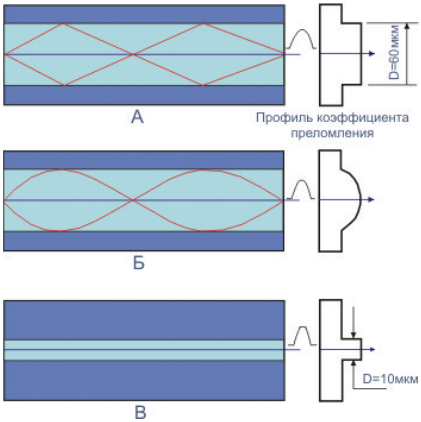


Рис. 3.14. Многомодовый (а, б) и одномодовый (в) оптоволоконные кабели

В *многомодовом кабеле* траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм, при этом наблюдается разброс длин волн около 30–50 нм. Допустимая длина кабеля составляет 2–5 км. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5–20 дБ/км. Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

Многомодовый кабель – это основной тип оптико-волоконного кабеля в настоящее время, так как он дешевле и доступнее.

Типовые характеристики различных оптико-волоконных кабелей приведены в таблице 3.3.

Таблица 3.3 – Типовые характеристики различных оптиковолоконных кабелей по данным ресурса [14]

Тип волокна	Диаметр ядра [мкм]	Диаметр клэдинга [мкм]	A	Затухание [дБ/км]			Полоса пропускания [МГц/км]
Длина волны				850	1300	1550	
Одномодовое	9,3 8,1	125 125	0,13 0,17		0,4 0,5	0,3 0,25	5000 для 850 нм
Со сглаженным индексом	50 62,5 85	125 125 125	0,2 0,275 0,26	2,4 3,0 2,8	0,6 0,7 0,7	0,5 0,3 0,4	600 для 850 нм; 1500 для 1300 нм
Ступенчатый индекс	200	380	0,27	6,0			6 при 850 нм

3.4.2. Технология WDM – мультиплексирование с разделением по длине волны

В последнее время заметного повышения эффективности оптических каналов удалось достичь за счет использования технологии мультиплексирования с разделением по длине волны WDM (wavelength-division multiplexing). Технология WDM позволяет существенно увеличить пропускную способность оптических каналов (к 2003 г., в коммерческих системах достигнута скорость 10,72 Тбит/с, а к 2015 г. – 27 Тбит/с), причём она позволяет использовать уже проложенные волоконно-оптические линии. Благодаря WDM удается организовать двустороннюю многоканальную передачу трафика по одному волокну.

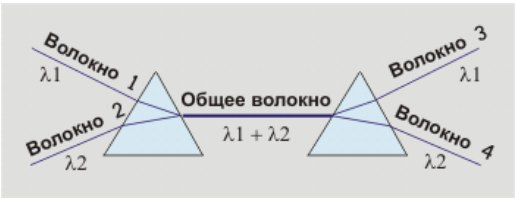


Рис. 3.15. Мультиплексирование с разделением по длине волны в оптическом волокне [14]

Схема мультиплексирования показана на рис. 3.15. На входе канала сигналы с помощью призмы объединяются в одно общее волокно. На выходе с помощью аналогичной призмы эти сигналы разделяются. Число волокон на входе и выходе может достигать 32 и более (вместо призм в последнее время используются миниатюрные зеркала, где применяется 2D-развертка (или 3D) по длине волны). Разработка технологии получения особо чистого материала волокон позволила расширить полосу пропуска-

ния одномодового волокна до 100 нм. Полоса одного канала может лежать в диапазоне от 2 до 0,2 нм.

Для осуществления требуемой маршрутизации часто бывает нужно в коммутационном узле сменить длину волны потока. Схема этой операции показана на рис. 5.18, a – для OADM (optical adddrop multiplexer), рис. 5.18, b – для оптического кросс-коммутатора OXC (optical cross-connect), рис. 5.18, c – для OXC со сменой длины волны.

Рис. 3.16. Схема многоканального мультиплексирования с делением по длине волны в оптическом волокне. TE – терминальное оборудование; L – лазер; M/D – оптический мультиплексор-демультиплексор [14]

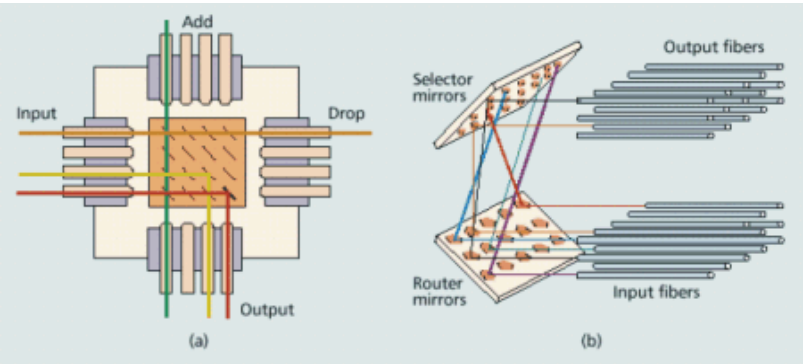


Рис. 3.17. Схема перенаправления оптических информационных потоков [14]

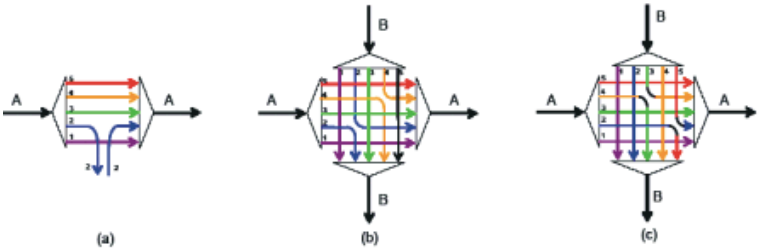


Рис. 3.18. Схема перенаправления оптических информационных потоков со сменой и без смены длины волны [14]

Современные системы оптической связи с WDM существуют в виде следующих технологий:

- CWDM (coarse WDM) – грубые WDM – системы с частотным разносом каналов более 2500 ГГц, позволяющие мультиплексировать не более 18 каналов. Используемые в настоящее время CWDM работают в полосе от 1271 нм до 1611 нм, промежуток между каналами 20 нм (2500 ГГц), что позволяет мультиплексировать 18 спектральных каналов. Частотный план для систем CWDM определяется стандартом ITU G.694.2. Область применения технологии CWDM – городские сети с диаметром сети до 50 км. Достоинством этого вида WDM систем является низкая (по сравнению с другими типами) стоимость оборудования вследствие меньших требований к компонентам;
- DWDM (dense WDM) – плотные WDM – системы с разносом каналов 100 ГГц, 50 ГГц, 25 ГГц, 12,5 ГГц позволяющие мультиплексировать до 40, 80, 160 и 320 каналов соответственно. Каналы отсчитываются по обе стороны от центральной частоты 193,1 ТГц, что соответствует длине волны 1552,52 нм. Частотный план для систем DWDM определяется стандартом ITU G.694.1. Область применения DWDM – магистральные транспортные сети. Этот вид систем WDM предъявляет более высокие требования к компонентам, чем CWDM (ширина спектра источника излучения, температурная стабилизация источника и т. д.);
- Flexible Grid DWDM – вариант технологии DWDM. Данная технология позволяет распределять спектральный ресурс оптического волокна, как и в DWDM, отсчитывая от центральной частоты 193,1 ТГц, но при этом использовать разные по ширине спектральные полосы для каждого из каналов (слотов). Ширина каждого такого слота должна быть кратна 12,5 ГГц, а центральная частота каждого слота определяется по 6,25 ГГц сетке DWDM. Допускается любая комбинация, при которой слоты не перекрывают друг друга.

3.5. Радиоканалы связи

Кроме кабельных каналов в компьютерных сетях также используются беспроводные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов. К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в

секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Главным недостатком радиоканала является его плохая защита от несанкционированного доступа (НСД), так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

Для локальных беспроводных сетей (WLAN – Wireless LAN) в настоящее время применяются подключения по радиоканалу на небольших расстояниях (обычно до 100 м) и в пределах прямой видимости. Чаще всего используются два частотных диапазона – 2,4 ГГц и 5 ГГц. Скорость передачи – до 54 Мбит/с (стандарт WiFi IEEE 802.11 g).

Использование радиоканалов связи осложняется недостаточностью частотного диапазона, особенно в России, а также ограниченностью видов сигналов, используемых при передаче. Недостаточный частотный ресурс порождает проблему электромагнитной совместимости (ЭМС) радиосредств.

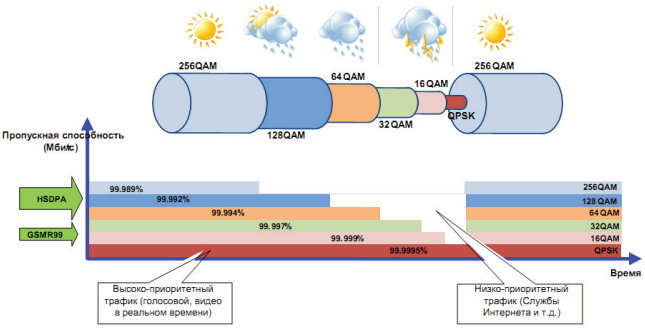


Рис. 3.19. Использование адаптивной модуляции сигналов в интересах обеспечения максимальной скорости передачи в заданных условиях

В современных системах радиосвязи используются адаптивные системы сигналов, позволяющие организовать связь с максимальной для данных погодных и радиоусловий скоростью (рис. 3.19). Кроме того, в настоящее время широко внедряются системы радиосвязи с широкополосными сигналами (ШПС) и системы с ортогональными поднесущими (OFDM), которые позволяют снизить остроту проблемы ЭМС и оптимизировать использование полосы частот (рис. 3.20, 3.21).

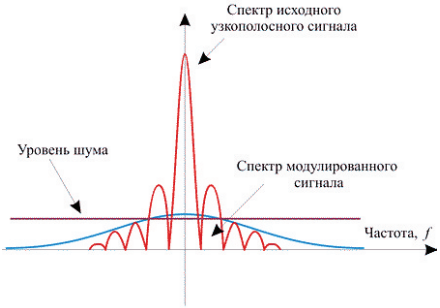


Рис. 3.20. Использование ШПС

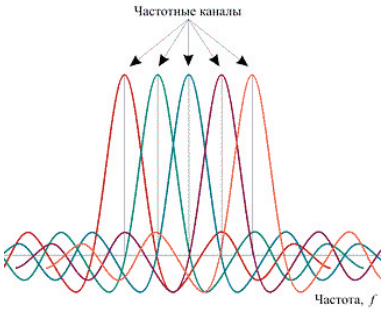


Рис. 3.21. Использование OFDM

Материал главы 3 основан на информации, представленной в работе [1] и материалах Интернет-ресурса [14].

4. Технологии проводных компьютерных сетей

4.1. Общая характеристика протоколов канального уровня

Канальный уровень предназначен для сетевого многостанционного использования среды распространения сигналов физического уровня, контроля и исправления ошибок, которые могут возникнуть при передаче. Полученные с физического уровня данные он упаковывает в кадры, проверяет их на целостность, если нужно исправляет ошибки (посылает повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями (обеспечивая передачу по нескольким различным физическим средам), контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет канальный уровень на два подуровня:

1. подуровень MAC (Media Access Control) – регулирует многостанционный доступ абонентов к разделяемой физической среде;
2. подуровень LLC (Logical Link Control) – обеспечивает обслуживание сетевого уровня. На этом уровне работают коммутаторы, мосты.

Канальный уровень реализуется аппаратно в виде сетевой платы и программно – в виде драйвера сетевой платы. В ОС имеется программный интерфейс взаимодействия канального и сетевого уровней между собой, это не новый уровень, а просто реализация модели канального уровня для конкретной ОС.

Так, как канальный уровень позволяет передавать данные в рамках одной топологии, необходимо ввести данное понятие. Термин «топология сети» относится к пути, по которому данные перемещаются по сети и структуре сети.

4.2. Понятие топологии сети

Для описания связей абонентов в сети используется понятие *топология*, под которой принято считать совокупность элементов и связей между ними в сети, «очищенных» от всех свойств, кроме свойств существования и связности.

Обычно топология задается графом $G(A, N)$, где A – множество вершин графа, т.е. элементов сети (пользователи, узлы, центры коммутации и т. п.), а N − множество его ребер, соответствующих линиям связи. Каждое ребро имеет вес, который эквивалентен некоторым параметрам ее использования, например, ее длине, пропускной способности, общей загрузке и

т.п. В случае, когда учитываются направления ребер задается ориентированный граф (орграф).

Пример геометрического представления орграфа показан на рис. 4.1.

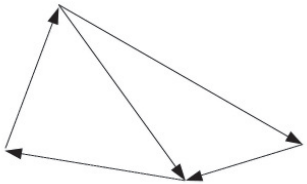


Рис. 4.1. Орграф

Существуют 3 основных типа топологий сетей передачи данных (СПД).

1. *Полносвязная топология* – узлы соединены линиями (каналами) по принципу «каждый с каждым» (рис. 4.2). Полносвязная топология на практике при большом количестве абонентских терминалов практически не используется из-за необходимости организации значительного числа каналов и низкой эффективности их использования, так как большую часть времени каналы простаивают. Тем не мене следует отметить, что такая сеть проста в управлении, обладает высокой живучестью, своевременностью, пропускной способностью.

2. *Древовидная топология* – узлы соединяются между собой минимальным числом линий (каналов) без образования замкнутых путей. Между любыми двумя узлами только один путь (рис. 4.3).

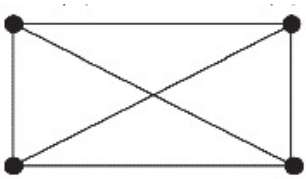


Рис. 4.2. Полносвязная топология сети

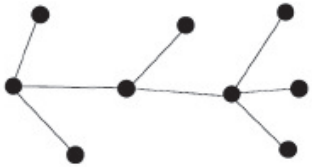


Рис. 4.3. Древовидная топология сети

В большинстве случаев сетью управляет узел на самом высоком уровне иерархии. Однако практический интерес, представляет распределенный подход к иерархической сети, при котором в системе подчиненных узлов определяются такие, которые обеспечивают непосредственное управление устройствами, находящимися ниже в иерархии.

Древовидная топология может иметь ряд частных случаев (рис. 4.4):

а) линейная;

б) звездообразная;

в) радиальная;

г) радиально-узловая.

а) линейная

б) звездообразная

в) радиальная

г) радиально-узловая

Рис. 4.4. Частные случаи древовидной топологии сети

Топология «звезда» – одна из наиболее распространенных среди древовидной топологии сети. В сетях с такой топологией вся информационная нагрузка исходит из центрального узла, который полностью управляет устройствами, подсоединенными к нему. Центральный узел отвечает за маршрутизацию трафика через себя в другие компоненты. Он также отвечает за локализацию неисправности, которая является относительно простой в звездообразной сети, поскольку решение проблемы обусловлено возможностью локализации линии. Подобно иерархической структуре, звездообразная топология сети также подвержена проблемам, связанным с наличием одного центрального узла.

3. *Топология типа «сеть»* – каждый узел соединен с несколькими ближайшими узлами так, что образуются замкнутые пути (рис. 4.5).

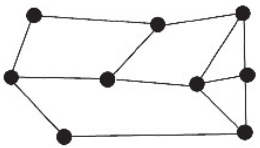


Рис. 4.5. Топология типа «сеть»

Топология типа «сеть» нашла широкое практическое применение. Ее привлекательность заключается в высокой надежности и относительной устойчивости к перегрузкам. Благодаря множественности путей трафик может быть направлен в обход отказавших или занятых узлов. Это достигается большей сложностью и дороговизной сети.

Частным случаем топологии типа «сеть» является:

а) *топология типа «кольцо»* (рис. 4.6). При кольцевой топологии в большинстве случаев данные распространяются только в одном направле-

нии, причем только одна станция принимает сигнал, а затем при необходимости передает его следующей станции в кольце.

Кольцевая топология привлекательна, т. к. перегрузки характерные для иерархической и звездообразной топологии, здесь достаточно редки. Так же следует отметить простоту организации кольцевой сети. Недостатком является то, что имеется только один канал, соединяющий все компоненты в кольцо. Если отказывает канал между двумя узлами, наступает отказ всей сети.

б) *топология типа «общая шина»* – при такой топологии все абонентские терминалы подключаются к одному каналу связи. При этом канал связи используется поочередно каждой из пар абонентских терминалов для обмена информацией между собой (рис. 4.7).

Данная топология нашла широкое распространение в локальных сетях. Это обусловлено относительно простым для управления трафиком, поскольку шина допускает, чтобы каждое сообщение принималось всеми станциями (одна единственная станция работает в широковещательном режиме на несколько станций).

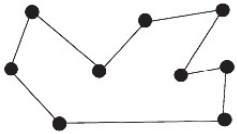


Рис. 4.6. Топология типа «кольцо»

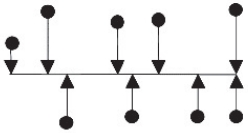


Рис. 4.7. Топология типа «общая шина»

Рассмотрим различные типовые архитектуры компьютерных сетей на канальном уровне OSI, соответствующих основным видам топологий.

4.3. Сети X.25

X.25 – семейство протоколов канального уровня сетевой модели OSI. Оно предназначалось для организации глобальных сетей на основе телефонных сетей с линиями с достаточно высокой частотой ошибок, поэтому содержит развитые механизмы коррекции ошибок и ориентировано на работу с установлением соединений.

X.25 разработан в 1976 г. Study Group VII Международного союза электросвязи (МСЭ). Существенные дополнения к стандарту X.25 были приняты в 1984 г., в частности для согласования имеющихся уровней X.25 с эталонной моделью OSI. В настоящее время для X.25 действует стандарт ISO 8208, а также стандартизовано применение пакетного уровня X.25 (протокол PLP) в локальных сетях (стандарт ISO 8881). Исторически X.25 является предшественником протокола Frame Relay.

Сеть X.25 состоит из пакетных коммутаторов PSE (Packet Switch Exchange), называемых также *центрами коммутации пакетов*, расположен-

ных в различных географических точках и соединенных высокоскоростными выделенными каналами. При этом выделенные каналы могут быть как цифровыми, так и аналоговыми. X.25 обеспечивает множество независимых виртуальных каналов типа PVC (Permanent Virtual Circuits) и SVC (Switched Virtual Circuits) в одной линии связи, идентифицируемых в X.25-сети по идентификаторам подключения к соединению, которую обеспечивают идентификаторы логического канала LCI (Logical Channel Identifyer) и номера логического канала LCN (Logical Channel Number). Абонентское оборудование DTE (Data Terminal Equipment) подсоединяется к сети X.25 через сетевое оборудование провайдера DCE (Data Circuit-terminating Equipment), обеспечивающего предоставление услуг связи. Как правило роль DCE обычно выполняет модем или коммутатор, который находится на стороне провайдера и транслирует данные от абонентского оборудования DTE в сеть X.25 (рис. 4.8).

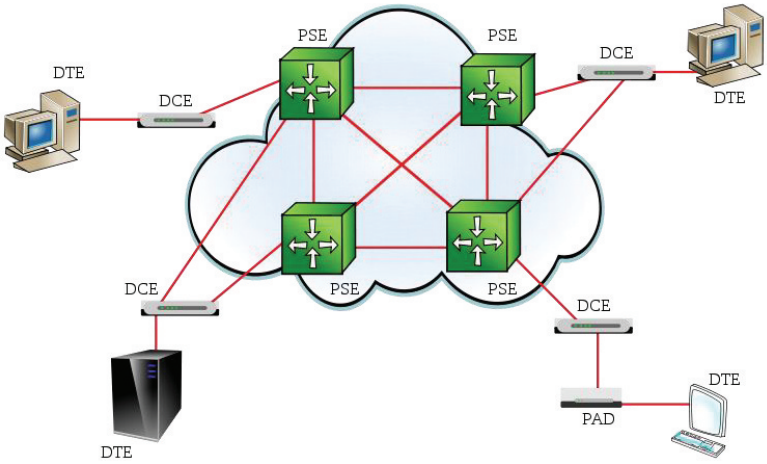


Рис. 4.8. Структура сети X.25

Несмотря на то, что сети X.25 вытесняется другими сетевыми технологиями канального уровня (Frame Relay, Ethernet и др.), а также протоколом IP, однако, эти сети достаточно распространены в странах и на территориях с неразвитой телекоммуникационной инфраструктурой. Основная причина такой ситуации состоит в том, что сети X.25 хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях – канальном и сетевом.

Технология сетей X.25 имеет несколько существенных признаков, отличающих ее от других технологий:

– наличие в структуре сети специального устройства – PAD (Packet Assembler Disassembler), предназначенного для выполнения операции сборки нескольких низкоскоростных байт-потоков от або-

нентов в пакеты, передаваемые по сети и направляемые компьютерам для обработки. Эти устройства имеют также русскоязычное название *«сборщик-разборщик пакетов»*.

– наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки.
– ориентация на однородные стеки транспортных протоколов во всех узлах сети – протокол сетевого уровня X.25 рассчитан на работу только с одним протоколом канального уровня и не может, подобно протоколу IP, объединять разнородные сети.

4.4. Сети Frame Relay

Frame relay (англ. «ретрансляция кадров», FR) – протокол канального уровня эталонной модели OSI. Протокол коммутации пакетов Frame Relay в настоящее время широко распространена во всём мире. Максимальная скорость, допускаемая протоколом Frame Relay – 34,368 Мб/с (каналы типа E3). Тип коммутации: точка – точка. Топология сети: звезда.

Frame Relay был создан Американским национальным институтом стандартов ANSI в начале 1990-х в качестве замены протоколу X.25 для быстрых надёжных каналов связи. В отличие от X.25, рассчитанного на линии с достаточно высокой частотой ошибок, Frame Relay изначально ориентировался на физические линии с низкой частотой ошибок. Если кадр искажался, он просто отбрасывался без повторной передачи. В основном Frame Relay применяется при построении территориально-распределённых корпоративных сетей, а также в составе сетевых решений, связанных необходимостью обеспечения гарантированной пропускной способности канала передачи данных (VoIP, видеоконференции и т. п.).

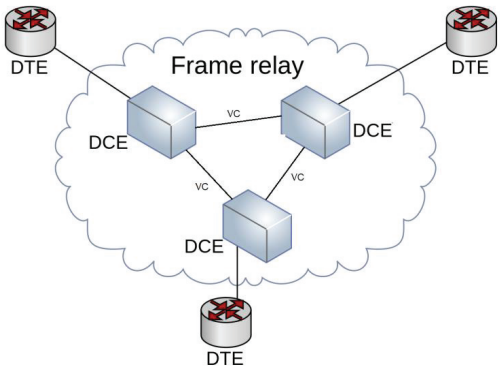


Рис. 4.9. Структура сети Frame Relay

Frame relay обеспечивает множество независимых виртуальных каналов VC (Virtual Circuits) в одной линии связи, идентифицируемых в

Frame Relay сети по идентификаторам подключения к соединению DLCI (Data Link Connection Identifier), но не имеет средств коррекции и восстановления передаваемых данных в случае сбоя. Вместо средств управления потоком Frame relay включает функции извещения о перегрузках в сети. Возможно назначение минимальной гарантированной скорости для каждого виртуального канала VC.

4.5. Сети Token Ring

Token Ring – «маркерное кольцо», архитектура кольцевой сети с маркерным доступом. Тип сети, в которой все абоненты логически объединены в кольцо. По кольцу от абонента к абоненту сети передается специальный блок данных, называемый *маркером* (от англ. *token*).

Сети с передачей маркера перемещают вдоль сети небольшой блок данных, называемый маркером. «Владение» этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки, он просто переправляет маркер к следующей конечной станции. Каждая станция может удерживать маркер в течение определенного времени. Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он окончательно удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения.

Рис. 4.10. Структура сети Token Ring с маркерным доступом

Данная технология предлагает вариант решения проблемы коллизий, которая возникает при работе локальной сети. В технологии Ethernet, такие коллизии возникают при одновременной передаче информации несколькими рабочими станциями, находящимися в пределах одного сегмента, то есть использующих общий физический канал данных.

Существовали 2-е модификации Token Ring со скоростями передачи 4 Мбит/с и 16 Мбит/с. В Token Ring 16 Мбит/с использовалась технология раннего освобождения маркера. Суть этой технологии заключается в том, что станция, «захватившая» маркер, по окончании передачи данных генерирует свободный маркер и запускает его в сеть. Попытки внедрить 100 Мбит/с технологию Token Ring не увенчались коммерческим успехом. Поэтому в настоящее время технология Token Ring не используется т.к. была полностью вытеснена технологией Ethernet.

4.6. Сети FDDI

FDDI (англ. Fiber Distributed Data Interface – распределённый волоконный интерфейс данных) – стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 км. Стандарт основан на протоколе Token Ring. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

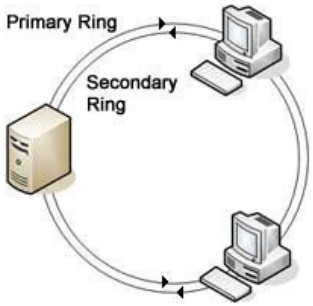
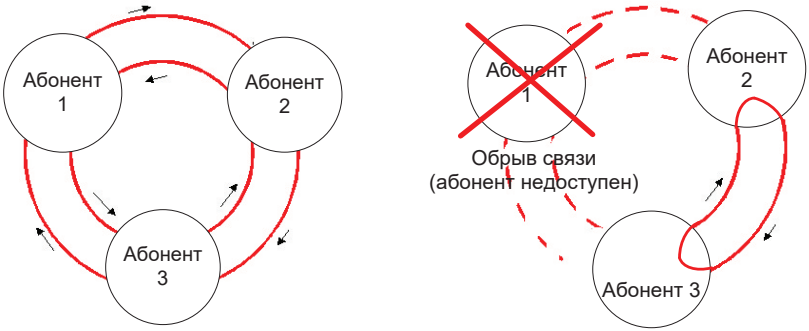


Рис. 4.11. Структура сети FDDI

В качестве среды передачи данных в FDDI рекомендуется использовать оптоволоконный кабель, однако можно использовать и медный кабель, в таком случае используется сокращение CDDI (Copper Distributed Data Interface). В качестве топологии используется схема двойного кольца, при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе – вспомогательным, по нему данные передаются в случае обрыва на первом кольце (рис. 4.12). Для контроля за состоянием кольца используется сетевой маркёр, как и в технологии Token Ring.

Поскольку дублирование повышает надёжность системы, данный стандарт с успехом применяется в сетях связи, в которых требуется повышенная надежность передачи данных.

В 2000-х гг. технология FDDI была вытеснена высокоскоростными вариантами Gigabit Ethernet на основе ВОЛС.



а) Нормальный режим функционирования сети FDDI

б) Функционирование сети FDDI при обрыве канала связи

Рис. 4.12. Функционирование сети FDDI при отказе

4.7. Сети Ethernet

4.7.1. Общий обзор технологии Ethernet

Ethernet (от лат. aether – эфир) – пакетная технология компьютерных сетей, преимущественно локальных. Технология Ethernet является классической реализацией топологии «общая шина».

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде – на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE 802.3. Ethernet стал самой распространённой технологией построения локальных сетей.

В стандарте первых версий Ethernet в качестве передающей среды использовался коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару, оптический кабель и радиоканал.

Метод управления доступом в Ethernet – множественный доступ с контролем несущей и обнаружением коллизий CSMA/CD (Carrier Sense Multiple Access with Collision Detection), скорость передачи данных 100 Мбит/с, размер пакета от 72 до 1526 байт. Количество узлов в одном разделяемом сегменте сети ограничено предельным значением в 1024 рабочих станции.

Для адресации абонента в Ethernet сети используется MAC (Media Access Control) адрес. Это уникальный шестнадцатеричный серийный но-

мер, назначаемый каждому сетевому устройству Ethernet, для идентификации его в сети. MAC адреса имеют длину 6 байт и обычно записываются шестнадцатеричным числом в виде 12:34:56:78:90:AB (двоеточия могут отсутствовать, но их наличие делает адрес более читабельным).

4.7.2. Технология случайного множественного доступа CSMA

CSMA/CD (Carrier-Sense Multiple Access with Collision Detection – множественный доступ с контролем несущей и обнаружением коллизий) – технология множественного доступа к общей передающей среде в локальной сети с контролем коллизий. Если во время передачи фрейма рабочая станция обнаруживает другой сигнал, занимающий передающую среду, она останавливает передачу, посылает «jam signal» («пробка») и ждет в течение случайного промежутка времени (известного как «backoff delay» и находимого с помощью алгоритма «truncated binary exponential backoff»), перед тем как снова отправить фрейм.

В радиосетях используется модификация случайного множественного доступа CSMA/CA.

Рис 4.13. Пример работы технологии CSMA/CD

Технология передачи CSMA/CD решает следующие задачи:

- контроль среды передачи (радиосреды, либо кабеля). Когда абонент собирается передавать данные в сеть методом CSMA/CD, он должен сначала проверить, передает ли в это же время по этому же кабелю свои данные другой абонент. Другими словами, проверить состояние носителя: занят ли он передачей других данных;

- *множественный доступ.* Это означает, что несколько абонентов могут начать передачу данных в сеть одновременно;
- *обнаружение конфликтов.* Это главная задача метода CSMA/CD. Когда абонент готов передавать данные, он проверяет состояние носителя. Если кабель занят, абонент не посылает сигналы, а ожидает когда освободится носитель. Если же абонент не слышит передаваемых данных в носителе, то он начинает передавать данные сам. Так же может случиться, что прослушивают носитель сразу два абонента готовые к передаче. И когда носитель освобождается, оба узла начинают передавать данные одновременно. В этом случае в носителе происходит смешение сигналов, из-за чего теряются данные. Такая ситуация называется конфликтом или *коллизией* (рис. 4.13).

Во время коллизии прием данных невозможен, поэтому оба абонента ожидают в течении случайного промежутка времени, после которого посылают сигналы заново. Случайные промежутки времени для разных абонентов создаются автоматически, для того чтобы не повторить коллизию. Абонент, у которого промежуток времени меньше, начнет передавать данные раньше. Таким образом, происходит «захват» носителя для передачи данных.

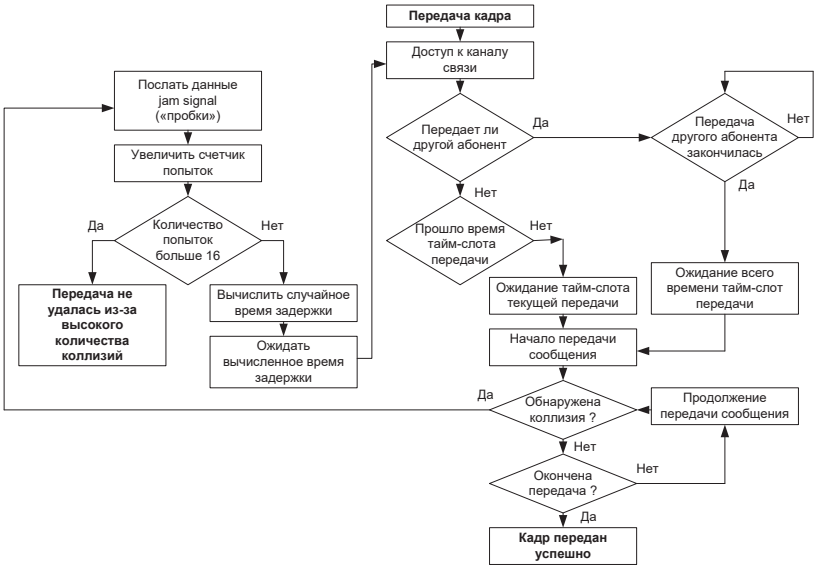


Рис. 4.14. Алгоритм CSMA/CD

Обнаружение коллизий (рис. 4.14) используется для улучшения производительности CSMA с помощью прерывания передачи сразу после обнаружения коллизии и снижения вероятности второй коллизии во время повторной передачи. Методы обнаружения коллизий зависят от используемого оборудования, но на электрических шинах, таких как Ethernet, коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия) и передача прерывается немедленно. Посылается «jam signal» («пробка»), что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.

Методы обнаружения коллизий зависят от используемого оборудования, но на электрических шинах, таких как Ethernet, коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия) и передача прерывается немедленно. Посылается «jam signal», что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.

4.7.3. Современные стандарты технологии Ethernet

После своего появления в 1972 г. технология Ethernet быстро стала доминирующей, сначала в сегменте локальных компьютерных сетей, а в дальнейшем – в сегменте больших корпоративных сетей, а версии Gigabit Ethernet со скоростями передачи 10, 40 и 100 Гбит/с на основе ВОЛС даже проникли в сегмент транспортных ТКС.

В зависимости от скорости передачи данных и передающей среды существует несколько вариантов технологии. Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех ниже перечисленных вариантах.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных, используя авто определение скорости и дуплексности, для достижения наилучшего соединения между двумя устройствами. Если авто определение не срабатывает, скорость подстраивается под сеть, и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10BASE-T и 100BASE-TX, а порт Ethernet 10/100/1000 – что он поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T.

Наиболее распространенными на сегодняшний день являются следующие стандарты Ehternet:

– 100BASE-T (основной, используемый в настоящий момент, часто называется Fast Ethernet) – общий термин для обозначения группы стандартов (включает в себя стандарты 100BASE-TX, 100BASE-

T4 и 100BASE-T2), использующих в качестве среды передачи данных витую пару категории UTP-5. Витая пара является самым распространенным физическим стандартом Ethernet сети. Расположение контактов при использовании витой пары UTP-5 и разъёма RJ-45 приведен на рис. 4.15. Длина сегмента до 100 м. Скорость передачи до 100 Мбит/с.

– 1000BASE-T (часто называется Gigabit Ethernet) – стандарт, использующий витую пару UTP категорий 5e или 6. В передаче данных участвуют все 4 пары. Скорость передачи данных – 250 Мбит/с по одной паре (всего до 1000 Мбит/с). Длина сегмента до 100 м.

В технологии Ethernet 100BASE-TX используется 8-контактный разъем (RJ-45) для витых пар UTP и STP или специальный оптоволоконный соединитель. Сравнительный анализ характеристик различных стандартов 100 BASE приведен в таблицах 4.1 – 4.3.

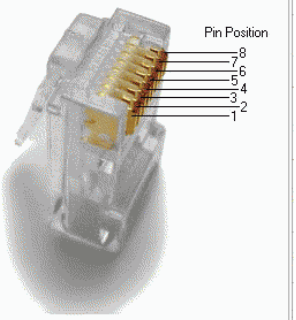
Pin	Connection 1 pair	Connection 2 pair	Connection 1	Connection 2	Pins on plug face (jack is reversed)
1	2	3	white/orange stripe	white/green stripe	
2	2	3	orange solid	green solid	
3	3	2	white/green stripe	white/orange stripe	
4	1	4	blue solid	white/brown stripe	
5	1	4	white/blue stripe	brown solid	
6	3	2	green solid	orange solid	
7	4	1	white/brown stripe	blue solid	
8	4	1	brown solid	white/blue stripe	

Рис. 4.15. Расположение контактов при использовании витой пары UTP-5 и разъема RJ-45

Таблица 4.1 – Максимальные размеры логического кабельного сегмента

Тип повторителя	Витые пары	Оптическое волокно
Один сегмент ЭВМ-ЭВМ	100 м	412 м
Один повторитель класса I	200 м	272 м
Один повторитель класса II	200 м	320 м
Два повторителя класса II	205 м	228 м

Таблица 4.2 – Типовые задержки для различных устройств Fast Ethernet

Сетевое устройство	Задержка [нс]
Повторитель класса I	700
Повторитель класса II (порты T4 и TX/FX)	460
Повторитель класса II (все порты T4)	340
Сетевая карта T4	345
Сетевая карта TX или FX	250

За счет использования повторителей и мостов возможна организация сетей Ethernet сложной конфигурации. Типовой вариант использования мостов и повторителей приведен на рис. 4.16, а требования к параметрам отдельных сегментов (на рис. 4.16) приведены в таблице 4.3.

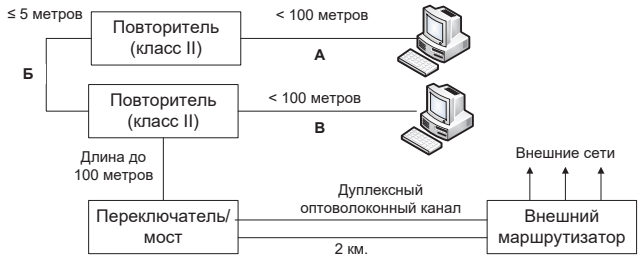


Рис. 4.16. Типовой вариант использования мостов и повторителей в сети Ethernet Fast Ethernet

Таблица 4.3 – Требования к параметрам отдельных сегментов на рис. 4.16

Тип кабеля А (категория)	Тип кабеля В (категория)	Класс повторителя	Макс. длина кабеля А	Макс. длина кабеля В	Макс. диаметр сети
5, 4, 3 (TX, FX)	5, 4, 3 (TX, FX)	I или II	100 м	100 м	200 м
5 (TX)	Оптоволокно	I	100 м	160,8 м	260,8 м
3 или 4 (T4)	Оптоволокно	I	100 м	131 м	231 м
Оптоволокно	Оптоволокно	I	136 м	136 м	272 м
5 (TX)	Оптоволокно	II	100 м	208,8 м	308,8 м
3 или 4 (T4)	Оптоволокно	II	100 м	204 м	304 м
Оптоволокно	Оптоволокно	II	160 м	160 м	320 м

4.7.4. Перспективные стандарты технологии Ethernet

Перспективные вариантами развития технологии Ethernet двигаются по пути наращивания скорости передачи, а также путем адаптации как к существующей кабельной инфраструктуре на основе витых пар UTP/STP, так и использования одно- и многомодовых ВОЛС.

2500BASE-T (стандарт IEEE 802.3bz) – инициативная разработка компаний Cisco и Broadcom по созданию стандарта Ethernet со скоростью, промежуточной между 1 и 10 Гбит/с. Целесообразность создания этого стандарта обусловлена необходимостью использовать существующую кабельную инфраструктуру UTP-5e на расстояниях до 100 м, предоставляя гигабитные скорости подключения для Wi-Fi маршрутизаторов, поддерживающих скорости 1 Гбит/с (802.11ac Wave 2, 802.11ad, 802.11ax, LiFi), и невозможность использования 10 Гбит/с стандартов Ethernet по кабелям UTP категорий 5e и 6. Обеспечивает скорость 2,5 Гбит/с с применением кабелей UTP-5e и 5 Гбит/с на кабелях категории UTP-6 расстояниях до 100 м.

10GBASE-T (стандарт 802.3-2018). Использует экранированную витую пару STP. Расстояние передачи — до 100 м. В отличие от предыдущих стандартов Ethernet, в 10-гигабитных вариантах Ethernet определены только полнодуплексные связи по схеме «точка-точка», которые обычно подключаются к сетевым коммутаторам. Топологии с общей шиной и алгоритмами CSMA здесь более не поддерживаются. Также, в отличие от предыдущих поколений стандартов Ethernet, не реализована полудуплексная работа и не поддерживаются репитеры (повторители). Обеспечивает скорость 10 Гбит/с на расстояние до 100 м при применении кабелей категории UTP-6a и на расстояние до 55 м – на кабелях категории UTP-6. Кабельная инфраструктура для 10GBASE-T обратно совместима с гигабитным стандартом 1000Base-T, что позволяет производить постепенное обновление оборудования. Оборудование 10GBASE-T способно работать в стандарте 1000Base-T, используя автоматическое определение скорости. Внедрение локальных сетей 10 гигабитного Ethernet 10GBASE-T происходит медленнее, чем с предыдущими стандартами Ethernet. По состоянию на 2012 г. цена коммутаторов Ethernet 10GBASE-T в несколько раз выше, чем коммутаторов для гигабитных Ethernet 1000BASE-T, что препятствуют их более широкому внедрению, хотя цена за гигабит пропускной способности в случае Ethernet 10GBASE-T в несколько раза ниже, чем для Ethernet 1000BASE-T.

40GBASE и 100GBASE – технологии Ethernet обеспечивающие передачу данных со скоростями до 40 и 100 Гбит/с соответственно, по одномодовому и многомодовому ВОЛС. Данные технологии активно конкурируют с традиционными технологиями SDH и OTH при построении транспортных ТКС. Возможные скорости передачи и максимальные длинны сегментов указаны для этих технологий указаны в таблице 4.4. Задача передачи сигнала со скоростями 40 и 100 Гбит/с по оптическому кабелю типа OM3 на 100 м (стандарты 40GBASE-SR4 и 100GBASE-SR10) была решена с использованием волн около 850 нм, сходной с таковой в стандарте 10GBASE-SR. Передача сигнала со скоростью 40 Гбит/с по печатным платам (например, объединительным платам корзин для блейд-серверов) на расстояния до 1 м (40GBASE-KR4) реализуется использованием 4 линий стандарта 10GBASE-KR. Работа на расстояниях 10 и 40 км реализуется с

использованием многомодовых оптических линий на четырёх разных длин волн (около 1310 нм) и использует оптические элементы со скоростью передачи данных 25 Гбит/с (для 100GBASE-LR4 и 100GBASE-ER4) и 10 Гбит/с (для 40GBASE-LR4).

Таблица 4.4 – Технологии Gigabit Ethernet 40GBASE и 100GBASE

Дальность распространения, в зависимости от физической среды	Технологии серии 40GBASE	Технологии серии 100GBASE
минимум 1 м по объединительной плате	40GBASE-KR4	
минимум 10 м по медному кабелю	40GBASE-CR4	100GBASE-CR10
минимум 100 м по многомодовому ВОЛС категории OM3	40GBASE-SR4	100GBASE-SR10
минимум 125 м по многомодовому ВОЛС категории OM4	40GBASE-SR4	100GBASE-SR10
минимум 10 км по одномодовому ВОЛС	40GBASE-LR4	100GBASE-LR4
минимум 40 км по одномодовому ВОЛС		100GBASE-ER4

Терабитный Ethernet (TbE) – условное понятие для обозначения будущих стандартов Ethernet, работающих на скоростях выше 100 Гбит/с. В частности, в 2017 г. был принят стандарт P802.3bs, обеспечивающий скорости 200 и 400 Гбит/с, за счет использования подходов, сходных со стандартом 100GBASE. В 2016 г. несколько производителей сетевого оборудования уже начали поставки собственных проприетарных компонентов для организации 200- и 400-гигабитных Ethernet сетей. При появлении одиночных приемопередатчиков на 100 Гбит/с возможно удвоение скоростей Ethernet до 800 Гбит/с. Также не исключается создание комплектов для достижения 1 Тбит/с или 1,6 Тбит/с путем комплексирования 10 или 16 параллельных 100-гигабитных приемопередатчиков (10 или 16 оптических трактов).

Материал главы 4 основан на информации, приведенной в работах [1, 12] и в материалах Интернет-ресурса [14].

5. Технологии беспроводных сетей передачи данных

5.1. Общая характеристика беспроводных технологий

Беспроводные технологии – класс технологий связи, которые служат для передачи данных на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации используются, в основном, радиоволны, реже – инфракрасное излучение или лазерное излучение. В настоящее время существует множество беспроводных технологий, как правило, известных по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth и т.д.

Каждая технология обладает определёнными характеристиками, которые определяют её область применения (рис. 5.1).

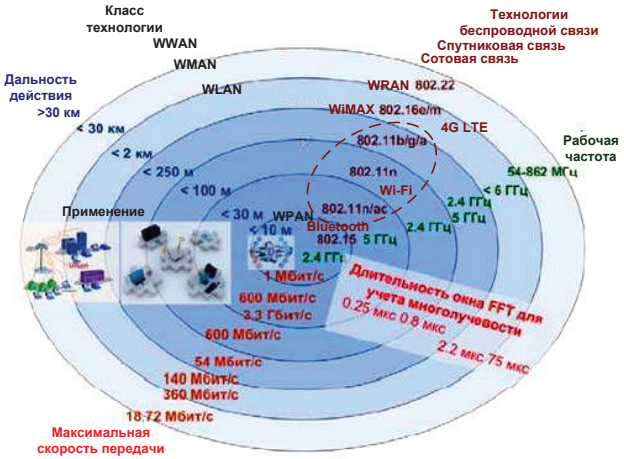


Рис. 5.1. Сравнение дальности и скорости передачи различных беспроводных технологий

Беспроводные технологии по дальности действия и применению можно классифицировать на:

- беспроводные технологии радиочастотной идентификации. Дальность действия до 0,1-10 м. Примеры технологий: RFID; NFC;
- беспроводные технологии телефонии. Дальность действия до 10-30 м. Пример технологии – DECT;
- беспроводные персональные сети/технологии (WPAN – Wireless Personal Area Networks). Дальность действия до 100 м. Примеры технологий: Bluetooth; ZigBee; UWB; IrDa;

– беспроводные локальные сети (WLAN – Wireless Local Area Networks). Дальность действия от 100 м до 2 км. Пример технологии – Wi-Fi;
– беспроводные сети городского масштаба (WMAN – Wireless Metropolitan Area Networks). Дальность действия до 5-30 км. Примеры технологий: WiMAX; LoRa; NB-IoT; NB-Fi; ZigBee-MAN;
– беспроводные сотовые сети (Cellular WWAN – Cellular Wireless Wide Area Network). Дальность действия: одной базовой станции (БС) – до 5-20 км; сети – неограниченно на территории развертывания БС. Примеры технологий: TETRA, HSPA, UMTS, LTE;
– беспроводные глобальные сети (WWAN – Wireless Wide Area Network). Дальность действия – по всей поверхности Земли. Пример технологии – спутниковая связь (например, Iridium, Starlink, Inmarsat и др.); системы глобальной КВ-радиосвязи (например – Navtex).

По топологии беспроводные технологии классифицируют на:
– «точка-точка».
– «точка-многоточка».

Наиболее распространенные стандарты беспроводных технологий приведены в таблице 5.1.

Таблица 5.1 – Сравнительный анализ технологий беспроводной связи

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Bluetooth v. 1.1	802.15.1	WPAN	до 1 Мбит/с	до 10 м	2,4 ГГц
Bluetooth v. 2.0	802.15.3	WPAN	до 2,1 Мбит/с	до 100 м	2,4 ГГц
Bluetooth v. 3.0	802.11	WPAN	3-24 Мбит/с	до 100 м	2,4 ГГц
UWB	802.15.3a	WPAN	110-480 Мб/с	до 10 м	7,5 ГГц
ZigBee	802.15.4	WPAN	20-250 Мбит/с	1-100 м	0,868, 0,915, 2,4 ГГц
Инфракрасная линия связи	IrDa	WPAN	до 16 Мбит/с	от 5 до 50 см, односторонняя связь – до 10 м	Инфракрасное излучение
Wi-Fi	802.11a	WLAN	до 54 Мбит/с	до 300 м	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбит/с	до 300 м	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбит/с	до 300 м	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбит/с (в перспективе до 600 Мбит/с)	до 300 м	2,4-2,5 или 5 ГГц
WiMAX	802.16d	WMAN	до 75 Мбит/с	25-80 км	1,5-11 ГГц
WiMAX	802.16e	Mobile WMAN	до 40 Мбит/с	1-5 км	2,3-13,6 ГГц

Технология	Стандарт	Использо-вание	Пропускная способность	Радиус действия	Частоты
WiMAX 2	802.16m	WMAN; Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	120-150 км	до 11 ГГц
WRAN	802.22	WMAN	до 22 Мбит/с	до 100 км	54-862 МГц
LTE	3GPP LTE 4G	Cellular WWAN	до 100 Мбит/с	до 3,2-20 км	0,45, 0,8, 0,9, 1,8, 2,1, 2,6 ГГц
LTE Advanced	3GPP LTE Advanced	Cellular WWAN	до 1 Гбит/с	до 3,2-20 км	0,45, 0,8, 0,9, 1,8, 2,1, 2,6 ГГц

5.2. Сети Wi-Fi

5.2.1. Общий обзор технологии Wi-Fi

IEEE 802.11 – стандарт связи, описывающий локальные компьютерные сети, построенные на основе беспроводных технологий. Пользователям этот стандарт более известен под наименованием Wi-Fi, фактически являющимся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Стандарт Wi-Fi использует технологию случайного множественного доступа абонентов CSMA/CA, аналогичную технологии CSMA/CD, которая используется в сетях Ethernet. Основными рабочими диапазонами Wi-Fi являются 2,4 ГГц (2412-2472 МГц), 5 ГГц (5160-5825 МГц) и 6-7 ГГц (5955-7115 МГц). Сигнал Wi-Fi сети может передаваться на километры даже при низкой мощности передачи, но для приема Wi-Fi сигнала с обычного Wi-Fi маршрутизатора на большом расстоянии нужна антенна с высоким коэффициентом усиления (например, параболическая антенна).

В настоящее время IEEE 802.11b/g/n – самые распространённые стандарты Wi-Fi, на базе которых построено большинство беспроводных локальных сетей. Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Принятая в 1999 г. первая версия стандарта IEEE 802.11b предусматривала использование не лицензируемого диапазона частот 2,4 ГГц, обеспечивая скорость передачи до 11 Мбит/с. Третья версия стандарта – IEEE 802.11g была утверждена в 2002 г. Она предусматривала использование диапазона частот 2,4 ГГц, обеспечивая скорость передачи до 54 Мбит/с. Четвертая версия стандарта 802.11n, утверждённая в 2009 г, обеспечивает скорость передачи до 150 Мбит/с на одну антенну и до 600 Мбит/с на пакет 4-х MIMO (Multiple Input Multiple Output) антенн. Технологии MIMO, впервые использованной в стандарте 802.11n, заключается в том, что при передаче и приеме данных используется несколько антенн. Разные антенны могут передавать как одни и те же данные (в этом случае повышается надежность передачи данных), так и

различные потоки данных (при этом увеличивается скорость передачи данных). Максимально в 802.11n поддерживается схема 4×4. Это означает, что на передающей и приемной стороне используется по 4 антенны.

Развитие стандартов Wi-Fi активно продолжается. В 2014 г. была принята 5-я версия стандарта IEEE 802.11ac, которая обеспечивает скорость передачи от 433 Мбит/с до 6,7 Гбит/с на пакет из 8-ми MIMO антенн. В 2021 г. была принята 6-я версия стандарта IEEE 802.11ax, которая обеспечивает скорость передачи до 11 Гбит/с на пакет из 8-ми MIMO антенн. В данном стандарте вводится режим ортогонального частотного мультиплексирования OFDMA (Orthogonal Frequency Division Multiple Access) для улучшения спектральной эффективности и расширение используемых типов сигнально-кодовых конструкций до 1024QAM R=5/6. Шестая версия стандарта Wi-Fi позволит в 4 раза увеличить среднюю пропускную способность, относительно 802.11ac, за счёт более эффективного использования спектра и улучшений для более плотного развёртывания сетей. Устройства данного стандарта позволят работать как в уже существующих диапазонах 2,4 ГГц и 5 ГГц, так и в дополнительных полосах частот в диапазонах от 1 до 7 ГГц.

Развертывание Wi-Fi рекомендуется там, где внедрение кабельной инфраструктуры было невозможно или экономически нецелесообразно. В нынешнее время во многих организациях используется Wi-Fi, так как сеть обеспечивает приемлемую скорость работы при этом пользователи могут перемещаться между точками доступа по территории покрытия сети Wi-Fi.

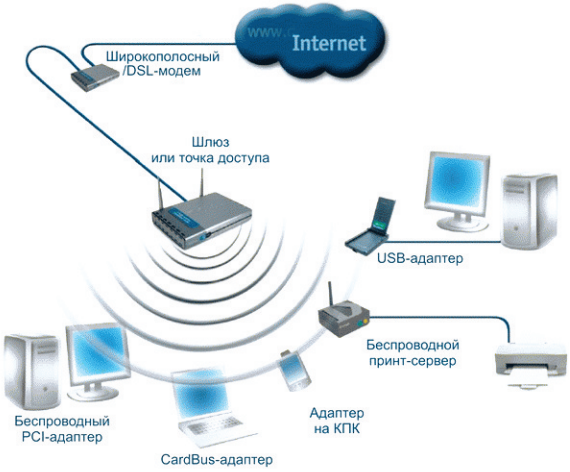


Рис. 5.2. Схема доступа абонентов к WiFi сети

Обычно схема сети Wi-Fi содержит не менее одной точки доступа и несколько абонентов (рис. 5.2). Также возможно подключение двух абонентов в режиме точка-точка (Ad-hoc), без использовании точки доступа, когда абоненты соединяются посредством Wi-Fi сетевых адаптеров

«напрямую». Точка доступа передаёт свой идентификатор сети SSID (Service Set Identifier) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия 2-х точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала.

5.2.2. Преимущества и недостатки Wi-Fi

Преимущества Wi-Fi:

- технология позволяет развернуть сеть без прокладки кабеля, может уменьшить стоимость развёртывания и расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями;
- Wi-Fi-устройства широко распространены на рынке, при этом устройства разных производителей могут взаимодействовать на базовом уровне сервисов;
- Wi-Fi сети поддерживают роуминг, поэтому абонент может перемещаться в пространстве без прерывания связи, переходя от одной точки доступа к другой;
- Wi-Fi – это набор глобальных стандартов. В отличие от сотовых телефонов, Wi-Fi оборудование может работать в разных странах по всему миру.

Недостатки Wi-Fi:

- в диапазоне Wi-Fi работает множество других устройств, таких как устройства Bluetooth, микроволновые печи и др., что ухудшает электромагнитную совместимость;
- скорость передачи данных в сети Wi-Fi всегда ниже заявленной максимальной скорости т.к. реальная скорость зависит от: количества подключенных абонентов, доли служебного трафика, наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.;
- частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы; во многих европейских странах разрешены два дополнительных канала, которые запрещены в США, в России точки беспроводного доступа, а также адаптеры Wi-Fi вне помещения, а также точки доступа с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации;
- самый популярный стандарт шифрования WEP (Wired Equivalent Privacy) в Wi-Fi может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости ключа). Несмотря на то, что новые устройства поддерживают более совер-

шенный протокол шифрования данных WPA (Wi-Fi Protected Access), многие старые точки доступа не поддерживают его и требуют замены. Принятие стандарта IEEE 802.11i (WPA2) в 2004 г. сделало доступной более безопасную схему, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями;

– Wi-Fi имеют ограниченный радиус действия. Типичный домашний Wi-Fi маршрутизатор стандарта 802.11b/g имеет радиус действия 45 м в помещении и 90 м снаружи. Микроволновая печь или зеркало, расположенные между устройствами Wi-Fi, ослабляют уровень сигнала. Расстояние зависит также от частоты;
– наложение сигналов закрытой или использующей шифрование точки доступа и открытой точки доступа, работающих на одном или соседних каналах может помешать доступу к открытой точке доступа. Эта проблема может возникнуть при большой плотности точек доступа, например, в больших многоквартирных домах, где многие жильцы ставят свои точки доступа Wi-Fi.

5.2.3. Особенности регламентации работы оборудования Wi-Fi в России

В России использование Wi-Fi без разрешения на использование частот от Государственной комиссии по радиочастотам (ГКРЧ) возможно для организации сетей внутри зданий, закрытых складских помещений и производственных территорий с использованием Wi-Fi устройств малого радиуса действия в диапазонах 2,4 ГГц (2400-2483,5 МГц, каналы 1-13), 5 ГГц (5150-5350 и 5650-5850 МГц, каналы 32-68 и 132-169), а также 60 ГГц (57-66 ГГц, каналы 1-25). Использование беспроводной сети Wi-Fi для организации фиксированного беспроводного доступа к данным в закрытых помещениях и на воздушных судах возможно без оформления индивидуальных разрешений ГКРЧ на использование частот и без регистрации радиоэлектронных средств в Роскомнадзоре при использовании передатчиков мощностью до 100 мВт (20 дБм) в полосах 2400-2483,5 МГц (стандарты IEEE 802.11, 802.11b, 802.11g, 802.11n, 802.11ax) и мощностью до 200 мВт (23 дБм) в полосах 5150-5350 МГц и 5650-5850 МГц (стандарты 802.11a/n/ac/ax) с шириной канала до 160 МГц и спектральной плотностью до 10 мВт/МГц, а также диапазона 57-66 ГГц (стандарты IEEE 802.11ad/ay WiGig) при мощности передатчика до 10 Вт (40 дБм) и ширине канала 2160 МГц. Правила использования Wi-Fi были приняты в 2010 г., тогда же было разрешено использование диапазона 6 ГГц (IEEE 802.11ax), в дополнение к диапазонам 2,4 и 5 ГГц. В 2015-2016 гг. в этих диапазонах было одобрено использование технологий 802.11ac и 802.11ad, а в 2020 г. – технологии 802.11ax.

Для легального использования беспроводной сети Wi-Fi вне зданий (например, организации радиоканала между двумя соседними домами), а

также для использования в закрытых помещениях части диапазона 5 ГГц (5470-5650 и 5850-5990 МГц, каналы 96-128 и 171-196) и диапазона 6 ГГц (5945-6425 МГц, каналы 1-93), необходимо проведение экспертизы об электромагнитной совместимости (ЭМС) оборудования с действующими и планируемыми радиосетями и получение разрешения на использование частот в Роскомнадзоре.

За нарушение правил использования радиоэлектронных средств предусматривается ответственность по статьям 13.3 и 13.4 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ). Так, в июле 2006 г. несколько компаний в Ростове-на-Дону были оштрафованы за эксплуатацию открытых сетей Wi-Fi (хот-спотов).

5.3. Технология WiMAX

5.3.1. Общий обзор технологии WiMAX

WiMAX (от англ. **W**orldwide **I**nteroperability for **M**icrowave **A**ccess) – беспроводная технология, разработанная с целью предоставления услуг связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным наименованием, так как это не технология, а название форума, на котором Wireless MAN и был согласован). Название «WiMAX» было создано WiMAX Forum – организацией, которая была основана в июне 2001 г. с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL». Технология WiMAX объединила в себя достижения не только более технологий беспроводного доступа Wi-Fi, но и технологии сотовых сетей поколения 3G и 4G. Именно это позволяет обеспечить скорости передачи данных до 1 Гбит/с на базовую ячейку не только стационарным, но и мобильным абонентам, двигающимся на скоростях до 150 км/ч.

Технология WiMAX подходит для решения следующих задач (рис. 5.3):

- соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета;
- обеспечения беспроводного широкополосного доступа в сеть Интернет, как альтернативы выделенным линиям FTTx и DSL;
- предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг на больших территориях;
- создание мобильных точек доступа, не привязанных к географическому положению;
- развертывания систем удалённого мониторинга объектов, систем обмена данными с объектами IoT (Internet of Things).

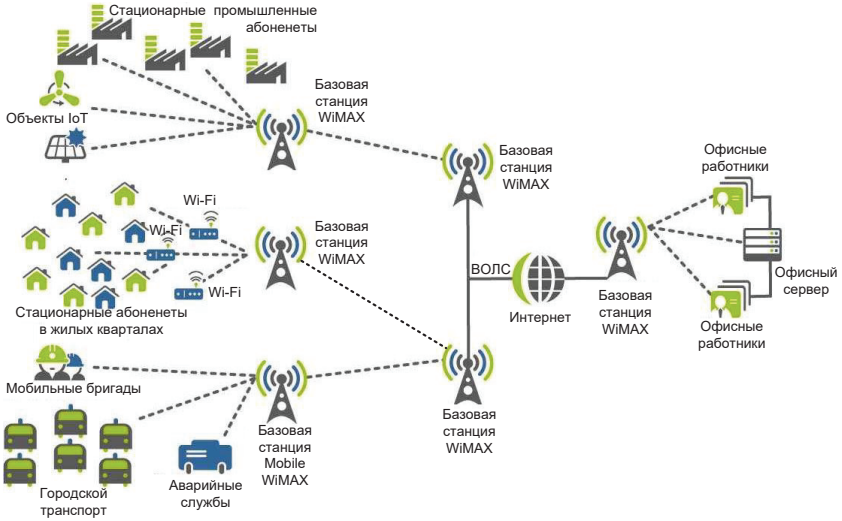


Рис. 5.3. Вариант развертывания и применения технологии WiMAX

WiMAX – это система дальнего действия, покрывающая километры пространства, которая обычно использует лицензированные спектры частот (хотя возможно и использование нелицензированных частот) для предоставления соединения с Интернетом типа «точка-точка» провайдером конечному пользователю. Разные стандарты семейства 802.16 обеспечивают разные виды доступа, от мобильного (схож с передачей данных с мобильных телефонов) до фиксированного (альтернатива проводному доступу, при котором беспроводное оборудование пользователя привязано к местоположению). Место систем WiMAX среди других технологий при оценке скорости информационного обмена и поддержки мобильных пользователей приведено на рис. 5.4.

Рис. 5.4. Место систем WiMAX среди других технологий

Технология WiMAX позволяет осуществлять доступ к сети на высоких скоростях, с гораздо большим покрытием, чем у WiFi сетей. Это позволяет использовать эту технологию в качестве «магистральных каналов», продолжением которых выступают традиционные DSL выделенные линии, а также локальные сети на основе технологий Ethernet и Wi-Fi. В результате подобный подход позволяет создавать масштабируемые высокоскоростные сети класса WMAN в рамках городов.

5.3.2. Фиксированная и мобильная версии технологии WiMAX

Фиксированная и мобильная версии WiMAX существенно отличаются друг от друга. Хотя ряд базовых требований совпадает, нацеленность технологий на разные ниши привела к созданию фактически 2-х отдельных версий стандарта. Поэтому WiMAX-системы, основанные на версиях e и d стандарта IEEE 802.16, практически несовместимы.

Технология 802.16-2004 (известна также как 802.16d или стационарный/фиксированный WiMAX) использует ортогональное частотное мультиплексирование OFDM, поддерживая фиксированный доступ в зонах прямой видимости. Пользовательские устройства представляют собой стационарные модемы для установки вне и внутри помещений. Под эту технологию отведены диапазоны 3,5 и 5 ГГц. Данная технология конкурирует или дополняет технологии проводного широкополосного доступа FTTx и DSL.

Технология 802.16-2005 (известна также как 802.16e или mobile WiMAX) оптимизирована для поддержки мобильных пользователей. Применяется масштабируемый OFDM-доступ (SOFDMA), возможна работа при наличии либо отсутствии прямой видимости. Используются частотные диапазоны: 2,3-2,5; 2,5-2,7; 3,4-3,8 ГГц. Конкурентами 802.16e являются все мобильные технологии сотовой 3G/4G (например, HSDPA и LTE).

Фиксированный WiMAX позволяет обслуживать только «статичных» абонентов, а мобильный – ориентирован на работу с пользователями, передвигающимися со скоростью до 150 км/ч. Мобильность означает наличие функций роуминга и «бесшовного» переключения между базовыми станциями при передвижении абонента (как это происходит в сетях сотовой связи). В частном случае, мобильный WiMAX может применяться и для обслуживания фиксированных пользователей.

Перспективным направлением развития технологии WiMAX является переход к стандарту 802.16m. Данный стандарт предполагает обратную совместимость с 802.16e и будет обладать пиковой пропускной способностью свыше 150 Мбит/с в соте радиусом до 5 км в нисходящем канале в полосе 20 МГц с задержкой передачи пакета данных IP-уровня не выше 10 мс. При увеличении радиуса соты до 30 км будет происходить постепенная деградация качества. Но 802.16m должна сохранять работоспособность на удалении от базовой станции до 100 км (когда ограничения про-

диктованы принципиальным барьером в виде теплового шума). При этом скорость мобильного абонента может составлять до 350 км/ч.

5.3.3. Технология WiMAX в России

В России сеть мобильного WiMAX стандарта 802.16e была развернута «Скартелом» под брендом Yota. К 2022 г. все крупные компании России перестали внедрять новые сети WiMAX и перешли на LTE, оставив только сопровождение уже развернутых сетей. При этом диапазон 3,4-3,8 ГГц был высвобожден под будущее использование сетей поколения 5G.

5.4. Технология LTE

5.4.1. Общий обзор технологии LTE

LTE (от англ. Long-Term Evolution, часто обозначается как 4G LTE) – стандарт беспроводной высокоскоростной передачи данных, разработанный консорциумом 3GPP, для мобильных телефонов и других терминалов 4-го поколения мобильной связи (4G).

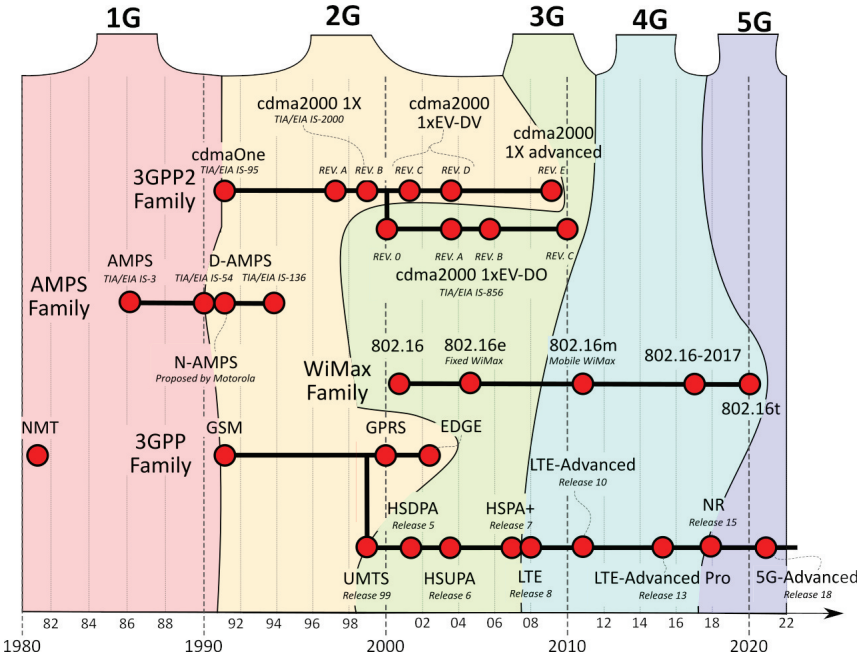


Рис. 5.5. Развитие беспроводных технологий мобильных сотовых сетей

LTE основана на сетевых технологиях прошлых поколений GSM (1G), EDGE (2G) и UMTS/HSPA+ (3G), обеспечивая увеличение пропускной

способности за счет использования нового метода цифровой обработки сигналов и модуляции. Технология LTE является несовместимым с 2G и 3G по сигналам и протоколам. Внедрение LTE началось с конца 2009 г.

5.4.2. Физический радиоинтерфейс технологии LTE

Технология LTE позволяет обеспечить скорость загрузки на абонентский терминал до 3 Гбит/с с задержкой передачи до 2 мс. LTE поддерживает полосы частот от 1,4 МГц до 20 МГц. Используется уплотнение каналов OFDMA, когда весь доступный спектр разбивается на поднесущие полосы частот, в которых передаются сигналы, ортогональные друг другу. В зависимости от используемой ширины канала общее количество поднесущих может быть 72, 180, 300, 600, 900 или 1200. Каждая из поднесущих может иметь свой вид модуляции. Для организации множественного доступа абонентов в «нисходящем» канале используется как частотное, так и временное разделение MF-TDMA за счет того, что одна часть поднесущих выделяется одному абоненту к кадре, другая часть – второму абоненту и т.д. В «восходящем» канале используется метод разделения SC-FDMA, кроме того в качестве дополнительной обработки сигнала используется преобразование Фурье. Как в «нисходящем» канале, так и в «восходящем» канале используются следующие виды модуляции: QPSK, 16QAM, 64QAM. Стандарт LTE также поддерживает технологию передачи MIMO (Multiple Input Multiple Output), которая позволяет существенно увеличить максимальную скорость передачи данных и значение спектральной эффективности. Суть технологии MIMO заключается в том, что при передаче и приеме данных используется несколько антенн с каждой стороны. Разные антенны могут передавать одни и те же данные, в этом случае повышается надежность передачи данных, но не скорость передачи. Также разные антенны могут передавать различные потоки данных, при этом увеличивается скорость передачи данных. Максимально в нисходящем канале технологией LTE поддерживается схема 4×4. Это означает, что на передающей и приемной стороне используется по 4 антенны.

Радиус действия базовой станции LTE зависит от мощности излучения, а максимальная скорость передачи данных зависит от частоты и удалённости абонента от базовой станции. Теоретический предел для скорости в 1 Мбит/с – от 3,2 км (2600 МГц) до 19,7 км (450 МГц). Базовые станции диапазона 800 МГц способны обеспечить такую скорость на расстоянии до 13,4 км. Диапазон 1800 МГц – наиболее используемый в мире для LTE т.к. он сочетает в себе высокую ёмкость и относительно большой радиус действия (6,8 км). Большинство операторов LTE работает в диапазонах 2600 МГц, 1800 МГц и 800 МГц (стандарт LTE-FDD).

5.4.3. Структура сети LTE

Сеть LTE представляет собой совокупность базовых станций eNB (Evolved NodeB или eNodeB), где соседние eNB соединены между собой интерфейсом X2. Интерфейсы X2 используются для организации хэндоверов абонентских станций UE (User Equipment) между соседними базовыми станциями eNB, в том числе и при балансировке нагрузки между ними. При этом интерфейсы X2 могут быть логическими, т.е. для их организации не обязательно реальное физическое соединение между eNB. Базовые станции eNB подключены к ядру сети EPC (Evolved Packet Core) посредством интерфейса передачи команд управления S1 (рис. 5.6) При этом в состав ядра сети EPC входят обслуживающие шлюзы S-GW (Serving Gateway), содержащие ПО управления сетью по протоколу MME (Mobility Management Entity).

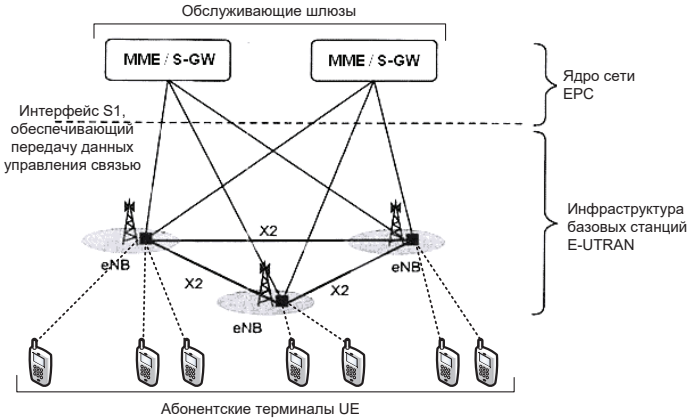


Рис. 5.6. Упрощенная архитектура сети LTE [15]

Радиоинтерфейс между абонентским терминалом UE и базовой станцией eNB описан в предыдущем подразделе.

Более подробно структура ядра EPC сети LTE приведена на рис. 5.7. Ядро сети EPC состоит из обслуживающих шлюзов S-GW, граничного шлюза сопряжения с пакетными сетями P-GW (Packet Data Network Gateway), системы управления по протоколу MME (Mobility Management Entity), связанной с обслуживающими шлюзами S-GW и базовыми станциями eNB сигнальными интерфейсами S1 (S1-U и S1-C). Интерфейс S1 поддерживает обмен данными между базовыми станциями eNB с обслуживающими шлюзами S-GW и системой сигнализации MME. Отметим, что eNB может иметь соединения с несколькими шлюзами S-GW.

Функциями базовой станции eNB в сети LTE являются:

– передачу трафика и сигналов сигнализации по радиоинтерфейсу абонентским терминалам UE;

– управление распределением радиоресурсов базовой станции eNB между абонентскими терминалами UE;
– обеспечение сквозной ретрансляции трафика от абонентских терминалов UE к обслуживающему шлюзу S-GW;
– поддержка синхронизации передач абонентских терминалов UE и контроль уровня помех в соте;
– шифрация и целостность передач по радиоинтерфейсу с абонентскими терминалами UE;
– выбор системы управления MME и организация сигнального обмена с ним,
– сжатие заголовков IP-пакетов;
– поддержка услуг мультимедийного вещания;
– организация управление антеннами по специальному интерфейсу, если базовой станцией eNB используется усилители мощности на антенной мачте.

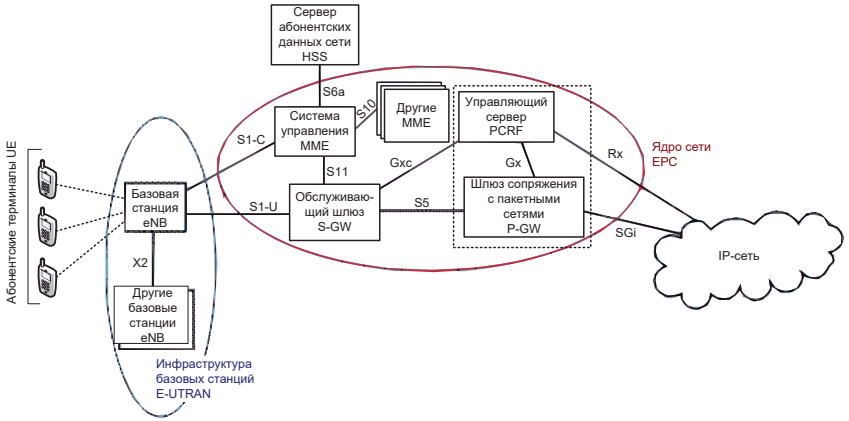


Рис. 5.7. Структура ядра EPC сети LTE [15]

Функциями обслуживающего шлюза S-GW в сети LTE является:
– маршрутизация передаваемых пакетов данных;
– обеспечение показателей качества обслуживания QoS (Quality of Service) предоставляемых услуг связи;
– буферизация пакетов для абонентских терминалов UE, пребывающих в состоянии Idle Mode;
– предоставление учетных данных для тарификации и оплаты оказанных услуг связи.

Шлюз S-GW является основным объектом, обеспечивающим мобильность абонентов UE. Каждого активного абонента UE обслуживает определенный шлюз S-GW. Теоретически абонент UE может быть связан с несколькими пакетными сетями; тогда ее будут обслуживать несколько шлюзов S-GW.

Шлюз сопряжения с пакетными сетями P-GW (Packet Data Network Gateway) организует «точку доступа» ядра сети EPC к внешним IP-сетям. Соответственно шлюз P-GW является граничным шлюзом для обеспечения передачи внешнего трафика. Если абонент UE имеет статический IP-адрес, то шлюз P-GW его активизирует. В случае, если абонент UE должен получить на время сеанса связи динамический IP-адрес, то шлюз P-GW запрашивает его с сервера DHCP (Dynamic Host Configuration Protocol) или сам выполняет необходимые функции DHCP, после чего обеспечивает доставку IP-адреса абоненту UE.

При обслуживании абонента в домашней сети функции шлюзов P-GW и S-GW могут выполнять как два разных, так и одно устройство. Интерфейс S5 представляет собой туннельное соединение GPRS или Proxy Mobile Ipv6. Если шлюзы P-GW и S-GW находятся в разных сетях (например, при обслуживании абонента UE в роуминге), то интерфейс S5 заменяют интерфейсом S8.

В состав ядра сети входит управляющий сервер PCEF (Policy and Charging Enforcement Function), который обеспечивает качество обслуживания внешних соединений через интерфейс Sgi, а также фильтрацию пакетов данных. Также сервер PCRF обеспечивает централизованное управление ресурсами сети, учет и тарификацию предоставляемых услуг. Как только появляется запрос на новое активное соединение, эта информация поступает на сервер PCRF. Он оценивает имеющиеся в его распоряжении ресурсы сети и направляет в шлюзы P-GW команды, устанавливающие требования к качеству услуг и к их тарификации.

Система управления MME (Mobility Management Entity) прежде всего поддерживает выполнение процедур обеспечения мобильности абонентов: обеспечение безопасности работы в сети при подключении абонентов UE, выбор шлюзов S-GW и P-GW. Система управления MME связана с сервером абонентских данных HSS (Home Subscriber Server) своей сети посредством интерфейса S6a. Интерфейс S10, соединяющий различные системы MME, позволяет обслуживать абонентов UE, при его нахождении в роуминге.

Сервер абонентских данных сети HSS представляет собой большую базу данных (БД) и предназначен для хранения служебной информации об абонентах:

- пользовательских идентификаторов, номеров и адресной информации;
- данных безопасности абонентов – информации для контроля доступа в сеть, аутентификации и авторизации;
- информации о местоположении абонента на межсетевом уровне, т.е. если даже абонент покинет текущую сеть LTE оператора, то в HSS сохранится информация о том в какую сеть он перешел для его поиска в случае входящего звонка;
- информация о профиле абонента.

Кроме того, сервер HSS генерирует данные, необходимые для осуществления процедур шифрования, аутентификации и т.п. Сеть LTE может включать один или несколько HSS. Количество HSS зависит от географической структуры сети и числа абонентов.

5.4.4. Технология LTE в составе сетей 4G в России

Первая сеть LTE в России была запущена ООО «Скартел» (бренд Yota) в 2011 г. в Новосибирске и состояла из 63 базовых станций. Первым среди операторов «большой тройки» технологию LTE запустил «МегаФон» в 2012 г. (так же в г. Новосибирске). По состоянию на 2019 г. сети LTE присутствуют в 85 регионах России покрывая зону проживания порядка 74% населения страны. Стоит учесть, что разные операторы предоставляют разный уровень покрытия – у многих операторов сети LTE развернуты только в городах и на наиболее оживленных транспортных магистралях.

5.5. Технология ZigBee

Zigbee – семейство сетевых протоколов верхних уровней OSI: уровня приложений и сетевого уровня, использующих услуги нижних уровней – канального и физического уровней, обеспечивающих формирование беспроводных низкоскоростных сетей с малым энергопотреблением: сетей IoT, сенсорных сетей, автоматизации жилья («Умный дом» и «Интеллектуальное здание»), медицинского оборудования, систем промышленного мониторинга и управления, а также бытовой электроники и «периферии» персональных компьютеров. Технология Zigbee ориентирована на применение, когда требуется гарантированная безопасная передача данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

Формирование сетей Zigbee регламентируются стандартом IEEE 802.15.4. Данная технология относится к классу технологий WPAN. Аналогом технологии Zigbee является Bluetooth, при этом Zigbee является более универсальной и лучшей технологией. Способность к самоорганизации и самовосстановлению связи, ячеистая (mesh) топология, защищённость, высокая помехоустойчивость, низкое энергопотребление и отсутствие необходимости получения частотного разрешения делают Zigbee сеть подходящей основой для беспроводной инфраструктуры систем IoT.

Стандарт Zigbee IEEE 802.15.4 был создан в мае 2003 г. К 2023 г. данный стандарт получил широкое распространение для обмена данными в промышленных/банковских сетях IoT, а также для устройств «умного дома» от Яндекса и Сбербанка.

Протокол Zigbee поддерживает узлы со включённым или с отключённым оповещением о присутствии в сети. В сети с выключенным оповещением о присутствии узлы Zigbee обычно являются включёнными постоян-

но, что требует дополнительного питания. Однако, это позволяет создавать гетерогенные Zigbee сети, в которых одни устройства постоянно принимают данные, в то время как другие передают данные только тогда, когда это необходимо. В сетях с оповещением о присутствии, узлы Zigbee сети передают периодические сообщения (маячки), которые подтверждают нахождение узлов в сети. Узлы могут находиться как в активном, так и в «спящем» состоянии, что снижает их энергопотребление. Интервалы сообщений-маячков в такой сети могут различаться от 15,36 мс до 786,432 с.

Рис. 5.8. Стек протоколов технологии Zigbee [14]

Данные передаются на частотах 2,4 ГГц (не лицензированная частота), 915 МГц (американский вариант) и 868 МГц (Европа). На частоте 2,4 ГГц есть 16 каналов Zigbee, при этом каждый канал имеет ширину в 5 МГц. Для передачи данных используется широкополосную модуляцию с прямым расширением спектра. Сигналы BPSK используются на частотах в 868 и 915 МГц, а сигналы OQPSK, передающие по 2 бита в символе, используется на частотах 2,4 ГГц. Скорость передачи данных составляет 250 кбит/с для каждого канала по 5 МГц на частоте 2,4 ГГц, 40 кбит/с – для каждого канала в диапазоне 915 МГц и 20 кбит/с – в диапазоне 868 МГц. Расстояние передачи – от 10 до 75 м. Максимальная выходная мощность передатчика – 1 мВт.

Протокол доступа абонентов к каналам ZigBee – случайный множественный доступ по CSMA/CA. Особенность технологии Zigbee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Протоколы маршрутизации в сетях Zigbee построены на алгоритме AODV и NeuRFon, предназначен-

ных для образования Ad-hoc сетей (децентрализованная беспроводная сеть, образованная случайными абонентами).

Применение сетей Zigbee в России в частотном диапазоне 2400-2483,5 МГц не требует получения частотных разрешений и дополнительных согласований (Решение ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001). Решения ГКРЧ постоянно обновляются, решение от 07.05.2007 № 07-20-03-001 давно претерпело несколько раз изменения, однако его смысл остается тем же.

5.6. Технология Bluetooth

Bluetooth (от слов англ. blue – синий и tooth – зуб) – технология организации беспроводных персональных сетей, обеспечивающих низкоскоростной обмен данными с ближней зоне между такими устройствами, как компьютеры, ноутбуки, мобильные телефоны, интернет-планшеты, принтеры, цифровые фотоаппараты, мыши, клавиатуры, джойстики, наушники, гарнитуры и др. Реальная дальность действия Bluetooth – до 16-20 м (при декларируемой разработчиками максимальной дальности до 100 м), до 1,5 км начиная с версии Bluetooth 5. Стандарт Bluetooth обеспечивает реальную скорость передачи данных 1-3 Мбит/с.

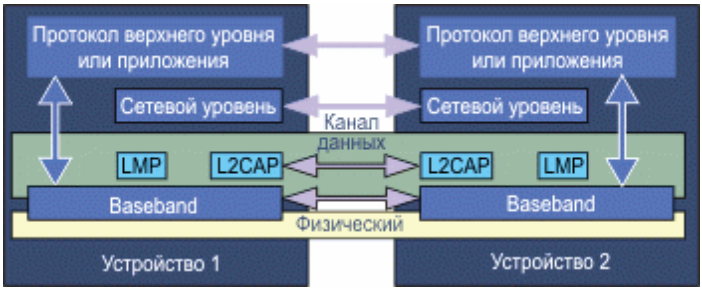


Рис. 5.9. Взаимодействие устройств в технологии Bluetooth [14]

Протокол LMP (Link Management Protocol) отвечает за управления соединениями (рис. 5.9). Протокол L2CAP отвечает за формирование пакетов, деление на кадры и сборку пакетов (нижележащий протокол Baseband позволяет иметь пакеты не длиннее 341 байта), которые в данном стандарте могут достигать размера 64 кбайт. Протокол Baseband управляет использованием буферов приемника/передатчика в режиме FIFO.

На физическом уровне Bluetooth осуществляется радиосвязь в диапазоне 2,402-2,48 ГГц. Применяется метод расширения спектра псевдослучайной перестройкой частоты (ППРЧ), который обеспечивает устойчивость связи к широкополосным помехам. Из-за использовании ППРЧ несущая частота сигнала скачкообразно меняется 1600 раз в секунду, совершая «прыжки» по 79 рабочим частотам шириной в 1 МГц. Последовательность переключения между частотами для каждого соединения является

псевдослучайной, определяются главным узлом (master) и известна только узлу-передатчику и узлу-приёмнику, которые каждые 625 мкс (длительность одного временного слота) синхронно перестраиваются с одной несущей частоты на другую. Протокол Bluetooth поддерживает соединение типа «точка-точка» и «точка-многоточка». Таким образом, если узел организует несколько соединений «точка-точка/многоточка», то они не мешают друг другу т.к. совершают «прыжки» по разным частотам. Режим ППРЧ является также составной частью системы защиты конфиденциальности передаваемых данных в Bluetooth. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно. Мощность передатчика – не более 0,0025 Вт.

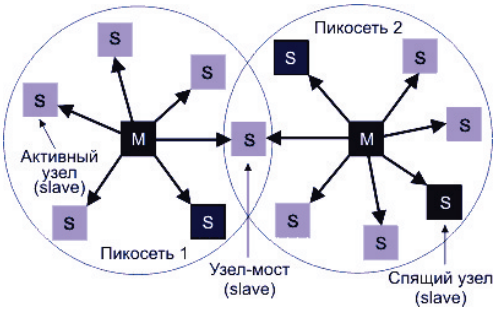


Рис. 5.10. Две пикосети Bluetooth, образующие рассеянную сеть [14]

Сетевой уровень технологии Bluetooth позволяет формировать пикосети (piconet), состоящие из одного главного узла (master) и до 7 клиентских узлов (slave), размещенных в радиусе 10 м (рис. 5.10). Все узлы такой пикосети работают на одной частоте и разделяют общую совокупность каналов. В одной достаточно большой комнате могут располагаться несколько пикосетей. Эти сети могут связываться друг с другом через узлы-мосты. Пикосети, объединенные вместе составляют рассеянную (scatternet) сеть. Поскольку в каждой пикосети имеется свой master, последовательность переключения их частот не будут совпадать. Если пикосети взаимодействуют друг с другом, это приводит к снижению пропускной способности. Устройство BlueTooth может выступать в качестве клиентского узла (slave) в нескольких пикосетях, но главным узлом (master) может быть только в одной пикосети. Кроме 7 активных клиентских узлов главный узел может поддерживать до 255 пассивных (спящих) узлов (переведенных главным узлом в режим пониженного энергопотребления).

Материал главы 5 основан на информации, приведенной в работе [1] и в материалах Интернет-ресурсов [14, 15].

6. Организация информационного обмена между сетями

6.1. Функции сетевого уровня в модели OSI

В эталонной модели OSI в функции сетевого уровня входит решение следующих задач:

- передача пакетов между конечными узлами в составных сетях;
- выбор маршрута передачи пакетов, наилучшего по некоторому критерию;
- согласование разных протоколов и технологий канального уровня, использующихся в отдельных подсетях большой составной сети.

Протоколы сетевого уровня реализуются, как правило, в виде программных модулей и выполняются на конечных узлах – компьютерах, называемых *хостами*, а также на промежуточных узлах – *маршрутизаторах*, называемых *шлюзами*, в случае если через этот маршрутизатор к составной сети подключается отдельная подсеть.

Основная идея введения сетевого уровня состоит в следующем. Сеть в общем случае рассматривается как совокупность нескольких сетей и называется *составной сетью* или *интерсетью* (internetwork или internet). Сети, входящие в составную сеть, называются *подсетями* (subnet), *составляющими сетями* или просто сетями (рис. 6.1).

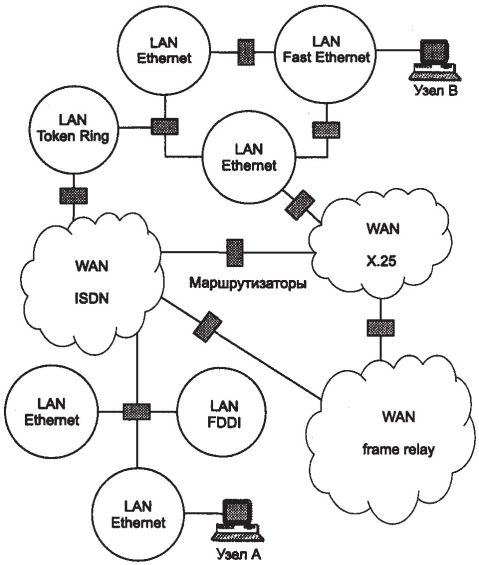


Рис. 6.1. Архитектура составной сети и ее подсети

Подсети соединяются между собой маршрутизаторами. Компонентами составной сети могут являться как локальные, так и глобальные сети. Внутренняя структура каждой сети на рис. 6.1 не показана, так как она не имеет значения при рассмотрении сетевого протокола.

Все узлы в пределах одной подсети взаимодействуют, используя единую для них сетевую технологию обмена пакетами и адресации узлов. Так, в составную сеть, показанную на рис. 6.1, входит несколько подсетей разных технологий: локальные сети Ethernet, Fast Ethernet, Token Ring, FDDI и глобальные сети frame relay, X.25, ISDN. Каждая из этих технологий достаточна для того, чтобы организовать взаимодействие всех узлов в своей подсети, но не способна построить информационную связь между произвольно выбранными узлами, принадлежащими разным подсетям, например между узлом А и узлом В на рис. 6.1.

Многие технологии локальных сетей (Ethernet, Token Ring, FDDI, Fast Ethernet и др.) используют одну и ту же систему адресации узлов на основе MAC-адресов. Адреса, присвоенные узлам в соответствии с технологиями подсетей, называют локальными. Чтобы сетевой уровень мог выполнить задачу межсетевого обмена информацией, ему необходима собственная система адресации, не зависящая от способов адресации узлов в отдельных подсетях, которая позволила бы универсальным и однозначным способами идентифицировать любой узел составной сети на сетевом уровне.

Естественным способом формирования сетевого адреса является уникальная нумерация всех подсетей составной сети и нумерация всех узлов в пределах каждой подсети. Таким образом, сетевой адрес представляет собой пару: номер сети (подсети) и номер узла.

В качестве номера узла может выступать некоторое число, никак не связанное с локальной технологией, которое однозначно идентифицирует узел в пределах данной подсети (что характерно для стека протоколов TCP/IP).

Если проводить аналогию между взаимодействием разнородных сетей и перепиской людей из разных стран, то сетевая информация – это индекс страны, добавленный к адресу письма, написанному на одном из сотни языков земного шара, например на санскрите. И даже если это письмо должно пройти через множество стран, почтовые работники которые не знают санскрита, прочтут понятный им индекс страны-адресата, который подскажет, через какие промежуточные страны лучше передать письмо, чтобы оно кратчайшим путем попало в Индию. А уже там работники местных почтовых отделений смогут прочитать точный адрес, указывающий город, улицу, дом и доставить письмо адресату, так как адрес написан на языке и в форме, принятой в данной стране.

Заголовок сетевого уровня должен содержать информацию, необходимую для успешного перехода пакета из сети одного типа в сеть другого типа:

- *номер сети-адресата*. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты при любой их топологии, в том числе альтернативные маршруты, если они имеются, что не умеют делать мосты и коммутаторы.
- *номер фрагмента пакета*, необходимый для успешного проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами пакетов;
- *время жизни пакета*, указывающее, как долго он путешествует по интерсети, это время может использоваться для уничтожения «заблудившихся» пакетов;
- *качество услуги* – критерий выбора маршрута при межсетевых передачах, например, узел-отправитель может потребовать передать пакет с максимальной надежностью, возможно, в ущерб времени доставки.

Когда две или более сети организуют совместную транспортную службу, то такой режим взаимодействия обычно называют межсетевым взаимодействием.

6.2. Адресация на сетевом уровне модели OSI

Стек протоколов TCP/IP является на настоящий момент наиболее распространенным протоколом сетевого и транспортного уровней. Поэтому реализацию конечных протоколов данных уровней OSI рассмотрим на их примере.

6.2.1. Адресация адресов в TCP/IP сетях

В стеке TCP/IP используются 3 типа адресов:

1) локальные адреса (называемые также аппаратными адресами или MAC-адресами);
2) символьные доменные имена;
3) IP-адреса.

В терминологии стека TCP/IP под *локальным адресом* (MAC-адресом) понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом более глобальной составной сети.

Если подсетью составной сети является локальная сеть, то локальный адрес – это MAC-адрес сетевого адаптера и сетевого интерфейса маршрутизатора. MAC-адреса назначаются производителями оборудования и являются уникальными. Для всех существующих технологий ло-

кальных сетей MAC-адрес имеет формат 6 байт, например: 11-AO-17-3D-BC-01.

Символьные имена в IP-сетях называются *доменными* и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке (справа – на лево):

- сначала простое имя конечного узла;
- затем имя группы узлов (например, имя организации);
- затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU – Россия, UK – Великобритания, SU – США).

Примером доменного имени может служить имя base2.sales.zil.ru. Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная служба доменных имен DNS (Domain Name System), которая устанавливает соответствие между доменными именами и IP-адресами узлов, на основе создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также *DNS-именами*.

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. IP-адрес состоит из 2-х частей: номера сети и номера узла, при этом в качестве признака номера сети выступает маска сети.

Когда протокол IP был стандартизирован в 1981 г., его спецификация требовала, чтобы каждое устройство, подключенное к сети, имело уникальный 32-битный адрес. Этот адрес делится на 2 части. Первая часть адреса идентифицирует сеть, в которой располагается устройство. Вторая часть однозначно идентифицирует само устройство. Такая схема создает двухуровневую адресную иерархию, которая показана на рис. 6.2.

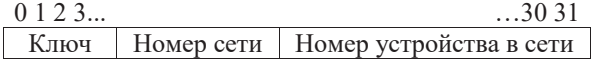


Рис. 6.2. Двухуровневая адресная иерархия

Поле номера сети в адресе так же называется *сетевым префиксом*, так как первая часть каждого IP-адреса идентифицирует номер сети. Все станции определенной сети используют один и тот же сетевой префикс, но при этом должны иметь уникальные номера узлов. Аналогично две любые станции, расположенные в разных сетях, должны иметь различные сетевые префиксы, но при этом они могут иметь одинаковые номера узлов.

IP-адрес имеет длину 4 или 6 байтов и обычно записывается в виде чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 – традиционная десятичная

форма представления адреса, а 10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

Маска – это число, которое используется в паре с IP-адресом; при этом двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети (сетевой префикс). Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность.

Для обеспечения гибкости в присвоении адресов компьютерным сетям разработчики определили, что адресное пространство протокола IP должно быть разделено на 3 различных класса – A, B и C. Каждый из этих основных классов фиксирует границу между сетевым префиксом и номером устройства в различных точках 4-байтного IP-адреса.

Таблица 6.1 – Диапазоны значений адресов 3-х классов

Класс адреса	Диапазоны значений
A	1. XXX.XXX.XXX–126. XXX.XXX.XXX
B	128.0.XXX.XXX–191.255.XXX.XXX
C	192.0.0.XXX–223.255.255.XXX

Для стандартных классов сетей маски имеют следующие значения:

– класс A:
  11111111. 00000000. 00000000. 00000000 (255.0.0.0);
– класс B:
  11111111. 11111111. 00000000. 00000000 (255.255.0.0);
– класс C:
  11111111. 11111111. 11111111. 00000000 (255.255.255.0).

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

IP-адрес:	129.64.134.5	10000001. 01000000. 10000110. 00000101
Маска:	255.255.128.0	11111111. 11111111. 10000000. 00000000

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Например, если рассмотренный выше адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов.

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов.

– Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет; этот режим используется только в некоторых сообщениях ICMP.

– Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.
– Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным. сообщением* (limited broadcast).
– Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети 192.190.21.0. Такая рассылка называется *широковещательным сообщением* (broadcast).

Таблица 6.2 – Зарезервированные IP-адреса

IP-адрес		Примечания
Все биты установлены в «0»		Данное устройство
Номер сети	Все биты номераравны 0	Данная IP-сеть
Все биты равны 0	Номер устройства	Устройство в данной IP-сети
Все биты установлены в «1»		Все устройства в данной IP-сети
Номер сети	Все биты номера равны 1	Все устройства в указанной IP-сети
127 (десятичное)	Что-нибудь (обычно 1)	Адрес обратной связи

При адресации необходимо учитывать те ограничения, которые вносятся особым назначением некоторых IP-адресов. Так, ни номер сети, ни номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Отсюда следует, что максимальное количество узлов, приведенное в таблице для сетей каждого класса, на практике должно быть уменьшено на 2.

Особый смысл имеет IP-адрес, первый сокет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины т. е. образуется как бы «петля». Данные не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127. Этот адрес имеет название *loopback*.

6.2.2. DHCP – протокол автоматического назначения IP-адресов

Назначение IP-адресов узлам сети даже при не очень большом размере сети может представлять для администратора утомительную процедуру. *Протокол автоматического назначения конфигурации DHCP* (Dy-

namic Host Configuration Protocol) освобождает администратора от этих проблем, автоматизируя процесс назначения IP-адресов.

DHCP может поддерживать способ автоматического динамического распределения адресов, а также более простые способы ручного и автоматического статического назначения адресов. Протокол DHCP работает в соответствии с моделью клиент-сервер.

Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес клиенту. Предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое *временем аренды*, что дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру. Основное преимущество DHCP – автоматизация рутинной работы администратора по конфигурированию адресации TCP/IP на каждом компьютере. Иногда динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой превышает количество имеющихся в распоряжении администратора IP-адресов.

6.2.3. Отображение доменных имен на IP адреса. Служба DNS

При идентификации аппаратного и программного обеспечения компьютеров в сетях протокол TCP/IP использует IP-адреса. Поэтому для доступа к сетевому ресурсу вполне достаточно указать его IP-адрес. Например, команда ftp://192.45.66.17 будет устанавливать сеанс связи с нужным ftp-сервером, а команда http://203.23.106.33 откроет начальную страницу на web-сервере. Однако пользователи обычно предпочитают работать с символьными именами. Следовательно, в сетях TCP/IP должны существовать символьные имена хостов и механизм для установления соответствия между символьными именами и IP-адресами.

В ОС, которые первоначально разрабатывались для работы в локальных сетях, пользователи всегда работали с символьными именами компьютеров. Так как локальные сети состояли из небольшого числа компьютеров, то использовались так называемые *плоские имена*, состоящие из последовательности символов, не разделенных на части. Примерами таких имен являются: NW1_1, mail2, MOSCOW_SALES_2 и т.д.

Для стека TCP/IP, рассчитанного в общем случае на работу в больших территориально-распределенных сетях, подобный подход оказывается неэффективным.

Для эффективной организации именования компьютеров в больших сетях применяют *иерархически составные имена*. В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную

структуру, допускающую использование в имени произвольного количества составных частей (рис. 6.3).

Иерархия доменных имен аналогична иерархии имен файлов, принятой во многих популярных файловых системах. *Дерево имен* начинается с *корня*, обозначаемого здесь точкой (**.**). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т.д. Младшая часть имени соответствует конечному узлу сети.

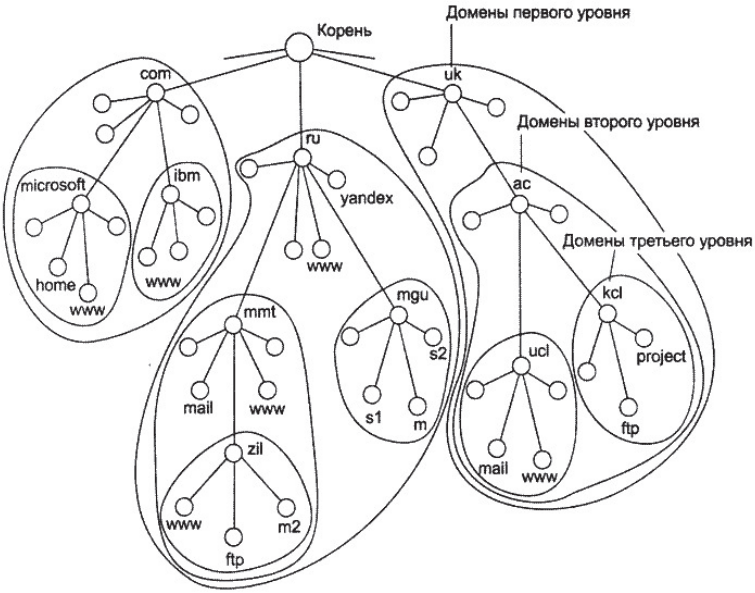


Рис. 6.3. Иерархия пространства доменных имен

В отличие от имен файлов, при записи которых сначала указывается самая старшая составляющая, затем составляющая более низкого уровня и т.д., запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей. Составные части доменного имени отделяется друг от друга точкой. Например, в имени partnering.microsoft.com составляющая partnering является именем одного из компьютеров в домене microsoft.com.

Необходимо подчеркнуть, что компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь совершенно различные IP-адреса, принадлежащие к различным сетям и подсетям. Например, в домен mgu.ru могут входить хосты с адресами 132.13.34.15, 201.22.100.33 и 14.0.0.6. Доменная система имен реализована в сети Интернет, но она может работать и как автономная система имен в крупной корпоративной сети, использующей стек TCP/IP, но не связанной с Интернетом.

В сети Интернет корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций – следующие обозначения:

- edu – образовательные (например, mitedu);
- gov – правительственные организации (например, nsf.gov);
- org – некоммерческие организации (например, fidonet.org);
- net – организации, поддерживающие сети (например, nsf.net).

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы, в качестве которой используется *система доменных имен DNS.*

DNS – это централизованная служба, основанная на распределенной базе отображений «доменное имя – IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты:

- DNS-серверы поддерживают распределенную базу отображений «доменное имя – IP-адрес»;
- DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными

Существуют 2 основные схемы разрешения DNS-имен.

1. В первом варианте работу по поиску IP-адреса координирует DNS-клиент:

- DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;
- DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;
- DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена, и т.д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

В такой схеме взаимодействия клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

2. Во втором варианте реализуется рекурсивная процедура:

– DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;
– если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;
– если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему DNS-серверу, поэтому схема называется косвенной или рекурсивной. Практически все DNS-клиенты используют рекурсивную процедуру.

6.3. Маршрутизация на сетевом уровне OSI

6.3.1. Принципы обмена сообщениями между сетями

Важнейшей задачей сетевого уровня является маршрутизация – передача пакетов между двумя конечными узлами в составной сети.

Рассмотрим принципы маршрутизации на примере составной сети, изображенной на рис. 6.4. В сети 20 маршрутизаторов объединяют 18 сетей в общую сеть; S1, S2, ... , S20 – это номера сетей. Маршрутизаторы имеют по нескольку портов (по крайней мере, по два), к которым присоединяются сети. Каждый порт маршрутизатора можно рассматривать как отдельный узел сети: он имеет собственный сетевой адрес и собственный локальный адрес в той подсети, которая к нему подключена. Например, маршрутизатор под номером 1 имеет 3 порта, к которым подключены сети S1, S2, S3. На рис. 6.4 сетевые адреса этих портов обозначены как M1(1), M1(2) и M1(3). Порт M1(1) имеет локальный адрес в сети с номером S1, порт M1(2) – в сети S2, а порт M1(3) – в сети S3. Таким образом, маршрутизатор можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть. Как единое устройство маршрутизатор не имеет ни отдельного сетевого адреса, ни какого-либо локального адреса.

В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами.

Маршрут – это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения. Так, пакет, отправленный из узла A в узел B, может пройти через маршрутизаторы 17,

12, 5, 4 и 1 или маршрутизаторы 17, 13, 7, 6 и 3. Нетрудно найти еще несколько маршрутов между узлами A и B.

Задачу выбора маршрута из нескольких возможных решают маршрутизаторы, а также конечные узлы. Маршрут выбирается на основании имеющейся у этих устройств информации о текущей конфигурации сети, а также на основании указанного критерия выбора маршрута. Обычно в качестве критерия выступает задержка прохождения маршрута отдельным пакетом или средняя пропускная способность маршрута для последовательности пакетов. Часто также используется весьма простой критерий, учитывающий только количество пройденных в маршруте промежуточных маршрутизаторов (хопов).

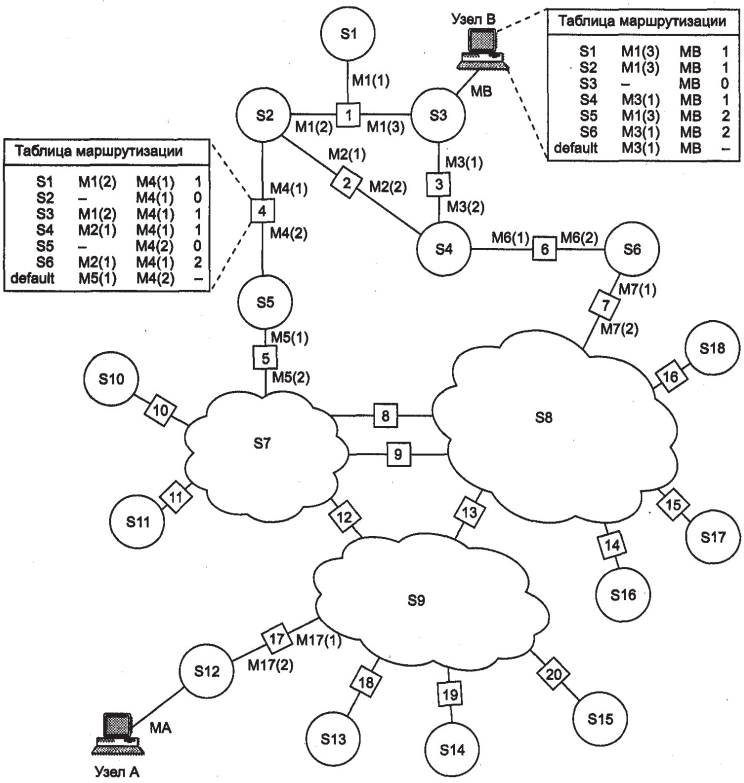


Рис. 6.4. Принципы маршрутизации в составной сети

Чтобы по адресу сети назначения можно было бы выбрать рациональный маршрут дальнейшего следования пакета, каждый конечный узел и маршрутизатор анализируют специальную информационную структуру, которая называется таблицей маршрутизации. Используя условные обозначения для сетевых адресов маршрутизаторов и номеров сетей в том ви-

де, как они приведены на рис. 6.4, посмотрим, как могла бы выглядеть таблица маршрутизации, например, в маршрутизаторе 4 (таблица 6.3).

В первом столбце таблицы перечисляются номера сетей, входящих в составную сеть. В каждой строке таблицы следом за номером сети указывается сетевой адрес следующего маршрутизатора (более точно – сетевой адрес соответствующего порта следующего маршрутизатора), на который надо направить пакет, чтобы тот передвигался по направлению к сети с данным номером по рациональному маршруту.

Таблица 6.3 – Таблица маршрутизации для маршрутизатора 4 на рис. 6.4

Номер сети назначения	Сетевой адрес следующего маршрутизатора	Сетевой адрес выходного порта	Расстояние до сети назначения
S1	M1(2)	M4(1)	1
S2	—	M4(1)	0 (подсоединена)
S3	M1(2)	M4(1)	1
S4	M2(1)	M4(1)	1
S5	—	M4(2)	0 (подсоединена)
S6	M2(1)	M4(1)	2
Default	M5(1)	M4(2)	—

Когда на маршрутизатор поступает новый пакет, номер сети назначения, извлеченный из поступившего кадра, последовательно сравнивается с номерами сетей из каждой строки таблицы. Строка с совпавшим номером сети указывает, на какой ближайший маршрутизатор следует направить пакет. Например, если на какой-либо порт маршрутизатора 4 поступает пакет, адресованный в сеть S6, то из таблицы маршрутизации следует, что адрес следующего маршрутизатора – M2(1), то есть очередным этапом движения данного пакета будет движение к порту 1 маршрутизатора 2.

Поскольку пакет может быть адресован в любую сеть составной сети, может показаться, что каждая таблица маршрутизации должна иметь записи обо всех сетях, входящих в составную сеть. Но при таком подходе в случае крупной сети объем таблиц маршрутизации может оказаться очень большим, что повлияет на время ее просмотра, потребует много места для хранения и т. п. Поэтому на практике число записей в таблице маршрутизации стараются уменьшить за счет использования специальной записи – «маршрутизатор по умолчанию» (default). Действительно, если принять во внимание топологию составной сети, то в таблицах маршрутизаторов, находящихся на периферии составной сети, достаточно записать номера сетей, непосредственно подсоединенных к данному маршрутизатору или расположенных поблизости, на тупиковых маршрутах. Обо всех же остальных сетях можно сделать в таблице единственную запись, указывающую на маршрутизатор, через который пролегает путь ко всем этим сетям. Такой маршрутизатор называется «маршрутизатором по умолчанию», а вместо номера сети в соответствующей строке помещается особая запись – default.

В нашем примере таким маршрутизатором по умолчанию для сети S5 является маршрутизатор 5, точнее его порт M5(1). Это означает, что путь из сети S5 почти ко всем сетям большой составной сети пролегает через этот порт маршрутизатора.

6.3.2. Протоколы маршрутизации

Для автоматического построения таблиц маршрутизации маршрутизаторы обмениваются информацией о топологии составной сети в соответствии со специальным служебным протоколом. Протоколы этого типа называются *протоколами маршрутизации*.

Во всех описанных выше примерах при выборе рационального маршрута определялся только следующий (ближайший) маршрутизатор, а не вся последовательность маршрутизаторов от начального до конечного узла. Таким образом, каждый маршрутизатор ответственен за выбор только одного шага маршрута, а окончательный маршрут складывается в результате работы всех маршрутизаторов, через которые проходит данный пакет (рис. 6.5). Такие протоколы называются *протоколами одношаговой маршрутизации*.

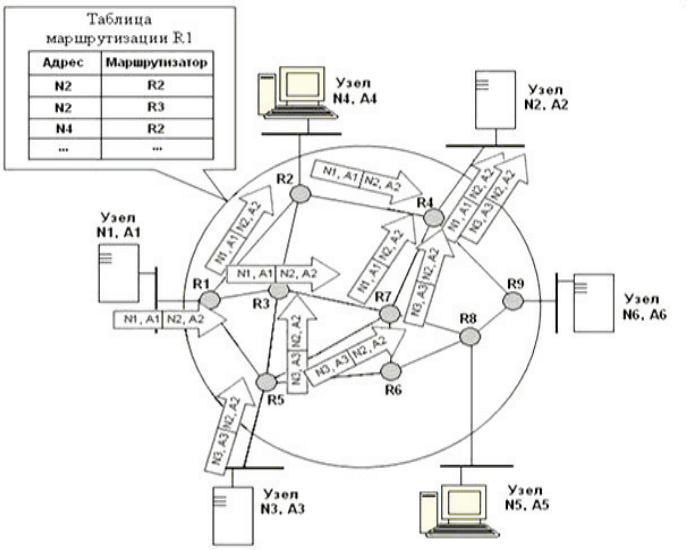


Рис. 6.5. Принцип одношаговой маршрутизации

Одношаговые протоколы в зависимости от способа формирования таблиц маршрутизации делятся на 3 класса:

1) протоколы фиксированной (или статической) маршрутизации;
2) протоколы простой маршрутизации;
3) протоколы адаптивной (или динамической) маршрутизации.

В протоколах *фиксированной маршрутизации* все записи в таблице маршрутизации являются статическими. Администратор сети сам решает, на какие маршрутизаторы надо передавать пакеты с теми или иными адресами, и вручную

В протоколах *простой маршрутизации* таблица маршрутизации либо вовсе не используется, либо строится без участия протоколов маршрутизации. Выделяют 3 типа простой маршрутизации:

- *случайная маршрутизация,* когда прибывший пакет посылается в первом попавшем случайном направлении, кроме исходного;
- *лавинная маршрутизация,* когда пакет широковещательно посылается по всем возможным направлениям, кроме исходного (аналогично обработке мостами кадров с неизвестным адресом);
- *маршрутизация по предыдущему опыту,* когда выбор маршрута осуществляется по таблице, но таблица строится по принципу моста путем анализа адресных полей пакетов, появляющихся на входных портах.

Самыми распространенными являются протоколы *адаптивной* (*или динамической*) *маршрутизации. Эти протоколы обеспечивают автоматическое обновление таблиц маршрутизации после изменения конфигурации сети.* Адаптивные протоколы позволяют всем маршрутизаторам собирать информацию о топологии связей в сети, оперативно отрабатывая все изменения конфигурации связей.

Адаптивные протоколы обмена маршрутной информацией делятся на 2 группы, каждая из которых связана с одним из следующих типов алгоритмов:

- дистанционно-векторные алгоритмы DVA (Distance Vector Algorithms);
- алгоритмы состояния связей LSA (Link State Algorithms).

В *алгоритмах дистанционно-векторного типа* каждый маршрутизатор периодически и широковещательно рассылает по сети вектор, компонентами которого являются расстояния (как правило – число хопов) от данного маршрутизатора до всех известных ему сетей. При получении вектора от соседа маршрутизатор наращивает расстояния до указанных в векторе сетей на расстояние до данного соседа. Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены к его портам) или из аналогичных объявлений других маршрутизаторов, а затем снова рассылает новое значение вектора по сети. В конце концов, каждый маршрутизатор узнает информацию обо всех имеющихся в интерсети сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях, В больших сетях они засоряют линии связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут

отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети. Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Вершинами графа являются как маршрутизаторы, так и объединяемые ими сети. «Широковещательная» рассылка (то есть передача пакета всем непосредственным соседям маршрутизатора) используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто. Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP.

Помимо одношаговой маршрутизации существует и прямо противоположный, многошаговый подход – *маршрутизация от источника* (Source Routing). В соответствии с ним узел-источник задает в отправляемом в сеть пакете полный маршрут его следования через все промежуточные маршрутизаторы (рис. 6.6). Это ускоряет прохождение пакета по сети, разгружает маршрутизаторы, но при этом большая нагрузка ложится на конечные узлы. Примерами протоколов, использующих маршрутизацию от источника, является протокол PNNI в составе стеков ATM и IP/MPLS.

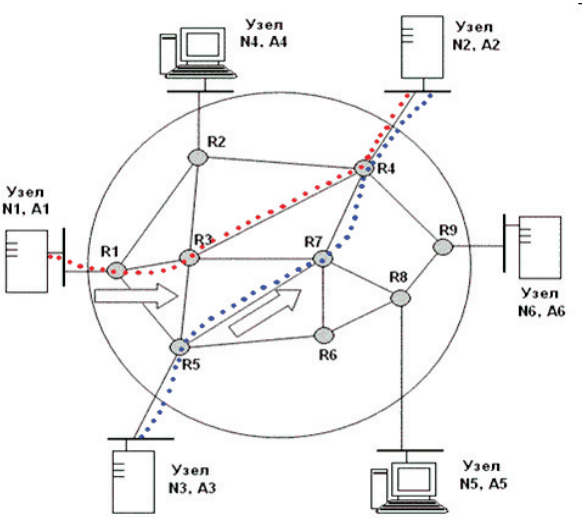


Рис. 6.6. Принцип маршрутизации от источника

6.3.3. Функции маршрутизатора

Основная функция маршрутизатора – чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, IP, AppleTalk или DECnet), и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Функции маршрутизатора могут быть разбиты на 3 группы в соответствии с уровнями модели OSI (рис. 6.7):

1) уровень интерфейсов;
2) уровень сетевого протокола;
3) уровень протоколов маршрутизации.

Рассмотрим эти группы более подробно.

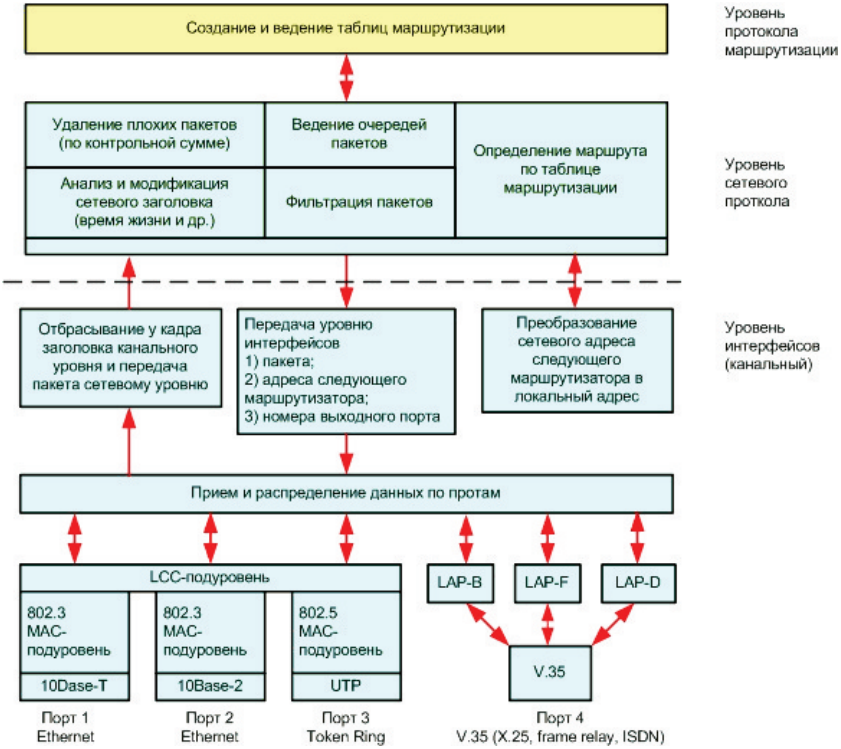


Рис. 6.7. Функциональная модель маршрутизатора

6.3.3.1. Уровень интерфейсов

На нижнем уровне (уровне интерфейсов) маршрутизатор, как и любое устройство, подключенное к сети, обеспечивает физический интерфейс со

средой передачи, включая согласование уровней электрических сигналов, линейное и логическое кодирование, оснащение определенным типом разъема.

В разных моделях маршрутизаторов часто предусматриваются различные наборы физических интерфейсов, представляющих собой комбинацию портов для подсоединения локальных и глобальных сетей. С каждым интерфейсом для подключения локальной сети неразрывно связан определенный протокол канального уровня – например, Ethernet, Token Ring, FDDI. Интерфейсы для присоединения к глобальным сетям чаще всего определяют только некоторый стандарт физического уровня, над которым в маршрутизаторе могут работать различные протоколы канального уровня. Например, глобальный порт может поддерживать интерфейс V.35, над которым могут работать протоколы канального уровня: LAP-B (используемый в сетях X.25), LAP-F (используемый в сетях frame relay), LAP-D (используемый в сетях ISDN). Разница между интерфейсами локальных и глобальных сетей объясняется тем, что технологии локальных сетей работают по собственным стандартам физического уровня, которые не могут, как правило, использоваться в других технологиях, поэтому интерфейс для локальной сети представляет собой сочетание физического и канального уровней и носит название по имени соответствующей технологии, например, интерфейс Ethernet.

Интерфейсы маршрутизатора выполняют полный набор функций физического и канального уровней по передаче кадра, включая получение доступа к среде (если это необходимо), формирование битовых сигналов, прием кадра, подсчет его контрольной суммы и передачу поля данных кадра верхнему уровню, в случае если контрольная сумма имеет корректное значение.

Как и любой конечный узел, каждый порт маршрутизатора имеет собственный аппаратный адрес (в локальных сетях MAC-адрес), по которому ему и направляются кадры, требующие маршрутизации, другими узлами сети.

Перечень физических интерфейсов, которые поддерживает та или иная модель маршрутизатора, является его важнейшей потребительской характеристикой. Маршрутизатор должен поддерживать все протоколы канального и физического уровней, используемые в каждой из сетей, к которым он будет непосредственно присоединен. На рис. 6.7 показана функциональная модель маршрутизатора с четырьмя портами, реализующими следующие физические интерфейсы: 10Base-T и 10Base-2 для двух портов Ethernet, UTP для Token Ring и V.35, над которым могут работать протоколы LAP-B, LAP-D или LAP-F, обеспечивая подключение к сетям X.25, ISDN или frame relay.

Кадры, которые поступают на порты маршрутизатора, после обработки соответствующими протоколами физического и канального уровней, освобождаются от заголовков канального уровня. Извлеченные из поля данных кадра пакеты передаются модулю сетевого протокола.

6.3.3.2. Уровень сетевого протокола

На уровне сетевого протокола извлекается из пакета заголовок сетевого уровня и анализируется содержимое его полей. Прежде всего, проверяется контрольная сумма, и если пакет пришел поврежденным, то он отбрасывается. Выполняется проверка, не превысило ли время, которое провел пакет в сети (время жизни пакета), допустимой величины. Если превысило – то пакет также отбрасывается. На этом этапе вносятся корректировки в содержимое некоторых полей, например, наращивается время жизни пакета, пересчитывается контрольная сумма.

На сетевом уровне выполняется одна из важнейших функций маршрутизатора – фильтрация трафика. Маршрутизатор, обладая более высоким «интеллектом», нежели мосты и коммутаторы, позволяет задавать и может отрабатывать значительно более сложные правила фильтрации. Пакет сетевого уровня, находящийся в поле данных кадра, для мостов/коммутаторов представляется неструктурированной двоичной последовательностью. Маршрутизаторы же, ПО которых содержит модуль сетевого протокола, способны производить разбор и анализ отдельных полей пакета. Они оснащаются развитыми средствами пользовательского интерфейса, которые позволяют администратору без особых усилий задавать сложные правила фильтрации. Они, например, могут запретить прохождение в корпоративную сеть всех пакетов, кроме пакетов, поступающих из подсетей этого же предприятия. Фильтрация в данном случае производится по сетевым адресам, и все пакеты, адреса которых не входят в разрешенный диапазон, отбрасываются. Маршрутизаторы, как правило, также могут анализировать структуру сообщений транспортного уровня, поэтому фильтры могут не пропускать в сеть сообщения определенных прикладных служб, например службы telnet, анализируя поле типа протокола в транспортном сообщении.

В случае если интенсивность поступления пакетов выше интенсивности, с которой они обрабатываются, пакеты могут образовать очередь. ПО маршрутизатора может реализовать различные дисциплины обслуживания очередей пакетов:

- FIFO (First Input First Output) – в порядке поступления по принципу «первый пришел – первым обслужен»,
- случайное раннее обнаружение перегрузок RED (Random Early Detection) – когда обслуживание идет по правилу FIFO, но при достижении длиной очереди некоторого порогового значения вновь поступающие пакеты отбрасываются;
- различные варианты приоритетного обслуживания.

К сетевому уровню относится и основная функция маршрутизатора – определение маршрута пакета. По номеру сети, извлеченному из заголовка пакета, модуль сетевого протокола находит в таблице маршрутизации строку, содержащую сетевой адрес следующего маршрутизатора, и номер порта, на который нужно передать данный пакет, чтобы он двигался в пра-

вильном направлении. Если в таблице отсутствует запись о сети назначения пакета и к тому же нет записи о маршрутизаторе по умолчанию, то данный пакет отбрасывается.

Перед тем как передать сетевой адрес следующего маршрутизатора на канальный уровень, необходимо преобразовать его в локальный адрес той технологии, которая используется в сети, содержащей следующий маршрутизатор. Для этого сетевой протокол обращается к *протоколу разрешения адресов* ARP. Протокол этого типа устанавливает соответствие между сетевыми и локальными адресами либо на основании заранее составленных таблиц, либо путем рассылки широковещательных запросов. Таблица соответствия локальных адресов сетевым адресам строится отдельно для каждого сетевого интерфейса. Протоколы разрешения адресов занимают промежуточное положение между сетевым и канальным уровнями.

С сетевого уровня пакет, локальный адрес следующего маршрутизатора и номер порта маршрутизатора передаются вниз, канальному уровню. На основании указанного номера порта осуществляется коммутация с одним из интерфейсов маршрутизатора, средствами которого выполняется упаковка пакета в кадр соответствующего формата. В поле адреса назначения заголовка кадра помещается локальный адрес следующего маршрутизатора. Готовый кадр отправляется в сеть.

6.3.3.3 Уровень протокола маршрутизации

Сетевые протоколы активно используют в своей работе таблицу маршрутизации, но ни ее построением, ни поддержанием ее содержимого не занимаются. Эти функции выполняют протоколы маршрутизации. На основании этих протоколов маршрутизаторы обмениваются информацией о топологии сети, а затем анализируют полученные сведения, определяя наилучшие по тем или иным критериям маршруты. Результаты анализа и составляют содержимое таблиц маршрутизации.

Помимо перечисленных выше функций, на маршрутизаторы могут быть возложены и другие функции, например операции, связанные с фрагментацией.

Материал главы 6 основан на обобщении информации, приведенной в работах [12, 16] и в материалах Интернет-ресурса [14]. Для более подробного изучения технологий адресации и маршрутизации на сетевом уровне рекомендуется обратиться к работе [12].

7. Обеспечение качества обслуживания при межсетевом обмене

7.1. Функции транспортного уровня в модели OSI

Транспортный уровень обеспечивает приложениям или верхним уровням стека (прикладному и сеансовому) передачу данных с той степенью качества, которая им требуется. Модель OSI определяет различные показатели качества и сервисы связи, предоставляемые транспортным уровнем.

Основными показателями качества обслуживания QoS, отслеживаемыми на транспортном уровне, являются:

- скорость передачи;
- своевременность передачи «из конца в конец»;
- джиттер (от англ «дрожание») – случайное изменение во времени своевременности прохождения сетевых пакетов «из конца в конец»;
- доля потерянных или безвозвратно искаженных пакетов при передаче «из конца в конец».

Основными функциями транспортного уровня, являются:

- преобразование транспортного адреса в сетевой;
- межоконечное мультиплексирование транспортных соединений в сетевые;
- установление и разрыв соединений, возможность восстановления прерванных соединений;
- межоконечное упорядочение блоков данных по отдельным соединениям;
- межоконечное обнаружение ошибок и необходимый контроль качества услуг;
- межоконечное обнаружение и исправление ошибок передачи, таких как искажение, потеря и дублирование пакетов;
- межоконечное сегментирование, объединение и сцепление;
- межоконечное управление потоками данных по отдельным соединениям, мультиплексирование нескольких соединений между различными прикладными протоколами через общий транспортный протокол;
- супервизорные функции;
- передача срочных служебных сообщений.

Термин «межоконечное» означает что протокол транспортного уровня обеспечивает QoS соединений и потоков данных «из конца в конец» всего маршрута – от узла-отправителя до узла-получателя.

Существует множество протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции, например, функции передачи данных без подтверждения приема, и

заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Примерами протоколов транспортного уровня в стеке TCP/IP являются довольно простые протоколы TCP и UDP, которые, как можно считать, реализуют архитектуру «Best Effort» – обслуживание с наилучшими усилиями, но без выделения дополнительной пропускной способности или использования тонких механизмов управления потоками трафика. В сетях с установлением соединений и поддержкой механизмов QoS (типа ATM и IP/MPLS) на транспортном уровне используются сложные архитектуры – IntServ и DiffServ.

7.2. Основные архитектуры обеспечения качества обслуживания в сетях

Основные архитектуры обеспечения QoS на транспортном уровне современных сетей (по мере усложнения и повышения эффективности) [17]:

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

Сравнение архитектур обеспечения QoS представлено в таблице 7.1. Рассмотрим суть данных архитектур более подробно далее.

Таблица 7.1 – Сравнение архитектур обеспечения QoS

Показатели сравнения	«Best Effort»	IntServ	DiffServ
Методы обеспечения QoS	Используются имеющееся ресурсы пропускной способности сети, в отдельных случаях – выделяется дополнительная пропускная способность	Приложение запрашивает необходимый уровень QoS, протокол RSVP резервирует необходимые ресурсы сети	Применение алгоритмов обработки пакетов в очередях узлов сети
Классы обслуживания	Нет	Предоставляет гарантийное обслуживание	На уровне приоритизации
Процедуры установления соединения	Нет	Да	Нет
Предоставление долговременных гарантий QoS	Нет	Нет (обеспечение QoS предоставляется только на время соединения)	Да (соответствующие параметры на узлах сети не сбрасываются во время отсутствия соединения)
Наличие служебного трафика во время соединения	Нет	Да (используется большой объем служебного трафика для процедур установления, поддержания и разъединения каждого соединения)	Отсутствует
Масштабируемость сети	Высокая	Низкая	Высокая
Сложность реализации	Низкая	Высокая	Низкая
Применение технологии на оборудовании различных производителей	Да	Да	Могут быть трудности
Возможная интеграция в сети MPLS	Да	Да	Да
Рекомендуемые области применения	На глобальных сетях, включая Интернет	В локальных и магистральных сетях для абонентов, использующих приложения с высокими требованиями QoS	На магистральных сетях, с минимальными требованиями QoS

7.2. Протоколы TCP и UDP, как реализация архитектуры «Best Effort» в сетях IP/TCP

TCP (*Transmission Control Protocol*) – протокол управления передачей в сетях и подсетях TCP/IP.

Для того чтобы обеспечить надежную доставку данных протокол TCP предусматривает установление логического соединения между узлом-отправителем и узлом-получателем данных. Это позволяет ему нумеровать пакеты, подтверждать их прием квитанциями, в случае потери пакетов организовывать повторные передачи, распознавать и уничтожать дубликаты, доставлять прикладному уровню пакеты в том порядке, в котором они были отправлены. Этот протокол позволяет объектам на узле-отправителе и на узле-получателе поддерживать обмен данными в дуплексном режиме. TCP дает возможность без ошибок доставить сформированный на одном из компьютеров поток байтов в любой другой компьютер, входящий в составную сеть. Каждое приложение отправляя свои данные работает с определенным портом протокола TCP. TCP делит поток байтов, поступающих от приложений, на сегменты и передает их нижележащему сетевому уровню, разделяющему сегменты на пакеты и организующему межсетевое взаимодействие (рис. 7.1). После того как эти фрагменты будут доставлены средствами сетевого уровня в пункт назначения, протокол TCP снова соберет их в непрерывный поток байтов и распределит по соответствующим приложениям.

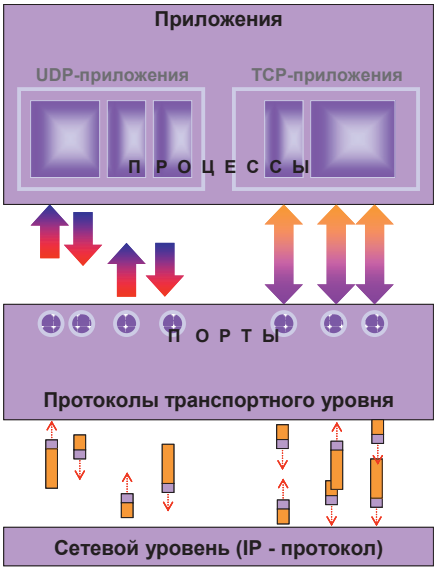


Рис. 7.1. Доступ приложений через порты к протоколам транспортного уровня в стеке TCP/IP

Протокол TCP обеспечивает три основных механизма управления передачей в соединениях в сетях TCP/IP:

– надёжная доставка;
– обнаружение и исправление ошибок передачи, таких как искажение, потеря и дублирование пакетов;
– адаптация скорости передачи к возможностям по приему узла-получателя и к надежности сети.

Протокол TCP обеспечивает надёжность доставки путем повторной пересылки недошедших по узла-получателя групп пакетов – сегментов. Каждый сегмент маркируется при помощи порядкового номера (sequence number). После отправки некоторого количества сегментов, TCP на узле-отправителе ожидает подтверждения от узла-получателя, в котором узел-получатель указывает порядковый номер следующего сегмента, который он желает получить. В случае, если такое подтверждение не получено, отправка сегмента автоматически повторяется. После некоторого количества неудачных попыток, TCP считает, что узел-получатель не доступен, и соединение разрывается. Таким образом, надёжная доставка в протоколе TCP не означает, что ваши данные дойдут до узла-получателя в случае сетевых сбоев. Она означает, что если сетевое соединение не разорвалась, то всё что узел-отправитель отправил будет доставлено узлу-получателю без потерь. Существует множество данных, критичных к потере любой порции информации. Например, если вы скачиваете приложение из интернета, то потеря одного байта будет означать, что вы не сможете воспользоваться тем что скачали. По этой причине многие протоколы уровня приложений используют для транспорта именно TCP.

Каждый сегмент на нижний уровнях стека TCP/IP обрабатывается индивидуально. Т.е. пакеты с целью балансировки нагрузки могут идти по сети разными путями, через разные промежуточные устройства, с разной скоростью. Таким образом узел-получатель, приняв их, может получить сегменты не в том порядке, в котором они отправлялись. В этом случае протокола TCP автоматически пересоберёт их в нужном порядке используя всё то же поле порядковых номеров и передаст после правильной сборки верхнеуровневым приложениям.

Адаптация скорости передачи к возможностям по приему узла-получателя и к надежности сети, производится благодаря механизму плавающего «окна». Механизм плавающего «окна» позволяет менять количество пересылаемых пакетов, на которые надо получать подтверждение от узла-получателя. Чем больше размер «окна», тем больший объём данных будет передан «за раз» до получения подтверждения (рис. 7.2). Для надёжных сетей подтверждения можно присылать редко, чтобы не увеличивать служебный трафик, поэтому размер окна в таких сетях автоматически увеличивается. Если же TCP обнаруживает, что данные теряются, размер окна автоматически уменьшается. Механизм плавающего «окна» позволяет TCP постоянно адаптироваться – увеличивать скорость пока пакеты уходят без

потерь и уменьшать, когда они не доходят. Таким образом, в любой момент времени размер «окна» будет более или менее адекватен состоянию сети.

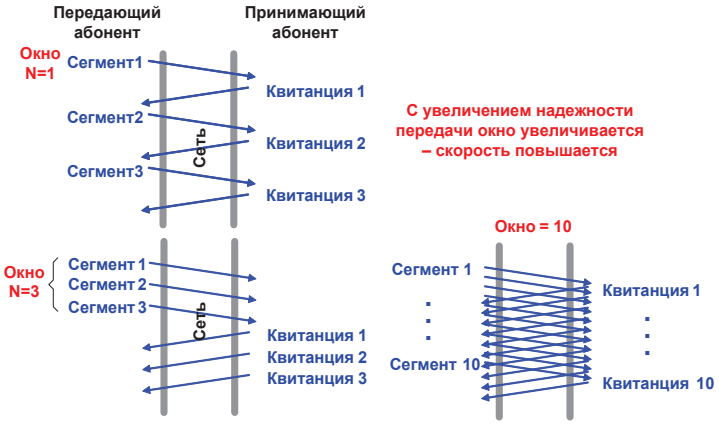


Рис. 7.2. Адаптация скорости передачи к возможностям по приему узла-получателя и к надежности сети, на основе механизма плавающего «окна»

При обмене данными узел-приёмник использует номер последовательности, содержащийся в получаемых пакета, для восстановления их исходного порядка. Приёмник уведомляет передающую сторону о номере последовательности, до которой он успешно получил данные, включая его в поле «номер подтверждения». Все получаемые данные, относящиеся к промежутку подтверждённых последовательностей, игнорируются. Если полученный сегмент содержит номер последовательности больший, чем ожидаемый, то данные из сегмента буферизируются, но номер подтверждённой последовательности не изменяется. Если впоследствии будет принят сегмент, относящийся к ожидаемому номеру последовательности, то порядок данных будет автоматически восстановлен исходя из номеров последовательностей в сегментах.

Протокол TPC в стеке TCP/IP реализует архитектуру «Best Effort» – обслуживание с наилучшими усилиями, но без выделения дополнительной пропускной способности и использования тонких механизмов управления потоками трафика.

Второй протокол этого уровня в стеке TCP/IP – протокол UDP (User Datagram Protocol – протокол пользовательских датаграмм). Протокол UDP использует простую модель передачи, без установления логического соединения, без использования «окон» для обеспечения надёжности, без функций упорядочивания или проверки целостности сегментов. В протоколе UDP сегменты могут прийти не по порядку, дублироваться или вовсе быть потерянными, но гарантируется, что если они придут, то в целостном

состоянии. Протокол UDP подразумевает, что проверка ошибок и исправление либо не нужны, либо должны исполняться в приложении. Чувствительные ко времени приложения (например, приложения потоковой видео- или аудио-трансляции) часто используют протокол UDP, так как для них предпочтительнее потеря пакетов, чем ожидание задержавшихся пакетов.

7.3. Архитектура интегрированного обслуживания IntServ

Протоколы TCP и UDP в стеке TCP/IP обеспечивают обслуживание «Best Effort» (обслуживание с наилучшими усилиями) при этом выдавая одинаковый приоритет всем соединениям и не делая различий при передачи информации различного типа (текст, данные, аудио, видео и т.д.). При этом при передаче по одной сети трафика потоковых мультимедийных приложений (VoIP, аудио- и видеоконференции и др.) или трафика с различными требованиями к пропускной способности, необходимо обеспечить возможность обработки и классификации различных типов сетевого трафика, либо в зависимости от требований к QoS, либо от его информационного содержания.

Архитектура интегрированного обслуживания Intserv, разработана в начале 1990-х гг., и основана на предварительном резервировании сетевых ресурсов и обеспечении сквозного (на всём пути передачи трафика «из конца в конец») качества обслуживания, гарантируя необходимую пропускную способность. Эту архитектуру также часто называют *жёстким QoS* в связи с предъявлением строгих требований к ресурсам сети.

Архитектура Intserv функционирует на основе протокола резервирования ресурсов RSVP (Resource ReSerVation Protocol). RSVP требует установления соединения и работает следующим образом: узел-отправитель до передачи данных, требующих определённого нестандартного качества обслуживания (например, постоянной полосы пропускания для передачи видеоинформации), посылает по сети специальное сообщение (path message) в формате протокола RSVP. Это сообщение содержит данные о типе передаваемой информации и требуемой пропускной способности. Оно передаётся между маршрутизаторами по всему пути от узла-отправителя до узла-получателя, при этом определяется последовательность маршрутизаторов, в которых необходимо зарезервировать определённую полосу пропускания. Маршрутизатор, получив такое сообщение, проверяет свои ресурсы с целью определения возможности выделения требуемой пропускной способности. При её отсутствии маршрутизатор запрос на предоставление пропускной способности отвергается, и данный маршрутизатор исключается из возможных маршрутизаторов устанавливаемого соединения. Если требуемая пропускная способность может быть выделена, то маршрутизатор поручает планировщику и классификатору пакетов зарезервировать часть своих ресурсов под обеспечение необходимого QoS, чтобы указанному соединению всегда предоставлялась требуемая пропускная способ-

ность, а затем передаёт сообщение следующему маршрутизатору вдоль пути. В результате, по всему пути от узла-отправителя до узла-получателя резервируется необходимая пропускная способность с целью обеспечения запрашиваемого качества обслуживания. После завершения передачи данных соединение разрывается, а зарезервированные ресурсы пропускной способности в маршрутизаторах высвобождаются.

Архитектура Intserv реализует следующие функции обеспечения QoS (рис. 7.3):

- контроль доступа трафика в сеть;
- классификация пакетов;
- планирование обработки пакетов;
- управление очередями.

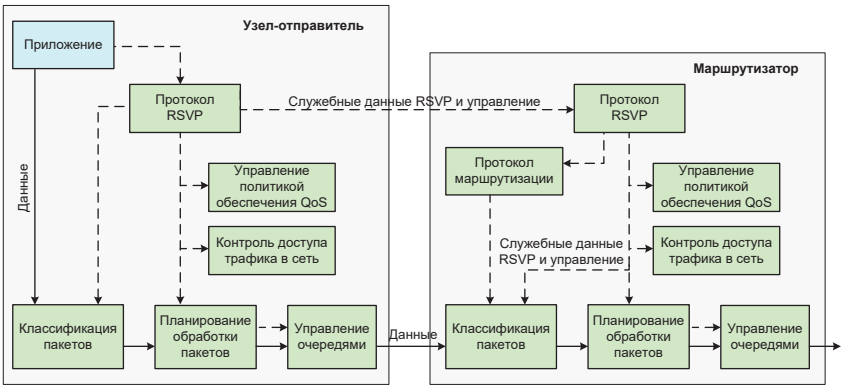


Рис. 7.3. Архитектура Intserv

Контроль доступа трафика в сеть осуществляется при обработке запроса на установление соединения от узла отправителя вышеописанным образом. При этом узел-отправитель может запросить следующие классы обслуживания:

- гарантированное обслуживание – для соединения гарантируется согласованная скорость передачи и отсутствие потерь пакетов. Данный класс отлично подходит приложениям реального времени;
- контролируемое обслуживание – для соединения сохраняется согласованная скорость передачи при отсутствии перегрузок сети, а уровень потерь сеть пытается обеспечить на низком уровне. Данный класс может быть адаптирован под приложения реального времени, но лучше всего подходит для просмотра web-страниц, FTP и др. подобных применений;
- обслуживание «Best Effort» (обслуживание с наилучшими усилиями) – трафик обслуживается по умолчанию, без предоставления каких-либо гарантий по скорости и потерям пакетов.

Классификация пакетов относит каждый входящий пакет к определённому классу. Будучи разделены по классам, пакеты получают одинаковую для своего класса обработку от планировщика пакетов. Выбор конкретного класса зависит от приоритетов отправителя и получателя, IP-адреса и номера порта в заголовке пакета. Как правило, однотипные потоки принадлежат одному классу.

Планирование обработки пакетов осуществляется с помощью системы управления очередями и регулирует отправку пакетов на маршрутизаторы в соответствии с проведённой классификацией, упомянутой выше, и заданными для каждого потока параметрами QoS. Планировщик пакетов должен функционировать в точке, где пакеты ставятся в очередь. Этой точкой обычно являются протоколы канального уровня маршрутизатора.

Управление очередями в архитектуре Intserv преимущественно направленно на контроль перегрузки сети и реализует три способа сброса пакетов в маршрутизаторах при перегрузках:

- tail drop – сбрасываются последние добавленные пакеты в конце очереди;
- QoS – исключаются пакеты с наихудшими требованиями к качеству обслуживания;
- RED – вероятность сброса пакета зависит от степени перегрузки буфера маршрутизатора. Если буфер практически пуст, то все пакеты пропускаются в обычном режиме. Когда очередь начинает расти, то вероятность отбрасывания пакетов также начинает расти. Когда буфер полностью заполняется, вероятность становится равной единице и все входящие пакеты отбрасываются. Данный способ является наиболее распространенным в архитектуре Intserv.

Спецификациями, описывающими архитектуру Intserv, являются: RFC-1633 «Интегрированные услуги в сети Интернет», RFC-2205 «Протокол резервирования ресурсов (RSVP)» и RFC-2212 «Спецификации гарантированного качества обслуживания».

Хотя в середине 1990-х гг. идея использования архитектуры IntServ и протокола RSVP вызывала большие надежды, со временем интерес к этой архитектуре угас. Главной причиной этого стала проблема масштабируемости, вызванная необходимостью хранить и поддерживать информацию о состоянии соединений в каждом маршрутизаторе. Эта проблема, переносимая на такие глобальные сети, как Интернет, делает RSVP сложным в практической реализации, что привело к широкому распространению более простых протоколов – TCP и UDP. Тем не менее, в последнее время, в связи с распространением технологии MPLS, прежде всего IP/MPLS, применение протокола RSVP в MPLS стало снова актуальным.

7.3. Архитектура дифференцированного обслуживания DiffServ

Когда в конце 1990-х гг. стало ясно, что декларируемый в архитектуре IntServ применительно к обслуживанию «из конца в конец» подход к резервированию ресурсов сложно реализуем на практике, в 1997 г. начались работы по разработке новой архитектуры, в основу которой были положены следующие принципы:

– минимизация служебной информации, рассылаемой по сети;
– проверка доступности ресурсов для обработки трафика не на каждом маршрутизаторе соединения, а на граничных маршрутизаторах сети при допуске трафика в сеть;
– использование классификации трафика, вместо классификации вариантов его обслуживания;
– введение ограниченного детерминированного, но гибкого набора действий по обработке трафика данных классов в узлах сети.

В результате в 1998 г. были разработаны RFC 2474 «Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers» и RFC 2475 «An Architecture for Differentiated Services» определяющие архитектуру DiffServ.

Основная идея архитектуры DiffServ (Differential Services) заключается в разделении входящего трафика в сеть на несколько крупных классов, для каждого из которых будет обеспечиваться определенное QoS в рамках некоторой области, называемой *доменом DiffServ*. На границах домена в граничных маршрутизаторах происходит анализ входящих в сеть пакетов, а также их классификация, подразумевающая отнесение их к одному из классов обслуживания, а также маркировка пакетов специальным кодовым словом DSCP (DiffServ Code Point). Далее обработка трафика на промежуточных узлах, принятие решения о направлении пакета в ту или иную очередь, осуществляется узлами самостоятельно, с ориентацией на значение кодового слова DSCP, расположенного в заголовке IP пакета – поле TOS. Поле ToS занимает 8 бит в заголовке IP-пакета оно может состоять из идентификатора приоритета (IP Precedence – IPP, 3 бита) или DSCP (6 бит).

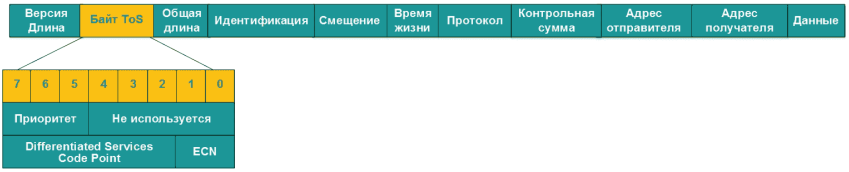


Рис. 7.4. Задание класса трафика в поле ToS в заголовке IP-пакета

Архитектура DiffServ поддерживает 3 базовых класса обслуживания, присваемого трафику в граничных маршрутизаторах при допуске его в домене [17]:

1) трафик «реального времени» (Real Time – RT);
2) приоритетный трафик (Priority – P);
3) неприоритетный трафик (Non priority – NP).

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

Граничные маршрутизаторы в каждом автономном домене DiffServ должны поддерживать классификацию и маркировку трафика, а также сопоставление интенсивности поступающего трафика и достаточности доступных сетевых ресурсов для его обслуживания (рис. 7.5). При этом при передаче трафика через несколько доменов DiffServ, в граничных маршрутизаторах трафик может перемаркироваться (повторно классифицироваться).

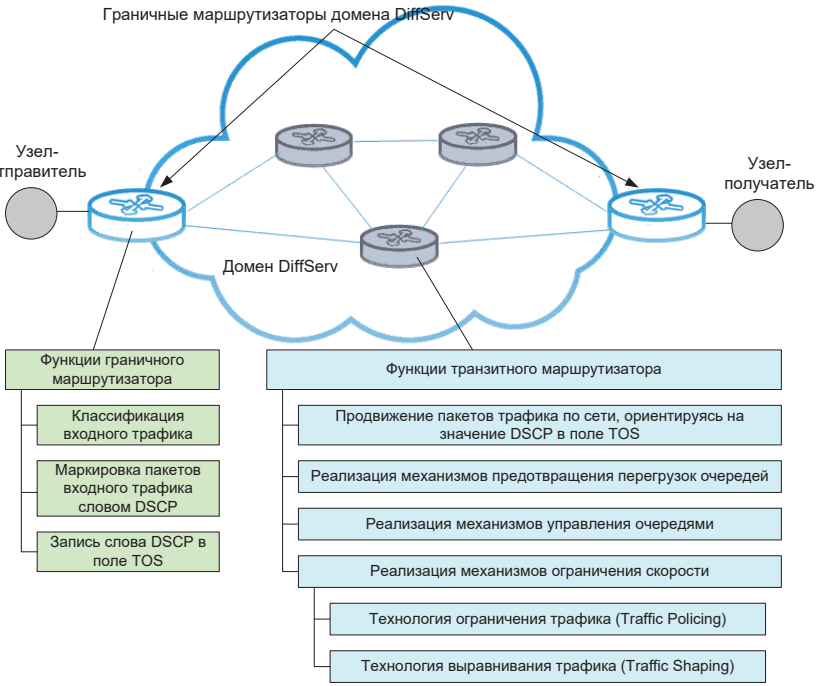


Рис. 7.5. Архитектура DiffServ

Для контроля перегрузок и выполнения ограничений по интенсивности и структуре трафика в своем домене DiffServ граничные маршрутизаторы должны использовать нижеуказанные механизмы предотвращения перегрузок и управления очередями, а также механизмы ограничения ско-

рости поступления трафика. При невозможности обслуживания трафика в домене DiffServ поступающий трафик либо сбрасывается, либо дополнительно буферизируется с пометкой «Best Effort». Данная пометка означает, что трафик будет обслужен без гарантий обеспечения требований к QoS, но с максимальными усилиями со стороны сетевых устройств по его соблюдению. Для технологии MPLS трафик IP инкапсулируется, а класс MPLS маркируется заново [17].

Сетевые устройства, поддерживающие DiffServ, используют различные входные/выходные очереди для трафика различных классов обслуживания, а также основанные на этих классах приоритетные механизмы обслуживания очередей CQ (Class based Queuing), к основным из которых относятся [17]:

- механизмы предотвращения перегрузок очередей;
- механизмы управления очередями;
- механизмы ограничения скорости.

К наиболее распространенным механизмам предотвращения перегрузок очередей в маршрутизаторах относятся [17]:

- раннее обнаружение перегрузок в очередях – RED (Random Early Detection);
- взвешенное раннее обнаружение перегрузок в очередях – WRED (Weighted Random Early Detection);
- адаптивное раннее обнаружение перегрузок в очередях – ARED (Adaptive Random Early Detection);
- многоуровневое раннее обнаружение перегрузок в очередях – MRED (Multilevel Random Early Detection);
- сброс пакетов в конце очереди (Tail Drop);
- случайный сброс пакетов (Random Drop);
- отказ в приеме пакетов, переполняющих очередь (Drop Front on Full) и др.

К наиболее распространенным механизмам управления очередями относятся [17]:

- «первый пришел – первый обслужился» – FIFO (First In – First Out);
- приоритетное обслуживание в очереди – PQ (Priority Queuing);
- настраиваемые очереди – CQ (Custom Queuing);
- справедливое обслуживание в очереди – FQ (Fair Queuing);
- взвешенное справедливое обслуживание в очереди – WFQ (Weighted Fair Queuing);
- взвешенное справедливое обслуживание в очереди на основе классов – CBWFQ (Class-Based Weighted Fair Queuing);
- приоритетное взвешенное справедливое обслуживание в очереди на основе классов (PQ-CBWFQ – Priority Class-Based Weighted Fair Queuing), обеспечивающее низкую задержку обслуживания очереди – LLQ (Low Latency Queuing);

– круговой циклический алгоритм обслуживания очереди – RR (Robin Round);
– взвешенный круговой циклический алгоритм обслуживания очереди – WRR (Weighted Robin Round);
– дефицитный взвешенный круговой циклический алгоритм обслуживания очереди – DWRR (Deficit Weighted Robin Round) и др.

К механизмам ограничения скорости относятся [17]:

– технологии ограничения трафика (Traffic Policing) – отбрасывает пакеты, создающие перегрузку;
– технологии выравнивания трафика (Traffic Shaping) – помещает пакеты, создающие перегрузку, в буфер и обслуживает их при снижении нагрузки.

Данные механизмы предназначены для сглаживания пульсаций «взрывного» трафика и уменьшения неравномерности продвижения пакетов.

При реализации обоих механизмов Traffic Policing и Traffic Shaping могут использоваться алгоритмы:

– алгоритм «дырявого ведра» (Leaky Bucket) – основан на том, что независимо от количества трафика, поступающего в буфер, выборка трафика из буфера ведется с постоянной скоростью (по аналогии с дырявым ведром);
– алгоритм «маркерного ведра» (Token Bucket) – основан на том, что выборка трафика из буфера регулируется виртуальными маркерами, каждый из которых соответствует передаче определенного объема трафика.

Материал главы 7 основан на информации, приведенной в работе [17] и материалах Интернет-ресурсов [14, 18].

8. Транспортные телекоммуникационные сети

8.1. Единая сеть электросвязи – национальная транспортно-магистральная телекоммуникационная сеть

Для организации информационного обмена между отдельными локальными сетями и глобальными сетями развертывается транспортная сеть (ТС), реализующая сервисы транспортировки информационных потоков между отдельными абонентами, а также предоставление потребителям информационных сервисов, таких как радио, ТВ, факсимильная и другие виды связи.

Транспортная сеть связи – это совокупность ресурсов, выполняющих функции транспортировки информационных потоков в телекоммуникационных сетях (ТКС) – рис. 8.1. Она включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления.

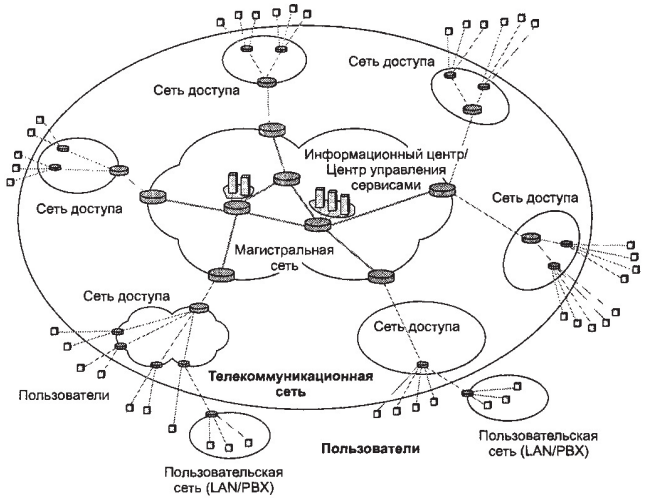


Рис. 8.1. Телекоммуникационная сеть, состоящая из магистральной транспортной сети и абонентов, подключенных к ней через сети доступа

Как правило, транспортные сети разворачиваются в национальном масштабе. В России такой транспортной системой является *единая сеть электросвязи* (ЕСЭ), которая ранее именовалась *взаимоувязанная сеть связи* (ВСС).

Организационно ЕСЭ – это совокупность взаимоувязанных сетей электросвязи, находящихся в ведении различных операторов связи (основным из которых является АО «Ростелеком») имеющих право предоставлять услуги электросвязи.

Единая сеть электросвязи России сегодня представляет собой совокупность сетей (рис. 8.2):

– сети связи общего пользования (СС ОП);
– ведомственных сетей и сети связи в интересах управления, обороны, безопасности и охраны правопорядка.

Главная составляющая ЕСЭ – это сети связи общего пользования, открытые для всех физических и юридических лиц на территории России.

Архитектура ЕСЭ России приведена на рис. 8.3.

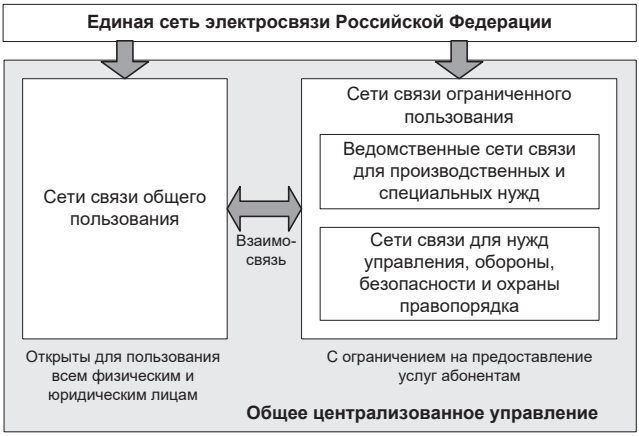


Рис. 8.2. Структура ЕСЭ РФ

Архитектурно ЕСЭ, как система связи, представляет собой иерархическую трехуровневую систему (рис. 8.3):

– *первый* уровень – первичная (транспортная) сеть передачи, представляющая типовые каналы и групповые тракты передачи для вторичных сетей (сетей абонентского доступа (САД));
– *второй* уровень – вторичные сети (САД), т. е. коммутируемые и некоммутируемые сети связи (телефонные, документальной электросвязи и др.);
– *третий* уровень – это системы электросвязи или службы электросвязи, представляющие пользователям конкретные услуги связи.

Услуги электросвязи предоставляются пользователям посредством оконечного оборудования сетей электросвязи. Телефонная связь, передача данных, телеграфная связь, передача газет, распределение программ телевизионного и звукового вещания, видеотелефонные сети – все эти системы

электросвязи общего пользования входят в структуру ЕСЭ в качестве вторичных сетей (САД).

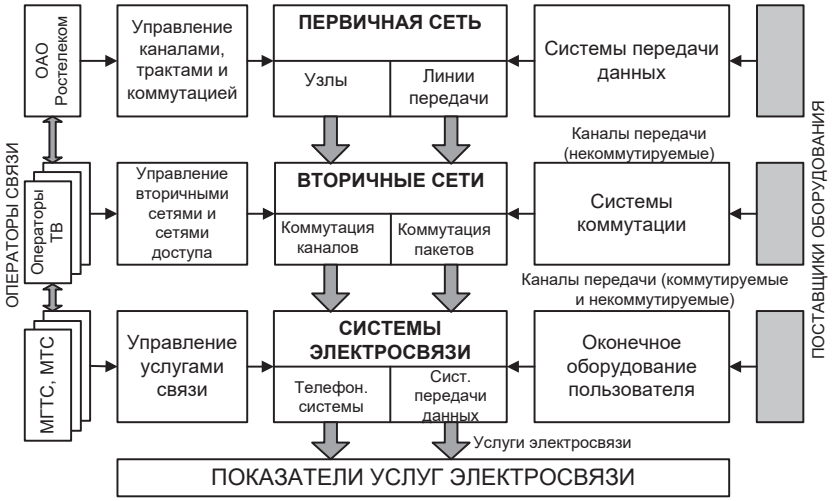


Рис. 8.3. Архитектура ЕСЭ РФ

Помимо сетей электросвязи общего пользования в состав ЕСЭ входят также вторичные сети, организованные различными ведомствами, корпорациями и коммерческими кампаниями. К таким сетям относятся:

- сети связи силовых структур;
- сети связи топливно-энергетического комплекса;
- сети связи транспортных и банковских структур;
- частные и корпоративные сети связи.

При построении вторичных сетей используются различные типы телекоммуникационных технологий, обеспечивающих эффективное использование каналов и типовых трактов, выделенных из состава первичной сети в данную вторичную сеть. К телекоммуникационным технологиям вторичных сетей относятся:

- кроссовая коммутация;
- традиционная коммутация каналов;
- коммутация сообщений и пакетов.

Помимо перечисленных последние годы активно внедряются новые более эффективные технологии построения вторичных сетей, которые относятся к телекоммуникационным технологиям интегрального типа. Эти технологии обеспечивают совместную передачу сообщений различных видов информации: речи, данных, факсимильной и видеоинформации, включая передачу телевизионных программ и т. д. К таким прогрессивным технологиям, получившим наибольшее распространение относятся в настоящее время: Gigabit Ethernet, xDSL, FTTx и PON.

Для примера на рис. 8.4 приведена транспортная сеть ЕСЭ АО «Ростелеком». Базовой технологией для построения магистральной первичной сети АО «Ростелеком» является технология SDH, при этом ведется постепенный переход сетей с SDH на IP/MPLS.

Рис. 8.4. Магистральная сеть АО «Ростелеком»

Основная задача ЕСЭ – транспортная, т. е. передача сообщений от его источника к получателю. Конечным результатом функционирования ЕСЭ являются услуги связи, предоставляемые пользователям.

Показатели, характеризующие функционирование ЕСЭ:

- скорость и своевременность доставки сообщений пользователям;
- достоверность сообщений (соответствие принятого сообщения переданному);
- надежность и устойчивость связи, т. е. способность сети выполнить транспортную функцию с заданными эксплуатационными характеристиками в повседневных условиях и при воздействии внешних дестабилизирующих факторов.

Помимо высокого быстродействия для систем связи, базирующиеся на ресурсе ЕСЭ, необходимо обеспечить требования по устойчивости и безопасности. Системы ЕСЭ могут обеспечить защиту информации от ряда угроз безопасности (блокирование, несанкционированный доступ и др.). Однако общая ответственность за общее решение вопросов безопасности информации (обеспечение свойств конфиденциальности, целостности и доступности) возлагается на пользователя (непосредственного собственника информации).

Устойчивость сети связи – это ее способность сохранять работоспособность в условиях воздействия различных дестабилизирующих факторов. Она определяется надежностью, живучестью и помехоустойчивостью сети.

Для повышения устойчивости ЕСЭ используются различные меры:

- оптимизация топологии сетей связи для упрощения их адаптации к условиям, возникающим в результате воздействия различных дестабилизирующих факторов, включая геополитические;
- рациональное размещение сооружений связи на местности с учетом зон возможных разрушений, наводнений, пожаров;
- применение специальных мер защиты сетей и их элементов от влияния источников помех различного характера;
- развитие систем резервирования;
- внедрение автоматизированных систем управления, организующих работу по перестройке и восстановлению сетей, поддержанию их работоспособности в различных условиях и др.

8.2. Цифровая первичная сеть

8.2.1. Общая характеристика первичных сетей

Первичной сетью называется совокупность типовых физических цепей, типовых каналов передачи и сетевых трактов системы электросвязи, образованная на базе сетевых узлов, сетевых станций, оконечных устройств первичной сети и соединяющих их линий передачи системы электросвязи.

В основе современной системы электросвязи лежит использование цифровой первичной сети, основанной на использовании цифровых систем передачи. Как следует из определения, в состав первичной сети входит среда передачи сигналов и аппаратура систем передачи.

Первичная сеть строится на основе типовых каналов, образованных системами передачи. Рассмотрим ту часть первичной сети, которая связана с передачей информации в цифровом виде.

Цифровой сигнал типового канала имеет определенную логическую структуру, включающую:

- цикловую структуру сигнала;
- тип линейного кода.

Цикловая структура сигнала используется для синхронизации, процессов мультиплексирования и демультиплексирования между различными уровнями иерархии каналов первичной сети, а также для контроля блоковых ошибок.

Линейный код обеспечивает помехоустойчивость передачи цифрового сигнала.

Аппаратура передачи осуществляет преобразование цифрового сигнала с цикловой структурой в модулированный электрический сигнал, передаваемый затем по среде передачи. Тип модуляции зависит от используемой аппаратуры и среды передачи. Современные системы передачи используют в качестве среды передачи сигналов электрический и оптический

кабель, а также радиочастотные средства (радиорелейные и спутниковые системы передачи) – рис. 8.5.

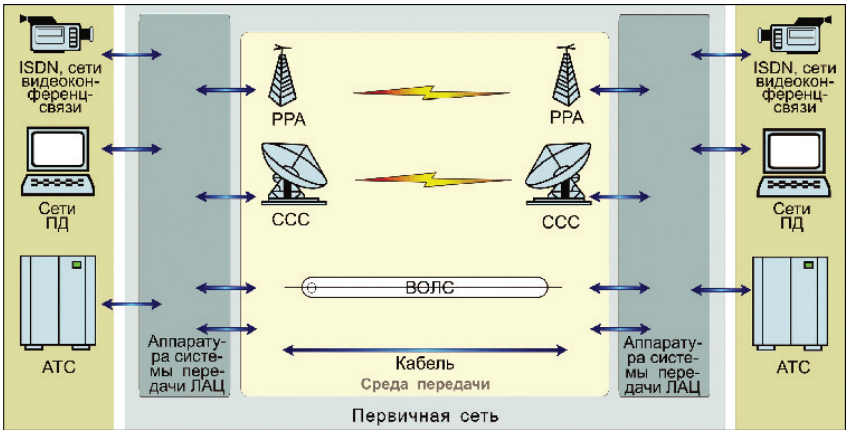


Рис. 8.5. Физические среды передачи первичной сети

Таким образом, внутри цифровых систем передачи осуществляется передача электрических сигналов различной структуры, на выходе цифровых систем передачи образуются каналы цифровой первичной сети, соответствующие стандартам по скорости передачи, цикловой структуре и типу линейного кода.

Обычно каналы первичной сети приходят на узлы связи, откуда кроссируются для использования во вторичных сетях. Можно сказать, что первичная сеть представляет собой банк каналов, которые затем используются вторичными сетями (сетью телефонной связи, сетями передачи данных, сетями специального назначения и т.д.). Существенно, что для всех вторичных сетей этот банк каналов един, откуда и вытекает обязательное требование, чтобы каналы первичной сети соответствовали общим стандартам.

8.2.2. Цифровые иерархии, используемые в первичной сети

Современная цифровая первичная сеть строится на основе 3-х основных технологий:

1) плезиохронная цифровая иерархия (PDH);
2) синхронная цифровая иерархия (SDH);
3) транспортная иерархия оптических сетей (OTH-OTN).

Кроме того, имеется технология асинхронного режима передачи (ATM), которая активно внедрялась в первичные сети в 1990-х гг., однако она не получила широкого распространения ввиду своего вытеснения к 2000 г. более дешевой и простой технологией Gigabit Ethernet.

В настоящее время идет активное внедрение новых оптических технологий, которые в ближайшем будущем наряду с вышеприведенными технологиями составят основу цифровой первичной сети:

– Gigabit Ethernet (GE) на ВОЛС;
– технология автоматически коммутируемых оптических сетей ASON (Automatic Switched Optical Network).

Из перечисленных технологий в настоящее время именно оборудование SDH, OTH и GE составляет подавляющее большинство средств построения цифровой первичной сети.

Рассмотрим более подробно историю построения и отличия плезиохронной и синхронной цифровых иерархий.

Первичная цифровая сеть на основе PDH/SDH состоит из следующих компонентов:

– узлов мультиплексирования (мультиплексоров), выполняющих роль преобразователей между каналами различных уровней иерархии стандартной пропускной способности (ниже);
– регенераторов, восстанавливающих цифровой поток на протяженных трактах;
– цифровых кроссов, которые осуществляют коммутацию на уровне каналов и трактов первичной сети.

8.2.2.1. Плезиохронные цифровые иерархии PDH

Схемы плезиохронных цифровых систем (ПЦС) были разработаны в начале1980-х годов. Всего их было три:

1) принятая в США и Канаде, в качестве скорости сигнала первичного цифрового канала (ПЦК) (DS1) была выбрана скорость 1544 кбит/с, которая давала последовательность DS1 – DS2 – DS3 – DS4 или последовательность вида: 1544 – 6312 – 44736 – 274176 кбит/с. Это позволяло передавать соответственно 24, 96, 672 и 4032 канала DS0 (основного цифрового канала (ОЦК) со скоростью 64 кбит/с);

2) принятая в Японии, использовалась та же скорость для DS1; она давала последовательность DS1 – DS2 – DSJ3 – DSJ4 или последовательность 1544 – 6312 – 32064 – 97728 кбит/с, что позволяло передавать 24, 96, 480 или 1440 каналов DS0;

3) принятая в Европе и Южной Америке – в качестве первичной была выбрана скорость 2048 кбит/с и давала последовательность E1 – E2 – E3 – E4 – E5 или 2048 – 8448 – 34368 – 139264 – 564992 кбит/с. Указанная иерархия позволяла передавать 30, 120, 480, 1920 или 7680 каналов DS0.

Комитетом по стандартизации ITU-T был разработан стандарт, согласно которому:

– были стандартизированы 3 первых уровня первой иерархии, 4 уровня второй и 4 уровня третьей иерархии в качестве основных, а также схемы кросс-мультиплексирования иерархий (рис. 8.6);

– последние уровни первой и третьей иерархий не были рекомендованы в качестве стандартных.

Указанные иерархии, известные под общим названием *плезиохронная цифровая иерархия* PDH, или ПЦИ, сведены в таблицу 8.1.

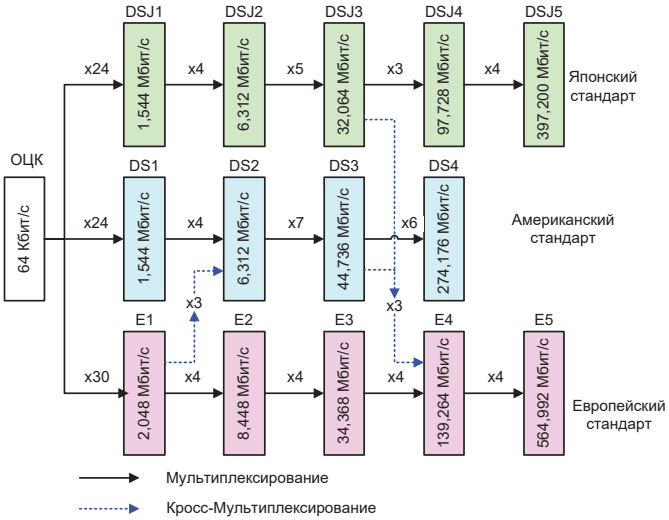


Рис. 8.6. Мультиплексирование цифровых потоков ПЦС (PDH)

Однако технология PDH обладала рядом недостатков, а именно:

– затруднённый ввод/вывод цифровых потоков в промежуточных пунктах;
– отсутствие средств сетевого автоматического контроля и управления;
– многоступенчатое восстановление синхронизации требует достаточно большого времени.

Также можно считать недостатком наличие трёх различных иерархий.

Таблица 8.1 – Три схемы ПЦС: американская схема (АС), японская (ЯС) и европейская (ЕС)

Уровень цифровой иерархии	Скорости передач, соответствующие различным схемам цифровой иерархии [кбит/с]		
	АС: 1544 кбит/с	ЯС: 1544 кбит/с	ЕС: 2048 кбит/с
0	64	64	64
1	1 544	1 544	2 048
2	6 312	6 312	8 448
3	44 736	32 064	34 368
4	---	97 728	139 264

8.2.2.2. Синхронная цифровая иерархия SDH

Указанные недостатки PDH, а также ряд других факторов привели к разработке в США ещё одной иерархии – иерархии синхронной оптической сети SONET, а в Европе аналогичной синхронной цифровой иерархии SDH, предложенных для использования на ВОЛС. Но из-за неудачно выбранной скорости передачи для сетей SONET, было принято решение отказаться от создания SONET, а создать на её основе SONET/SDH со скоростью передачи 51,84 Мбит/с. В результате три потока SONET/SDH соответствовали STM-1 иерархии SDH. Скорости передач иерархии SDH представлены в таблице 8.2.

Таблица 8.2 – Скорости передач иерархии SDH

Уровень SDH	Скорость передачи, Мбит/с
SONET/SDH	51,84
STM-1	155,52
STM-4	622,08
STM-8	1 244,16
STM-12	1 866,24
STM-16	2 487,32
STM-64	9 953,28
STM-256	39 813,12

Иерархии PDH и SDH взаимодействуют через процедуры мультиплексирования и демультиплексирования потоков PDH в системы SDH.

Основным отличием системы SDH от системы PDH является переход на новый принцип мультиплексирования.

Система PDH использует принцип плезиохронного (или почти синхронного) мультиплексирования, согласно которому для мультиплексирования, например, четырех потоков E1 (2048 кбит/с) в один поток E2 (8448 кбит/с) производится процедура выравнивания тактовых частот приходящих сигналов методом *стаффинга*. В результате при демультиплексировании необходимо производить пошаговый процесс восстановления исходных каналов.

Например, во вторичных сетях цифровой телефонии наиболее распространено использование потока E1. При передаче этого потока по сети PDH в тракте E3 необходимо сначала провести пошаговое мультиплексирование E1–E2–E3, а затем – пошаговое демультиплексирование E3–E2–E1 в каждом пункте выделения канала E1.

В системе SDH производится синхронное мультиплексирование / демультиплексирование, которое позволяет организовывать непосредственный доступ к каналам PDH, которые передаются в сети SDH. Это довольно важное и простое нововведение в технологии привело к тому, что в целом технология мультиплексирования в сети SDH намного сложнее, чем технология в сети PDH – усилились требования по синхронизации и параметрам качества среды передачи и системы передачи, а также увеличилось ко-

личество параметров, существенных для работы сети. Как следствие, методы эксплуатации и технология измерений SDH намного сложнее аналогичных для PDH.

8.2.2.3. Технология ATM

Технология ATM отличается от технологий PDH и SDH тем, что охватывает не только уровень первичной сети, но и технологию вторичных сетей, в частности, сетей передачи данных и широкополосной ISDN (B-ISDN). В результате при рассмотрении технологии ATM трудно отделить ее часть, относящуюся к технологии первичной сети, от части, тесно связанной со вторичными сетями.

В таблице 8.3 приведены ключевые отличия технологии ATM от SDH. К ключевым отличиям стоит отнести наличие встроенных механизмов обеспечения качества обслуживания и динамическое выделение каналов с заданной пропускной способностью для обслуживания пользователей. Это позволяет обеспечить гибкое управление телекоммуникационным ресурсом и гарантировать требуемое качество обслуживание пользователей.

Таблица 8.3 – Сравнительный анализ технологий ATM и SDH

Характеристики сетей	ATM	SDH
Скорость передачи информации	2 Мбит/с … 2,5 Гбит/с	2 Мбит/с … 10 Гбит/с
Способ установления соединения	Коммутируемые и постоянные виртуальные каналы	Постоянные соединения
Ширина полосы пропускания	По требованию	2 Мбит/с, 34 Мбит/с, 155 Мбит/с, 622 Мбит/с
Динамическое распределение полосы пропускания	Да	Нет
Набор услуг, предоставляемых сетью	Широкий набор служб для передачи трафика различного рода	Выделенные каналы с постоянной пропускной способностью и гарантированным временем задержки
Управление сетью	С использованием SNMP, установление соединений, выбор маршрутов передачи трафика лежат на ATM-коммутаторах	С использованием внутренних протоколов производителя оборудования, выбор маршрутов, определение альтернативного маршрута при нарушениях в каналах

Международным союзом электросвязи ITU-T предусмотрены рекомендации, стандартизирующие скорости передачи и интерфейсы систем PDH, SDH и ATM, процедуры мультиплексирования и демультиплексирования, структуру цифровых линий связи и нормы на вероятностно-временные параметры. Основные из этих рекомендаций приведены на рис. 8.7.

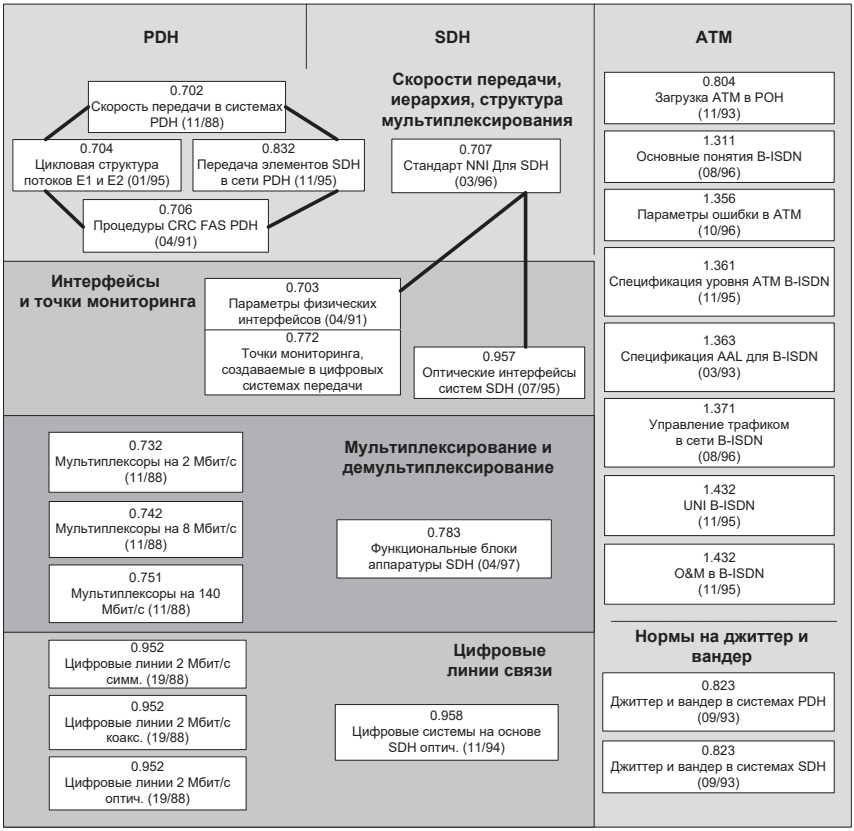


Рис. 8.7. Стандарты первичной цифровой сети, построенной на основе технологий PDH, SDH и ATM

8.2.2.4. Оптическая цифровая иерархия OTH-OTN

Однако, как отмечалась ранее, технология ATM не получила широкого распространения и в 2000-х гг. была вытеснена более дешевой и простой технологией Gigabit Ethernet. Кроме того, тенденцией развития первичных сетей являлось внедрение цифровой транспортной иерархии оптических сетей OTH-OTN, которые строились на основе ВОЛС с DWDM. Технология OTN для построения своей иерархии скоростей использует коэффициент мультиплексирования, равный 4. Начальная скорость иерархии скоростей OTN обозначаемая как OTU1 составляет 2,5 Гбит/с, что соответствует потоку STM-16 в технологии SDH. В настоящее время стандартизованы четыре скорости, которые выбраны так, чтобы прозрачным образом передавать широкий спектр клиентских сигналов, в том числе сигналы

SDH и Gigabit Ethernet. Цифровая иерархия OTH-OTN, регламентированная стандартом G.709, представлена в таблице 8.4.

Таблица 8.4 – Цифровая иерархия скоростей OTH-OTN

Интерфейс G.709	Битовая скорость, Гбит/с	Скорость сигнала нагрузки, Гбит/с
OTU1	255/238 × 2 488 320 = 2,666 057 143	2,488320
OTU2	255/237 × 9,953 280 = 10,709 225 316	9,953 280
OTU3	255/236 × 39,813 120 = 43.018 413 559	39,813 120
OTU4	255/227 × 99,532 800 =111,809 973 568	99,532 800

8.3. Типовые каналы и тракты аналоговой и цифровой сети электросвязи

Первичная сеть представляет собой совокупность линий передачи, на которых с помощью соответствующих систем передачи образуются типовые каналы передачи и групповые тракты, и сетевых узлов (станций) для образования и распределения каналов.

По территориальному признаку сети связи классифицируют на:

- местные;
- зоновые;
- магистральные.

Первичная сеть базируется на современных кабельные линиях связи (витые пары, коаксиальные и волоконно-оптические кабели) при их гармоничном сочетании со спутниковыми, радио- и радиорелейными линиями связи. Сетевые узлы первичной сети обеспечивают организацию и транзит типовых каналов и групповых трактов первичной сети, их коммутацию и предоставление вторичным сетям.

В первичной сети существуют, и по всей видимости, еще долго будут сосуществовать вместе аналоговые и цифровые каналы связи, образованные соответственно аналоговыми (АСП) и цифровыми (ЦСП) системами передачи. При этом наличие аналоговых систем передачи – «наследство» 1940-70-х годов, когда реализовывались масштабные проекты обеспечения телефонной и телеграфной связью максимального количества населенных пунктов в национальных масштабах, однако основой такой сети связи являлись аналоговые каналы связи. В настоящее время ведутся работы по замене АСП на ЦСП, однако это довольно длительный и дорогостоящий процесс, который может растянуться на долгие годы.

Канал электросвязи – это тот индивидуальный путь между двумя абонентами или оконечными абонентскими устройствами, разнесенными в пространстве, по которому передается сигнал электросвязи.

Типовым каналом называют канал (групповой тракт), параметры которого стандартизированы. В первичной сети выделяют следующие типовые каналы.

Типовые каналы передачи аналоговых систем передачи:

- канал тональной частоты (ТЧ) – совокупность технических средств, обеспечивающая передачу сигналов в эффективно передаваемой полосе частот 300-3400 Гц;
- канал звукового вещания (высшего класса – 30-15000 Гц; первого класса: 50 -10 000 Гц; второго класса: 100-6 300 Гц);
- канал передачи сигналов изображения аналогового телевидения с полосой частот от 50 Гц до 6 МГц;
- канал звукового сопровождения сигналов аналогового телевидения (высшего класса: 30-15 000 Гц, 1 класса: 50-10 000 Гц);
- типовые групповые аналоговые тракты:
  - первичный – 60-108 кГц (12 каналов ТЧ);
  - вторичный – 312-552 кГц (60 каналов ТЧ);
  - третичный – 812-2044 кГц (300 каналов ТЧ).

Типовые каналы передачи цифровых систем передачи:

- основной цифровой канал (ОЦК) с номинальной скоростью передачи 64 кбит/с (канал типа В) – является цифровым эквивалентом канала аналогового канала тональной частоты (ТЧ), так как обеспечивает передачу телефонного сигнала в полосе частот 300 - 3400 Гц методом импульсно-кодовой модуляции (ИКМ);
- цифровой канал абонентского окончания цифровой сети интегрального обслуживания (ЦСИО-ISDN):

  $$144 \text{ кбит/с} = 2 \cdot 64 \text{ кбит/с} + 16 \text{ кбит/с} = 2B + D,$$

  где D – канал передачи данных;
- цифровые тракты плезиохронной цифровой иерархии (ПЦИ):
  - субпервичный – 0,512 Мбит/с;
  - вторичный – 8,448 Мбит/с;
  - третичный – 34,368 Мбит/с;
  - четверичный – 139,264 Мбит/с;
- цифровые тракты синхронной цифровой иерархии (СЦИ) – цифровые потоки синхронных транспортных модулей (СТМ):
  - поток СТМ-1 = 155,52 Мбит/с;
  - поток СТМ-4 = 622,08 Мбит/с;
  - поток СТМ-16 = 2 488,32 Мбит/с;
  - поток СТМ-64 = 9 953,28 Мбит/с;
  - поток СТМ-256 = 39 813,12 Мбит/с.

8.4. Вторичные сети связи – сети абонентского доступа

На базе типовых каналов и трактов первичной сети строятся *вторичные сети* (их еще называют – *сети абонентского доступа* (САД)), которые обеспечивают передачу соответствующих видов информации (деление вторичных сетей по информационному признаку) или обеспечивают передачу требуемых видов информации в рамках одного ведомства (деление вторичных сетей по ведомственному признаку) – рис. 8.8.

Каналы первичной сети служат базой для построения вторичных сетей, которые разделяются по виду передаваемой информации (телефонная сеть, телеграфная сеть, сеть передачи данных и т. д.) или ведомственной принадлежности.

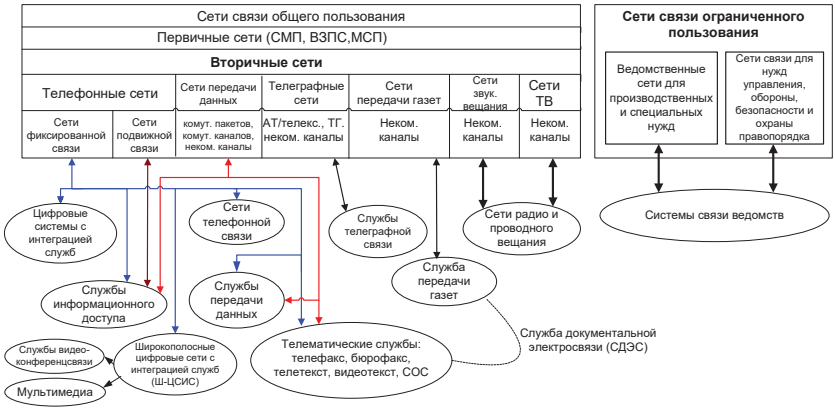


Рис. 8.8. Принцип деления вторичных сетей связи

Назначением конкретной вторичной сети электросвязи является доставка информации определенного вида (преобразованной в соответствующие сигналы электросвязи). Как следует из определения первичной сети, она обеспечивает связь только между определенными узлами. При этом магистраль прокладывается далеко не между всеми узлами первичной сети. Поэтому для образования путей передачи информации на любой из узлов сети необходимо осуществлять соединения между каналами (или группами каналов) различных магистралей, оканчивающихся на одном и том же узле (рис. 8.9).

Если на всех узлах первичной сети или некоторых из них установить кроссовые соединения, то на базе первичной сети будет создана *вторичная некоммутируемая сеть*.

В узлы некоммутируемой сети могут включаться абонентские линии, которые соединяются с каналами сети также с помощью кроссовых соединений. Однако в большинстве случаев каналы вторичных сетей являются

коллективными для всех или группы абонентских пунктов, включенных в данный узел. На узле в этом случае устанавливается аппаратура коммутации, обеспечивающая подключение абонентской линии к каналу лишь на время передачи информации.

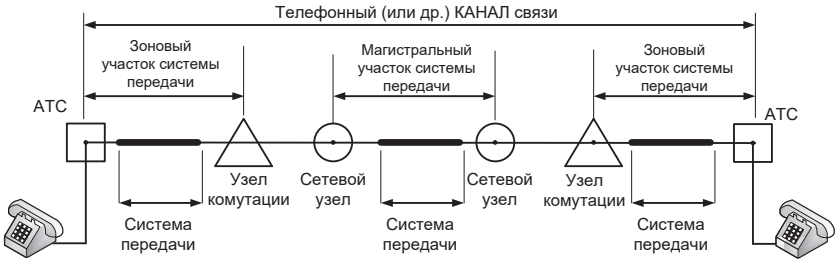


Рис. 8.9. Структура составного канала сети ЕСЭ

Таким образом, на базе вторичной некоммутируемой сети образуется вторичная сеть другого типа – *вторичная коммутируемая сеть*. Узел, в котором установлена аппаратура коммутации каналов и линий, обеспечивающая подключение абонентских линий к каналам, называется *узлом коммутации*.

Вторичные коммутируемые сети подразделяются по способу коммутации на:

– сети с коммутацией каналов;
– сети с коммутацией сообщений;
– сети с коммутацией пакетов, кадров и ячеек.

В зависимости от числа абонентов и размеров территории вторичные сети могут иметь различную топологическую структуру. Типовыми топологическими структурами вторичных сетей являются:

– радиальная;
– полносвязная;
– радиально-узловая;
– сочетание радиально-узловой и полносвязной.

8.5. Узлы связи

Для образования путей передачи информации на любой из узлов сети необходимо осуществлять соединения между каналами (или группами каналов) различных магистралей, оканчивающихся на одном и том же узле. Кроме соединения отдельных каналов и магистралей в узлах связи осуществляется ввод/вывод отдельных информационных потоков из транспортной сети к потребителям (рис. 8.10).

Рис. 8.10. Схема взаимодействия абонентов через телекоммуникационную сеть

Телекоммуникационные узлы – это организационно-техническое объединение средств и комплексов связи (канального, коммутационного, абонентского и др. оборудования), характеризуемого определенными структурными свойствами и предназначенного для ввода, вывода информации, каналообразования, коммутации каналов связи (сообщений, пакетов) в соответствии с потребностью пользователей (абонентов) сети.

В узлах осуществляется формирование путей передачи информации между оконечными пунктами сети. С этой целью на узле предусматривается возможность непосредственного (для сетей с коммутацией каналов) или косвенного, через промежуточную буферную память (для сетей коммутации сообщений или пакетов), соединения между каналами линий связи, инцидентных (смежных) данному узлу.

Обобщенная структура узла связи приведена на рис. 8.11.

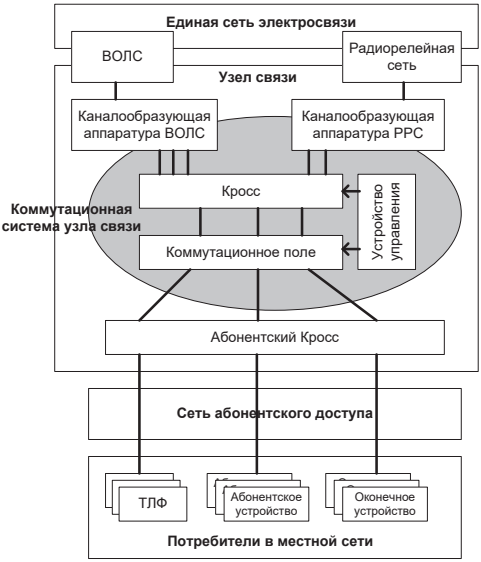


Рис. 8.11. Обобщенная структурная схема узла связи

Каналы связи от смежных узлов кроссируются непосредственно в кроссе или коммутируются в коммутационном поле узла. Управляющее устройство может воздействовать на коммутационное поле и кросс и хранит, в общем случае, как информацию о свободных, занятых и поврежденных каналах связи, инцидентных данному узлу, так и информацию, используемую при поиске пути установления соединения в коммутационном поле узла. Коммутационное поле по командам устройства управления обеспечивает оперативное установление соединения между коммутируемыми каналами.

Абонентский КРОСС, обеспечивает возможность подключения оконечных устройств пользователей, терминалов телефонной сети и других абонентских устройств через абонентские линии к коммутационной системе узла.

Посредством коммутационной системы, содержащей коммутационное поле, устройство управления и КРОСС каналообразующей аппаратуры, абонентские сигналы коммутируются на входы каналов систем электросвязи различных родов связи (например, волоконно-оптической системы передачи или радиорелейная станция) и т. д. Далее групповые сигналы с выхода каналообразующей аппаратуры передаются соответствующим линиям связи к другим узлам связи.

Применение систем передачи, относящихся к различным родам связи, использование основных и обходных направлений связи, а также альтернативной маршрутизации сообщений обеспечивает высокую живучесть и устойчивость сети связи.

Для передачи различных видов информации на базе каналов первичной сети ЕСЭ, разворачиваются соответствующие вторичные сети по видам передаваемой информации:

- телефонная сеть;
- сеть передачи телеметрической информации;
- сеть передачи сигналов телевидения;
- сеть телеграфной связи;
- сеть передачи данных, и др.

Для оказания услуг связи потребители и абоненты осуществляют доступ к узлу связи транспортной сети через сети абонентского доступа. При этом наблюдаются следующие тенденции развития систем абонентского доступа:

- использование существующих медных телефонных линий для предоставления широкополосного доступа средствами модемов xDSL (Digital Subscriber Line) в его различных разновидностях (HDSL, ADSL, VDSL), со скоростями 64 кбит/с – 50 Мбит/с на расстояниях от десятков и сотен метров до нескольких километров;
- использование технологий: «волокно в дом», «волокно в распределительный шкаф», «волокно в офис» и т. д., обозначаемых

FTTx (Fiber To The Home,…), например, пассивной оптической сети PON (Passive Optical Network), основанных на сети волоконно-оптических линий, для организации доступа к любым видам услуг;

– использование широкополосных радио технологий WiMAX, UMTS, LTE и др. для фиксированного и мобильного доступа с разделением радиочастотных ресурсов по спектру частот, по времени, кодовым разделением, пакетной передачей.

8.6. Этапы развития технологий транспортных телекоммуникационных сетей

8.6.1. Этапы развития первичных и вторичных сетей

Телекоммуникационные системы в своем развитии прошли несколько этапов, схематично представленных на рис. 8.12. Чем ниже лежит слой, соответствующей технологии, тем более высокоскоростной она является, а следовательно, может обеспечивать передачу видов информации вышележащих технологий. Передача информации между вторичными сетями, построенными на базе различных телекоммуникационных технологий, осуществляется с использованием переходных элементов, называемых шлюзами, которые располагаются на их границах.

На первом этапе первичная сеть строилась на основе типовых каналов и трактов АСП.

Второй этап характеризовался созданием цифровых систем передачи на основе иерархии плезиохронных цифровых систем, которые образовывали первичную цифровую сеть. При этом на обоих этапах развития жестко закреплялся соответствующий ресурс первичной сети в виде типовых каналов и трактов за соответствующими вторичными сетями. Такой подход, основанный на жестком закреплении ресурсов первичной сети за вторичными сетями связи, не позволял осуществлять динамическое перераспределение ресурсов первичной сети в условиях нестационарной нагрузи различных видов информации, характеризовался использованием разнотипного каналообразующего и коммутационного оборудования и являлся неэффективным в экономическом плане. Наличие взаимного существования АСП и ЦСП вызвало необходимость решения задачи сопряжения между собой аналоговых каналов и трактов с цифровыми, что также приводило к дополнительному усложнению и повышению стоимости связи (модемы, АЦП-ЦАП, TMUX – трансмультиплексоры).

Вторичные сети связи на этих этапах использовали, как правило, кроссовую коммутацию, традиционную коммутацию каналов аналоговых и цифровых, в телеграфных сетях связи применялась как коммутация каналов, так и коммутация сообщений, передача данных осуществлялась по некоммутируемым и коммутируемым каналам связи, а также с использованием метода коммутации пакетов. Видео и телевизионная информация

передавалась по выделенным для этих целей широкополосным аналоговым или высокоскоростным цифровым трактам передачи АСП и ЦСП соответственно.

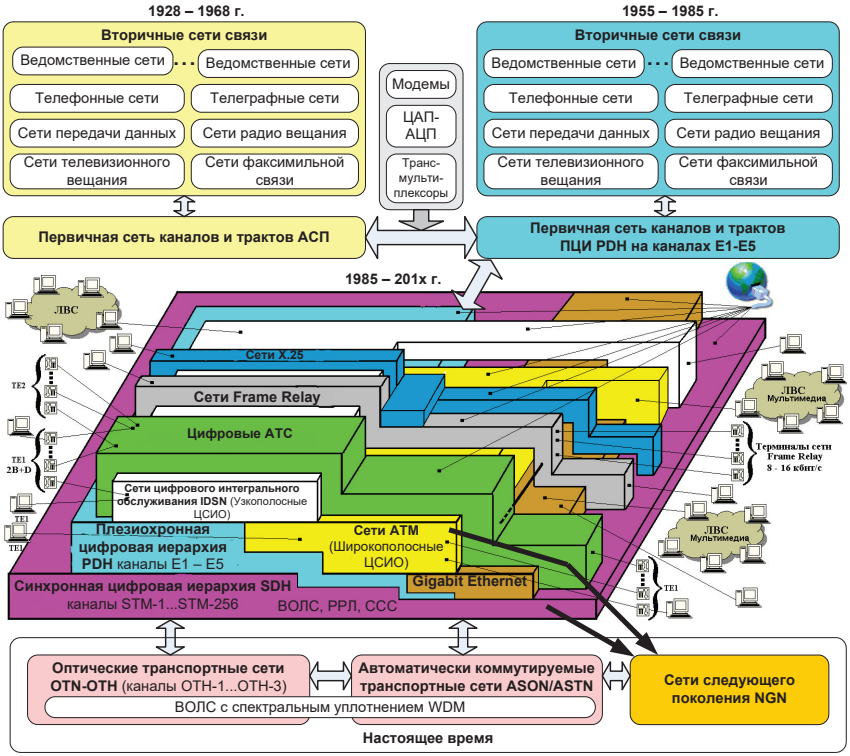


Рис. 8.12. Этапы развития телекоммуникационных технологий

Третий этап развития телекоммуникационных систем связан с появлением новых технологий передачи информации, как при построении первичной сети, так и использовании новых технологий интегрального типа для построения вторичных сетей.

На этом этапе вторичные сети обеспечивают в едином цифровом виде совместную передачу различных видов информации, осуществляя динамическое перераспределение имеющегося ресурса между сообщениями различных видов информации. При этом в рамках каждой технологии вторичной сети используется однотипное коммутационное оборудование.

Основу первичной сети третьего этапа составляют цифровые системы передачи плезиохронной и синхронной иерархий, которые обеспечивают функционирование всех вторичных сетей, использующих различные методы оперативной коммутации: быструю коммутацию каналов, быструю коммутацию пакетов, коммутацию кадров, пакетов и ячеек.

8.6.2. Сети связи NGN

В последнее время при развитии телекоммуникационных систем получила развитие концепция *сетей связи следующего/нового поколения NGN* (Next/New Generation Network). Концепция NGN предусматривает создание новой мультисервисной сети, при этом с ней осуществляется интеграция существующих служб путем использования распределенной программной коммутации (soft-switches).

Эволюция корпоративных сетей от аналого-цифрового варианта к NGN-архитектуре иллюстрируется рис. 8.13.

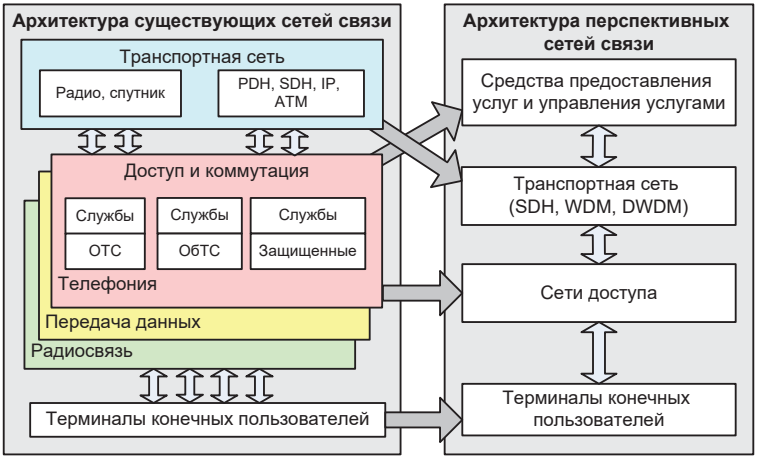


Рис. 8.13. Эволюция архитектуры телекоммуникационных сетей

Сети следующего поколения (NGN) представляют собой новую концепцию сети, комбинирующую в себе голосовые функции, качество обслуживания (QoS) и коммутируемые сети с преимуществами и эффективностью пакетной сети. Сети NGN означают эволюцию существующих телекоммуникационных сетей, отражающуюся в слиянии сетей и технологий. Благодаря этому обеспечивается широкий набор услуг начиная с классических услуг телефонии и кончая различными услугами передачи данных или их комбинацией.

Рекомендация МСЭ-Т Y.2001 определяет терминологический базис NGN следующим образом:

Концепция NGN – концепция построения сетей связи следующего/нового поколения (Next/New Generation Network), обеспечивающих предоставление неограниченного набора услуг с гибкими настройками по их:

- управлению;
- персонализации;
- созданию новых услуг за счет унификации сетевых решений.

Мультисервисная сеть – сеть связи, которая построена в соответствии с концепцией NGN и обеспечивает предоставление неограниченного набора инфокоммуникационных услуг (VoIP, Интернет, VPN, IPTV, VoD и др.).

Сеть NGN – сеть с пакетной коммутацией, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортировки с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от примененных технологий, обеспечивающих транспортировку.

Возможности сети NGN:

- реализация универсальной транспортной сети с распределенной коммутацией;
- вынесение функций предоставления услуг в оконечные сетевые узлы;
- интеграция с традиционными сетями связи.

Сеть NGN должна обладать широким спектром возможностей – предоставлять возможности (инфраструктуру, протоколы) для целей создания, развертывания и управления всеми возможными видами услуг (известными или пока не известными). В данное понятие входят услуги, использующие данные различных типов (например, голосовые, видео, текстовые данные их различные комбинации и сочетания с другими типами данных).

Передача может осуществляться со всеми типами схем кодирования и технологий передачи данных, например, диалоговые передачи, с адресацией конкретному устройству, групповой адресацией и вещанием, услуги передачи сообщений, простой передачи данных в реальном масштабе времени и в автономном режиме, с регулированием задержки и устойчивые к задержке услуги. Услуги, предъявляющие различные требованиями к ширине полосе, с гарантированной полосой или без нее, должны поддерживаться с учетом технических возможностей используемой технологии передачи данных.

Особое внимание в сетях NGN уделяется гибкости реализации услуг в стремлении к наиболее полному удовлетворению всех требований заказчика. В некоторых случаях возможно также предоставление пользователю возможности настройки используемых им услуг. NGN должна поддерживать открытые интерфейсы программирования приложений, чтобы поддерживать создание, предоставление и управление услугами.

8.6.3. Современное состояние развития телекоммуникационных технологий связи

Обобщая вышеизложенное, можно сказать, что современное развитие телекоммуникационных сетей связи происходит через интеграцию всех функциональных возможностей, заложенных в модели транспортных сетей. Интеграция привела к созданию универсальных мультисервисных транспортных платформ с электрическими и оптическими интерфейсами, с

электрической и оптической коммутацией каналов и пакетов (кадров и ячеек), с предоставлением любых видов транспортных услуг, включая услуги автоматически коммутируемых оптических сетей с сигнальными протоколами, основанными на обобщённом протоколе коммутации по меткам GMPLS (Generalized Multi-Protocol Label Switching).

На рис. 8.14 представлена обобщенная архитектура транспортной платформы, в которой указаны возможные источники информационной нагрузки, протоколы согласования и транспортные технологии по информации из работы.

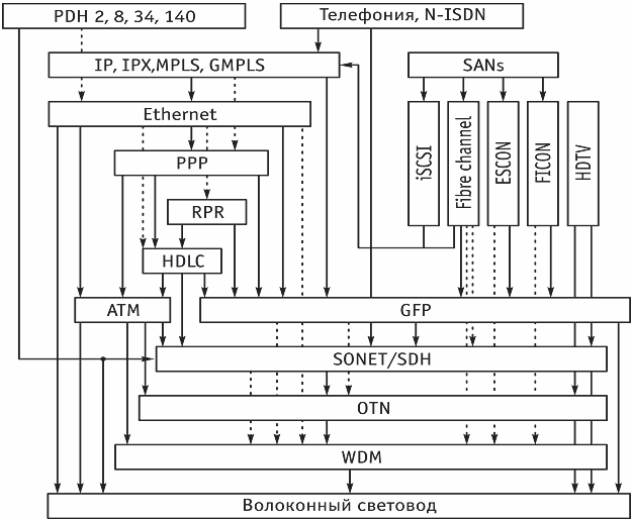


Рис. 8.14. Обобщенная архитектура оптической мультисервисной транспортной платформы

Обозначения на рис. 8.14:

- PDH, Plesiochronous Digital Hierarchy — плезиохронная цифровая иерархия (скорости 2, 8, 34 и 140 Мбит/с);
- N-ISDN, Narrowband Integrated Services Digital Network — узкополосная цифровая сеть с интеграцией служб (У-ЦСИС);
- IP, Internet Protocol — межсетевой протокол;
- IPX, Internet Packet eXchange — межсетевой обмен пакетами;
- MPLS, Multi-Protocol Label Switching — многопротокольная коммутация по меткам;
- GMPLS, Generalised MPLS — протокол обобщенной коммутации по меткам;
- SANs, Storage Area Networks — сети хранения данных (серверы услуг, базы данных);

- iSCSI, internet Small Computer System Interface — протокол для установления взаимодействия и управления системами хранения данных, серверами и клиентами;
- HDTV, High-Definition Television – телевидение высокой четкости;
- ESCON, Enterprise Systems Connection — соединение учрежденческих систем (с базами данных, серверами);
- FICON, Fiber Connection — волоконное соединение для передачи данных;
- PPP, Point-to-Point Protocol — протокол «точка-точка»;
- RPR, Resilient Packet Ring — протокол пакетного кольца с самовосстановлением;
- HDLC, High-level Data Link Control — протокол управления каналом высокого уровня;
- GFP, Generic Framing Procedure — процедура формирования общего кадра.

Протоколы PPP, RPR, HDLC, GFP в транспортных сетях выполняют функции согласования информационных данных от источников нагрузки с транспортными структурами с целью повышения эффективности использования ресурсов этих структур, например, виртуальных контейнеров высокого и низкого порядков в сети SDH или оптических каналов в сети OTN, или физических ресурсов кадров передачи сети Ethernet.

8.6.4. Общие понятия о глобальной сети Интернет

Интернет (англ. Internet) – всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство, служит физической основой для «всемирной паутины» (World Wide Web, WWW) и множества других систем (протоколов) передачи данных. Часто упоминается как «всемирная сеть» и «глобальная сеть», в обиходе иногда употребляют сокращённое наименование «Инет».

История Интернета началась в 1969 г., когда министерство обороны (МО) США организовало компьютерную сеть ARPANet (Advanced Research Project Agency Net – сеть Агентства перспективных исследовательских проектов). Сеть соединяла 4 компьютеров, которые находились в следующих учреждениях: Калифорнийском университете (Лос-Анджелес), Стэндфордском НИИ, университете г. Санта-Барбара и университете штата Юта. Через год сеть включала уже в 4 раза больше узлов (компьютеров). А к 1973 г. она разрослась и стала международной благодаря подключению узлов в Норвегии и в Англии (рис. 8.15).

В 1984 г. Национальный научный фонд США создал сеть NSFNET (National Science Foundation Network) для связи между компьютерами университетов и вычислительными центрами. В отличие от военной сети ARPANET подключение к сети NSFNET было достаточно свободным, и к

1992 г. к ней подключились более 7 500 небольших частных сетей, включая 2 500 сетей за пределами США. С передачей опорной сети NSFNET в 1995 г. в коммерческое использование появилась техническая основа современного Интернета.

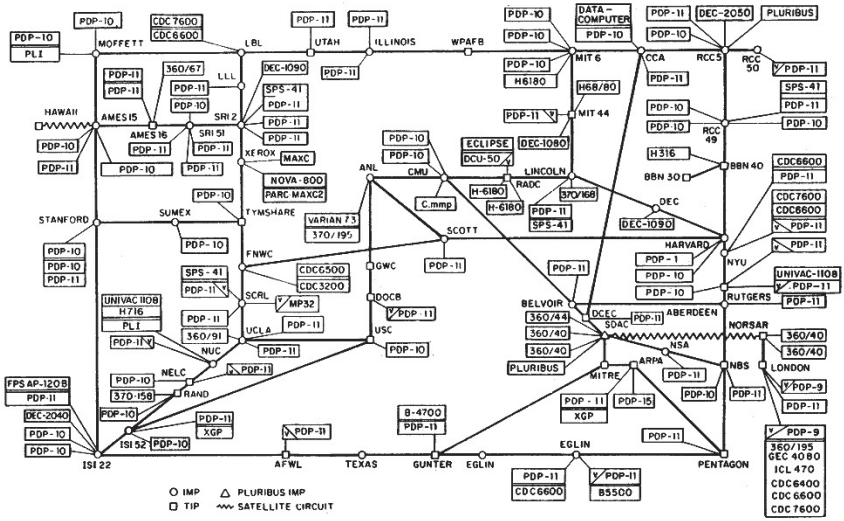


Рис. 8.15. Топологическая структура сети ARPANet в 1977 г.

На этапе зарождения сети Интернет, специалистами решались задачи обеспечения технической, программной и информационной совместимости различных компьютерных систем, функционирующих под управлением различных ОС и имеющих различное ПО, формирования разветвленной сетевой инфраструктуры, разработки и внедрения единого стека сетевых протоколов и интерфейсов. Фактически это были самые первые шаги в области обеспечения интероперабельности больших информационных ОТС.

В 1971 г. была разработана первая программа для отправки электронной почты и протокол отправки файлов по сети FTP (File Transfer Protocol), тогда же в 1970-х гг. появились первые коммуникационные программы – списки почтовых рассылок, новостные группы и электронные доски объявлений. Однако в то время сети ещё не могли легко взаимодействовать друг с другом из-за того, что были построены на различных технических стандартах. Это потребовало разработки и внедрения стандарта единых сетевых протоколов, которые были созданы и стандартизированы в 1982-1983 гг. С 1983 г. сеть ARPANET, перешла на единый сетевой протокол адресации и обмена данными TCP/IP, а в 1984 г. был разработан единый протокол разрешения доменных имен DNS (Domain Name System), которые используются до сих пор. В 1988 г. был разработан протокол мгно-

венного обмена сообщениями IRC (Internet Relay Chat), благодаря чему в Интернете стало возможно общение в чатах в режиме реальном времени. В 1989 г. был внедрен протокол BGP (Border Gateway Protocol), позволяющий объединять различные области маршрутизации, функционирующие на различных стеках сетевых протоколах. Именно протокол BGP, наряду с протоколами TCP/IP и DNS, является одним из основных технических решений, обеспечивающих функционирование сети Интернет. Наконец, в 1989 г. была разработана, а в 1991 г. уже внедрена концепция всемирной паутины WWW (World Wide Web), которая была основана на протоколе доступа к сайтам HTTP (HyperText Transfer Protocol), языке разметки сайтов HTML (HyperText Markup Language) и использовании гипертекстовых ссылок URL (Uniform Resource Identifier) которые позволяли связывать разные информационные ресурсы на различных сайтах между собой. С появлением браузеров – специальных программ просмотра информационных ресурсов WWW и перехода по URL, сеть Интернет приобрела те черты, которые знакомы сейчас каждому ее пользователю – множество сайтов, наполненных различными информационными ресурсами, связанными между собой гипертекстовыми URL ссылками.

В процессе своего развития топология сети Интернет прошла развитие (рис. 8.16):

– централизованные сети передачи данных;
– ячеистые децентрализованные сети;
– сетевой децентрализованный принцип построения сети.

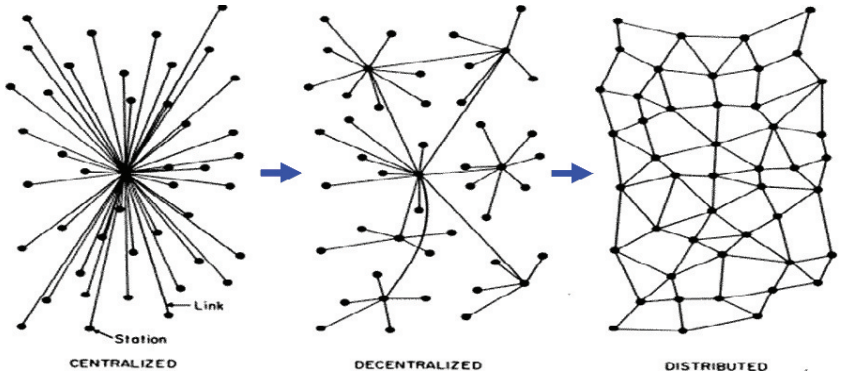


Рис. 8.16. Топологические изменения сети Интернет

В 1990-е годы Интернет объединил в себе большинство существовавших тогда сетей. Такое объединение происходило благодаря приоритетному использованию единых открытых сетевых стандартов. К 1997 г. в Интернете насчитывалось уже около 10 млн компьютеров и было зарегистрировано более 1 млн доменных имён. Интернет стал популярным сред-

ством для обмена информацией. Во второй половине 2010-х годов Интернет фактически подменил собой все классические средства получения информации, связи и коммуникации. Телевидение, радио и печатные издания – все они имеют полноценные онлайн-сайты, кроме того, существует безграничное множество интернет-сайтов, объединяющих все возможные формы коммуникации. К началу 2020 г. число пользователей Интернета достигло 4,5 млрд человек, что составляет более 50 % от всех жителей Земли. Во многом это обусловлено широким распространением единых протоколов сотовых сетей связи стандартов 3G, 4G и 5G, обеспечивающих высокоскоростной доступ в Интернет всех пользователей мобильных устройств (смартфонов), развитием социальных сетей и удешевлением стоимости интернет-трафика. По состоянию на 2022 г. самыми популярными Интернет-ресурсами являются социальные сети Facebook, Instagram, Twitter, мессенджеры WhatsApp, Viber, Telegram, а также энциклопедия Wikipedia и видеохостинг YouTube.

Несмотря на взрывное развитие сети Интернет, ее проникновение во многие стороны нашей повседневной жизни, нужно отметить что ее развитие шло во многом спонтанно и определялось теми или иными успешными коммерческими проектами, которые формировали де-факто некий общепринятый стандарт, который в дальнейшем становился стандартом де-юре. При развитии сети Интернет было решено множество технических и организационных задач:

- создание и внедрение единых открытых сетевых протоколов обмена различными типами данных (текстовые данные, файлы, речевые сообщения, видеоданные, финансовые транзакции и т.д.);
- разработка процедур обеспечения информационной безопасности пользователей;
- формирование единых форматов формирования, передачи, хранения и обработки данных.

Однако в решении этих задач зачастую отсутствовал единый замысел и системный подход к обеспечению интероперабельности, а преобладала коммерческая выгода и распространенность тех или иных протокольных, интерфейсных или технических решений. Все это нередко приводило к существенным проблемам. Так Интернет продолжает функционировать на основе стека протоколов TCP/IP, разработанного еще в 1983 г., чьи возможности по адресации узлов на основе 4-х байтного адреса были исчерпаны в 2011 г. Новые перспективные сетевые протоколы на основе технологий MPLS и ASON/ASTN внедряются медленно из-за необходимости обеспечения их обратной совместимости с устаревшими протоколами и парком старого сетевого оборудования. Коммерческие проприетарные протоколы таких ведущих производителей сетевого оборудования как Cisco, Juniper, Huawei широко используются в их маршрутизаторах и коммутаторах, но по факту они являются закрытыми программными решениями,

что повышает риски несовместимости между собой целых сетевых сегментов. Некоторые страны, например, Китай и Россия, приняли политические решения о частичной дезинтеграции своих национальных сегментов Интернета, от глобальной сети. Указанные обстоятельства, а также отсутствие единого системного подхода к развитию сети Интернет могло являться существенным барьером в последующем развитии мирового единого информационного пространства.

Материал главы 8 основан на обобщении информации, приведенной в работах [1, 19-23] и в материалах Интернет-ресурса [14]. Более подробные сведения о технологиях транспортных сетей представлены в работе [20].

9. Сети и системы абонентского доступа

9.1. Понятие сетей абонентского доступа

Одной из самых проблемных и динамично развивающейся частей современных сетей связи является доступ пользователей и абонентов к узлам связи транспортных сетей для предоставления телекоммуникационных услуг. При этом наблюдаются следующие тенденции развития доступа:

- использование существующей инфраструктуры низкочастотных медных линий для предоставления доступа к узкополосным и широкополосным услугам средствами модемов цифровых абонентских линий xDSL (Digital Subscriber Line) в разновидностях симметричных, асимметричных и высокоскоростных линий (HDSL, ADSL, VDSL), в которых могут передаваться сигналы на скоростях от десятков кбит/с до десятков Мбит/с (64 кбит/с – 50 Мбит/с) на относительно небольших расстояниях от десятков и сотен метров до нескольких километров;
- использование технологий: «волокно в дом», «волокно в распределительный шкаф», «волокно в офис» и т. д., обозначаемых FTTx (Fiber to the Home, …), например, пассивной оптической сети PON (Passive Optical Network), основанных на сети волоконно-оптических линий, для организации доступа к любым видам услуг;
- использование технологий радиодоступа RLL (Radio Local Loop) для фиксированного и мобильного, узкополосного и широкополосного доступа с разделением радиочастотных ресурсов по спектру частот, по времени, кодовым разделением, пакетной передачей; пример последнего – технология WiMAX.

Плоскость пользовательских услуг отражает все известные и востребованные услуги электросвязи, к которым относятся:

- телефония с коммутацией каналов и IP-телефония;
- видеосвязь, видеоконференции;
- Интернет, электронная почта;
- звуковое вещание;
- цифровое телевидение;
- и т. д.

Для реализации услуг необходимы различные терминалы для пользователей. Это и обычные телефонные аппараты, теле- и радиоприемники, терминалы сетевых подключений цифровых сетей с интеграцией услуг (ЦСИУ) или служб (ЦСИС) – ISDN (Integrated Services Digital Network), персональные компьютеры и т. д.

В связи с качественными изменениями, происходящими в развитии современных ТКС, и в частности с созданием мультисервисных сетей, осуществляется внедрение современных технологий и на абонентских сетях доступа. Новые концептуальные подходы к их построению приводят к тому, что понятие «абонентская линия» уже не отражает самой сути элемента сети электросвязи между терминалом пользователя и коммутационной станцией. Поэтому появился новый, принятый уже в международных стандартах и рекомендациях термин *«Access Network» – «сеть доступа»*. В отечественных концепциях ТКС чаще используется словосочетание *«сеть абонентского доступа»* (*САД*), что дает более четкое представление о соответствующем фрагменте телекоммуникационной системы. На рис. 9.1 показан фрагмент телекоммуникационной сети с выделенными типовыми элементами САД [24, 25].

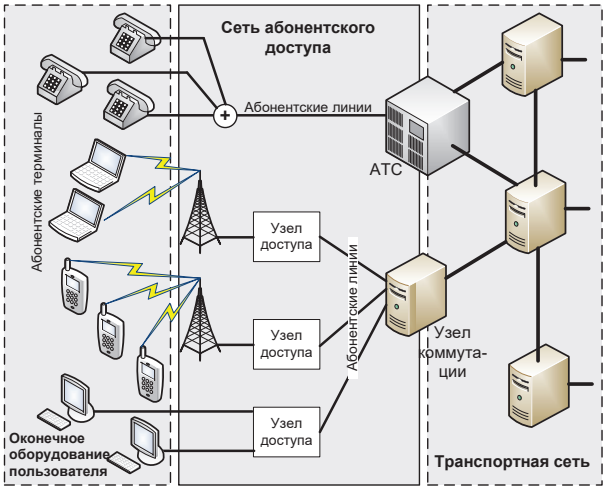


Рис. 9.1. Типовая структура и состав сетей абонентского доступа [24, 25]

Абонентская сеть в простейшем случае состоит из трех основных элементов:

– абонентского (пользовательского) терминала (АТ);
– абонентской (пользовательской) линии (АЛ);
– узла коммутации (УК).

В общем случае под *сетями пользовательского (абонентского) доступа* понимается совокупность линий, оконечных и промежуточных узлов, включаемых в коммутационное оборудование транспортной сети непосредственно или через выносной модуль (концентратор, мультиплексор) [24, 25].

Структурно САД располагается между оборудованием, помещающимся непосредственно в месте расположения абонентов (пользователей),

и транспортной сетью. Границей между САД и терминальным оборудованием может быть распределительная коробка или розетка, к которой подключается АТ. Граница между САД и транспортной сетью проходит в месте установки УК, в абонентские комплекты которого входят подключаемые АЛ [24].

На рис. 9.2 представлена модель САД, основанная на новых подходах к ее построению. В соответствии с этой моделью, САД состоит из двух узловых элементов. Первый представляет собой совокупность подсетей АЛ, образующих сеть АЛ, а второй – непосредственно подсеть доступа (именуемую еще базовой сетью, распределительной сетью или сетью переноса).

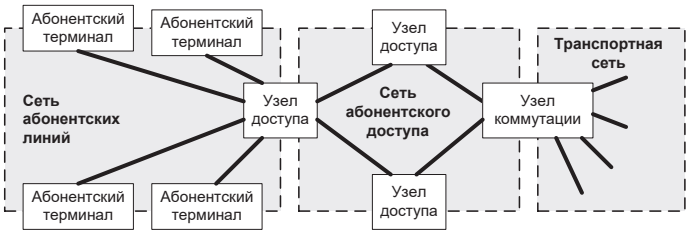


Рис. 9.2. Модель сети абонентского доступа

Каждая подсеть АЛ обеспечивает подключение абонентов (пользователей) к узлу доступа (УД) или УК непосредственно или через мультиплексор [1, 24].

9.2. Проблема «последней мили»

Проблему абонентского доступа к услугам телекоммуникационной сети на участке «абонентский терминал – узел доступа» с тем же качеством, что и непосредственно в телекоммуникационной сети, принято называть проблемой «*последней мили*» [1, 24].

Сети абонентского доступа с малой пропускной способностью (низкой скоростью передачи информации и соответственно с узкой полосой пропускания – «узким горлышком бутылки») в настоящее время перестали обеспечивать растущие потребности пользователей. Поэтому во многих странах мира построение высокоскоростных, т. е. широкополосных, сетей доступа стало приоритетным направлением их развития.

Различные концептуальные решения по этому направлению разрабатывались в международных организациях. Так, например, в отчете МСЭ-Т за 2001 г. *широкополосный доступ* (ШПД) определяется как возможность передачи с достаточной полосой пропускания, позволяющей предоставлять услуги голосовой связи, передачи данных и видео в одном потоке. Более точные требования к полосе пропускания определяются используемыми абонентом приложениями: такими как электронная почта, просмотр

Web-страниц, загрузка аудио- и видеоклипов, игры on-line (infotainment – информация и развлечения), видеоконференции, интерактивное телевидение, доступ к дискуссионным группам и базам данных и т. п.

Исследователями и разработчиками международных организаций и промышленных компаний в последние годы формировались различные концептуальные положения по решению проблемы «последней мили». Эти положения базируются на ряде технологий, физической основой для которых способны стать как проводные, так и радиосреды передачи [1, 24].

Специальные технологии абонентского доступа прежде всего нацелены на образование цифровых каналов на основе доступной физической среды, разновидности которой можно разделить на две группы [1, 24]:

1. Физические среды проводного доступа [1, 24]:
– оптическое волокно;
– коаксиальный медный кабель;
– витая пара (тоже медный кабель).
2. Физические среды беспроводного доступа [1, 24]:
– оптические электромагнитные волны;
– радиоволны (тоже электромагнитные);
– звуковые (акустические) волны (неэлектромагнитные).

Перспективные концепции построения САД ориентируются, в основном, на физические среды, позволяющие передавать высокоскоростные потоки информации, то есть, прежде всего – на оптоволокно.

9.2.1. Направления решения проблемы «последней мили»

Главной движущей силой развития технологий абонентского доступа становятся новые информационные потребности абонентов (пользователей) в услугах электросвязи. При этом с одной стороны (со стороны сети) появились службы, готовые удовлетворить данные потребности (в основном, в виде соединений с заданным качеством отдельных абонентов и в виде предоставления доступа к общим информационным ресурсам), а с другой стороны (со стороны абонентов) остались преимущественно старые физические линии доступа, не способные реализовать новые потребности.

Выделяют три направления удовлетворения новых информационных потребностей пользователей за счет развития технологий абонентского доступа [1, 24]:

1) увеличение скорости передачи и предоставление новых услуг тем абонентам, которые уже имели доступ к сети, и в тех точках доступа, которые уже существовали ранее;
2) подключение новых абонентов в тех местах, где прежде не было точек подключения, с предоставлением полного набора современных услуг;

3) подключение подвижных абонентов и предоставление им сервисов, соизмеримых по качеству с услугами, которые предоставляются фиксированным абонентам.

Если первые два направления не исключают «персональную мобильность абонентов», перемещающихся между фиксированными точками доступа (подключения), то третье направление призвано обеспечить «мобильность терминалов». В целом же от сети абонентского доступа требуется гарантировать персональный доступ к любым информационным и телекоммуникационным услугам любым абонентам – независимо от их местонахождения, то есть обеспечить персональную глобальную связь по принципу «всегда и везде».

В настоящее время наметились четыре наиболее характерных пути решения проблемы «последней мили» [1, 24].

1) *Строительство ВОЛС на абонентском участке*. Строительство ВОЛС на участке «последней мили» имеет ряд очевидных достоинств и соответствует перспективным концепциям. Стоимость оптического кабеля (ОК) неуклонно снижается, причем оптические АЛ служат достаточно долго и не требуют особого внимания. Однако для прокладки кабеля необходимы трудовые и временные затраты специально подготовленных работников, а также недешевое оконечное оборудование приема/передачи и мультиплексирования, что увеличивает стоимость АЛ.

2) *Прокладка медно-кабельных абонентских линий.* Это традиционное решение имеет ряд положительных моментов: простое проектирование, наличие опытного персонала по строительству и эксплуатации, приемлемая стоимость. Основные недостатки: дорогое обслуживание и ограниченная – по сравнению с ВОЛС – пропускная способность при тех же трудовых и временных затратах на строительные работы. В последнее время отмечается еще один «специфический» недостаток – привлекательность медных кабелей для сборщиков металлолома.

3) *Уплотнение существующих* (*медно-кабельных*) *абонентских линий.* Идея уплотнения АЛ родилась давно. Аналоговое оборудование высокочастотного уплотнения широко используется в телекоммуникационных сетях до сих пор. Однако своим подлинным развитием данное решение обязано появлению цифровых абонентских линий ЦАЛ (DSL – Digital Subscriber Loop или Line). Технологии xDSL (где x является обобщенным символом различных аббревиатур, соответствующих различным вариантам DSL) позволили организовать высокоскоростную цифровую передачу по существующим АЛ.

Технологии DSL открыли новые возможности для предоставления коммуникационных услуг, так как полоса пропускания абонентского шлейфа теперь не ограничивается 4 кГц, как это было в традиционной аналоговой телефонии. Расширить полосу пропускания оказалось реальным с помощью специальных линейных кодов и техники цифровых сигнальных процессоров. Технологии DSL используют различные схемы линейного кодирования: CAP, 2B1Q, PAM и др. Линейное кодирование – это алго-

ритм преобразования сигнала, предназначенный для надежной помехоустойчивости передачи данных по медному проводу. Например, новая технология линейного кодирования Trellis Coded – PAM (TC-PAM), лежащая в основе нового перспективного стандарта SHDSL, уменьшает мощность сигнала, увеличивает дальность передачи и позволяет кодировать больше данных внутри частотного спектра [1, 24 26].

Допустимая длина ЦАЛ, как правило, составляет не более 5-6 км (в случае диаметра жилы кабеля 0,4-0,5 мм). Используя регенераторы, несложно увеличить допустимую длину ЦАЛ. «Допустимой» обычно считается длина, при которой вероятность ошибки на бит не превышает 10^{-7}. Существуют и более строгие международные и российские ведомственные нормативы, разработанные для цифровых первичных сетей, которые часто применяют для оценки пригодности ЦАЛ.

Дополнительным резервом построения САД на базе существующих проводных «абонентских линий» служат [1, 24]:

- проводная разводка радиоточек;
- линии электропередач (например, известны технологии X.10 и DPL – Digital Power Line, которая позволяет передавать данные по электропроводке со скоростью до 1 Мбит/с и др.);
- сети кабельного телевидения (во многих городах уже применяются для доступа в Интернет).

4) *Использование технологий беспроводного абонентского доступа.* В последнее время значительно возрос интерес к технологиям беспроводного абонентского доступа, именуемым WLL-технологиями (Wireless Local Loop). Более распространенные технологии радиодоступа (в отличие от технологий оптического беспроводного доступа) сокращенно называют RLL (Radio Local Loop) [1, 24].

Технологии беспроводного абонентского доступа имеют бесспорное преимущество перед проводными решениями [1, 24]:

- применение в местах отсутствия кабельной инфраструктуры, а также в труднодоступных и малонаселенных районах;
- быстрое развертывание и ввод в эксплуатацию;
- организация доступа в любом месте (в пределах зон покрытия);
- поддержание связи при движении абонентов.

Главные недостатки WLL – ограниченная пропускная способность и относительно высокая стоимость в расчете на одного абонента, а также традиционные для радиосвязи проблемы «открытости» к внешним воздействиям.

В настоящее время существует огромное множество WLL-технологий, которые условно разделяются на две большие группы [1]:

- фиксированной связи;
- подвижной связи.

Традиционно аббревиатуру WLL применяют в узком смысле для обозначения первой группы технологий – фиксированного беспроводного

абонентского доступа. Технологии же подвижной, или иначе мобильной, связи обычно рассматривают как самостоятельную группу технологий, среди которых принято различать технологии сотовой, транкинговой, пейджинговой и спутниковой связи.

Очевидно, что подвижную связь всегда можно использовать как фиксированную. Обратное же не всегда приемлемо. С другой стороны, фиксированная связь позволяет обеспечить предоставление широкополосных услуг с качеством, соизмеримым с качеством услуг, предоставляемых проводными технологиями, что пока не в состоянии позволить себе подвижная связь.

9.2.2. Технологии решения проблемы «последней мили»

Технологии обеспечения доступа к транспортным сетям можно разделить на три категории, в зависимости от того, какая физическая среда используется для передачи данных [1, 27]:

- витая пара телефонных проводов;
- оптико-волоконные кабели (к этой категории также следует отнести системы, в которых вместе с оптико-волоконными кабелями используются также и коаксиальные кабели);
- беспроводные системы (например, системы сотовой, радиорелейной или спутниковой связи).

Рассмотрим все три категории более подробно, причем начнем в обратном порядке.

1) Беспроводные системы доступа. Развитие беспроводных систем доступа идет в двух основных направлениях [1, 27]:

- системы персональной сотовой связи, которые позволяют обеспечить доступ мобильных пользователей (рис. 9.3);
- наземные радиорелейные системы на СВЧ;
- спутниковые системы (рис. 9.4).

2) Системы доступа, основанные на новых и уже существующих оптико-волоконных и коаксиальные кабелях [1, 27]:

- оптико-волоконные систем передачи (рис. 9.5);
- сети кабельного телевидения (рис. 9.6);
- телефонные сети связи на витой медной паре (рис. 9.7).

Рис. 9.3. Доступ в транспортную сеть может быть организован посредством существующей системы сотовой связи

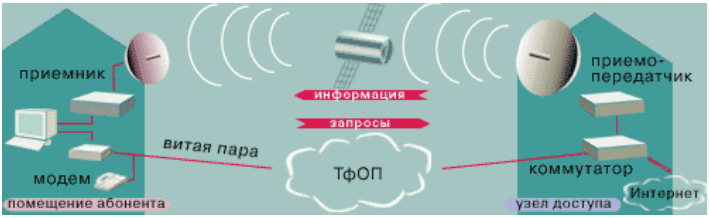


Рис. 9.4. Спутниковая система связи с ассиметричным каналом связи

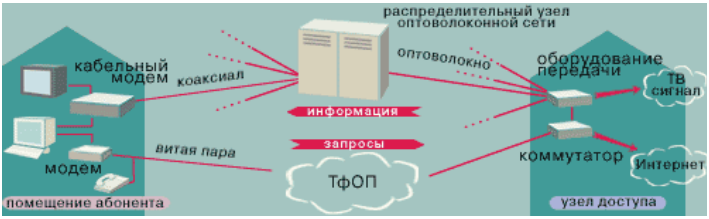


Рис. 9.5. Гибридная система кабельного телевидения, построенная на комбинации оптико-волоконных и коаксиальных кабелей

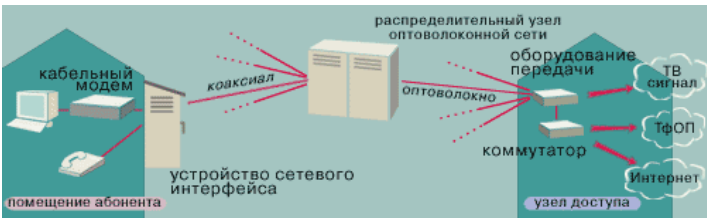


Рис. 9.6. Система кабельного телевидения, позволяющая организовать высокоскоростную передачу данных в обоих направлениях

Рис. 9.7. Организация доступа по существующим телефонным проводам по технологии xDSL

9.3. Классификация и краткая характеристика технологий проводного абонентского доступа

В соответствии с работой [1, 28] технологии проводного абонентского доступа можно разбить на пять основных групп по критерию среды передачи и категориям пользователей (рис. 9.8):

1. LAN (Local Area Network) – технологии предоставления корпоративным пользователям услуг доступа к ресурсам локальных вычислительных сетей и использующих в качестве среды передачи структурированные кабельные системы категорий 3, 4 и 5, коаксиальный кабель и оптоволоконный кабель.
2. DSL (Digital Subscriber Line) – технологии предоставления пользователям ТфОП услуг мультимедиа и использующих в качестве среды передачи существующую инфраструктуру ТфОП.
3. Optical Access Networks (OAN) – технологии предоставления пользователям широкополосных услуг, линии доступа к мультимедийным услугам и использующих в качестве среды передачи оптоволоконный кабель (технологии PON) или смешанные медно-оптические линии связи (технология FTTx).
4. Кабельное телевидение (КТВ) – технологии предоставления пользователям сетей КТВ мультимедийных услуг (за счет организации обратного канала) и использующих в качестве среды передачи оптоволоконный и коаксиальный кабели.
5. Сети коллективного доступа (СКД) – гибридные технологии для организации сетей доступа в многоквартирных домах; в качестве среды передачи используется существующая в домах инфраструктура ТфОП, радиотрансляционных сетей и сетей электропитания.

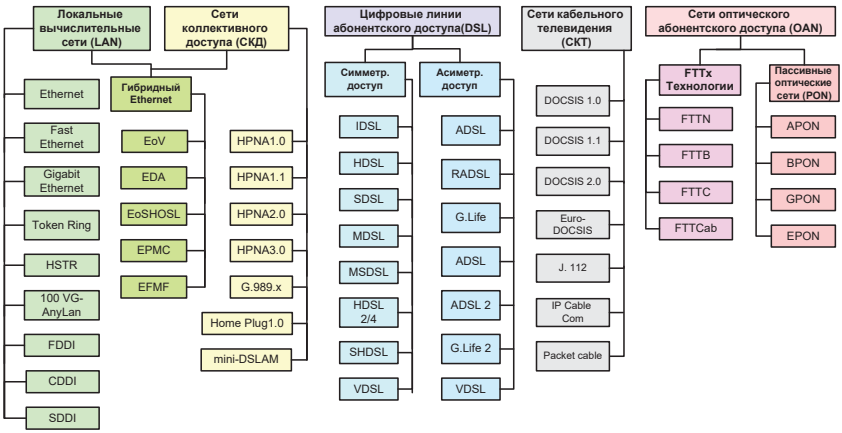


Рис. 9.8. Классификация технологий проводного доступа [1, 28]

9.4. Технологии локальных сетей, коллективного доступа и кабельного телевидения

9.4.1. Технологии локальных сетей

В группе САД типа LAN более 90% всех сетей построены с использованием технологии Ethernet, она обеспечивает пользователям корпоративных сетей скорости передачи информации от 10 Мбит/с до 1 Гбит/с. Широкое распространение сетей Ethernet при организации LAN, в первую очередь, связано с низкой стоимостью, легкостью управления и простотой используемого оборудования. Разрабатывавшаяся в конце 1970-х гг. исключительно для передачи данных технология Ethernet обеспечивает сейчас поддержку широкого набора услуг, включая передачу речи и видео с требуемым качеством обслуживания QoS (IEEE 802.1p), а также организацию VLAN (IEEE 802.1Q). Подробно основы технологии Ethernet представлены в п. 4.7 данной работы и здесь не рассматриваются.

В технологиях доступа в последнее время наметилась интеграция технологии Ethernet с различными технологиями DSL (*гибридный Ethernet*). Наиболее известным вариантом такой интеграции является *технология EoV* (Ethernet-over-VDSL). При скорости передачи порядка 10 Мбит/с сеть Ethernet может располагаться на расстоянии до 1,5 км от узла доступа, а при скоростях 3-4 Мбит/с это расстояние возрастает до 3-4 км. Стандарт на EoV разрабатывается в двух вариантах [1, 28, 29]:

- *EFMC* (*EFM Copper*), имеющий характеристики обслуживания, аналогичные EoV;
- *EFMF* (*EFM Fiber*), обеспечивающий скорость передачи от 100 Мбит/с до 1 Гбит/с на расстояние в несколько десятков километров до узла доступа.

Известны также следующие решения [1]:

- Ethernet с использованием ADSL компании Ericsson (EDA – Ethernet DSL Access) со скоростями передачи 8/2,8 Мбит/с и дальностью до 4 км;
- Ethernet с использованием SHDSL компании Shmid telecom со скоростью передачи 2,3 Мбит/с и дальностью до 5 км.

Необходимо отметить, что в настоящее время в данной группе все большее распространение получают беспроводные сети доступа к глобальной сети, организованные по стандартам WiFi, WiMAX, а также доступ через сети мобильных операторов сотовой связи по стандарту 4G. Эти технологии подробно рассмотрены в п. 5 данной работы.

9.4.2. Технологии сетей коллективного доступа

Для организации относительно недорогого доступа в Интернет жителей многоквартирных домов разработаны технологии сетей коллективного доступа (СКД) [1, 28]:

– Home PNA (HPNA);
– Power Line Communication (PLC).

Сеть доступа развертывается на существующей в доме кабельной инфраструктуре (витая медная пара, проводка радиотрансляционных сетей, электрическая проводка), а концентратор трафика может подключаться к узлу служб с использованием различных систем передачи (кабельных, радио и др.).

Для домашних сетей подходит оборудование гибридных Ethernet или mini-DSLAM при использовании в качестве концентратора трафика мультиплексоров DSL [1, 28].

Стандарты HPNA появились в результате деятельности альянса Home Phoneline Networking Alliance, созданного в 1996 г. для разработки технологии, которая на основе существующей в домах кабельной сети должна была обеспечить относительно недорогой доступ в Интернет. Технология HPNA стандартизована в ITU-T (рекомендации G.989.1 и G.989.2). Стандарт HPNA 1.0 создан в 1998 г. Для передачи сигналов используется полоса частот 4…10 МГц, поэтому системы HPNA не оказывают влияния па телефонные и другие системы, работающие по тому же кабелю.

Системы доступа HPNA 1.0 обеспечивают коллективный доступ к каналу с пропускной способностью 1 Мбит/с на расстояние до 150 м. В качестве метода доступа к среде передачи применяется CSMA/CD. Для передачи информации используется модуляция DMT. Типовая топология сети – «звезда». Ядро сети – коммутатор HPNA, порты которого подключаются к соответствующей абонентской линии. Максимальное количество абонентов в сети – 32. В стандарте HPNA 1.1 дальность действия оборудования увеличена до 300 м.

В сетях стандарта HPNA 2.0, появившегося в 2000 г., пропускная способность коллективного канала увеличена до 10 Мбит/с при дальности действия системы до 350 м. Типовая топология сети – «шина». Работа такой сети не требует применения коммутаторов и других активных устройств.

В настоящее время ведется разработка нового стандарта HPNA 3.0, по которому пропускная способность домашней сети должна достигнуть 100 Мбит/с [1, 28].

Разработкой стандартов технологии PLC (Power Line Communications), реализуемой на базе инфраструктуры сетей электропитания, занимаются различные международные организации, такие как PLC Forum. Powerline World и Home Plug Powerline Alliance. Последняя из них приняла в 2001 году единый стандарт HomePlug 1.0 specification, в котором определены скорости передачи данных до 14 Мбит/с, методы доступа к среде передачи CSMA/CD или CSMA/CA и модуляции OFDM. Стандартизация PLC-технологии ведется также и в ETSI (стандарты: TS 101 867, TS 101 896, TR 102 049) [1, 28].

9.4.3. Технологии кабельных телевизионных сетей

Использование сетей кабельного телевидения (КТВ) для построения интерактивных сетей доступа к мультимедийным услугам стало возможным с появлением в 1997 г. стандарта DOCSIS (Data over Cable Service Interface Specification), разработанного по инициативе организации операторов кабельных сетей Северной Америки MCNS (Multimedia Network System Partners Ltd.). Для построения гибридных (HFC – Hybrid Fiber Coaxial) сетей КТВ сегодня имеется следующие стандарты:

- четыре американских (DOCSIS);
- один европейский (Euro-DOCSIS);
- международные (рек. ITU-T J.112, J.222), объединяющий требования американских и европейского стандартов.

Дальнейшее развитие европейского (Euro-DOCSIS) и американского (Euro-DOCSIS) вариантов спецификаций на HFC-сети продолжается в части создания дополнительных возможностей и внедрения новых услуг. Отличие европейских и американских сетей КТВ обусловлено методами сигнализации и организации интерфейса V5, методами обеспечения безопасности и т.д. Для организации прямого канала в сетях КТВ США применяется полоса частот 6 МГц (рек. J.83.B. ITU-T) в диапазоне частот 88-860 МГц. При использовании модуляции 256QAM скорость передачи данных в прямом канале достигает 42 Мбит/с. В Европе для этих целей занимается полоса частот 8 МГц (рек. J.83.A ITU-T) в диапазоне частот 108-862 МГц, а скорость передачи составляет 52 Мбит/с. Разработки европейской спецификации технологии интерактивных HFC-сетей ведется в настоящее время под общим названием IPCablcCom. В США подобная разработка проводится в лаборатории CableLabs в рамках проекта PacketCable. Совершенствование этих технологий идет по пути создания дополнительных возможностей и внедрения новых услуг. Основные отличия спецификации связаны с особенностями построения телекоммуникационных сетей в Европе и США [1, 28, 31].

Рассмотрим различные реализации стандартов КТВ.

DOCSIS 1.0. Этот стандарт был создан для сетей КТВ США. Он определяет физический и MAC-уровни, уровень управления для кабельных модемов и головных станций, принципы обеспечения сетевой безопасности и качества обслуживания. Для организации обратного канала используется диапазон 5…42 МГц. Метод доступа к обратному каналу – TDMA, методы модуляции – QPSK и 16QAM, скорость передачи – до 1 Мбит/с. Для защиты информации используется стандарт цифрового шифрования DES с длиной ключа 40 бит. Модель обеспечения качества обслуживания основана на классах обслуживания QoS. Прямой канал с полосой частот 6 МГц (рек. J.83.B ITU-T) может быть организован в диапазоне частот 88…860 МГц. Методы модуляции в прямом канале – 64QAM и 256QAM, скорости передачи соответственно 30,34 и 42,88 Мбит/с.

DOCSIS 1.1. Вторая версия стандарта была создана в 1999 г. В ней была увеличена скорость передачи в обратном канале до 5 Мбит/с, улучшена эффективность использования пропускной способности обратного канала за счет введения механизмов фрагментации пакетов и подавления заголовков, повышена сетевая безопасность благодаря введению аутентификации кабельных модемов.

DOCSIS 2.0. В третьей версии стандарта, опубликованной в 2002 г., пропускная способность обратного канала увеличена до 30,72 Мбит/с при ширине полосы частот до 6,4 МГц. В качестве метода доступа к обратному каналу используются варианты Advanced TDMA (A-TDMA) или Synchronous CDMA (S-CDMA). В обратном канале дополнительно используются методы модуляции 8QAM, 32QAM, 64QAM, а также 128QAM с решетчатым кодированием.

Euro-DOCSIS. Эта спецификация представляет собой вариант американского стандарта DOCSIS, адаптированного к европейским кабельным сетям. Для организации обратного канала выделен диапазон 5…65 МГц, для прямого канала – 108…862 МГц. Полоса частот в прямом канале – 8 МГц (рекомендация J.83.A ITU-T). Методы модуляции в прямом канале – 64QAM и 256QAM, скорости передачи соответственно около 37 Мбит/с и 52 Мбит/с.

Международный стандарт ITU-T J.222. В 2006 г. ITU-T утвердил спецификацию DOCSIS 3.0. в качестве международного стандарта. Он позволяет объединять каналы, тем самым увеличивая скорость доступа. Объединяются до 16 прямых и 8 обратных каналов. Скорость прямого канала до 400 Мбит/с и до 122 Мбит/с – обратного. Также в DOCSIS 3.0 появилась поддержка multicast, шифрования AES и др.

DOCSIS 3.1. Впервые представлен в 2013 г. Стандарт DOCSIS 3.1 регламентирует скорость прямого канала 10 Гбит/с и более и 1 Гбит/с обратного канала, за счёт использования схемы модуляции 4096QAM. Здесь вместо частотного разделения каналов шириной 6 МГц и 8 МГц используются поднесущие шириной от 20 кГц до 50 кГц с OFDM-мультиплексированием. Поднесущие можно уложить в спектр шириной вплоть до 200 МГц. DOCSIS 3.1 также регламентирует средства управления энергопотреблением что позволит снизить энергоёмкость индустрии кабельного телевидения. Коммерческое внедрение нового стандарта ведется с 2019 г.

DOCSIS 4.0. Стандарт обеспечивает симметричные сервисы, оставаясь обратно совместимым с DOCSIS 3.1. КCableLabs выпустила полную спецификацию стандарта в 2017 г. вначале как DOCSIS 3.1 Full Duplex, однако в последствии этот новый стандарт впоследствии был переименован в DOCSIS 4.0.

Таблица 9.1 – Максимальная скорость передачи в Мбит/с для различных версия стандартов КТВ

Версия	DOCSIS		EuroDOCSIS	
	Прямой канал (Down)	Обратный канал (Up)	Прямой канал (Down)	Обратный канал (Up)
1.x	42,88 (38)	10,24 (9)	55,62 (50)	10,24 (9)
2.0	42,88 (38)	30,72 (27)	55,62 (50)	30,72 (27)
3.0 4-х канальная версия	+171,52 (+152)	+122,88 (+108)	+222,48 (+200)	+122,88 (+108)
3.0 8-ми канальная версия	+343,04 (+304)	+122,88 (+108)	+444,96 (+400)	+122,88 (+108)
3.1	10 000	2 000	10 000	2 000
4.0	10 000	10 000	10 000	10 000

9.5. Технологии доступа на основе цифровых телефонных абонентских линий DSL

9.5.1. Обзор технологии DSL

В последние годы развитие САД является наиболее динамичным сегментом телекоммуникационной отрасли. Они непосредственно связаны с предоставлением операторских услуг абонентам, поэтому САД хорошо окупаются даже в условиях неблагоприятной экономической ситуации. Поэтому можно с уверенностью сказать, что САД находятся в фазе развития, что делает их технически и финансово привлекательными.

Традиционно абонентские кабельные сети состояли из двух видов:

- телефонные сети на медных НЧ кабелях;
- распределительные коаксиальные сети кабельного или эфирного телевидения.

Хотя телефония и сейчас остается наиболее востребованной услугой, значительно вырос спрос на услуги доступа к транспортным сетям (не только среди офисных центров, но и среди домашних пользователей. В последнее время популярна концепция «тройной услуги» которая предусматривает предоставление через одну сеть услуг: телефонии, передачи данных и видеоинформации. Кроме того, повышение спроса на широкополосный доступ определяется развитием новых технологий [27]:

- видео по запросу (VOD – Video on Demand);
- потоковое видео, видеоконференции;
- интерактивные игры;
- передача голоса в компьютерных сетях (VoIP);
- телевидение высокой четкости (HDTV) и др.

Сеть, состоящая из пар витых медных проводов, которая изначально предназначалась только для обеспечения телефонной связи между различными абонентами (рис. 9.9), постепенно превращается в сеть широкополосных каналов, способных поддержать высокоскоростную передачу данных и другие широкополосные телекоммуникационные службы.

Разработанная для аналоговых телефонных линий технология (аналоговые модемы, предназначенные для передачи по телефонным линиям) имеет очень ограниченную скорость передачи данных – до 56 кбит/с. Но, благодаря использованию на абонентской кабельной сети современных технологий, разработанных специально для витых пар проводов, те же самые линии, которые ранее использовались для традиционной телефонной связи и передачи данных со скоростью до 56 Кбит/с, могут поддерживать эффективную высокоскоростную передачу данных, при этом сохраняя возможность одновременного использования абонентской линии и для традиционной телефонной связи.

Новую ступень развития удалось преодолеть благодаря использованию технологий DSL (рис. 9.10) [27].

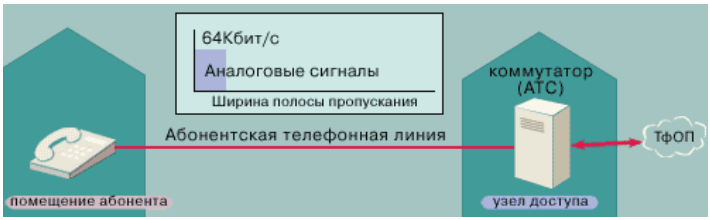


Рис. 9.9. Использование полосы пропускания канала в телефонии [27]

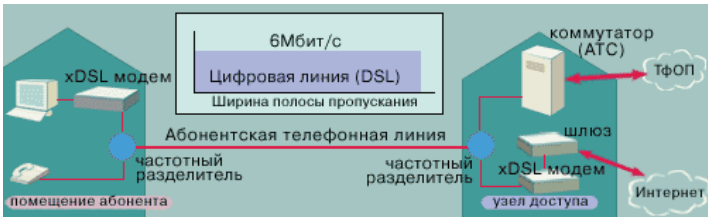


Рис. 9.10. Использование полосы пропускания канала при организации DSL [27]

Для конечных пользователей технологии DSL обеспечивают высокоскоростное и надежное соединение между сетями или с сетью Интернет, а телефонные компании получают возможность исключить потоки данных из своего коммутационного оборудования, оставляя его исключительно для традиционной телефонной связи.

Обеспечение высокоскоростной передачи данных по медной двухпроводной абонентской телефонной линии достигается установкой оборудования DSL на абонентском конце линии и на «конечной остановке» маги-

стральной сети высокоскоростной передачи данных, которая должна находится на телефонной станции, которой подключена данная абонентская линия. Если на абонентской линии с использованием технологии DSL организована высокоскоростная передача данных, информация передается в виде цифровых сигналов в полосе гораздо более высоких частот, чем та, которая обычно используется для традиционной аналоговой телефонной связи. Это позволяет значительно расширить коммуникационные возможности существующих витых пар телефонных проводов [27].

Использование технологий DSL на абонентской телефонной линии позволило превратить абонентскую кабельную сеть в часть сети высокоскоростной передачи данных [27]. Кроме обеспечения высокоскоростной передачи данных, технологии DSL являются эффективных средством организации многоканальных служб телефонной связи. С помощью технологии VoDSL (голос по DSL) можно объединить большое количество каналов телефонной (голосовой) связи и передать их по одной абонентской линии, на которой установлено оборудование DSL [27]. Все технологии DSL (ISDN, HDSL, SDSL, ADSL, VDSL и SHDSL) разработаны для обеспечения высокоскоростной передачи данных по телефонным линиям, изначально предназначенным для осуществления голосовой связи в спектре частот 300 Гц-3,4 кГц.

Развитие технологий цифровой обработки сигнала (DSP) в сочетании с новейшими алгоритмами и технологиями кодирования позволили поднять информационную емкость сетей доступа до 55 Мбит/с. Ширина используемой полосы частот увеличилась на два порядка за последнее десятилетие: от приблизительно 100 кГц для узкополосной ISDN до более чем 10 МГц для VDSL [27].

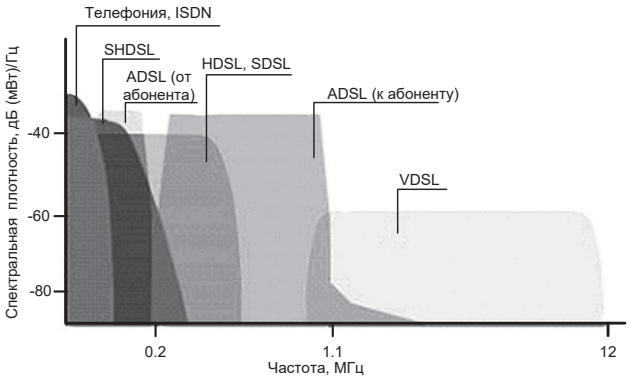


Рис. 9.11. xDSL-технологии и занимаемые ими частоты (по данным компании ZyXEL)

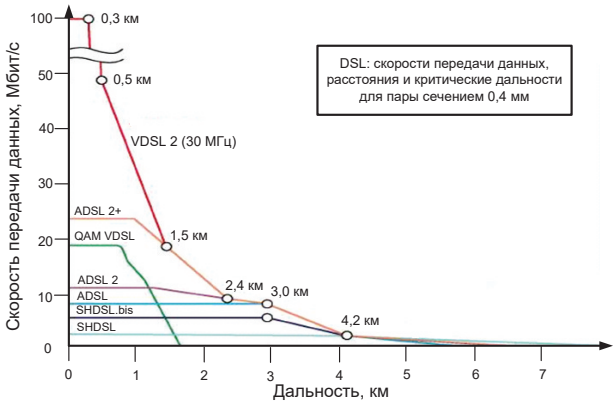


Рис. 9.12. Зависимость скорости передачи данных от расстояния для пары сечением 0,4 мм (по данным компании ZyXEL)

Пополняемое семейство технологий DSL (Digital Subscriber Line, цифровая абонентская линия) является достаточно новым и позволяет эффективно использовать полосу пропускания медных телефонных линий. Благодаря многообразию xDSL пользователь может выбрать для себя подходящий вариант по скорости приема/передачи данных – от 32 Кбит/с до более чем 50 Мбит/с. И в первую очередь выбор будет основываться на типе и количестве имеющихся у пользователя пар, их качестве и протяженности. При этом следует определиться с необходимостью одновременного использования и аналоговой телефонной связи, и цифровой высокоскоростной передачи данных по одним и тем же линиям, соединяющим телефонные станции с абонентами [27].

На данный момент все многообразие протоколов DSL можно разделить на два класса [27]:

– симметричные;
– несимметричные.

Первые, как правило, требуются крупным компаниям для налаживания равноправного обмена. Например, SHDSL-оборудование изначально нацелено на решение задач, требующих высокой надежности передачи данных с гарантированным качеством обслуживания. Передачи симметричных потоков данных в обе стороны необходимы, при многоканальном голосовом обмене и для видеоконференц-связи.

Вторые отражают суть работы с IT-технологиями мелких компаний, филиалов, удаленных офисов и частных пользователей – большая часть трафика загружается из глобальных сетей, а от клиента зачастую исходят лишь запросы на получение информации и отсылаются квитанции-подтверждения. Поэтому вполне закономерно, что по числу подключенных клиентов ADSL стала наиболее востребованной и массовой технологией широкополосного удаленного доступа в мире [27].

Подробные технические характеристики отдельных технологий DSL, а также их типовое применение приведены в таблицах 9.2–9.5 ниже.

Таблица 9.2 – Сравнительные возможности наиболее значимых технологий xDSL

Критерий	G.SHDSL	ADSL	ADSL2	ADSL2+	ADSL2++	VDSL
Число пар в линии	До 4	1	1	1	1	до 2
Длина линии сечением 0,4 мм, км	до 6 без регенерации, до n×6 с регенерацией	5	5	5	5	до 1,2 по 1 паре до 2 по 2 парам
Максимальная скорость (к абоненту/от абонента), Мбит/с	2,3 по 1 паре 4,6 по 2 парам	8/1	12/1	24/2	48/3	18/16 (QAM) 50/30 (DMT)
Работа «поверх» телефонной линии	нет	да	да	да	да	да
Регенерация	Только для цифровых потоков	нет	нет	нет	нет	нет
Возможность работы модема «друг на друга»	да	нет	нет	нет	нет	да

Таблица 9.3 – Сравнение технологий xDSL

Технология DSL	Тип передачи Максимальная скорость (прием/передача)	Max расстояние	Кол-во телефонных пар	Основное применение
ADSL	Асимметричный 24 Мбит/с / 3,5 Мбит/с	5,5 км	1	Доступ в Интернет, голос, видео, HDTV (ADSL2+)
IDSL	Симметричный 144 кбит/с	5,5 км	1	Передача данных
HDSL	Симметричный 1,544…2,048 Мбит/с	4,5 км	1,2	Объединение сетей, услуги E1
SDSL	Симметричный 2 Мбит/с	3 км	1	Объединение сетей, услуги E1
VDSL	Асимметричный 62 Мбит/с / 26 Мбит/с	1,3 км на max. скорости	1	Объединение сетей, HDTV
SHDSL	Симметричный 2,32 Мбит/с	до 7,5 км	1	Объединение сетей
UADSL	Асимметричный 1,5 Мбит/с / 384 кбит/с	3,5 км на max. скорости	1	Доступ в Интернет, голос, видео
RADSL	Асимметричный 8 Мбит/с / 640 кбит/с	3-5 км в зависимости от диаметра провода	--	--

Технология DSL	Тип передачи Максимальная скорость (прием/передача)	Max расстояние	Кол-во телефонных пар	Основное применение
MDSL	Диапазон может быть в любой пропорции разделен между нисходящим и восходящим трафиком 768 кбит/с	3-5 км в зависимости от диаметра провода	--	--
Ether Loop	Симметричный до 1,5 Мбит/с	--	--	--

Таблица 9.4 – Подробные технические характеристики популярных технологий DSL в зависимости от дальности расположения абонентов

		ADSL	ADSL2	ADSL2+	SHDSL[1]	VDSL2
Симметрия по скорости передачи		Нет	Нет	Нет	Да	Да/нет
Макс. скорость передачи [5, 7]	Нисходящий поток	8 Мбит/с	11 Мбит/с 10 Мбит/с	25 Мбит/с 23 Мбит/с	5,7 Мбит/с	100 Мбит/с
	Восходящий поток	1 Мбит/с	1 Мбит/с 3 Мбит/с	1 Мбит/с 3 Мбит/с	5,7 Мбит/с	100 Мбит/с
	На дистанции	1,5 км	1,5 км	1,0 км	3,0 км	0,3 км
Макс. Дистанция [5,6]		5-6 км	7-8 км [7]	5-6 км	> 10 км	< 3 км [5]
Скорость передачи для дистанции 1 км [5,7]	Нисходящий поток	8 Мбит/с	7 Мбит/с	14 Мбит/с	4 Мбит/с	25 Мбит/с
	Восходящий поток	1 Мбит/с	2 Мбит/с	2 Мбит/с	4 Мбит/с	5 Мбит/с
Скорость передачи для дистанции 3 км [5,7]	Нисходящий поток	1,6 Мбит/с	1,4 Мбит/с	1,7 Мбит/с	1 Мбит/с	1,7 Мбит/с
	Восходящий поток	0,5 Мбит/с	0,7 Мбит/с	0,5 Мбит/с	1 Мбит/с	1 Мбит/с
Скорость передачи для дистанции 8 км [5,7]	Нисходящий поток	-	-	-	1 Мбит/с	-
	Восходящий поток	-	-	-	1 Мбит/с	-
Регенератор		Нет	Нет	Нет	Да	нет
Объединение PHY		1	1	1	1/2/3/4	1
Голосовой интерфейс		POTS/ ISDN	POTS/ ISDN	POTS/ ISDN	Внутриполосный (inband)	POTS/ ISDN
Стандарты		ITU G992.1, T1.413, ET-SI TS 101388	ITU G992.3, G.bis	ITU G992.5	ITU G991.2, T1.413, ETSI TS 101524	ITU G993.2

Примечания: [1]Поддерживает SHDSL.bis; [2]макс. восходящий поток; [3]PSD макс. дистанции; [4]Более этой дистанции инициализация критична; [5]канал без шума; [6]шум: 12 selfNEXT disturber для VDSL, FSAN B – для других; [7]все результаты основаны на симуляции для PE04 медных проводов.

Таблица 9.5 – Типовое применение популярных стандартов DSL

Приложение	ISDL Цифровая абонентская линия ISDN (дуплекс 128 Кбит/с)	SDSL/HDSL (дуплекс до 2 Мбит/с)	ADSL (до 8 Мбит/с от сети и до 800 Кбит/с к сети)	VDSL
Доступ к удаленной LAN	+	+	+	
Доступ к интернет	+	+	+	
Размещение информации на узле Web		+		
Видеоконференция		+		
Видео по требованию			+	+
Пакеты программ офиса бизнеса	+	+		
Пакеты программ малого офиса (много пользователей)		+	+	
Пакеты программ домашнего офиса (один пользователь)	+	+	+	
Сеть с полным набором услуг				+

9.5.2. Технологии симметричного DSL-доступа

Технологии симметричного DSL-доступа используются при предоставлении услуг объединения LAN, организации выносов, подключении оборудования пользователя к транспортным сетям по симметричным медным линиям. К этой группе относятся технологии: HDSL, SDSL, MDSL, MSDSL, SHDSL, HDSL2/4 и VDSL [1, 28].

Симметричные технологии xDSL различают по числу пар используемых проводов. При этом часть «родословное дерево» xDSL для симметричных технологий представлена на рис. 9.13 [1, 28, 29].

Сначала появился вариант HDSL для двух пар, нормированный в ANSI, который использует кодирование 2B1Q. Затем прошла стандартизация HDSL для трех, двух и одной пар в ETSI с использованием 2B1Q или CAP. Часто употребляются обозначения HDSL2 и SDSL2, причем технология HDSL2 рассчитана исключительно на передачу T1, а SDSL2 поддерживает скорости от 384 кбит/с до 2,304 Мбит/с (с шагом 64 кбит/с).

Зачастую полная скорость (544 или 2,304 Мбит/с) не требуется или необходимая дальность при этих скоростях не достигается. Поэтому появились новые системы, заполняющие «зазоры в скоростях»: сначала это были системы MDSL, работающие со скоростью от 160 до 784 кбит/с, позднее – системы MSDSL, обеспечивающие скорость передачи 160-320 кбит/с. MDSL представляет собой множество подсистем MSDSL, которые не были нормированы, а используемая технология соответствует HDSL.

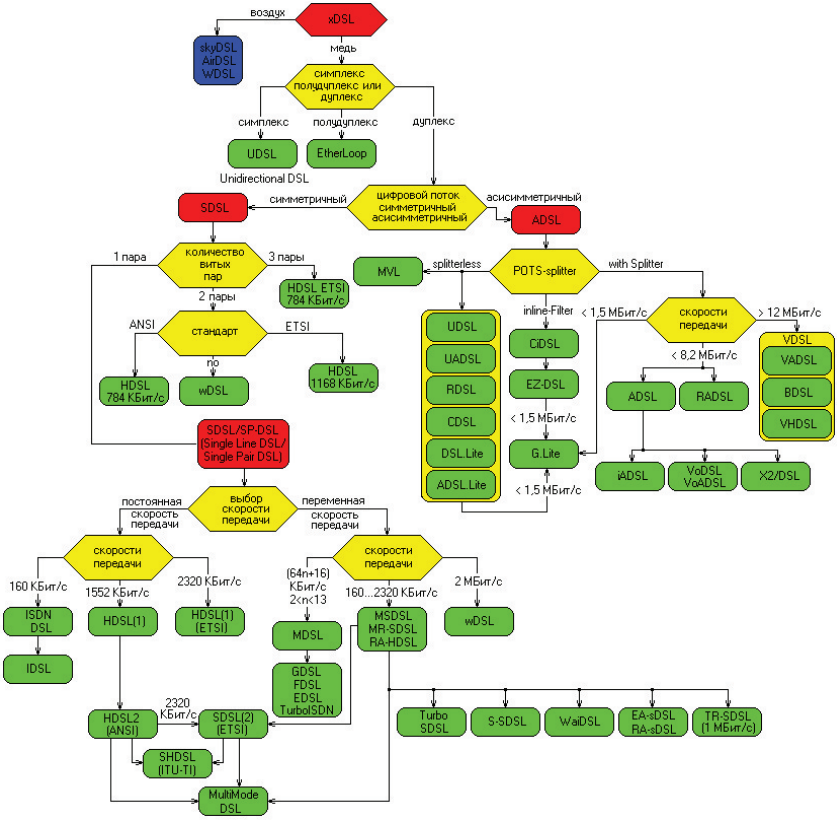


Рис. 9.13. «Родословное дерево» xDSL с разделением по средствам и направлению передачи [1, 28, 29]

Технологии SDSL2 предназначались в основном для делового сектора. Но возможности комбинированной передачи речи и данных, повышенная потребность частного сектора в скорости передачи и хороших технических характеристиках (таких, как спектральная совместимость, аварийное питание и т. д.) могут в будущем привести к тому, что SDSL2 заменят ISDN в частном секторе и тем самым создадут серьезную конкуренцию асимметричным службам xDSL.

Системы SHDSL способны работать по одной или по двум витым парам со скоростью передачи соответственно от 192 до 2312 кбит/с с шагом 8 кбит/с и от 384 до 4624 кбит/с с шагом 16 кбит/с (рис. 9.14, 9.15).

В линии может быть установлено до 8 регенераторов (рек. G.991.2 ITU-T). Длина линии при максимальной скорости достигает 20-30 км в зависимости от диаметра провода. Технология HDSL2/4 является аналогом SHDSL для потока T1 и стандартизирована в ANSI T1.TRQ.06-2001.

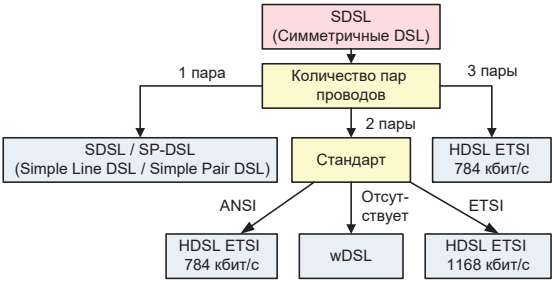


Рис. 9.14. Классификация симметричных xDSL-технологий по числу пар используемых проводов [1]

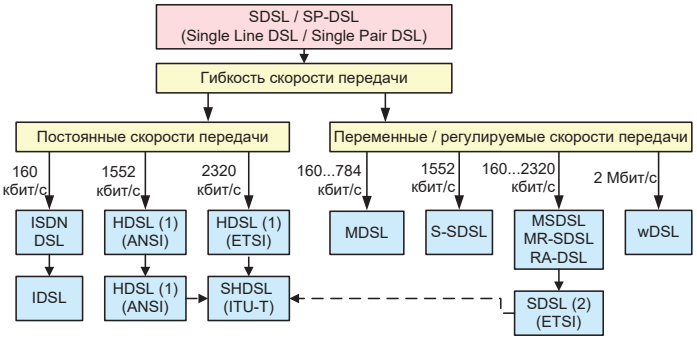


Рис. 9.15. Симметричные технологии xDSL для одной пары [1]

9.5.3. Технологии асимметричного DSL-доступа

Если первоначально развитие симметричных технологий xDSL в основном было ориентировано на потребности делового сектора, то асимметричные технологии xDSL (ADSL) предназначались для частного сектора. Такой подход определяет существенную разницу в требованиях к ним. В частном секторе было необходимо, чтобы уже существующая телефонная служба (ТфОП или BRI-ISDN) продолжала работать и при переходе на ADSL.

Классификация асимметричных xDSL-технологий приведена на рис. 9.16.

ADSL (так называемая Full-rate ADSL) первоначально требовала наличия разветвителя. Технология обеспечивала максимальную скорость передачи в прямом направлении – 6,144 Мбит/с, а в обратном – 0,640 Мбит/с. Разделение осуществляется с помощью эхокомпенсации или методом частотного разделения. Разветвители необходимы как со стороны АТС, так и со стороны абонентов. В ADSL после долгой конкуренции CAP

(амплитудно-фазовая модуляция) и DMTV (дискретная мультитоновая технология) последний вид модуляции получил наибольшее распространение.

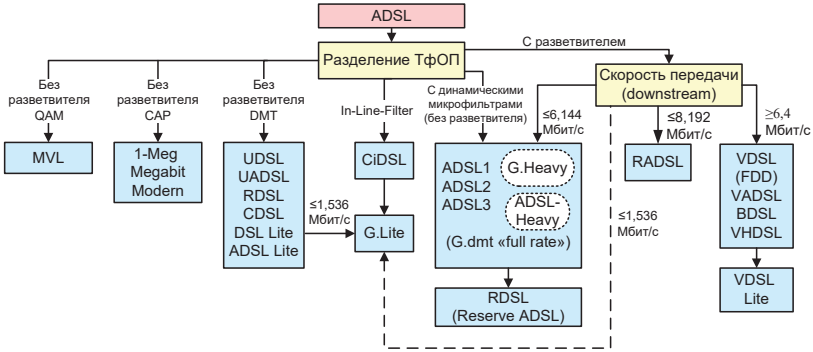


Рис. 9.16. Классификация асимметричных xDSL-технологий [1]

Первые линии ADSL предполагали работу только на постоянных скоростях. Между тем современные решения ADSL могут регулировать скорость передачи в зависимости от качества линии. Из-за адаптивности скорости передачи эту технологию иногда называют RADSL (Rate Adaptive DSL). Она базируется на CAP и включена ANSI в спецификацию TR-59. Различают ADSL over POTS и ADSL over ISDN. В зависимости от вида применения используются различные диапазоны частот.

Первые версии ADSL имели следующие отношения скоростей передачи в прямом и обратном направлениях [1]:

- ADSL1: 1,5 Мбит/с-16 кбит/с;
- ADSL2: 3 Мбит/с-16 кбит/с;
- ADSL3: 6 Мбит/с-64 кбит/с.

Очень высокие скорости передачи в прямом и обратном направлениях достигаются с помощью VDSL. Ранее для VDSL использовались также обозначения VADSL, BDSL (Broadband DSL) или VHDSL (Very High bitrate DSL). Стандартизация VDSL пока не закончена и не решено, какая из технологий будет выбрана: упомянутая выше технология, основанная на TDD, или технология на основе FDD. В настоящее время нормирование этих технологий не может быть полностью завершено, так как ни у одной из них нет особых преимуществ по сравнению с другой.

Внедрение ADSL на практике показало, что установка разветвителей связана с большими затратами, поэтому были начаты поиски технологий ADSL без разветвителя. Целым рядом фирм были предложены различные варианты, исходя из уменьшения скорости передачи в обоих направлениях по сравнению с ADSL (например, MVL – Multiple virtual Line DSL, CDSL – Consumer DSL, CiDSL – Consumer installable DSL). Удалось реализовать

без разветвителя и «full rate ADSL». Технологии ADSL, не требующие разветвителя, были нормированы в МСЭ (G.992.1) и получили название G.Lite (а также ADSL.Lite или DSL.Lite). VDSL.Lite – технология, которая должна занять нишу между ADSL и VDSL.

Одним из самых популярных в последнее время является термин – VoDSL (Voice over DSL), что буквально означает передачу речевых сигналов по цифровым линиям сети абонентского доступа. В целом данное обозначение подходит почти ко всем высокоскоростным технологиям xDSL. Отдельно выделяют VoSDSL и VoADSL, особенностью которых является сочетание сжатия речевых сигналов и ATM.

Положительный опыт производства и использования DSL-оборудования в сетях абонентского доступа привел к появлению аналогичных систем для цифровизации существующих магистральных медно-кабельных линий, которые пока еще слишком дорого заменять на волокно. Поэтому хотя технологии xDSL и рассматриваются как временная замена оптоволоконных абонентских линий, они еще долго будут востребованы в сетях абонентского доступа, включая сети специального назначения.

9.6. Технологии доступа на волоконно-оптических и смешанных медно-оптических линиях

В настоящее время для предоставления пользователям широкополосных услуг используются обычно смешанные медно-оптические сети доступа. В настоящее время существует несколько основных концепций разворачивания сети доступа смешанного типа с использованием волоконно-оптических линий связи [5]:

- *технология HFC* (*Hybrid Fiber Coaxial*) предполагает доведение оптики до точки концентрации, при этом распределительная абонентская сеть строится на основе коаксиальных кабелей. Данная архитектура не получила широкого распространения в России и используется обычно лишь отдельными операторами КТВ;
- *концепция FTTx* и ее различные варианты;
- *технология пассивных оптических сетей* (*PON*).

Варианты доступа FTTH и FTTB не так широко распространены, как системы DSL доступа. Связано это в основном с тем, что их реализация требует от оператора значительно больших инвестиций, чем построение DSL-инфраструктуры, поскольку для предоставления абоненту высокоскоростного канала (до нескольких Гбит/с) необходимо во много раз увеличить пропускную способность опорных сетей, протянуть оптоволокно до абонента, разработать немало новых приложений и, самое главное, убедить абонента заплатить за это деньги. Поэтому многие операторы до сих пор стараются использовать имеющуюся медно-кабельную инфраструктуру.

Таким образом, вложения в инфраструктуру ВОЛС являются эффективными и долговременными, а внедрение технологий FTTx становится

оправданным и весьма перспективным направлением, в том числе и в России. Актуальность применения технологий FTTx и PON их технические параметры и особенности реализации рассматриваются более подробно в работе [5].

9.6.1. Технологии группы FTTx – доступ на основе смешанных медно-оптических линий связи

Группа технологий FTTx (Fiber to the x – оптическое волокно до…) предназначена для совместного использования оптического волокна с технологиями ADSL и VDSL, что позволяет более эффективно использовать пропускную способность этих технологий благодаря сокращению длины медно-кабельных линий связи.

Есть несколько вариантов реализации FTTx, из них можно выделить основные:

- FTTH – Fiber To The Home (доведение волокна до квартиры);
- FTTB – Fiber To The Building (доведение волокна до здания).

Варианты, по сути, дублирующие FTTH и FTTB с небольшими изменениями:

- FTTN (Fiber to the Node) – волокно до сетевого узла;
- FTTO – Fiber To The Office (доведение волокна до офиса);
- FTTC – Fiber To The Curb (доведение волокна до кабельного шкафа);
- FTTCab – Fiber To The Cabinet (аналог FTTC);
- FTTR – Fiber To The Remote (доведение волокна до удаленного модуля, концентратора);
- FTTOpt – Fiber To The Optimum (доведение волокна до оптимального пункта);
- FTTP – Fiber To The Premises (доведение волокна до точки присутствия клиента).

Отдельно нужно отметить концепцию FITB (Fiber In The Building) – организация распределительной сети внутри здания.

Выше указанные технологии отличаются главным образом тем, на сколько близко к пользовательскому терминалу подходит оптический кабель (рис. 9.17).

На данный момент интенсивно растет интерес к развертыванию оптических сетей доступа с прокладкой кабеля до здания (FTTB), а также непосредственно до абонента (FTTH). В большей степени, такая ситуация объясняется постоянным ростом требований к пропускной способности каналов связи, поскольку сейчас наблюдается бум развития «тяжелых» интернет-приложений, включая онлайн-видео, онлайн-игры и прочие сервисы.

При этом запланированный набор услуг и необходимая для его предоставления полоса пропускания имеют самое непосредственное влияние на выбор технологии FTTx. Поэтому чем выше скорость доступа и чем

больше набор предоставляемых абоненту услуг, тем ближе к абонентскому терминалу должно подходить оптическое волокно, т. е. нужно использовать технологии FTTH. В случае, когда приоритетом является сохранение уже имеющейся сетевой инфраструктуры и оборудования, оптимальным выбором будет FTTB.

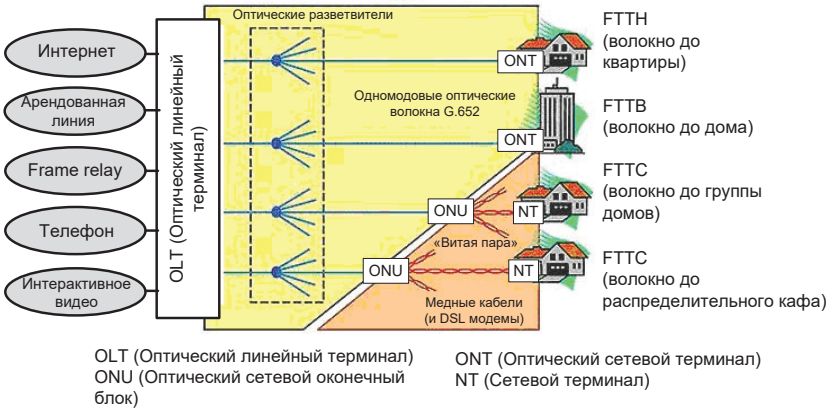


Рис. 9.17. Технологии оптического доступа FTTx

Если же говорить о сегодняшних реалиях, архитектура FTTB преобладает в новостройках и у крупных операторов связи, тогда как FTTH востребована в новом малоэтажном строительстве (например, в коттеджных городках в окрестностях крупных городов).

Рассмотрим особенности реализации и применении наиболее распространенных технологий.

9.6.1.1. Технология FTTB

Технология FTTB предполагает доведение волокна до здания, и получила наибольшее распространение, так как при строительстве сетей FTTx на базе Ethernet – это, зачастую, единственная технически возможная схема построения сети. Кроме того, в структуре затрат на создание Ethernet-сети разница между вариантами FTTC и FTTB относительно небольшая. Также не следует забывать, что операционные расходы при эксплуатации сети FTTB ниже, а пропускная способность выше.

Технологию FTTB целесообразно применять в случае развертывания сети в многоквартирных домах и бизнес-центрах. Российские операторы связи разворачивают сети FTTB пока только в крупных городах, но в перспективе планируется использование данной технологии повсеместно. В FTTB нет необходимости прокладывать дорогостоящий оптический кабель с большим количеством волокон, как при использовании FTTH [5].

В случае FTTB оптическое волокно заводится в дом, как правило, на цокольный этаж или на чердак и подключается к устройству ONU (Optical Network Unit). На стороне оператора связи устанавливается терминал оптической линии OLT (Optical Line Terminal). OLT является primary устройством и определяет параметры обмена трафика (например, интервалы времени приема/передачи сигнала) с абонентскими устройствами ONU (или ONT, в случае FTTH). Дальнейшее распределение сети по дому происходит по «витой паре» (рис. 9.18).

9.6.1.2. Технология FTTH

Технология FTTH является наиболее затратной, но в то же время и наиболее перспективной, среди всех типов доступа FTTx. FTTH подразумевает доведение оптического волокна до квартиры или частного дома пользователя. В этом случае оптическое волокно заводится в дом, как правило, на цокольный этаж или на чердак (что более экономически целесообразно) и подключается к устройству ONU (Optical Network Unit). На стороне оператора связи устанавливается терминал оптической линии OLT (Optical Line Terminal). OLT является primary устройством и определяет параметры обмена трафика (например, интервалы времени приема/передачи сигнала) с абонентскими устройствами ONU (или ONT, в случае FTTH). Дальнейшее распределение сети по дому происходит по «витой паре» (рис. 9.19).

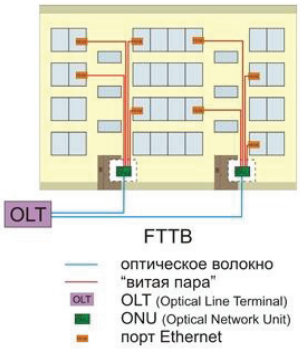


Рис. 9.18. Технология FTTB

Рис. 9.19. Технология FTTH

На первый взгляд, строительство сети FTTH – это очень трудоемкий и дорогостоящий процесс, но опыт подсказывает, что основные затраты при развертывании сети FTTH приходятся на строительные работы, а стоимость самого оптоволоконного кабеля составляет относительно небольшую часть. Это означает, что в случае необходимости проведения строительных работ количество прокладываемого оптоволоконного кабеля уже не имеет большого значения.

Более того, хотя жизненный цикл сети FTTH и ее электронных компонентов составляет несколько лет, оптоволоконный кабель и оптическая распределительная сеть имеют более длительный срок службы (по крайней мере, 30 лет).

Архитектуры развернутых сетей FTTH можно разделить на три основные категории:

1) «кольцо» Ethernet-коммутаторов;
2) «звезда» Ethernet-коммутаторов;
3) «дерево» с использованием технологий пассивной оптической сети PON.

9.6.1.3. Технология Ethernet FTTH

В решении Ethernet FTTH для коммутации линий подразумевается использование коммутаторов с оптическими портами или оптическими трансиверами.

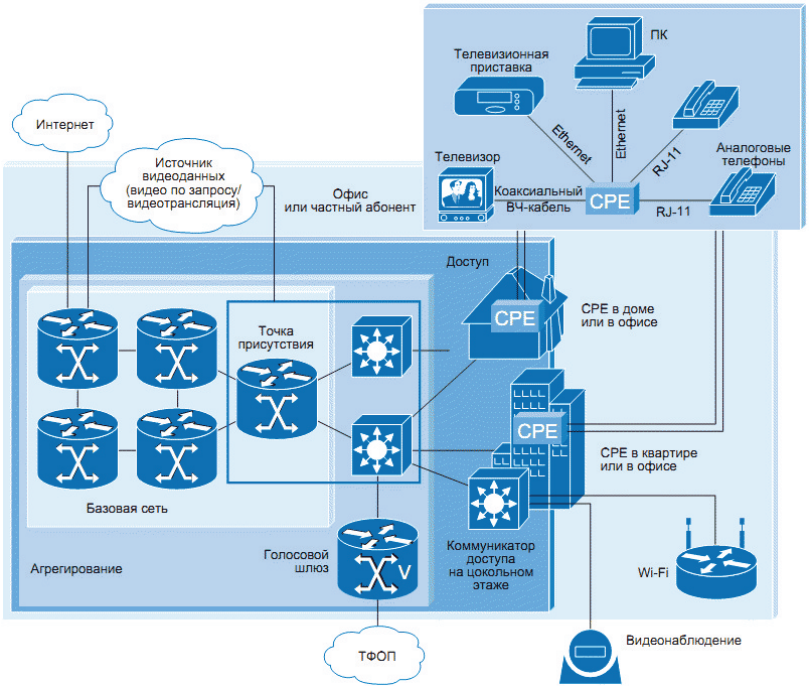


Рис. 9.20. Архитектура сети Ethernet FTTH типа «звезда»

В основе европейских проектов сетей Ethernet FTTH лежала архитектура Ethernet типа «звезда» (рис. 9.20). Такая архитектура предполагает наличие выделенных оптоволоконных линий (обычно одномодовых, одноволоконных линий с передачей данных Ethernet по технологии 100BX или 1000BX) от каждого оконечного устройства к точке присутствия (point of

presence, POP), где происходит их подключение к коммутатору. К портам коммутатора подключаются устройства конечных пользователей. Такой подход обеспечивает высокий уровень надежности за счет возможности резервирования оптических каналов, и обеспечивает преемственность с существующей «медной» инфраструктурой.

Основные преимущества решений Ethernet FTTH перед архитектурой на базе PON:

- широкая дискретная полоса пропускания, обусловленная использованием ВОЛС;
- радиус действия до 10 км;
- гибкое масштабирование размера сети и скорости обслуживания абонентов.

К недостаткам Ethernet FTTH можно отнести узкую полосу пропускания.

9.6.2. Технология пассивной оптической сети PON

Технологии пассивных оптических сетей (*PON*) – это семейство быстроразвивающихся, наиболее перспективных технологий широкополосного мультисервисного множественного доступа по оптическому волокну. Суть технологии пассивных оптических сетей, вытекающая из ее названия, состоит в том, что ее распределительная сеть строится без каких-либо активных компонентов: разветвление оптического сигнала осуществляется с помощью пассивных делителей оптической мощности – сплиттеров.

Следствием этого преимущества является снижение стоимости системы доступа, уменьшение объема необходимого сетевого управления, высокая дальность передачи и отсутствие необходимости в последующей модернизации распределительной сети.

Суть технологии PON заключается в том, что между приемопередающим модулем центрального узла OLT (optical line terminal) и удаленными абонентскими узлами ONT (optical network terminal) создается полностью пассивная оптическая сеть, имеющая топологию дерева (рис. 9.21).

В промежуточных узлах дерева размещаются пассивные оптические разветвители (сплиттеры) с коэффициентом разветвления до 1:64 или даже 1:128. – компактные устройства, не требующие питания и обслуживания. Один приемопередающий модуль OLT позволяет передавать информацию множеству абонентских устройств ONT.

Число ONT, подключенных к одному OLT, может быть настолько большим, насколько позволяет бюджет мощности и максимальная скорость приемопередающей аппаратуры.

Для передачи прямого и обратного канала используется одно оптическое волокно, полоса пропускания которого динамически распределяется между абонентами, или два волокна в случае резервирования. Нисходящий поток (downstream) от центрального узла к абонентам идет на длине волны 1490 нм и 1550 нм для видео. Восходящие потоки (upstream) от абонентов

идут на длине волны 1310 нм с использованием протокола множественного доступа с временным разделением (TDMA). В некоторых случаях используется дополнительная длина волны нисходящего потока (downstream), что позволяет предоставлять традиционные аналоговые и цифровые телевизионные услуги пользователям без применения телевизионных приставок с поддержкой IP.

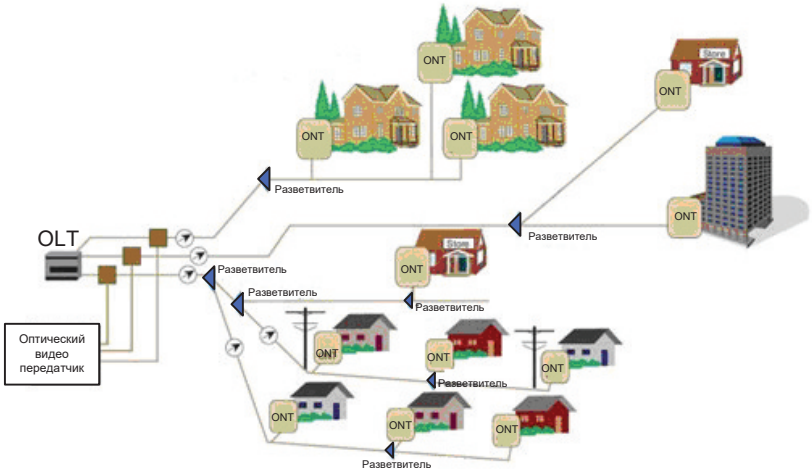


Рис. 9.21. Архитектура PON сети

Для построения PON используется топология «точка – многоточка» и сама сеть имеет древовидную структуру. Каждый волоконно-оптический сегмент подключается к одному приемопередатчику в центральном узле (в отличие от топологии «точка-точка»), что также дает значительную экономию в стоимости оборудования. Один волоконно-оптический сегмент сети PON охватывает до 32 абонентских узлов в радиусе до 20 км для технологий EPON / BPON и до 128 абонентских узлов в радиусе до 60 км для технологии GPON (рис. 9.21).

Каждый абонентский узел рассчитан на обычный жилой дом или офисное здание и в свою очередь может охватывать сотни абонентов. Все абонентские узлы являются терминальными, и отключение или выход из строя одного или нескольких абонентских узлов никак не влияет на работу остальных.

Архитектура FTTH на базе PON обычно поддерживает протокол Ethernet. Центральный узел PON может иметь сетевые интерфейсы ATM, SDH (STM-1), Gigabit Ethernet для подключения к магистральным сетям. Абонентский узел может предоставлять сервисные интерфейсы 10/100Base-TX, FXS (2, 4, 8 и 16 портов для подключения аналоговых телефонных абонентов), E1, цифровое видео, ATM (E3, DS3, STM-1) – рис. 9.21.

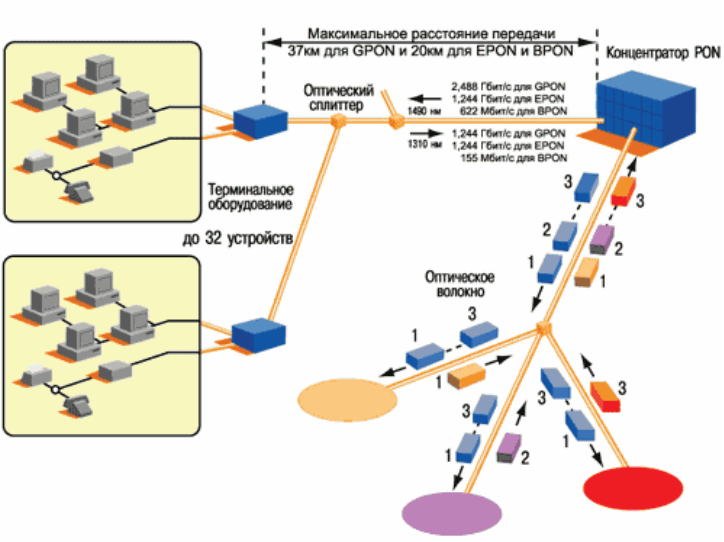


Рис. 9.21. Принцип временного разделения абонентов в технологии PON

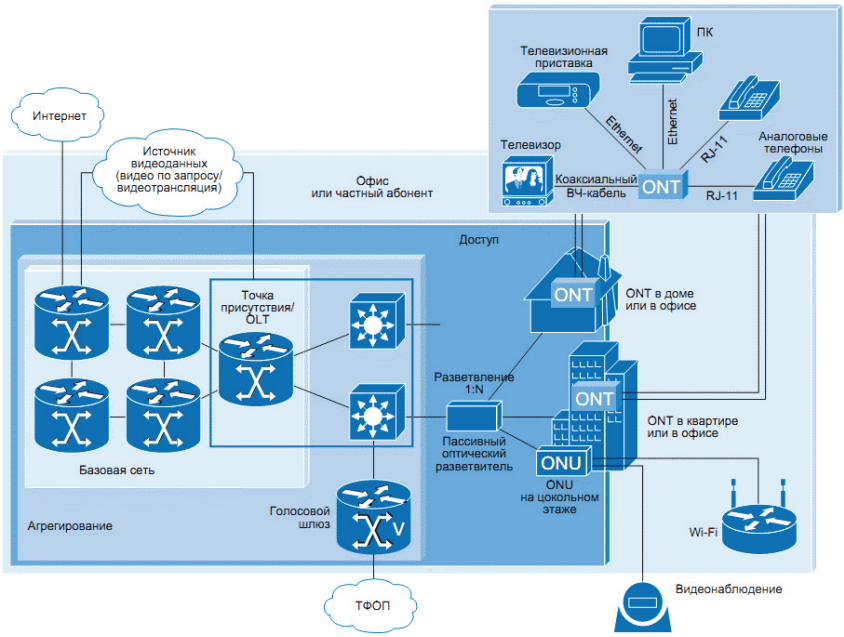


Рис. 9.22. Структура типичной пассивной оптической сети PON

На рис. 9.22 изображена типичная пассивная оптическая сеть PON, в которой используются различные терминаторы оптической сети (optical network termination, ONT) или устройства оптической сети (optical network unit, ONU). ONT предназначены для использования отдельным конечным пользователем. Устройства ONU обычно располагаются на цокольных этажах или в подвальных помещениях и совместно используются группой пользователей. Голосовые сервисы, а также услуги передачи данных и видео доводятся от ONU или ONT до абонента по кабелям, проложенным в помещении абонента.

В семействе сетей PON существует несколько разновидностей, отличающихся, в первую очередь, базовым протоколом передачи. Причем стандарты PON активно совершенствуются в направлении увеличения скорости передачи и дальности связи. Отдельные разновидности PON (таблица 9.6) имеют свои преимущества и недостатки, но в целом технология GPON является более удачной для сетей большой протяженности и емкости. При этом все российские операторы, использующие пассивные оптические сети доступа PON, остановили свой выбор на варианте GPON и ее более упрощенном варианте GEPON.

Таблица 9.6 – Сравнительная таблица по характеристикам стандартов PON

Характеристики	APON (BPON)	EPON (GEPON)	GPON
Институты стандартизации / альянсы	ITU-T SG15 / FSAN	IEEE / EFMA	ITU-T SG15 / FSAN
Дата принятия стандарта	октябрь 1998	июль 2004	октябрь 2003
Стандарт	ITU-T G.981.x	IEEE 802.3ah	ITU-T G.984.x
Скорость передачи, прямой/обратный поток, Мбит/с	155/155 622/155 622/622	1000/1000	1244/155, 622, 1244 2488/622, 1244, 2488
Базовый протокол	ATM	Ethernet	SDH (GFP)
Линейный код	NRZ	8B/10B	NRZ
Максимальный радиус сети, км	20	20 (>30[1])	20
Максимальное число абонентских узлов на одно волокно	32	16	64 (128[2])
Приложения	любые	IP, данные	любые
Коррекция ошибок FEC	предусмотрена	нет	необходима
Длины волн прямого/обратного потоков, нм	1550/1310 (1480/1310)	1550/1310 (1310/13103)	1550/1310 (1480/1310)
Динамическое распределение полосы	есть	поддержка[4]	есть
IP-фрагментация	есть	нет	есть
Защита данных	шифрование открытыми ключами	нет	шифрование открытыми ключами

Характеристики	APON (BPON)	EPON (GEPON)	GPON
Резервирование	есть	нет	есть
Оценка поддержки голосовых приложений и QoS	высокая	низкая	высокая
Динамический диапазон, дБ:			
– класс А	5-20		5-20
– класс В	10-25		10-25
– класс С	15-30		15-30
Интерфейс PX-10 (10 км)		5-20	
Интерфейс PX-20 (20 км)		10-24	

Примечания:
[1] обсуждается в проекте;
[2] стандарт допускает наращивание сети до 128 ONT;
[3] допускается передача в прямом и обратном направлении на одной и той же длине волны;
[4] осуществляется на более высоких уровнях.

Технология GPON обеспечивает скорости передачи – 1244 Мбит/с, 2488 Мбит/с (в асимметричном режиме) и 1244 Мбит/с (в симметричном режиме) считается наиболее удачной для больших операторов, строящих большие разветвленные сети с системами резервирования. За основу GPON был принят базовый транспортный протокол SDH (а точнее SDH на протоколе GFP). В GPON возможно подключение до 32 (или 64) абонентов на расстоянии до 20 км (с возможностью расширения до 60 км). GPON поддерживает трафик ATM, IP, речь и видео (инкапсулированные в кадры GEM – GPON Encapsulated Method), а также модули SDH. Сеть работает в синхронном режиме с постоянной длительностью кадра. Линейный код NRZ со скремблированием обеспечивают высокую эффективность полосы пропускания. Единственным серьезным недостатком GPON является высокая стоимость оборудования.

Технология GEPON, является упрощенным вариантом GPON, в котором, в отличие от GPON, отсутствуют специфические функции поддержки TDM, синхронизации и защитных переключений, что делает эту технологию самой экономичной из всего семейства PON. Особенно это касается небольших операторов, ориентированных на IP-трафик, а впоследствии и IPTV. К тому же предполагается дальнейшее развитее этого ряда – 10GEPON (по аналогии с 10 Gb Ethernet). Поэтому из-за наилучшего соотношения цена/качество при среднем размере сети, в нашей стране вариант GEPON получил наибольшее распространение.

Технология WDM PON является следующим шагом по увеличению скорости передачи построенных систем PON за счет применения систем спектрального уплотнения WDM. В рекомендации ITU-T G.983.2 описана возможность передачи сигналов на выделенных для каждого абонента длинах волн. В сети передается общий поток, а каждый абонентский терминал имеет оптический фильтр для выделения своей длины волны. Тех-

нически возможно обеспечить производительность системы со скоростями около 4-10 Гбит/с по каждому каналу. После такой реконструкции провайдеры получат возможность настраивать пропускную способность в соответствии с требованиями клиента и успешно добавлять или удалять устройства ONU без вмешательства в общую систему, т. е. в будущем внедрение систем WDM PON принесет реальные преимущества операторам при незначительных затратах.

9.7. Анализ распространенности технологий широкополосного доступа к сети Интернет в России

В соответствии с докладом [47] по состоянию на 2020 г. наиболее используемыми технологиями при организации фиксированного ШПД к Интернету в России являются:

- технологии FTTx (в частности – технологии FTTH/FTTB, где ВОЛС строятся на основе технологии PON) – в России с их использованием к Интернету подключены 77,6% абонентов;
- технологии xDSL (преимущественно по технологии ADSL2+) – подключены 15,1% российских абонентов;
- другие проводные технологии – 5,9% российских абонентов.

В России почти 20% аудитории охвачены ШПД в Интернет на скоростях от 2 до 10 Мбит/с, и только 73,4% абонентов имеют доступ со скоростью более 10 Мбит/с.

Охват населения мобильным ШПД в интернет по технологиям LTE и WiMAX в России составляет 62%, по технологии 3G – 77%. При этом 7% населения охвачено мобильным ШПД со скоростью от 256 Кбит/с до 2 Мбит/с; 19% населения – от 2 до 10 Мбит/с; 73% населения – от 10 Мбит/с и выше.

В России доля пользователей ШПД в Интернет со скоростью от 30 до 100 Мбит/с вдвое превосходит долю организаций, подключенных к сети с максимальной скоростью доступа выше 100 Мбит/с. В 2018 г. эти показатели составили соответственно 20,5 и 10,4%. Причем за 2015–2018 гг. спрос на высокоскоростной ШПД в интернет вырос лишь немногим более чем на 1% (в 2015 г. 9,1% организаций предпринимательского сектора использовали Интернет с максимальной скоростью доступа выше 100 Мбит/с).

Материал раздела 9 подготовлен на основе работ [1, 5] и за счет обобщения материалов [24-47]. Более подробные сведения о технологиях САД представлены в работе [5].

ЧАСТЬ II. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

10. Типовые информационно-технические воздействия на телекоммуникационные сети

Телекоммуникационные сети (ТКС) постоянно подвергаются информационно-техническим воздействия (ИТВ) со стороны профессиональных и непрофессиональных злоумышленников.

Атакующие ИТВ ориентированы на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня ИБ или эффективности функционирования. Применение атакующих ИТВ против ТКС направлено на срыв выполнения системой своих целевых задач – передачи информации с заданным качеством.

Далее обзорно представлена классификация и основные типы атакующих ИТВ. Более подробная информация об атакующих ИТВ представлена в работах [48-53].

10.1. Классификация атакующих информационно-технических воздействий со стороны злоумышленников

Классификация средств и способов атакующих ИТВ представлена на рис. 10.1.

Атакующие ИТВ, в зависимости от их ориентированности на нарушение конкретного свойства ИБ, можно классифицировать на четыре основных типа:

- ориентированные на нарушение конфиденциальности информации;
- ориентированные на нарушение целостности информации;
- ориентированные на нарушение доступности информации;
- ориентированные на информационно-психологическое воздействие (компьютерное психотронное воздействие) на пользователей информационной системы.

По способу реализации ИТВ классифицируются на:

- алгоритмические:
  - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);

- эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
- эксплойты, ориентированные на сетевые протоколы информационной системы;
- эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования;

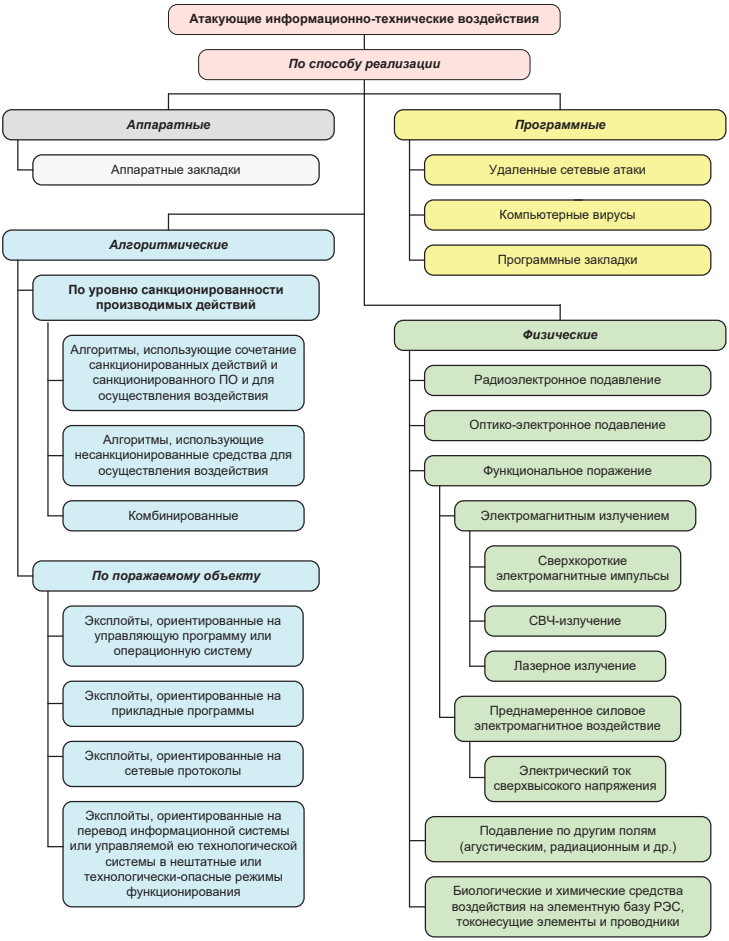


Рис. 10.1 Классификация средств и способов атакующих ИТВ

- программные:
  - компьютерные вирусы;
  - программные закладки;
  - нейтрализаторы тестовых программ и программ анализа кода;
- аппаратные:
  - аппаратные закладки;
- физические:
  - электромагнитные:
    - радиоэлектронное подавление;
    - оптико-электронное подавление;
    - функциональное поражение электромагнитным излучением (электромагнитные импульсы, СВЧ-излучение, лазерное излучение);
    - функциональное поражение преднамеренными силовыми электромагнитными воздействиями (электрический ток сверхвысокого напряжения);
  - по другим полям (акустическим, радиационным и др.);
  - биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники.

Рассмотрим более подробно основные широко распространенные атакующие ИТВ, которые могут быть использованы против элементов ТКС:

- удаленные сетевые атаки;
- компьютерные вирусы;
- программные закладки;
- аппаратные закладки.

10.2. Удаленные сетевые атаки

10.2.1. Определение и классификация удаленных сетевых атак

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленных в работах [51, 52] можно дать следующее определение.

Удаленная сетевая атака – это разрушающее или дестабилизирующее информационно-техническое воздействие, осуществляемое по каналам связи, удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Удаленные сетевые атаки становятся возможными благодаря уязвимостям в существующих протоколах обмена данными и в подсистемах защиты распределенных информационных систем. При этом к основным уязвимостям информационных систем, которые позволяют проводить против них успешные удаленные сетевые атаки, относятся [51, 52]:

– открытость информационной системы, свободный доступ к информации по организации сетевого взаимодействия и способам защиты, применяемым в системе;
– наличие ошибок в операционных системах, в прикладном ПО и в протоколах сетевого обмена;
– разнородность используемых версий ПО и операционных систем;
– сложность организации защиты межсетевого взаимодействия;
– ошибки конфигурирования систем и средств защиты;
– неправильное или ошибочное администрирование систем;
– несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации эксплойтов и ошибок в ПО;
– «экономия» на средствах и системах обеспечения безопасности или игнорирование их.

Удаленные сетевые атаки можно классифицировать в соответствии с различными основаниями. Общая схема классификации удаленных сетевых атак представлена на рис. 10.2.

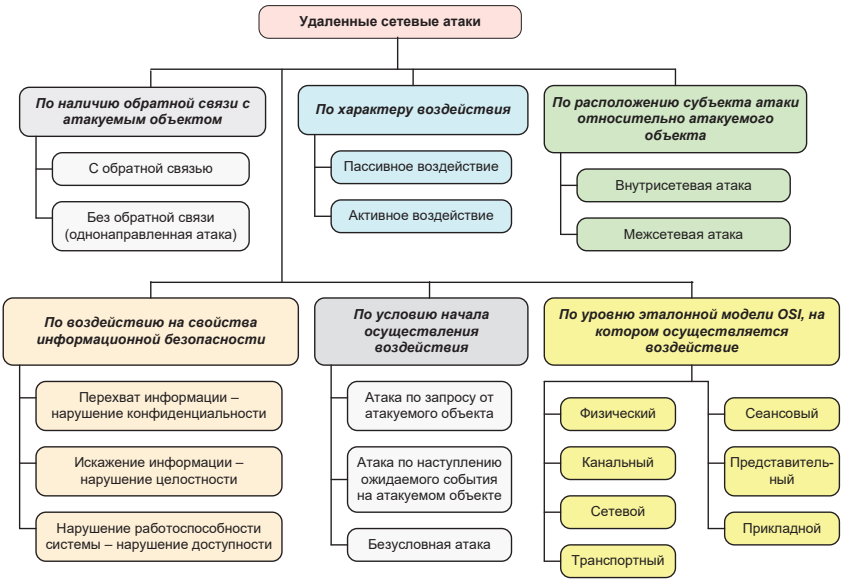


Рис. 10.2. Классификация удаленных сетевых атак

1. По характеру воздействия [51, 52]:
– пассивное воздействие;
– активное воздействие.

Пассивное воздействие не оказывает непосредственного влияния на работу информационной системы, но может нарушать ее политику безопасности. Отсутствие непосредственного влияния на функционирование

атакуемой системы приводит к тому, что пассивную сетевую атаку практически невозможно обнаружить. Примером типовой пассивной удаленной сетевой атаки является прослушивание канала связи.

Активное воздействие оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все типы удаленных сетевых атак относятся к активным воздействиям. Очевидной особенностью активного воздействия, по сравнению с пассивным, является принципиальная возможность его обнаружения, так как в информационной системе происходят определенные деструктивные изменения.

2. По воздействию на свойства информационной безопасности ресурсов системы [51, 52]:

– перехват информации – нарушение конфиденциальности;
– искажение информации – нарушение целостности;
– нарушение работоспособности системы – нарушение доступности.

Перехват информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. В этом случае осуществляется несанкционированный доступ к информации без возможности ее искажения. Также очевидно, что нарушение конфиденциальности информации является пассивной сетевой атакой. Примером такой атаки, связанной с перехватом информации, может служить прослушивание канала связи в сети.

Искажение информации означает либо полный контроль над информационным потоком между объектами информационной системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, искажение информации ведет к нарушению целостности информационных ресурсов системы. Примером удаленной сетевой атаки, целью которой является нарушение целостности информационных ресурсов, может служить атака, связанная с внедрением ложного сетевого объекта в систему, например, внедрения ложного DNS-сервера.

При нарушении работоспособности системы атакующей стороной не предполагается получение несанкционированного доступа к информации. Ее основная цель – добиться, чтобы элементы распределенной информационной системы на атакуемом объекте вышли из строя, а для всех остальных объектов системы доступ к информационным ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить DoS-атака.

3. По условию начала осуществления воздействия [51, 52]:

– атака по запросу от атакуемого объекта;
– атака по наступлению ожидаемого события на атакуемом объекте;
– безусловная атака.

При атаке по запросу от атакуемого объекта атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов могут служить DNS- и ARP-запросы. Важно отметить, что этот тип удаленных атак наиболее характерен для распределенных сетевых информационных систем.

При атаке по условию наступления ожидаемого события атакующий осуществляет наблюдение за состоянием информационной системы, которая является целью атаки. При возникновении определенного события в этой системе атакующий начинает воздействие на нее. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сама атакуемая система. Такие сетевые атаки довольно распространены. Примером такой атаки может быть атака, связанная с несанкционированным доступом к информационным ресурсам компьютера по сети после факта его успешного заражения backdoor-вирусом, который создает дополнительные уязвимости в подсистеме защиты компьютера.

При безусловной атаке она осуществляется немедленно и безотносительно к состоянию информационной системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. По наличию обратной связи с атакуемым объектом [51, 52]:

– с обратной связью;
– без обратной связи (однонаправленная атака).

Удаленная сетевая атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ. Следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адаптивно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных сетевых информационных систем.

В отличие от атак с обратной связью, удаленным сетевым атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки такого вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную сетевую атаку можно называть однонаправленной удаленной атакой. Примером такой однонаправленной атаки может служить DoS-атака.

5. По расположению субъекта атаки относительно атакуемого объекта [51, 52]:

– внутрисетевая атака;
– межсетевая атака.

В случае внутрисетевой атаки субъект и объект атаки находятся в одной сети. При межсетевой атаке субъект и объект атаки находятся в разных сетях. Важно отметить, что межсетевая удаленная атака представляет

гораздо бóльшую опасность, чем внутрисетевая. Это связано с тем, что в случае межсетевой атаки ее объект и непосредственно атакующий могут находиться на значительном расстоянии друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

6. По уровню эталонной модели OSI, на котором осуществляется воздействие [51, 52]:

- физический;
- канальный;
- сетевой;
- транспортный;
- сеансовый;
- представительный;
- прикладной.

Удаленные атаки могут быть ориентированы на сетевые протоколы, функционирующие на различных уровнях модели OSI. При этом надо отметить, что атаки, ориентированные на физический, канальный, сетевой и транспортный уровни, как правило, направлены против сетевой инфраструктуры – оборудования узлов сети и каналы связи. Атаки, ориентированные на сеансовый, представительный и прикладной уровни, как правило, направлены против оконечных терминалов сети. В связи с этим, в зависимости от уровня OSI, на который ориентирована атака, конкретный вид используемого воздействия может значительно меняться. Это может быть воздействие средств РЭП или ЭМИ при атаке, ориентированной на физический уровень, при этом эффекты от такого воздействия отображаются на более верхних уровнях модели OSI. Либо DoS-атака на узловое оборудование сети, либо вирус, поражающий операционную систему конечного терминального оборудования.

10.2.2. Примеры способов информационно-технических воздействий на основе удаленных сетевых атак

В связи с тем, что удаленные сетевые атаки совместно с воздействием вирусных средств составляют подавляющее большинство всех информационно-технических воздействий, рассмотрим их более подробно.

Общая классификация способов информационно-технического воздействия на основе удаленных сетевых атак представлена на рис. 10.3.

К основным способам информационно-технического воздействия, которые можно отнести к удаленным сетевым атакам, относятся [51, 52]:

- анализ сетевого трафика;
- подмена доверенного объекта или субъекта информационной системы;
- внедрение ложного объекта в информационную систему:
    - внедрение ложного объекта путем навязывания ложного сетевого маршрута;

- внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети;
- путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
- путем формирования потока ложных ответов, не дожидаясь запросов от узлов сети;

– использование ложного сетевого объекта для организации удаленной атаки на информационную систему:
- селекция информации и сохранение ее на ложном сетевом объекте;
- модификация информации, проходящей через ложный сетевой объект;
- подмена информации, проходящей через ложный сетевой объект;

– атаки типа «отказ в обслуживании»:
- отказ в обслуживании (DoS-атака);
- распределенная атака «отказ в обслуживании» (DDoS-атака);
- зацикливание процедуры обработки запроса.

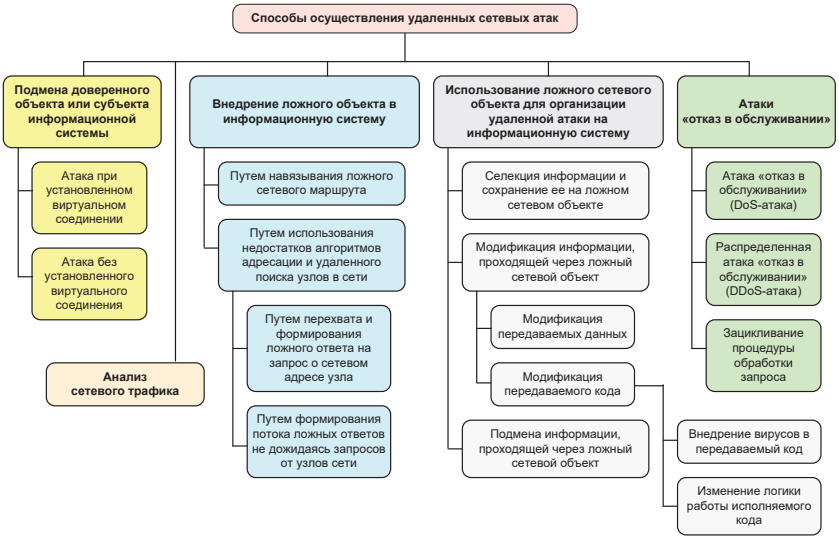


Рис. 10.3. Классификация способов осуществления удаленных сетевых атак

10.2.2.1. Анализ сетевого трафика

Основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве и связь между ними осуществляется по сетевым соединениям. Таким образом, сообщения и данные, пересылаемые между объектами информационной системы, передаются по каналам связи в виде пакетов. Эта особенность привела к появлению специфичного для сетевой информационной системы типового удаленного воздействия, заключающегося в прослушивании канала связи. Такое воздействие называется *анализом сетевого трафика*.

Анализ сетевого трафика позволяет [51, 52]:

- изучить логику работы сетевой информационной системы, то есть получить взаимно однозначное соответствие событий, происходящих в системе, команд и данных, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов сетевого трафика. Знание логики работы информационной системы позволяет смоделировать и осуществлять другие удаленные сетевые атаки;
- перехватить поток данных, которыми обмениваются объекты сетевой информационной системы. Таким образом, эта атака заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером информации, перехваченной при помощи такой типовой удаленной атаки, могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

В соответствии с выше представленной классификацией анализ сетевого трафика является пассивным воздействием. Осуществление такой атаки без обратной связи ведет к нарушению конфиденциальности информации внутри одного сегмента сети на канальном или сетевом уровне OSI. При этом начало атаки является безусловной по отношению к цели атаки [51, 52].

10.2.2.2. Подмена доверенного объекта или субъекта информационной системы

Одной из проблем безопасности сетевой информационной системы является недостаточная идентификация и аутентификация ее объектов, удаленных друг от друга. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами сетевого взаимодействия. Обычно в сетевых информационных системах эта проблема решается следующим образом: в процессе создания виртуального канала объекты системы обмениваются определенной информацией, уникально идентифицирующей этот канал. Однако такой обмен производится не всегда. Зачастую, особенно при передаче слу-

жебной и адресной информации, в сети используются одиночные сообщения, не требующие подтверждения. Так как сетевой адрес достаточно просто подделывается, его можно использовать для виртуальной подмены доверенного объекта или субъекта информационной системы. Таким образом, в том случае, когда в сети используются нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной удаленная атака *подмена доверенного объекта или субъекта информационной системы*, заключающаяся в передаче по сети сообщений от имени произвольного объекта или субъекта информационной системы [51, 52].

Существуют две разновидности этой сетевой атаки, в зависимости от принятой в системе политики информационной безопасности и подхода к защите сетевых соединений [51, 52]:

– атака при установленном виртуальном соединении;
– атака без установленного виртуального соединения.

В случае если в сети для сеанса обмена данными устанавливаются виртуальные соединения, атака будет заключаться в присвоении прав доверенного субъекта сетевого взаимодействия, легально подключившегося к объекту системы. Это позволит атакующему вести сеанс работы с объектом информационной системы от имени доверенного субъекта. Реализация таких удаленных атак обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Однако для осуществления атаки этого типа необходимо преодолеть систему идентификации и аутентификации сетевых сообщений [51, 52].

Атаки на информационную систему, в которой не используются виртуальные соединения, заключаются в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов. В этом случае возможна подделка сетевого адреса отправителя. Например, так реализуется удаленная атака, использующая навязывание ложного маршрута путем посылки ложных адресных сообщений [51, 52].

Подмена доверенного объекта или субъекта информационной системы может быть классифицирована как активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации по наступлению на атакуемом объекте определенного события. Такая удаленная атака может являться как внутрисетевой, так и межсетевой, как с обратной связью, так и без обратной связи с атакуемым объектом и осуществляться на сетевом или транспортном уровнях модели OSI [51, 52].

10.2.2.3. Внедрение ложного объекта в информационную систему

Зачастую в распределенной информационной системе бывают недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов) при их взаимодействии с

объектами системы. В этом случае такая распределенная система может подвергнуться сетевой атаке, связанной с изменением параметров маршрутизации и внедрением в сеть ложного объекта. В том случае, если настройки сети таковы, что для взаимодействия объектов необходимо использовать алгоритмы удаленного поиска узлов, то это также может быть использовано для внедрения в систему ложного объекта. Таким образом, существуют два принципиально разных способа проведения атаки «внедрение ложного объекта в информационную систему» [51, 52]:

- внедрение ложного объекта путем навязывания ложного сетевого маршрута;
- внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети:
    - путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
    - путем формирования потока ложных ответов, не дожидаясь запросов от узлов сети.

Современные глобальные сети представляют собой совокупность сетевых сегментов, связанных между собой через узлы-маршрутизаторы. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждой пары адресатов сети указывается оптимальный маршрут. Основная цель атаки, связанной с внедрением ложного объекта путем навязывания ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте сетевой информационной системы так, чтобы новый маршрут проходил через ложный объект сети – узел атакующего. Реализация этой атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Данная атака проходит в две стадии [51, 52].

1. Атакующему необходимо от имени сетевых управляющих устройств (например, маршрутизаторов) произвести рассылку по сети специальных служебных сообщений, что приведет к изменению маршрутизации в сети. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, который будет проходить через его узел.
2. Атакующий наращивает количество трафика, перенаправленного через свой узел, и получает возможность вести прием, анализ и передачу сообщений, передаваемых по сети.

Внедрение ложного объекта путем навязывания ложного сетевого маршрута – активное воздействие безусловное по отношению к цели атаки. Данная удаленная атака может осуществляться как внутри одного сегмента сети, так и межсетевым образом, как с обратной связью, так и без обратной связи с атакуемым объектом на сетевом, транспортном и прикладном уровне модели OSI [51, 52].

В распределенной информационной системе часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, не-

обходимой для адресации передаваемых сообщений. Обычно такой информацией являются аппаратные и логические адреса объектов системы. Для получения подобной информации в распределенных системах используются различные алгоритмы удаленного поиска, заключающиеся в передаче по сети специальных поисковых запросов. После получения ответа на запрос запросивший субъект системы обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект системы начинает передачу информации. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить ARP- и DNS-запросы в сети Интернет [51, 52].

В случае использования в распределенной информационной системе механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный узел. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через этот ложный объект информационной системы [51, 52].

Другой вариант внедрения в распределенную информационную систему ложного объекта использует недостатки алгоритма удаленного сетевого поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса – и тогда его ложный ответ будет немедленно принят и обработан. Такая удаленная атака чрезвычайно распространена в глобальных сетях, когда у атакующего из-за нахождения его в другом сетевом сегменте относительно цели атаки просто нет возможности перехватить поисковый запрос [51, 52].

Внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети – активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации, которое может являться атакой по запросу от атакуемого объекта, а также безусловной атакой. Данная удаленная атака может быть как внутрисетевой, так и межсетевой, имеет обратную связь с атакуемым объектом и осуществляется на канальном, сетевом и прикладном уровнях модели OSI [51, 52].

10.2.2.4. Использование ложного объекта для организации удаленной атаки на систему

После внедрения ложного объекта в сеть и получения контроля над проходящим потоком информации в сети ложный объект может применяться для различных способов воздействия на перехваченную информацию. Выделяют следующие основные воздействия на информацию, перехваченную ложным объектом [51, 52]:

– селекция информации и сохранение ее на ложном сетевом объекте;
– модификация информации, проходящей через ложный сетевой объект;
– подмена информации, проходящей через ложный сетевой объект.

Селекция информации и сохранение ее на ложном сетевом объекте являются пассивной сетевой атакой, сходной с атакой «анализ сетевого трафика», которая дополнена динамическим семантическим анализом, производимым на ложном объекте. Вместе с тем наибольший интерес представляет возможность использования ложного объекта для модификации или подмены информации.

Рассматривают два основных вида модификации информации [51, 52]:

– модификация передаваемых данных;
– модификация передаваемого кода:
  - внедрение вирусов в передаваемый код;
  - изменение логики работы исполняемого кода.

Для модификации передаваемых данных на внедренном объекте производятся селекция потока перехваченной информации и его анализ. При этом может быть распознан тип передаваемых файлов (исполняемый или файл, содержащий данные). При обнаружении файла данных появляется возможность модифицировать эти данные, проходящие через ложный объект. При этом, если модификация данных является достаточно стандартным воздействием, то на модификации передаваемого кода стоит остановиться отдельно.

Ложный объект, проводя семантический анализ информации, проходящей через него, может выделять среди потока информации файлы, содержащие исполняемый код. Для того чтобы определить, что передается по сети – код или данные, – необходимо распознавать определенные особенности, свойственные конкретным типам исполняемых файлов. При этом можно выделить два различных по цели вида модификации кода [51, 52]:

– внедрение вирусов в передаваемый код;
– изменение логики работы исполняемого кода.

При внедрении вирусов в передаваемый код к исполняемому файлу дописывается тело вируса, а также изменяется точка начала исполнения кода так, чтобы она указывала на начало кода внедренного вируса. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что файл оказывается заражен вирусом в момент передачи его по сети. Такое возможно лишь при использовании воздействия «внедрение ложного объекта» [51, 52].

При изменении логики работы исполняемого файла при передаче его по сети происходит похожая модификация исполняемого кода. Однако ее цель – алгоритмическое воздействие, ориентированное на внедрение про-

граммных закладок, внесение в исполняемый файл дополнительных уязвимостей или эксплойтов. Сложностью такого воздействия является то, что для него, как правило, требуется предварительное исследование логики функционирования исполняемого файла [51, 52].

Внедрение ложного объекта позволяет не только модифицировать, но и подменять перехваченную им информацию. При возникновении в сети определенного контролируемого ложным объектом события одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация, в зависимости от контролируемого события, может быть, как исполняемым кодом, так и данными.

10.2.2.5. Атаки типа «отказ в обслуживании»

В общем случае в сетевой информационной системе каждый ее субъект должен иметь возможность подключиться к любому объекту системы и получить в соответствии со своими правами удаленный доступ к его информационным ресурсам. Обычно в сетевых информационных системах возможность предоставления удаленного доступа реализуется следующим образом: на объекте системы запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т. п.), предоставляющих удаленный доступ к ресурсам этого объекта. В случае получения запроса на соединение сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. Очевидно, что сервер способен отвечать лишь на ограниченное число запросов. Эти ограничения зависят от параметров информационной системы, пропускной способности ее сети и быстродействия ЭВМ, на которых он функционирует. Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов за счет отправки большого числа запросов к нему.

Различают три типа этих удаленных атак.

1. *Отказ в обслуживании* (DoS-атака) – передача с одного адреса такого количества запросов на атакуемый объект, которое позволяет передать пропускная способность канала связи. В данном случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) системы, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная блокировка объекта из-за невозможности системы заниматься ничем другим, кроме обработки запросов.
2. *Распределенная атака «отказ в обслуживании»* (DDoS-атака) – передача с нескольких объектов системы на другой атакуемый объект бесконечного числа запросов на подключение от имени этих или других объектов. Результатом применения этой удаленной атаки является нарушение на атакованном объекте рабо-

тоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов сетевой информационной системы.

3. *Зацикливание процедуры обработки запроса* – передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно переполнение буфера с последующим зависанием системы.

Удаленная сетевая атака «отказ в обслуживании» классифицируется как активное воздействие, осуществляемое с целью нарушения работоспособности системы, безусловное относительно цели атаки. Данная атака является однонаправленным воздействием, осуществляемым как межсетевым, так и внутрисетевым образом, осуществляемым на сетевом, транспортном и прикладном уровнях модели OSI [51, 52].

Схема классификации основных способов осуществления атаки «отказ в обслуживании» представлена на рис. 10.4.

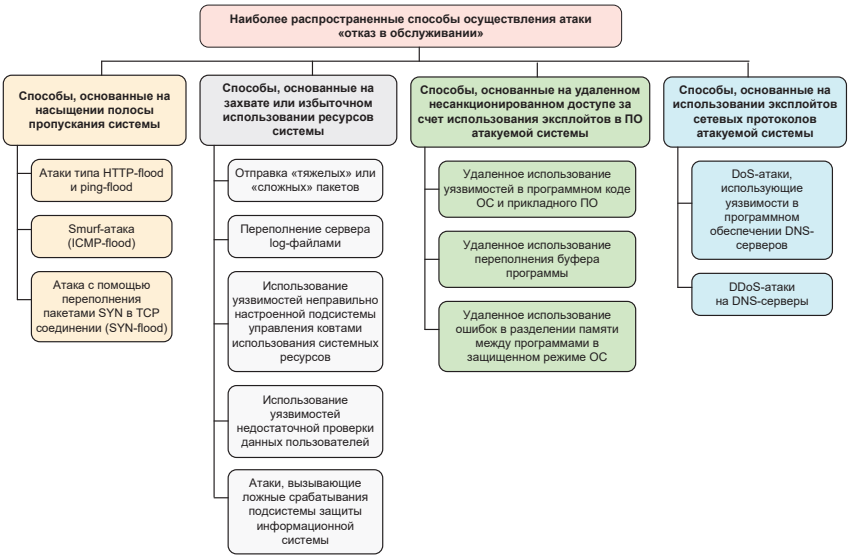


Рис. 10.4. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

Наиболее распространенными способами осуществления атаки «отказ в обслуживании» являются следующие.

1. Способы, основанные на насыщении полосы пропускания системы, – атаки, связанные с большим количеством, как правило, бессмысленных или сформированных в неправильном формате запросов к информационной системе или ее сетевому оборудованию, с целью обеспечить отказ

в работе системы из-за исчерпания ее системных ресурсов (процессорного времени, памяти или пропускной способности каналов связи). К наиболее распространенным таким способам относятся [7]:

– атаки типа HTTP-flood и ping-flood;
– Smurf-атака (ICMP-flood);
– атака с помощью переполнения пакетами SYN в TCP соединении (SYN-flood).

2. Способы, основанные на недостатке ресурсов системы, – атаки, связанные с захватом или избыточным использованием ресурсов информационной системы. К наиболее распространенным таким способам относятся [7]:

– отправка «тяжелых» или «сложных» пакетов;
– переполнение сервера log-файлами;
– использование уязвимостей неправильно настроенной подсистемы управления квотами использования системных ресурсов;
– использование уязвимостей недостаточной проверки данных пользователей;
– атаки, вызывающие ложные срабатывания подсистемы защиты информационной системы.

3. Способы, основанные на удаленном несанкционированном доступе за счет использования эксплойтов в ПО атакуемой системы. К наиболее распространенным таким способам относятся [7]:

– удаленное использование уязвимостей в программном коде операционной системы и прикладного ПО информационной системы;
– удаленное использование переполнения буфера программы;
– удаленное использование ошибок в разделении памяти между программами в защищенном режиме операционной системы.

4. Способы, основанные на использовании эксплойтов сетевых протоколов атакуемой системы. К наиболее распространенным таким способам относятся [7]:

– DoS-атаки, использующие уязвимости в ПО DNS-серверов;
– DDoS-атаки на DNS-серверы.

В настоящее время атаки типа «отказ в обслуживании» являются не только наиболее распространенными, но и наиболее опасными воздействиями. Так в ноябре 2002 г. была проведена глобальная DDoS-атака на корневые DNS-серверы с целью полного блокирования общедоступной сети Интернет. В результате этой атаки злоумышленники смогли вывести из строя 7 из 13 корневых DNS-серверов [7].

10.3. Компьютерные вирусы и другие вредоносные программы

В настоящее время вирусы являются наиболее известным и широко распространённым средством ИТВ воздействия на удаленные системы, в том числе, на ТКС, а также на их сетевые ОС и ПО.

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве профессиональных средств информационно-технического воздействия начато сравнительно недавно. К первому случаю такого использования относится использование в 2010 г. вируса Stuxnet с целью срыва ядерной программы Ирана за счет инфицирования АСУ технологическим процессом обогащения урана [53]. Особенностью современных профессиональных вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам и ориентированы на решение конкретной задачи (модули типа «классический вирус» – для саморазмножения в информационной системе, модули типа «червь» – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

В отличие от своих «непрофессиональных собратьев», средства информационно-технического воздействия на основе вирусов обладают следующими особенностями функционирования [53]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей 0-дня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД-атак;
- высокое качество кода и возможности обработки некорректных ситуаций.

Классификация компьютерных вирусов, до сих пор обладает некоторой неоднозначностью, т.к. многие вирусы сложно отнести к какому-либо одному типу. Вместе с тем по базовой функциональности и по способами распространения вирусы можно классифицировать по четырем основным типам (рис. 10.5) [7]:

1. классические вирусы – размножаются путем самокопирования, как правило, поражая отдельные вычислительные системы;
2. программы типа «червь» – предусматривает функционал самостоятельного перемещается по сети и проникает в ее отдельные узлы;
3. программы типа «троян» – имитирует полезную для пользователя функциональность, провоцируя его на активные действия по своему запуску или активации;
4. другие вредоносные программы.

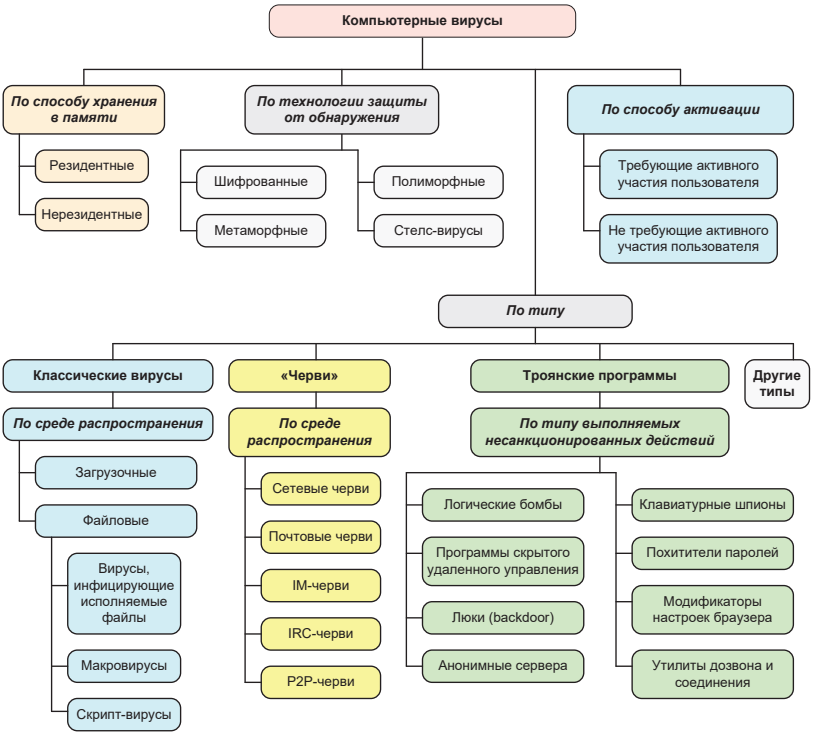


Рис. 10.5. Классификация компьютерных вирусов

По способу хранения в памяти информационной системы компьютерные вирусы можно классифицировать на [7]:

– резидентные;
– нерезидентные.

Резидентные вирусы после активации хранят свои копии в оперативной памяти системы, способны перехватывать события операционной системы и программ (например, обращения к файлам или дискам) и инициировать при этом процедуры заражения обнаруженных объектов. Поэтому резидентные вирусы опасны не только во время работы инфицированной программы, но и после ее окончания. Резидентные копии таких вирусов остаются жизнеспособными вплоть до выключения или перезагрузки информационной системы [7].

Нерезидентные вирусы, напротив, активны на довольно непродолжительных интервалах времени – пока функционирует инфицированная вирусом программа [7].

Для защиты от обнаружения со стороны антивирусов и средств защиты информационной системы в вирусах могут применяться следующие технологии [7]:

- *шифрование* – вирус состоит из двух функциональных элементов: собственно вирус и шифратор. При этом каждая конкретная копия вируса состоит из шифратора, собственного случайного ключа и собственно вируса, зашифрованного этим ключом;
- *метаморфизм* – создание различных копий вируса путем замены блоков команд на эквивалентные, путем перестановки местами участков кода, вставки между значащими участками кода незначащих команд и др.;
- *перехват управления* при обращении операционной системы или системы защиты к инфицированным элементам информационной системы.

Использование этих технологий маскировки вирусов привело к появлению следующих типов вирусов, которые классифицируются по технологии защиты от обнаружения [7]:

- *шифрованный вирус* – вирус, использующий простое шифрование своего тела со случайным ключом и неизменный шифратор. Такие вирусы могут быть обнаружены по сигнатуре шифратора;
- *метаморфный вирус* – вирус, применяющий метаморфизм ко всему своему телу для создания новых копий;
- *полиморфный вирус* – вирус, использующий метаморфный шифратор для шифрования тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора, также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм шифрования;
- *стелс-вирус* (*stealth virus* – вирус-невидимка) – вирус, полностью или частично скрывающий свое присутствие в системе путем перехвата обращений к операционной системе на осуществление чтения или записи в инфицированных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.) и подмены их содержимого с целью демонстрации подсистеме защиты оригинального содержимого объекта до его заражения.

Кроме того, компьютерные вирусы можно классифицировать по способу активации [7].

- *Требующие активного участия пользователя*. Отличительной особенностью таких компьютерных вирусов является использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с «почтовым червем», тем самым активируя его.
- *Не требующие активного участия пользователя*. Активация компьютерных вирусов без участия пользователя возможна за счет того, что вирус самостоятельно находит и использует уязвимости в безопасности информационной системы.

Далее представлены особенности основных типов вирусов более подробно.

10.3.1. Классические компьютерные вирусы

Основное свойство классического компьютерного вируса – это способность к саморазмножению [7].

Вирус – это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные системы и/или файлы, системные области операционных систем и прочие информационные ресурсы. При этом дубликаты сохраняют способность к дальнейшему распространению [7].

Условно жизненный цикл вируса можно разделить на пять стадий [7]:

1) проникновение на чужой компьютер;
2) активация;
3) поиск объектов для заражения;
4) подготовка копий;
5) внедрение копий.

Путями проникновения вируса могут служить мобильные носители, сетевые соединения, а также любые другие каналы, по которым можно скопировать файл. Однако, в отличие от «червей», вирусы не используют сетевые ресурсы – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал [7].

После проникновения следует активация вируса. В соответствии с выбранным методом активации вирусы делятся на следующие виды [7]:

- *загрузочные вирусы* – заражают загрузочные сектора жестких дисков и мобильных носителей;
- *файловые вирусы* – заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют следующие типы вирусов:
    - *вирусы, инфицирующие исполняемые файлы* – различными способами внедряются в исполняемые файлы программ (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;
    - *макровирусы* – инструкции, написанные на внутреннем языке команд заражаемого приложения (на так называемых, макросах);
    - *скрипт-вирусы* – инструкции, написанные на внутреннем языке для определенной командной оболочки (скриптов).

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или про-

граммной оболочке, для которой каждый конкретный вирус был написан [7].

Основная цель вируса – распространение на другие ресурсы информационной системы и выполнение деструктивных действий при определенных событиях или действиях пользователя [7].

10.3.2. Черви

В отличие от классических вирусов, программы типа «червь» – это вполне самостоятельные программы, которые также способны к саморазмножению, однако при этом они способны и к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «*сетевой червь*» [7].

Программа типа «червь» – это программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению подсистем защиты информационных систем, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом [7].

Жизненный цикл «червей» состоит из следующих стадий [7]:

- проникновение в информационную систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему «черви» классифицируются на следующие типы [7]:

- «сетевые черви» – используют для распространения локальные сети, каналы в информационно-вычислительных сетях, глобальные сети, в том числе и Интернет;
- «почтовые черви» – распространяются с помощью почтовых программ;
- «IM-черви» – используют для распространения системы мгновенного обмена сообщениями типа Internet Massager;
- «IRC-черви» – распространяются по каналам IRC (Internet Relay Chat) для обмена информацией в чатах и форумах;
- «P2P-черви» – распространяются при помощи пиринговых файлообменных P2P-сетей.

Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса) [7].

10.3.3. Троянские программы

В отличие от вирусов и червей, в программах типа «троянский конь» не всегда предусмотрен функционал саморазмножения. Довольно большая часть таких программ функцией саморазмножения вообще не обладает [7].

Программа типа «троян» (*«троянский конь»*) – программа, осуществляющая вредоносное воздействие, при этом отличительной чертой программы этого типа является то, что она имитирует полезную для пользователя функциональность, провоцируя его на активные действия по своему запуску или активации [7].

Некоторые «трояны» способны к самостоятельному преодолению подсистемы защиты информационной системы с целью проникновения в нее. Однако в большинстве случаев они проникают в систему вместе с вирусом либо с червем. В этом случае вирус или червь следует рассматривать как средство доставки, а «троян» – как средство информационного поражении [7].

Жизненный цикл «троянов» состоит всего из трех стадий [7]:

1) проникновение в систему;
2) активация;
3) выполнение вредоносных действий.

Как уже говорилось выше, проникать в информационную систему «трояны» могут двумя путями – самостоятельно и за счет кооперации с вирусом или «сетевым червем». В первом случае может быть использована маскировка, когда «троян» выдает себя за полезное приложение, которое пользователь самостоятельно копирует и запускает. При этом программа-носитель действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные «трояну» [7].

Для проникновения в информационную систему «трояну» необходима активация, и здесь он похож на «червя»: либо требует активных действий от пользователя, либо самостоятельно заражает его, используя уязвимости в защите информационной системы [7].

Программы типа «троян», как правило, классифицируются по типу выполняемых несанкционированных действий [7].

– *Программы скрытого удаленного управления* – это «трояны», которые обеспечивают несанкционированный удаленный контроль над инфицированной информационной системой. Такие программы предоставляют удаленному пользователю возможность скрытого исполнения программ в информационной системе, поиска, модификации и удаления информации, возможности скрыто загружать или отсылать информацию.
– *Анонимные сервера* – разновидность «троянов», которые используют ресурсы зараженной информационной системы в своих целях, связанных с несанкционированной сетевой активностью: создание bot-сетей и управление ими, выполнение несанкционированных распределенных вычислений, организация и координация DDOS-атак, массовая отправка электронной почты и другие подобные действия.
– *Клавиатурные шпионы* – находясь в оперативной памяти, записывают все данные, набираемые на клавиатуре, с целью последующей их передачи.

– *Похитители паролей* – предназначены для кражи паролей и другой конфиденциальной информации путем поиска на зараженной системе специальных файлов, которые ее содержат.
– *Модификаторы настроек браузера* (или других программ просмотра информации в сети) – изменяют настройки браузера таким образом, чтобы стали возможными удаленное исполнение кода в браузере, доступ к хранящейся в нём конфиденциальной информации, подмена сертификатов безопасности, перенаправление на ложные страницы и т. п.
– *Утилиты дозвона и соединения* – в скрытом от пользователя режиме инициируют несанкционированное подключение к удаленным сервисам.

Отдельно отметим, что существуют программы из класса «троянов», которые наносят вред другим удаленным информационным системам и сетям, при этом не нарушая работоспособности инфицированной системы. Примером таких программ могут служить анонимные сервера – организаторы DDoS-атак [7].

10.3.4. Примеры средств информационно-технических воздействий на основе компьютерных вирусов

Рассмотрим наиболее известные к настоящему времени средства информационно-технических воздействий на основе вирусов, а также особенности их применения в информационных операциях современности.

Stuxnet. Вирус Stuxnet – компьютерный червь, поражающий компьютеры под управлением операционной системы Microsoft Windows и промышленные системы, управляющие технологическими процессами. Это первое широко известное вирусное программное средство, имеющее точечную целевую функцию инфицирования конкретной АСУ с целью функционального поражения управляемого ею технологического процесса [53].

Вирус Stuxnet, внедренный в АСУ технологическим процессом обогащения урана, за счет перехвата и модификации команд от промышленного контролера марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens, в течение длительного времени задавал для центрифуг нештатный режим работы, что привело к отказу более 1000 центрифуг на иранском заводе по обогащению урана. Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру [53].

По заявлению бывших сотрудников NSA и JCS DoD, этот вирус был разработан в рамках американо-израильской операции противодействия ядерным планам Ирана. Stuxnet включает десяток выполняемых компонент общим объемом в 1,2 Мбайта, написанных в основном на языках *C* и *C++*. Базовой функциональной средой является Win32 [53].

Stuxnet поддерживает как минимум 8 способов саморазмножения, эксплуатацию более десяти уязвимостей, в том числе программной закладки (мастер-пароля), осуществляет контроль и управление через удаленные компьютеры (при обнаружении выхода в Интернет), включает Windows- и PLC-руткиты и другие способы маскировки и скрытия, а также выполняет обработку ошибочных ситуаций и др. Кроме того, Stuxnet способен внедряться в ряд системных «доверенных» процессов, в том числе инициируемых антивирусными продуктами, такими как: Avira, BitDefender, Computer Associates, Eset, F-Secure, Kaspersky Lab, McAfee, Symantec и Trend Micro [53].

Отличительными особенностями Stuxnet являются [53]:

- использование уязвимостей 0-дня;
- возможность распространения в изолированной среде (без выхода в Интернет), посредством flash-накопителей или собственной локальной p2p-сети;
- наличие компонент, подписанных 2 похищенными электронными цифровыми подписями;
- заражение системы управления технологическими процессами Siemens Simatic Step7;
- выполнение модификации PLC-кода на контроллерах Siemens с целью деструктивного воздействия на физическое оборудование (центрифуг обогащения урана) и дезинформацию операторов завода.

Функциональные клоны Stuxnet, адаптированные под новые цели, могут успешно использоваться для диверсий в АСУ промышленных предприятий, электростанций, управления движением транспорта и т. п.

Flame. Вирус-червь Flame, известный также как Skywiper или Flamer, является примером средства, ориентированного на решение конкретных разведывательных задач на Ближнем Востоке, в первую очередь в Иране. Отмечено около 700 заражений этим вирусом. Активный период действия вируса составлял порядка 6 лет до момента его обнаружения в 2012 г. [53].

Вирус Flame представляет собой комплекс программ объемом около 20 Мбайт (устанавливается поэтапно) и значительно превосходит в этом отношении вирус Stuxnet. В состав Flame входят: криптобиблиотеки, библиотеки архивирования zlib, libbz2, ppmd, СУБД sqlite3, веб-сервер, виртуальная машина Lua. Базовой функциональной средой является Win32 [53].

Ключевыми особенностями Flame являются [53]:

- использование уязвимостей, в том числе 0-дня;
- компрометация ЭЦП в ОС Windows (путем атаки на MD5);
- поиск офисных документов, проектной документации и чертежей (например, pdf и drw файлов), контактной информации, в том числе из соцсетей;
- возможность перехвата аудио и экранной информации;
- поиск и подключение к Bluetooth-устройствам;
- закрытая передача информации на удаленный компьютер;

– наличие инструментария для взлома механизмов защиты.

Что касается последнего, то в составе Flame имеются средства инвентаризации, мониторинга трафика, включая подсистему сбора парольной информации, поиска остаточной информации, анализа файловой системы, архивов и множества типов файлов, кейлогер и т. п. [53].

Flame может распространяться через USB-носители и сеть, также имеет оригинальную возможность обновления путем компрометации обновлений ОС Windows. Работа программы обеспечивается сложной динамичной инфраструктурой – например, известно около сотни доменов, задействованных для передачи данных на командные серверы Flame, попеременно располагавшиеся в различных странах мира. Несмотря на явно разведывательные цели, Flame содержит модуль удаления файлов [53].

Предположительно вирусы Flame и Stuxnet были разработаны одной командой в рамках американо-израильского сотрудничества и использовались совместно. При этом Flame имел разведывательные цели, а Stuxnet – диверсионные.

Duqu – вирус-червь, обнаруженный в 2011 г. Некоторые исследователи полагают, что он связан с червем Stuxnet. Распространение этого вируса происходило через электронную почту. Заражение системы происходит посредством использования уязвимости в ядре Windows, допускающей выполнение вредоносного кода. После заражения системы и установления связи с сервером происходит загрузка и установка дополнительного модуля, предназначенного для сбора сведений о системе, поиска файлов, снятия скриншотов, перехвата паролей и ряда других функций. Особенностью вируса Duqu является то, что он использует объектно-ориентированный фреймворк, написан на чистом C и скомпилирован Microsoft Visual C++ с необычными настройками оптимизации [53].

Специалисты компании Symantec считают, что создатели Duqu имели доступ к исходному тексту Stuxnet и целью Duqu был сбор информации для следующей версии Stuxnet.

Regin – вирус-червь, инфицирующий компьютеры под управлением ОС Windows. Этот вирус обнаружен Лабораторией Касперского и Symantec в 2014 г. Первые сообщения об этом вирусе появились весной 2012 г., а самые ранние выявленные экземпляры датируются 2003 г. Статистика заражений вирусом Regin по странам: 28% – в России; 24% – в Саудовской Аравии; по 9% – в Мексике и Ирландии; и по 5% – в Индии, Афганистане, Иране, Бельгии, Австрии и Пакистане. Статистика по объектам заражений: 28% – телекоммуникационные компании; 48% – частные лица и малый бизнес; остальные 24% – компьютеры государственных, энергетических, финансовых и исследовательских компаний. Regin представляет собой вирус-троянец, использующий модульный подход, который позволяет ему загрузить функции, необходимые для учета индивидуальных особенностей заражаемого компьютера или сети. Структура вируса рассчитана на постоянное, долговременное целевое наблюдение за многочисленными объектами. Regin не хранит данные в файловой системе зараженного

компьютера, вместо этого он имеет свою собственную зашифрованную виртуальную файловую систему (EVFS), которая выглядит как единый файл. В качестве метода шифрования EVFS использует вариант блочного шифра RC5. Regin осуществляет коммуникации через Интернет с использованием ICMP/Ping, команд, встраиваемых в HTTP cookie и протоколов TCP и UDP, превращая заражаемую сеть в ботнет [53].

Эксперты по уровню сложности и ресурсоемкости разработки сравнивают Regin с вирусом Stuxnet, в связи с чем высказываются мнения, что вирус мог быть создан на государственном уровне в качестве многоцелевого инструмента сбора данных.

Следует отметить, что для вышеперечисленных вирусных программ: Stuxnet, Flame, Duqu, а также других боевых вирусов (Gauss, MiniFlame, MiniDuqu и др.) эксперты отмечают общие высокотехнологические черты, такие как: библиотеки (в том числе open source), среды, используемые уязвимости, приемы противодействия средствам защиты, а также качество кода. Однако среди вирусных средств встречаются и программы другой архитектуры, уровня технологичности и качества реализации. Наглядным примером может быть троянская программа Sputnik, используемая в рамках разведывательной операции Red October.

Sputnik – троянская программа, предназначения для шпионажа. Целевой функцией программы Sputnik является сбор информации, касающейся деятельности дипломатических, правительственных, научных организаций. Максимальное число заражений пришлось на Россию. Особенностями указанной вредоносной программы являются [53]:

- использование известных уязвимостей Windows-приложений (Word, Excel, Outlook) и механизма социальных атак;
- сбор нескольких десятков типов офисных, графических, почтовых, адресных файлов, в том числе удаленных;
- сбор данных со сменных носителей, дистанционных почтовых серверов и мобильных устройств (iPhone, Nokia, Windows Mobile);
- сбор параметров сетевых устройств;
- сложная распределенная система управления (около 60 доменов).

По отношению к Sputnik отмечают следующие его особенности, такие как поддержка кириллицы и сбор файлов, закрытых с помощью Cryptofiler и PGP. Sputnic использует итерационные атаки с участием людей, когда в очередных атаках используются данные, полученные ранее [53].

Несмотря на то, что Sputnik не так технологически изящен, как вирусы класса Stuxnet, указанный вирус встречается с 2007 г. по сей день [53].

Wanna Crypt – сетевой червь, специализирующийся на шифровании пользовательских данных и требовании денег за расшифровку. Этот вирус не использовался как боевое средство, а использовался злоумышленниками. Однако в основу вируса Wanna Cry был положен код вирусного средства, разработанного АНБ США и украденного у него в результате хакер-

ской атаки. Украденный код использовал эксплойт Eternal Blue в Microsoft Windows [53].

Использование в вирусе Wanna Crypt боевого ядра оказалось весьма впечатляющим. Вирус имел просто сверхвысокую скорость распространения. Во время атаки в мае 2017 г. этот вирус заразил более 75 000 компьютеров в 99 странах, заблокировав работу многих организаций. Среди них – организации национальной службы здравоохранения Великобритании, основной железнодорожный оператор Германии компания Deutsche Bahn, телефонные компании Испании и Португалии, а также различные компании из США, Китая, Италии, Вьетнама, Тайваня. В России в результате атаки вируса Wanna Crypt были дестабилизирована работа телефонных операторов «Йота», «Мегафон», «Билайн», компаний «Сбербанк», «Связной», «РЖД», нарушена работа информационно-управляющих систем МВД, МЧС и Следственного комитета. Большое количество атак этого вируса именно на государственные учреждения России, в том числе на информационные системы ее силовых ведомств позволило некоторым специалистам сделать вывод, что атака Wanna Crypt является проверкой эффективности воздействия вирусных средств против критической информационной инфраструктуры России, которая проводится спецслужбами США под прикрытием некой «хакерской группировки» [53].

Факты применения представленных выше вирусных средств показывают, что противодействие таким программам не связано исключительно с использованием антивирусных средств. Так, в современных вирусных средствах используются технологии, которые позволяет им успешно преодолевать средства антивирусной защиты. К таким технологиям относятся [53]:

- наличие программных закладок, главным образом мастер-паролей;
- наличие уязвимостей 0-дня;
- отсутствие своевременного закрытия известных уязвимостей;
- нарушения политики безопасности;
- другие факторы, связанные с недостаточностью традиционных мер защиты.

10.3.5. Проблемные вопросы использования средств информационно-технических воздействий на основе компьютерных вирусов

Необходимо отметить, что использование вирусных средств не только позволяет решать целевые задачи ВС и органам безопасности, но и требует корректности в их конфигурировании и использовании.

Как показано в работе [53], использование вирусного ПО для целей обеспечения государственной безопасности, которое не обладает широким спектром защиты собственных каналов управления, может привести к утрате контроля над этими программами и бот-сетями на их основе. Кроме

того, при использовании таких средств необходимо тщательно продумывать тактику действий вируса и допустимый уровень вреда, который он может причинять инфицируемой системе.

Так в Германии для проведения оперативно-розыскных мероприятий правоохранительными органами был использован вирус-троян типа backdoor под названием R2D2. Этот вирус был предназначен для прослушивания телефонных разговоров через Skype и перехвата шифрованных SSL-соединений. При этом троян был способен запускать произвольный код на инфицированном компьютере, к тому же в него были встроены средства для наращивания функциональности путем дополнительной установки компонентов через сеть. Например, можно было добавлять компоненты для дистанционного включения через Интернет микрофона и видеокамеры, встроенных в компьютер, и использовать их для непосредственной слежки. Однако, внедряя широкую функциональность в области оперативно-розыскных мероприятий, разработчики не снабдили это вирусное средство элементарными функциями собственной информационной безопасности. Так, шифрование передаваемых данных об итогах работы R2D2 происходит лишь в одну сторону – в зашифрованном виде отсылаются лишь снимки экрана и аудиофайлы перехвата; при этом во всех версиях трояна применяется один и тот же ключ, который жестко встроен в код. Команды управления поступают к трояну в отрытом виде. При этом ни управляющие команды для троянца, ни его ответные сигналы совершенно никак не аутентифицированы и не содержат никакой защиты для обеспечения целостности соединения [53].

Эти факты позволили экспертному сообществу продемонстрировать перехват управления сетью вирусов-троянов R2D2. В результате успешного перехвата управления можно либо использовать получаемые от вирусов-троянов данные по своему усмотрению, либо фальсифицировать их с последующей передачей правоохранительным органам. Кроме этого, возможен сценарий, при котором серверные информационные системы правоохранительных органов могут быть атакованы через слабо защищенный служебный канал управления троянами [53].

Кроме вышесказанных собственных уязвимостей, троян R2D2 отличался тем, что существенно снижал уровень информационной безопасности инфицируемой системы, тем самым делая возможным несанкционированный доступ к ее информационным ресурсам со стороны других нарушителей [50].

Еще одним проблемным вопросом при использовании вирусных средств является контроль над профессиональными способами их создания, применения и распространения со стороны государственных служб.

В мае 2017 г. произошла одна из крупнейших мировых атак вирусом Wanna Crypt. Данный вирус продемонстрировал сверхбыструю скорость распространения и высокую результативность поражения пользовательских данных. За 2 недели своего функционирования Wanna Crypt заразил более 75 000 компьютеров в 99 странах, заблокировав работу многих орга-

низаций. Отличительной особенностью вируса Wanna Cry является то, что в его основу был положен код вирусного средства, разработанного АНБ США и украденного у него в результате хакерской атаки [53].

Низкая стоимость разработки и наличие большого количества документации по принципам функционирования критической информационной инфраструктуры делают весьма вероятными разработку и использование вирусных средств со стороны иррегулярных воинских формирований и террористических групп и организованной преступности для проведения акций информационной войны.

В настоящее время уже имеются профессиональные платформы для создания вирусных средств, разработка которых финансируется международной организованной преступностью.

Одним из таких вирусных средств является троян CosmicDuke, собранный на платформе BotGenStudio, которая позволяет индивидуально сконфигурировать трояна-шпиона с учетом особенностей цели, против которой ведется шпионаж, а также выпускать индивидуальное обновление для этого вируса. В зависимости от настроек троян CosmicDuke может использовать различные способы для маскировки в информационной системе, собирать различные наборы данных и отправлять их несколькими способами. Троян CosmicDuk маскируется под легитимные приложения, которые санкционированно обращаются к Интернету: агенты обновления Java, Acrobat, Chrome и др. Троян CosmicDuke способен копировать документы разных типов, следить за клавиатурой, делать снимки экрана, получать доступ к адресным книгам из почтовых приложений и к паролям, сохраненным в системе и популярных мессенджерах, а также к файлам сертификатов безопасности. Собранная информация передается на управляющие серверы несколькими способами: по FTP и тремя вариантами HTTP-взаимодействия. При этом CosmicDuke использует все возможности для продолжения непрерывного функционирования – к примеру, он даже умеет запускаться через планировщик задач операционной системы [53].

Аналитики Лаборатории Касперского полагают, что платформа BotGenStudio может быть создана не только для нужд разработавшей ее группы, но и для продажи узкому кругу заказчиков [53].

Таким образом, уже сейчас наблюдается процесс, в результате которого иррегулярные воинские формирования, террористические группы и организованная преступность могут перейти от использования вирусов в качестве средств шпионажа и хищения финансовой информации к созданию этих вирусных средств на основе профессиональных технологий, а в дальнейшем – их применения для организации высокоэффективных терактов, ориентированных на информационные системы государственного и военного управления, энергосети, транспортную инфраструктуру и особо опасные промышленные производства.

10.4. Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа, либо намеренно измененный фрагмент программы, которые позволяют осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств подсистемы защиты. При этом в большинстве случаев закладка внедряется самим разработчиком ПО для реализации в информационной системе некоторых сервисных или недекларируемых функций.

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но, в отличие от вирусов, деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки играют роль перехватчиков паролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако, в отличие от вирусов, программные закладки не обладают способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом особенностью закладок, внедренных на стадии разработки ПО, является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы.

Классификация программных закладок представлена на рис. 10.6.

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности ПО. В связи с этим средства маскировки программных закладок преимущественно ориентированы на противодействие отладчикам программ, анализаторам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация (запутывание) программ, в которые внедрена закладка.

К отдельным типам программных закладок можно отнести:

– *логические бомбы* – характеризуются способностью при выполнении заранее заложенных в них условий (конкретный день, время суток, определенное действие пользователя или команда извне) выполнять несанкционированные действия по уничтожению или искажению информации, воспрещения доступа к тем или иным важным фрагментам информационного ресурса, либо дезорганизации работы технических средств;

– *люки* (*backdoor*) – программы, находящие или создающие уязвимости в защите информационной системы с целью дальнейшего предоставления удаленного несанкционированного доступа к ней.

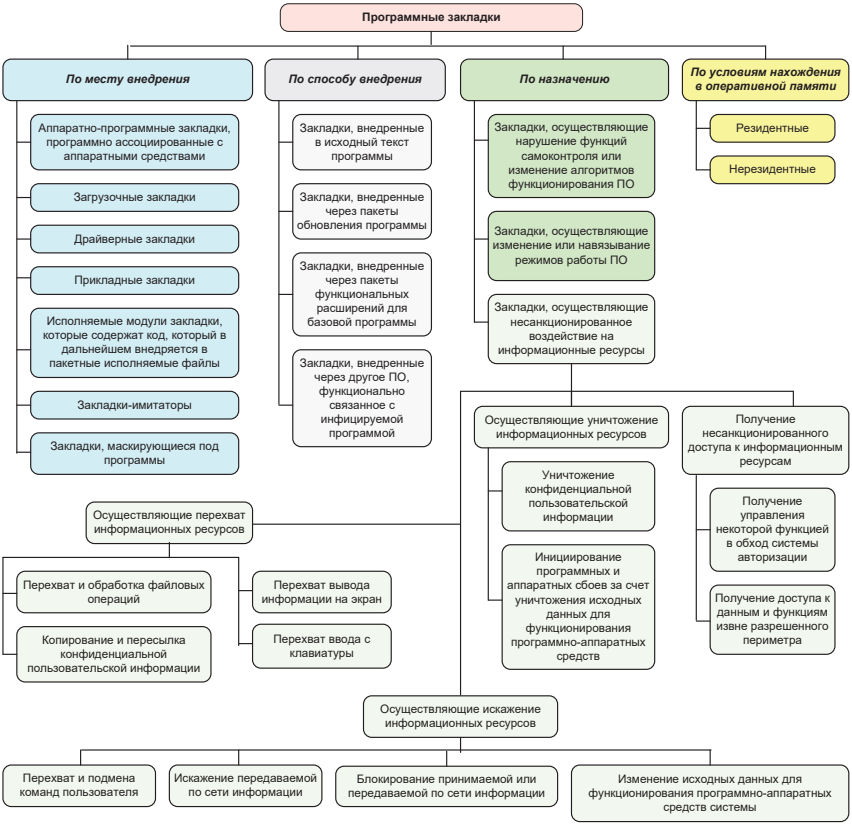


Рис. 10.6. Классификация программных закладок

10.5. Аппаратные закладки

Аппаратная закладка – электронное устройство, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных или технических средств информационной системы.

Результатом работы аппаратной закладки может быть, как полное выведение системы из строя, так и нарушение ее нормального функционирования, например, несанкционированный доступ к информации, ее изменение или блокирование.

Классификация аппаратных закладок приведена на рис. 10.7.

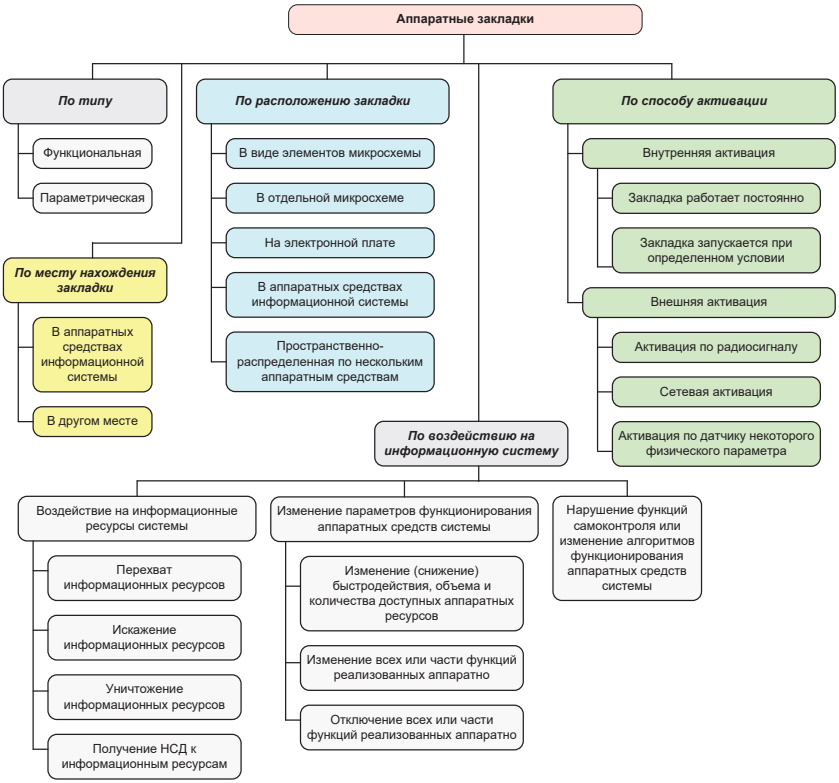


Рис. 10.7. Классификация аппаратных закладок

Схематическая сложность современного микроэлектронного оборудования, тенденции к миниатюризации его элементов ведут к тому, что производители такого оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, функционирующих в интересах тестирования такого оборудования, а при подключении устройств к глобальной сети – осуществлять обновление алгоритма их функционирования, а также условий срабатывания. Краткая характеристика технологий современных аппаратных закладок представлена в таблице 10.1.

Таблица 10.1 – Технологии современных аппаратных закладок

Методы внедрения	Методы обнаружения	Методы маскировки
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной рабо-	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486)

той и блокировка и замена неисправных узлов для продления срока службы СБИС)	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, недоступной пользователю. Шифрование (мутирование) участков кода, антитрассировка
Виртуализация вычислений	Анализ контента проходящих по сети данных	
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радио-мониторинг. Электромагнитный контроль.	

Материал раздела 10 подготовлен на основе работ [48-53, 55].

11. Механизмы реализации удаленных атак в глобальной сети Интернет

В настоящее время отдельный ТКС зачастую интегрируются через сеть Интернет. При этом, такое подключение к сети Интернет создают угрозы для реализации ИТВ типа «уделенные сетевые атаки» на ТКС. Возможности по реализации удаленных сетевых атак в сети Интернет настолько многообразны, что рассмотреть их все не представляется возможным. Цель данного раздела, не производя исчерпывающего анализа механизмов отдельных удаленных сетевых атак, на отдельных простых примерах продемонстрировать реализации типовых уязвимостей рабочих станций в сети Интернет.

В основу рассмотренных примеров положены типовые удаленные сетевые атаки, представленные в Базовой модели угроз безопасности персональных данных при их обработке в информационных системах [54], утвержденной ФСТЭК России.

11.1. Анализ сетевого трафика

В сети Интернет основными базовыми протоколами удаленного доступа являются TELNET и FTP (File Transfer Protocol). TELNET – это протокол виртуального терминала (ВТ), позволяющий с удаленных хостов подключаться к серверам Интернет в режиме ВТ. FTP-протокол, предназначенный для передачи файлов между удаленными хостами. Для получения доступа к серверу по этим протоколам пользователю необходимо пройти на нем процедуру идентификации и аутентификации. В качестве информации, идентифицирующей пользователя, выступает его идентификатор (имя), а для аутентификации используется пароль. Особенностью протоколов FTP и TELNET является то, что пароли и идентификаторы пользователей передаются по сети в открытом, незашифрованном виде. Таким образом, необходимым и достаточным условием для получения удаленного доступа к хостам по протоколам FTP и TELNET являются имя и пароль пользователя.

Одним из способов получения паролей и идентификаторов пользователей в сети Интернет является анализ сетевого трафика. Сетевой анализ осуществляется с помощью специальной программы – анализатора пакетов, перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль (рис. 11.1). Сетевой анализ протоколов FTP и TELNET показывает, что TELNET разбивает пароль на символы и пересылает их по одному, помещая каждый символ из пароля в соответствующий пакет, а FTP, напротив, пересылает пароль целиком в одном пакете.

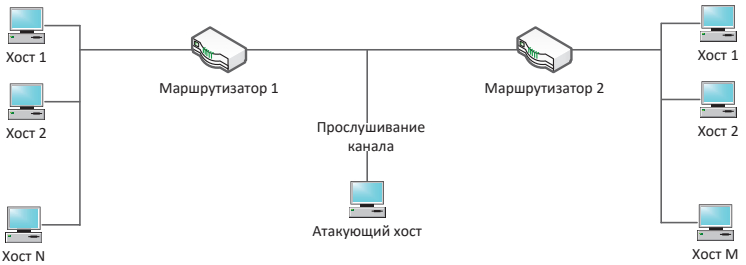


Рис. 11.1. Анализ сетевого трафика

11.2. Ложный ARP-сервер

В вычислительных сетях связь между двумя удаленными хостами осуществляется путем передачи по сети сообщений, которые заключены в пакеты обмена. В общем случае передаваемый по сети пакет независимо от используемого протокола и типа сети (Token Ring, Ethernet, X.25 и др.) состоит из заголовка пакета и поля данных. В заголовок пакета обычно заносится служебная информация, определяемая используемым протоколом обмена и необходимая для адресации пакета, его идентификации, преобразования и т. д. В поле данных помещаются либо непосредственно данные, либо другой пакет более высокого уровня OSI.

Так, например, пакет транспортного уровня может быть вложен в пакет сетевого уровня, который, в свою очередь, вложен в пакет канального уровня. Таким образом, пакет TCP (транспортный уровень) вложен в пакет IP (сетевой уровень), который, в свою очередь, вложен в пакет Ethernet (канальный уровень). Схема на рис. 11.2 наглядно иллюстрирует как выглядит, например, TCP-пакет в сети Интернет.

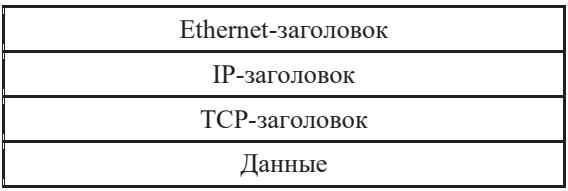


Рис. 11.2. Структура TCP-пакета

Базовым сетевым протоколом обмена в сети Internet является протокол IP (Internet Protocol). Протокол IP – это межсетевой протокол, позволяющий передавать IP-пакеты в любую точку глобальной сети. Для адресации на сетевом уровне (IP-уровне) в сети Интернет каждый хост имеет уникальный 32-разрядный IP-адрес. Для передачи IP-пакета на хост необходимо указать в IP-заголовке пакета в поле Destination Address IP-адрес этого хоста. Однако, как видно из рис. 11.2, IP-пакет находится внутри

Ethernet-пакета, поэтому каждый пакет в конечном счете адресуется на аппаратный адрес сетевого адаптера, непосредственно осуществляющего прием и передачу пакетов в сеть (при рассмотрении Ethernet-сети).

То есть, для адресации IP-пакетов в сети Internet кроме IP-адреса хоста необходим еще либо Ethernet-адрес его сетевого адаптера (в случае адресации внутри одной подсети), либо Ethernet-адрес маршрутизатора (в случае межсетевой адресации). Первоначально хост может не иметь информации о Ethernet-адресах других хостов, находящихся с ним в одном сегменте, в том числе и о Ethernet-адресе маршрутизатора. Следовательно, перед хостом встает стандартная проблема, решаемая с помощью алгоритма удаленного поиска.

В сети Интернет для решения проблемы удаленного поиска Ethernet-адресов используется протокол ARP (Address Resolution Protocol). Протокол ARP позволяет получить взаимно однозначное соответствие IP- и Ethernet-адресов для хостов, находящихся внутри одного сегмента.

Это достигается следующим образом.

- При первом обращении к сетевым ресурсам хост отправляет широковещательный ARP-запрос на Ethernet-адрес FFFFFFFFFFFFh, в котором указывает IP-адрес маршрутизатора и просит сообщить его Ethernet-адрес. Этот широковещательный запрос получат все станции в сегменте сети, в том числе и маршрутизатор.
- Получив такой запрос, маршрутизатор внесет запись о запросившем хосте в свою ARP-таблицу, а затем отправит на запросивший хост ARP-ответ, в котором сообщит свой Ethernet-адрес.
- Полученный в ARP-ответе Ethernet-адрес будет занесен в ARP-таблицу, находящуюся в памяти операционной системы на запросившем хосте и содержащую записи соответствия IP- и Ethernet-адресов для хостов внутри одного сегмента.

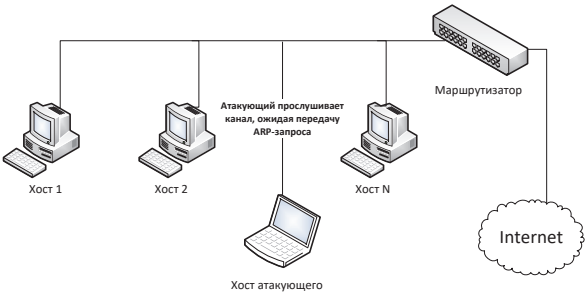
В случае использования в сети алгоритмов удаленного поиска существует возможность осуществления в такой сети типовой удаленной атаки «Ложный объект сети». Из анализа безопасности протокола ARP становится ясно, что, перехватив на атакующем хосте внутри конкретного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым хостом (например, маршрутизатором), и в дальнейшем активно контролировать и воздействовать на сетевой трафик «обманутого» хоста по схеме «Ложный объект сети».

Рассмотрим обобщенную функциональную схему ложного ARP-сервера (рис. 11.3):

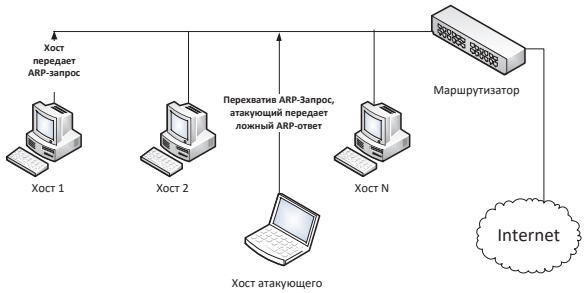
- ожидание ARP-запроса;
- при получении ARP-запроса передача по сети на запросивший хост ложного ARP-ответа, в котором указывается адрес сетевого адаптера атакующей станции (ложного ARP-сервера) или тот Ethernet-адрес, на котором будет принимать пакеты ложный ARP-сервер (совершенно необязательно указывать в ложном ARP-ответе свой настоящий Ethernet-адрес, так как при работе

непосредственно с сетевым адаптером его можно запрограммировать на прием пакетов на любой Ethernet-адрес);

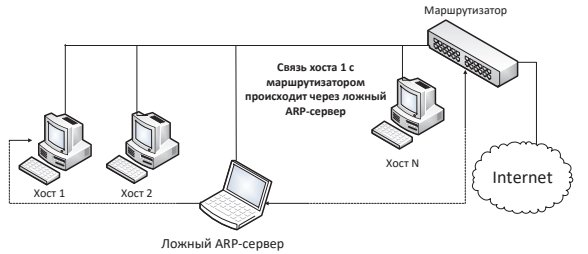
– прием, анализ, воздействие и передача пакетов обмена между взаимодействующими хостами, а также по возможности воздействие на перехваченную информацию.



а) Фаза ожидания ARP-запроса



б) Фаза атаки



в) Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном ARP-сервере

Рис. 11.3. Ложный ARP-сервер

В заключение необходимо отметить, что, во-первых, причина успеха такой удаленной атаки кроется, не столько в Интернете, сколько в широковещательной среде Ethernet и, во-вторых, очевидно, что эта удаленная ата-

ка является внутрисегментной и поэтому представляет угрозу только в случае нахождения атакующего внутри вашего сегмента сети.

11.3. Ложный DNS-сервер

Как известно, для обращения к хостам в сети Интернет используются 32-разрядные IP-адреса, уникально идентифицирующие каждый сетевой компьютер в этой глобальной сети. Однако, для пользователей применение IP-адресов при обращении к хостам является не слишком удобным и далеко не самым наглядным. Использование в Интернете породило проблему преобразования имен в IP-адреса. Такое преобразование необходимо, так как на сетевом уровне адресация пакетов идет не по именам, а по IP-адресам, следовательно, для непосредственной адресации сообщений в Интернете имена не годятся. Для решения задачи преобразования мнемонически понятных для пользователей имен в IP-адреса была создана система преобразования имен, позволяющая хосту в случае отсутствия у него информации о соответствии имен и IP-адресов получить необходимые сведения от ближайшего информационно-поискового сервера – DNS (Domain Name System)-сервера.

Основной задачей, решаемой службой DNS является поиск по имени удаленного хоста его IP-адреса, который и необходим для непосредственной адресации.

Рассмотрим DNS-алгоритм удаленного поиска IP-адреса по имени в сети Интернет.

- Хост посылает на IP-адрес ближайшего DNS-сервера (он устанавливается при настройке сетевой ОС) DNS-запрос, в котором указывает имя сервера, IP-адрес которого необходимо найти.
- DNS-сервер, получив запрос, просматривает свою базу имен на наличие в ней указанного в запросе имени. В случае, если имя найдено, а, следовательно, найден и соответствующий ему IP-адрес, то на запросивший хост DNS-сервер отправляет DNS-ответ, в котором указывает искомый IP-адрес.
- В случае, если указанное в запросе имя DNS-сервер не обнаружил в своей базе имен, то DNS-запрос отсылается DNS-сервером на один из корневых DNS-серверов и описанная в этом пункте процедура повторяется, пока имя не будет найдено (или не найдено).

Анализируя с точки зрения безопасности уязвимость этой схемы удаленного поиска с помощью протокола DNS, можно сделать вывод о возможности осуществления в сети, использующей протокол DNS, типовой удаленной атаки «ложный объект сети». Практические изыскания и критический анализ безопасности службы DNS позволяют предложить три возможных варианта удаленной атаки на эту службу.

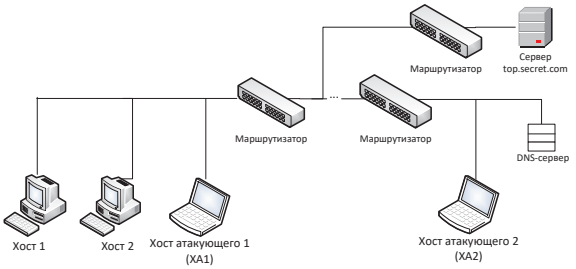
11.3.1. Внедрение в сеть ложного DNS-сервера путем перехвата DNS-запроса

Для реализации атаки путем перехвата DNS-запроса атакующему необходимо перехватить DNS-запрос, извлечь из него номер UDP-порта отправителя запроса, двухбайтовое значение ID идентификатора DNS-запроса и искомое имя и затем послать ложный DNS-ответ на извлеченный из DNS-запроса UDP-порт, в котором указать в качестве искомого IP-адреса настоящий IP-адрес ложного DNS-сервера. Это позволит в дальнейшем полностью перехватить трафик между атакуемым хостом и сервером и активно воздействовать на него по схеме «ложный объект сети».

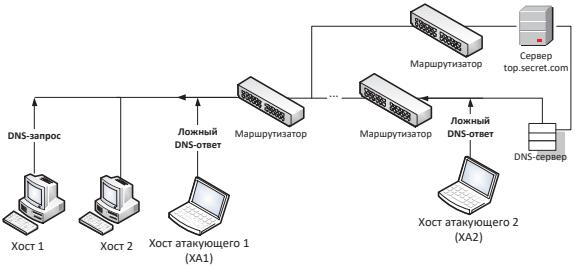
Рассмотрим обобщенную схему работы ложного DNS-сервера (рис. 11.4):

– ожидание DNS-запроса;
– извлечение из полученного запроса необходимых сведений и передача по сети на запросивший хост ложного DNS-ответа, от имени (с IP-адреса) настоящего DNS-сервера, в котором указывается IP-адрес ложного DNS-сервера;
– в случае получения пакета от хоста, изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на сервер (то есть ложный DNS-сервер ведет работу с сервером от своего имени);
– в случае получения пакета от сервера, изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на хост (для хоста ложный DNS-сервер и есть настоящий сервер).

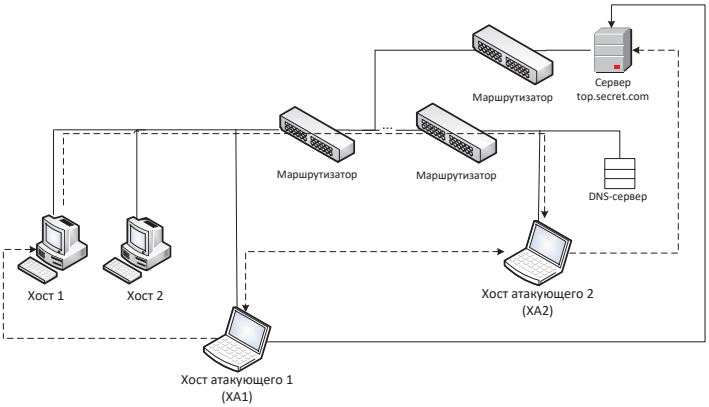
Необходимым условием осуществления такого варианта атаки является перехват DNS-запроса. Это возможно только в том случае, если атакующий находится либо на пути основного трафика, либо в сегменте настоящего DNS-сервера. Выполнение одного из этих условий местонахождения атакующего в сети делает подобную удаленную атаку трудно осуществимой на практике. Однако в случае выполнения этих условий возможно осуществить межсегментную удаленную атаку на сеть Интернет.



а) Фаза ожидания атакующим DNS-запроса
(он находится на XA1, либо на XA2)



б) Фаза передачи атакующим ложного DNS-ответа



в) Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 11.4. Функциональная схема ложного DNS-сервера

11.3.2. Внедрение в сеть ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост

Другой вариант осуществления удаленной атаки, направленной на службу DNS, основан на второй разновидности типовой УА «ложный объект сети» (при использовании недостатков алгоритмов удаленного поиска). В этом случае атакующий осуществляет постоянную передачу на атакуемый хост заранее подготовленного ложного DNS-ответа от имени настоящего DNS-сервера без приема DNS-запроса! Другими словами, атакующий создает в сети Интернет направленный «шторм» ложных DNS-ответов.

Это возможно, так как обычно для передачи DNS-запроса используется протокол UDP, в котором отсутствуют средства идентификации пакетов.

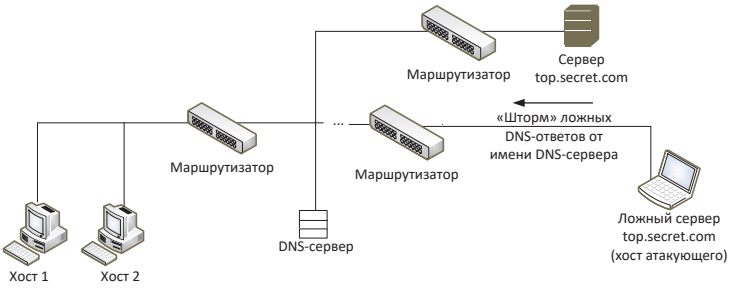
Критериями, предъявляемыми сетевой ОС хоста к полученному от DNS-сервера ответу, является:

- совпадение IP-адреса отправителя ответа с IP-адресом DNS-сервера;
- DNS-ответ должен содержать то же имя, что и в DNS-запросе;
- DNS-ответ должен быть направлен на тот же UDP-порт, с которого был послан DNS-запрос (в данном случае это первая проблема для атакующего);
- в DNS-ответе поле идентификатора запроса в заголовке DNS (ID) должно содержать то же значение, что и в переданном DNS-запросе (а это вторая проблема).

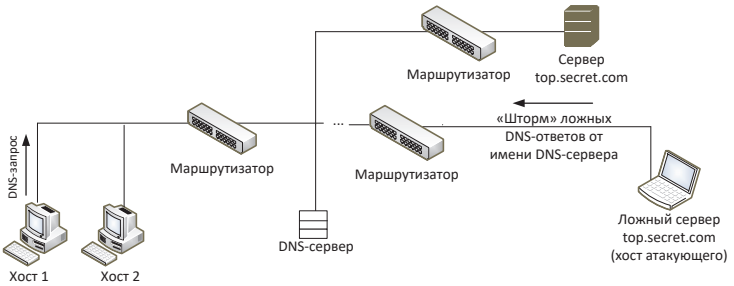
В данном случае, так как атакующий не имеет возможности перехватить DNS-запрос, то основную проблему для него представляет номер UDP-порта, с которого был послан запрос. Однако, как было отмечено ранее, номер порта отправителя принимает ограниченный набор значений (≥ 1023), поэтому атакующему достаточно действовать простым перебором, направляя ложные ответы на соответствующий перечень портов. На первый взгляд, второй проблемой может быть двухбайтовый идентификатор DNS-запроса, но, в связи с особенностями функционирования протокола DNS он либо равен единице, либо в случае DNS-запроса от Netscape Navigator (например) имеет значение близкое к нулю (один запрос – ID увеличивается на 1).

Поэтому для осуществления такой удаленной атаки атакующему необходимо выбрать интересующий его хост (например, top.secret.com), маршрут к которому требуется изменить так, чтобы он проходил через ложный сервер – хост атакующего. Это достигается постоянной передачей (направленным «штормом») атакующим ложных DNS-ответов на атакуемый хост от имени настоящего DNS-сервера на соответствующие UDP-порты. В этих ложных DNS-ответах указывается в качестве IP-адреса хоста top.secret.com IP-адрес атакующего.

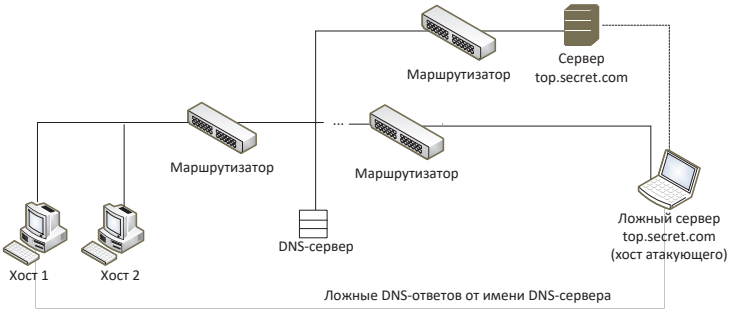
Далее атака развивается по следующей схеме. Как только цель атаки (атакуемый хост) обратится по имени к хосту top.secret.com, то от этого хоста в сеть будет передан DNS-запрос, который атакующий никогда не получит, но этого ему и не требуется, так как на хост сразу же поступит постоянно передаваемый ложный DNS-ответ, что и будет воспринят ОС атакуемого хоста как настоящий ответ от DNS-сервера. Все! Атака состоялась, и теперь атакуемый хост будет передавать все пакеты, предназначенные для top.secret.com, на IP-адрес хоста атакующего, который, в свою очередь, будет переправлять их на top.secret.com, воздействуя на перехваченную информацию по схеме «ложный объект сети».



а) Атакующий создает направленный «шторм» ложных DNS-ответов на Хост 1



б) Хост 1 посылает DNS-запрос и немедленно получает ложный DNS-ответ



в) Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 11.5. Внедрение в Интернет ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост

Рассмотрим функциональную схему предложенной удаленной атаки на службу DNS:

- постоянная передача атакующим ложных DNS-ответов на атакуемый хост на различные UDP-порты и, возможно, с различными ID, от имени (с IP-адреса) настоящего DNS-сервера с указанием имени интересующего хоста и его ложного IP-адреса, которым будет являться IP-адрес ложного сервера – хоста атакующего;
- в случае получения пакета от хоста, изменение в IP-заголовке пакета его IP-адреса на IP-адрес атакующего и передача пакета на сервер (то есть ложный сервер ведет работу с сервером от своего имени – со своего IP-адреса);
- в случае получения пакета от сервера, изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного сервера и передача пакета на хост (для хоста ложный сервер и есть настоящий сервер).

Таким образом, реализация такой удаленной атаки, использующей пробелы в безопасности службы DNS, позволяет из любой точки сети Интернет нарушить маршрутизацию между двумя заданными объектами (хостами)! Данная удаленная атака осуществляется межсегментно по отношению к цели атаки и угрожает безопасности любого хоста Интернет, использующего обычную службу DNS.

11.3.3. Внедрение в сеть ложного сервера путем перехвата DNS-запроса или создания направленного «шторма» ложных DNS-ответов на атакуемый DNS-сервер

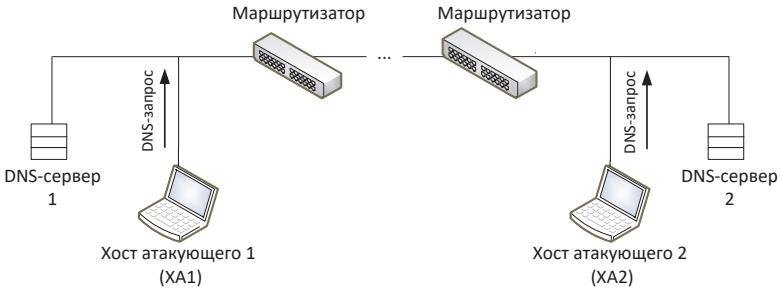
Из рассмотренной схемы удаленного DNS-поиска следует, что в том случае, если указанное в запросе имя DNS-сервер не обнаружил в своей базе имен, то запрос отсылается сервером на один из корневых DNS-серверов, адреса которых содержатся в файле настроек сервера root.cache.

Итак, в случае если DNS-сервер не имеет сведений о запрашиваемом хосте, то он сам, пересылая запрос далее, является инициатором удаленного DNS-поиска. Поэтому ничто не мешает атакующему, действуя описанными в предыдущих пунктах методами, перенести свою атаку непосредственно на DNS-сервер. В качестве цели атаки теперь будет выступать не хост, а DNS-сервер и ложные DNS-ответы будут направляться атакующим от имени корневого DNS-сервера на атакуемый DNS-сервер.

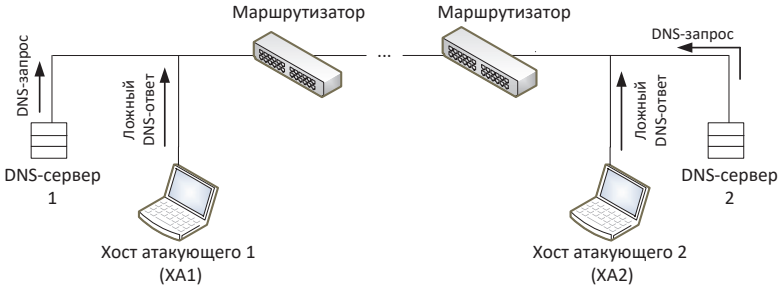
При этом важно учитывать следующую особенность работы DNS-сервера. Для ускорения работы каждый DNS-сервер кэширует в области памяти свою таблицу соответствия имен и IP-адресов хостов. В том числе в кэш заносится динамически изменяемая информация об именах и IP-адресах хостов, найденных в процессе функционирования DNS-сервера, а именно, если DNS-сервер, получив запрос, не находит у себя в кэш-таблице соответствующей записи, он пересылает ответ на следующий сервер и, получив ответ, заносит найденные сведения в кэш-таблицу в память.

Таким образом, при получении следующего запроса DNS-серверу уже не требуется вести удаленный поиск, так как необходимые сведения уже находятся у него в кэш-таблице.

Из анализа только что описанной схемы удаленного DNS-поиска становится очевидно, что в том случае, если в ответ на запрос от DNS-сервера атакующий направит ложный DNS-ответ (или в случае «шторма» ложных ответов будет вести их постоянную передачу), то в кэш-таблице сервера появится соответствующая запись с ложными сведениями и в дальнейшем все хосты, обратившиеся к этому DNS-серверу, будут дезинформированы, и при обращении к хосту, маршрут к которому атакующий решил изменить, связь с ним будет осуществляться через хост атакующего по схеме «ложный объект сети». И, что хуже всего, с течением времени эта ложная информация, попавшая в кэш DNS-сервера, будет распространяться на соседние DNS-серверы высших уровней, а, следовательно, все больше хостов в сети Интернет будут дезинформированы и атакованы!



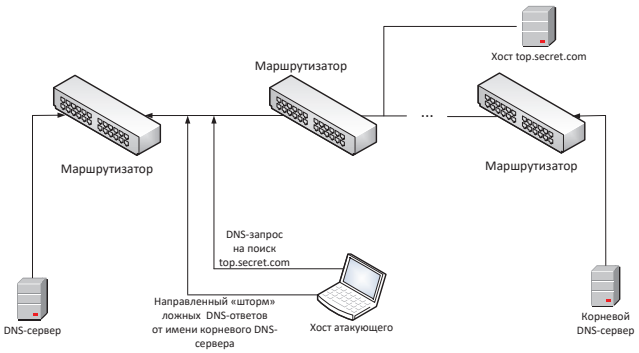
а) Фаза ожидания атакующим DNS-запроса от DNS-сервера (для ускорения атакующий генерирует необходимый DNS-запрос)



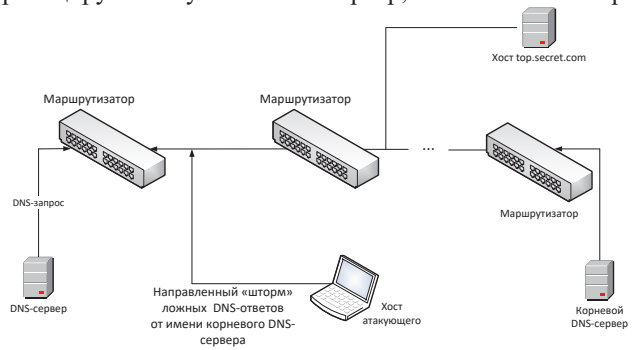
б) Фаза передачи атакующим ложного DNS-ответа на DNS-сервер 1

Рис. 11.6. Внедрение в Интернет ложного сервера путем перехвата DNS-запроса от DNS-сервера

В том случае, если атакующий не может перехватить DNS-запрос от DNS-сервера, то для реализации атаки ему необходим «шторм» ложных DNS-ответов, направленный на DNS-сервер. При этом возникает следующая проблема, отличная от проблемы подбора портов в случае атаки, направленной на хост. Как уже отмечалось ранее, DNS-сервер, посылая запрос на другой DNS-сервер, идентифицирует этот запрос двухбайтовым значением (ID). Это значение увеличивается на единицу с каждым передаваемым запросом. Узнать атакующему это текущее значение идентификатора DNS-запроса не представляется возможным. Поэтому предложить что-либо, кроме перебора 2^{16} возможных значений ID, достаточно сложно. Зато исчезает проблема перебора портов, так как все DNS-запросы передаются DNS-сервером на 53 порт.



а) Атакующий создает направленный «шторм» ложных DNS-ответов от имени одного из корневых DNS-серверов и при этом провоцирует атакуемый DNS-сервер, посылая DNS-запрос



б) DNS-сервер передает DNS-запрос на корневой DNS-сервер и немедленно получает ложный DNS-ответ от атакующего

Рис. 11.7. Внедрение в Интернет ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый DNS-сервер

Следующая проблема, являющаяся условием осуществления этой удаленной атаки на DNS-сервер при направленном «шторме» ложных DNS-ответов, состоит в том, что атака будет иметь успех только в случае, если DNS-сервер пошлет запрос на поиск имени, которое содержится в ложном DNS-ответе. DNS-сервер посылает этот столь необходимый и желанный для атакующего запрос в том и только том случае, когда на него приходит DNS-запрос от какого-либо хоста на поиск именно этого имени и такого имени не оказывается в кэш-таблице DNS-сервера. В принципе, этот запрос может возникнуть, когда угодно, и атакующему придется ждать результатов атаки неопределенное время. Однако, ничто не мешает атакующему, не дожидаясь никого, самому послать на атакуемый DNS-сервер подобный DNS-запрос и спровоцировать DNS-сервер на поиск указанного в запросе имени. Тогда эта атака с большой вероятностью будет иметь успех практически сразу же после начала ее осуществления.

Для примера приведем скандал (28 октября 1996 г.) с одним из московских провайдеров Интернет – компанией РОСНЕТ, когда пользователи этого провайдера при обращении к обычному информационному WWW-серверу попадали, как было сказано в репортаже СМИ, на WWW-сервер «сомнительного» содержания. В связи с абсолютным непониманием случившегося как журналистами (их можно понять – они не специалисты в этом вопросе), так и теми, кто проводил пресс-конференцию (специалистов к общению с прессой, наверное, просто не допустили) информационные сообщения об этом событии были настолько убоги, что понять, что случилось, было толком невозможно. Тем не менее, этот инцидент вполне укладывается в только что описанную схему удаленной атаки на DNS-сервер. С одним исключением: вместо адреса хоста, атакующего в кэш-таблицу DNS-сервера был занесен IP-адрес хоста www.playboy.com.

Использование в сети Интернет службы удаленного поиска DNS позволяет атакующему организовать в Интернете удаленную атаку на любой хост, пользующийся услугами этой службы, и может пробить серьезную брешь в безопасности этой и так отнюдь не безопасной глобальной сети.

11.4. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети ложного маршрутизатора

В сети Интернет используется управляющий протокол ICMP, одной из функций которого является удаленное управление маршрутизацией на хостах внутри сегмента сети. Удаленное управление маршрутизацией необходимо для предотвращения возможной передачи сообщений по неоптимальному маршруту. В сети Интернет удаленное управление маршрутизацией реализовано в виде передачи с маршрутизатора на хост управляющего ICMP-сообщения: Redirect Message. Исследование протокола ICMP показало, что сообщение Redirect бывает двух типов:

1) первый тип сообщения носит название Redirect Net и уведомляет хост о необходимости смены адреса маршрутизатора, то есть default-маршрута;
2) второй тип – Redirect Host – информирует хост о необходимости создания нового маршрута к указанной в сообщении системе и внесения ее в таблицу маршрутизации. Для этого в сообщении указывается IP-адрес хоста, для которого необходима смена маршрута (адрес будет занесен в поле Destination), и новый IP-адрес маршрутизатора, на который необходимо направлять пакеты, адресованные этому хосту (этот адрес заносится в поле Gateway).

Необходимо обратить внимание на важное ограничение, накладываемое на IP-адрес нового маршрутизатора: он должен быть в пределах адресов этой же подсети!

Что касается управляющего сообщения ICMP Redirect Host, то единственным идентифицирующим его параметром является IP-адрес отправителя, который должен совпадать с IP-адресом маршрутизатора, так как это сообщение может передаваться только маршрутизатором. Особенность протокола ICMP состоит в том, что он не предусматривает никакой дополнительной аутентификации источников сообщений. Таким образом, ICMP-сообщения передаются на хост маршрутизатором однонаправленно, без создания виртуального соединения.

Следовательно, ничто не мешает атакующему послать ложное ICMP-сообщение о смене маршрута от имени маршрутизатора. Приведенные выше факты позволяют осуществить типовую удаленную атаку «внедрение в сеть ложного объекта путем навязывания ложного маршрута».

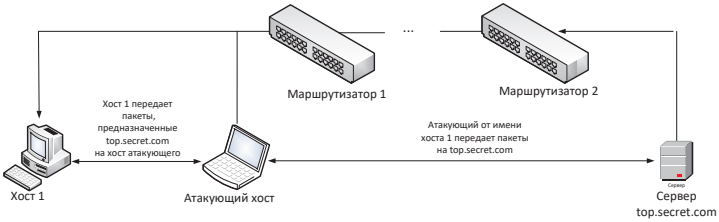
Для осуществления этой удаленной атаки необходимо подготовить ложное ICMP Redirect Host сообщение, в котором указать конечный IP-адрес маршрута (адрес хоста, маршрут к которому будет изменен) и IP-адрес ложного маршрутизатора. Далее это сообщение передается на атакуемый хост от имени маршрутизатора. Для этого в IP-заголовке в поле адреса отправителя указывается IP-адрес маршрутизатора. В принципе, можно предложить два варианта этой удаленной атаки.

В первом случае атакующий находится в том же сегменте сети, что и цель атаки. Тогда, послав ложное ICMP-сообщение, он в качестве IP-адреса нового маршрутизатора может указать либо свой IP-адрес, либо любой из адресов этой же подсети. Это даст атакующему возможность изменить маршрут передачи сообщений, направляемых атакованным хостом на определенный IP-адрес, и получить контроль над трафиком между атакуемым хостом и интересующим атакующего сервером. После этого атака перейдет во вторую стадию, связанную с приемом, анализом и передачей пакетов, получаемых от «обманутого» хоста.

Рассмотрим функциональную схему осуществления этой удаленной атаки (рис 11.8):

– передача на атакуемый хост ложного ICMP Redirect Host сообщения;
– отправление ARP-ответа в случае, если пришел ARP-запрос от атакуемого хоста;
– перенаправление пакетов от атакуемого хоста на настоящий маршрутизатор;
– перенаправление пакетов от маршрутизатора на атакуемый хост;
– при приеме пакета возможно воздействие на информацию по схеме «ложный объект сети».

а) Фаза передачи ложного ICMP Redirect сообщения от имени маршрутизатора

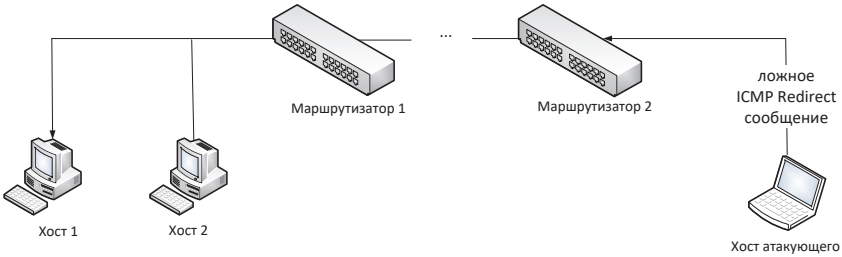


б) Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 11.8. Внутрисегментное навязывание хосту ложного маршрута при использовании протокола ICMP

В случае осуществления второго варианта удаленной атаки атакующий находится в другом сегменте относительно цели атаки. Тогда, в случае передачи на атакуемый хост ложного ICMP Redirect сообщения, сам атакующий уже не сможет получить контроль над трафиком, так как адрес нового маршрутизатора должен находиться в пределах подсети атакуемого хоста, поэтому использование такого варианта этой удаленной атаки не позволит атакующему получить доступ к передаваемой по каналу связи информации. Однако, в этом случае атака достигает другой цели: нарушается работоспособность хоста.

Атакующий с любого хоста в Интернете может послать подобное сообщение на атакуемый хост. В случае, если сетевая ОС на этом хосте не проигнорирует это сообщение, то связь между таким хостом и сервером, указанным в ложном ICMP-сообщении, будет нарушена. Это произойдет из-за того, что все пакеты, направляемые хостом на этот сервер, будут отправлены на IP-адрес несуществующего маршрутизатора. Схема этой атаки приведена на рис. 11.9.



а) Передача атакующим на хост 1 ложного ICMP Redirect сообщения от имени маршрутизатора 1

б) Дезинформация хоста 1. Его таблица маршрутизации содержит информацию о ложном маршруте к хосту top.secret.com

Рис. 11.9. Межсегментное навязывание хосту ложного маршрута при использовании протокола ICMP, приводящее к отказу в обслуживании

Оба варианта рассмотренной удаленной атаки удается осуществить (как межсегментно, так и внутрисегментно) на ОС Linux, Windows. Остальные сетевые ОС (Linux 2.0 и защищенный по классу B1 UNIX), игнорировали такое ICMP Redirect сообщение (что, не правда ли, кажется вполне логичным с точки зрения обеспечения безопасности).

11.5. Подмена одного из субъектов TCP-соединения в сети

Протокол TCP (Transmission Control Protocol) является одним из базовых протоколов транспортного уровня сети Интернет. Этот протокол

позволяет исправлять ошибки, которые могут возникнуть в процессе передачи пакетов, и является протоколом с установлением логического соединения – виртуального канала. По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление потоком пакетов, организовывается повторная передача искаженных пакетов, а в конце сеанса канал разрывается. При этом протокол TCP является единственным базовым протоколом из семейства TCP/IP, имеющим дополнительную систему идентификации сообщений и соединения. Именно поэтому протоколы прикладного уровня FTP и TELNET, предоставляющие пользователям удаленный доступ на хосты Интернета, реализованы на базе протокола TCP.

Для идентификации TCP-пакета в TCP-заголовке существуют два 32-разрядных идентификатора, которые также играют роль счетчика пакетов. Их названия – *Sequence Number* и *Acknowledgment Number*. Также нас будет интересовать поле, называемое *Control Bits*.

Это поле размером 6 бит может содержать следующие командные биты (слева направо):

– *URG*: Urgent Pointer field significant;
– *ACK*: Acknowledgment field significant;
– *PSH*: Push Function;
– *RST*: Reset the connection;
– *SYN*: Synchronize sequence numbers;
– *FIN*: No more data from sender.

Далее рассмотрим схему создания TCP-соединения (рис 11.10).

Предположим, что хосту *A* необходимо создать TCP-соединение с хостом *B*. Тогда *A* посылает на *B* следующее сообщение:

1. $A \rightarrow B$: *SYN*, *ISSa*

Это означает, что в передаваемом *A* сообщении установлен бит *SYN* (synchronize sequence number), а в поле *Sequence Number* установлено начальное 32-битное значение *ISSa* (Initial Sequence Number).

2. *B* отвечает:

$$B \rightarrow A: SYN, ACK, ISSb, ACK(ISSa+1)$$

В ответ на полученный от *A* запрос *B* отвечает сообщением, в котором установлен бит *SYN* и установлен бит *ACK*; в поле Sequence Number хостом *B* устанавливается свое начальное значение счетчика – *ISSb*; поле Acknowledgment Number содержит значение *ISSa*, полученное в первом пакете от хоста *A* и увеличенное на единицу.

3. *A*, завершая рукопожатие (handshake), посылает:

$$A \rightarrow B: ACK, ISSa+1, ACK(ISSb+1)$$

В этом пакете установлен бит *ACK*; поле *Sequence Number* содержит *ISSa* + 1; поле *Acknowledgment Number* содержит значение *ISSb* + 1. Посылкой этого пакета на хост *B* заканчивается трехступенчатый *handshake*, и TCP-соединение между хостами *A* и *B* считается установленным.

4. Теперь хост *A* может посылать пакеты с данными на хост *B* по только что созданному виртуальному TCP-каналу:

$A \rightarrow B$: *ACK*, *ISSa*+1, *ACK*(*ISSb*+1); *DATA*

Из рассмотренной выше схемы создания TCP-соединения видно, что единственными идентификаторами TCP-абонентов и TCP-соединения являются два 32-битных параметра Sequence Number и Acknowledgment Number. Следовательно, для формирования ложного TCP-пакета атакующему необходимо знать текущие идентификаторы соединения – *ISSa* и *ISSb*.

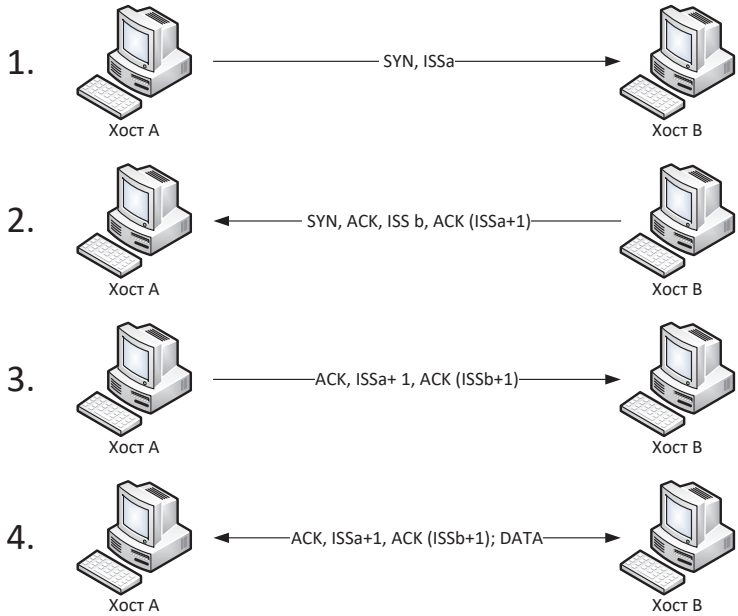


Рис. 11.10. Схема создания TCP-соединения

Проблема возможной подмены TCP-сообщения становится еще более важной, так как анализ протоколов FTP и TELNET, реализованных на базе протокола TCP, показал, что проблема идентификации FTP- и TELNET-пакетов целиком возлагается этими протоколами на транспортный уровень, то есть на TCP. Это означает, что атакующему достаточно, подобрав соответствующие текущие значения идентификаторов TCP-пакета для конкретного TCP-соединения (например, такое соединение может представлять собой FTP- или TELNET-подключение), послать пакет с любого хоста в сети Интернет от имени одного из участников соединения (например, от имени клиента), и такой пакет будет воспринят как верный! К тому же, так как FTP и TELNET не проверяют IP-адреса отправителей, от которых им приходят сообщения, то в ответ на полученный ложный пакет, FTP- или TELNET-сервер отправит ответ на указанный в ложном пакете настоящий IP-адрес атакующего, то есть атакующий начнет работу с

FTP- или TELNET-сервером со своего IP-адреса, но с правами легально подключившегося пользователя, который, в свою очередь, потеряет связь с сервером из-за рассогласования счетчиков.

11.6. Нарушение работоспособности хоста в сети путем использовании направленного «шторма» ложных TCP-запросов на создание соединения, либо при переполнении очереди запросов

Из рассмотренной в предыдущем пункте схемы создания TCP-соединения следует, что на каждый полученный TCP-запрос на создание соединения операционная система должна сгенерировать начальное значение идентификатора ISN и отослать его в ответ на запросивший хост. При этом, так как в сети Интернет (стандарта IPv4) не предусмотрен контроль за IP-адресом отправителя сообщения, то невозможно отследить истинный маршрут, пройденный IP-пакетом, и, следовательно, у конечных абонентов сети нет возможности ограничить число возможных запросов, принимаемых в единицу времени от одного хоста. Поэтому возможно осуществление типовой удаленной атаки «Отказ в обслуживании», которая будет заключаться в передаче на атакуемый хост как можно большего числа ложных TCP-запросов на создание соединения от имени любого хоста в сети (рис. 11.11).

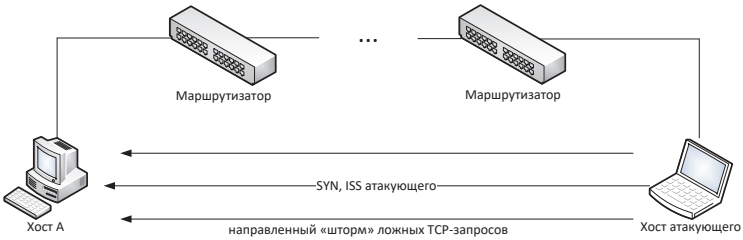


Рис. 11.11. Нарушение работоспособности хоста в сети Интернет, использующее направленный шторм ложных TCP-запросов на создание соединения

При этом атакуемая сетевая ОС в зависимости от вычислительной мощности компьютера либо – в худшем случае – практически зависает, либо – в лучшем случае – перестает реагировать на легальные запросы на подключение (отказ в обслуживании). Это происходит из-за того, что для всей массы полученных ложных запросов система должна, во-первых, сохранить в памяти полученную в каждом запросе информацию и, во-вторых, выработать и отослать ответ на каждый запрос. Таким образом, все ресурсы системы «съедаются» ложными запросами: переполняется очередь запросов и система занимается только их обработкой. Эффективность такой удаленной атаки тем выше, чем больше пропускная способ-

ность канала между атакующим и целью атаки, и тем меньше, чем больше вычислительная мощь атакуемого компьютера (число и быстродействие процессоров, объем ОЗУ и т. д.).

Другая разновидность атаки «Отказ в обслуживании» состоит в передаче на атакуемый хост нескольких десятков (сотен) запросов на подключение к серверу, что может привести к временному (до 10 минут) переполнению очереди запросов на сервере. Это происходит из-за того, что некоторые сетевые ОС устроены так, чтобы обрабатывать только первые несколько запросов на подключение, а остальные – игнорировать. То есть при получении *N* запросов на подключение, ОС сервера ставит их в очередь и генерирует соответственно *N* ответов. Далее, в течение определенного промежутка времени, сервер будет дожидаться от предполагаемого клиента сообщения, завершающего handshake («рукопожатия») и подтверждающего создание виртуального канала с сервером. Если атакующий пришлет на сервер количество запросов на подключение, равное максимальному числу одновременно обрабатываемых запросов на сервере, то в течение тайм-аута остальные запросы на подключение будут игнорироваться и к серверу будет невозможно подключиться.

Необходимо отметить, что в существующем стандарте сети Интернет IPv4 нет приемлемых способов надежно обезопасить свои системы от этой удаленной атаки. К счастью, атакующий в результате осуществления описанной атаки не сможет получить несанкционированный доступ к вашей информации. Он сможет лишь «съесть» вычислительные ресурсы вашей системы и нарушить ее связь с внешним миром. Остается надеяться, что нарушение работоспособности вашего хоста просто никому не нужно.

Материал раздела 11 подготовлен на основе работ [52, 55] и за счет обобщения материалов [51, 53, 54].

12. Обеспечение безопасности систем, входящих в состав телекоммуникационных сетей

Рассмотренные ранее угрозы нарушения ИБ в ТКС, способствуют активному развитию средств защиты, ориентированных на анализ трафика и сетевой активности пользователей. К основным таким средствам относятся:

– межсетевые экраны (firewall);
– виртуальные частные сети;
– системы предотвращения вторжений.

В данном подразделе, вышеуказанные средства защиты ТКС будут рассмотрены более подробно.

12.1. Межсетевые экраны (Firewall)

Межсетевой экран (*firewall*) – это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Межсетевые экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как Windows и Unix) или на специализированной аппаратно-программной платформе. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты. Правила политики безопасности усиливаются посредством использования модулей доступа.

Типы межсетевых экранов:

– межсетевые экраны прикладного уровня;
– межсетевые экраны с пакетной фильтрацией;
– гибридные межсетевые экраны.

12.1.1. Межсетевые экраны прикладного уровня

В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола.

Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности. При использовании межсетевого экрана прикладного уровня все соединения проходят через него (см. рис. 12.1).

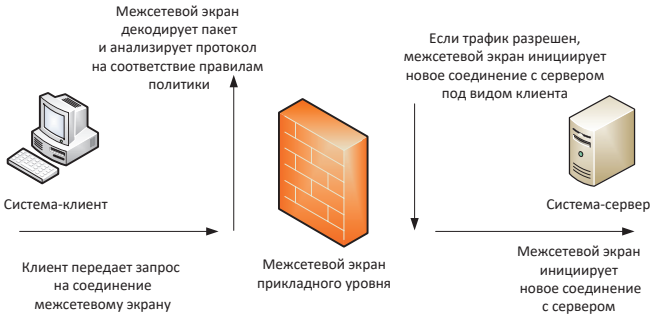


Рис. 12.1. Соединения модуля доступа межсетевого экрана прикладного уровня

Как показано на рисунке, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли этот трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

12.1.2. Межсетевые экраны с пакетной фильтрацией

Правила политики в межсетевых экранах с пакетной фильтрацией устанавливаются посредством использования *фильтров пакетов*. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране (см. рис. 12.2), а направляются непосредственно к конечной системе. При поступлении пакетов

межсетевой экран выясняет, разрешена ли передача этого пакета и соединение в соответствии с правилами политики безопасности. Если это так, то пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

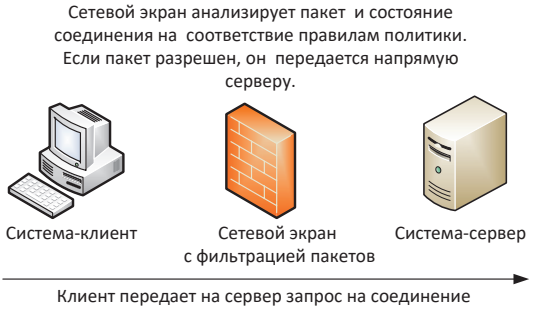


Рис. 12.2. Передача трафика через межсетевой экран с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое – для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

12.1.3. Гибридные межсетевые экраны

Как и многие другие устройства, межсетевые экраны изменяются и совершенствуются с течением времени, т. е. эволюционируют. Так технология модуля доступа Generic Services Proxy (GSP) разработана для поддержки модулями доступа прикладного уровня других протоколов, необходимых системе безопасности и при работе сетевых администраторов. В действительности GSP обеспечивает работу межсетевых экранов прикладного уровня в качестве экранов с пакетной фильтрацией.

Производители межсетевых экранов с пакетной фильтрацией также добавили некоторые модули доступа в свои продукты для обеспечения более высокого уровня безопасности некоторых широко распространенных протоколов. В то время как базовая функциональность межсетевых экранов обоих типов осталась прежней, (что является причиной большинства «слабых мест» этих устройств), сегодня на рынке присутствуют гибридные межсетевые экраны. Практически невозможно найти межсетевой экран,

функционирование которого построено исключительно на прикладном уровне или фильтрации пакетов. Это позволяет администраторам, отвечающим за безопасность, настраивать устройство для работы в конкретных условиях.

12.1.4. Пример конфигурирования межсетевого экрана

Стандартная архитектура использования межсетевого экрана показана на рис. 12.3. В представленной архитектуре используется только один межсетевой экран для защиты как внутренней сети, так и любых других систем, доступных из интернета. Эти системы располагаются в отдельной сети.

Рис. 12.3. Использование межсетевого экрана

Таблица 12.1 – Правила межсетевого экрана для сети на рис. 12.3

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, Telnet	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Таблица 12.2 – Краткий список номеров портов (для протокола TCP)

Протокол : номер порта	Протокол : номер порта
HTTP: 80, 8080	FTP: 21 для команд, 20 для данных
SSH: 22	TFTP: 69/UDP
POP3: 110	ICQ: 5190
SMTP: 25	telnet: 23
IMAP: 143	DNS: 53 (обычно UDP)

12.2. Организация и эксплуатация виртуальных частных сетей (VPN)

Частные сети состоят из каналов связи, арендуемых у различных телефонных компаний и поставщиков услуг интернета. Эти каналы связи характеризуются тем, что они соединяют только два объекта, будучи отделенными от другого трафика, так как арендуемые каналы обеспечивают двустороннюю связь между двумя сайтами.

Частные сети обладают множеством преимуществ:

- информация сохраняется в секрете;
- удаленные сайты могут осуществлять обмен информацией незамедлительно;
- удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ.

К сожалению, этот тип сетей обладает одним большим недостатком – высокой стоимостью. С увеличением числа пользователей интернета многие организации перешли на использование виртуальных частных сетей (Virtual Private Network – VPN). Виртуальные частные сети обеспечивают многие преимущества частных сетей за меньшую цену.

12.2.1. Определение виртуальных частных сетей

Значительная часть Интернет-трафика передается в открытом виде, и любой пользователь, наблюдающий за этим трафиком, сможет его распознать. Это относится к большей части почтового и веб-трафика, а также сеансам связи через протоколы telnet и FTP. Трафик Secure Shell (SSH) и Hyper text Transfer Protocol Secure (HTTPS) является шифруемым трафиком, и его не сможет просмотреть пользователь, отслеживающий пакеты. Тем не менее, трафик типа SSH и HTTPS не образует виртуальную частную сеть VPN.

Виртуальные частные сети обладают следующими характеристиками:

- трафик шифруется для обеспечения защиты от прослушивания;
- осуществляется аутентификация удаленного сайта;
- виртуальные частные сети обеспечивают поддержку множества протоколов;
- соединение обеспечивает связь только между двумя конкретными абонентами.

Так как SSH и HTTPS не способны поддерживать несколько протоколов, то же самое относится и к реальным виртуальным частным сетям. VPN-пакеты смешиваются с потоком обычного трафика в интернете и существуют отдельно по той причине, что такой трафик может считываться только конечными точками соединения.

VPN соединяет два конкретных объекта, образуя таким образом уникальный канал связи между двумя абонентами. Каждая из конечных точек VPN может единовременно поддерживать несколько соединений VPN с

другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.

Виртуальные частные сети, по методу использования, подразделяются на два типа:

1) пользовательские VPN;
2) узловые VPN.

12.2.2. Пользовательские VPN

Пользовательские VPN представляют собой виртуальные частные сети, построенные между отдельной пользовательской системой и узлом или сетью организации (часто пользовательские VPN используются сотрудниками, находящимися в командировке или работающими из дома).

Сервер VPN может являться межсетевым экраном организации либо быть отдельным VPN-сервером. Пользователь подключается к интернету через телефонное подключение к локальному поставщику услуг, через канал DSL или кабельный модем и инициирует VPN-соединение с узлом организации через интернет. Узел организации запрашивает у пользователя аутентификационные данные и, в случае успешной аутентификации, позволяет пользователю осуществить доступ ко внутренней сети организации, как если бы пользователь находился внутри узла и физически располагался внутри сети.

Пользовательские VPN позволяют организациям ограничивать доступ удаленных пользователей к системам или файлам. Это ограничение должно базироваться на политике организации и зависит от возможностей продукта VPN.

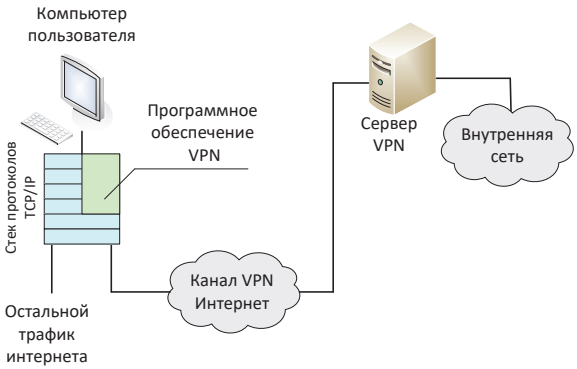


Рис. 12.4. Конфигурация пользовательской VPN

Пользовательские VPN обладают следующими двумя основными преимуществами.

1) Сотрудники, находящиеся в командировке, могут осуществлять доступ к электронной почте, файлам и внутренним системам в

любое время без необходимости в осуществлении дорогостоящих междугородних и международных телефонных вызовов для соединения с серверами.

2) Сотрудники, работающие из дома, могут осуществлять доступ к службам сети, как и сотрудники, работающие в организации, без аренды дорогостоящих выделенных каналов.

Оба эти преимущества можно приписать к экономии денежных средств. Экономия может заключаться в отказе от использования дорогостоящих междугородних и международных соединений, арендуемых каналов связи и т.д.

Самой большой проблемой безопасности при использовании VPN сотрудником является одновременное соединение с другими сайтами интернета. Как правило, программное обеспечение VPN на компьютере пользователя определяет, должен ли трафик передаваться через VPN, либо его необходимо отправить на какой-либо другой сайт в открытом виде. Если на компьютер пользователя была произведена атака с использованием «троянского коня», возможно, что некий внешний нелегальный пользователь использует компьютер сотрудника для подключения к внутренней сети организации. Атаки такого типа осуществляются довольно сложно, но они совершенно реальны.

12.2.3. Узловые VPN

Узловые виртуальные частные сети используются организациями для подключения к удаленным узлам без применения дорогостоящих выделенных каналов или для соединения двух различных организаций, между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством (см. рис. 17.5).

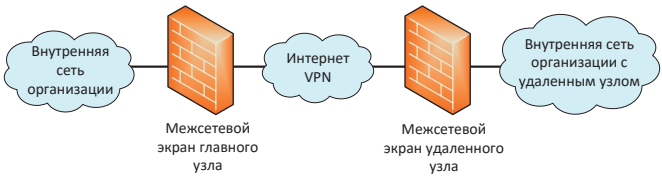


Рис. 12.5. Межузловое соединение VPN, проходящее через Интернет

Чтобы инициировать соединение, один из узлов осуществляет попытку передать трафик другому узлу. Вследствие этого на обоих противоположных узлах соединения VPN инициируется VPN. Оба конечных узла определяют параметры соединения в зависимости от политик, имеющихся на узлах. Оба сайта будут аутентифицировать друг друга посредством некоторого общего предопределенного секрета либо с помощью сертификата

с открытым ключом. Некоторые организации используют узловые VPN в качестве резервных каналов связи для арендуемых каналов.

Основным преимуществом узловой VPN является экономичность. Организация с небольшими, удаленными друг от друга офисами может создать виртуальную частную сеть, соединяющую все удаленные офисы с центральным узлом (или даже друг с другом) со значительно меньшими затратами. Сетевая инфраструктура также может быть применена значительно быстрее, так как в удаленных офисах могут использоваться локальные ISP для каналов ISDN или DSL.

Проблемы, связанные с узловыми VPN. Узловые VPN расширяют периметр безопасности организации, добавляя новые удаленные узлы или даже удаленные организации. Если уровень безопасности удаленного узла невелик, VPN может позволить злоумышленнику получить доступ к центральному узлу и другим частям внутренней сети организации. Следовательно, необходимо применять строгие политики и реализовывать функции аудита для обеспечения безопасности организации в целом. В случаях, когда две организации используют узловую VPN для соединения своих сетей, очень важную роль играют политики безопасности, установленные по обе стороны соединения. В данной ситуации обе организации должны определить, какие данные могут передаваться через VPN, а какие – нет, и соответствующим образом настроить политики на своих межсетевых экранах.

12.2.4 Понятие стандартных технологий функционирования VPN

Сеть VPN состоит из четырех ключевых компонентов.

1. *Сервер VPN.* Сервер VPN представляет собой компьютер, выступающий в роли конечного узла соединения VPN. Сервер должен обладать характеристиками, достаточными для поддержки ожидаемой нагрузки. Большая часть производителей программного обеспечения VPN должна предоставлять рекомендации по поводу производительности процессора и конфигурации памяти, в зависимости от числа единовременных VPN-соединений.

2. *Алгоритмы шифрования.* Выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Неправильно реализованная система может сделать бесполезным самый мощный алгоритм шифрования. Приняв во внимание, сказанное выше, давайте изучим риски, связанные с использованием VPN.

3. *Система аутентификации.* Система аутентификации VPN должна быть двухфакторной. Пользователи могут проходить аутентификацию с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем.

4. *Протокол VPN.* Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN. В настоящее время стандартным протоколом для VPN является IPSec. Этот протокол представляет собой дополнение к IP, осуществляющее инкапсуляцию и шифрование заголовка TCP и полезной информации, содержащейся в пакете. IPSec также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). IPSec использует UDP-порт: 500 для начального согласования, после чего используется IP-протокол 50 для всего трафика. Для правильного функционирования VPN эти протоколы должны быть разрешены.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований.

Определение требований по безопасности в VPN должно включать в себя следующие аспекты:

- количество времени, в течение которого необходимо обеспечивать защиту информации;
- число одновременных соединений пользователей;
- ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке);
- число соединений с удаленным сервером;
- типы сетей VPN, которым понадобится соединение;
- ожидаемый объем входящего и исходящего трафика на удаленных узлах;
- политика безопасности, определяющая настройки безопасности.

При разработке системы также может оказаться полезным указать дополнительные требования, связанные с местоположением сотрудников, находящихся в поездке (имеются в виду узлы в других организациях или в номерах отелей), а также типы служб, которые будут работать через VPN.

12.2.5. Типы систем VPN

На настоящее время можно выделить три типа систем, на основе которых организуются VPN:

1) аппаратные системы;
2) программные системы;
3) веб-системы.

12.2.5.1. Аппаратные системы VPN

Аппаратные системы VPN, как правило, базируются на аппаратной платформе, используемой в качестве VPN-сервера. На этой платформе выполняется программное обеспечение производителя, а также, возможно, некоторое специальное программное обеспечение, предназначенное для улучшения возможностей шифрования. В большинстве случаев для построения VPN на системе удаленного пользователя необходимо наличие соответствующего программного обеспечения.

Аппаратная система VPN имеет два преимущества.

1) Скорость. Оборудование, как правило, оптимизировано для поддержки VPN, посредством чего обеспечивается преимущество в скорости по сравнению с компьютерными системами общего назначения. За счет этого достигается возможность поддержки большего числа одновременных VPN-соединений.
2) Безопасность. Если аппаратная платформа специально разработана для приложения VPN, из ее системы удалены все лишние программы и процессы. За счет этого снижается степень подверженности атакам по сравнению с компьютерной системой общего назначения, в которой работают другие процессы. Это не значит, что компьютер общего назначения не может быть должным образом защищен. Как правило, использование компьютера общего назначения требует дополнительных усилий по настройке безопасности.

12.2.5.2. Программные VPN

Программные VPN работают на компьютерных системах общего назначения. Они могут быть установлены на выделенной для VPN системе либо совместно с другим программным обеспечением, таким как межсетевой экран. При загрузке программного обеспечения необходимо обеспечить достаточную мощность аппаратной платформы для поддержки VPN. Так как VPN-продукт устанавливается на компьютеры, имеющиеся в организации, руководство организации должно позаботиться о соответствии компьютеров предъявляемым требованиям.

12.2.5.3. Веб-системы VPN

Веб-системы. Главным недостатком большинства пользовательских систем VPN является потребность в установке программного обеспечения на систему-клиент. Указанные проблемы привели к тому, что некоторые производители VPN стали рассматривать веб-браузеры в качестве VPN-клиентов и реализовывать этот подход на практике. Он заключается в том, что пользователь с помощью браузера подключается к VPN через SSL. SSL обеспечивает шифрование трафика, а подтверждение подлинности пользователя выполняется с помощью средств аутентификации, встроенных в систему. Для предоставления пользователю необходимых услуг используется

несколько различных механизмов. Среди них можно выделить надстройки браузера и виртуальные машины Java.

В то время как стоимость поддержки и обслуживания несомненно ниже, на момент написания этой книги ни одна из бесклиентных систем VPN не обеспечивает полную функциональность. Этим сетям VPN присущи ограничения, заключающиеся в наборе используемых приложений и методе подключения пользователей к внутренним системам.

12.3. Системы предотвращения вторжений (IDS)

12.3.1. Общие понятия о функционировании IDS

Обнаружение вторжений – задача, выполняемая сотрудниками, ответственными за безопасность информации в организации, при обеспечении защиты от атак, это активный процесс, при котором происходит обнаружение хакера при его попытках проникнуть в систему.

Система обнаружения вторжений (Intrusion detection system – IDS) обнаруживает несанкционированные попытки проникновения в защищаемый периметр. Обнаружение вторжений помогает при превентивной идентификации активных угроз посредством оповещений и предупреждений о том, что злоумышленник осуществляет сбор информации, необходимой для проведения атаки.

Базовая концепция системы обнаружения вторжений заключается в необходимости определения периметра защиты компьютерной системы или сети.

Периметр защиты сети представляет собой виртуальный периметр, внутри которого находятся компьютерные системы. Этот периметр может определяться межсетевыми экранами, точками разделения соединений или настольными компьютерами с модемами. Периметр может быть расширен для содержания домашних компьютеров сотрудников, которым разрешено соединяться друг с другом, или партнеров по бизнесу, которым разрешено подключаться к сети. С появлением в деловом взаимодействии беспроводных сетей периметр защиты организации расширяется до размера беспроводной сети. В случае если компания имеет части информационных ресурсов доступных напрямую из глобальной сети периметр защиты дополняется демилитаризированной зоной (DMZ – Demilitarized Zone). Суть DMZ заключается в том, что она не входит непосредственно ни во внутреннюю, ни во внешнюю сеть, и доступ к ней может осуществляться только по заранее заданным правилам межсетевого экрана. В DMZ нет пользователей – там располагаются только серверы.

Демилитаризованная зона DMZ служит для предотвращения доступа из внешней сети к ресурсам и компьютерам внутренней сети за счет выноса из локальной сети в особую зону всех сервисов, требующих доступа извне.

Сигнализация, оповещающая о проникновении злоумышленника, предназначена для обнаружения любых попыток входа в защищаемую область т. е. система обнаружения вторжений IDS предназначена для разграничения авторизованного входа и несанкционированного проникновения.

Цели использования IDS определяют требования для политики IDS. Потенциально целями применения IDS являются следующие.

– *Обнаружение атак.* Распознавание атак является одной из главных целей использования IDS. Система IDS запрограммирована на поиск определенных типов событий, которые служат признаками атак. В качестве простого примера приведем соединение через TCP-порт: 80 (HTTP), за которым следует URL, содержащий расширение .bat. Это может быть признаком того, что злоумышленник пытается использовать уязвимость на веб-сервере IIS.
– *Предотвращение атак.* При обнаружении атаки IDS должна выполнить действия по нейтрализации угрозы.
– *Обнаружение нарушений политики.* Целью системы IDS, настроенной на отслеживание политики, является отслеживание выполнения или невыполнения политики организации. В самом простом случае NIDS можно настроить на отслеживание всего вебтрафика вне сети. Такая конфигурация позволяет отслеживать любое несоответствие политикам использования Интернета.
– *Принуждение к использованию политик безопасности.* Применение системы IDS в качестве средства принудительного использования политики выводит конфигурацию мониторинга политики на более высокий уровень. При отслеживании политики IDS настраивается на выполнение действий при нарушении политики.
– *Принуждение к следованию политикам соединений.* Использования принудительного блокирования не запрошенных или запрещенных соединений.
– *Сбор доказательств.* Система IDS может оказаться полезной после обнаружения инцидента. В этом случае с помощью IDS можно собрать доказательства. Сетевую IDS можно настроить на отслеживание определенных соединений и ведение полноценного журнала по учету трафика.

Существуют два основных типа IDS:

1) *узловые* (Host IDS – HIDS) – располагается на отдельном узле и отслеживает признаки атак на этот узел;
2) *сетевые* (Network IDS – NIDS) – находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети.

На рис. 12.6 показаны два типа IDS, которые могут присутствовать в сетевой среде.

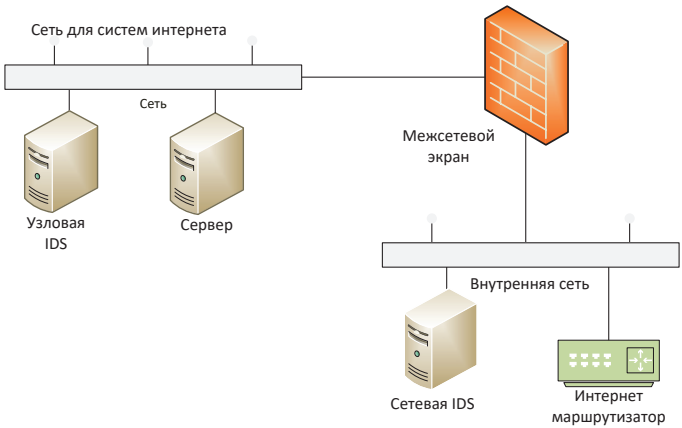


Рис. 12.6. Примеры размещения IDS в сетевой среде

17.3.2. Узловые IDS

Узловые IDS (Host Intrusion Detection System – HIDS) представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные типы событий (более детальное рассмотрение этих событий приводится в следующем разделе) и предпринимают определенные действия на сервере либо передают уведомления. Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик.

Существует пять основных типов датчиков HIDS.

1. *Анализаторы журналов.* Большая часть анализаторов журналов настроена на отслеживание записей журналов, которые могут означать событие, связанное с безопасностью системы. Анализаторы журналов по своей природе являются реактивными системами. Иными словами, они реагируют на событие уже после того, как оно произошло. Таким образом, журнал будет содержать сведения о том, что проникновение в систему выполнено. В большинстве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

2. *Датчики признаков.* Системы, основанные на сопоставлении признаков, обеспечивают возможность отслеживания атак во время их выполнения в системе, поэтому они могут выдавать дополнительные уведомления о проведении злоумышленных действий. Тем не менее, атака будет успешно или безуспешно завершена перед вступлением в действие датчика HIDS, поэтому датчики этого типа считаются реактивными. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

3. *Анализаторы системных вызовов.* Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью. Датчики HIDS этого типа размещают в программном слое между операционной системой и приложениями. Когда приложению требуется выполнить действие, его вызов к операционной системе анализируется и сопоставляются с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора IDS. Анализаторы системных вызовов отличаются от анализаторов журналов и датчиков признаков HIDS тем, что они могут предотвращать действия. Если приложение генерирует вызов, соответствующий, например, признаку атаки на переполнение буфера, датчик позволяет предотвратить этот вызов и сохранить систему в безопасности.

4. *Анализаторы поведения приложений.* Анализаторы поведения приложений аналогичны анализаторам системных вызовов в том, что они применяются в виде программной спайки между приложениями и операционной системой. В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять такое действие, вместо определения соответствие вызова признакам атак. Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места или открыть новые сетевые соединения, датчик обнаружит несоответствующее норме поведение сервера и заблокирует действие.

5. *Контролеры целостности файлов.* Контролеры целостности файлов отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла. Конечная цифровая подпись файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть атрибуты файла, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

17.3.3. Сетевые IDS

Сетевые IDS (Network Intrusion Detection System – NIDS) представляет собой программный процесс, работающий на специально выделенной системе. NIDS переключает сетевую карту в режим работы, при котором сетевой адаптер пропускает весь сетевой трафик (а не только трафик, направленный на данную систему) в программное обеспечение NIDS. После этого происходит анализ трафика с использованием набора правил и признаков атак для определения того, представляет ли этот трафик какой-либо интерес. Если это так, то генерируется соответствующее событие.

На данный момент большинство систем NIDS базируется на признаках атак. Это означает, что в системы встроен набор признаков атак, с которыми сопоставляется трафик в канале связи. Если происходит атака, признак которой отсутствует в системе обнаружения вторжений, система NIDS не реагирует на такую атаку.

NIDS-системы позволяют указывать интересуемый трафик по адресу источника, конечному адресу, порту источника или конечному порту. Это дает возможность отслеживания трафика, не соответствующего признакам атак.

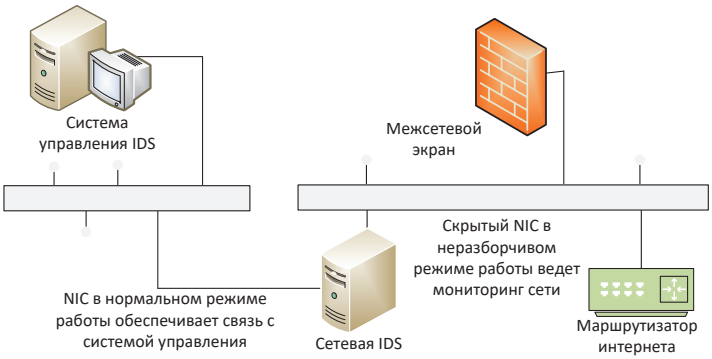


Рис. 12.7. Конфигурация NIDS с двумя сетевыми картами

Среди преимуществ использования NIDS можно выделить следующие аспекты.

- NIDS можно полностью скрыть в сети таким образом, что злоумышленник не будет знать о том, что за ним ведется наблюдение.
- Одна система NIDS может использоваться для мониторинга трафика с большим числом потенциальных систем-целей.
- NIDS может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков NIDS необходимо отметить следующие аспекты.

- Система NIDS может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам.
- NIDS может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов.
- Система NIDS не может определить, была ли атака успешной.
- Система NIDS не может просматривать зашифрованный трафик.
- В коммутируемых сетях (в отличие от сетей с общими носителями) требуются специальные конфигурации, без которых NIDS будет проверять не весь трафик.

12.3.4. Использование IDS

Пример использования IDS приведен на рис. 12.8.

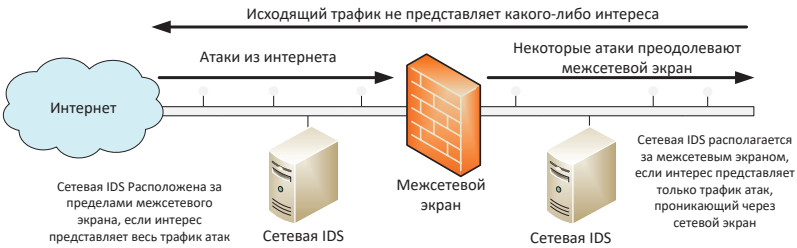


Рис. 12.8. Пример выбора объекта мониторинга

Таблица 12.3 – События, отслеживаемые при наличии политики IDS

Политика	NIDS	HIDS
Обнаружение атак	Весь трафик, поступающий на потенциально атакуемые системы (сетевые экраны, веб-серверы, серверы приложений и т.д.)	Неудачные попытки входа. Попытки соединения. Удачный вход с удаленных систем.
Предотвращение атак	То же, что и для обнаружения атак	То же, что и для обнаружения атак.
Обнаружение нарушений политики	Весь трафик HTTP, формируемый на системах клиентах. Весь трафик FTP, формируемый на системах клиентах	Успешные HTTP-соединения. Успешные FTP соединения. Загружаемые файлы.
Принуждение к использованию политик	То же, что и для обнаружения нарушений политики	То же, что и для обнаружения нарушения политики.
Принуждение к соответствию политикам соединений	Весь трафик, нарушающий принудительно используемую политику соединения	Успешные соединения с запрещенных адресов или по запрещенным портам.
Сбор доказательств	Содержимое всего трафика, формируемого на системе-цели или атакующей системе	Все успешные подключения, исходящие с атакующей системы. Все неудачные соединения с атакующих систем. Все нажатия клавиш из интерактивных сеансов на атакующих системах.

При обнаружении вторжения IDS должна выработать методы противодействия вторжению.

Рассматривают следующие виды действий при обнаружении вторжений.

– *Пассивная обработка* – это наиболее распространенный тип действий, предпринимаемых при обнаружении вторжения. Причина

этому проста – пассивные ответные действия обеспечивают меньшую вероятность повреждения легитимного трафика, являясь, в то же время, наиболее простыми для автоматического применения. Как правило, пассивные ответные действия осуществляют сбор большего числа информации или передают уведомления лицам, имеющим право на принятие более жестких мер.

– *Активная обработка события* – позволяет наиболее быстро предпринять возможные меры для снижения уровня вредоносного действия события. Однако если недостаточно серьезно отнестись к логическому программированию действий в различных ситуациях и не провести должного тестирования набора правил, активная обработка событий может вызвать повреждение системы или полный отказ в обслуживании легитимных пользователей. Среди активной обработки событий различают следующие.
– *Прерывание соединений, сеансов или процессов.* Вероятно, самым простым действием для понимания является прерывание события. Оно может осуществляться посредством прерывания соединения, используемого атакующим злоумышленником (это возможно только в том случае, если событие использует TCP-соединение), с закрытием сеанса пользователя или завершением процесса, вызвавшего неполадку.
– *Определение того, какой объект подлежит уничтожению*, выполняется посредством изучения события. Если процесс использует слишком много системных ресурсов, лучше всего завершить его. Если пользователь пытается использовать конкретную уязвимость или осуществить нелегальный доступ к файлам, то рекомендуется закрыть сеанс этого пользователя. Если злоумышленник использует сетевое соединение в попытках изучения уязвимостей системы, то следует закрыть соединение.

Таблица 12.4 – Примеры ответных действий, определяемые политикой IDS

Политика	Пассивные ответные действия	Активные ответные действия
Обнаружение атак	Ведение журналов. Ведение дополнительных журналов. Уведомление	Нет ответного активного действия.
Предотвращение атак	Ведение журналов. Уведомление.	Закрытие соединения. Завершение процесса. Возможна перенастройка маршрутизатора или межсетевого экрана.
Обнаружение нарушений политики	Ведение журналов. Уведомление	Нет ответного активного действия
Принудительное использование политик	Ведение журналов. Уведомление	Закрытие соединения. Возможно перенастройка прокси

Политика	Пассивные ответные действия	Активные ответные действия
Принудительное использование политик соединения	Ведение журналов. Уведомление	Закрытие соединения. Возможно перенастройка маршрутизатора или межсетевого экрана
Сбор доказательств	Ведение журналов. Ведение дополнительных журналов. Уведомление	Обманные действия. Возможно закрытие соединения

Материал раздела 12 подготовлен на основе работ [52, 55, 58] и за счет обобщения учебных материалов [56, 57].

13. Обеспечение безопасного взаимодействия в телекоммуникационных сетях

Рассмотренные в гл. 10-11 угрозы нарушения ИБ в ТКС, способствуют активному развитию средств защиты. Однако средства защиты не ограничиваются только такими средствами анализа трафика и сетевой активности пользователей, как межсетевые экраны, виртуальные частные сети, системы предотвращения вторжений. Существенной частью способов обеспечения безопасности является аутентификация пользователей, использование цифровых подписей и шифрования. Кроме того, используемые способы обеспечения безопасности не должны использоваться бессистемно – отдельные способы и средства должны применяться совместно по единому замыслу, определяемому политикой информационной безопасности. Данная глава посвящена рассмотрению именно этих аспектов ИБ.

13.1. Аутентификация и управление сертификатами

13.1.1. Электронные цифровые подписи

Электронная цифровая подпись (*ЭЦП*) — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи, позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки – подтвердить факт подписания электронного документа (неотказуемость).

С помощью ЭЦП можно повысить уровень этой защиты и обезопасить информацию от изменения после получения и дешифрования.

До настоящего времени наиболее часто для построения схемы цифровой подписи использовался алгоритм RSA. В основе этого алгоритма лежит концепция Диффи-Хеллмана. Она заключается в том, что каждый пользователь сети имеет свой закрытый ключ, необходимый для формирования подписи; соответствующий этому секретному ключу открытый ключ, предназначенный для проверки подписи, известен всем другим пользователям сети.

На рис. 13.1 показана схема формирования цифровой подписи по алгоритму RSA. Подписанное сообщение состоит из двух частей: незашифрованной части, в которой содержится исходный текст *T*, и зашифрованной части, представляющей собой цифровую подпись.

Если результат расшифровки цифровой подписи совпадает с открытой частью сообщения, то считается, что документ подлинный, не претерпел никаких изменений в процессе передачи, а автором его является именно тот человек, который передал свой открытый ключ получателю. Если

сообщение снабжено ЭЦП, то получатель может быть уверен, что оно не было изменено или подделано по пути.

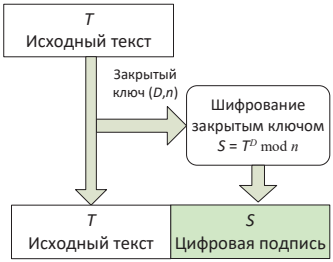


Рис. 13.1. Схема формирования ЭЦП по алгоритму RSA

Цифровые подписи применяются к тексту до того, как он шифруется. Если помимо снабжения текста электронного документа цифровой подписью надо обеспечить его конфиденциальность, то вначале к тексту применяют цифровую подпись, а затем шифруют все вместе: и текст, и цифровую подпись (рис. 13.2).

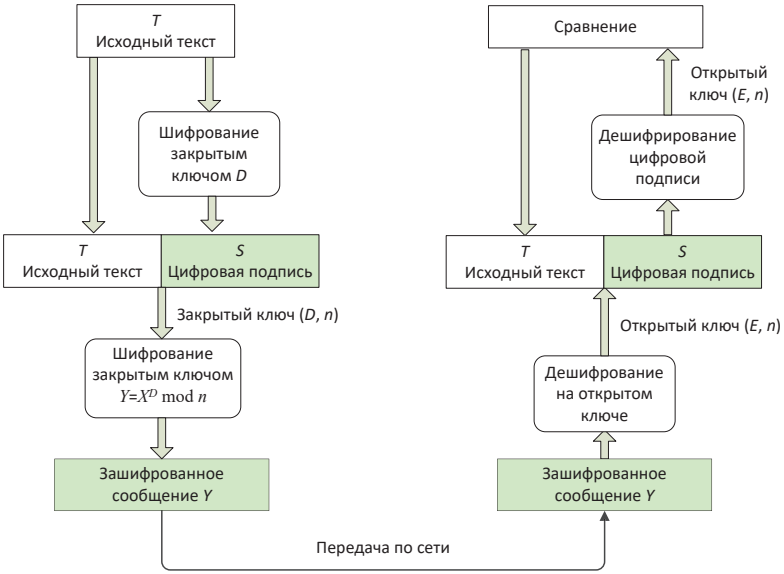


Рис. 13.2. Обеспечение конфиденциальности документа с ЭЦП

13.1.2. Управление ключами и сертификация ключей

Управление ключами является самой неприятной задачей при использовании любой системы шифрования. Ключи представляют собой самые важные объекты во всей системе, так как если злоумышленник получает ключ, у него появляется возможность расшифровывать все данные, зашифрованные с помощью этого ключа. Управление ключами заключается не только в защите их при использовании. Данная задача предусматривает создание надежных ключей, безопасное распространение ключей среди удаленных пользователей, обеспечение корректности ключей, отмену в случае их раскрытия или истечения срока действия.

Если ключи некоторым образом передаются в удаленное место расположения, они должны проверяться при получении на предмет того, не подверглись ли они вмешательству в процессе передачи. Это можно делать вручную либо использовать некоторую форму цифровой подписи.

Открытые ключи предназначены для публикации или передачи другим пользователям и должны *сертифицироваться* как принадлежащие владельцу ключевой пары. Сертификация осуществляется с помощью *центрального бюро* сертификатов (Certificate Authority – CA). В данном случае CA предоставляет цифровую подпись на открытом ключе, и благодаря этому CA с доверием воспринимает тот факт, что открытый ключ принадлежит владельцу ключевой пары (см. рис. 13.3).

Цифровой сертификат представляет собой цифровой документ (небольшой файл), заверяющий подлинность и статус владельца для пользователя или компьютерной системы.

Бюро сертификатов (Certificate Authority – CA) – объединение, включающее сервер сертификатов и создающее сертификаты.

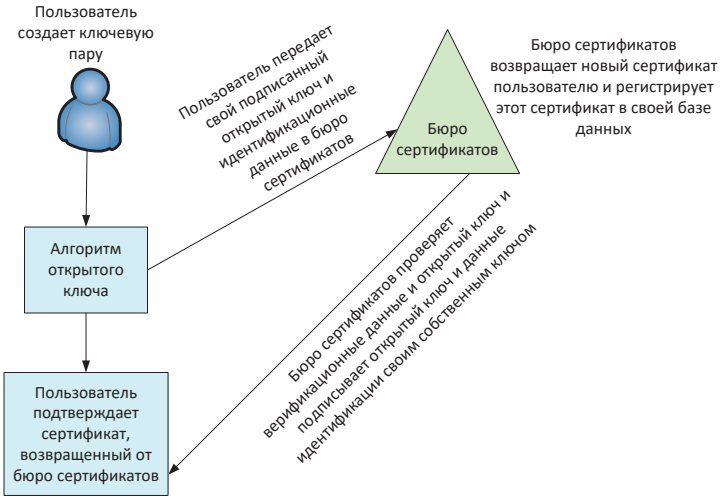


Рис. 13.3. Сертификация открытого ключа в бюро сертификатов

13.1.3. Концепция доверия в информационной системе

Концепция доверия является основополагающим принципом информационной безопасности и шифрования, в частности. Для работы шифрования необходима уверенность в том, что ключ шифра не будет раскрыт, и что используемый алгоритм шифрования является достаточно мощным. В случае с аутентификацией и цифровыми подписями необходима также уверенность в том, что открытый ключ на самом деле принадлежит тому, кто его использует.

13.1.3.1. Иерархическая модель доверия

Иерархическая модель доверия наиболее проста для восприятия. Говоря простым языком, в данном случае вы доверяете человеку, который находится выше в иерархической цепи, так как от него было получено соответствующее указание о необходимости доверия. На рис. 13.4 изображена схема этой модели.

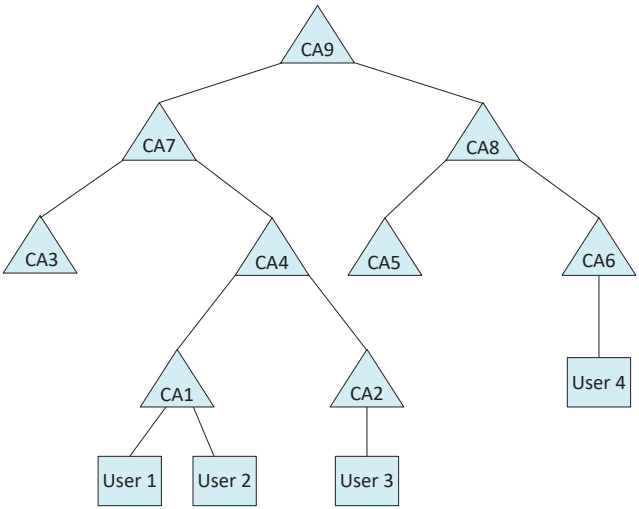


Рис. 13.4. Иерархическая модель доверия

Как видно из рисунка, пользователи $User_1$ и $User_2$ располагаются под CA_1. Следовательно, если CA_1 говорит, что сертификат открытого ключа принадлежит пользователю $User_1$, пользователь $User_2$ будет верить этому. На практике $User_2$ передает пользователю $User_1$ свой сертификат открытого ключа, подписанный CA_1. Пользователь $User_1$ проверяет подпись CA_1 с использованием открытого ключа CA_1. Так как CA_1 находится в иерархии

выше, чем $User_1$, то $User_1$ доверяет CA_1 и, следовательно, доверяет сертификату пользователя $User_2$.

Если пользователю $User_1$ нужно проверить информацию от пользователя $User_3$, все несколько усложняется. CA_1 не знает о пользователе $User_3$, в отличие от CA_2. Тем не менее, пользователь $User_1$ не доверяет CA_2, так как это бюро сертификатов напрямую не принадлежит цепочке пользователя $User_1$. Следующий уровень вверх по цепочке – CA_4. Пользователь $User_1$ может верифицировать информацию от пользователя $User_3$ посредством проверки с помощью CA_4 следующим образом.

- Пользователь $User_1$ смотрит на сертификат пользователя $User_3$. Он подписан в CA_2.
- Пользователь $User_1$ получает сертификат пользователя CA_2. Он подписан в CA_4.
- Так как пользователь $User_1$ доверяет CA_4, открытый ключ CA_4 может использоваться для верификации сертификата *CA2*.
- Как только сертификат CA_2 верифицирован, пользователь $User_1$ может верифицировать сертификат пользователя $User_3$.
- Как только будет верифицирован сертификат пользователя $User_3$, пользователь $User_1$ может использовать открытый ключ пользователя $User_3$ для верификации данных.

13.1.3.2. Сетевая модель доверия

Сеть с доверием представляет собой альтернативную модель доверия. Эта концепция была впервые использована в технологии Pretty Good Privacy (PGP).

Сетевая модель доверия заключается в том, что каждый пользователь сертифицирует свой сертификат и передает его известным ассоциированным объектам. Эти объекты могут подписать сертификат другого пользователя, так как он известен (см. рис. 13.5).

В такой модели не существует центрального бюро сертификатов. Если пользователю $User_1$ требуется верифицировать информацию, поступающую от пользователя $User_2$, он запрашивает сертификат пользователя $User_2$. Так как пользователь $User_1$ знает пользователя $User_2$, то доверяет сертификату и даже может его подписать.

Теперь рассмотрим ситуацию, в которой $User_1$ получает информацию от $User_3$. Пользователь $User_3$ не известен пользователю $User_1$, но у пользователя $User_3$ есть сертификат, подписанный пользователем $User_2$. Таким образом, рассматриваемая модель распространяется на всю компьютерную сеть. Единственным решением, которое должно приниматься в процессе работы, является число переходов, которому доверяет пользователь. Как правило, это число равно 3 или 4. Кроме того, может возникнуть ситуация, в которой для установления доверия другому пользователю есть два пути. Например, $User_2$ может использовать два пути установления доверия с пользователем $User_5$: один через пользователя $User_3$ и другой через

пользователя $User_4$. Так как оба пользователя $User_3$ и $User_4$ сертифицируют пользователя $User_5$, пользователь $User_2$ может быть уверен в сертификате пользователя $User_5$.

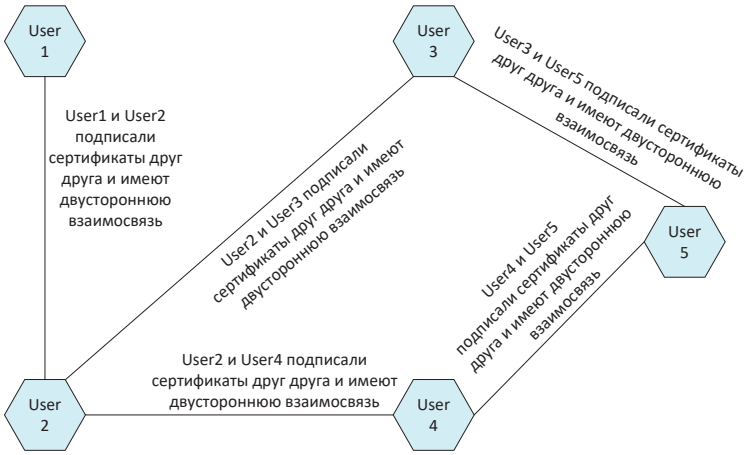


Рис. 13.5. Сетевая модель доверия

Главной проблемой, связанной с такой моделью доверия, является *недостаток масштабируемости.* Так как модель сети состоит из двусторонних взаимоотношений, каждый пользователь должен иметь некоторое число таких взаимосвязей, чтобы пользоваться в сети каким-либо доверием. На практике такие взаимосвязи могут отсутствовать, так как большинство пользователей работают с небольшим числом связей и редко выходят на уровень трех или четырех переходов.

13.1.4. Аутентификация с использованием протоколов открытого ключа

Протоколы открытых ключей позволяют устанавливать авторизованные шифруемые связи между узлами внутренних сетей и в интернете.

Существуют три модели аутентификации, проводимой в этих протоколах; они используются как по отдельности, так и в комбинации.

– *Аутентификация клиента.* Позволяет серверу Windows 2012 VPN или веб-серверу IIS идентифицировать пользователя с использованием стандартных методов шифрования на открытом ключе. Осуществляет проверку подлинности сертификата клиента и общего ID, а также проверку того, что эти данные сгенерированы бюро сертификатов, корневой сертификат которого установлен в перечне доверенных CA. Эта проверка очень важна, если сервером является банк, который передает конфиденциальную финан-

совую информацию клиенту и должен подтвердить личность получателя. На рис. 13.6 отображен процесс аутентификации.

– *Аутентификация сервера.* Позволяет клиенту VPN или браузеру клиента SSL/TLS подтверждать идентичность сервера, проверяя правильность сертификата сервера и идентификатора ID, а также то, что сертификаты выпущены бюро сертификатов (CA), корневой сертификат которого присутствует в перечне доверенных CA клиента. Это подтверждение имеет важное значение для пользователя веб-сайта, который отправляет номер кредитной карты через сеть и хочет удостовериться в том, что это именно тот сервер, который ему нужен.
– *Взаимная аутентификация.* Позволяет клиенту и серверу авторизовать друг друга единовременно. Взаимная аутентификация требует, чтобы клиент и сервер имели цифровые сертификаты и соответствующие корневые сертификаты CA в перечнях доверенных CA.

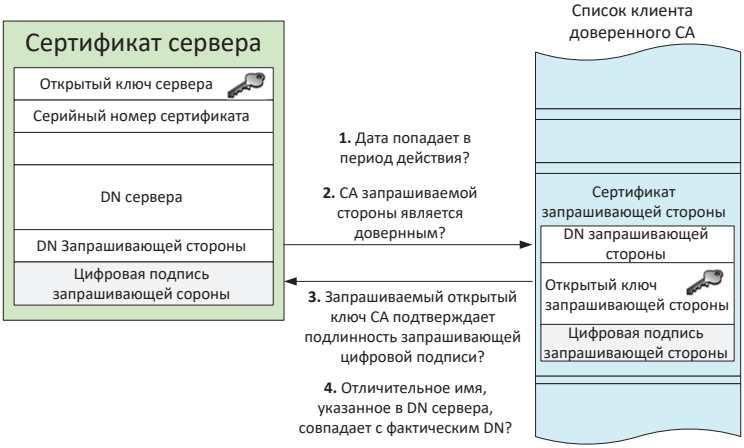


Рис. 13.6. Аутентификация сервером сертификата клиента

13.2. Протокол конфиденциального обмена данными SSL

Протокол SSL спроектирован для обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера. Он предоставляет возможность аутентификации сервера и, опционально, клиента. SSL требует применения надежного транспортного протокола (например, TCP).

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д.

могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт данных.

Все протокольные прикладные данные в SSL передаются зашифрованными с гарантией конфиденциальности.

Протокол SSL предоставляет «безопасный канал», который имеет три основные свойства.

- *Канал является частным.* Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.
- *Канал аутентифицирован.* Серверная сторона диалога всегда аутентифицируется, в то время как клиентская – аутентифицируется опционально.
- *Канал надежен.* Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC – Message Authentication Code).

Сеанс SSL между клиентом и сервером устанавливается следующим образом.

1) Клиент открывает сокет и запрашивает подключение к серверу.
2) Сервер аутентифицирует клиента (либо по паролю, либо посредством сертификата, отправляемого клиентом).
3) После установки соединения сервер передает браузеру свой открытый ключ посредством отправки сертификата сервера, выпущенного доверенным бюро сертификатов.
4) Клиент аутентифицирует сертификат.
5) Клиент и сервер осуществляют обмен настроечной информацией для определения типа и силы шифрования, используемых в сеансе соединения.
6) Клиент создает сеансовый ключ, используемый для шифрования данных.
7) Клиент шифрует сеансовый ключ с помощью открытого ключа сервера (полученного из сертификата сервера) и отправляет его серверу. Секретный ключ, с помощью которого можно расшифровать сеансовый ключ, находится только на сервере.
8) Сервер расшифровывает сеансовый ключ и использует его для создания безопасной сессии, через которую будет осуществляться обмен данными с клиентом.

В несколько упрощенном варианте диалог SSL представлен на рис. 13.7.

Необходимым условием успешной реализации этих шагов является заранее установленный на клиенте корневой сертификат, полученный от доверенного бюро сертификатов. При использовании сертификата, полученного от коммерческого CA, корневой сертификат которого уже имеется в браузере (например, Verisign), не нужно беспокоиться об этом. При ис-

пользовании сертификатов клиентов серверу необходимо установить клиентский корневой сертификат, выпущенный клиентским бюро сертификатов.

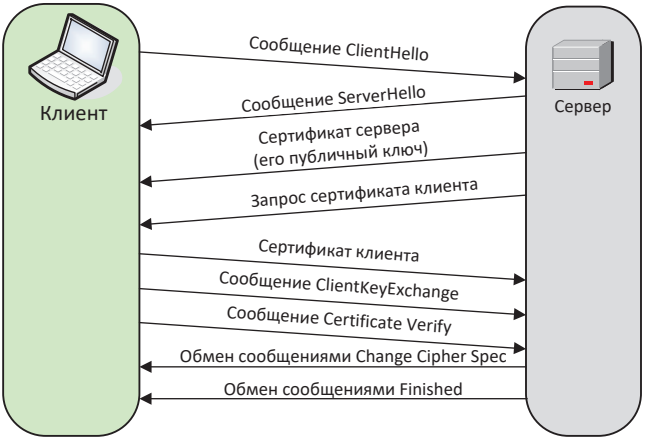


Рис. 13.7. Алгоритм работы SSL

Протокол диалога SSL имеет две основные фазы. Первая фаза используется для установления конфиденциального канала коммуникаций. Вторая служит для аутентификации клиента.

Фаза 1. Первая фаза является фазой инициализации соединения, когда оба партнера посылают сообщения HELLO. Клиент инициирует диалог посылкой сообщения CLIENT-HELLO. Сервер, получив это сообщение, обрабатывает его и откликается сообщением SERVER-HELLO.

К этому моменту, как клиент, так и сервер имеют достаточно информации, чтобы знать, нужен ли новый мастерный ключ. Когда новый мастерный ключ не нужен, клиент и сервер немедленно переходят в фазу 2.

Когда нужен новый мастерный ключ, сообщение SERVER-HELLO будет содержать достаточно данных, чтобы клиент мог сформировать такой ключ. Сюда входит:

- подписанный сертификат сервера;
- список базовых шифров (см. ниже);
- идентификатор соединения (последний представляет собой случайное число, сформированное сервером и используемое на протяжении сессии).

Клиент генерирует мастерный ключ и посылает сообщение CLIENT-MASTER-KEY (или сообщение ERROR, если информация сервера указывает, что клиент и сервер не могут согласовать базовый шифр).

Здесь следует заметить, что каждая оконечная точка SSL использует пару шифров для каждого соединения (т.е. всего 4 шифра). На каждой ко-

нечной точке, один шифр используется для исходящих коммуникаций и один – для входящих. Когда клиент или сервер генерирует ключ сессии, они в действительности формируют два ключа, SERVER-READ-KEY (известный также как CLIENT-WRITE-KEY) и SERVER-WRITE-KEY (известный также как CLIENT-READ-KEY). Мастерный ключ используется клиентом и сервером для генерации различных ключей сессий.

Наконец, после того как мастерный ключ определен, сервер посылает клиенту сообщение SERVER-VERIFY. Этот заключительный шаг аутентифицирует сервер, так как только сервер, который имеет соответствующий общедоступный ключ, может знать мастерный ключ.

Фаза 2. Вторая фаза является фазой аутентификации. Сервер уже аутентифицирован клиентом на первой фазе, по этой причине здесь осуществляется аутентификация клиента. При типичном сценарии серверу необходимо получить что-то от клиента, и он посылает запрос. Клиент пришлет позитивный отклик, если располагает необходимой информацией, или пришлет сообщение об ошибке, если нет. Эта спецификация протокола не определяет семантику сообщения ERROR, посылаемого в ответ на запрос сервера (например, конкретная реализация может игнорировать ошибку, закрыть соединение, и т.д. и, тем не менее, соответствовать этой спецификации). Когда один партнер выполнил аутентификацию другого партнера, он посылает сообщение FINISHED. В случае клиента сообщение CLIENT-FINISHED содержит зашифрованную форму идентификатора CONNECTION-ID, которую должен верифицировать сервер. Если верификация терпит неудачу, сервер посылает сообщение ERROR.

Раз партнер послал сообщение FINISHED он должен продолжить воспринимать сообщения до тех пор, пока не получит сообщение FINISHED от партнера. Как только оба партнера послали и получили сообщения FINISHED, протокол диалога SSL закончил свою работу. С этого момента начинает работать прикладной протокол.

13.3. Обеспечение безопасности беспроводных сетей

В беспроводных локальных сетях главным образом используется группа стандартов 802.11x (a, b, g и т. д.) технологии Wi-Fi. Эти стандарты позволяют соединять рабочие станции каналами с пропускной способностью до 54 Мбит/с с использованием беспроводной точки доступа, которая подключается к кабельной сети или напрямую к другой рабочей станции (см. рис. 13.8).

Так как беспроводные сети используют воздух и пространство для передачи и приема информации (сигналы являются открытыми для любого лица, находящегося в зоне действия), безопасность передачи данных является очень важным аспектом безопасности всей системы в целом. Без обеспечения должной защиты конфиденциальности и целостности информации при ее передаче между рабочими станциями и точками доступа

нельзя быть уверенным в том, что информация не будет перехвачена злоумышленником, и что рабочие станции и точки доступа не будут подменены посторонним лицом.

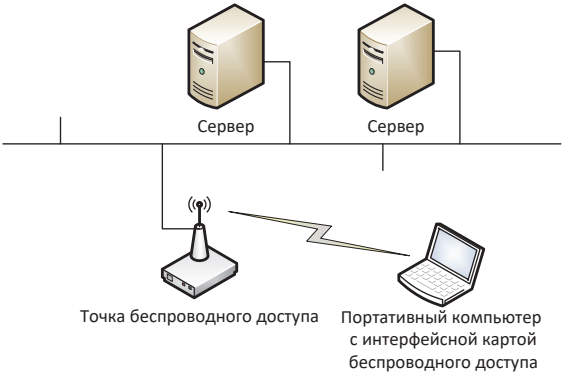


Рис. 13.8. Типичная архитектура беспроводной сети

13.3.1. Угрозы безопасности беспроводных соединений

13.3.1.1. Обнаружение беспроводных сетей

Обнаружить WLAN очень легко. Действительно, именно для этой цели был разработан ряд средств. Одной из таких утилит является NetStumber (http://www.netstumber.com/); она работает в операционных системах семейства Windows и может использоваться совместно со спутниковым навигатором (ресивером глобальной системы позиционирования, GPS) для обнаружения беспроводных сетей WLAN. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней WEP. Существуют и другие средства, идентифицирующие рабочие станции, подключенные к точке доступа, а также их MAC-адреса например, Kismet (http://www.kismetwireless.net/).

13.3.1.2. Прослушивание

Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Такой подход позволит подключиться к беспроводной сети организации, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним (см. рис. 13.9).

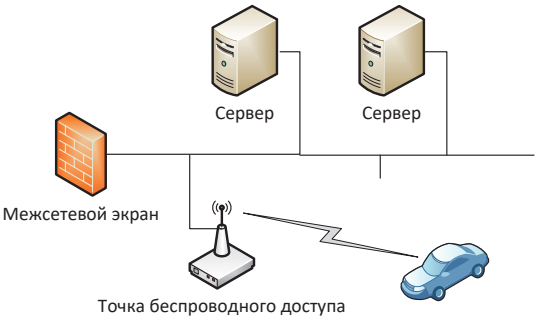


Рис. 13.9. Прослушивание сети WLAN

13.3.1.3. Активные атаки

Несмотря на то, что прослушивание сети представляет серьезную опасность, активные атаки могут быть еще более опасными. Основной риск, связанный с беспроводными сетями, состоит с том, что злоумышленник может успешно преодолеть периметр сетевой защиты организации. Не следует полагать, что атаки с использованием уязвимостей – это единственный способ злонамеренного воздействия злоумышленников. Если хакер прослушивает сеть, он может также перехватить пароли и пользовательские идентификаторы. Основные атаки, проводимые на WLAN, связанны с перехватом информации передаваемой по сети за счет низкой криптостойкости алгоритмов шифрования WEP.

13.3.2. Протокол WEP

Стандарт 802.11x определяет протокол Wired Equivalent Privacy (WEP) для защиты информации при ее передаче через WLAN.

WEP предусматривает обеспечение трех основных аспектов, обеспечивающих безопасность.

- *Аутентификация.* Служба аутентификации WEP используется для аутентификации рабочих станций на точках доступа. В аутентификации открытых систем рабочая станция рассматривается как аутентифицированная, если она отправляет ответный пакет с MAC-адресом в процессе начального обмена данными с точкой доступа. В реальных условиях данная форма аутентификации не обеспечивает доказательства того, что к точке доступа подключается именно конкретная рабочая станция, а не какой-либо другой компьютер.
- *Конфиденциальность.* Механизм обеспечения конфиденциальности базируется на RC4. RC4 – это стандартный мощный алгоритм шифрования, поэтому атаковать его достаточно сложно. WEP

определяет систему на базе RC4, обеспечивающую управление ключами, и другие дополнительные службы, необходимые для функционирования алгоритма. WEP поддерживает ключи длиной 40 бит и 128 бит (непосредственный ключ комбинируется с вектором инициализации алгоритма). К сожалению, WEP не определяет механизм управления ключами. Это означает, что многие инсталляции WEP базируются на использовании статических ключей. Действительно, часто на всех рабочих станциях сети используются одни и те же ключи.

- *Целостность.* Спецификация протокола WEP включает контроль целостности для каждого пакета. Используемая проверка целостности представляет собой циклическую 32-битную проверку избыточности (CRC). CRC вычисляется для каждого пакета перед его шифрованием, после чего данные в комбинации с CRC шифруются и отправляются в пункт назначения. Несмотря на то что CRC с криптографической точки зрения небезопасна, она защищается шифрованием. Используемая здесь система шифрования может быть достаточно надежной, если алгоритм шифрования обладает достаточной мощностью. Однако недостатки WEP представляют угрозу и для целостности пакетов.

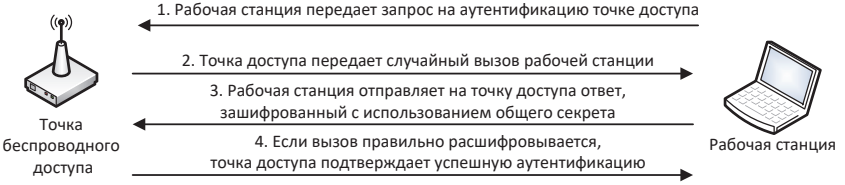


Рис. 13.10. Аутентификационный обмен WEP

Протокол WEP предусматривает использование службы аутентификации. К сожалению, эта служба осуществляет только аутентификацию рабочей станции относительно точки доступа. Она не обеспечивает взаимную аутентификацию, поэтому рабочая станция не получает доказательства того, что точка доступа действительно является авторизованной точкой доступа к сети. Таким образом, использование WEP не предотвращает перехват данных или атаки через посредника (см. рис. 13.11).

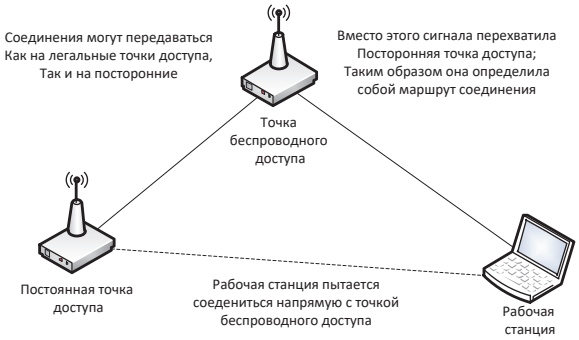


Рис. 18.11. Атака на WEP через посредника

13.3.3. Протокол 802.1X – контроль доступа в сеть по портам

Протокол 802.1X разработан в качестве надстройки для всех протоколов контроля доступа 2 уровня, включая Ethernet и WLAN. Так как этот протокол был разработан в то время, когда создатели WLAN искали решения проблем, связанных с WEP, он пришелся как нельзя кстати.

Протокол предназначен для обеспечения обобщенного механизма аутентификации при доступе в сеть и предусматривает следующий набор элементов.

1) Аутентификатор. Сетевое устройство, осуществляющее поиск других объектов для аутентификации; для WLAN это может быть точка доступа.
2) Соискатель. Объект, которому требуется доступ. В случае с WLAN это может быть рабочая станция.
3) Сервер аутентификации. Источник служб аутентификации. 802.1X разрешает централизацию этой функции, поэтому данный сервер является, например, сервером RADIUS.
4) Сетевая точка доступа. Точка присоединения рабочей станции к сети. По сути, это порт на коммутаторе или концентраторе. В беспроводной технологии является связью между рабочей станции и точкой доступа.
5) Процесс доступа через порт (PAE). PAE – это процесс, выполняющий протоколы аутентификации. PAE есть как у аутентификатора, так и у соискателя.
6) Расширяемый протокол аутентификации (EAP). Протокол EAP (определен в стандарте RFC 2284) представляет собой протокол, используемый при обмене аутентификационными данными. Поверх EAP могут работать и другие протоколы аутентификации более высокого уровня.

Использование протокола 802.1x позволяет применить более надежный механизм аутентификации, нежели возможности, доступные в 802.11x. При использовании совместно с сервером RADIUS становится возможным централизованное управление пользователями.

13.4. Обеспечение безопасности электронной почты

13.4.1. Риски, связанные с использованием электронной почты

Электронная почта – технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе – сети Интернет). Электронная почта – один из наиболее широко используемых видов сервиса, как в корпоративных сетях, так и в Интернет. Она является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в бизнесе. Роль электронной почты становится очевидной, если рассмотреть функции, которые выполняет почта:

- обеспечивает внутренний и внешний информационный обмен;
- является компонентом системы документооборота;
- формирует транспортный протокол корпоративных приложений;
- является средством образования инфраструктуры электронной коммерции.

Благодаря выполнению этих функций электронная почта решает одну из важнейших на настоящий момент задач – формирует единое информационное пространство. В первую очередь это касается создания общей коммуникационной инфраструктуры, которая упрощает обмен информацией между отдельными людьми, подразделениями одной компании и различными организациями.

Электронная почта обладает рядом преимуществ по сравнению с обычными способами передачи сообщений (традиционная почта или факсимильная связь). К ним относятся следующие.

1) Оперативность и легкость использования.
2) Доступность практически в любом месте.
3) Универсальность форматов писем и вложений.
4) Дешевизна сервиса.
5) Надежность и скорость инфраструктуры доставки.
6) Использование для обработки электронной почты прикладного специального программного обеспечения.

Электронная почта обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные риски, связанные с ее использованием. К примеру, доступность электронной почты превращается в недостаток, когда пользователи начинают применять почту для рассылки спама, легкость в использовании и бесконтрольность приводит к

утечкам информации, возможность пересылки разных форматов документов – к распространению вирусов и т.д.

В конечном итоге любой из этих рисков может привести к серьезным последствиям для компании. Это и потеря эффективности работы, и снижение качества услуг информационных систем, и разглашение конфиденциальной информации. Недостаточное внимание к этой проблеме грозит значительными потерями в бизнесе, а в некоторых случаях, даже привлечением к юридической ответственности в связи с нарушением законодательства.

Компания подвергается этим рискам в силу ряда свойств электронной почты. Например, благодаря применению MIME-стандарта электронная почта может переносить большие объемы информации различных форматов данных в виде прикрепленных к сообщениям файлов. Такой возможностью сразу воспользовались злоумышленники.

Достоинство электронной почты превратилось в угрозу, поскольку электронная почта стала представлять собой практически идеальную среду для переноса различного рода «опасных» вложений, а именно компьютерных вирусов, вредоносных программ, «троянских» программ и т.п.

Если надлежащий контроль за использованием электронной почты не обеспечен, это может привести к чрезвычайно серьезным последствиям и даже нанести непоправимый ущерб. Избавиться от этого риска можно лишь путем блокировки писем с «опасными» вложениями, а также антивирусной проверки прикрепленных файлов. На практике же оптимальным средством может оказаться блокировка определенных типов файлов. Это, как правило, исполняемые файлы (exe, com, bat) и файлы, содержащие макросы и OLE-объекты (файлы, созданные в приложениях MS Office).

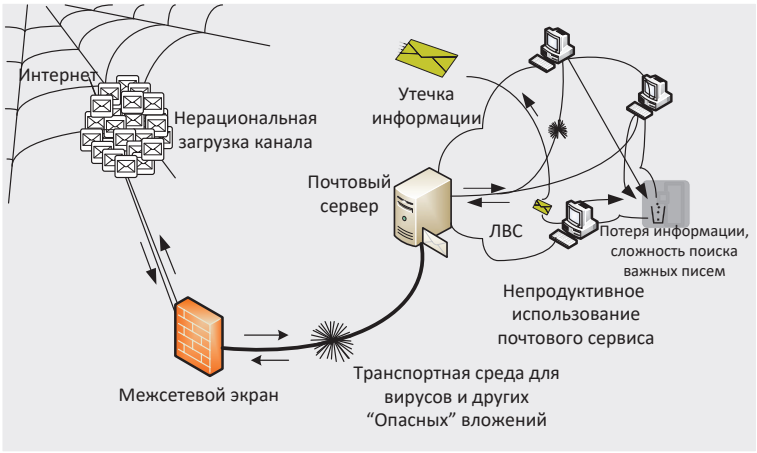


Рис. 13.12. Негативное воздействие различных факторов на незащищенную почтовую систему

Серьезную опасность для корпоративной сети представляют различного рода атаки с целью «засорения» почтовой системы. Это, в первую очередь, пересылка в качестве вложений в сообщениях электронной почты файлов больших объемов или многократно заархивированных файлов. «Открытие» таких файлов или попытка «развернуть» архив может привести к «зависанию» системы. При этом одинаково опасны как умышленные атаки этого типа, например, «отказ в обслуживании» (Denial of Service) и «почтовые бомбы» (mail-bombs), так и «неумышленные», когда пользователи отправляют электронные письма с вложениями большого объема, просто не подумав о том, к каким последствиям может привести открытие подобного файла на компьютере адресата.

Действенный способ избавиться от «засорения» почтовой системы и ее перегрузки – фильтрация по объему передаваемых данных, по количеству вложений в сообщения электронной почты и глубине вложенности архивированных файлов.

Другой особенностью электронной почты является ее доступность и простота в использовании. Во многом результатом этого стало широкое и повсеместное применение этого вида сервиса Интернет. Стихийность развития и отсутствие единых правил функционирования почтового сервиса привели к неконтролируемому использованию электронной почты, а в связи с этим, и к возникновению целого ряда рисков, связанных с неуправляемой циркуляцией электронной почты в сети.

Отсутствие контроля над почтовым потоком, как правило, становится причиной того, что сотрудники компании используют электронную почту в целях, не связанных с деятельностью компании (например, для обмена видео-файлами и графикой, частной переписки, ведения собственного бизнеса с использованием почтовых ресурсов компании, рассылки резюме в различные организации и т.п.).

Кроме того, к такому же результату может привести непродуктивное использование почтовых ресурсов в трудовой деятельности сотрудников (например, чрезмерное увлечение почтовой перепиской в случаях, когда необходимости в такой переписке нет, использование электронной почты не по назначению и т.п.). Причиной этого, как правило, является отсутствие в компании правил, регламентирующих использование системы электронной почты. Последствиями непродуктивного использования почтового сервиса являются снижение производительности труда в компании, а также излишние финансовые затраты. Сэкономить средства в значительной степени поможет проведение анализа эффективности использования системы электронной почты, который основывается на базе статистических данных о функционировании системы. Подобную статистику возможно получить лишь в случае ведения архива электронной почты. Обработка информации, содержащейся в архиве, позволяет получать отчеты о различных параметрах электронной почты, ее объемах и структуре, представить наглядную картину использования почтового трафика сотрудниками компании, а это, в свою очередь, поможет предотвратить использова-

ние электронной почты, несвязанное с деятельностью компании, и повысить эффективность работы корпоративной почтовой системы.

Передача в электронных письмах графических, видео и звуковых файлов, которые, как правило, имеют большой объем даже если такая передача предусмотрена условиями ведения бизнеса, приводит к значительной перегрузке сети, соответственно к дополнительным финансовым затратам на ее обслуживание. Избежать этого, а значит и добиться значительной экономии средств компании, поможет, так называемая, отложенная доставка писем, которая позволяет доставлять сообщения больших объемов в то время, когда загрузка сети не имеет критического значения (например, в ночное время, в выходные дни и т.п.).

К «засорению» трафика также ведет рассылка спама. Как правило, это письма, содержащие навязчивые предложения самых разнообразных услуг, товаров и т.п. Такого рода почта является «группой риска» с точки зрения переноса вирусов. Большое количество ненужной почты загружает каналы, «замусоривает» почтовые ящики, отнимает время на удаление ненужных писем и повышает вероятность случайного удаления нужных. Конечно рассылка, например, сообщений рекламного характера, напрямую не преследует цели «засорить» почтовую систему организации, однако косвенно приводит к негативным последствиям. Использование списков рассылки, в которую могут входить все пользователи одной корпоративной сети, и получение одновременно всеми этими пользователями сообщений рекламного характера грозит компании снижением производительности ее сетевых ресурсов. Блокировка спама, в первую очередь, связана с контекстным анализом сообщений, то есть проверкой электронной почты на наличие ключевых слов и выражений, которые обычно употребляются в сообщениях рекламного характера.

Переписка с внешними корреспондентами представляет наибольшую угрозу из-за особенностей электронной почты (невозможность контролировать маршрут передачи писем, а также их копирование и перенаправление, осуществлять аутентификацию отправителя/получателя, возвращать письма после их отправления). Кроме того, невозможен либо затруднен контроль количества отправляемых копий письма. Содержимое сообщения может быть прочитано в процессе передачи его по Интернету, поскольку заголовки и содержимое электронных писем часто передаются в открытом виде.

Другой проблемой, связанной с особенностями электронной почты, является то, что электронная почта позволяет неконтролируемое накопление информации в архивах и практически неуничтожима. В противоположность бытующему мнению, удалить электронную почту непросто. Резервные копии сообщений могут оставаться на персональных компьютерах отправителя и получателя или в сети компаний, где они работают. Если электронное почтовое сообщение отправлено через коммерческую службу или через Интернет, то оно будет передаваться через несколько различных серверов. Каждый сервер в цепочке между отправителем и получателем

может сохранить копию сообщения в своих архивах. Даже методичное выяснение местонахождения каждой копии электронного письма с последующим его удалением не дает никакой гарантии того, что сообщение не осталось на жестком диске компьютера или сервера.

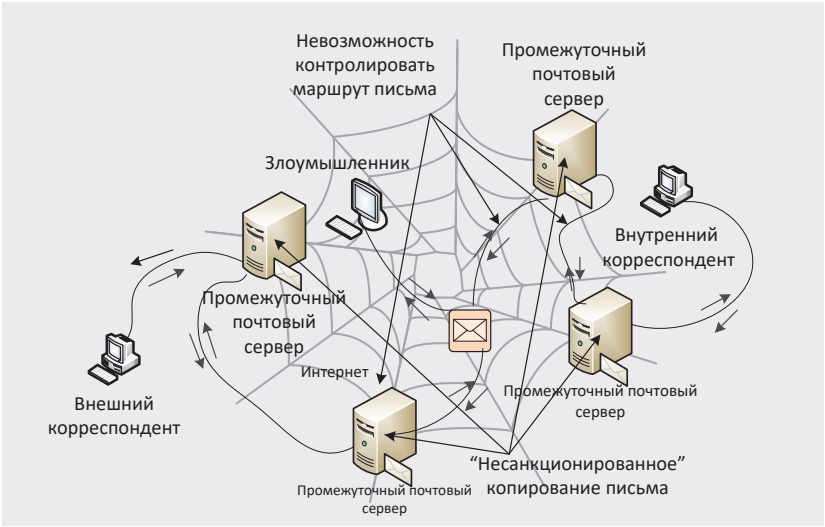


Рис. 13.13. Проблемы, возникающие при пересылке электронной почты через Интернет

Все эти особенности, а также простота копирования электронного сообщения и невозможность проконтролировать данную операцию приводят к тому, что сотрудник может передать корпоративную информацию любому количеству людей как внутри, так и за пределами компании анонимно и без соответствующего разрешения, сразу или по истечении какого-либо времени. При этом, такая информация может представлять собой служебную информацию компании это грозит серьезным нарушением конфиденциальности и может привести к неприятным для компании последствиям.

Чтобы обеспечить защиту от утечки конфиденциальной информации из сети, необходимо осуществлять контроль адресатов, фильтрацию передаваемых данных на наличие в текстах сообщений или в прикрепленных к электронному письму файлах слов и выражений, имеющих отношение к «закрытой» тематике, осуществлять разграничение доступа различных категорий пользователей к архивам электронной почты и т.п.

Одно из основных отличий электронной почты состоит в формальном к ней отношении (по сравнению с другими видами коммерческих коммуникаций):

– во-первых, большинство пользователей относятся к электронной почте как к чему-то временному, то есть поступают с ней по принципу «прочитал и выкинул». При таком отношении существует риск случайного удаления значимой информации. Кроме того, существует опасность потери переписки с важным клиентом. Все эти проблемы решаются путем создания в организации архива электронной почты;
– во-вторых, такое отношение к электронной почте приводит к тому, что из-за кажущейся недолговечности электронных сообщений люди часто используют их для того, чтобы выразить чувства и мнения в выражениях, которые они никогда не позволили бы себе употребить в традиционных письмах. Публикация таких писем в сети может нанести серьезный ущерб репутации компании или явиться причиной юридических исков к ней.

Еще одна область связана с возможностью привлечения к юридической ответственности компании и ее сотрудников – за нарушение авторского права. Защищенные этим правом материалы могут содержаться или в сообщении электронной почты, или в присоединенных файлах. К подобным материалам относятся графическая, аудио, видео и различная текстовая информация, т. е. любая информация, которая может быть представлена в электронном виде и передана по компьютерным сетям. Копирование или распространение этих материалов без предварительного согласия автора или владельца авторских прав является нарушением закона. Если компания допускает, чтобы материалы почты, защищенные авторским правом, использовались сотрудниками, не имеющими на это полномочий, то она может быть привлечена к ответственности за прямое или косвенное пособничество нарушению авторского права.

13.4.2. Средства обеспечения безопасности электронной почты

Учитывая описанные выше риски, связанные с использованием электронной почты, организациям необходимо принять соответствующие меры для защиты от них.

Подход к защите должен быть всесторонним и комплексным – необходимо сочетать организационные меры с использованием соответствующих технических средств.

К организационным мерам относятся разработка и внедрение в компании политики использования электронной почты. Технические средства должны обеспечить выполнение этой политики как за счет мониторинга почтового трафика, так и за счет адекватного реагирования на нарушения.

Очень важно отметить, что политика использования электронной почты первична по отношению к средствам ее реализации, поскольку составляет основу для формирования комплекса мер по защите информационной системы от вышеперечисленных рисков. Сначала необходимо

сформулировать политику, составить правила использования электронной почты, определить, как созданная система должна реагировать на определенные нарушения политики и только затем переводить правила на компьютерный язык того средства, которое используется для контроля выполнения положений политики использования электронной почты.

К таким техническим средствам относится специальное программное обеспечение, называемое система контроля содержимого электронной почты (content security software). В функции таких систем входит контроль почтового трафика и ведение архива переписки по электронной почте. К таким системам предъявляются следующие требования:

- проведение текстового анализа;
- фильтрация передаваемых данных:
  - по размеру и объему данных;
  - по количеству вложений в сообщения электронной почты;
  - по типу файлов (вложенных в электронную почту);
  - по адресу электронной почты;
- контроль использования почтовых ресурсов и разграничение доступа к ним различных категорий пользователей;
- отложенную доставку сообщений электронной почты по расписанию;
- ведение полнофункционального архива электронной почты.

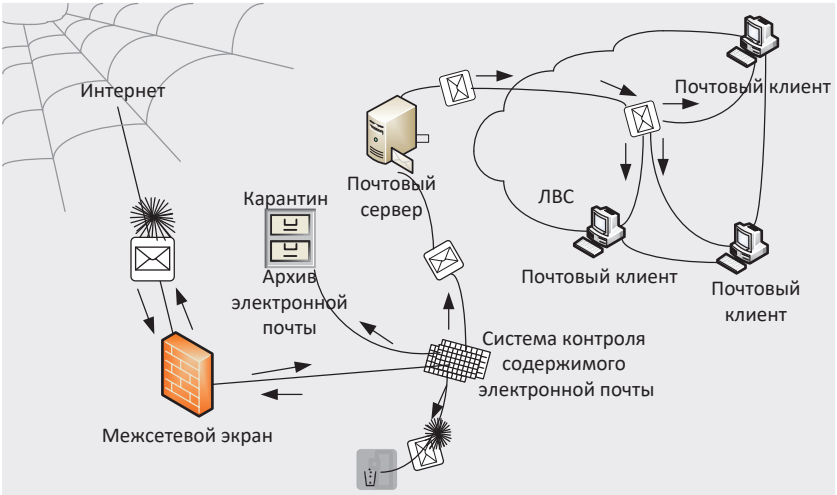


Рис. 13.14. Решение проблем защиты почтовой системы

Выполнение этих требований обеспечивается применением в средствах защиты определенных механизмов. К таким механизмам могут относиться:

- рекурсивная декомпозиция (специальный алгоритм, применяемый для разбора сообщений электронной почты на составляющие компоненты с последующим анализом их содержимого);
- эвристическое определение кодировок текстов;
- определение типа файлов по сигнатуре;
- полнотекстовый поиск по архиву электронной почты и т.п.

13.4.3. Политика использования электронной почты

Средство защиты – система контроля содержимого электронной почты, само по себе никаких задач по обеспечению безопасности не решает. Это всего лишь «машина», которая помогает человеку в решении этой проблемы. Поэтому задачу по обеспечению безопасности необходимо такой «машине» поставить. Это означает, что должен быть выработан специальный набор правил, который в дальнейшем будет переведен на язык машины. Этот набор правил называется «*политикой использования электронной почты*».

Во многих организациях такие правила существуют уже длительное время. Как и всякая ограничительная мера, они создают определенные неудобства пользователям системы, а если пользователю что-то неудобно, он либо перестает этим пользоваться, либо старается обойти препятствия. Поэтому такого рода политики, не подкрепленные техническими средствами контроля за их выполнением, постепенно теряют силу. Программные системы, ориентированные на фильтрацию почты, следует позиционировать именно как инструмент для внедрения и контроля исполнения этих правил.

Таким образом, *политика использования электронной почты* – это закрепленные в письменном виде и доведенные до сотрудников инструкции и другие документы, которые регламентируют их деятельность и процессы, связанные с использованием системы электронной почты. Эти документы и инструкции обладают юридическим статусом и, как правило, предоставляются для ознакомления сотрудникам организации.

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности и неотделима от нее.

Политика должна соответствовать следующим критериям:

- быть лаконично изложенной и понятной всем сотрудникам компании, простота написания не должна привести к потере юридического статуса документа;
- исходить из необходимости защиты информации в процессе экономической деятельности компании;

– быть согласованной с другими организационными политиками компании (регламентирующими финансовую, экономическую, юридическую и другие сферы деятельности компании);
– иметь законную силу, т.е. политика, как документ, должна быть одобрена и подписана всеми должностными лицами руководящего звена компании, а ее выполнение должно быть детально продумано;
– не противоречить федеральным и местным законам;
– определять меры воздействия на сотрудников, нарушивших положения этой политики;
– соблюдать баланс между степенью защищенности информации и продуктивностью деятельности компании;
– детально определять мероприятия по обеспечению политики использования электронной почты в компании.

Политика использования электронной почты, как правило, рассматривается с двух сторон – как официально оформленный юридический документ и как материал, который описывает технику реализации политики.

Как документ политика должна включать:
– положение, что электронная почта является собственностью компании и может быть использована только в рабочих целях;
– указание на то, что применение корпоративной системы электронной почты не должно противоречить законодательству РФ и положениям политики безопасности;
– инструкции и рекомендации по использованию и хранению электронной почты;
– предупреждение о потенциальной ответственности сотрудников компании за злоупотребления при использовании электронной почты в личных целях и возможном использовании электронной почты в судебных и служебных разбирательствах;
– письменное подтверждение того, что сотрудники компании ознакомлены с политикой использования электронной почты и согласны с ее положениями.

С технической точки зрения политика устанавливает правила использования электронной почты, то есть определяет следующее.

Что контролируется	Прохождение каких сообщений входящей, исходящей или внутренней электронной почты должно быть разрешено или запрещено.
На кого распространяется	Категории лиц, которым разрешено или запрещено отправлять исходящие или получать входящие сообщения электронной почты.
Как реагирует система	Что необходимо делать с теми или иными сообщениями электронной почты, которые удовлетворяют или не удовлетворяют критериям, определенным правилами использования электронной почты.

13.4.4. Системы контроля содержимого электронной почты

Внедрение политики использования электронной почты требует от руководства компании понимания, что наличие только документально оформленной политики не гарантирует ее выполнения. Необходимо создание в компании соответствующих условий реализации этой политики. При этом важнейшим условием является наличие в корпоративной сети программно-технических средств контроля выполнения положений и требований политики. К таким средствам относятся системы контроля содержимого электронной почты.

Системы контроля содержимого электронной почты – это ПО, способное анализировать содержание письма по различным компонентам и структуре в целях реализации политики использования электронной почты.

К особенностям такого ПО относится:

- применение при анализе содержания специально разработанной политики использования электронных писем;
- способность осуществлять «рекурсивную декомпозицию» электронных писем;
- возможность распознавания реальных форматов файлов вне зависимости от различных способов их маскировки (искажение расширения файлов, архивирование файлов и т.п.);
- анализ множества параметров сообщения электронной почты;
- ведение архива электронной почты;
- анализ содержимого сообщения электронной почты и прикрепленных файлов на наличие запрещенных к использованию слов и выражений.

Системы контроля электронной почты помимо основной своей задачи мониторинга почтового трафика способны выполнять и другие функции. Практика показала, что в настоящее время такие системы используются в качестве:

- средств управления почтовым потоком;
- средств управления доступом;
- средств администрирования и хранения электронной почты;
- средств аудита контента (важнейшую функцию которого осуществляет архив электронной почты);
- основы системы документооборота.

13.4.5. Требования к системам контроля содержимого электронной почты

Спектр возможностей всех категорий систем контроля содержимого электронной почты достаточно широк и существенно меняется в зависимости от производителя. Однако ко всем системам предъявляются наибо-

лее общие требования, которые позволяют решать задачи, связанные с контролем почтового трафика.

Основные требования, предъявляемые к таким системам – полнота и адекватность.

1. *Полнота* – это способность систем контроля обеспечить наиболее глубокую проверку сообщений электронной почты. Это предполагает, что фильтрация должна производиться по всем компонентам письма. При этом ни один из объектов, входящих в структуру электронного сообщения, не должен быть «оставлен без внимания». Условия проверки писем должны учитывать все проблемы, риски и угрозы, которые могут существовать в организации, использующей систему электронной почты.

2. *Адекватность* – это способность систем контроля содержимого как можно более полно воплощать словесно сформулированную политику использования электронной почты, иметь все необходимые средства реализации написанных людьми правил в понятные системе условия фильтрации.

К другим наиболее общим требованиям относятся следующее.

3. *Текстовый анализ электронной почты* – анализ ключевых слов и выражений с помощью встроенных словарей. Данная возможность позволяет обнаружить и своевременно предотвратить утечку конфиденциальной информации, установить наличие запрещенного содержания, остановить рассылку спама, а также передачу других материалов, запрещенных политикой безопасности. При этом качественный анализ текста должен предполагать морфологический анализ слов, то есть система должна иметь возможность генерировать и определять всевозможные грамматические конструкции слова. Эта функция приобретает большое значение в связи с особенностями русского языка, в котором слова имеют сложные грамматические конструкции.

4. *Контроль отправителей и получателей сообщений электронной почты.* Данная возможность позволяет фильтровать почтовый трафик, тем самым реализуя некоторые функции межсетевого экрана в почтовой системе.

5. *Разбор электронных писем на составляющие их компоненты* (MIME-заголовки, тело письма, прикрепленные файлы и т.п.), устранение «опасных» вложений и последующий сбор компонентов письма воедино, причем с возможностью добавлять к сообщению электронной почты необходимые для администраторов безопасности элементы (например, предупреждения о наличии вирусов или «запрещенного» текста в содержании письма).

6. *Блокировка или задержка сообщений большого размера* до того момента, когда канал связи будет менее всего загружен (например, в нерабочее время). Циркуляция в почтовой сети компании таких сообщений может привести к перегрузке сети, а блокировка или отложенная доставка позволит этого избежать.

7. *Распознавание графических, видео и звуковых файлов.* Как правило, такие файлы имеют большой размер, и их циркуляция может привести к потере производительности сетевых ресурсов. Поэтому способность распознавать и задерживать эти типы файлов позволяет предотвратить снижение эффективности работы компании.

8. *Обработка сжатых/архивных файлов.* Это дает возможность проверять сжатые файлы на содержание в них запрещенных материалов.

9. *Распознавание исполняемых файлов.* Как правило, такие файлы имеют большой размер и редко имеют отношение к коммерческой деятельности компании. Кроме того, исполняемые файлы являются основным источником заражения вирусами, передаваемыми с электронной почтой. Поэтому способность распознавать и задерживать эти типы файлов позволяет предотвратить снижение эффективности работы компании и избежать заражения системы.

10. *Контроль и блокирование спама.* Циркуляция спама приводит к перегрузке сети и потере рабочего времени сотрудников. Функция контроля и блокирования спама позволяет сберечь сетевые ресурсы и предотвратить снижение эффективности работы компании. Основными способами защиты от спама являются: проверка имен доменов и IP-адресов источников рассылки спама по спискам, запрос на указанный адрес отправителя (блокировка в случае отсутствия ответа), текстовый анализ спам-сообщения на наличие характерных слов и выражений в заголовках электронной почты (from/subject), проверка заголовков на соответствие спецификации RFC-822 и т.п.

11. *Способность определять число вложений в сообщениях электронной почты.* Пересылка электронного письма с большим количеством вложений может привести к перегрузке сети, поэтому контроль за соблюдением определенных политикой информационной безопасности ограничений на количество вложений обеспечивает сохранение ресурсов корпоративной сети.

12. *Контроль и блокирование программ-закладок* (cookies), вредоносного мобильного кода (Java, ActiveX, JavaScript, VBScript и т.д.), а также файлов, осуществляющих автоматическую рассылку (так называемые «Automatic Mail-to»). Эти виды вложений являются крайне опасными и приводят к утечке информации из корпоративной сети.

13. *Категоризация ресурсов почтовой системы* («административный», «отдел кадров», «финансы» и т.д.) и разграничение доступа сотрудников компании к различным категориям ресурсов сети (в т.ч. и в зависимости от времени суток).

14. *Реализация различных вариантов реагирования*, в том числе: удаление или временная блокировка сообщения; задержка сообщения и помещение его в карантин для последующего анализа; «лечение» зараженного вирусом файла; уведомление администратора безопасности или любого другого адресата о нарушении политики безопасности и т.п.

15. *Возможность модификации данных*, которая предусматривает, например, удаление неприемлемых вложений и замену их на тексты заданного содержания. Такая возможность позволит администратору удалять из писем прикрепленные файлы, тип которых запрещен политикой безопасности компании. К таким типам могут относиться исполняемые, видео и звуковые файлы, не имеющие отношения к деятельности компании. А это, в конечном итоге, позволит избежать заражения сети вирусами и добиться от сотрудников продуктивного использования почтового сервиса.

16. *Ведение полнофункционального архива электронной почты*, способного обеспечить хранение в режиме on-line большого количества электронной почты с высоким уровнем доступности данных. На основании хранящейся в архиве информации, возможно проводить дальнейший анализ почтового потока компании, корректировать работу системы, осуществлять анализ инцидентов, связанный с злоупотреблением сотрудниками компании почтовым сервисом и т.п.

На рис. 13.15 представлена последовательность работы типичной системы контроля содержимого электронной почты. Схема обработки сообщения, как правило, включает в себя следующие этапы: рекурсивная декомпозиция электронного письма; анализ содержимого электронного письма; «категоризация» электронного письма (отнесение к определенной категории); действие над письмом по результатам присвоения категории.

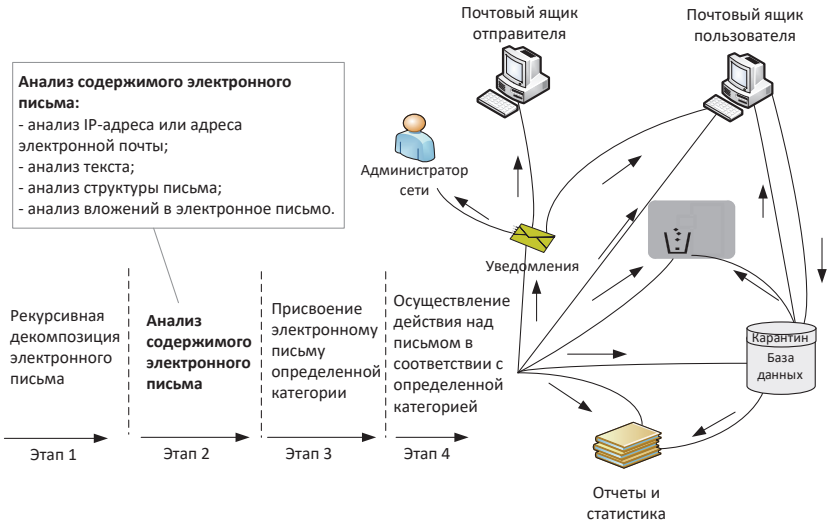


Рис. 13.15. Схема обработки сообщения системой контроля содержимого электронной почты

13.4.6. Принципы функционирования систем контроля содержимого электронной почты

Каждое попадающее в систему электронное письмо должно проверяться на соответствие заданным условиям. При этом, по меньшей мере, должны выполняться следующие условия отбора писем:

- условия на почтовые заголовки;
- условия на структуру письма (наличие, количество и структура вложений);
- условия на типы вложений (MS Office, исполняемые файлы, архивы и т.п.);
- условия на содержимое (текст) писем и вложений;
- условия на результат обработки письма.

Кроме того, система должна позволять анализировать почтовые сообщения по всем их составляющим: атрибутам конверта, заголовкам сообщения, MIME-заголовкам, телу сообщения, присоединенным файлам.

13.4.6.1. Категоризация писем и фильтрация спама

Рассмотрим вопрос категоризации писем. Важно отметить, что гибкость при фильтрации почтовых сообщений особенно необходима, когда это касается такой проблемы, как спам. Одним из главных критериев выбора системы контроля содержимого электронной почты в настоящее время является как раз ее способность как можно более качественно справляться с этой проблемой.

Существует четыре основные методики определения, какое письмо относится к спаму, а какое нет.

1) Выявление спама по наличию в письме определенных признаков, таких как наличие ключевых слов или словосочетаний, характерное написание темы письма (например, все заглавные буквы и большое количество восклицательных знаков), а также специфическая адресная информация.

2) Определение адреса отправителя и его принадлежности к, так называемым, «черным спискам» почтовых серверов Open Relay Black List (ORBL). В эти списки заносятся те серверы, которые замечены в массовых рассылках спама, и идея состоит в том, чтобы вообще не принимать и не транслировать почту, исходящую с этих серверов.

3) Совместное использование методик по фильтрации по определенным признакам и проверкой «черного списка». По продуктивности мало чем отличается от двух первых. Результаты тестирования хорошо настроенного фильтра с применением обеих методик показывают, что из 100% спам-сообщений обнаруживается только 79,7%. При этом был выявлен значительный процент ложных срабатываний, а это значит, что к спаму были отнесены обычные письма (1,2% от задержанных писем), а это грозит для компании потерей важной информации. Некачественное разделение спама и обычных писем обусловлено, в том числе и некоторой «однобокостью» стандартных фильтров. При отбраковке писем учитываются «пло-

хие» признаки и не учитываются «хорошие», характерные для полезной переписки.

4) автоматическая настройка фильтров согласно особенностям индивидуальной переписки, а при обработке учет признаков как «плохих», так и «хороших» фильтров. Эта четвертая методика, предложенная американским программистом и предпринимателем П. Грэмом. Методика основывается на теории вероятностей и использует для фильтрации спама статистический алгоритм Байеса. По имеющимся оценкам, этот метод борьбы со спамом является весьма эффективным. Так, в процессе испытания через фильтр были пропущены 8000 писем, половина из которых являлась спамом. В результате система не смогла распознать лишь 0,5% спам-сообщений, а количество ошибочных срабатываний фильтра оказалось нулевым.

Требование полного разбора письма при решении задачи категоризации следует дополнить требованием устойчивости.

- Во-первых, система должна быть устойчивой по отношению к обработке писем с некорректной структурой. Структура письма подчиняется определенным правилам. Разбор письма на составляющие основан на применении этих правил к конкретному письму. Возможны случаи, когда почтовая программа автора письма формирует письмо с нарушением этих правил. В этом случае письмо не может быть корректно разобрано.
- Во-вторых, система должна надежно определять типы файлов-вложений. Под «надежностью» имеется в виду определение, не основанное на имени файла, а также на информации, вписываемой в письмо почтовым клиентом при прикреплении файла (mime-type). Такая информация может быть недостоверна либо в результате сознательных попыток обмануть систему контроля, либо в результате неправильных настроек почтовой программы отправителя. Бессмысленно запрещать пересылку файлов типа JPEG, если файл picture.jpg после переименования в page.txt пройдет незамеченным.
- В-третьих, система должна обеспечивать полноту проводимых проверок, то есть высокое количество и разнообразие критериев анализа электронной почты. При этом система должна осуществлять фильтрацию по любым атрибутам сообщений, по объему сообщений и вложенных файлов, по количеству и типу вложений, по глубине вложенности, а также уметь анализировать содержимое прикрепленных файлов вне зависимости от того, являются ли эти файлы сжатыми или архивными. Существенным преимуществом многих продуктов является возможность создания собственного сценария обработки сообщений электронной почты.

При анализе текста нужно иметь возможность работать с нормализованными словоформами и т.д.

13.4.6.2. Реализация политики использования

Рассмотрим не отдельные правила, а все множество правил, составляющих политику. Любая реалистичная политика состоит из целого множества правил, которые, естественно, объединяются в группы. Очевидно, что правила для исходящей почты отличаются от правил для входящей, правила для руководства компании – от правил для рядовых сотрудников и т.д. Более того, поскольку правила применяются к письму в определенной последовательности, хотелось бы, чтобы эта последовательность была логичной и могла зависеть от результатов анализа письма. Все это вместе приводит к требованию «прозрачности»: правила, заданные в системе, должны «читаться» как правила, написанные на естественном языке, понятном человеку.

Все сказанное выше относилось к анализу письма. Однако сам по себе анализ ничего не дает. По его результатам письмо должно быть отнесено к какой-нибудь категории (безопасное, важное, неразрешенное и т.п.). Если такая категоризация проведена, то можно говорить о каких-либо действиях по отношению к проанализированному письму, например, доставить его адресату, заблокировать, и т.д. Другими словами, необходима возможность задавать системе правила, по которым она обрабатывает письма.

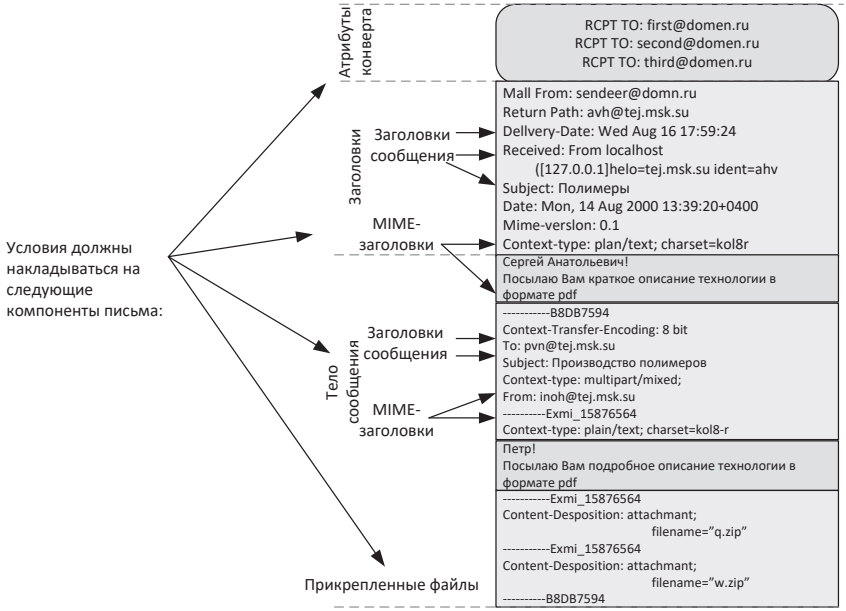


Рис. 13.16. Фильтрация по всем компонентам письма

Любое правило можно представить себе, как связку «условие + действие». Какие же действия нужны для того, чтобы обеспечить реализацию разумной политики?

Само по себе отнесение письма к определенной категории уже может рассматриваться как неявное действие. На этом действии следует остановиться подробнее. Дело в том, что жесткая категоризация как основа для принятия решений по электронному письму оказывается весьма непрактичной. Действительно, пусть мы выделили категорию писем «письмо, отправленное на запрещенный адрес» для того, чтобы блокировать доставку. С другой стороны, у нас может быть категория «письма руководства компании», которые надо отправлять безусловно. Что делать с письмом президента, отправленным по «запрещенному» адресу? Здравый смысл подсказывает, что приоритет должен быть отдан категории «письма руководства компании», что, безусловно, и будет сделано в системе с жесткой категоризацией. Однако будет потеряна существенная информация о письме. Разумный выход из таких ситуаций заключается в возможности относить письма сразу к нескольким категориям. Такая «свободная категоризация» позволит системе гибко реагировать на самые различные комбинации данных, содержащихся в письмах.

На рис. 13.17 показана схема действий, поддерживаемых правилами фильтрации почтовых сообщений типичной системы контроля содержимого электронной почты.

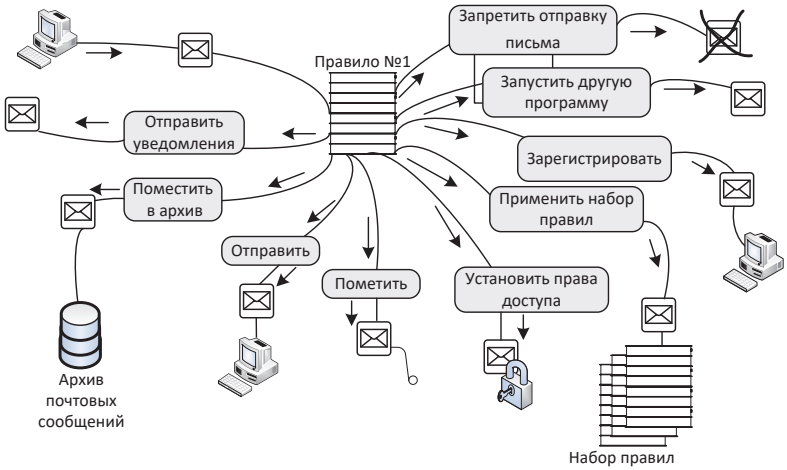


Рис. 13.17. Схема реагирования типичной системы контроля содержимого электронной почты

13.4.6.3. Долговременное хранение и архивирование

В последнее время большое значение для обеспечения безопасности информационных систем приобрело наличие в компании архива почтовых сообщений. Некоторые разработчики систем контекстного анализа предусматривают прикрепление к своим продуктам специальных модулей архивирования. Именно наличие архива электронной почты и определяет в настоящее время полнофункциональность продуктов этой категории. При этом ведение архива – это не просто автоматическая архивация почтовых сообщений в файл, а способность регистрации сообщений и учета необходимой информации на протяжении всего жизненного цикла сообщения, возможность получения любых выборок и статистики из архива по запросам, созданным с использованием любых критериев.

Кроме того, долговременный архив предоставляет возможность ретроспективного анализа почтовых потоков и не только позволяет найти виновных в нарушении принятых в компании правил по прошествии определенного времени, но и дает материал для построения объективной и обоснованной политики использования электронной почты.

13.4.6.4. Контекстный контроль содержимого

Отличительным признаком средств контекстного анализа является способность накопления статистики и генерации отчетов. Многие продукты имеют в своем арсенале только встроенные формы отчетов, другие способны осуществлять только просмотр статистики работы конкретного пользователя системы электронной почты.

Одним из основных критериев оценки систем контекстного анализа для российского рынка является поддержка продуктом различных кодировок кириллицы (CP1251, CP866, ISO8859-5, KOI8-R, MAC), что дает возможность анализа русскоязычных текстов. Кроме того, «проклятие» множественных кодировок тяготеет над российскими информационными системами. Все осложняется тем, что разные части письма, включая почтовые заголовки, могут быть написаны в разных кодировках. Вдобавок эти кодировки не всегда указаны или не всегда указаны верно.

Рассмотрим вопрос, касающийся архитектуры систем контроля содержимого электронной почты. В подобных продуктах уникальной особенностью является открытая архитектура, которая позволяет разработчикам расширять функциональные возможности системы, интегрируя в нее дополнительные модули и не затрагивая ее ядра. Это дает возможность постоянно наращивать способности системы контроля содержимого по защите электронной почты и одновременно с этим экономить значительные средства, которые могут потребоваться на модернизацию всей системы.

Материал раздела 13 подготовлен за счет обобщения работ [52, 55-62].

Заключение

Проблема обеспечения информационной безопасности телекоммуникационных систем становится все более актуальной для российских компаний. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень. Многие из них уже не могут обеспечить защиту коммерческой информации собственными силами и вынуждены пользоваться услугами профильных профессиональных IT-консультантов. Особое значение имеет обеспечение информационной безопасности для критической инфраструктуры – ТКС специального и государственного назначения.

В течение многих лет компании отчаянно боролись с вирусными эпидемиями, обносили периметр межсетевыми экранами и системами предотвращения вторжений, внедряли мощные инструменты против неавторизованного доступа. Однако компании упустили из вида главную опасность. Отсутствие единой политики информационной безопасности, а также единой концепции построения профиля информационной защиты компании зачастую обесценивает многомиллионные затраты на программные и аппаратные комплексы ИБ. Еще пару лет назад ИТ-службы отвечали за защиту от внешних угроз, а с внутренними угрозами разбиралась служба безопасности. Сегодня она просто физически не может контролировать перемещение информации по электронным сетям и с помощью переносных носителей. Для этого нужны специально разработанные регламенты, ликбез сотрудников, специально подготовленные сотрудники безопасности и технические средства для выявления попыток несанкционированного доступа или перемещения информации. Все эти меры должны реализоваться специалистом ИБ в рамках единой концепции.

Бурное развитие ИТ технологий (ОС, ПО и ТКС), а также направления ИБ приводит к росту спроса на профессиональных специалистов в этой области. Это актуализирует получение образования в области ИБ и широкой востребованности полученных профильных знаний на рынке труда.

Хочется надеется, что представленное учебное пособие поможет будущим профессионалам в сфере ИТ получить тот общий набор знаний и умений в области ТКС и ИБ, чтобы оказаться востребованными и высокооплачиваемыми сотрудниками престижных компаний.

Список сокращений

2B1Q – 2 Binary 1 Quaternary – линейное кодирование в котором каждые два бита (2B) передаются за один такт (1) сигналом, имеющим четыре состояния (Q – Quadra)
2G – 2th Generation – 2-е поколение мобильной связи
3G – 3th Generation – 3-е поколение мобильной связи
4G – 4th Generation – 4-е поколение мобильной связи
5G – 5th Generation – 5-е поколение мобильной связи
ADSL – Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия
AODV – Ad hoc On-Demand Distance Vector – протокол динамической маршрутизации для мобильных ad-hoc сетей (MANET) и других беспроводных сетей
ARED – Adaptive Random Early Detection – адаптивное раннее обнаружение перегрузок в очередях
ARP – Address Resolution Protocol – протокол разрешения адресов
ARPANET – Advanced Research Projects Agency Network – глобальная сеть являющаяся праобразом сети Internet
ASON – Automatic Switched Optical Network – автоматически коммутируемая оптическая сеть
ASTN – Automatic Switched Transport Network – автоматически коммутируемая транспортная сеть
ATM – Asynchronous Transfer Mode – технология асинхронной передачи данных
BC – Business Critical – трафик, критичный к полосе пропускания
BE – Best Effort – трафик терпимый к потерям и задержкам / обслуживание трафика по принципу «наибольших усилий»
BGP – Border Gateway Protocol – протокол межсетевой маршрутизации
CA – Certificate Authority – бюро сертификатов
CAP – Carrierless Amplitude Modulation – амплитудная модуляция с подавлением несущей
CBWFQ – Class-Based Weighted Fair Queuing – взвешенное справедливое обслуживание в очереди на основе классов
CDMA – Code Division Multiple Access – множественный доступ с кодовым разделением – технология связи, при которой каналы передачи имеют общую полосу частот, но разные кодирующие последовательности
CoS – Class of Service – классы обслуживания
CQ – Class based Queuing – классы обслуживания очередей
CQ – Custom Queuing – настраиваемые очереди

CRC – Circle Redundancy Check – контрольная сумма
CSMA/CA – Carrier Sense Multiple Access With Collision Avoidance – множественный доступ с контролем несущей и предотвращением коллизий
CSMA/CD – Carrier Sense Multiply Access / Collision Detection – метод множественного доступа с контролем несущей и обнаружением коллизий
CWDM – Coarse Wavelength Division Multiplexing – грубое спектральное мультиплексирование с разделением по длине волны
DARPA – Defense Advanced Research Projects Agency — Управление перспективных исследовательских проектов Министерства обороны США
DCE – Data Circuit-terminating Equipment – сетевое оборудование провайдера
DDoS – Distributed Denial of Service – распределённая атака «отказ в обслуживании»
DHCP – Dynamic Host Configuration Protocol – протокол автоматического назначения конфигурации адресов
DiffServ – Differentiated Service – дифференцированное обслуживание
DLCI – Data Link Connection Identifier – идентификатор подключения к соединению
DMT – Discrete Multi Tone – передача по нескольким несущим
DMZ – Demilitarized Zone – демилитаризированная зона
DNS – Domain Name System – система доменных имён
DOCSIS – Data over Cable Service Interface Specification – стандарт передачи данных по коаксиальному (телевизионному) кабелю
DoS – Denial of Service – компьютерная атака «отказ в обслуживании»
DPL – Digital Power Line – цифровая линия связи по электрическим кабелям
DSCP – DiffServ Code Point – кодовый указатель класса обслуживания
DSL – Digital Subscriber Line – цифровая абонентская линия
DSP – Digital Signal Processing – цифровая обработка сигнала
DTE – Data Terminal Equipment – оконечное оборудование абонента
DVA – Distance Vector Algorithms – класс дистанционно-векторных алгоритмов маршрутизации, основанных на учете вектора расстояний в сети
DWDM – Dense Wavelength Division Multiplexing – плотное мультиплексирование с разделением по длине волны

DWRR – Deficit Weighted Robin Round – дефицитный взвешенный круговой циклический алгоритм обслуживания очереди

E1 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 2048 кбит/с

E2 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 8448 кбит/с

E3 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 34368 кбит/с

E4 – стандарт цифровой передачи данных PDH, соответствующий скорости передачи 139264 кбит/с

EAP – Extensible Authentication Protocol – расширяемый протокол аутентификации

EDA – Ethernet DSL Access – Ethernet с использованием ADSL компании Ericsson

EDGE – Enhanced Data rates for GSM Evolution – цифровая технология беспроводной передачи данных для сетей мобильной связи, которая функционирует как надстройка над технологиями 2G

eNB – Evolved NodeB – базовая станция в сети LTE

eNodeB – Evolved NodeB – базовая станция в сети LTE

EoV – Ethernet-over-VDSL – технология Ethernet поверх VDSL

EPC – Evolved Packet Core – ядро сети LTE

EPON – Ethernet Passive Optical Networking – пассивная оптическая сеть Ethernet

ESCON – Enterprise Systems Connection – соединение учрежденческих систем (с базами данных, серверами и т.д.)

ETSI – European Telecommunications Standards Institute – Европейский институт по стандартизации в области телекоммуникаций

EV-DO – Evolution-Data Only – технология передачи данных, используемая в сетях мобильной связи стандарта CDMA

FDDI – Fiber Distributed Data Interface – распределённый волоконный интерфейс данных

FEC – Forward Error Correction – прямая коррекция ошибок

FICON – Fiber Connection – волоконное соединение для передачи данных

FIFO – First In – First Out – «первый пришел – первый обслужился»

FQ – Fair Queuing – справедливое обслуживание в очереди

FR – Frame Relay – технология пакетной сети

FTP – File Transfer Protocol – протокол отправки файлов по сети

FTTB – Fiber To The Building – доведение волокна до здания

FTTC – Fiber To The Curb – доведение волокна до кабельного шкафа

FTTCab – Fiber To The Cabinet – доведение волокна до кабельного шкафа
FTTH – Fiber To The Home – доведение волокна до квартиры
FTTN – Fiber to the Node – волокно до сетевого узла
FTTO – Fiber To The Office – доведение волокна до офиса
FTTOpt – Fiber To The Optimum – доведение волокна до оптимального пункта
FTTP – Fiber To The Premises – доведение волокна до точки присутствия клиента
FTTR – Fiber To The Remote – доведение волокна до удаленного модуля, концентратора
FTTx – Fiber to the x – оптическое волокно до…
GE – Gigabit Ethernet – Ethernet со скоростью 1 Гбит/с и более
GEM – GPON Encapsulated Method – метод инкапсуляции в кадры GPON
GFP – Generic Framing Procedure – процедура формирования общего кадра
GII – Global Information Infrastructure – концепция глобальной информационной инфраструктуры
GMPLS – Generalized Multi-Protocol Label Switching – обобщённый протокол коммутации по меткам
GPRS – General Packet Radio Service – пакетная радиосвязь общего пользования – надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных
GPS – Global Position System – глобальная система определения местоположения
GSM – Global System for Mobile Communications – глобальный стандарт цифровой мобильной сотовой связи с разделением каналов по времени и частоте
GSP – Generic Services Proxy – технология модуля доступа прикладного уровня для поддержки внешних протоколов обеспечения безопасности
HDLC – High-level Data Link Control – протокол управления каналом высокого уровня
HDSL – High Bit-Rate Digital Subscriber Line – высокоскоростная цифровая абонентская линия
HDTV – High-Definition Television – телевидение высокой четкости
HFC – Hybrid Fiber Coaxial – гибридная сеть кабельного телевидения
HIDS – Host Intrusion Detection System – узловая система обнаружения вторжений
HPNA – Home Phoneline Networking Alliance – объединённая ассоциация некоммерческих промышленных компаний

HSPA – High Speed Packet Access – технология беспроводной широкополосной радиосвязи для сетей мобильной связи, использующая пакетную передачу данных
HSS – Home Subscriber Server – сервер абонентских данных
HTML – HyperText Markup Language – язык гипертекстовой разметки для представления информации в сети Интернет
HTTP – HyperText Transfer Protocol – протокол передачи гипертекстовых документов в сети Интернет
HTTPS – Hypertext Transfer Protocol Secure – расширение протокола HTTP, поддерживающее шифрование
ICMP – Internet Control Message Protocol – протокол межсетевых управляющих сообщений в IP сетях
ICQ – Internet Relay Chat – кроссплатформенная система мгновенного обмена сообщениями
IDS – Intrusion Detection System – система обнаружения вторжений
IEEE – Institute of Electrical and Electronics Engineers – Институт инженеров электротехники и электроники
IIS – Internet Information Services – сервер службы Web определяющий тип запрашиваемого ресурса
IM – Internet Massager – Интернет-мессенджер
IntServ – Integrated Service – интегрированное обслуживание
IoT – Internet of Things – Интернет вещей
IP – Internet Protocol Address – уникальный сетевой адрес узла в компьютерной сети
IPP – IP Precedence – идентификатора приоритета
IPSec – IP Security – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP
IPTV – IP TVset – IP-телевидение
IPX – Internet Packet eXchange – стандарт межсетевого обмена пакетами
iSCSI – internet Small Computer System Interface – протокол для установления взаимодействия и управления системами хранения данных, серверами и клиентами
ISDN – Integrated Services Digital Network – цифровая сеть интегрального обслуживания
IS-IS – Intermediate System to Intermediate System – протокол динамической маршрутизации, основанный на технологии оценки состояния каналов
ISN – Initial Sequence Number – начальный номер последовательности
ISP – Internet Service Provider – провайдер Интернет услуг
ITU-T – International Telecommunication Union – Telecommunication sector – сектор стандартизации электросвязи Международного союза электросвязи

LAN – Local Area Network – локальные сети
LAP-B – Link Access Procedure, Balanced – сбалансированный протокол доступа к каналу передачи данных. Является протоколом канального уровня, используемым для передачи пакетов стандарта X.25
LAP-D – Link Access Procedure on the D-channel – протокол канального уровня стандарта X.25, управляющий потоком кадров, передаваемых по D-каналу в сетях ISDN
LAP-F – Link Access Procedure for Frame mode bearer services – протокол канального уровня стандарта X.25, используемым для передачи пакетов в сетях frame relay
LCI – Logical Channel Identifyer – идентификатор логического канала
LCN – Logical Channel Number – номер логического канала
LLC – Logical Link Control – контролер обслуживания сетевого уровня
LLQ – Low Latency Queuing – низкая задержка обслуживания очереди
LMP – Link Management Protocol – протокол управления соединением в Bluetooth
LSA – Link State Algoritms – класс алгоритмов маршрутизации, основанный на учете состояния каналов
LTE – Long Term Evolution – «долговременное развитие» – проект разработки сетей 4G стандарта с усовершенствованной технологией мобильной передачи данных
LTE-FDD – Frequency Division Duplex LNE – разновидность стандарта LTE, который использует частоту для разделения потоков данных
MAC – Media Access Control – управление доступом к разделяемой физической среде
MDSL – Moderate Speed Digital Subscriber Line – среднескоростная цифровая абонентская линия
MIME – Multipurpose Internet Mail Extension – стандарт, описывающий передачу различных типов данных по электронной почте
MIMO – Multiple Input – Multiple Output – система «множество входов – множество выходов»
MME – Mobility Management Entity – система управления в сети LTE
MPLS – Multi-Protocol Label Switching – многопротокольная коммутация по меткам
MRED – Multilevel Random Early Detection – многоуровневое раннее обнаружение перегрузок в очередях
MSDSL – Moderate Speed Digital Subscriber Line – среднескоростная цифровая абонентская линия

NGN – Next Generation Networks – сеть связи следующего поколения
NIDS – Network Intrusion Detection System – сетевая система обнаружения вторжений
N-ISDN – Narrowband Integrated Services Digital Network – узкополосная цифровая сеть с интеграцией служб
NSFNET – National Science Foundation Network – сеть связи между компьютерами университетов и вычислительными центрами
NP – Non Priority – неприоритетный трафик
OAD – Optical Add Drop (Multiplexer) – оптический мультиплексор ввода-вывода
OADM – Optical Add Drop Multiplexer – оптический мультиплексор ввода-вывода
OAN – Optical Access Networks – оптическая сеть доступа
OFDM – Orthogonal Frequency-Division Multiplexing – мультиплексирование с ортогональным частотным разделением каналов
OFDMA – Orthogonal Frequency Division Multiple Access – ортогональный частотный множественный доступ
OLE – Object Linking and Embedding – технология связывания и внедрения объектов в другие документы и объекты
OLT – Optical Line Terminal – терминал (абонент) оптической линии
ONT – Optical Network Terminal – терминал (абонент) оптической сети
ONU – Optical Network Unit – модуль центрального узла
OQPSK – Offset QPSK – квадратурно-фазовая манипуляция со сдвигом частоты
ORBL – Open Relay Black List – «черный список» почтовых серверов
OSI – Open System Interconnect – эталонная модель взаимодействия открытых систем
OSPF – Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала
OTH – Optical Transport Hierarchy – оптическая транспортная иерархия
OTN – Optical Transport Network – оптическая транспортная сеть
OTU – Optical Transport Unit – оптический транспортный блок
OXC – Optical Cross-Connect – оптический кросс-коммутатор
P – Priority – приоритетный трафик
P2P – Pear-to-Pear – пиринговая файлообменная сеть

PAD – Packet Assembler Disassembler – сборщик-разборщик пакетов
PAE – процесс доступа через порт
PAM – Pulse Amplitude Modulation – амплитудно-импульсная модуляция
PCEF – Policy and Charging Enforcement Function – управляющий сервер в сети LTE
PDH – Plesiochronous Digital Hierarchy – плезиохронная цифровая иерархия
PDN – Packet Data Network – сеть с коммутацией пакетов
PGP – Pretty Good Privacy – протокол с открытым ключом для шифрования сообщений электронной почты
P-GW – Packet Data Network Gateway – шлюз сопряжения с пакетными сетями в сети LTE
PLC – Power Line Communication – обмен данными по линии электропередачи
PON – Passive Optical Network – пассивная оптическая сеть
POP – Point of Presence – точка присутствия/подключения
PPP – Point-to-Point Protocol – протокол «точка-точка»
PQ – Priority Queuing – приоритетное обслуживание в очереди
PQ-CBWFQ – Priority Class-Based Weighted Fair Queuing – приоритетное взвешенное справедливое обслуживание в очереди на основе классов
PSE – Packet Switch Exchange – пакетный коммутатор
PVC – Permanent Virtual Circuits – постоянно скоммутированные виртуальные каналы
QAM – Quadrature Amplitude Modulation – квадратурная амплитудная модуляция
QoS – Quality of Service – качество обслуживания
QPSK – Quadro Phase-Shift Keying – квадратичная фазовая манипуляция
RED – Random Early Detection – раннее обнаружение перегрузок в очередях;
RIP – Routing Information Protocol – внутренний протокол маршрутизации
RLL – Radio Local Loop – технология абонентского радиодоступа
RPR – Resilient Packet Ring – протокол пакетного кольца с самовосстановлением
RR – Robin Round – круговой циклический алгоритм обслуживания очереди
RSA – Rivest, Shamir, Adleman – криптографический алгоритм с открытым ключом
RSVP – Resource ReSerVation Protocol – протокол резервирования ресурсов

RT – Real Time – трафик «реального времени»
SANs – Storage Area Networks – сеть хранения данных (серверы услуг, базы данных)
SCADA – Supervisory Control and Data Acquisition – диспетчерское управление и сбор данных
SC-FDMA – Single Carrier Frequency Division Multiple Access – множественный доступ с частотным разделением каналов с одной несущей частотой
SDH – Synchronous Digital Hierarchy – синхронная цифровая иерархия
SDSL – Symmetric Digital Subscriber Line – симметричная цифровая абонентская линия симметричная абонентская линия, работающая по одной паре
S-GW – Serving Gateway – обслуживающий шлюз в сети LTE
SHDSL – Simmetric High Speed Digital Subscriber Line - симметричная высокоскоростная цифровая абонентская линия
SONET – Synchronous Optical NETworking – синхронная цифровая иерархия
SSH – Secure SHell — сетевой протокол прикладного уровня «безопасная оболочка», позволяющий туннелировать TCP-соединения
SSID – Service Set Identifier – символьное наименование беспроводной точки доступа Wi-Fi
SSL – Secure Socket Layer – протокол секретного обмена сообщениями
STM – Synchronous Transport Module – синхронный транспортный модуль технологии SDH
STM – Synchronous Transfer Mode – синхронный режим передачи
STP – Shielded Twisted Pair – экранированная витая пара
SVC – Switched Virtual Circuits – перекоммутируемые виртуальные каналы
Tail Drop – сброс пакетов в конце очереди
TCP – Transmission Control Protocol – протокол управления передачей
TC-PAM – Trellis Coded Pulse Amplitude Modulation – амплитудно-импульсная модуляция с треллис-кодированием
TDM – Time Division Multiplexing - временное мультиплексирование
TETRA – TErrestrial Trunked RAdio – открытый стандарт цифровой транкинговой радиосвязи
TLS – Transport Layer Security – протокол обеспечения безопасности транспортного уровня
TMN – Telecommunications Management Network – концепция управления сетью

TMUX – Trans Multiplexor – трансмультиплексор
ToS – Terms of Service - условия предоставления услуг
UDP – User Datagram Protocol – протокол пользовательских датаграмм
UE – User Equipment – абонентский терминал в сети LTE
URL – Uniform Resource Locator – символьный указатель ресурса в сети Интернет
USB – Universal Serial Bus — интерфейс универсальной последовательной шины
UTP – Unshielded Twisted Pair – неэкранированная витая пара
V.35 – стандарт, описывающий протокол и интерфейс абонентского модемного доступа к сети по медному кабелю
VC – Virtual Circuit – виртуальный канал
VDSL – Very High Bit-Rate Digital Subscriber Line – сверхвысокоскоростная цифровая абонентская линия
VDSL – Very High Bit-Rate Digital Subscriber Line – сверхвысокоскоростная цифровая абонентская линия
VHDSL – Very High Bit-Rate Digital Subscriber Line – сверхвысокоскоростная цифровая абонентская линия
VLAN – Virtual Local Area Network – виртуальная локальная компьютерная сеть
VOD – Video on Demand – видео по запросу
VoDSL – Voice over DSL – одновременная передача данных и голоса в цифровом виде
VoIP – Voice over IP – одновременная передача данных и голоса
VPN – Virtual Private Network – виртуальная частная сеть
VSAT – Very Small Aperture Terminal – технология спутниковой связи с использованием центральной земной станции, вещающей на абонентские терминалы с малой апертурой антенны
WAN – Wide Area Network – глобальная сеть
WDM – Wavelength Division Multiplexing – система оптического уплотнения по длине волны
WEP – Wired Equivalent Privacy – алгоритм для обеспечения безопасности сетей Wi-Fi
WFQ – Weighted Fair Queuing – взвешенное справедливое обслуживание в очереди
WiMAX – Worldwide Interoperability for Microwave Access – телекоммуникационная технология высокоскоростного радиодоступа
WLAN – Wireless Local Area Network – беспроводная локальная сеть
WLL – Wireless Local Loop – технологии беспроводного абонентского доступа

WMAN – Wireless Metropolitan Area Network – беспроводная сеть городского масштаба
WPA – Wi-Fi Protected Access – стандарт обеспечения безопасности сетей Wi-Fi
WPAN – Wireless Personal Area Network – беспроводная персональная сеть
WRED – Weighted Random Early Detection – взвешенное раннее обнаружение перегрузок в очередях
WRR – Weighted Robin Round – взвешенный круговой циклический алгоритм обслуживания очереди
WWAN – Wireless Wide Area Network – беспроводная глобальная сеть
WWW – World Wide Web – «всемирная паутина»
X.25 – стек стандартов для коммуникационных протоколов доступа к сетям с коммутацией пакетов
xDSL – Digital Subscriber Line – цифровая абонентская линия одного из стандартов DSL
АЛ – абонентская линия
АМ – амплитудная модуляция
АНБ – Агентство национальной безопасности (США)
АРМ – автоматизированное рабочее место
АСП – аналоговая система передачи
АСУ – автоматизированная система управления
АТ – абонентский терминал
АЦП – аналогово-цифровой преобразователь
БД – база данных
БС – базовая станция
ВОЛС – волоконно-оптическая линия связи
ВСС – взаимоувязанная сеть связи
ВТ – виртуальный терминал
ГГС – громко-говорящая связь
ГКРЧ – Государственная комиссия по радиочастотам
ДВ – длинные волны
ЕСЭ – единая сеть электросвязи
ЗС – земная станция
ИБ – информационная безопасность
ИКМ – импульсно-кодовая модуляция
ИТ – информационные технологии
ИТВ – информационно-техническое воздействие
ИУС – информационно-управляющая система
КВ – короткие волны
КТВ – кабельное телевидение
МО – Министерство обороны
МСЭ – Международный союз электросвязи
НСД – несанкционированный доступ

НЧ – низкая частота
ОЗУ – оперативное запоминающее устройство
ОК – оптический кабель
ОКС – общий канал сигнализации
ОНЧ – очень низкая частота
ОС – операционная система
ОЦК – основной цифровой канал
ПО – программное обеспечение
ППРЧ – псевдослучайная перестройка рабочей частоты
ПЦИ – плезиохронная цифровая иерархия
ПЦК – первичный цифровой канал
ПЦС – плезиохронная цифровая система
ПЭМИН – побочные электромагнитные излучения и наводки
РРС – радиорелейная станция
РФ – Российская Федерация
САД – система абонентского доступа
СВ – средние волны
СВЧ – сверхвысокие частоты
СДВ – сверхдлинные волны
СКД – сеть коллективного доступа
СМИ – средства массовой информации
СПД – сеть передачи данных
СС – система связи
СС ОП – система связи общего пользования
СС СН – система связи специального назначения
ССС – спутниковая система связи
СУБД – система управления базой данных
СЦИ – синхронная цифровая иерархия
США – Соединенные Штаты Америки
ТВ – телевидение
ТВ – телевидение
ТКС – телекоммуникационная система
ТС – транспортная сеть
ТфОП – телефонная сеть общего пользования
ТЧ – (канал) тональной частоты
УД – узел доступа
УК – узел коммутации
УКВ – ультракороткие волны
У-ЦСИС – узкополосная цифровая сеть с интеграцией служб
ФСТЭК – Федеральная служба по техническому и экспортному контролю (России)
ЦАЛ – цифровая абонентская линия
ЦАП – цифро-аналоговое преобразование
ЦСИО – цифровая сеть интегрального обслуживания
ЦСИУ – цифровая сеть с интеграцией услуг

ЦСП	–	цифровая система передачи
ШПД	–	широкополосный доступ
ШПС	–	широкополосный сигнал
ЭВМ	–	электронная вычислительная машина
ЭИИМ	–	эквивалентная изотропно излучаемая мощность
ЭМС	–	электромагнитная совместимость
ЭЦП	–	электронная цифровая подпись

Литература

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

2. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.

3. Макаренко С. И., Сапожников В. И., Захаренко Г. И., Федосеев В. Е. Системы связи: учебное пособие для студентов (курсантов) вузов. – Воронеж: ВАИУ, 2011. – 285 с.

4. Ефимов С. Н., Акмолов А. Ф., Макаренко С. И. Основы построения инфокоммуникационных систем и сетей: учебное пособие. – СПб.: ВКА им. А.Ф. Можайского, 2012. – 201 с.

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

6. Макаренко С. И., Коровин В.М. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Часть 1: Принципы функционирования аппаратных средств телекоммуникационных и вычислительных систем. – СПб.: ВКА имени А. Ф. Можайского, 2014. – 197 с.

7. Макаренко С. И., Ковальский А. А., Краснов С. А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях. – СПб.: Наукоемкие технологии, 2020. – 357 с.

8. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

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

10. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

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

12. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.

13. Илюхин Б. В. Сетевые информационные технологии. Учебное пособие. – Томск: Томский межвузовский центр дистанционного образования, 2005. – 180 с.

14. Семенов Ю. А. Телекоммуникационные технологии [Электронный ресурс]. М.: МФТИ. 2023. – URL: book.itep.ru (дата обращения 10.12.2023).

15. Принципы построения и функционирования сетей LTE // G1234: Портал о современных технологиях мобильной и беспроводной связи [Электронный ресурс]. 2023. – URL: http://1234g.ru/4g/lte/printsip-raboty-seti-lte/printsipy-postroeniya-i-funktsionirovaniya-setej-lte (дата обращения 10.12.2023).

16. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003. – 992 с.

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

18. Механизмы DiffServ // Сети для самых маленьких [Электронный ресурс], 2023. – URL: https://linkmeup.gitbook.io/sdsm/15.-qos/2.-mekhanizmy-diffserv-1 (дата обращения 10.12.2023).

19. Recommendation ITU-T Y.2011. General principles and general reference model for next generation networks. 2004.

20. Фокин В. Г. Оптические системы передачи и транспортные сети. Учебное пособие. – М.: Эко-Трендз, 2008.

21. Брейман А. Д. Сети ЭВМ и телекоммуникации. Глобальные сети. Учебное пособие. – М.: МГУПИ, 2006. – 116 с.

22. Каррыев Б. Интернет: цифровая революция эры мгновенной коммуникации. Мегасила, история и влияние на общество. – М.: Litres, 2018. – 490 с.

23. Диков А. В. Эволюция интернета от начала до наших дней и далее // Школьные технологии. 2019. № 2. С. 3-8.

24. Барабаш П., Воробьев С., Махровский О. Новые времена, новые сети // Каталог «Технологии и средства связи» [Электронный ресурс]. 2008. – URL: www.tssonline.ru/articles2/Oborandteh/new-times-new-networks (дата обращения 1.09.2023).

25. Ги Кайя. Об абонентском доступе // Сети и системы связи. 1996. № 6.

26. Горнак А.М. Организация доступа на базе xDSL: современные технологии // Технологии и средства связи. Специальный выпуск «Системы абонентского доступа», 2004.

27. Современные технологии доступа в сеть Интернет // Технологии DSL [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 1.09.2023).

28. Барабаш П., Воробьев С., Махровский О. Проводные технологии сетей абонентского доступа: принципы построения, классификация // Каталог «Технологии и средства связи» [Электронный ресурс]. 2008. – URL: www.tssonline.ru/articles2/Oborandteh/provodnye-technologii-sad (дата обращения 1.09.2023).

29. Орлов С. Ethernet в сетях доступа // LAN. Журнал сетевых решений. 2004. № 1.

30. Блушке А. «Родословная» xDSL, или попытка классификации технологии xDSL для «последней мили» // Технологии и средства связи. 2000. № 1.

31. Барабаш П. А., Воробьев С. П., Махровский О. В., Шибанов В. С. Мультисервисные сети кабельного телевидения. – СПб.: Наука, 2004.

32. Котиков И. М. Классификация и сравнительный анализ технологий проводного доступа // Технологии и средства связи. Специальный выпуск «Системы абонентского доступа», 2004.

33. Пассивные оптические сети PON. Абонентский участок FTTH // Компания ДЕПС [Электронный ресурс]. – URL: www.etkis.ru/documents/pon/ftth-pon.htm (дата обращения 1.09.2023).

34. Судьба медной абонентской линии в цифровом мире: переход от аналоговой к цифровой абонентской кабельной сети // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

35. Общие аспекты технологий DSL // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

36. Быстрый Интернет по телефонной паре. Как работает xDSL // Портал Itc.ua [Электронный ресурс]. – URL: http://itc.ua/articles/bystryj_internet_po_telefonnoj_pare_kak_rabotaet_xdsl_20388/ (дата обращения 01.09.2023).

37. Технология DSL // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

38. Симонина А. В., Гусельцов Д. Ю. Концентраторы xDSL (DSLAM) // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

39. Чепусов Е. Цифровые системы передачи: от HDSL к G.shdsl // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

40. Никифоров А. В. Технология PLC – телекоммуникации по сетям электропитания // Сети и системы связи [Электронный ресурс]. 2002. № 5. – URL: www.ccc.ru/magazine/depot/02_05/read.html?0301.htm (дата обращения 01.09.2023).

41. Комаров С. Беда пришла, откуда не ждали… // Broadcasting. 2005. № 7. С. 71. – URL: www.radiostation.ru/drm/plc1.html (дата обращения 01.09.2023).

42. Анализ конфигураций широкополосного абонентского доступа // DSL-технологии [Электронный ресурс]. – URL: www.xdsl.ru (дата обращения 01.09.2023).

43. Технология FTTx // Prointex telecomminication equipment [Электронный ресурс]. – URL: www.prointech.ru (дата обращения 01.09.2023).

44. Гасымов И. Архитектура оптических сетей доступа FTTH (Fiber-to-the-Home) // Официальный документ компании Cisco System Inc. 2007. – 12 с.

45. Петренко И. И., Убайдуллаев Р. Р. Сети PON. Стандарты // Terra Link: технологии стандарты протоколы [Электронный ресурс]. 06.10.2004. – URL: www.teralink.ru (дата обращения 01.09.2023).

46. Технология PON // Связь комплект [Электронный ресурс]. – URL: www.skomplekt.com (дата обращения 01.09.2023).

47. Абдрахманова Г. И., Баскакова О. Е., Вишневский К. О., Гохберг Л. М. и др. Тенденции развития интернета в России и зарубежных странах: аналитический доклад. – М.: НИУ ВШЭ, 2020. – 144 с. – URL: https://issek.hse.ru/mirror/pubs/share/345060549.pdf (дата обращения 01.09.2023).

48. Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь. 2011. № 3. С. 41-47.

49. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376.

50. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1-29.

51. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.

52. Медведовский И. Д., Семьянов П. В., Платонов В. В. Атака через Интернет / Под ред. П.Д. Зегжды. – СПб.: НПО «Мир и семья-95», 1997.

53. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

54. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – М.: ФСТЭК России, 2008. – 69 с.

55. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с.

56. Мэйволд Э. Безопасность сетей // ИНТУИТ: национальный открытый университет [Электронный ресурс], 2006. – URL: https://intuit.ru/studies/courses/102/102/info (дата обращения 01.09.2023).

57. Кобб М. Джост М. Безопасность IIS // ИНТУИТ: национальный открытый университет [Электронный ресурс], 2006. – URL: https://intuit.ru/studies/courses/1002/122/info (дата обращения 01.09.2023).

58. Бейс Р. Введение в обнаружение атак и анализ защищенности // НИП «Информзащита» [Электронный ресурс], 2007. – URL: http://bugtraq.ru/library/books/icsa/ (дата обращения 01.09.2023).

59. Семенов Ю. А. Процедуры, диагностики и безопасность в Интернет // ИНТУИТ: национальный открытый университет [Электронный

ресурс], 2007. – https://intuit.ru/studies/courses/1124/201/info (дата обращения 01.09.2023).

60. Пировских А. Взлом WPA // TNG.ru [Электронный ресурс], 2005. – URL: www.thg.ru/network/20050806/print.html

61. Таранов А., Слепов О. Безопасность систем электронной почты // Jet Info [Электронный ресурс], 2003. – URL: www.citforum.ru/security/internet/email/article1.6.2003.html#AEN11 (дата обращения 01.09.2023).

62. Иржавский А. Безопасность электронной почты // CIO. 2003. № 8. – URL: offline.cio-world.ru/2003/18/29383/index.html (дата обращения 01.09.2023).

63. Макаренко С. И., Бережнов А. Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в вооруженных силах Российской Федерации // Вестник Академии военных наук. 2011. № 4 (37). С. 64-68.

64. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2.

65. Цветков К. Ю., Макаренко С. И., Михайлов Р. Л. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-телекоммуникационных сетей // Информационно-управляющие системы. 2014. № 2 (69). С. 71-78.

66. Макаренко С. И., Квасов М. Н. Модифицированный алгоритм Беллмана-Форда с формированием кратчайших и резервных путей и его применение для повышения устойчивости телекоммуникационных систем // Инфокоммуникационные технологии. 2016. Т. 14. № 3. С. 264-274. DOI: 10.18469/ikt.2016.14.3.06

67. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. 2015. № 2. С. 45-98. DOI: 10.24411/2410-9916-2015-10203

68. Макаренко С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60-97. DOI: 10.24411/2410-9916-2017-10106

69. Макаренко С. И. Аудит безопасности критической информационной инфраструктуры. Учебное пособие. – СПб.: Наукоемкие технологии, 2023. – 122 с.

70. Макаренко С. И. Тестирование на проникновение на основе стандарта NIST SP 800-115 // Вопросы кибербезопасности. 2022. № 3 (49). С. 44-57. DOI: 10.21681/2311-3456-2022-3-44-57

71. Макаренко С. И., Смирнов Г. Е. Модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями // Труды учебных заведений связи. 2021. Т. 7. № 1. С. 94-104. DOI: 10.31854/1813-324X-2021-7-1-94-104

72. Макаренко С. И. Критерии и показатели оценки качества тестирования на проникновение // Вопросы кибербезопасности. 2021. № 3 (43). С. 43-57. DOI: 10.21681/2311-3456-2021-3-43-57

73. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6 (46). С. 12-25. DOI: 10.21681/2311-3456-2021-6-12-25

74. Смирнов Г. Е. Модель анализа защищенности объекта информатизации железнодорожного транспорта и методика обоснования набора тестовых информационно-технических воздействий для этого // Системы управления, связи и безопасности. 2022. № 4. С. 137-189. DOI: 10.24412/2410-9916-2022-4-137-189

Макаренко Сергей Иванович

Защита компьютерных сетей и телекоммуникаций

Учебное пособие

Рецензенты:

Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета Государственной противопожарной службы Министерства чрезвычайных ситуаций России

Михайлов Роман Леонидович, доктор технических наук, доцент, научно-педагогический сотрудник Военного университета радиоэлектроники

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197350, г. Санкт-Петербург, пр-кт Комендантский, 59-2-1-204
http://publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

Гарнитура «TimesNewRoman». 19,5 п.л.
Тираж 200 экз. Подписано в печать 10.01.2024 г.

Материалы изданы в авторской редакции

ISBN 978-5-907618-79-4