2.4. Телекоммуникации

2.4.1. Телекоммуникационная революция

Основоположник идеологии информационного общества Д.Белл в книге "Социальные рамки информационного общества" большое значение придает конвергенции электронно-вычислительной техники с техникой средств связи и утверждает, что "в наступающем столетии решающее значение для экономической и социальной жизни, для способов производства знания, а также для характера трудовой деятельности человека приобретет становление нового социального уклада, зиждущегося на телекоммуникациях". Сегодня реализация идеологии работы компании, ориентированной на ее клиентов и партнеров невозможна без современных средств телекоммуникаций.

Телекоммуникации (от греческого tele — вдаль, далеко, и латинского communicatio —- общение) — это технические средства и способы дистанционной передачи информации.

В настоящее время для передачи информации в различном её виде (текст, изображение, звук, цифра) на большие расстояния изобретено огромное количество разнообразных технических средств, таких как телеграф и его разновидность телекс, телефон, радио, телевидение, а также появившиеся сравнительно недавно — телефакс, цифровая телефония (ISDN), сотовая, транкинговая и пейджинговые виды радиосвязи, компьютерные коммуникации. Все перечисленные виды связи в настоящее время немыслимы без спутниковой связи. Все перечисленные виды связи дополняя и взаимодействуя друг с другом образуют единую информационную магистраль.

2.4.2. Компоненты и функции телекоммуникационных систем

Любые виды сообщений передаются с помощью сигналов. Сигналы могут быть звуковые, световые, тепловые и другие, но сообщения передаются преимущественно электрическими сигналами с помощью систем электрорадиосвязи, а в последнее время все большее развитие получают системы оптоволоконной связи.

Источники сообщений и соответствующие им первичные сигналы могут быть непрерывными (аналоговыми) и дискретными. Аналоговым называется источник, который за конечный интервал времени может иметь бесконечное множество состояний (например, генератор электрического тока на электростанции и электрический ток в сети). Другими словами, аналоговый сигнал — это непрерывное изменение какой-либо физической величины во времени (напряжения, тока, давления и т.п.). Дискретный сигнал представляется обычно двумя состояниями какой-либо физической величины. Простейший пример — азбука Морзе, двоичный код (0,1).

При осуществлении связи отправитель подает сообщение на передатчик, в котором сообщение, представленное сигналами любого вида (речь, изображение и т.п) превращается в электрический сигнал (аналоговый или дискретный), а в приемнике происходит обратное преобразование электромагнитного сигнала в сообщение. Передатчик и приемник связаны между собой каналом связи.

Канал (канал связи) — средство односторонней передачи данных (ПД). Примером канала может быть полоса частот, выделенная одному передатчику при радиосвязи. В некоторой линии можно образовать несколько каналов связи, по каждому из которых передается своя информация. При этом говорят, что линия разделяется между несколькими каналами. Существуют два метода разделения линии передачи данных: временное мультиплексирование (иначе разделение по времени или TDM), при котором каждому каналу выделяется некоторый квант времени, и частотное разделение (FDM — Frequency Division Method), при котором каналу выделяется некоторая полоса частот. *Канал передачи данных* — средство двустороннего обмена данными, включающие средства кодирования данных и линию передачи данных. По природе физической среды передачи данных различают каналы на оптических линиях связи, в которых сигнал распространяется по световодам (стеклянным трубкам, внутренняя сторона которых имеет зеркальное покрытие), проводных (медных) линиях связи и беспроводные. В свою очередь, медные каналы могут быть представлены волноводами (медными параллелепипедами, посеребренными внутри), коаксиальными кабелями (центральный провод внутри цилиндрического диэлектрика, покрытый сверху металлической оплеткой, например, кабель для подключение телевизора к антенне) и симметричными кабелями (многожильные, витая пара), а беспроводные — радио- и инфракрасными каналами.

По способу обмена сведениями между абонентами различают три вида связи. Дуплексная связь позволяет осуществлять одновременный, двусторонний обмен. При полудуплексной связи обмен информацией в обоих направлениях осуществляется попеременно. Возможна также работа только на прием или только на передачу (симплексный канал).

В зависимости от числа каналов связи в аппаратуре ПД различают одно- и многоканальные средства ПД. В локальных вычислительных сетях и в цифровых каналах передачи данных обычно используют временное мультиплексирование, в аналоговых каналах — частотное разделение.

Если канал ПД монопольно используется одной организацией, то такой канал называют выделенным, в противном случае канал является разделяемым или виртуальным (общего пользования). К передаче информации

имеют прямое отношение телефонные сети, вычислительные сети передачи данных, спутниковые системы связи, системы сотовой радиосвязи.

Кратко рассмотрим каждый из видов связи.

Виды каналов связи: проводная, многоканальная, кабельная, оптоволоконная.

Телеграфная связь является исторически первым видом электросвязи и в настоящее время утрачивает свои позиции вследствие развития более прогрессивных видов телекоммуникаций. Однако в России, где еще недостаточно развита телекоммуникационная инфраструктура, она пока обеспечивает более надежную и более доступную для многих регионов связь, чем телефон. Значение телеграфной связи заключается и в том, что здесь впервые был использован двоичный код, который нашел исключительное применение в современных ЭВМ и системах связи.

В телеграфе сообщения передаются дискретными кодированными сигналами (сначала код Морзе, а затем код Бодо). Каждый знак сообщения, передаваемый по телеграфу, содержит 7 бит. Используемый код состоит из двух служебных (старт и стоп) и пяти значащих битов длительностью 20 миллисекунд. Поэтому для передачи одной буквы сообщения требуется 0.15 секунды, что и определяет низкую скорость передачи сообщений (~ 50 бит/сек).

Наряду с низкой скоростью передачи сообщений, другим недостатком телеграфа является ограниченные возможности для выхода в международную телеграфную сеть. Абонентские пункты международной телеграфной связи размещены обычно на центральных телеграфах городов. Телеграфные аппараты, в которых наряду с общепринятой для такого вида связи системой кодирования используются различные сокращения и упрощенная конструкция фраз, получили название телекс. Такие устройства используют для обмена служебной текстовой информацией между предприятиями. С этой целью создана специальная сеть абонентских пунктов, на которых устанавливаются телетайпы.

Телефонная связь, начавшая действовать в 1876 г. (изобретена А. Беллом), к настоящему времени превратилась в разветвленную глобальную систему связи. С помощью нее передается речь, факсимильные данные. Новое революционное развитие телефонная связь получила с появлением сотовой радиотелефонии, Интернет и цифровой телефонии (ISDN).

Телефонная сеть России представляет собой единую, иерархическую систему узлов соединений абонентов. Основу сети составляют автоматические телефонные станции. АТС соединяются между собой и абонентами с помощью кабельной сети. Узлы коммутации разделены на классы: класс 1, класс 2, междугородние АТС и районные АТС. Абоненты соединяются между собой по радиальному принципу. АТС 1 и 2 класса по принципу

«каждый с каждым», а промежуточные узлы коммутации могут использовать смешанный принцип соединения.

Неотъемлемой частью любого среднего и крупного офиса современной компании стала учрежденческая АТС. Учрежденческие АТС, представленные сейчас на рынке по принципу работы делятся на 2 класса: аналоговые и цифровые. Аналоговая телефонная станция представляет собой интеллектуально-управляемый набор реле, способный осуществлять коммутацию каналов между телефонными портами станции (включая музыку на ожидание), осуществлять удержание линии и ряд других функций, жестко привязанных к конструкции конкретной модели. Цифровая АТС представляет собой специализированный компьютер, имеющий цифровые и аналоговые порты для подключения, соответственно, цифровых или аналоговых телефонных линий, других периферийных устройств, и выполняющий те действия с поступающей из портов информацией, которые запрограммированы в его памяти. Цифровая АТС является очень гибким устройством, способным предоставить ряд исключительно важных для бизнеса функций, множество дополнительных возможностей, обеспечивающих удобство эксплуатации. К ним относятся многосторонняя конференц – связь, гибкое направление входящих вызовов на различные аппараты, перенаправление вызова со своего аппарата на другой, поисковый вызов по всем аппаратам, выход на внешнюю линию.

Факсимильная связь. Для оперативной передачи документов предприниматель может использовать факсимильную связь, которая является разновидностью телефонной связи. Сам факсимильный аппарат скомбинирован с номеронабирателем и телефонной трубкой. Факсимиле (от латинского facsimile – «делай подобное») это точное воспроизведение на бумаге передаваемого плоского изображения. В передающем аппарате документ считывается с помощью линейки светочувствительных элементов, расположенной перпендикулярно сканируемому листу. Информация о яркости отдельных точек преобразуется в электрический сигнал, кодируется, и передается по телефонной линии. Принимающий аппарат декодирует получаемые сигналы и передает их на печатающее устройство. В большинстве типов телефаксов используется термопечать и специальная термобумага, потемнение которой зависит от степени нагревания. Поэтому в приемном устройстве имеется линейка точечных нагревательных элементов, температура нагрева которых пропорциональна величине протекшего тока, определяемого степенью яркости точек передаваемого документа. Сканируемый документ в передающем устройстве и термобумага в приемном устройстве протягиваются с одинаковой скоростью. Протяжка осуществляется последовательными шагами. Один цикл длится несколько миллисекунд, что обеспечивает высокую скорость печати. Режим передачи и приема

изображения автоматически согласуются с помощью специальных сигналов перед началом сеанса.

В телефаксах последних модификаций вместо термопечатающих устройств используются струйные и лазерные принтеры. Время передачи документа формата А 4 у большинства телефаксов составляет 10-15 секунд.

Модем. Если телефонная связь используется для обмена данными между компьютерами, то необходимо устройство согласования аналоговой телефонной сети с цифровым представлением данных для обработки их на компьютере.

Большинство современных модемов позволяют организовать связь не только между персональными компьютерами, но и между компьютером и телефаксом (факсмодем), телеграфом и компьютером (телеграфный модем). Обмен сообщениями между компьютерами в малонаселенных районах без телефонной сети может осуществляться с помощью радимодема. Выбор модема определяется конкретной задачей, которую ставит перед собой пользователь и качества и типа линии связи.

Цифровые системы телекоммуникаций. Аналоговые системы связи все меньше отвечают требованиям времени, хотя из-за своей доступности они еще достаточно широко используются для телефонии и низкоскоростной передачи данных. Более высокими скоростями передачи отличаются выделенные цифровые каналы связи, построенные на основе медных кабелей, оптоволокна, беспроводных и спутниковых каналов связи. Сейчас развиваются очень перспективные сети с асинхронным режимом передачи данных (АТМ). Реально доступны, в том числе в ряде городов России, услуги сетей с ретрансляцией кадров (frame relay), обычно базирующихся на выделенных линиях и поддерживающих многоточечные топологии. Сети frame relay могут использоваться для передачи различных видов трафика. В ряде стран, прежде всего в США, началось внедрение технологий высокоскоростной передачи интегрированных данных по сетям кабельного телевидения (КТВ) и обычным телефонным проводам (xDSL). Получают развитие такие технологии, как SMDS (Synchronous Multimegabit Digital Service — многоточечная передача данных на основе коммутации ячеек) и B-ISDN (Broadband ISDN - широкополосная ISDN). Эти технологии очень перспективны, но пока мало доступны и дороги.

Технология ISDN. В России наибольшее распространение уже получила технология ISDN. Что же такое ISDN? Согласно определению Международного Союза Связи, головной организации по разработке телекомуникационных стандартов, ISDN представляет собой "набор стандартных интерфейсов для цифровой сети связи". По своей сути ISDN — это цифровой вариант аналоговых телефонных линий с коммутацией цифровых по-

токов, или, иначе, сеть из цифровых телефонных станций, соединенных друг с другом цифровыми каналами передачи данных.

Рассмотрим возможности ISDN, а также в общих чертах определим сферу применения данной технологии. В первую очередь следует сказать о значительно более высоких скоростях передачи информации по отношению к аналогичным показателям, характерных для аналоговой телефонии. Обмен данными по линиям ISDN осуществляется с более высокими скоростями и значительно большей надежностью, чем с помощью самых скоростных модемов. Технология ISDN обеспечивает передачу данных со скоростью 64 Кбит/с при одном и 128 Кбит/с при двух каналах связи. Вторая примечательная особенность, отличающая ISDN от аналоговых принципов передачи сигналов, заключается в значительно более широком диапазоне типов передаваемых сообщений. Собственно говоря, весь "диапазон", используемый в аналоговой телефонии, ограничивался передачей речевых сигналов. ISDN же предоставляет пользователям поистине уникальный сервис: помимо традиционного обмена звуковой информацией, они получают возможность обмениваться цифровыми данными, текстом и движущимся видеоизображением. При этом и скорость, и надежность, и качество передаваемых сообщений настолько высоки, что способны удовлетворить требованиям самого взыскательного пользователя. Третьей важной особенностью, весьма привлекательной для пользователей, является адаптируемость средств ISDN с существующими аналоговыми телефонными сетями. К числу важных факторов следует также отнести простоту использования, дружественный и удобный интерфейс, эффективные средства управления, большое количество сервисных функций (до 230), высокое качество передачи информации и высокую гарантию ее сохранности при ее прохождении по каналам связи.

Перечисленные возможности ISDN позволяют широко использовать данную технологию в самых различных областях. Помимо применения ISDN в качестве привычного средства телефонной связи, цифровая технология передачи сигналов является идеальной системой для многих предприятий и фирм в плане работы с удаленными пользователями, а также для организации эффективного доступа в Internet, организации видеоконференций и т . д.

Радиоканалы: пейджинговая, сотовая, транкинговая, спутниковая системы связи.

Одним из существенных недостатков проводных типов связи является отсутствие мобильности, поскольку абонент жестко привязан к линии связи. Этого недостатка лишены различные виды радиосвязи. Широкое распространение в настоящее время получили пейджинговая, сотовая и транкинговая виды мобильной радиосвязи.

Пейджинговая связь. Системы персонального радиовызова, обеспечивающие одностороннюю передачу информации своим абонентам в пределах обслуживаемой зоны, являются сегодня одним из массовых и наиболее доступных средств связи. Сети этой подвижной связи в России создаются на основе систем и средств, соответствующих международным стандартам.

Необходимость разработки и использования систем персонального радиовызова обусловлена тем, что до недавнего времени в различных отраслях производства, на транспорте и в сфере обслуживания между работниками, деятельность которых сопряжена с пребыванием на каких-либо объектах или с передвижением по городу, могла осуществляться только радиотелефонная связь. Сложность реализации такой связи определялась ограниченностью и занятостью диапазона радиочастот, громоздкостью и высокой стоимостью аппаратуры. Использование же систем персонального радиовызова позволяет избежать указанных трудностей и осуществить избирательный вызов по узкополосному каналу любого из абонентов, свободно передвигающихся в пределах города и его окрестностей

Устройство, которое обеспечивает этот вид связи называется пейджер. Термин пейджер происходит от американизированного английского глагола «to page – вызывать, громко выкликать фамилию». Пейджер – это миниатюрный постоянно включенный радиоприемник с жидкокристаллическим дисплеем. Сообщение по пейджинговой связи передается следующим образом. Абонент, отправляющий сообщение, звонит по телефону оператору, называет номер абонента получателя и диктует сообщение, которое заносится в компьютер. С компьютера оператора сообщение поступает на пейджинг – консоль, где оно кодируется и поступает на базовый передатчик, обслуживающий данную территорию. Время получения сообщения колеблется от 15 сек до 5 минут. При получении сообщения пейджер подает звуковой или вибрационный сигнал. Если сообщение не прочитано на экране дисплея, то пейджер один раз в две минуты будет сигнализировать об этом. Зона уверенного приема пейджинговой связи составляет 50 –100 км в зависимости от мощности передающей радиостанции.

Применение систем персонального радиовызова в значительной мере сокращает потерю времени на поиски требуемого абонента. Системы персонального радиовызова, рационально сочетающиеся с телефонной сетью, доступны для значительного числа абонентов. Они завоевали широкое признание во многих странах. В мире общее число абонентов таких систем исчисляется миллионами. Наряду с системами персонального радиовызова городского типа разработаны системы государственных и континентальных масштабов, использующие спутники.

В последнее время все большее распространение получают ведомственные, или локальные пейджинговые сети, построенные по радиальному принципу и используемые в рамках какого-либо предприятия для обеспечения оперативной связи руководства с сотрудниками. Такие сети предназначены для организации связи внутри зданий и на прилегающих к ним территориях. Типичные области применения локальных сетей: гостиницы, больницы, аэропорты, крупные промышленные предприятия. Основными особенностями ведомственных сетей является ограниченное число абонентов и сравнительно небольшой радиус действия (до 5 км).

Таким образом, внедрение систем персонального радиовызова во многие отрасли производства, торговли и т.п., позволяет повысить производительность труда на подвижных объектах, добиться экономии материально-трудовых ресурсов, обеспечить автоматизированный контроль технологических процессов, создать надежную систему управления транспортными средствами, распределенными на большой территории.

Американские компании SkyTelCorp и Motorola организовали разработку и выпуск пейджеров нового поколения, которые обеспечивают двухсторонний обмен сообщениями на частотах 1930 — 1990 МГц. В отличие от пейджинга возможно подтверждение получения сообщения и даже проведение некоторого подобия диалога. Двухсторонние пейджеры позволяют при помощи Internet посылать и принимать сообщения, передаваемые по электронной почте абонентам, постоянно находящимся в разъездах.

Сотовая радиосвязь.В мобильной радиотелефонной связи используется ультракоротковолновый диапазон радиоволн (450 – 1800 МГц). Радиоволны в этом частотном диапазоне распространяются только в пределах прямой видимости. Поэтому для увеличения дальности связи потребовались особые решения. В 70-е годы в Швеции появился новый принцип организации связи, который позволил увеличить дальность связи, число абонентов и повысить качество связи. Было предложено разбивать обслуживаемую территорию на небольшие участки, называемые сотами, или ячейками. Наиболее подходящей фигурой для построения сот является шестиугольник, так как, если антенну с круговой диаграммой направленности устанавливать в его центре, то будет обеспечен доступ почти ко всем участкам соты (Рис.5).

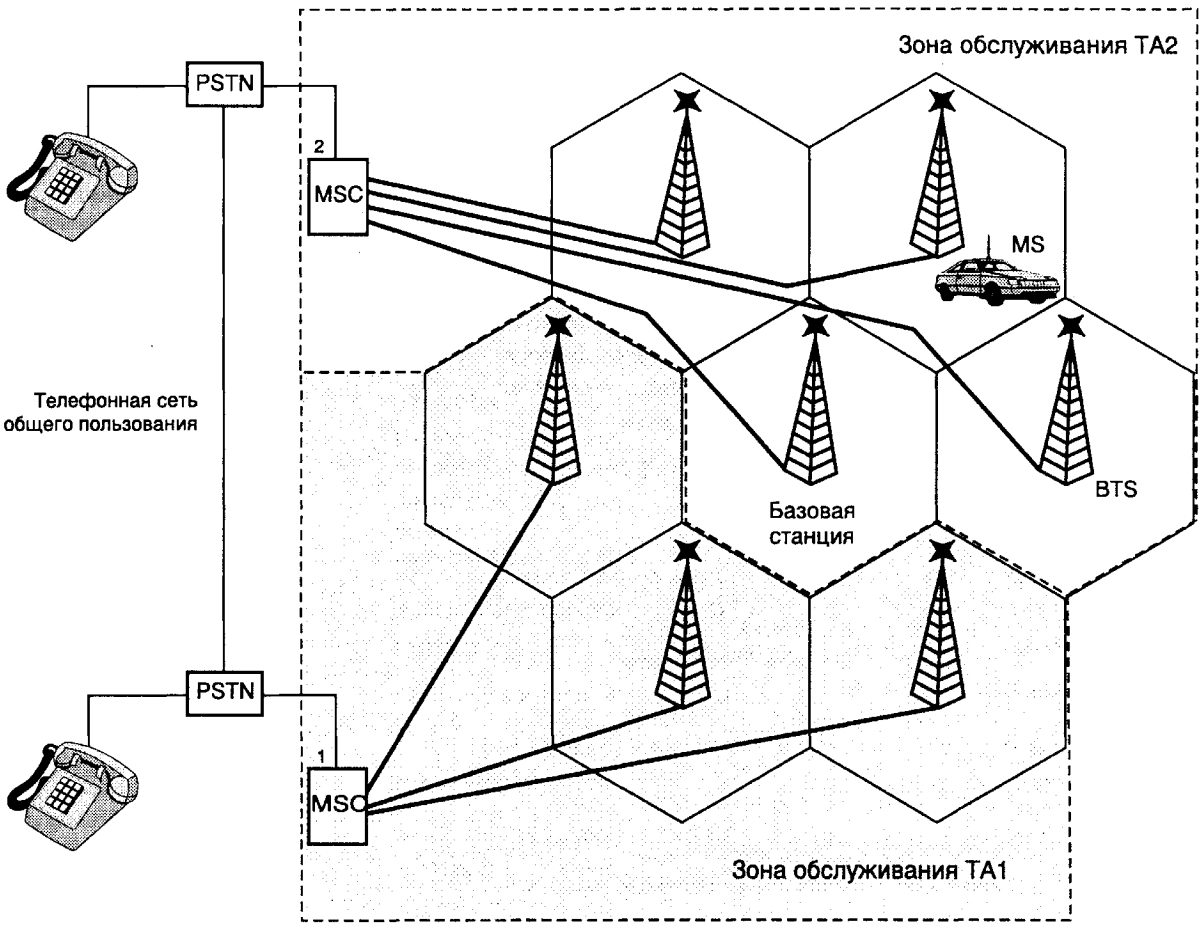

Рис.5. Структурная схема построения сети сотовой связи

MS — подвижная станция; BTS — базовая станция; MSC – центры коммутации, PSTN— телефонная сеть общего пользования

Вся территория, обслуживаемая сотовой связью, разбивается на равновеликие ячейки — соты. В центре каждой соты размещается базовая станция (BTS). Базовые станции соединяются кабелем с центрами коммутации (MSC), которые в свою очередь соединяются с АТС (PSTN). В соседних ячейках для переговоров используются разные частоты (f1, f2, f3). Эти же частоты используются через одну ячейку. В этом и заключается одно из преимуществ сотовой связи, которое позволяет на трех частотах обслуживать большую территорию. Радиотелефоны при перемещении из одной ячейки в другую автоматически настраиваются на нужную частоту. Настройка осуществляется контроллером базовой станции по уровню поступающего сигнала. Когда уровень сигнала, поступающего на базовую станцию становится ниже уровня для обеспечения качественной связи, базовые станции обслуживающие соседние ячейки ищут сигнал этого радиотелефона и при обнаружении сигнала заданного уровня переключают управле-

ние. Радиотелефон автоматически переходит на частоту другой ячейки. Размер соты колеблется от 500 метров до 15 километров

В настоящее время для организации связи используются аналоговые и цифровые системы связи, но последние постепенно вытесняют аналоговые системы. Наибольшее распространение в России получает стандарт GSM (Global Systems for Mobile Communications) — цифровой стандарт, который изначально разрабатывался как общий стандарт сотовой связи для объединенной Европы. С 1991 г. GSM получил широкое распространение в Европе, Австралии, Африке, на Среднем Востоке. Цифровое кодирование сигнала позволяет избежать помех и обеспечить конфиденциальность переговоров. Появление "двойников" у абонентов сетей GSM практически невозможно. Однако главное достоинство этого стандарта состоит в другом — он предоставляет пользователям возможность перемещения по городам и странам без изменения номера телефона. Правда, технология GSM требует большего, чем другие стандарты, числа базовых станций и, как следствие, - больших инвестиций для обеспечения хорошей связи. Другой недостаток заключается в том, что пока не удалось разработать технические решения, позволяющие реализовать скорость передачи данных свыше 9,6 кбит/с. А работать на канале с подобной пропускной способностью — не самое большое удовольствие.

В рамках стандарта GSM приняты пять классов подвижных станции: от модели 1-го класса с выходной мощностью до 20 Вт, устанавливаемой на транспортных средствах, до модели 5-го класса с максимальной выходной мощностью до 0,8 Вт. Цифровые системы сотовой подвижной связи представляют собой системы второго поколения. По сравнению с аналоговыми системами они предоставляют абонентам больший набор услуг и обеспечивают повышенное качество связи, а также взаимодействие с цифровыми сетями с интеграцией служб (ISDN) и пакетной передачи данных (PDN).

Стандарт GSM, кроме того, предоставляет своим пользователям ряд услуг, которые не реализованы (или реализованы не полностью) в других стандартах сотовой связи. К ним относятся:

- Использование интеллектуальных SIM-карт для обеспечения доступа к каналу и услугам связи;
- Шифрование передаваемых сообщений;
- Закрытый от прослушивания радиоинтерфейс;
- Аутентификация абонента и идентификация абонентского оборудования по криптографическим алгоритмам;
- Использование служб коротких сообщений, передаваемых по каналам сигнализации;

• Автоматический роуминг[1] абонентов различных сетей GSM в национальном и международном масштабах;

• Межсетевой роуминг абонентов GSM с абонентами сетей стандартов DCS1800, PCS1900, DECT, а также со спутниковыми сетями персональной радиосвязи (Globalstar, Inmarsat-P, Iridium).

Кроме перечисленных функций, стандарт GSM сегодня является наиболее развитым средством, которое позволяет связать персональный компьютер с Internet через сотовый телефон. Аппарат, весящий около 400 г, обеспечивает не только полный набор традиционных функций GSM-телефона, но и возможности факсимильной связи, электронной почты. Он также служит адресной книгой, блокнотом и терминалом для передачи кратких сообщений.

Стандарт GSM предусматривает работу передатчиков в двух диапазонах частот. Полоса частот 890 — 915 МГц используется для передачи сообщений с подвижной станции на базовую, а полоса частот 935 — 960 МГц — для передачи сообщений с базовой станции на подвижную (абоненту). В отведенной для приема/передачи полосе частот шириной 25 МГц размещается 124 канала связи.

Кроме стандарта GSM, в России используются стандарты NMT (450 МГц аналоговая связь), стандарт AMPS (800 МГц).

Перспективным считается использование многомодового телефонного аппарата, который позволит абоненту пользоваться одновременно системами спутниковой, сотовой и, так называемой, микросотовой связи, которая обеспечивает коммуникацию в пределах одного или нескольких близко расположенных зданий. Многомодовый аппарат безпроводной телефонии является, по сути, разновидностью средства сотовой телефонной связи и основан на использовании разных уровней доступа к абоненту:

- первый уровень (пикосота) — поддерживает доступ в пределах квартиры или одного этажа здания, характеризуется минимальной дальностью связи, максимальной телефонной нагрузкой и ограниченной мобильностью;
- второй уровень (микросота) позволяет осуществлять связь большей дальности, например, в пределах здания, но отличается меньшей нагрузкой;
- третий уровень (макросота) отличается большей мобильностью, чем первые две, осуществляет связь за пределами здания, но характеризуется более низкой полезной нагрузкой (системы сотовой связи типа GSM-900/1800);

---

[1] Слово роуминг (или роаминг) происходит от английского roam - бродить. Автоматический роуминг в GSM - это возможность перемещаться в пространстве (в том числе и за границу) со своим телефоном.

- четвертый уровень (гиперсота) осуществляет связь с абонентами, находящимися вне зоны действия обычных сотовых систем, например, на борту самолета или океанского лайнера.

К сожалению, развитие сотовых сетей в России сдерживается высокой стоимостью услуг. Сотовая связь здесь обходится дороже, нежели в большинстве других стран.

Многоканальная транкинговая радиосвязь.До появления сотовых телефонов в России для организации мобильной, адресной, производственной связи (милиция, нефтяные компании, железные дороги и т.д.) широко использовалась и продолжает развиваться многоканальная транкинговая система. Сегодня эти системы приобрели новые свойства и стали удобными для массового пользователя, составив серьезную конкуренцию сотовой связи.

Транкинг – это автоматическое предоставление по запросу для связи любого свободного канала. Транковая система представляет собой сеть, состоящую из нескольких вышек-ретрансляторов, оснащенных специальной аппаратурой, соединенной с городской телефонной сетью. Транкинговый телефон сочетает в себе функции мобильного сотового телефона и радиостанции. В зависимости от запросов потребителей и функционального предназначения, все радиостанции делятся на три типа. Носимые (портативные) — имеют небольшие размеры и вес, выходная мощность такой радиостанции не превышает 5 Ватт**.** Автомобильные — имеют габариты автомобильной магнитолы и специально сконструированы для установки в автомобилях. Выходная мощность — до 25 Ватт**.** Стационарные — предназначены для размещения в закрытых помещениях. Их выходная мощность — 40 Ватт

Несмотря на то, что сотовая связь имеет два бесспорных преимуществах по сравнению с транкинговой, обеспечивая двустороннюю (дуплексную) связь и малые размеры самого аппарата, и являясь более комфортной, она достаточно дорога за счет абонентской платы. Кроме того, транкинговая связь имеет и ряд других преимуществ для предпринимателя.

- Она позволяет организовать на предприятии корпоративную сеть для оперативного управления мобильным рабочим персоналом независимо от их местонахождения.
- Дает возможность осуществлять режим групповой связи и проводить селекторные совещания.
- В режиме индивидуальной связи обеспечивает необходимую конфиденциальность переговоров.
- Обеспечивает выход в городскую телефонную сеть

Современные системы транковой связи позволяют осуществлять односторонюю и двустороннюю связь емкостью до 2000 абонентов и обслуживать зону протяженностью до 100 км.

Спутниковые системы связи. Для передачи данных на большие расстояния используются медные и волоконнооптические кабельные линии, радиорелейные линии и спутниковые системы связи. Спутниковые системы связи в силу своих преимуществ занимают все большее место в системе передачи данных. Так, если в 1997 г. 30% международного трафика проходило по спутниковым каналам, а 70% — по наземным линиям, то в 2001 г. доля спутниковых каналов увеличилась до 42%. Кроме того, спутниковые системы позволяют реализовать такие применения информационных технологий, которые недоступны при других способах телекоммуникаций.

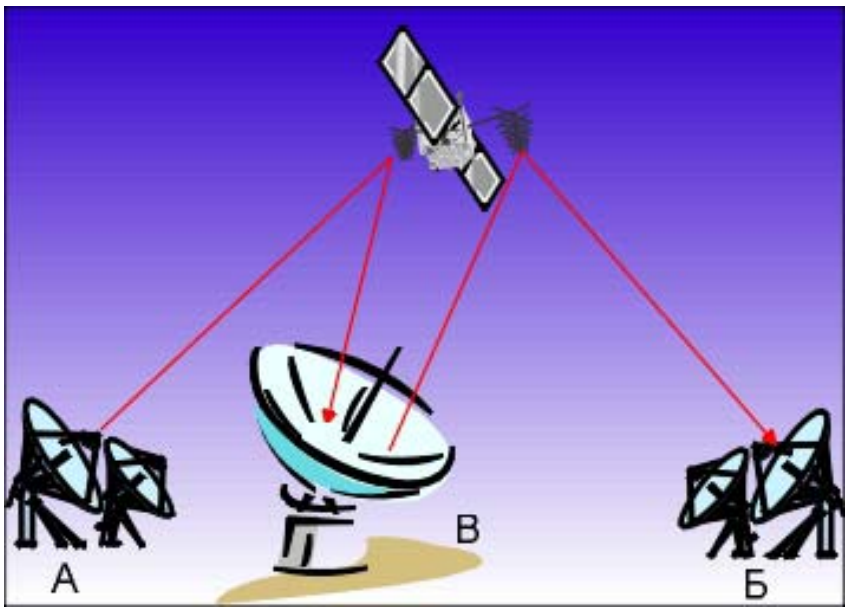

Рис.6. Спутниковая связь

Структура спутниковых каналов передачи данных проиллюстрирована на примере широкоизвестной системы VSAT (Very Small Aperture Terminal) (Рис.6). Наземная часть системы представлена совокупностью комплексов, в состав каждого из них входят центральная станция ЦС (В) и абонентские пункты АП (А,Б). Связь ЦС со спутником происходит по радиоканалу (пропускная способность 2 Мбит/с) через направленную антенну диаметром 1...3 м и приемопередающую аппаратуру. АП подключаются к ЦС с помощью многоканальной аппаратуры через телефонные линии или по радиоканалу через спутник. Те АП, которые соединяются по радиоканалу (это подвижные или труднодоступные объекты), имеют свои антенны, и для каждого АП выделяется своя частота. ЦС передает свои сообще-

ния широковещательно на одной фиксированной частоте, а принимает на частотах АП.

Спутниковые системы, ориентированные на предоставление услуг радиотелефонной связи и передачи данных, разделяют на несколько типов. В основу их классификации положены следующие признаки: тип используемых орбит, вид предоставляемых услуг и принадлежность системы к службе.

Спутники могут находиться на геостационарных (высота 36 тысяч км) или низких орбитах (от 200 до 12000 км). При геостационарных орбитах заметны задержки на прохождение сигналов (туда и обратно около 520 мс). Возможно покрытие поверхности всего земного шара с помощью четырех спутников. В низкоорбитальных системах обслуживание конкретного пользователя происходит попеременно разными спутниками. Чем ниже орбита, тем меньше площадь покрытия и, следовательно, нужно или больше наземных станций, или требуется межспутниковая связь, что естественно утяжеляет спутник. Число спутников также значительно больше (обычно несколько десятков).

Спутники на геостационарных орбитах оптимальны для систем радио— и телевизионного вещания, где задержки не сказываются на качественных характеристиках сигналов. Однако они не могут вследствие задержки сигнала обеспечить высокое качество телефонной связи. Зона охвата геостационарных КА не включает в себя высокоширотные районы (выше 76,50 с.ш. и ю.ш.), т. е. действительно глобальное обслуживание не гарантируется. Поэтому для обеспечения телефонной связи используются средневысотные и низковысотные спутники.

Низкоорбитальные системы связи подразделяются по виду предоставляемых услуг на системы передачи данных , радиотелефонные системы и системы широкополосной связи.

В соответствии с Регламентом радиосвязи различаются три основные службы — фиксированная спутниковая служба (ФСС), подвижная спутниковая служба (ПСС) и радиовещательная спутниковая служба (РСС).

Сегодня наиболее интенсивно осваиваются низкие наклонные и полярные орбиты высотой 700—1500 км, а также экваториальные высотой 2 тыс. км. Системы с низкими наклонными и полярными орбитами существуют уже около 30 лет и применяются для организации мобильной и персональной связи, для научно-исследовательских целей, дистанционного зондирования, навигации, метеорологических наблюдений, фотографирования поверхности Земли. На их основе также созданы системы слежения за перемещением особо важных грузов, предметов и людей, системы диспетчеризации общественного и специального транспорта, системы обеспе-

чения безопасности стационарных объектов (коттеджей, офисов) и автомобильные охранные системы.

Спутники на низких орбитах обладают значительными преимуществами перед другими КА по энергетическим характеристикам, но проигрывают им в продолжительности сеансов связи и времени активного существования КА. Если период обращения спутника составляет 100 мин, то в среднем 30% времени он находится на теневой стороне Земли. Аккумуляторные бортовые батареи испытывают приблизительно 5 тыс. циклов зарядки/разрядки в год, вследствие чего срок их службы, как правило, не превышает 5—8 лет.

Примерами российских систем спутниковой связи с геостационарными орбитами могут служить системы Инмарсат и Runnet. Так, в Runnet применяются геостационарные спутники "Радуга". Один из них, с точкой стояния 85 градусов в.д., охватывает почти всю территорию России. В качестве приемопередающей аппаратуры (ППА) используются станции, работающие в сантиметровом диапазоне волн (6,18...6,22 ГГц и 3,855...3,895 ГГц соответственно). Диаметр антенн 4,8 м.

Примеры сетей с низкоорбитальными спутниками — система глобальной спутниковой телефонной связи "Глобалстар". В систему входит 48 низкоорбитальных (высота 1400 км) спутников. Каждая наземная станция имеет одновременно связь с тремя спутниками. У спутника шесть сфокусированных лучей по 2800 дуплексных каналов каждый. Обеспечиваются телефонная связь для труднодоступных районов, навигационные услуги, определение местонахождения подвижных объектов. Другая глобальная спутниковая сеть Iridium, имеющая и российский сегмент, включает 66 низкоорбитальных спутников, диапазон частот 1610-1626,5 МГц. В российской системе Глоснасс — 24 спутника.

2.4.3. Типы и классификация компьютерных сетей

Компьютерные коммуникации служат для дистанционной передачи данных с одного компьютера на другой и являются не только самым новым, но и самым перспективным видом телекоммуникаций. Они обладают рядом неоспоримых преимуществ по сравнению с традиционными средствами общения людей и передачи информации — позволяют не только передавать, получать, но и хранить, и обрабатывать информацию. Проблема передачи информации с одного компьютера на другой возникла практически одновременно с появлением компьютеров. Можно, конечно, передавать информацию с помощью внешних носителей информации – магнитных или компакт – дисков. Но этот способ достаточно медленный и неудобный. Значительно лучше соединить компьютеры кабелем, загрузить специальную программу для передачи информации и, таким образом, по-

лучить простейшую компьютерную сеть. Например, для создания прямого соединения компьютеров, работающих под управлением операционной системы Windows, не требуется специального программного и аппаратного обеспечения.

При объединении нескольких компьютеров процесс обмена информацией становится сложнее, однако принципы соединения остаются те же, что и для двух компьютеров. Для подключения компьютеров к линиям связи используются модемы или сетевые карты, если связь осуществляется по специальным выделенным линиям. Кроме того, на каждом компьютере устанавливаются программы для работы в сети. Таким образом***: компьютерная сеть*** *— это объединение компьютеров с помощью модемов, линий связи и программ, обеспечивающих обмен информацией.* Компьютерные сети позволяют осуществлять новую технологию обработки информации и совместного использования ресурсов – аппаратных, программных и информационных. Новая технология получила название – распределенная обработка данных.

В соответствии с используемыми протоколами компьютерные сети разделяют на локальные и распределенные (глобальные и территориальные). ***Локальной*** называется компьютерная сеть, объединяющая компьютеры, расположенные в одном помещении, в одном здании или в соседних зданиях. В локальной сети используют единый комплект протоколов для всех пользователей. Сегодня наиболее распространенными сетевыми операционными системами, обеспечивающими работу пользователей в сети по единому протоколу, являются NetWare фирмы Novell, Windows NT Server фирмы Microsoft и сетевые ОС семейства UNIX. Все большее распространение получает система Linux. Важно отметить, что эта операционная система распространяется свободно, т.е. является free – ware программным обеспечением.

Если же соединенные компьютеры находятся в разных частях города, в разных городах или странах, то такие сети называются ***распределенными.*** К распределенной сети могут подключаться не только отдельные компьютеры, но и локальные сети. Распределенные сети мирового масштаба называют ***глобальными***.

Самой известной глобальной сетью является INTERNET. Основой функционирования глобальной сети ИНТЕРНЕТ является базовая семиуровневая эталонная модель взаимосвязи открытых систем — протокол TCP/IP (Transfere Communication Protocol /Internet Protocol).

Основное различие между всеми названными сетями заключается в управлении доступом к информации и в том, как происходит обмен данными. В зависимости от способов управления доступом и обмена данными сети подразделяются по топологии и технологии. Последовательно рас-

смотрим представление данных в сетях, виды используемых топологий и технологий.

Топология — это схема соединения каналами связи компьютеров или узлов сети между собой. Используются следующие виды соединений: общая шина, звезда, кольцо.

Метод доступа — это технология, определяющая использование канала передачи данных, соединяющего узлы сети на физическом уровне. Самыми распространенными технологиями сегодня являются Ethernet, Arcnet и Token - Ring (говорящее кольцо).

Сеть шинной топологии представляет собой подключение компьютеров вдоль одного кабеля. Технологией обеспечивающей такой способ соединения компьютеров является Ethernet — метод доступа с прослушиванием несущей частоты и обнаружением конфликтов. При этом методе доступа узел, прежде чем послать данные по каналу связи, прослушивает его, и только убедившись, что канал свободен, посылает пакет. Если канал занят, узел повторяет попытку передать пакет через случайный промежуток времени. Данные, переданные одним узлом сети, поступают во все узлы, но распознает и принимает их компьютер, которому предназначены данные. В качестве линий связи в топологии Ethernet используются кабель типа витая пара, коаксиальные и оптоволоконные кабели. Эта технология обеспечивает дуплексную передачу данных со скоростями от 10 до 100 Мбит/сек. Шинная топология позволяет эффективно использовать пропускную способность канала, устойчива к неисправностям отдельных узлов и дает возможность наращивания сети.

Сеть кольцевой топологии использует в качестве канала связи замкнутое кольцо из компьютеров, соединенных коаксиальным или оптическим кабелем. Технология доступа в сетях этой топологии реализуется методом передачи маркера. Маркер – это пакет, снабженный специальной последовательностью бит (его можно сравнить с конвертом для письма). Он последовательно предается по кольцу от компьютера к компьютеру в одном направлении. Каждый узел ретранслирует передаваемый маркер. Компьютер может передать свои данные, если он получил пустой маркер. Маркер с пакетом передается, пока не обнаружится компьютер, которому предназначен пакет. В этом компьютере данные принимаются, но маркер движется дальше и возвращается к отправителю. После того, как отправивший пакет компьютер убедится, что пакет доставлен адресату, маркер освобождается. Скорость передачи данных в таких сетях достигает 4 Мбит/сек.

При звездообразной топологии все компьютеры сети подключаются к центральному компьютеру отдельной линией связи. Центральный компьютер управляет рабочими станциями, подключенными к нему через концен-

тратор, который выполняет функции распределения и усиления сигналов. Надежность работы сети при такой топологии полностью зависит от центрального компьютера. Метод доступа реализуется с помощью технологии Arcnet. Этот метод доступа также использует маркер для передачи данных. Маркер передается от компьютера к компьютеру в порядке возрастания адреса. Как и в кольцевой топологии, каждый компьютер регенерирует маркер. Данный метод доступа обеспечивает скорость передачи данных 2 Мбит/сек.

В настоящее время существуют еще более скоростные, но и более дорогие варианты организации вычислительных сетей в виде распределенного двойного кольца на базе оптико-волоконных каналов (вариант FDDI) и витой пары (вариант CDDI). Данные варианты организации и технологии

построения предназначаются для больших корпоративных вычислительных сетей.

Локальные сети могут интегрироваться в более сложные единые сетевые структуры. При этом, однотипные по используемым в них аппаратуре и протоколам сети, объединяются с помощью общих для соединяемых сетей узлов-«мостов», а разнотипные сети (работающих под управлением различных операционных систем) объединяются с помощью общих узлов-***«шлюзов».***

Шлюзы могут быть как аппаратными, так и программными. Например, это может быть специальный компьютер (шлюзовой сервер), а может быть и компьютерная программа, шлюзовое приложение. В последнем случае компьютер может выполнять не только функции шлюза, но и функции рабочей станции.

Интеграция нескольких сетей в единую систему требует обеспечения межсетевой маршрутизации информационных потоков в рамках единой сети. Межсетевая маршрутизация организуется путем включения в каждую из объединяемых подсетей специальных узлов-***«маршрутизаторов»*** (часто функции «маршрутизаторов» и «шлюзов» интегрируются в одном узле). Узлы-«маршрутизаторы» должны «распознавать», какой из пакетов относится к «местному» трафику сети станции-отправителя, а какой из них должен быть передан в другую сеть, входящую в единую интегрированную систему.

При подключении локальной сети предприятия к глобальной сети особое внимание обращается на обеспечение информационной безопасности. В частности, должен быть максимально ограничен доступ в сеть для внешних пользователей, а также ограничен выход во внешнюю сеть сотрудников предприятия. Для обеспечения сетевой безопасности устанавливают ***брандмауэры***. Это специальные компьютеры или компьютерные програм-

мы, препятствующие входу в локальную сеть и несанкционированной передаче информации.

Пользователи (клиенты) локальной сети могут иметь различные права доступа и полномочия по обработке информации, хранящейся в базах данных коллективного пользования. Полномочия пользователей локальной сети определяются правилами разграничения доступа, а совокупность приемов распределения полномочий называется политикой сети. Управление сетевыми политиками называется администрированием сети, которым занимается уполномоченное лицо – ***системный администратор***.

Порядок доступа и использования ресурсов сети Интернет определяет организация или уполномоченное лицо – ***провайдер***.

Концепция открытых информационных систем. Для реализации технологии распределенной обработки данных необходимо согласовать правила использования и взаимодействия аппаратных ресурсов, изготовленных разными фирмами, программных ресурсов, созданных разными языковыми средствами и информационных ресурсов, имеющих разные форматы представления данных. В настоящее время основной тенденцией в области информационных технологий и компьютерных коммуникаций является идеология открытых систем. Идеологию открытых систем реализуют в своих последних разработках все ведущие фирмы – поставщики средств вычислительной техники, передачи информации, программного обеспечения и разработки прикладных информационных систем. Их результативность на рынке информационных технологий определяется согласованной научно-технической политикой и реализацией стандартов открытых систем.

Что понимается под открытыми системами в данном контексте? «Открытая система — это система, которая состоит из компонентов, взаимодействующих друг с другом через стандартные интерфейсы, службы и форматы данных». Сущность технологии открытых систем заключается в обеспечении следующих задач:

- Унификации обмена данными между различными компьютерами;
- Переносимости прикладных программ между различными компьютерами;
- Мобильности пользователей, т.е. возможности пользователей переходить с одного компьютера на другой, независимо от его архитектуры и используемых программ без необходимости переобучения специалистов.

Основой, обеспечивающей реализацию открытых систем служит совокупность стандартов, с помощью которых унифицируется взаимодействие аппаратуры и всех видов программного обеспечения: языков программи-

рования, средств ввода – вывода, графических интерфейсов, систем управления базами данных, протоколов передачи данных в компьютерных сетях.

2.4.4. Технологии распределенной обработки данных. Модель клиент-сервер

Информационные системы, построенные на базе компьютерных сетей, обеспечивают решение следующих задач: хранение данных, обработка данных, организация доступа пользователей к данным, передача данных и результатов обработки данных пользователям. Потребность в данных коллективного пользования в последнее время все более возрастает. Это и послужило причиной усиливающегося внимания к различным системам распределенной обработки данных.

Существует несколько понятий в этой области, которые необходимо определить более точно. Вначале выделим эти понятия:

- распределенная обработка данных;
- базы данных с сетевым доступом;
- архитектура «клиент-сервер»;
- распределенные базы данных.

Под распределенной обработкой данных понимают обработку приложений несколькими территориально распределенными компьютерами.

Технология распределенной обработки данных базируется на двух концепциях. Первая концепция носит название «файл – сервер», а вторая — «клиент сервер».

Сервер — это машина, обеспечивающая функционирование той части сетевой версии СУБД, которая осуществляет управление данными в терминах базы данных и называется *сервером файлов или файл-сервером* (File Server).

Клиент — задача, рабочая станция или пользователь компьютерной сети. В процессе обработки данных клиент может сформировать запрос на сервер для выполнения сложных процедур, чтение файла, поиск информации в базе данных и т. д.

Предполагается, что центральная машина (сервер) обладает жестким диском достаточно большой емкости, на котором хранится совместно используемая централизованная база данных. Все другие машины сети выполняют функции *рабочих станций* (клиентов), с помощью которых поддерживается доступ пользователей системы к централизованной базе данных. В соответствии с пользовательскими запросами файлы базы данных передаются на рабочие станции, где в основном и производится их обработка. Рабочая станция должна иметь достаточно ресурсов для обеспечения приемлемого уровня реактивности при обработке пользовательских запросов.

Первая концепция распределенной обработки данных реализуется следующим образом. В сети имеется главный компьютер, который называется

файловым сервером. Сервер предоставляет в совместное пользование информационные (файлы, базы данных) и аппаратные ресурсы (принтеры, модемы). Сетевая операционная система, обеспечивающая взаимодействие пользователей с сервером состоит из двух частей: одна (основная) часть находится на файловом сервере, а вторая (оболочка) устанавливается на компьютерах сети (рабочих станциях). Оболочка обеспечивает взаимодействие (является интерфейсом) между программами рабочей станции и сервера. Файловый сервер в рамках такой архитектуры используется только как хранилище данных, а их обработка осуществляется на компьютере пользователя (рабочей станции).

В рамках концепции «клиент – сервер» сервер используется не только как хранилище программ и данных, но и как вычислительная среда. Программное обеспечение в рассматриваемой модели состоит из двух взаимосвязанных программ: «файл-сервера» и программы клиента – пользователя. Программа – клиент формирует запрос и посылает его файл – серверу (программе), установленной на компьютере с общим доступом. Обработка данных и осуществляется на мощном компьютере общего пользования, а на компьютере-клиенте с помощью соответствующего протокола отображаются результаты выполненного запроса. При этом постарайтесь не запутаться в терминах: «сервером» называют как компьютер, так и программное обеспечение.

Системы баз данных, построенные с помощью сетевых версий, иногда неправомерно называют распределенными базами данных, в то время как они фактически являются лишь распределенным (сетевым) доступом к централизованной базе данных. Такие системы создаются на основе оборудования и программного обеспечения различных типов локальных вычислительных сетей.

2.5. Интернет, Интранет, Экстранет

2.5.1. Эталонная модель взаимодействия открытых систем

Протоколы – это специальные стандарты, которые обеспечивают совместимость программ и данных (программы поддержки протоколов) и аппаратных средств (аппаратные протоколы) при взаимодействии компьютеров в сетях. Программы поддержки протоколов часто называют просто «протокол», а функции поддержки аппаратных протоколов физически выполняют специальные устройства – интерфейсы (разъемы, кабели и т.п.).

Главным международным стандартом сетевых взаимодействий, принятым в 1983 году является базовая семиуровневая эталонная модель взаимосвязи открытых систем. Она получила название протокол TCP/IP (Transfere Communication Protocol /Internet Protocol). Каждому уровню в модели соответствуют различные сетевые операции, оборудование и протоколы.

Рассмотрим функции, которые выполняет каждый из семи уровней:

1-й, физический уровень осуществляет физические соединения для передачи данных между объектами, а также кодирование и декодирование данных;

2-й, уровень звена данных (канальный) управляет передачей данных по каналу

3-й, сетевой уровень «прокладывает» путь между системой отправителем и системой адресатом, обеспечивает маршрутизацию сообщения;

4-й, транспортный уровень управляет передачей информации по этому пути.

5-й, сеансовый уровень предназначен для организации и управления сеансами взаимодействия прикладных процессов (обменом данными);

6-й, уровень представления данных (представительный) подготавливает информацию в таком виде, в каком требуют прикладные процессы. Так, если, например, используется дисплей, то информация формируется в виде страницы с заданным числом строк определенной длины;

7-й, прикладной уровень связан с прикладными процессами, обеспечивает соответствующий сервис пользователю (http, ftp, smtp).

Теперь остановимся на способах передачи данных в сетях.

Данные обычно содержатся в больших по размерам файлах. Однако, существует две причины, затрудняющие передачу больших блоков данных. Во-первых, такой блок, отправляемый с одного компьютера, заполняет весь канал и «связывает» работу всей сети, т.е. препятствует взаимодействию остальных компонентов сети. Во-вторых, возникновение ошибок при передаче крупных блоков приведет к повторной передаче всего блока. По этим причинам файлы разбивают на небольшие управляемые пакеты или кадры.

Пакет – основная единица информации в компьютерных сетях. При разбиении файлов на пакеты скорость их передачи возрастает настолько, что каждый компьютер в сети получает возможность передавать и принимать данные практически одновременно с остальными компьютерами. На компьютере – получателе пакеты накапливаются и выстраиваются в должном порядке для восстановления исходного файла.

При разбиении файлов на пакеты сетевая операционная система добавляет к каждому пакету специальную управляющую информацию. Она обеспечивает:

- Передачу исходных данных небольшими пакетами (от 512 байт до 4 Кбайт);
- Сбор данных в надлежащем порядке на компьютере – получателе;
- Проверку данных на наличие ошибок;

Пакеты могут содержать различные сведения:

- Собственно передаваемую информацию;
- Данные и команды, управляющие компьютером;
- Коды управления сеансом;
- Адрес источника и адрес получателя;
- Инструкцию о маршруте пакета;

Компоненты пакета группируются в три раздела: заголовок, данные и трейлер. В заголовке передается сигнал о передаче пакета, адрес отправителя и получателя и синхронизирующий сигнал. Вторая часть пакета — передаваемые данные. Трейлер содержит информацию для проверки ошибок (контрольную сумму пакета).

2.5.2. Структура, информационные ресурсы и принципы работы в сети Интернет

Интернет — это всемирная компьютерная сеть, объединяющая миллионы компьютеров по всему миру. Фактически Интернет является конгломератом многих глобальных, региональных, университетских и учрежденческих сетей, а также сетей, обслуживаемых коммерческими провайдерами. В таблице 7 представлена история создания и развития сети Интернет.

Таблица 7

История создания и развития компьютерной сети Интернет

Год	Событие
1962 год	Джон Ликлайдер (John Licklider) концепция «Галактической сети» (Galactic Network);
1962 год	Проект по созданию сети, связывающей компьютеры оборонительных учреждений в Управлении перспективных исследований и разработок Министерства обороны США (Advanced Research Projects Agency, ARPA)
1969 год	Создание сети ArpaNet, в основе функционирования которой лежали принципы, на которых позже был построен Интернет;
1972 год	Появилось первое приложение — электронная почта (E-Mail). Рэй Томлинсон (Ray Tomlinson);
конец 70-х	Разработан стек протоколов для сетевого взаимодействия TCP/IP.
1983 год	ARPAnet полностью перешла на стек протоколов TCP/IP;
середина 80-х	Создана NFSnet (сеть Национального научного фонда США (NFS). Основу сети составили пять СуперЭВМ;
1987 год	Создан NFSnet Backbone (базовая часть или хребет сети).
1988 год	К NFSnet присоединяются Канада, Дания, Финляндия, Франция, Норвегия и Швеция. 1990 год — ликвидирована ARPAnet
1991 год	В Европейской лаборатории физики частиц (European Laboratory for Participle Physics,CERN) Тимоти Бернерсом-Ли (Timothy Berners-Lee) разработана служба «Всемирная паутина» (World Wide Web, WWW).
1993 год	К NFSnet подключилась Россия

В Интернет нет центрального управляющего органа, а следовательно, выход любого узла из строя или появление нового узла не оказывают никакого влияния на общую работоспособность сети. Однако архитектура коммуникационной системы Интернет имеет вполне определенный иерархический характер. В этой иерархической архитектуре ограниченный набор дорогостоящих магистральных каналов с высокой пропускной способностью, составляющих так называемую опорную или базовую сеть, соединяет между собой сети со средней пропускной способностью, к которым, в свою очередь, подключаются отдельные организации. Понятно, что для сети такого масштаба и организации очень остро стоит проблема адресации и маршрутизации.

Связь между компьютерами в Интернет осуществляется посредством комплекса сетевых протоколов TCP\IP. Для идентификации компьютеров (host-узлов), подключенных к Интернет, и межсетевой маршрутизации пакетов каждому из компьютеров присваивается уникальный четырехбайтный адрес (IP-адрес). Запись IP-адреса состоит из четырех сегментов, разделенных точками. Каждый сегмент представляет собой десятичное число в диапазоне от 0 до 255, что соответствует одному байту. Примером записи IP-адреса является строка: 197.25.17.34. Числа 0,127 и 255 зарезервированы для специальных нужд и не могут быть использованы в обычном IP-адресе.

Сегменты IP-адреса делятся на две части. Левая — сетевая часть IP-адреса — обозначает сеть или иерархию подсетей, на нижнем уровне которой находится адресуемый компьютер. Правая — машинная часть IP-адреса — указывает на конкретный номер host-компьютера в сети нижнего уровня иерархии. Количество сегментов в сетевой и машинной части IP-адреса зависит от того, к какому классу сети он принадлежит.

Номера сетей выделяются административным центром InterNIC (Network Information Center) научным организациям, учебным заведениям, коммерческим структурам и пр. по их официальным запросам. Данные номера являются постоянными, или статическими. При этом, присваивание номеров конкретным машинам пользователей происходит непосредственно в самих организациях.

Каждый Интернет-провайдер, компания, предоставляющая доступ в Интернет индивидуальным клиентам (Internet service provider, ISP), предварительно получив комплект постоянных номеров сетей в NIC и создав на их базе набор (пул) IP-адресов, выделяет клиенту при каждом его подключении один из них. В этом случае, IP-адрес клиента рассматривается как временный, или динамический. Данный механизм использования адресов Интернет в условиях множества непостоянных клиентов сети позволяет экономить ограниченное пространство статических адресов, которое в настоящее время составляет примерно два миллиона.

В силу того, что числовые IP-адреса host-узлов, обеспечивающие межсетевую маршрутизацию пакетов на втором уровне протоколов TCP\IP, не очень удобны

для пользователей (отметим, что аппаратные адреса сетевых устройств первого уровня протоколов TCP\IP полностью скрыты от них), IP-адреса были дополнены иерархической системой символических адресов компьютеров, работа с которой обеспечивается в Интернет особой сетевой службой доменных имен DNS (Domain Name System).

Доменная система имен — это весьма сложная распределенная база данных, содержащая информацию о компьютерах (в основном, о компьютерах-серверах), включенных в Интернет. К информации данной базы относятся символьные адреса (имена) компьютеров, их числовые IP-адреса, данные для маршрутизации почты и многое другое. Основной задачей службы DNS при сетевом взаимодействии является поиск адресуемых компьютеров с преобразованием символьных адресов в числовые IP-адреса и наоборот.

Пространство имен доменной системы представляет собой дерево с корневым каталогом. Под корневым каталогом располагаются домены верхнего уровня, ниже — второго и так далее. Таким образом, доменная система имен выполняет еще одну функцию — обеспечивает иерархическую организацию адресов компьютеров, входящих в сеть, по принципу отличному от иерархии их физического подключения. Для доменного имени «info.isea.ru» ru является именем домена верхнего уровня, isea — именем домена второго уровня, а info — именем домена третьего уровня. При этом в качестве домена самого нижнего уровня выступает символическое имя компьютера.

Имена домен DNS верхнего уровня строго определены и могут быть трехили двух-символьными. Первый тип домен верхнего уровня исторически предназначался для организаций, расположенных на территории США, и информировал об их организационно-политической принадлежности.

К трехсимвольным доменам DNS верхнего уровня относятся следующие:

COM — коммерческие организации;

EDU — учебные заведения;

NET — организации, предоставляющие сетевые услуги;

MIL — военные учреждения;

GOV —- правительственные учреждения;

ORG — некоммерческие организации;

INT — международные организации.

Двухсимвольные домены DNS верхнего уровня предназначаются для других стран и совпадают с кодами ISO. Например, RU — Россия, US — США, CA — Канада, DE — Германия, FR — Франция.

Имена доменов второго уровня на территории США выделяются административным центром сети Интернет InterNIC. В Европе заявки на получение доменных имен второго уровня принимает RIPE (Reseaux IP Europeens). При таком централизованном выделении имен второго уровня дается гарантия того, что выданный домен второго уровня уникален в пределах соответствующего домена перво-

го уровня. Организация вправе самостоятельно делить полученный домен второго уровня на поддомены, обеспечивая при этом уникальность новых имен на нижних уровнях иерархии.

В России регистрация доменных имен осуществляется Всероссийским научно-исследовательским институтом развития открытых систем (ВНИИРОС).

Пользователи, подключенные к Интернет, получают доступ ко всем ресурсам сети. Они могут с помощью программных средств telnet, rlogin и т. п. осуществить регистрацию и выполнить свою работу на одном из удаленных многопользовательских компьютеров сети; совместно с другими пользователями объединять свои файловые системы в рамках распределенной в пространстве сетевой файловой системы NFS (Network File System) или воспользоваться услугами доступной практически в любой точке земного шара электронной почты E-mail, которая почти по всем параметрам превосходит обыкновенную почту.

В Интернет существует множество, так называемых, FTP-серверов, на которых хранится огромное количество файлов. Пользователь, соединившись с одним из таких серверов с помощью сетевой службы FTP (File Transfer Protocol), получает возможность поиска на сервере и переноса на собственный компьютер необходимой ему информации. Правда, иногда, для того чтобы копировать файлы, необходимо иметь пользовательский бюджет на данном сервере, но многие FTP-серверы позволяют регистрироваться под пользовательским именем anonymous и с адресом электронной почты в качестве пароля (такие серверы называются анонимными FTP-серверами).

Для облегчения поиска необходимой информации в Интернет существует отдельная сетевая служба Archie. Данная служба обеспечивает поиск по ключевым словам в специальной регулярно обновляемом базе данных о файлах, доступных по анонимному FTP.

Служба WAIS (Wide Area Information Server) аналогична Archie, однако позволяет проводить более глубокий поиск не только по именам и общим характеристикам файлов, но и по их содержанию.

Сервисная система Gopher связывает все три вышеназванные службы воедино. Средства поиска Gopher хорошо совмещаются с Archie и WAIS, а средства ее пользовательского интерфейса позволяют просматривать и копировать документы, найденные в результате поиска.

Для представления хранимой в Интернет информации в удобной для пользователя. форме существует специальная сетевая служба WWW (World Wide Web), которая представляет собой своего рода распределенную по множеству узлов базу различного рода данных, построенную на гипертекстовой технологии. Для поиска в этой базе используются различные поисковые серверы, например, Yandex, Rambler, Lycos, Yahoo и др.

Помимо названных сетевых служб в Интернет существуют и другие службы, в частности, IRC и ICQ, обеспечивающие возможность интерактивного общения

удаленных пользователей сети. С помощью IRC (Internet Relay Chat) множество пользователей могут заходить на так называемые «каналы» («комнаты», «виртуальные места», как правило, имеющие тематическую направленность), чтобы «поговорить» с группой людей или с конкретным человеком. Служба ICQ (I Seek You) очень популярный в последнее время Интернет-пейджер, позволяющий в любое время узнать, находится ли некоторый пользователь в сети, «поговорить» с ним, обменяться файлами и т. д.

Воспользоваться услугами всех перечисленных выше сетевых служб можно при наличий у пользователя специальной программы-клиента. Отметим, что некоторые из таких программ-клиентов носят интегральный характер, обеспечивая взаимодействие пользователя с несколькими сетевыми службами. Например, Web-браузер фирмы Netscape позволяет работать, не только с WWW, но и с FTP, с GOPHER и даже с некоторыми другими службами.

2.5.3. Интранет и Экстранет

Распределенные сети, работающие по технологии и принципу организации сети INTERNET, и использующие протокол TCP/IP, но принадлежащие одной организации получили название INTRANET. Фирмы, которым необходимо делиться информацией с деловыми партнерами, часто организуют общую базу данных и объединяют ИНТРАСЕТи, работающие на основе протокола TCP/IP в сети называемые ЭКСТРАНЕТ. Обмен данными в сетях Интранет и Экстранет осуществляется по закрытым, выделенным каналам связи, доступным только работникам предприятий – владельцам сети.

2.6.Информационные технологии электронного бизнеса

Сегодня мы становимся свидетелями рождения нового сектора в экономике, который все чаще называют электронным бизнесом, Интернет-экономикой, Интернет-бизнесом, электронной коммерцией (ЭК). Темпы развития этого сектора высоки, его оборот ежегодно удваивается. По данным Центра исследования электронной коммерции, функционирующего под эгидой Высшей школы бизнеса Университета штата Техас, суммарный доход компаний, предлагающих услуги через Интернет, а также занимающихся технической поддержкой Сети, превышает 500 млрд. долл. Многие фирмы используют "Всемирную паутину" (Web), как транспортную среду для осуществления товарных и финансовых операций.

На мировом рынке Интернет-коммерции доминируют США (примерно 73% всего оборота). На долю Европы приходится лишь 16%, а на азиатские страны — 7%, все остальные регионы — 4%.

Доля рынка ЭК не только в Восточной Сибири, но и в России невелика, поэтому о существенном влиянии на экономику говорить пока рано, хотя

все современные виды электронной коммерции уже существуют и в России.

Прежде всего необходимо определиться с понятием электронной коммерции. Существует несколько определений электронной коммерции. С одной стороны, это получение прибыли от ведения хозяйственной деятельности по предоставлению новых видов электронных услуг, продажи компьютерной техники и программного обеспечения. С другой стороны, под электронной коммерцией понимается проведение операций с партнерами и клиентами, а также различные платежи и расчеты с использованием новых информационных сред и различного рода электронных сетей. В данном аспекте нас интересует второй случай.

Более строгое определение электронной коммерции дано в специальном документе Администрации президента США, объявляющем мораторий на дополнительное налогообложение сделок, заключенных через Интернет. В нем электронной коммерцией (ЭК) называется любая транзакция, совершенная через компьютерную сеть, в результате которой право собственности или право пользования вещественным товаром или услугой было передано от одного лица к другому. Данное определение на наш взгляд является наиболее полным.

Рассмотрим основные понятия, связанные с электронной коммерцией.

Такой вид ЭК как ***B2B (Business-to-Business)*** или бизнес-бизнес — представляет собой ЭК между предприятиями, основной особенностью этого вида ЭК является автоматическое взаимодействие в электронном виде систем управления предприятием.

B2C (Business-to-Consumer, Customer) или бизнес-потребитель — вид ЭК, связанный с электронными коммерческими операциями, производимыми между предприятием и потребителями. Предприятия на базе Интернета конкурируют или сотрудничают с традиционными предприятиями в сфере розничной торговли. Функционируют они следующим образом. Компания-продавец размещает на своем Web узле интерфейс, с помощью которого потребитель может разместить заказ в ее системе управления предприятием. Системы ЭК позволяют покупателю не общаться с продавцом, не тратить время на беготню по магазинам, иметь более полную информацию о товарах. Продавец, в свою очередь, может быстрее реагировать на изменение спроса, анализировать поведение покупателей, экономить средства на персонале, аренде помещений.

Преимуществами использования ЭК можно назвать следующие.

- Простота развертывания приложений и управление ими. Использовать Web достаточно просто. Покупателям следует лишь освоить программу для просмотра, и они сразу получают доступ к средствам электронной торговли.

- Уменьшение времени на доставку информации о товаре потребителю — одно из необходимых условий ведения успешной торговли.
- Сокращение числа промежуточных звеньев (посредников), установление прямой связи производитель — покупатель.
- Уменьшение затрат времени на приобретение необходимого товара.
- Неограниченный рост числа потенциальных заказчиков. При использовании Интернет вы можете расширить рынок сбыта за счет зарубежных покупателей.
- Информацию о товаре вы можете представлять в различном виде. Web позволяет передавать не только текст, графику, но и видео, голос.
- Возможность проводить анализ спроса, предпочтений для планирования своей деятельности.
- Возможность идентифицировать покупателя.
- Сокращение затрат на персонал и аренду помещений.
- Возможность круглосуточного доступа.

Если на западе системы доставки, платежей, торговли по каталогам, автоматизации предприятий и стандартов ЭК складывались годами, то у нас все это находится в стадии зарождения. Всего же в сегменте Интернета, охватывающего страны СНГ, существует более 600 сайтов, их можно увидеть в каталоге на сайте Magazin.ru, предлагающих различные платные услуги. Заметим, что большинство из них электронной коммерции, в строгом смысле этого слова не ведут, так как они не интегрированы с системой автоматизации предприятия, не позволяют осуществлять онлайновые платежи, требуют участия менеджера на тех или иных фазах оформления покупки.

В любой стране, если пользователей Интернета менее 10% населения, развивать направление B2C очень сложно. По России этот показатель на 1 января 2003г. составил 4,2%, по Москве около 10%. Создание полноценного Интернет-магазина стоит не менее 10 тыс. долл. У многих фирм таких денег нет, но они могут воспользоваться услугами таких фирм как "АйТи" и Tops, которые предлагают в аренду законченную инфраструктуру для открытия Интернет-магазинов на своих "торговых рядах" (www.imbs.ru, www.ipassage.ru). Аренда магазина в "торговых рядах" Tops обходится владельцам в 150 долл. в месяц.

Электронные магазины - не единственный путь оказания услуг через Интернет. Популярны сегодня аукционы, финансовые, банковские услуги, туристические, медицинские, страховые, платные информационные сервисы, онлайновая оплата счетов. 1999 г. был отмечен расцветом Web-аукционов. Например на eBay было заключено 3 млн. аукционных сделок, на Yahoo — 1 млн. Обороты же отечественных аукционов

(www.molotok.ru, www.stavka.ru) пока невелики, и цены на них ненамного ниже чем в магазинах.

Финансовые и банковские услуги в Интернет представлены несколькими направлениями: Интернет-торговля ценными бумагами, телебанкинг, онлайновое предоставление залоговых кредитов и т.п. Как и другие сферы электронного бизнеса, эта сфера быстро развивается. Онлайновые услуги предлагают практически все банки США, по отчетам British Telecom неплохо обстоит дело в Германии и Франции. Значительно отстают в предоставлении Интернет-услуг банки Великобритании, на начало 2000г. там было зарегистрировано всего 10 банковских Web-узлов.

Перенос услуг страхования в Интернет пока идет очень медленно, страховые компании неохотно вкладывают деньги в Интернет.

В настоящее время в российской части Интернета преобладает модель ЭК, ориентированная на потребительский рынок, т.е. B2C, но есть и интересные решения, которые можно отнести к модели B2B. Рассмотрим несколько примеров.

Сайт Фактура.ru (www.faktura.ru) предоставляет сервис по организации торговли между предприятиями через Интернет, связывая в единое целое службы сбыта поставщиков и службы снабжения покупателей, при этом полностью автоматизирован процесс взаимодействия предприятий на этапе поиска товаров и согласования условий заказов, позволяя контрагентам в защищенном режиме планировать, заказывать и контролировать поставки товаров и услуг.

Сайт "Зерно" (www.mtszerno.ru) — представляет собой межрегиональную систему торговли сельхозпродуктами в режиме реального времени.

Платежные системы в Интернет. Важным моментом в развитии ЭК является проведение электронных платежей. В настоящее время проблему оплаты через Интернет можно считать уже решенной. В российском секторе Интернета, который часто называют Рунетом, имеется больше десятка различных систем, позволяющих перечислять деньги за товары в онлайновам режиме. Со списками этих систем и их описанием можно познакомиться на сайтах Money.ru и Magazin.ru. Эти системы можно разделить на несколько типов:

- для платежей по пластиковым картам (ППК) международных систем Visa, Eurocard/Mastercard, American Express и т.п.;
- для платежей с пользовательских счетов провайдеров;
- для платежей с использованием "электронного кошелька";
- для платежей по смарт-карточкам.

Наиболее популярной системой первого типа является Assist-CyberPlat, созданная совместно банком "Платина" и петербургской компанией "Рек-

софт", эта система работает как для расчетов "бизнес-бизнес" так и для расчетов "бизнес-потребитель". В мае 2000г. система "Assist" была подключена к процессинговому центру карточной системы "СТБ КАРТ", а в сентябре 2000г. - к процессинговому центру Альфа-банка.

Рассмотрим технологию оплаты покупки со счета в банке с использованием платежной системы CyberPlat. Заметим, что покупатель и Интернет-магазин должны иметь открытый счет в банке, поддерживающем данную платежную систему.

1. Покупатель через Интернет подключается к Web-серверу магазина, формирует корзину товаров и направляет магазину запрос на выставление счета.

2. Магазин в ответ на запрос покупателя направляет ему заверенный своей электронной цифровой подписью (ЭЦП) счет, в котором указывает наименование товара (услуги), код магазина, время и дату совершения операции. С гражданско-правовой точки зрения этот счет является предложением заключить договор (офертой).

3. Покупатель заверяет своей ЭЦП предъявленный ему счет и отправляет его обратно в магазин, совершая тем самым акцепт. Договор считается заключенным с момента подписания покупателем выставленного ему счета. В системе счет, подписанный покупателем, становится чеком.

4. Подписанный двумя ЭЦП (магазина и покупателя) чек направляется магазином в Банк для авторизации.

5. Банк производит обработку подписанного чека: проверяет наличие в системе магазина и покупателя, проверяет ЭЦП покупателя и магазина, проверяет остаток и лимиты средств на счете покупателя, сохраняет копию чека в базе данных банка.

В результате проверок формируется разрешение или запрет проведения платежа. При разрешении платежа банк переводит денежные средства со счета покупателя на счет магазина, передает магазину разрешение на оказание услуги (отпуск товара), а магазин оказывает услугу (отпускает товар). При запрете платежа банк передает магазину отказ от проведения платежа, а покупатель получает отказ с описанием причины.

Покупатель полностью контролирует процесс совершения покупки. В качестве документального подтверждения совершенной сделки у каждой стороны остаются подписанные ЭЦП чеки, удостоверяющие факт совершения сделки и имеющие юридическую силу.

Другим вариантом расчета является оплата по кредитной карточке. Общая схема взаимодействия в этом случае выглядит следующим образом.

1. Покупатель через Интернет подключается к Web-серверу Интернет-магазина, формирует корзину товаров и выбирает форму оплаты по кредитным карточкам.

2. Магазин формирует заказ и переадресует покупателя на сервер авторизации, одновременно туда же передаются код магазина, номер заказа и его сумма.

3. Сервер авторизации устанавливает с покупателем соединение по защищенному протоколу (SSL) и принимает от покупателя параметры его кредитной карточки (номер карточки, дату окончания действия карточки, имя держателя карточки в той транскрипции, как оно указано на карточке). Информация о карточке передается в защищенном виде только на сервер авторизации и не предоставляется магазину при операциях покупателя.

4. Авторизационный сервер производит предварительную обработку принятой информации и передает ее в банк.

5. Банк проверяет наличие магазина в системе, проверяет соответствие операции установленным системным ограничениям. По результатам проверок формируется запрет или разрешение проведения авторизации транзакции в карточную платежную систему.

6. При запрете авторизации: банк передает серверу авторизации отказ от проведения платежа, сервер авторизации передает покупателю отказ с описанием причины, а магазину — отказ с номером заказа.

7. При разрешении авторизации запрос на авторизацию передается через закрытые банковские сети банку-эмитенту карточки покупателя или процессинговому центру карточной платежной системы, уполномоченному банком-эмитентом.

8. При положительном результате авторизации, полученном от карточной платежной системы: банк передает серверу авторизации положительный результат авторизации, сервер авторизации передает покупателю положительный результат авторизации, а магазину — положительный результат авторизации с номером заказа, магазин оказывает услугу (отпускает товар), банк осуществляет перечисление средства на счет магазина в соответствии с существующими договорными отношениями между банком и магазином.

9. При отказе в авторизации: банк передает серверу авторизации отказ от проведения платежа, сервер авторизации передает покупателю отказ с описанием причины.

10. Сервер авторизации передает магазину отказ с номером заказа.

Существуют и свои сложности, в первую очередь это касается обеспечения безопасности расчетов. Разработчики прилагают немалые усилия для защиты данных, но полной гарантии пока быть не может.

Открывая электронный магазин, следует иметь ввиду, что число владельцев карточек в России невелико, из них около 90% приходится на зарплатные проекты.

Системы второго типа позволяют использовать деньги, внесенные на лицевой счет Интернет-провайдера (ISP). Такой метод дает возможность осуществлять микроплатежи ($1-$2), для которых системы с пластиковыми карточками неэффективны (в них рентабельны операции на сумму не менее $20). К минусам данной системы оплаты можно отнести то, что провайдер выполняет несвойственные ему функции банка, хотя банк в этой схеме тоже участвует, кроме того, число пользователей системы напрямую зависит от количества "охваченных" ею провайдеров.

Деятельность систем с использованием ***"электронного кошелька"*** базируется на применении специального программного обеспечения, хранящего виртуальные деньги. Однако электронные деньги возникают в кошельке только после того, как пользователь перевел на счет компании-владельца системы свои реальные накопления. И вы должны очень сильно доверять организации, поддерживающей эту систему. Наличие комиссионного сбора, например, у Webmoney в размере 0,8% от каждой операции, также не очень привлекает пользователей. Но тем не менее, по общемировому прогнозу технология "электронных кошельков" в будущем вытеснит из Интернета платежи по электронным картам.

Из систем платежей по смарт-карточкам пока существует только одна — фирмы "СмартКардСервис". Для оплаты используются карточки "СБЕРКАРТ" Сбербанка России.

Смарт-карта представляет собой новый вид носителя информации, основанный на микропроцессорной электронике. Преимущества смарт-карт перед карточками с магнитной полосой очевидны: процессор, расположенный на карточке, позволяет клиенту обойтись без ONLINE авторизации (исключает связь по телефону), что значительно экономит время, делает ненужным введение неснижаемого остатка и исключает ошибки связанные с передачей данных по каналам связи. Для расчётов по смарт-картам владельцу карты необходимо ввести личный код (PIN-код), без знания которого, операция проведена не будет, кроме того, после троекратного неправильного набора PIN-кода, карточка будет заблокирована, что сводит на нет риск воровства денежных средств с карты.

Со смарт-карты нельзя сделать дубликат, микропроцессор карты следит за целостностью данных при помощи внутренних уникальных алгоритмов. В случае утери смарт-карты денежные средства, находящиеся на ней, не пропадают, а переводятся на новую карту.

Платежи, происходящие с помощью электронных денег, очень быстры во времени, а сами электронные деньги по своей сути лишь информация о реально существующих средствах. Самые большие проблемы в расчетах в Интернете — обеспечение их безопасности и признание законности новых платежных систем.

Сдерживание развития электронного бизнеса в России связано со следующими проблемами.

- Недостаточное число пользователей Интернет.
- Необходимость расширения системы кредитных карточек.
- Необходимость развития инфраструктуры системы связи.
- Необходимость повышения безопасности передачи данных в Интернет.
- Необходимость принятия соответствующих законодательных актов.
- Нехватка средств на финансирование Интернет-проектов.

Здесь есть определенные успехи. Принят "Закон об информации, информатизации и защите информации", “Закон об электронно-цифровой подписи”, в новом Уголовном Кодексе РФ есть статьи, позволяющие привлекать к ответственности за нарушения, связанные с компьютерами, разработана "Концепция информационной безопасности", "Концепция формирования информационного общества в России". Все проблемы заключения контрактов, регистрации доменных имен, торговых марок должны быть решены с помощью соответствующих законов или инструкций.

2.7. Безопасность информационных систем в экономике

2.7.1. Информационная безопасность — составляющая экономической безопасности

Становление рыночной экономики в России породило ряд проблем. Одной из таких проблем является обеспечение безопасности бизнеса. На фоне высокого уровня криминализации общества, проблема безопасности любых видов экономической деятельности становится особенно актуальной. Информационная безопасность среди других составных частей экономической безопасности (финансовой, интеллектуальной, кадровой, технико-технологической, политико-правовой, экологической, маркетинговой и физической) является одной из главных составляющих.

Термин "безопасность" в законе РФ «О безопасности» определяется как "состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз». Состояние защищенности — это стабильно прогнозируемое во времени состояние окружения, в котором предприятие может осуществлять свои уставные задачи без перерывов, нарушений и потери конкурентоспособности

Следует различать понятия информационная безопасность и безопасность информации. Первое понятие охватывает более широкий круг проблем. Согласно Доктрине информационной безопасности России информационная безопасность — состояние защищённости информационной сферы (информационной среды общества), обеспечивающее её формиро-

вание и развитие в интересах граждан, организаций и государства. Жизненно важные интересы — совокупность потребностей, обеспечивающих существование и прогрессивное развитие. Объекты безопасности — личность, её права и свободы, общество — его духовные и материальные ценности, государство — его конституционный строй, суверенитет и территориальная целостность. С точки зрения информационной безопасности необходимо защитить граждан (информационная безопасность личности) от ненужной информации, от разрушающего психику и сознание потока информации. С другой стороны, необходимо обеспечить право граждан на информацию.

Информационная безопасность как составная часть экономической безопасности предпринимательской деятельности включает в себя: а) комплексную программу обеспечения безопасности информационных ресурсов предприятия и б) экономически обоснованную технологическую систему защиты, обеспечивающую должный уровень защищенности, готовности, надежности ИС и безопасность информации.

Безопасность информации — это обеспечение ее конфиденциальности, целостности и доступности законным пользователям. Безопасность информации – состояние защищённости информации, обрабатываемой средствами вычислительной техники (ВТ), находящуюся на машинных и традиционных носителях, от внутренних и внешних угроз.

Угрозам — случайным или намеренным действиям, выводящим фирму, независимо от рода ее деятельности, из состояния безопасности со стороны внешнего окружения и внутренних источников подвержены персонал, имущество, информация и товары при перемещении. Кроме того, фирма может быть признана виновной в судебном порядке за ущерб, нанесённый третьим лицам (включая и собственных служащих) или собственности.

Таким образом, можно определить цель обеспечения безопасности информации, которая заключается в защите прав собственности на неё, и задачи безопасности, которые заключаются в защите её от утечки, копирования, блокирования, модификации и утраты.

2.7.2. Концептуальная модель защиты информации

Для организации системы защиты на конкретном предприятии необходимо провести анализ источников и видов информации, требующих защиты, выполнить анализ угроз безопасности и возможные способы реализации угроз, а также выбрать соответствующие способы и средства защиты.

В самом общем виде решению такой задачи может помочь концептуальная модель защиты информации (см. рис.7)

Рис.7. Концептуальная модель защиты информации

.Схема в виде последовательных блоков представляет содержание системы обеспечения защиты информации. Рассмотрим последовательно каждый из блоков.

Источники информации. Источник информации — это материальный объект, обладающий определёнными сведениями (информацией), представляющей конкретный интерес для злоумышленников или конкурентов. Выделяются следующие категории источников:

1. Люди (сотрудники, обслуживающий персонал, продавцы, клиенты и т.д.)

2. Документы различного характера и назначения.

3. Публикации: доклады, статьи, интервью, проспекты, книги, специализированные периодические издания.

4. Технические носители информации. Наиболее точное описание носителей дано в законе "О государственной тайне" " Носители сведений — материальные объекты, в том числе физические поля, в которых сведения, составляющие тайну, находят своё отображение в виде символов, образов, сигналов, технических решений и процессов.

5. Технические средства обработки информации, средства связи и средства обеспечения производственной и трудовой деятельности.

6. Выпускаемая продукция.

7. Производственные и промышленные отходы.

Рассмотрим ***особенности источников с точки, зрения вероятности реализации угроз безопасности.***

Люди как носители информации с точки зрения её защиты занимают особое место — как активные элементы, имеющие волевое начало, не только владеющие, но и обобщающие различные сведения. Поэтому необходим тщательный подбор персонала и анализ окружения..

Документы. Документ (документированная информация) – это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать. К документированной относится информация не только на бумажных, но и на электронных носителях, в том числе и хранящаяся на жестком диске и в оперативной памяти ЭВМ. Для защиты документов организуется регламентируемое и контролируемое их движение.

Публикации. Например: "Коммерсант DAILY", "Деловой мир", "Финансовая Россия", "Деньги", "Финансовые известия", "Экономическая газета", "Обозреватель — Observer" и др. За рубежом: "Business Week", "Financial Times", "Wall Street Journal", Dun's Review", "Commerce & Business Daily", "Business Horizons" и др. По заключению западных специалистов более 60% секретной военной и 90% экономической информации можно получить из открытых источников. Поэтому обязательным подразделением службы безопасности предприятия является информационно-аналитический отдел, обрабатывающий открытую информацию.

Производственные и промышленные отходы. По мнению специалистов в области защиты информации "В мусорной корзине можно найти 1000$ банкнот.” Поэтому при обработке конфиденциальной информации предъявляются особые требования к уничтожению документов, принтерных распечаток, копировальных лент и очистка оперативной памяти компьютеров и магнитных носителей.

Поэтому в обеспечении безопасности деятельности предприятия и эксплуатации ИС важно учитывать все угрозы, которые могут возникнуть со стороны источников информации.

Виды информации по условиям защиты. Статья 21 Закона РФ "Об информации, информатизации и защите информации" определяет, что защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб её собственнику, владельцу и иному лицу. Закон подразделяет информацию по уровню доступа на следующие категории: общедоступная, открытая информация, информация о гражданах (персональные данные) и конфиденциальная информация. ***Конфиденциальная информация*** — документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ. В свою очередь, документированная информация с ограниченным доступом по условиям её защиты подразделяется на информацию отнесённую к государственной тайне и конфиденциальную. К конфиденциальной информации относятся сведения, определяемые общим понятием — тайна. В законах встречается 32 вида тайн. Однако, обобщённый перечень сведений, отнесённых к разряду конфиденциальных, приводится в Указе Президента РФ №188 от 6.03.97 г.

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским Кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Следует отметить, что согласно ст.139 Гражданского Кодекса РФ к коммерческой тайне относятся сведения, представляющие потенциальную ценность для её обладателя в силу неизвестности третьим лицам. Здесь же

определено, что обладатель коммерческой тайны должен сам предпринимать меры к её сохранности. Поэтому, с точки зрения обладателя коммерческой тайны, необходимо обеспечить защиту как документированной, так и недокументированной информации.

Угрозы безопасности деятельности предприятий и информации подразделяются на внешние и внутренние. Их перечень обширен и для каждого предприятия индивидуален. Общими для всех являются угрозы стихийных бедствий, техногенных катастроф и деятельность людей – непреднамеренные ошибки персонала (нарушители) или преднамеренные действия (злоумышленники), приводящие к нарушениям безопасности. В Доктрине информационной безопасности России приводится следующий перечень угроз информационным системам:

- Противоправный сбор и использование информации;
- Нарушения технологии обработки информации;
- Внедрение аппаратных и программных закладок, нарушающих нормальное функционирование ИС;
- Создание и распространение вредоносных программ
- Уничтожение и повреждение ИС и каналов связи
- Компрометация ключей и средств криптографической защиты;
- Утечка информации по техническим каналам;
- Внедрение устройств для перехвата информации;
- Хищение, повреждение, уничтожение носителей информации;
- Несанкционированный доступ в ИС, базы и банки данных.

2.7.3. Требования, принципы и модель системы защиты информационной системы

Под системой защиты информационной системы понимается совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам установленным соответствующими документами в области защиты. Система защиты строится на основе политики безопасности – набора норм, правил и практических рекомендаций на которых строится управление, защита и порядок обработки информации в информационной системе. Перечислим главные принципы построения системы защиты

- Эшелонирование;
- Непрерывность;
- Равнопрочность;
- Минимизация полномочий доступа;
- Разумная экономическая достаточность.

Эти принципы реализуются в модели системы защиты, которая с различными модификациями реализуется сегодня на всех предприятиях (см. рис.8).

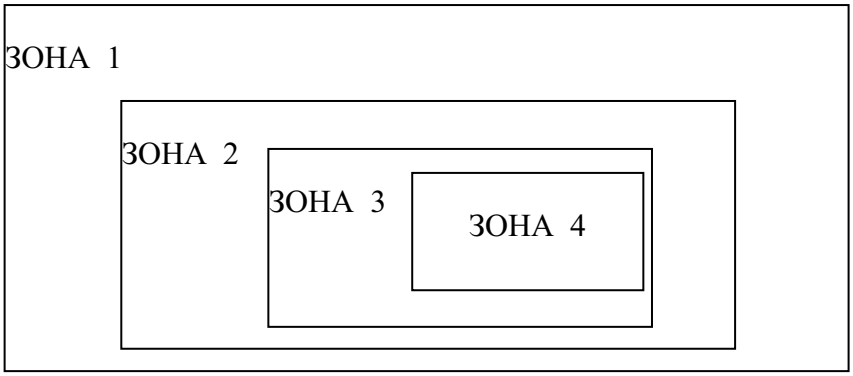

Рис.8. Модель системы защиты

Зона 1 — внешние заграждения. Зона 2 — контроль доступа в здание. Зона 3 — контроль доступа в помещение с системами обработки и хранения информационных ресурсов и ценных материальных активов. Зона 4 — контроль доступа в систему обработки информации.

Вероятность реализации угрозы Q в зоне 4 зависит от вероятностей преодоления рубежей защиты в зонах 1, 2 ,3.

2.7.4. Методы и способы защиты

На каждом предприятии, независимо от его размеров, вида собственности и направления деятельности применяются однотипные методы и способы защиты, реализующие модель системы защиты. Блок методов защиты – это препятствия, регламентация, разграничение доступа, маскировка, побуждение и принуждение. Перечисленные методы реализуются применением следующих способов защиты. *Препятствия* (физический способ) – установка ограждений вокруг предприятий, ограничения доступа в здание и помещения, установка сигнализации, охрана. *Разграничение доступа* осуществляется физическим способом и программно – техническим. *Маскировка* предусматривает использование криптографических программных средств. *Побуждение* – соблюдение пользователями этических норм при обработке и использовании информации. *Регламентация* подразумевает наличие инструкций и регламентов по обработке информации, а *запрещение* предполагает наличие правовых норм, закрепленных в нормативных документах и определяющих юридическую ответственность в случае их нарушения.

Согласно руководящим документам Государственной технической комиссии при президенте РФ, органу, который определяет порядок защиты

информации и контролирует применение программно-технических средств защиты, перечисленные выше методы и способы защиты, объединяются в четыре подсистемы, которые устанавливаются в информационных системах:

1. *Подсистема разграничения доступа* — осуществляет защиту входа в информационную систему с помощью программных (пароли) и программно-технических средств (электронные ключи, ключевые дискеты, устройства распознавания пользователей по биометрическим признакам и др.).
2. *Подсистема регистрации и учета* — осуществляет регистрацию в специальном электронном журнале пользователей и программ, получивших доступ в систему, к файлам, программам или базам данных, время входа и выхода из системы и другие операции, выполняемые пользователями.
3. *Криптографическая подсистема* — набор специальных программ, осуществляющих шифрование и расшифрование информации. Наличие криптографической подсистемы особенно необходимо в информационных системах, используемых для электронного бизнеса.
4. *Подсистема обеспечения целостности* (неизменности) информации включает в себя наличие физической охраны средств вычислительной техники и носителей, наличие средств тестирования программ и данных, использование сертифицированных средств защиты.

2.7.5. Криптография с публичным ключом и электронная цифровая подпись

Защита информации особенно актуальна в электронном бизнесе. Здесь возникают проблемы не только защиты данных при передаче по каналам связи от перехвата, подделки или уничтожения, но и задачи аутентификации деловых партнеров, подтверждения подлинности передаваемых документов, а также их юридической силы. Криптография является надежным способом решения перечисленных задач.

Криптография (от греческого kripto – тайна) представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать зашифрованные данные бесполезными для злоумышленника. Шифрование (необходимо отличать от кодирования) – это многократное однотипное математическое преобразование текста по определенному алгоритму с помощью ключа шифрования. Ключ шифрования – это конкретное состояние алгоритма из множества возможных состояний. В качестве алгоритмов используют замены, перестановки или их сочетание, осуществляемые по определенным законам. Например, в качестве алгоритма можно выбрать матрицу размерностью M x N. Исходный текст записывается

по строкам, а зашифрованный считывается по столбцам. Здесь ключом шифрования будет размерность матрицы.

Существует два метода шифрования – симметричный и асимметричный или метод шифрования с публичным ключом. Последний метод и позволяет решить задачи обеспечения конфиденциальности, целостности передаваемого документа и аутентификации лица, передавшего документ.

При симметричном методе шифрование и расшифровка документа осуществляется одним ключом, сгенерированным по заданному алгоритму специальным генератором (программой). Одним из существенных недостатков этого метода является трудность в передаче ключа. Однако, в современных информационных системах этот метод широко используется совместно со специальными методами передачи ключей для канального (поточного) шифрования данных, передаваемых в сети Интернет. Для этих целей используются сеансовые ключи, которые действуют непродолжительное время, что делает бесполезным их определение для злоумышленника даже в случае перехвата зашифрованного сообщения. В России алгоритм симметричного шифрования утвержден государственным стандартом ГОСТ 28147 – 89.

Метод несимметричного шифрования является основой коммерческой криптографии. В этом методе специальной программой генерируется два ключа – публичный (открытый для всех пользователей информационной системы) и закрытый ключ, хранящийся в секрете у пользователя, сгенерировавшего эти ключи. Математической основой метода шифрования с публичным ключом служит утверждение о том, что в настоящее время отсутствуют математические доказательства какого-либо способа нахождения сомножителей двух простых чисел по известному их произведению. Впервые это было показано американскими математиками Райвестом, Шамилем и Адельманом. Поэтому в их честь один из алгоритмов шифрования называется RSA.

Суть алгоритма заключается в последовательности следующих действий. Выбираются (генерируются) два простых числа q и p большой размерности (до 200 знаков). Затем вычисляется произведение этих чисел [n = q*p]. Ищется число e совместно простое с произведением [e U (q-1)*(p-1)]. Затем находится число d , удовлетворяющее условию e*d mod (q-1)*(p-1) = 1. Операция mod n означает остаток от деления. В качестве ключей шифрования выбираются пары чисел: {e, n) – открытый ключ, {d, n} – закрытый ключ. Открытый ключ рассылается всем заинтересованным партнерам, а закрытый ключ хранится у отправителя. Подчеркнем важное свойство алгоритма шифрования: сообщение зашифрованное открытым ключом может быть расшифровано только связанным с ним закрытым ключом, причем открытый ключ не позволяет вычислить ключ закрытый.

Процедура шифрования выполняется по формуле C = M^e mod N. Здесь M открытый текст, а C – зашифрованное сообщение, e – открытый ключ, N – произведение исходных простых чисел, на основе которых вычислялись ключи шифрования. Процедура расшифрования заключается в вычислениях по формуле M= C^d mod N (d – закрытый ключ). Не забываем, что обрабатываемые на компьютере тексты, представлены в двоичном коде.

В России для асимметричного шифрования используется алгоритм, усложненный по отношению к алгоритму RSA и утвержденный государственным стандартом ГОСТ Р3410 –10.

Электронная цифровая подпись. В традиционном бумажном документообороте авторство документа и его подлинность (аутентификация) подтверждаются рукописной подписью и печатью, поскольку текст документа и удостоверяющие реквизиты жестко связаны с материальным носителем. В электронных документах такой связи нет.

Поэтому для установления подлинности автора электронного документа и отсутствия изменений, в полученном по каналу связи документе, используется электронная цифровая подпись (ЭЦП). Согласно Закона РФ «Об электронной цифровой подписи» от 10.01.02 — электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и, позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Электронная цифровая подпись признается равнозначной собственноручной подписи на бумажном носителе. ЭЦП выполняет следующие функции:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность (неизменность) подписанного документа.

ЭЦП представляет собой несколько буквенно-цифровых символов, передаваемых вместе с электронным документом.

Технология получения и проверки ЭЦП включает в себя следующие процедуры: 1) процедуру вычисления дайджеста (хэш – функции) сообщения; 2) процедуру зашифрования дайджеста закрытым ключом отправителя; 3) процедуру вычисления дайджеста сообщения (хэш – функции) получателем; 4) проверку полученного дайджеста, путем расшифрования его открытым ключом; 5) сравнение вычисленного получателем дайджеста с полученным в результате расшифрования (верификация).

Получение дайджеста сообщение (хэширование) осществляется путем обработки текста с помощью специального преобразования. Хэш-функция строится на основе однонаправленной математической функции (например, дискретного логарифмирования), т.е. это преобразование строится таким образом, что после преобразования невозможно восстановить исходный текст. Хэш – функция предназначена для сжатия подписываемого документа произвольной длины до нескольких десятков или сотен бит. Значение хэш – функции (дайджеста) сложным образом зависит от документа и даже внесение пробела или изменение одного символа в тексте приводит к полному изменению дайджеста и, соответственно, ЭЦП. Программы для вычисления дайджеста и у отправителя, и у получателя идентичны. Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. В качестве подписываемого документа может быть использован любой файл. В России алгоритм хэш – функции утвержден государственным стандартом Р 3411-94.

Самый лучший и надежный способ распространения открытых ключей – воспользоваться услугами сертификационных центров, которые сейчас создаются в России. Сертификационный центр выступает как хранилище цифровых сертификатов. Он принимает открытые ключи вместе с доказательствами личности лица, приславшего ключ. Сертификаты выступают в роли варианта удостоверения личности. Они позволяют убедиться корреспондентам, что лицо распространяющее ключи, является тем, за кого себя выдает.

«Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и, которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи» (Закон РФ «Об электронной цифровой подписи»). Таким образом, на основании закона, сертификация ключей будет производиться специальными удостоверяющими центрами, которые будут являться посредниками между пользователями информационных систем, использующими ЭЦП. Главная роль удостоверяющего центра заключается в подтверждении факта (в случае возникновения спорной ситуации), что данный ключ подписи принадлежит именно тому лицу, которое отправило ключ в сертификационный центр.

При использовании ЭЦП в деловом обороте необходимо помнить, что юридическая сила электронного документа признается лишь при использовании сертифицированных специальными лабораториями (здесь серти-

фикация понимается как соответствие утвержденным стандартам) программно – технических средств для генерации ключей.

Технология использования ЭЦП является надежным средством обеспечения безопасности при ведении электронного бизнеса.

2.7.6. Правовая защита информации

Среди различных методов защиты информации, особая роль отводится правовой защите. При всех своих возможностях и обязательности использования, физические и программно-технические способы защиты не смогут обеспечить безопасность информационных систем, если отсутствует адекватная правовая база, регламентирующая деятельность в информационной сфере. Под адекватной правовой базой понимается совокупность правовых норм, содержащихся в законах и других источниках, признаваемых государством, и являющихся общеобязательным критерием дозволенного, предписанного и запрещенного поведения пользователей информационных технологий. Нарушение норм влечет юридическую ответственность: дисциплинарную, гражданскую, административную и уголовную.

К настоящему времени насчитывается свыше 1000 нормативных актов различного уровня, регулирующих правоотношения в области создания, распространения, обработки, хранения и использования информации и правоотношения в области создания и эксплуатации информационных систем.

Виды защищаемой информации. Статья 21 Закона РФ "Об информации, информатизации и защите информации" определяет, что защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб её собственнику, владельцу и иному лицу. Однако требования к системам защиты и нормы ответственности зависят от категории защищаемой информации. Закон подразделяет информацию по уровню доступа на следующие категории: общедоступная, открытая информация, информация о гражданах (персональные данные) и конфиденциальная информация. Конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ. В свою очередь, документированная информация с ограниченным доступом по условиям её защиты подразделяется на информацию, отнесённую к государственной тайне и конфиденциальную. К конфиденциальной информации относятся сведения, определяемые общим понятием — тайна. В действующих сегодня законах встречается 32 вида тайн. Это обстоятельство затрудняет применение норм права и вызывает противоречия при их применении. С целью упорядочения, сделана попытка, систематизировать перечень сведений, отнесённых к разряду конфи-

денциальных, подзаконным актом — Указом Президента РФ №188 от 6.03.97 г.

Еще раз подчеркнем, что режим защиты различается в зависимости от категории информации по уровню доступа к ней. Так, в отношении сведений, отнесенных к государственной тайне, режим защиты устанавливается уполномоченными органами на основании Закона РФ «О государственной тайне». В отношении конфиденциальной документированной информации режим защиты устанавливается собственником этой информации на основании соответствующих законов**.** Так, согласно ст.139 Гражданского Кодекса РФ к коммерческой тайне относятся сведения, представляющие потенциальную ценность для её обладателя в силу неизвестности третьим лицам. Здесь же определено, что обладатель коммерческой тайны должен сам предпринимать меры к её сохранности. Поэтому, с точки зрения обладателя коммерческой тайны, необходимо обеспечить защиту как документированной, так и недокументированной информации.

Возникает вопрос – если обладатель коммерческой тайны сам должен обеспечить ее сохранность, в чем тогда заключается суть правовой защиты? Ответ на этот вопрос заключается в том, что законом предусмотрена юридическая ответственность (дисциплинарная, административная и уголовная) в случае нарушения порядка использования информации и информационных технологий, незаконный сбор и разглашение коммерческой тайны, нарушение системы защиты.

Так, Трудовой Кодекс РФ согласно ст. 81 п. в) предусматривает расторжение трудового договора по инициативе работодателя в случае разглашения работником охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

Согласно Статье 13.14 Кодекса РФ об административных правонарушениях, разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда; на должностных лиц — от сорока до пятидесяти минимальных размеров оплаты труда.

В случае, если разглашение коммерческой или банковской тайны причинило ее обладателю крупный материальный ущерб, согласно ст. 183 Уголовного Кодекса РФ к лицу, виновному в совершении преступления, могут быть применены наказания от штрафа до двухсот минимальных зарплат и даже лишения свободы на срок до десяти лет.

Особенности защиты сведений, составляющих коммерческую тайну. По неофициальным оценкам сотрудников ФСБ России практически каждая крупная отечественная фирма крадет информацию у своих конкурентов и одновременно страдает от аналогичных действий с их стороны. Поэтому предприниматели должны обращать особое внимание на защиту коммерческой тайны. Прежде всего, необходимо определить какая информация требует защиты, выяснить возможные внешние и внутренние угрозы безопасности и разработать соответствующую угрозам систему защиты.

К информации, имеющей коммерческую значимость, относят сведения о количестве выпускаемой продукции и объемах продаж, сведения о поставщиках и производителях, продавцах и дилерах, договорах и клиентах. Планы фирмы, предельные цены, себестоимость продукции, имена и адреса сотрудников, маркетинговые и аналитические исследования. Финансовое состояние фирмы, размеры оплаты труда, денежный наличный оборот, особенно каналы движения денежной массы.

Для обеспечения режима коммерческой тайны весьма важными являются организационно-правовые меры. Прежде всего, должен быть организован конфиденциальный документооборот. Каждый документ, содержащий сведения, отнесенные к коммерческой тайне должен иметь соответствующий гриф (конфиденциально, КТ и т.п.). Гриф «секретно» используется только для документов, содержащих сведения, относимые к государственной тайне. Должен быть определен круг лиц, которые имеют доступ к соответствующим документам и базам данных, разработаны правила разграничения доступа в информационную систему, порядок хранения, учета и уничтожения материальных носителей, заведен журнал учета движения конфиденциальных документов.

Кроме того, при приеме на работу, с будущими сотрудниками проводится соответствующий инструктаж, а в контракте (заявлении о приеме на работу) должны быть предусмотрены соответствующие пункты о неразглашении конфиденциальных сведений.

РАЗДЕЛ 3. СОВРЕМЕННЫЕ ПОДХОДЫ К РЕИНЖИНИРИНГУ БИЗНЕС-ПРОЦЕССОВ И ПОСТРОЕНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ

3.1. Совершенствование управления и реинжиниринг бизнес-процессов (БП)

3.1.1. Реструктуризация управления

В постоянно изменяющихся экономических условиях, существует необходимость в инструментах и методах, которые могут помочь организациям стать более эффективными. В мире конкуренции существует потреб-