МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ

Н.Р. Шевко
С.Я. Казанцев
О.Э. Згадзай

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

под редакцией заслуженного юриста России,
профессора С.Я. Казанцева

Казань 2016

ББК 32.81
Ш 37
Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:
Доктор технических наук, доцент **И.Г. Дровникова**
(Воронежский институт МВД России)
Кандидат технических наук, доцент **М.В. Питолин**
(Воронежский институт МВД России)
Кандидат технических наук, доцент **Н.Г. Подчерняев**
(Орловский юридический институт МВД России им. В.В. Лукьянова)
Кандидат педагогических наук **М.А. Шелепова** (Тюменский институт повышения квалификации сотрудников МВД России)

Шевко Н.Р.

Ш 37 Информационные технологии в юридической деятельности: учебное пособие / Н.Р. Шевко, С.Я. Казанцев, О.Э. Згадзай; под ред. С.Я. Казанцева. – Казань: КЮИ МВД России, 2016. – 230 с.

Рассмотрены основные понятия и категории информатики в юриспруденции, программное обеспечение, охватывающие практически все области юридической деятельности. Предложена оригинальная схема направлений информатики в аспекте их изучения в юридическом вузе. Достаточно полно описано аппаратное обеспечение персонального компьютера. Приведены примеры использования в юридической деятельности современных информационных технологий, таких как мультимедиа, экспертные системы и др. Отдельные главы посвящены рассмотрению технологий работы с правовыми информационными системами, рассмотрению структуры, состава и принципов функционирования программного обеспечения информационных технологий.

Изложены основы информационной безопасности и защиты информации в компьютерных системах. Разобраны проблемы защиты информации на персональном компьютере от потери и разрушения, несанкционированного доступа, вопросы восстановления утраченных данных, надежного удаления данных и т.д. Особое место отведено вопросам обеспечения защиты информации в компьютерных сетях: угрозам безопасности, службам безопасности.

Для студентов учреждений высшего профессионального образования, обучающихся по специальностям 030900.62 – Юриспруденция и 031001.65 – Правоохранительная деятельность.

ББК 32.81

ISBN 978-5-901593-69-1

ПРЕДИСЛОВИЕ

Процесс информатизации общества, охвативший большинство сфер человеческой деятельности, не обошел стороной и право. Компьютер стал инструментом юриста, его помощником в повседневной работе. Возрастание роли информации, превращение ее в основной ресурс привело и к тому, что появились новые виды преступности, связанные с незаконным хищением, копированием и распространением информации – информационные преступления. Использование современных средств и методов работы с информацией сделалось жизненно важной потребностью при решении правовых и управленческих задач. Очевидно, что складывающаяся ситуация требует от юриста соответствующей подготовки в области современных информационных технологий, овладения необходимой культурой работы с информацией.

Информатизация правовой сферы непосредственно связана с внедрением компьютерной техники и созданием на ее основе автоматизированных систем сбора, хранения, обработки и выдачи информации. Компьютер из мощного вычислительного устройства превратился в средство обработки и хранения информации любого вида. Это позволяет применять его для моделирования правовых ситуаций, вынесения судебных решений, анализа правовых норм, в качестве средства связи в системах коммуникации. Следует отметить, что решение проблем правовой информатизации находится на пути создания информационных сетей на разных уровнях управления. Функционирование и интеграция таких сетей способствует организации безбумажного обмена информацией, созданию условий для формирования единого информационно-правового пространства России.

Квалифицированный специалист в области права должен знать устройство и основные принципы работы персонального компьютера (ПК), иметь необходимые навыки алгоритмизации и программирования профессиональных задач, владеть со-временными методами сбора, хранения и переработки информации, в том числе с использованием средств телекоммуникации, представлять себе основные возможности искусственного интеллекта в решении правовых задач. Только глубокие специальные знания могут обеспечить соответствующий уровень информационной культуры.

Содержание предлагаемого читателю учебного пособия в целом соответствует программе дисциплины “Информационные технологии в юридической деятельности” для юридических специальностей, в рамках которого осуществляется базовая подготовка. Предметом курса являются информационные отношения, складывающиеся в процессе деятельности по сбору, переработке, передаче, хранению и выдаче информации. Объектом изучения являются информационные технологии.

Основная **цель курса** – освоить работу в среде новейших информационных технологий, применяемых в юридической деятельности, в объеме, достаточном для осуществления в дальнейшем профессиональной деятельности. **Задачи курса** можно сформулировать следующим образом: изучить основные понятия и определения информатики, устройство персонального компьютера, основные виды системного и прикладного программного обеспечения, методы и приемы сбора, обработки и анализа данных.

Система курса определяется содержанием юридической деятельности в условиях информатизации общества. Что должен знать и освоить юрист для успешной

организации профессиональной деятельности с использованием компьютерной технологии работы с информацией?

Во-первых, основные понятия и термины информатики, состав и основные принципы работы устройств ПК, а также элементы программного обеспечения, в том числе:

• назначение и основные функции операционной системы ПК;

• практическое использование распространенных пакетов прикладных программ общего назначения (текстовые редакторы, электронные таблицы);

• функциональные настройки инструментальных программных средств;

• основные методы защиты информации от несанкционированного доступа и разрушения.

Во-вторых, организацию, функциональные возможности и способы использования автоматизированного рабочего места, а именно:

• программный и аппаратный состав автоматизированных рабочих мест различных служб;

• работу в составе локальной вычислительной сети и работу в режиме удаленного терминала в глобальных сетях.

В-третьих, методы обработки деловой, статистической информации, проведение аналитической работы с использованием персонального компьютера, включающие:

• использование функциональных возможностей пакетов прикладных программ общего назначения (табличных процессоров, систем управления базами данных);

• работу со справочными правовыми системами.

Таким образом, дисциплина «Информационные технологии в юридической деятельности» направлена на формирование и развитие у будущих юристов умений и навыков работы с современными информационными технологиями, активно используемыми во всех видах юридической деятельности. Эффективность работы будущего юриста существенным образом будет зависеть от того, насколько быстро он будет способен адаптироваться к их стремительному развитию.

По мнению авторов, в основу совершенствования информационной подготовки в системе профессионального юридического образования должна быть положена общая концепция информатизации образования. Изучение дисциплины «Информационные технологии в юридической деятельности» способствует приобретению следующих общекультурных компетенций:

• владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения (ОК-3);

• культура поведения, готовность к кооперации с коллегами, работе в коллективе (ОК-5).

Проблемы информационного обеспечения функционирования правовой сферы общества требуют комплексного подхода к их решению, координации деятельности специалистов – юристов, математиков, программистов – с целью получения искомого результата: достижения требуемого уровня информационной культуры.

ВВЕДЕНИЕ

Информационные процессы и технологии существуют и используются столько тысячелетий, сколько существует человеческое общество.

Информационные технологии – процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[1]. Таким образом, информационные технологии – это система приемов, способов, методов осуществления информационных процессов.

Потребность человека общаться с окружавшими его людьми, т.е. выражать и передавать информацию, привела к появлению языка и речи – древнейшей природной информационной технологии, которой каждый человек овладевает в самые первые годы после появления на свет. Для сознательных процессов в мозгу каждого человека эта технология является *внутренней*, а для передачи своих мыслей другим – *внешней*. Каждый человек мыслит с помощью речи, словами, только не произносит их вслух. Даже когда мы молчим, мы говорим сами с собой, мыслим не только образами, но и словами. Речь позволяет ученикам усвоить жизненный опыт учителя вместо того, чтобы методом проб и ошибок постигать все самим. Именно с появлением языка и речи началась **История человека** как человека разумного, так как речь требует некоторого минимума абстрактного мышления.

Дальнейшие *основные этапы* в развитии информационных технологий выглядят следующим образом:

1. *Изобретение письменности.* Это позволило обходиться без личного общения с учителем для усвоения его опыта. Письменные *документы* доходят до людей через время и расстояния, а до потомков – через годы, века и тысячелетия.

2. *Изобретение книгопечатания.* Печатный станок дал возможность быстро и дешево *тиражировать* информацию, избегая ошибок, допускаемых переписчиками.

3. *Изобретение средств связи:* сигнализации, почты, телеграфа, телефона, радио, телевидения.

4. *Изобретение звукозаписи, фотографии, кино, видеозаписи.*

5. *Изобретение компьютера,* который позволяет не только значительно ускорить любые расчеты, но и преобразовывать в соответствии с программой любую информацию, в том числе текст, звук, рисунки и движущиеся изображения.

6. *Изобретение персонального компьютера,* позволяющего отдельному пользователю обходиться без помощи программистов за счет использования заранее разработанных программ.

7. *Изобретение всемирной сети Internet и электронной почты,* позволяющих каждому человеку пользоваться информационными ресурсами всего человечества, вносить свой личный вклад в эти ресурсы и общаться между собой, а также с частными и государственными организациями.

Информационные технологии принято делить по принципу – до появления и после появления компьютеров. Появление компьютеров – это начало новой эры информационных технологий (*цифровой*). Широкое распространение компьютеров обеспечило человеку совершенно новые возможности поиска, получения, накопле-

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Российская газета. 2006. 29 июля.

ния, передачи и, главное, обработки информации. В связи со стремительным внедрением компьютеров практически во все сферы нашей жизни и стал применяться сам термин «информационные технологии».

В настоящее время под информационными технологиями понимают *технические* и *программные* средства реализации информационных процессов. В связи с бурным развитием таких новейших средств связи, как спутниковая и сотовая мобильная связь, волоконно-оптические линии связи, появился и новый термин – *информационно-коммуникационные технологии* (ИКТ).

Человек живет в *пространстве и времени*. В пространстве он может перемещаться, в том числе с помощью различных видов транспорта, но во времени он перемещаться не может – ни в прошлое, ни в будущее. Информационные технологии дают возможность человеку получать информацию о событиях не только в данном месте и о настоящем времени, но и в других местах и о прошлом времени. Информацию о событиях в других местах обеспечивают средства связи, информацию о событиях в прошлом времени – *носители информации* или *устройства памяти* (камень, бумага, книга, грампластинка, фотография, кинопленка, магнитная пленка, компакт-диск, дискета, карта флэш-памяти и др.), с помощью которых эта информация сохраняется во времени (запоминается) с целью последующего воспроизведения. Благодаря средствам связи и носителям информации человек может узнавать о событиях, происходящих в настоящее время в других местах и происходивших в прошлом.

В наше время информация систематически распространяется через *средства массовой информации* – печать, радио, телевидение, кино-, звуко-, видеозапись – с целью утверждения духовных ценностей данного общества и оказания идеологического, политического, экономического или организационного воздействия на оценки, мнения и поведение людей. При этом используются реклама, агитация и пропаганда. К традиционным средствам массовой информации в последние годы добавился Internet. И все это стало возможным благодаря бурному развитию современных информационных технологий во второй половине XX века.

Особенность современных информационных технологий по сравнению с промышленными технологиями XX заключается в том, что в ней и предметом, и продуктом труда является информация, а орудиями труда служат средства вычислительной техники и связи. Современные информационные технологии делятся на **аналоговые** и **цифровые**. Основное различие между аналоговыми и цифровыми сигналами заключается в самой структуре сигнального потока.

Аналоговые и цифровые сигналы **коренным образом** отличаются друг от друга. *Аналоговые технологии* основаны на способе представления информации в виде какой-либо непрерывной (аналоговой) физической величины (например, напряжения или силы электрического тока), значение которой (сигнал) является характеристикой информации. Аналоговые сигналы представляют собой непрерывный поток, характеризующийся изменениями частоты и амплитуды.

Цифровые технологии основаны на дискретном способе представления информации в виде чисел (обычно с использованием двоичной системы счисления), значения которых являются характеристикой информации. Простота цифровых сигналов обеспечивает (по сравнению с аналоговыми сигналами) их несоизмеримо

большую защищенность от помех, в том числе при передаче по каналам связи. При цифровом представлении информации точность зависит от числа разрядов в числах. Увеличивая число этих разрядов, можно обеспечить любую наперед заданную точность вычислений.

Цифровые технологии, имеющие столь очевидные преимущества, не могли появиться раньше аналоговых. Причина в том, что аналоговые технологии проще цифровых, и поэтому именно они могли быть осуществлены на уровне техники прежних времен. Органы чувств человека (и прежде всего органы слуха) способны воспринимать аналоговые сигналы. Поэтому для применения цифровых технологий нужны достаточно сложные устройства (компьютеры, аналого-цифровые и цифро-аналоговые преобразователи), массовое использование которых стало возможным только в последние десятилетия в результате стремительного развития микроэлектроники.

Наиболее важные цифровые информационные технологии нашего времени – сотовая мобильная связь, Internet, электронная почта, цифровая фотография, видеосъемка, кино и телевидение, технология мультимедиа (объединяющая текст и графику со звуком и движущимися изображениями), пластиковые карточки и штриховой код, виртуальная реальность, виртуальная торговля в сети Internet, цифровые методы криптографии, цифровые методы идентификации личности, системы беспроводной передачи данных *Bluetooth* («Синий зуб») и *Hand's Free* («Свободные руки»), цифровые методы сжатия информации (MPEG), интернет-телефония, спутниковая навигация в автомобиле GPS и многие другие. Все они осуществляются с помощью современных средств цифровой вычислительной техники.

Создание информационной сети Internet позволило любому владельцу компьютера приобщиться к информационным ресурсам всего человечества и даже внести в них свой вклад. При объединении множества компьютеров с помощью средств связи в сеть происходит объединение информационных ресурсов каждого из них в один общий массив информации, что открывает поистине неограниченные возможности для получения любой информации. Особую услугу сети Internet составляет *электронная почта* (E-mail). Главное преимущество электронной почты – скорость доставки сообщений независимо от географического положения отправителя письма и получателя. Значительная часть пользователей сети Internet общается через E-mail. Для этого каждый пользователь электронной почты снабжается специальным электронным адресом.

Число пользователей сети Internet стремительно возрастает. В 1999 г. их во всем мире насчитывалось 201 млн чел., в том числе в США и Канаде – 112,4 млн (43%), в Европе – 47, 15 млн, в Азии – 33,61 млн, Латинской Америке – 29 млн, в России – 5,4 млн. Число пользователей Internet в мире в 2015 г. составило более 3 млрд чел.

Технологии Internet – это экономическая и техническая революция конца XX века, перешедшая в третье тысячелетие. До настоящего времени информационные технологии только обслуживали экономику, а теперь они начинают создавать ее.

Информационная сеть будет играть главную роль и в процессе образования. Она способна объединить труды и способности лучших преподавателей и лекторов. Учителя и преподаватели высших учебных заведений смогут использовать накопленные материалы в своей работе, а школьники и студенты смогут изучать

их в интерактивном режиме. Таким образом, создаются *равные возможности* в получении образования всем желающим учиться. Все более популярным становится «виртуальное» образование – современная форма заочного обучения. Ученики, не имеющие возможности посещать занятия из-за удаленности от школы или инвалидности, обучаются через Internet. Информационная сеть Internet создает условия для домашней работы пенсионеров и инвалидов, которые могут с помощью домашних компьютеров выполнять задания, не выходя из дома.

Все перечисленное – *признаки информационного общества,* в котором практически каждый человек, в какой бы точке земного шара он ни находился, будет иметь реальную возможность легко связаться с другим человеком или организацией, передать и получить любую необходимую информацию – деловую и бытовую. Понятие «информационное общество» появилось в середине 60-х годов XX века в Японии и США. Смысл его заключался в том, что большая часть населения развитых стран будет заниматься информационной деятельностью, а главным продуктом производства и основным товаром станет информация.

Формирование информационного общества началось с создания междугородной и международной телефонной сетей и значительно ускорилось с изобретением радио и телевидения. С появлением микропроцессора, персонального компьютера, цифровых технологий, Internet, электронной почты, спутниковой, сотовой и волоконно-оптической связи формирование информационного общества достигает стадии зрелости. Областями применения современных информационных технологий становятся все сферы жизни: государственное и муниципальное управление, экономика, хозяйственная деятельность, промышленность, строительство, транспорт, связь, оборона, научные исследования, образование, медицина, сфера развлечений и досуга.

Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти[1].

В условиях становления в России информационного общества овладение юристами основами современных информационных технологий является необходимым и обязательным условием успешной профессиональной деятельности.

[1] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212) // Российская газета. 2008. 16 февраля.

Часть I.
ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глава 1. Сфера информационных технологий

1.1. Понятие и состав информационных технологий

Понятие информационной технологии

Информационная технология – сравнительно новое понятие, появившееся в связи с понятием «информационный взрыв» – значительное возрастание роли информации и ее объемов, качественное изменение средств ее обработки. Это выявило проблему рационализации работы с информацией, технологичности этого вида деятельности.

В переводе с греческого «технология» (techne) – это искусство, мастерство, умение. Этому термину дается неоднозначное толкование в разных источниках: в одних он определяется как «инструмент создания искусственного мира», в других – как «наука о материализации идей», в-третьих, например, в энциклопедическом словаре, как «совокупность методов изготовления, производства продукции». Аналогично этому определяется информационная технология в Словаре по кибернетике: как «…комплекс методов, способов и средств, обеспечивающих хранение, обработку, передачу и отображение информации»[1]. Вместе с тем понятно, что совокупность методов должна быть связана в единый процесс, выступать единой процедурой достижения оптимального результата, опять же оптимальным набором средств.

Понятие информационной технологии будет означать, что предметом технологии и объектом, на который направлены процедуры преобразования, будет выступать информация. Иными словами, информационную технологию будет отличать то, что она представляет собой процесс работы с информацией в целях получения нового информационного продукта.

Приведенные выше размышления позволяют сформулировать следующее определение:

Информационная технология *– четко регламентированный процесс, определяющий формы представления данных и порядок выполнения операций по переработке информации людьми и техническими средствами и приводящий к получению информационного продукта с заданными свойствами.*

Вместе с тем сегодня часто используют понятие информационной технологии в менее строгом значении. Например, «технология создания документа в Word» означает не строгую последовательность операций, а определенный их набор. Применение этих операций может осуществляться в разных последовательностях, предусматривать многочисленные альтернативы действий и т.д.

Информационная технология тесно связана с *информационными системами*, которые являются для нее основной средой функционирования. Информационная технология является процессом, состоящим из четко регламентированных правил выполнения этапов, действий, операций разной

[1] Словарь по кибернетике под ред. В.С. Михалевича. Киев: Гл. ред. им. М.П. Бажана, 1989. С. 238.

степени сложности над данными, хранящимися в компьютере.

Цель информационной технологии – производство информации для ее анализа человеком и принятия на его основе решения по выполнению какого-либо действия[1]. Основная ***задача информационной технологии*** – в результате целенаправленных действий по переработке первичной информации получить необходимую для пользователя информацию.

Информационная система (ИС) является средой, основная цель которой состоит в организации хранения и передачи информации. По существу, информационная система выступает как совокупность средств, с помощью которых решается основная задача информационной технологии. Поэтому представляется важным определить еще одно понятие: автоматизированная информационная технология.

Автоматизированная информационная технология – *это системно организованный для решения задач управления процесс работы с потоками информации на базе автоматизированной информационной системы.*

Автоматизация дает как минимум два существенных преимущества. Первое заключается в возможности значительного увеличения объемов находящейся в работе информации при одновременном существенном сокращении времени ее обработки. Второе выражается в создании качественно новых форм информационной поддержки различных сфер деятельности за счет возможности решения менее формализованных задач, повышения «интеллектуальности» информационной технологии.

Существенный прогресс информационных технологий в последнее время способствовал тому, что это понятие стало чаще употребляться с определением «новая». Новая информационная технология отличается от традиционной, в первую очередь, использованием специальных средств их обеспечения – компьютерной техники. Применение компьютеров существенным образом изменило сущность работы с информацией, сделало ее более быстрой и эффективной, позволило обрабатывать огромные массивы информации, недоступные ранее известным средствам, оперативно получать информационный продукт в объеме и виде, адекватном поставленной задаче. Внедрение персонального компьютера определило начало нового этапа развития информационных технологий, и именно это подчеркивается как определением «новая», так и встречающимися в литературе понятиями «современная» или «компьютерная» технология[2].

Новая информационная технология – процедура реализации информационных процессов с использованием компьютерной техники.

Выделяют *три основных принципа* новой (компьютерной) информационной технологии:

1. интерактивный (диалоговый) режим работы с компьютером;

---

[1] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 87.

[2] Об использовании дефиниций «новая», «современная», «компьютерная» применительно к информационной технологии см., например: Родин А.Ф., Вехов В.Б. Использование компьютерных технологий в деятельности следователя. Волгоград: ВА МВД России, 2003. С. 10.

2. интегрированность используемых для реализации конкретной технологии программ с другими программными продуктами;

3. гибкость процесса изменения как данных, так и постановок задач[1].

Таким образом, новая информационная технология – технология, использующая в качестве основного средства компьютерную технику и средства коммуникации.

Состав информационных технологий

Сущность технологии как процесса получения информационного продукта требует рассматривать ее состоящей из комбинации определенных деятельностных актов: этапов, действий, операций. Такое понимание работы с информацией как раз отражает ее технологичность – строгую регламентацию процесса работы с информацией. Здесь действием выступает относительно стандартный и элементарный прием выполнения информационной технологии. Операцию составляет относительно законченная совокупность действий, приведшая к получению каких-либо промежуточных результатов. Этап – наиболее крупная составляющая. Она представляет собой относительно длительную процедуру, состоящую из комбинации операций и действий.

Общими этапами для любой информационной технологии являются:

• сбор первичной информации;

• обработка первичной и получение итоговой информации;

• передача полученной информации пользователю.

Ясно, что более точно определить состав для абстрактной информационной технологии в целом не представляется возможным, это можно сделать лишь для технологии конкретной, то есть для решения каждой частной задачи.

Необходимо понимать, что освоение информационной технологии и дальнейшее её использование должны свестись сначала к овладению набором элементарных операций, число которых ограничено. Из этого ограниченного числа элементарных операций в разных комбинациях составляется действие, а из действий, также в разных комбинациях, составляются операции, которые определяют тот или иной технологический этап. Совокупность технологических этапов образует технологический процесс, или собственно технологию.

Информационная технология, как и любая другая, должна отвечать следующим требованиям:

• обеспечивать высокую степень расчленения всего процесса обработки информации на этапы (фазы), операции, действия;

• включать весь набор элементов, необходимых для достижения поставленной цели;

• иметь регулярный характер[2].

Этапы, действия, операции технологического процесса могут быть стандартизированы и унифицированы, что позволит более эффективно осуществлять целенаправленное управление информационными процессами.

[1] Информатика: учебник / под ред. Н.В. Макаровой. - М.: Финансы и статистика, 2004. – С. 89.

[2] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 92.

1.2. Средства информационных технологий

Информационная технология достигает своей цели путем последовательного выполнения определенных операций. Как любой процесс, информационная технология реализуется посредством применения определенных средств, с помощью которых и производится переработка исходной информации в информацию нового качества. Средствами информационной технологии выступают отдельные составляющие той среды, в которой она функционирует, то есть элементы (подсистемы) информационной системы. Такими элементами выступают информационное, техническое, математическое, программное, организационное и правовое обеспечение.

Один из элементов – программное обеспечение – называют *программным инструментарием* информационной технологии, тем самым подчеркивая его если не основную, то достаточно важную роль среди всех средств информационной технологии.

Информационное обеспечение

Назначение подсистемы информационного обеспечения состоит в своевременном формировании и выдаче достоверной информации для принятия управленческих решений.

Информационное обеспечение является основой разработки всего комплекса средств информационной технологии, определяя организационное, техническое и программное обеспечение.

Информационное обеспечение *– это система концепций, методов и средств, предназначенных для обеспечения пользователей (потребителей) информацией*[1].

Информационное обеспечение чаще всего определяют через ряд составляющих: совокупность справочных данных, классификаторов информации (справочно-нормативное информационное обеспечение); унифицированных систем документации; специально организованных массивов информации[2].

Справочно-нормативное информационное обеспечение составляют федеральные, ведомственные и локальные информационные массивы. Федеральное справочно-нормативное информационное обеспечение содержит законодательные акты и организационно-технические документы – ГОСТы и федеральные *классификаторы*. Ведомственные массивы содержат информацию о нормативном регулировании в области, в которой функционирует данная информационная технология, локальные ориентированы на решения локальных прикладных задач.

Система классификаторов формируется для:

• обеспечения однозначности и точности при заполнении различных

[1] Никитов В.А. Информационное обеспечение государственного управления / В.А. Никитов и др.; под ред. Ю. В. Гуляева. М.: Славянский диалог, 2000. С. 14.

[2] См., например: Мартынов В.П., Миронов Я.А. Управление техническим обеспечением органов внутренних дел: практикум по вопросам комплексной информатизации / под ред. проф. В.А. Минаева. М.: Радио и связь, 2001. С. 343.

первичных документов;

• адекватности представления и отображения информации в различных информационных подсистемах;

• обеспечения возможности обмена информационным обеспечением.

Среди федеральных классификаторов следует отметить общероссийский классификатор административно-территориального деления (ОКАТО); общероссийский классификатор информации о населении (ОКИН); общероссийский классификатор продукции (ОКП); общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов (ОКПДТР); идентификационный номер налогоплательщика ИНН, системы ведомственных классификаторов[1].

Массивы информации составляют данные по предметной области, специально организованные в виде баз данных.

Под ***данными*** в области информационных технологий принято понимать информацию, представленную в виде, пригодном для её передачи и обработки автоматическими или автоматизированными средствами.

База данных – специально организованная совокупность данных в виде таблицы: столбцы – поля, строки – записи базы данных.

Построение баз данных часто представляется на практике в виде двух этапов:

1-й этап – обследование всех функциональных подразделений организации с целью:

• понять специфику и структуру ее деятельности;

• построить схему информационных потоков;

• проанализировать существующую систему документооборота;

• определить информационные объекты и соответствующий состав реквизитов (параметров, характеристик), описывающих их свойства и назначение.

2-й этап – построение концептуальной информационно-логической модели данных для обследованной на 1-м этапе сферы деятельности. В этой модели должны быть установлены и оптимизированы все связи между объектами и их реквизитами. Информационно-логическая модель является фундаментом, на котором будет создана база данных[2].

Часто в информационном обеспечении выделяют еще один элемент – **схемы информационных потоков**. Они отражают маршруты движения информации и ее объемы, места возникновения первичной информации и использования результат-ной информации. Анализ информационных потоков должен проводиться с целью оптимизации организации, повышения интенсивности передачи и обработки информации, поступающей от источника к потребителю. Построение схем информационных потоков обеспечивает:

---

[1] Мартынов В.П., Миронов Я.А. Управление техническим обеспечением органов внутренних дел: практикум по вопросам комплексной информатизации / под ред. проф. В.А. Минаева. - М.: Радио и связь, 2001. – С. 109-130.

[2] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 72-73.

• исключение дублирующей и неиспользуемой информации;

• классификацию и рациональное представление информации.

Подробно должны рассматриваться вопросы взаимосвязи движения информации по уровням управления. Каждому исполнителю должна поступать только та информация, которая им используется.

Таким образом, для создания информационного обеспечения необходимо:

• ясное понимание целей, задач, функций всей системы управления;

• представление движения информации от момента возникновения и до ее использования в виде схем информационных потоков;

• использование системы классификации и кодирования;

• совершенствование системы документооборота;

• составление концептуальных информационно-логических моделей, отражающих взаимосвязь информации;

• организация массивов информации на машинных носителях, что требует наличия современного технического обеспечения[1].

Техническое обеспечение

Техническое обеспечение *– технические средства, аппаратура и оборудование, используемые в информационных технологиях.*

В техническом обеспечении можно выделить:

• аппаратные компоненты;

• телекоммуникационную аппаратуру и элементы;

• дополнительные компоненты.

Под аппаратными компонентами понимают компьютеры, устройства сбора, накопления, обработки информации, средства оргтехники и т.д.

К телекоммуникационной аппаратуре следует отнести системы и технические средства, с помощью которых организуется компьютерная сеть и осуществляется удаленный доступ. Это модемы, кабельные линии, устройства беспроводной связи и т.д.[2]

К настоящему времени сложились две основные формы организации технического обеспечения: централизованная и децентрализованная.

Централизованная форма базируется на использовании в информационной системе больших компьютеров и вычислительных центров. Это дает возможность обрабатывать большие массивы входной информации, которая хранится в одном месте.

Достоинства централизованной формы:

• возможность обращения пользователя к большим массивам информации в виде баз данных и информационных массивов;

• сравнительная легкость внедрения методологических решений по совершенствованию информационной технологии.

Недостатки централизованной формы:

---

[1] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 73.

[2] См.: Мартынов В.П., Миронов Я.А. Управление техническим обеспечением органов внутренних дел: практикум по вопросам комплексной информатизации / под ред. проф. В.А. Минаева. М.: Радио и связь, 2001. С. 133-180.

• ограничение возможностей пользователя в оперативном получении информации, затрудняющее принятие решений;

• ограничение возможностей пользователя в процессе использования информации[1].

Децентрализация технических средств предполагает реализацию функциональных подсистем непосредственно на рабочих местах. Она получила распространение в связи с развитием персональных компьютеров и сетей и дает пользователю широкие возможности в работе с информацией.

Достоинствами такой формы являются:

• гибкость структуры;

• усиление ответственности низшего звена сотрудников;

• уменьшение потребности в пользовании центральным компьютером и контроле со стороны вычислительного центра;

• более полная реализация творческого потенциала пользователя.

Однако эта форма имеет свои недостатки:

• сложность стандартизации из-за большого числа уникальных разработок;

• психологическое неприятие пользователями рекомендуемых вычислительным центром стандартов;

• неравномерность развития уровня информационной технологии на локальных местах, что в первую очередь определяется уровнем квалификации конкретного работника[2].

Наиболее перспективным следует считать частично децентрализованную форму – организацию технического обеспечения на базе распределенных сетей, состоящих из персональных компьютеров и большой ЭВМ для хранения баз общих данных и информационных массивов. При этом вычислительный центр берет на себя выработку общей стратегии использования информационной технологии и осуществляет помощь пользователям, а пользователь остается относительно свободен в выборе применяемых программных средств.

Математическое и программное обеспечение

Математическое и программное обеспечение *– совокупность математических методов, моделей, алгоритмов, системных и прикладных программ, реализующих цели информационной технологии, а также информацию о них.*

К средствам математического обеспечения относятся математический аппарат, который используется для решения задач информационной технологии. Они включают многочисленные методы моделирования, математической статистики, теории массового обслуживания и др.

В состав программного обеспечения входит системное и прикладное программное обеспечение, а также техническая документация[3].

---

[1] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 95.

[2] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 95-96.

[3] См.: Мартынов В.П., Миронов Я.А. Управление техническим обеспечением органов вну-

К системному программному обеспечению относятся программы, рассчитанные в основном для управления внутренними процессами компьютера. Это операционные системы, инструментальные средства программирования, средства диагностики и контроля и аналогичные.

К прикладному программному обеспечению относят комплексы программ, ориентированные на пользователей и предназначенные для решения конкретных задач обработки информации. Выделяют несколько типов программ. *Функциональные* программы предназначены для организации более эффективной работы технических средств и пользователей. Это текстовые и графические редакторы, электронные таблицы, электронные записные книжки, электронные календари и т.д. *Проблемно-ориентированные* пакеты программ используются для решения как типовых, так и оригинальных управленческих задач. Это настольные издательские, финансовые, бухгалтерские системы, экспертные системы, системы интеллектуального анализа данных и другие. *Интегрированные* пакеты программы представляют собой объединение нескольких проблемно-ориентированных программ с комплектом функциональных программ.

Организационное обеспечение

Организационное обеспечение *– совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной технологии.*

Организационное обеспечение реализуется при подготовке к проектированию информационной технологии и выполняет следующие функции:

• анализ существующей системы управления организацией, где будет использоваться ИС, и выявление задач, подлежащих автоматизации;

• подготовку задач к решению на компьютере, включая техническое задание на проектирование ИС и технико-экономическое обоснование ее эффективности;

• разработку управленческих решений по составу и структуре организации, методологии решения задач, направленных на повышение эффективности системы управления[1].

Правовое обеспечение

Правовое обеспечение *– совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных технологий, регламентирующих порядок получения, преобразования и использования информации.*

В состав правового обеспечения входят законы и подзаконные акты, в том числе и нормативные документы министерств, ведомств, организаций, регулирующие порядок работы информационной технологии.

В правовом обеспечении можно выделить два уровня. На первом уров-

---

тренних дел: практикум по вопросам комплексной информатизации / под ред. проф. В.А. Минаева. М.: Радио и связь, 2001. С. 181-211.

[1] Информатика: учебник / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. С. 74-75.

не (общая часть) происходит регламентация функционирования любой информационной системы. Это уровень законов РФ, указов Президента и постановлений Правительства РФ. Второй уровень (локальная часть) предназначен для регулирования конкретной информационной технологии. Здесь также могут применяться нормы указов Президента и постановлений Правительства РФ, если регламентируется работа технологии общероссийского уровня, например, ГАС «Выборы». Однако на этом уровне чаще применяются нормы конкретного министерства, ведомства, субъекта РФ или конкретной организации.

Правовое обеспечение этапов функционирования информационной системы включает:

- статус информационной системы;
- права, обязанности и ответственность персонала;
- правовые положения отдельных видов процесса управления;
- порядок создания и использования информации и др.[1]

1.3. Виды информационных технологий

Современные информационные технологии составляют сложную композицию взаимосвязанных элементов, предназначенных для решения многочисленных задач с помощью комплекса средств. Остановимся лишь на некоторых из них, обратив особое внимание на наиболее распространенные ИТ, работающие в правовой сфере:

- информационная технология автоматизации офиса;
- информационная технология обработки данных;
- информационная технология управления;
- информационная технология поддержки принятия решений;
- информационная технология экспертных систем;
- геоинформационная технология;
- информационная технология анализа текста.

Информационная технология автоматизация офиса

Это наиболее распространенная информационная технология. Ее структура довольно демократична – целесообразно использование не всех возможностей, а некоторого набора средств, наиболее оптимального для конкретной организационной структуры.

Основные цели технологии заключаются в оптимизации подготовки документов и развитии средств коммуникации сотрудников. Практика показала, что использование средств автоматизации офиса способствует повышению качества принимаемых решений на уровне среднего звена.

К средствам автоматизации офиса сейчас относится широкая гамма программных средств широкого применения, ряд специализированных средств организационно-управленческой работы, а также средства оргтехники.

Составляющие технологии автоматизации офиса

Текстовый редактор предназначен для создания, обработки и под-

[1] Информатика: учебник / под ред. Н.В. Макаровой. - М.: Финансы и статистика, 2004. – С. 75.

готовки к печати текстовых документов. Текстовый редактор имеет возможность ввода текста с клавиатуры и загрузки сохраненного документа, исправления текста, выбора видов и начертания шрифтов, перемещения фрагментов по тексту, имеет широкий потенциал по форматированию абзацев, страниц и теста в целом, позволяет вставлять в документ рисунки и другие объекты, устанавливать сноски и колонтитулы, распечатывать подготовленный текст на принтере, обладает рядом других функций. Тем самым современный текстовый редактор, наиболее распространенным из которых в настоящее время является Microsoft Word, является мощным инструментом работы с документами.

Электронные таблицы. Представляют собой универсальную систему обработки данных, обладающими широкими возможностями. Они позволяют проводить сложные технические или экономические расчеты, оформлять полученный результат и распечатывать полученный документ. Электронные таблицы позволяют создавать табличные документы с большим количеством строк и столбцов, достаточных для большинства задач, вводя данные с клавиатуры, редактируя содержание каждой ячейки таблицы, проводить расчеты путем записи формул и широкого набора встроенных функций, вставку в документы различных объектов, изображений, рисунков, построение графиков по содержащимся в таблице числовым данным, осуществлять макропрограммирование с применением последовательности команд и операций. В электронную таблицу встроены средства управления данными, что позволяет ее использование как простой СУБД (системы управления базой данных).

Системы обработки изображений. Увеличение объемов памяти компьютеров и скорости обработки ими данных сделали перспективным компьютерные технологии обработки изображений.

Документы переводятся в цифровую форму с помощью сканера или цифрового фотоаппарата и могут храниться на жестком диске компьютера или на оптических дисках. При размере файла документа в 100 Кб на 560 Мб оптическом диске может разместиться около 5,6 тыс. документов. Изображения могут корректироваться в графических редакторах. С помощью графических редакторов осуществляется ввод изображения с внешнего устройства, его коррекция разнообразными алгоритмами обработки, редактирование, внесение надписей, соединение нескольких изображений в одно, их печать и т.д.

Электронная почта (E-mail). Электронная почта становится сегодня одним из основных средств коммуникации между людьми. Она может работать как в компьютерной сети организации, так и в глобальной сети Интернет. С помощью электронной почты можно передать любое сообщение: текст, рисунки, программы, архивные файлы и т.п. Программы, управляющие рассылкой электронной почты, позволяют передать сообщение одному или нескольким адресатам, сделать сообщение доступным для группы пользователей. Существует режим уведомления о прочтении сообщения получателем.

Системы управления базами данных находят все большее распространение в офисных технологиях. В них могут храниться разнообразные сведения. Это и справочная информация, и данные о работе организации, и многое другое. Справочные правовые системы (СПС «Гарант», «Консультант +» или иные) имеет сейчас практически каждая организация.

Информационные менеджеры объединяют в себе целый ряд функций, характерных для офисных технологий. Они реализуют функции электронной почты, персонального календаря, с помощью которого осуществляется персональное и групповое планирование, содержат персональную информацию – книгу контактов и список заданий. Информационным менеджером является программа Microsoft Outlook.

Средства оргтехники. Это традиционные средства коммуникации, такие, как телефон, факсимильная связь, позволяющая передавать изображения по телефонной линии, ксероксы, быстро копирующие документы и т.д.

Следует отметить, что офисная технология предусматривает обмен данными между всеми программными средствами, входящими в ее состав. Так, документ из электронной таблицы или текстового редактора может быть отправлен по электронной почте, а информация из базы данных переводится в текстовый редактор и используется для подготовки текстовых документов.

Информационная технология обработки данных

Основой технологии является база данных: специально организованная совокупность данных, состоящих из однотипных элементов, называемых записями. Простая база данных может представлять собой таблицу, как, например, приведенная ниже таблица 1.1.

Обычно база данных состоит из совокупности связанных по определенным полям таблиц (реляционные базы данных). Например, приведенная выше таблица может быть связана по полю «Подразделение» с другой таблицей, где содержатся данные на все подразделения ОВД.

База данных содержит структурированные данные. Основная функция технологии – ввод данных, их обработка, получение сведений по текущим запросам, формирование разнообразных отчетов. Использование технологии позволяет существенно увеличить эффективность управленческой работы на уровне выполнения отдельных операций – формировать ведомости на сдачу экзамена, вести достаточно большие по объему учеты сотрудников, товаров и их перемещений в процессе производства и т.д.

Основным элементом информационной технологии обработки данных является система управления базой данных (СУБД). СУБД – специальный пакет программ, посредством которого реализуется управление базой данных и обеспечивается доступ к данным[1]. Это сложные программные комплексы, выполняющие всю совокупность функций, связанных с использованием и эксплуатацией баз данных. С помощью СУБД реализуется: ввод данных (новых файлов и записей), управление ими (сортировка, формиро-

[1] Четвериков В.Н., Ревунков Г.И., Самохвалов Э.Н. Базы и банки данных. М.: Высшая школа, 1987. С. 19.

Таблица 1.1.

Пример организации простой базы данных

№ п/п	Фамилия	Имя	Отчество	Подразделение	…
1.	Иванов	Иван	Иванович	ОБЭП	…
2.	Петров	Петр	Петрович	УР	…
3.	Русаков	Руслан	Романович	МОБ	…
…	…	…	…	…	…
…	Якимов	Ярослав	Яковлевич	УР	…

вание и выполнение поисковых запросов, производство вычислений), формирование отчетов. Важнейшим элементом СУБД являются ее языковые средства. Через языковые средства данные становятся доступными пользователю. С их помощью выполняются две основные функции – описание представления базы данных и инициирование выполнения операций манипулирования данными[1].

Информационная технология управления

Данная технология предназначена для обеспечения информацией на всех уровнях управления. Как правило, технология управления ориентирована на широкий круг пользователей и содержит в себе множество запросов к данным. От технологии обработки данных она отличается детализацией и специализацией функций. Основу технологии составляет база данных, включающая два уровня:

• данные о функционировании организации;

• нормативно-справочная документация.

Отличительной особенностью технологии управления является возможность подготовки большого количества видов отчетов, характерных для управленческой деятельности. При этом информация представляется в агрегированном виде для того, чтобы были видны тенденции изменения показателей функционирования организации, отклонения от заданных значений и т.д.

Информационная технология поддержки принятия решений

Информационная технология поддержки принятия решений предназначена для того, чтобы помочь лицу в выборе оптимальной стратегии поведения в определенной ситуации или группе ситуаций. Существует большое количество компьютерных систем, использующих данную технологию, разных по своим возможностям и принципам построения, включая системы искусственного интеллекта.

Существенным отличием технологий поддержки принятий решений является использование наряду с базой данных базы моделей. Характерной особенностью технологии является то, что применение математических и логических правил оперирования данными (правил вывода) дает возможность получать новую информацию, иными словами, определенные

[1] Когаловский М.Р. Технология баз данных на персональных ЭВМ. М.: Финансы и статистика, 1992. С. 54-55.

рекомендации действий. Модели могут быть разнообразны по структуре и функциям. Простейшие модели реализуют лишь элементарные математические операции. Большие и сложные модели могут содержать большое количество ситуаций и правил. Соответственно, становится возможным моделирование сложных процессов.

Аналитические информационные технологии

В базах данных накоплены огромные массивы информации. Они несут большие потенциальные возможности для анализа, на основе которого можно выявлять внутренние тенденции, делать прогнозы, находить новые решения. Это обстоятельство потребовало реализовать аналитические информационные технологии хранения и использования данных. Рассматриваемые технологии характеризуются рядом особенностей.

Большие массивы данных потребовали новых технологий их хранения, которые получили наименование хранилищ данных. В хранилище данные сформированы в виде гиперкуба или многомерного куба, в ячейках которого и хранятся анализируемые данные. Поскольку структура таких данных достаточно сложна, для их представления используются так называемые витрины данных – часть данных, необходимая для решения поставленной задачи.

Для представления данных пользователю системы необходимо иметь развитые инструменты доступа и обработки данных хранилища. Эти функции реализует инструмент оперативной аналитической обработки (OLAP). Инструмент OLAP обеспечивает обобщение и агрегацию данных, работу с агрегированными данными, многомерный анализ гиперкубического представления данных.

Аналитическая технология реализует *интеллектуальный анализ данных* – ИАД (Data Mining). Его задачей является поиск функциональных и логических закономерностей в накопленной информации, построение на этой основе моделей и правил, их объясняющих, прогнозирование развития анализируемых процессов.

Интеллектуальный анализ данных – метод, основанный на анализе зависимостей между данными, поиске в данных скрытых закономерностей. Автоматизированный поиск закономерностей выступает отличительной чертой технологии ИАД.

Технологии ИАД реализуются по двум направлениям. В первом случае пользователь сам выдвигает гипотезы относительно зависимостей между данными, во втором – зависимости между данными ищутся автоматически. Это считается наиболее перспективным в настоящее время.

Процессы ИАД подразделяются на три стадии: поиск зависимостей, прогнозирование и анализ аномалий. *Поиск зависимостей* состоит в автоматическом обнаружении зависимостей в данных. *Прогнозирование* заключается в том, что система прогнозирует значения, которые может запросить пользователь. *Анализ аномалий* состоит в обнаружении данных, отличающихся от устойчивых зависимостей.

Аналитические информационные технологии используют большое

количество методов: логических и математических, статистических. Применяется и новейший метод нейронных сетей. На практике оперативная аналитическая обработка и интеллектуальный анализ данных выступают как две составные части единого процесса поддержки принятия решений.

Информационные технологии искусственного интеллекта

Под *искусственным интеллектом* понимается способность системы решать интеллектуальные задачи, свойственные человеческому разуму[1]. Это значит, что эта информационная технология должна раскрывать взаимосвязи между явлениями, быть способной вырабатывать структуру действия в новой ситуации, уметь обучаться и самообучаться. Основными технологиями искусственного интеллекта являются технологии экспертных систем (ЭС) и нейронных сетей.

Отличительной особенностью экспертной системы является то, что полученное с помощью нее решение основывается на эвристических правилах, формируемых на основе практических знаний экспертов. Это решение не может быть получено иначе, поскольку задача не поддается математическому описанию.

Другой особенностью является способность получать с помощью ЭС новое знание, построенное на логическом выводе. Логический вывод основан на знаниях, предварительно сформулированных экспертами – людьми, профессионалами в узкой области. Знания экспертов накапливаются в базе знаний, которая и является основой логического вывода.

Таким образом, технология экспертных систем включает в себя базу знаний с механизмами логического и эвристического манипулирования этими знаниями с целью формирования гипотез. В основе технологии находится модель предметной области. Под моделью предметной области понимаются знания в определенной сфере деятельности, организованные с помощью особых средств их представления.

Экспертная система – программно-аппаратный комплекс, который использует знания специалистов о некоторой конкретной предметной области и в пределах этой области способствует принятию решений на уровне эксперта-профессионала[2].

Следует отметить, что применение экспертных систем в правоохранительной деятельности, особенно в расследовании преступлений, оказалось весьма перспективным. Практическую реализацию нашли и интеллектуальные консультационные системы. Совет, даваемый экспертной системой, не является обязательным и выступает как одна из возможных альтернатив реальной деятельности по расследованию преступлений, т.е. ЭС обеспечивает, дополняет и увеличивает возможности в сфере выбора и принятия решения в условиях неопределенности ситуации.

---

[1] Якубайтис Э.А. Информатика – Электроника - Сети.М.: Финансы и статистика, 1989. С. 71.
[2] Баранов А.К., Карпычев В.Ю., Минаев В.А. Компьютерные экспертные технологии в органах внутренних дел. М.: Академия МВД РФ, 1992. С. 35.

В криминалистике следует отметить работы В.В. Крылова[1], разработавшего систему тактического характера по выбору технических средств, и А.К. Баранова, разработавшего ЭС для раскрытия преступных организованных формирований[2]. Представляют интерес ряд экспертных систем по методикам расследования, разработанных А.Ф. Лубиным и Н.Б. Бобрыниным[3]. В целом же ученые признают, что научное направление информационных технологий искусственного интеллекта находится в стадии формирования.

Геоинформационные технологии

Геоинформационные системы (ГИС) получили широкое распространение около 20 лет назад, хотя первые системы появились значительно раньше, к 70-м годам. Причина этого очевидна и заключается в возможностях современной компьютерной техники, позволяющей обрабатывать огромные массивы графической информации, требуемые для ГИС.

Геоинформационные системы могут найти применение в правоохранительных органах для решения следующих задач:

• планирование спасательных операций и охранных мероприятий;

• моделирование чрезвычайных ситуаций;

• навигация служб быстрого реагирования и других служб силовых ведомств.

Основными компонентами геоинформационной технологии являются графические и тематические (атрибутивные) базы данных, обладающие модельными и расчетными функциями для принятия на этой основе разнообразных решений и осуществления контроля. В графических базах данных хранится метрическая основа компьютерной карты. Атрибутивные базы данных содержат в себе описания территории и дополнительную информацию. Для работы с этими данными имеется одна или две системы управления данными (СУБД). Функции СУБД – поиск, сортировка, добавление и исправление информации в базах данных. Система вывода данных предназначена для визуализации данных на экране в виде карт, таблиц, схем и т.п.

Система ввода отвечает за получение данных, источниками которых могут являться разнообразные электронные устройства (дигитайзер, сканер, электронные теодолиты и другие геодезические приборы). Информация может быть введена с клавиатуры вручную или получена из другой компьютерной системы[4].

На практике хорошо себя зарекомендовали такие ГИС, как ArcInfo и ArcView GIS (разработка США) и отечественная система GeoDraw[5].

---

[1] См.: Крылов В.В., Исмаилова Л.Ю. Консультационные системы // Компьютерные технологии в юридической деятельности. М.: БЕК, 1994. С. 100.

[2] Там же.

[3] См.: Бобрынин Н.Б. Структура экспертной системы для поддержки оперативных решений в сфере борьбы с экономической преступностью // Права человека и проблемы обеспечения законности. – Нижний Новгород, 1993. – С. 119–130.

[4] Минаев В.А., Умеренков В.В. Космические навигационные системы в деятельности оперативных служб: учебное пособие. Орел, 1999. С. 41-43.

[5] Применение современных информационных технологий в деятельности органов и подраз-

Технологии поиска информации

В последнее годы наметилась тенденция сбора и обработки неструктурированной информации. Доля структурированных данных (баз данных) в современных архивах составляет не более 20%, остальные же 80% приходятся на долю различных документов, текстов и другой информации, хранящихся в произвольном, чаще текстовом виде. Это обстоятельство существенно обострило проблему поиска и анализа данных.

Выделяют три группы методов поиска информации: методы индексного поиска, статистические методы и методы, основанные на базах знаний[1].

Индексный поиск применяется чаще всего. Он используется при поиске по текстовым полям баз данных и основан на формальном совпадении символов. Такой режим реализован в справочных правовых системах при поиске по тексту документа.

Системы индексного поиска имеют ряд существенных недостатков. Во-первых, они имеют низкую точность поиска. Это связано с тем, что один и тот же смысл может быть выражен различными словами: то слово, поиск которого задал пользователь, может отсутствовать в тексте. Во-вторых, система не может оценить, насколько точно смысл найденного документа соответствует поисковому запросу. Поэтому нужный документ может оказаться в конце списка найденных системой.

Статистические методы отличаются тем, что они исходят из предположения – чем чаще встречается слово в документе, тем в большей степени этот документ соответствует запросу. Документы с часто встречающимся искомым словом выводятся первыми, тем самым происходит ранжирование списка найденных документов, что существенно повышает эффективность работы. Однако остается проблема пропуска нужного документа, если его содержание выражается иными словами, чем введенными в запросе.

Системы, основанные на базе знаний. Такое название получили методы поиска, которые каким-либо образом учитывают смысловое значение искомого слова. Для этого чаще всего ищут не только заданное слово, но и те слова, которые ему близки по смыслу. Это реализуется путем использования словаря синонимов.

Более сложные системы основаны на так называемых *лингвистических правилах.* В таких системах осуществляется грамматический разбор и анализ исходных документов, что позволяет выявить слова, определяющие основную тему документа. По этим словам и осуществляется поиск, что в итоге позволяет найти документ, близкий к теме запроса.

Наиболее перспективным технологическим методом считается использование *семантических сетей.* Семантическая сеть отражает значение (смысл) не конкретного слова, а целой фразы. Для этого предметная область отображается в виде совокупности связанных между собой понятий.

делений внутренних дел МВД России в целях повышения ее эффективности и безопасности: лекция. М., 2004. С. 32.

[1] Карташева Е. Интеллектуальные поисковые системы Excalibur //Сети. 1997. № 6.

Понятия задаются не одним словом, а совокупностью слов, близких по значению. Такая базовая семантическая сеть поддерживается многоуровневыми структурами словарей по отдельным отраслям знаний.

При построении семантической сети используются сложные алгоритмы синтаксического, грамматического и морфологического разбора. Учитываются и устойчивые словосочетания, например, «подложный документ», которые воспринимаются как единое понятие. Реализуется распознавание разных значений слов.

Подход, основанный на построении семантических сетей, обладает достаточной гибкостью, доступен для расширения и не слишком громоздок при эксплуатации. Наиболее мощная и распространенная система данного типа – Convera компании Excalibur Technologies[1].

Контрольные вопросы

1. Раскройте содержание понятия «информационная технология».
2. Дайте определение информационной системы.
3. Перечислите три основных принципа новой информационной технологии.
4. Какие общие этапы включает в себя любая информационная технология?
5. Какие средства формируют основу информационной технологии?
6. Что включает в себя подсистема информационного обеспечения информационных технологий?
7. Какие преимущества и недостатки имеет централизованная форма организации технического обеспечения ИТ?
8. Какие преимущества и недостатки имеет децентрализованная форма организации технического обеспечения ИТ?
9. Какие компоненты входят в состав программного обеспечения ИТ?
10. Какие функции выполняет организационное обеспечение информационных технологий?
11. Что входит в состав правового обеспечения информационных технологий?
12. Назовите основные виды информационных технологий, используемых в правовой сфере.
13. Какие компоненты являются составляющими технологии автоматизации офиса.
14. Что является основой ИТ обработки данных?
15. В чем заключаются основные особенности информационных технологий искусственного интеллекта?

[1] Карташева Е. Интеллектуальные поисковые системы Excalibur //Сети. 1997. № 6.

Глава 2. Техническое обеспечение информационных технологий

2.1. История развития и принципы построения персонального компьютера

В настоящее время основная работа по информационному обслуживанию ведется на компьютерах, называемых также персональными компьютерами (ПК). При работе с ПК часто используется английская терминология, поэтому представляется целесообразным давать ее перевод на русский язык, например: PC (Personel Computer) ПК.

Первые промышленные модели ПК (PC) появились в августе 1981г. В настоящее время персональными компьютерами оснащаются все структуры, на их базе создаются автоматизированные рабочие места сотрудников.

Важнейший *принцип* построения ПК – ***открытая архитектура*** – означает модульный принцип построения и возможность замены блоков на новые по мере развития. В ПК имеются специальные разъемы расширения для подключения дополнительных периферийных устройств.

Информационные технологии, использующие ПК, включают в себя две обязательные составляющие – аппаратное обеспечение (*hardware*) и программное обеспечение (*software*), дополняющие друг друга. При разработке hardware и software для ПК соблюдается *принцип* ***совместимости "сверху–вниз"***, т.е. улучшенные версии подсистем должны содержать все возможности старых версий. Например, программы, разработанные на старых версиях IBM PC, должны работать на новых моделях.

Принципы, заложенные в основу построения ПК, привели к созданию семейства PC-совместимых ПК, которое называется «клоном». Первая модель этого семейства появилась в 1982 году и называлась IBM PCjr. Родословное дерево PC представлено на рис.2.1.

Центральная линия обозначает главную ветвь семейства, на которой модели располагаются в соответствии с их мощностями: от наименее мощной PCjr до наиболее мощной Pentium IV. Ветви в стороны – это модели со сходными характеристиками.

• IBM PC/XT (IBM PC/eXTended version) IBM PC/расширенная версия на основе микропроцессора Intel 8088;

• IBM PC/AT (IBM PC/ Advanced Technology) IBM PC/усовершенствованная технология на основе микропроцессора Intel 80286;

• IBM PC/AT/386 и IBM PC/AT/486 на микропроцессорах Intel 80386 и Intel 80486, соответственно;

• Pentium, Pentium II, Pentium III, Pentium IV – на микропроцессорах Intel Pentium, Intel Pentium II, Intel Pentium III, Intel Pentium IV, соответственно.

Возможности ПК, расположенных на главной ветви семейства, определяются именно типом используемого микропроцессора.

Intel 8088 был разработан в 1979 г., имел 8-ми разрядную шину данных и 20-ти разрядную адресную шину, т.е. адресуемый RAM до 1 Мбайт. Intel

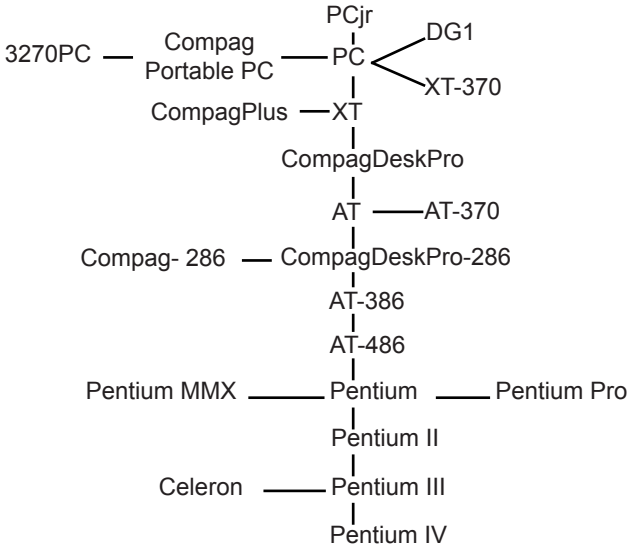

Рис. 2.1. Семейство PC совместимых ПК

80286, созданный в 1982 г., имел 16-ти разрядную шину данных и 24-разрядную адресную шину, т.е. адресовался к RAM до 16Мбайт. Intel 80386 и 80486 имели 32-битные шины данных и адреса, т.е. доступный RAM до 4 Гбайт.

В конце 1990-х годов PC-совместимые компьютеры составили 90% рынка персональных компьютеров. Принцип открытой архитектуры способствовал широкому распространению IBM PC-совместимых микрокомпьютеров-клонов. Их сборкой из готовых блоков и устройств занялось большое число фирм во всем мире. Пользователи, в свою очередь, получили возможность самостоятельно модернизировать свои ПК и оснащать их дополнительными устройствами.

За последние десятилетия XX века компьютеры многократно увеличили свое быстродействие и объемы перерабатываемой и запоминаемой информации. Еще в 1965 г. Гордон Мур, один из основателей корпорации «Intel», лидера в области разработки компьютерных интегральных схем – чипов, высказал предположение, что число транзисторов в них будет ежегодно удваиваться. Действительно, до настоящего времени число транзисторов в микропроцессорах удваивается каждые 18 месяцев. Специалисты по компьютерной технике назвали эту тенденцию **законом Мура**. Похожая закономерность наблюдается и в области разработки и производства устройств оперативной памяти и накопителей информации.

В 2016 г. персональным компьютерам клона PC исполнилось 35 лет. Как они изменились за эти годы? Первые ПК, оборудованные микропроцессором «Intel», работали с тактовой частотой всего 4,77 МГц и имели

оперативную память 16 Кбайт. Современные ПК, оборудованные микропроцессором «Pentium IV», созданном в 2001 г., имеют тактовую частоту 2–3 ГГц, оперативную память 512 Мбайт – 8 Гбайт и более, долговременную память (винчестер) емкостью 80 Гбайт – 1Тбайт и более. Такого гигантского прогресса не наблюдается ни в одной отрасли техники.

2.2. Аппаратное обеспечение ПК

К аппаратному обеспечению ПК относятся, например:

- датчики различных параметров (температуры, давления, влажности, а также оптические, звуковые и др.);
- аналого-цифровые (АЦП) и цифроаналоговые (ЦАП) преобразователи;
- модемы (модуляторы-демодуляторы);
- факс-модемы;
- сканеры;
- клавиатура;
- компьютерная мышь;
- графические планшеты;
- трекбол;
- трекпойнт;
- тачпад;
- джойстик;
- световое перо;
- мониторы;
- акустические системы;
- принтеры;
- плоттеры и др.

Перечисленные устройства представляют собой устройства ***ввода-вывода*** информации. Основные устройства ***обработки*** и ***хранения*** информации сосредоточены в ***системном блоке*** ПК.

Устройства ввода информации

Большинство параметров (температура, давление, звук и др.) воспринимаются человеком в аналоговой форме. Поэтому для обработки этих параметров в компьютере они предварительно должны быть преобразованы в цифровую форму с помощью *аналого-цифрового преобразователя* (АЦП).

Примером такого преобразования служит перевод звука, представляющего собой переменное звуковое давление, в цифровую форму при записи на оптический компакт-диск. Полученный при записи звука с микрофона аналоговый сигнал – переменное электрическое напряжение – преобразуется в цифровой код с помощью АЦП. Для этого АЦП непрерывно, с очень высокой частотой измеряет уровень этого аналогового сигнала – напряжения – и каждый раз кодирует его числом в двоичном коде, т.е. оценивает и выражает его наиболее близким по значению двоичным числом. Таким образом, вместо непрерывного аналогового сигнала образуется последовательность двоичных чисел, а сама операция называется квантованием. Последователь-

ность двоичных чисел значительно устойчивее к помехам и искажениям, чем аналоговый сигнал. Точность такой оценки аналогового сигнала с помощью двоичного кода зависит от частоты и числа разрядов квантования. Для получения высокого качества звучания компакт-диска используется частота 44,1 кГц и 16 разрядов квантования. Это дает возможность получить 216, или 65 536 уровней квантования. Эти 16-разрядные двоичные числа записываются последовательно с частотой 44,1 кГц, одно за другим, с помощью лазерного луча на оптический диск в виде впадин и гладких участков.

Человек способен слышать только аналоговые сигналы звукового давления. Поэтому при воспроизведении звука происходит обратный процесс. С помощью лазерного луча эти двоичные числа последовательно считываются, затем с помощью *цифроаналогового преобразователя* (ЦАП) преобразуются в аналоговые сигналы (с точностью до 1/65 536), усиливаются и в громкоговорителе превращаются в звук. Для улучшения качества звука используются специальные фильтры.

Подобное преобразование с помощью АЦП и ЦАП происходит и в *модеме (модуляторе-демодуляторе)* персонального компьютера. Модем (от англ. *modulator* и *demodulator*) – устройство для обмена информацией между компьютерами. Оно осуществляет преобразование дискретных сигналов в непрерывные модулированные сигналы для передачи по телефонной линии связи и обратное преобразование (с демодуляцией) при приеме.

Режим работы модемов, когда передача данных осуществляется только в одном направлении, называется *полудуплексом (half duplex)*, в обе стороны – *дуплексом (full duplex)*. Модемы бывают *внутренними* (в виде электронной платы, подключаемой к шине ISA или PCI компьютера) и *внешними* (в виде отдельного устройства). Отличаются модемы поддерживаемыми протоколами связи и скоростью модуляции (*modulation speed*). Она определяет физическую скорость передачи данных, которая измеряется количеством бит в секунду (бит/с).

Устройство, сочетающее возможности модема и средства для обмена факсимильными изображениями, называется *факс-модемом*. Факс-модем осуществляет электронную передачу обычного текста, чертежей, фотографий и схем. Он обеспечивает сканирование документа на передающей стороне, преобразование информации в форму, пригодную для передачи по имеющемуся каналу связи, и формирование на бумажном носителе на приемной стороне дубликата – факсимиле – исходного документа. В состав любого телефакса входят *сканер* для считывания документа, *модем*, передающий и принимающий информацию по телефонной линии, а также *принтер*, печатающий принимаемое сообщение на термо- или обычной бумаге.

Сканер (scaner) представляет собой устройство ввода в компьютер графических изображений (текстов, рисунков, слайдов, фотографий, чертежей). В большинстве сканеров для преобразования изображения в цифровую форму применяются светочувствительные элементы на основе приборов с зарядовой связью (ПЗС) (англ. CCD). По способу перемещения

считывающей головки и изображения относительно друг друга сканеры подразделяются на *ручные, рулонные, планшетные* и *проекционные*. Разновидностью проекционных сканеров являются слайд-сканеры, предназначенные для сканирования фотопленок.

Принцип работы однопроходного планшетного сканера состоит в том, что вдоль сканируемого изображения, расположенного на прозрачном неподвижном стекле, движется сканирующая каретка с источником света. Отраженный свет через оптическую систему сканера (состоящую из объектива и зеркал или призмы) попадает на три расположенных параллельно друг другу фоточувствительных полупроводниковых элемента на основе ПЗС. Каждый элемент принимает информацию о компонентах изображения.

Клавиатура – основное устройство ввода информации в компьютер, представляет собой совокупность механических датчиков, при нажатии на клавиши замыкающих определенную электрическую цепь. Наиболее распространены два типа клавиатур: *с механическими* и *мембранными переключателями*. Внутри корпуса любой клавиатуры, помимо датчиков клавиш, расположены электронные схемы дешифрации и микроконтроллер клавиатуры.

Мышь (англ. *mouse*) – это компьютерный манипулятор, указательное устройство для ввода информации в компьютер. Представляет собой легко умещающуюся в ладони коробочку с кнопками. При перемещении мыши по столу или иной поверхности происходит аналогичное перемещение курсора на экране монитора. С помощью кнопок мыши можно подавать команды компьютеру. Мышь делает очень удобным манипулирование такими широко распространенными в графических пакетах объектами, как окна, меню, пиктограммы.

Подавляющее число компьютерных «мышей» используют оптико-механический принцип кодирования перемещения. С поверхностью стола соприкасается тяжелый, покрытый резиной шарик сравнительно большого диаметра. Ролики, прижатые к поверхности шарика, установлены на перпендикулярных друг другу осях с двумя датчиками. Более точного позиционирования курсора позволяет добиться оптическая (лазерная) мышь. С помощью мыши можно создавать простые рисунки. Однако рисовать на экране компьютера гораздо удобнее с помощью графического планшета.

Графический планшет (или *digitizer*) – кодирующее устройство, позволяющее вводить в компьютер двумерное, в том числе и многоцветное, изображение в виде растрового образа. Графические планшеты применяют в основном в области компьютерной графики. В состав графического планшета входит специальный указатель (перо) с датчиком. Контроллер планшета посылает импульсы по расположенной под поверхностью планшета сетке проводников. Полученные сигналы контроллер преобразует в координаты, передаваемые в персональный компьютер, который переводит эту информацию в координаты точки на экране монитора. Планшеты, предназначенные для рисования, обладают чувствительностью к силе нажатия пера, преобразуя эти данные в толщину или оттенок линии.

Трекбол (англ. *trackball*) – шаровой манипулятор, является разновидно-

стью мыши, применяемой в портативных ПК – ноутбуках (*notebook*). Рука приводит в движение не корпус мыши, а шарик, а он занимает меньше места, что важно при малых габаритах ноутбука. Обычно шарик трекбола встроен в клавиатуру.

Трекпойнт (англ. trackpoint) представляет собой миниатюрный рычаг с шершавой вершиной диаметром 5–8 мм. Трекпойнт расположен на клавиатуре между клавишами и управляется нажатием пальца.

Тачпад (англ. *touchpad*) представляет собой сенсорную панель, движение пальца по которой вызывает перемещение курсора. В подавляющем большинстве современных ноутбуков применяется именно тачпад, так как отсутствие в нем движущихся частей обусловливает его высокую надежность.

Джойстик (*joystick*), или рычажный манипулятор, является аналоговым координатным устройством ввода информации. Рукоятка джойстика связана с двумя резисторами, изменяющими свое сопротивление при ее перемещении. Один резистор определяет перемещение по координате *X*, другой – по *Y*, Адаптер джойстика преобразует изменения параметра сопротивления в соответствующий цифровой код. Джойстик используется в компьютерных играх и различных тренажерах.

Световое перо – светочувствительное устройство для снятия координат точек экрана и ввода их в компьютер. По форме оно напоминает пишущую ручку. Световое перо предназначено для взаимодействия с экраном монитора. В наконечнике пера установлен фотоэлемент, который реагирует на световой сигнал, передаваемый экраном в точке прикосновения пера. Световое перо не требует создания специального экрана или его покрытия; как у сенсорного устройства. Оно позволяет выделять точку, указываемую пользователем, и вводить информацию в компьютер. Таким образом, можно записать и затем осуществить распознавание рукописного текста, сделать рисунок. Если же на экране изображено меню символов, пиктограмм, то можно указывать пером на выбранный символ или пиктограмму. Например, можно использовать псевдоклавиатуру, изображенную на экране.

Системный блок персонального компьютера

Современные *персональные компьютеры* (ПК) выпускают в настольном и в портативном исполнении. Настольные ПК в большинстве случаев состоят из отдельного системного блока, к которому подсоединяются внешние устройства: клавиатура, манипулятор-мышь, джойстик, сканер, внешний модем, монитор, акустические системы и др.

Системный блок ПК – это металлический корпус, в котором размещаются источник питания, материнская (системную, или основную) плата с процессором и оперативной памятью, платы расширения (видеокарту, звуковую карту), различные накопители (жесткий диск, дисководы, приводы CD-ROM), дополнительные устройства (см. рис. 2.2.).

Таким образом, в состав системного блока входят:

• процессор (микропроцессор), который выполняет поступающие на его вход команды, проводит вычисления и управляет работой остальных

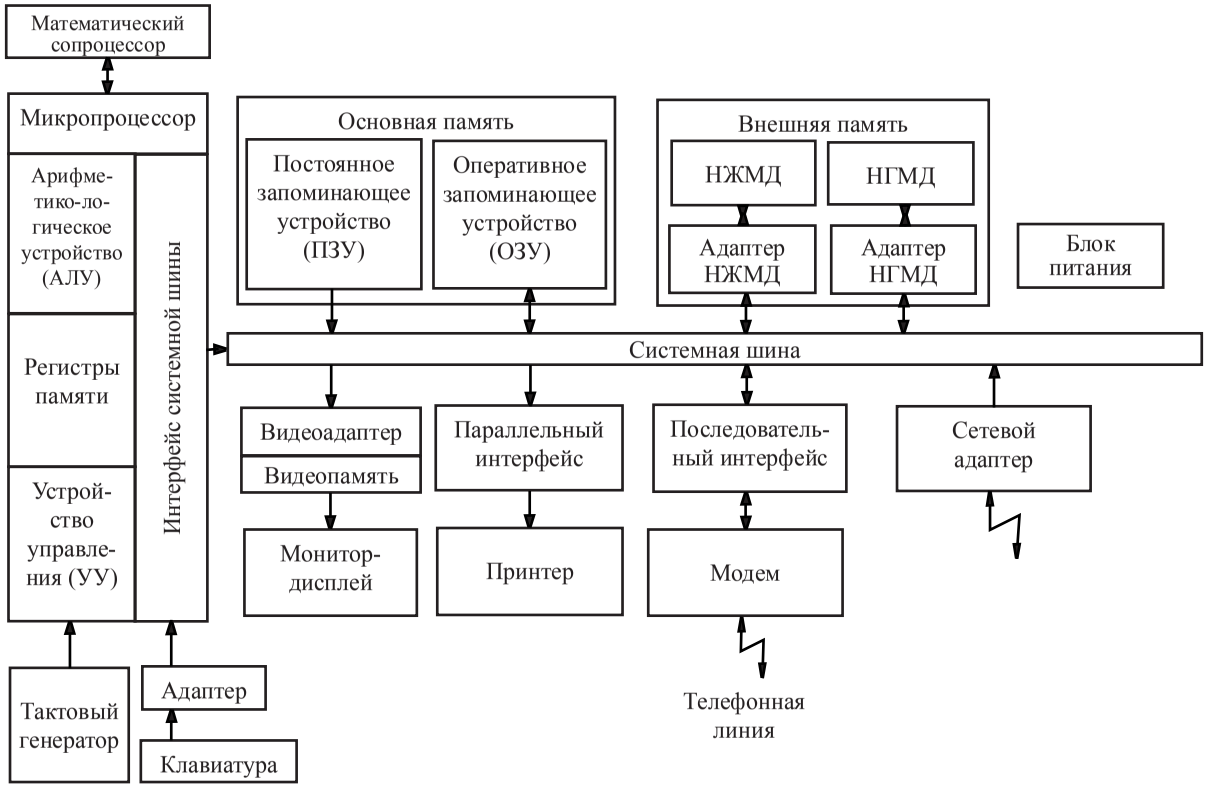

Рис. 2.2. Структурная схема ПК

элементов компьютера. Он состоит из ячеек-регистров, в которых Данные могут не только храниться, но и изменяться;

• постоянная память (ПЗУ – постоянное запоминающее устройство), в которой записана информация, необходимая постоянно, и программы, без которых компьютер вообще не запускается;

• оперативная память (ОЗУ – оперативное запоминающее устройство), служащая для временного хранения программ, данных;

• электронные схемы, управляющие элементами компьютера и обменом данными между памятью и другими средствами запоминания и отображения информации (например, монитором, принтером);

• блок питания;

• накопители на жестких дисках – винчестеры;

• дисководы оптических дисков CD-ROM и CD, записываемых CD-R и перезаписываемых CD-RW, DVD, DVD-RW оптических дисков

• внутренний модем – устройство для ввода и вывода с использованием телефонной сети для связи.

Системный блок обычно имеет несколько параллельных и последовательных портов, которые используются для подключения устройств ввода и вывода, таких как клавиатура, мышь, монитор, принтер.

В портативном ПК – *ноутбуке* – все внешние и внутренние устройства объединены в одном корпусе. Жидкокристаллический дисплей размещается в откидной крышке корпуса, имеющего форму и размеры плоского чемоданчика. Так же как и к стационарному ПК, к ноутбуку могут быть подсоединены дополнительные внешние устройства ввода и вывода данных, устройства хранения данных и т.п.

Микропроцессор (МП) (или центральное процессорное устройство) представляет собой сверхбольшую интегральную схему, выполненную на кристалле кремния. В персональном компьютере микропроцессор выполняет функции управления и обрабатывает большую часть информации.

Базовыми элементами микропроцессора являются транзисторные переключатели, на основе которых строятся регистры – совокупность устройств, имеющих два устойчивых состояния и предназначенных для хранения информации и быстрого доступа к ней. Выполняемые микропроцессором команды обеспечивают арифметические действия, логические операции, передачу управления и перемещение данных (между регистрами, оперативной памятью и портами ввода и вывода).

Микропроцессор предназначен для обработки сигналов в двоичном коде и представляет собой целую сверхминиатюрную цифровую вычислительную машину, помещенную на одном кристалле. Микропроцессоры различаются между собой разрядностью и тактовой частотой. *Разрядность* – это количество битов, воспринимаемых микропроцессором как единое целое, 4, 8, 16, 32, 64 (целые степени числа 2). От разрядности зависят производительность персонального компьютера и максимальный объем его внутренней памяти. *Тактовая частота*, измеряемая в герцах

(МГц – ГГц), в основном определяет быстродействие компьютера.

Основные типы и характеристики микропроцессоров фирмы Intel, являющейся лидером по производству микропроцессоров для PC совместимых ПК.

Микропроцессор связан с остальными устройствами системного блока сетью электронных проводников, так называемой системной шиной. Она состоит из трех групп: адресной (обычно 32-разрядные) с адресами регистров, шины данных и командной шины.

В корпусе системного блока размещается ***материнская*** *(системная)* ***плата***. На ней располагаются микропроцессор, модули оперативной памяти (ОЗУ), системная шина, микросхемы-контроллеры, управляющие работой системной шины, портов, винчестера и других устройств хранения информации, а также микросхема постоянного запоминающего устройства (ПЗУ), в которую записывается BIOS – программа, управляющая взаимодействием отдельных частей компьютера. На материнской плате имеются разъемы для подключения плат (или карт) других устройств.

Оперативная память используется для хранения программ, выполняемых в текущий момент, и используемых в них цифровых данных. Она представляет собой совокупность специальных электронных ячеек, каждая из которых может хранить конкретную комбинацию из нулей и единиц – один байт. Каждая такая ячейка имеет адрес (адрес байта) и содержимое (значение байта). Адрес нужен для обращения к содержимому ячейки: для записи и считывания информации. Оперативное запоминающее устройство (ОЗУ) хранит информацию только во время работы компьютера, другими словами, оно является энергозависимым. При отключении или временном нарушении электропитания компьютера ОЗУ тут же «забывает» заложенную в нем информацию. Емкость оперативной памяти современного ПК составляет 2–8 Гбайт и более.

При выполнении микропроцессором вычислительных операций в любой момент должен быть обеспечен доступ к любой ячейке оперативной памяти. Поэтому ее называют *памятью с произвольной выборкой* RAM (*Random Access Memory*). RAM выполняется на микросхемах двух типов – динамического (DRAM – *Dynamic* RAM) и статического (SRAM – *Static* RAM).

Кроме оперативной памяти в персональном компьютере для согласования работы быстродействующего микропроцессора с более «тихоходными» оперативной памятью и долговременными запоминающими устройствами используется сверхоперативная память, так называемая кэш-память. Для ее реализации используется статическая память.

Чтобы процессор не простаивал, пока идет медленное считывание из ОЗУ или запись в него, вводится небольшая, но сравнительно быстродействующая *кэш-память*. Пока процессор занят другими операциями, она считывает из ОЗУ заранее заказанную информацию, а затем быстро сбрасывает ее процессору. С введением кэш-памяти сократились вынужденные простои процессора, а значит, увеличилось его реальное быстродействие. Описанная память – так называемая *кэш-память второго уровня*. Но есть

и *кэш-память первого уровня*: она сформирована на самом кристалле процессора, т.е. находится в его корпусе. Из ОЗУ информация поступает в кэш-память второго уровня, затем с возрастающей скоростью – в кэш-память первого уровня и, наконец, еще быстрее – в процессор.

В компьютере есть и ***постоянная память*** (ПЗУ), хранящая информацию при отключении питания. В ней содержатся наиболее важные данные – базовая система ввода-вывода (*Basic Input Output System* – BIOS). Запись информации в постоянную память выполняют «аппаратно» – с помощью специальных устройств. Микросхемы постоянной памяти разделяются на программируемые изготовителем (ROM – *Read Only Memory*), однократно программируемые пользователем (PROM – *Programmable ROM*) и многократно программируемые пользователем (EPROM – *Erasable PROM*).

Еще один вид постоянной памяти – CMOS (*Complimentary Metal-Oxide-Semicondactdr*)или CMOS RAM – служит для сохранения некоторых характеристик ПК и среды. Микросхемы CMOS питаются от аккумуляторов и поэтому энергонезависимы. Это дает возможность постоянно сохранять важные характеристики, используемые при загрузке операционной системы.

Внешние запоминающие устройства

Для долговременного хранения, накопления и считывания цифровой информации используются *долговременные* ***запоминающие устройства*** – носители и накопители. Все они являются энергонезависимыми, т.е. хранят информацию вне зависимости от того, включен или выключен компьютер.

Накопители и носители информации делятся на устройства с *прямым* и *последовательным* доступом. Все магнитные диски (дискеты, винчестеры) имеют прямой доступ – информация почти мгновенно доступна из любой части диска. Ленточные накопители имеют последовательный доступ: данные, содержащиеся в произвольном участке ленты, могут быть считаны только после ее перемотки к этому участку.

Носитель данных (информации) – это физическое тело или среда, используемые для записи и постоянного хранения информации. ***Накопитель*** – устройство для записи и считывания информации. Так, бумага или звуковой компакт-диск CD – это носители, а дискета и стример представляют собой накопители.

Жесткий диск (винчестер) – устройство для постоянного хранения информации, используемой при работе персонального компьютера. Конструктивно такой накопитель содержит пакет из нескольких дисков, смонтированных на одной общей оси – шпинделе. Он вращается вместе с дисками со скоростью несколько тысяч оборотов в минуту.

Каждый диск представляет собой алюминиевую или стеклокерамическую пластину с магнитным покрытием – тонким слоем оксида железа или оксида хрома. Весь пакет дисков заключен в герметичный корпус, обеспечивающий необходимую чистоту и постоянное давление очищенного от пыли воздуха с помощью сложной системы специальных фильтров. Чтение и запись информации осуществляются головками чтения и записи, укреплен-

ными на поворотных рычагах-позиционерах. Головки не касаются поверхностей дисков, а перемещаются над ними на расстоянии не более 0,07 мкм.

Каждый диск разбит на последовательно расположенные дорожки – концентрические окружности, соответствующие зонам остаточной намагниченности, созданной головками. На каждом диске пакета – одинаковое число дорожек, а каждая из них разбита на последовательно расположенные секторы вместимостью 512 байт.

Винчестер содержит гермоблок и отдельно от него – плату электроники. В гермоблоке расположена механика и предварительный усилитель, а на плате – управляющая электроника. Электронная плата расшифровывает команды *контроллера* жесткого диска, стабилизирует скорость вращения двигателя, генерирует сигналы для головок записи и усиливает их от головок чтения.

Одной из основных характеристик жесткого диска является среднее время, в течение которого винчестер находит нужную информацию. Это время обычно представляет собой сумму времени, необходимого для позиционирования головок на нужную дорожку и ожидания требуемого сектора.

Другой характеристикой винчестера является скорость чтения и записи: она зависит не только от самого диска, но и его контроллера, шины, быстродействия процессора.

Стример (англ. *streamer*) – компьютерное устройство для записи информации на кассеты (картриджи) с магнитной лентой. Используется для создания резервных копий информации, размещенной на жестких дисках профессиональных компьютеров. В настоящее время используется очень редко.

Широкое применение в современных компьютерах нашли ***оптические диски*** – носители и накопители. Основным отличием оптической записи является полное отсутствие физического контакта механизма дисковода с поверхностью оптического диска. Запись и считывание информации производится бесконтактно с помощью лазерного луча. К тому же этот луч фокусируется не на поверхности, а в глубине прозрачного диска. Поэтому оптической записи не страшны неглубокие царапины на поверхности диска. Это обеспечивает очень высокую долговечность и надежность хранения информации на оптических дисках. К тому же их отличает от магнитной записи полная независимость от внешних магнитных полей.

К оптическим дискам относятся прежде всего звуковые компакт-диски и CD-ROM. Они изготавливаются на поточном производстве с помощью штампов и предназначены только для чтения.

Звуковые компакт-диски могут проигрываться как в музыкальных центрах, CD-проигрывателях и плеерах, так и с помощью дисководов персональных компьютеров. Время звучания этих дисков составляет 74 мин.

За последние годы стало возможным объединить на ПК текст и графику со звуком и движущимися изображениями на одном носителе или накопителе. В качестве носителей информации в таких мультимедийных компьютерах используются оптические компакт-диски CD-ROM (*Compact Disk Read Only Memory*) – память на компакт-диске «только для чтения»).

Внешне они не отличаются от звуковых компакт-дисков, используемых в проигрывателях и музыкальных центрах. Информация в них записывается также в цифровой форме.

Компакт-диски CD-ROM выпускаются двух диаметров – 12 и 8 см. Емкость одного CD-ROM диаметром 12 см достигает 650 Мбайт. Для чтения компакт-дисков используется CD-дисковод. Скорость чтения данных в нем зависит от скорости вращения диска. Сейчас используются уже 24, 32, 40 и 50-скоростные дисководы, а скорость считывания информации при этом приближается к скорости считывания с винчестера. Компакт-диск так же легко сменить, как и дискету. Информация на компакт-диск записывается только один раз в промышленных условиях, а на ПК ее можно только читать. С помощью CD-дисковода можно проигрывать и звуковые компакт-диски (разумеется, при наличии в ПК звуковой карты и звуковых колонок).

Компакт-диск CD-ROM содержит три слоя – подложку из поликарбоната с отштампованным рельефом диска, напыленное на нее отражающее покрытие из алюминия, серебра или золота и тонкий защитный слой из поликарбоната или лака – на него наносятся рисунки и подписи. Некоторые «пиратские» диски имеют слишком тонкий защитный слой либо лишены его совсем.

В состав дисковода или привода CD-ROM входят плата электроники, шпиндельный двигатель, устройство загрузки диска и система считывающей оптической головки. Система загрузки диска, как правило, имеет горизонтальный выдвижной лоток (*tray*), на который кладется оптический диск. В лотке имеются два соосных углубления диаметром 8 и 12 см для дисков.

Информация на диске записана с постоянной линейной скоростью. Поэтому для достижения постоянной линейной скорости считывания скорость вращения диска изменяется в зависимости от перемещения считывающей головки. Стандартная скорость вращения диска – 500 об/мин при чтении информации с внутренних зон и 200 об/мин при чтении с внешних зон диска (информация на диск записывается от центра к периферии). При стандартной скорости вращения диска скорость передачи данных составляет приблизительно 150 Кбайт/с.

Дисководы CD-ROM могут читать:

• собственно цифровую, компьютерную информацию (до 670 Мбайт);

• звуковую информацию в формате CD-Audio (продолжительность звуковой записи до 74 мин);

• видеоинформацию в формате Video CD и CD-I (продолжительность видеозаписи до 1 ч);

• библиотеки изображений, записанные в формате Kodak Photo CD;

• множество других, в том числе комбинированных, видов информации, например звуковой и видео, записанной со сжатием по стандарту MPЗ.

Наряду с форматом компакт-дисков используется и другой стандарт носителей информации – **DVD** (*Digital Versatile Disc* или цифровой диск общего назначения). Их геометрические размеры одинаковы. Основное отличие DVD-диска – значительно более высокая плотность записи информации. Он

вмещает в 7–26 раз больше информации. Это достигнуто благодаря более короткой длине волны лазера и меньшему размеру пятна сфокусированного луча, что дало возможность уменьшить вдвое расстояние между дорожками. Кроме того, DVD-диски могут иметь один или два слоя информации.

У DVD-диска каждый слой информации вдвое тоньше, чем у CD-диска. Поэтому можно соединять два диска толщиной 0,6 мм в один со стандартной толщиной 1,2 мм, при этом емкость удваивается. Всего DVD-стандарт предусматривает 4 модификации: односторонний однослойный на 4,7 Гбайт (133 мин), односторонний двухслойный на 8,8 Гбайт (241 мин), двухсторонний однослойный на 9,4 Гбайт (266 мин) и двухсторонний двухслойный на 17 Гбайт (482 мин). Указанное в скобках время в минутах – время проигрывания видеопрограмм высокого цифрового качества с цифровым многоязычным объемным звуком.

Принцип *однократной записи* на диске **CD-R** (*CD-Recordable*) основан на «выжигании» лучом лазера битов информации на записывающем слое диска, состоящем из органического красителя. Этот краситель способен однократно изменить отражающую способность диска. При считывании лазерным лучом фиксируется изменение отражательной способности. Записываемый CD-R, начиная с обратной (блестящей) стороны, состоит из пяти слоев.

Многократная запись на диске **CD-RW** (*CD-Rewritable*) производится несколько по-другому. В этом случае применяется специальный комбинированный слой, который при нагреве лазерным лучом способен многократно менять свои характеристики. Вещество такого слоя при этом может многократно переходить из кристаллического состояния в аморфное и обратно. Изменение отражающей способности фиксируется лазерным лучом при считывании информации с диска. Перезаписываемый диск CD-RW содержит не пять слоев, а семь.

Записываемый диск CD-R читается с помощью любого дисковода CD-ROM. Запись информации на диски CD-R представляет собой самый дешевый и оперативный способ хранения больших объемов данных.

Записывать на CD-R можно со скоростью 600 Кбайт/с (для скорости 4х) и 1,2 Мбайт/с (для скорости 8х). Скорость считывания – до 24х (дисковода CD-ROM). Диск CD-R можно записывать либо весь сразу (за одну «сессию»), либо по частям (за несколько «сессий» записи). Но при этом нужно иметь в виду, что при каждой «сессии» теряется от 14 до 23 Мбайт, которые используются для записи заголовков.

Если записи делаются для длительного пользования и хранения, то лучше использовать более дешевые записываемые диски CD-R. Для оперативного хранения информации больше подходят перезаписываемые диски CD-RW. Цена их выше, однако они быстро окупаются всего за несколько циклов записи.

Для записи выпускаются только дисководы CD-RW. Их можно использовать как для однократной записи на диски CD-R, так и для много-кратной перезаписи на диски CD-RW. Читать они могут все виды дисков –

CD-ROM, CD-R, CD-RW. Скорость записи и перезаписи для дисководов CD-RW составляет 4х, а чтения – 20х.

Формат **DVD-RAM** с возможностью перезаписи был создан для записи видео- и компьютерной информации. Формат DVD-RAM обеспечивает быстрое преобразование информации и быстрый прямой доступ к ней. DVD-RAM можно переписывать 100 000 раз. Для их записи разработаны DVD-RAM – рекордеры. Диски DVD-RAM все шире используются в самых различных устройствах.

В *магнитооптических дисках* (МОД) используют комбинацию магнитных и оптических методов записи и чтения. Магнитный слой применяется для записи и стирания информации. Для этого лазерным лучом нагревают этот слой выше точки Кюри, при которой может изменяться ориентация намагниченности. После этого магнит записывает данные на диск. На магнитооптическом диске процесс перезаписи информации может быть повторен до 1 миллиона раз. Большим преимуществом магнитооптического метода записи по сравнению с магнитным является независимость от внешних магнитных полей при нормальных температурах, поскольку перемагничивание возможно только при температуре выше 150°С.

Современные МО-диски сочетают в себе большую емкость, устойчивость к воздействию электромагнитных полей, температуры и влажности. Объединение двух технологий – магнитной и лазерной – является залогом высокой надежности хранения данных на МО-носителях.

Сменные твердотельные полупроводниковые носители – флэш-карты являются универсальными и используются для записи любой информации – текстов, звука, изображений.

Название «флэш» (*flash*) было введено фирмой «Toshiba», так как содержимое памяти в них можно стереть мгновенно (англ. *in a flash*). В отличие от магнитной, оптической и магнитооптической памяти она не требует применения дисководов с использованием сложной прецизионной механики и вообще не содержит ни одной подвижной детали. В этом состоит ее основное преимущество перед всеми остальными носителями информации. Флэш-память – это микросхема на кремниевом кристалле. Она построена на принципе сохранения электрического заряда в ячейках памяти транзистора в течение длительного времени с помощью так называемого плавающего затвора при отсутствии электрического питания.

Флэш-память находит широкое применение – МРЗ-проигрыватели, стереосистемы, цифровые фото- и видеокамеры, сотовые телефоны и т.д. используют в качестве носителя информации флэш-карту, на которой хранятся звук, изображения, документы и другая информация. Такие карты выпускаются целым рядом фирм и имеют различные габариты: *Compact Flash, SmartMedia* (SMART – *Self-Monitoring, Analisys and Reporting Technology*) и др. Общий стандарт для всех флэш-карт не выработан.

К твердотельной флэш-памяти относится память *Memory Stick* фирмы «Sony». Она представляет собой универсальный носитель для самых раз-

личных приложений. Масса ее – всего 4 г, а габариты – не больше пластины жевательной резинки (21,5х50х2,8 мм). Предусмотрена возможность ее подключения к миниатюрным МРЗ-проигрывателям-плеерам, нескольким моделям видеокамер, цифровых фотоаппаратов, к цифровому принтеру и новой цифровой фоторамке. Вставив *Memory Stick* в такую фоторамку, можно воспроизвести изображение из ее памяти на высококачественном жидкокристаллическом экране размером 5,5 дюйма. Предусмотрена также возможность присоединения *Memory Stick* к последовательному и параллельному портам персонального компьютера с помощью специальных адаптеров.

Компании «Matsushita Electric Co», «SanDick Co» и «Toshiba Co» разработали карты флэш-памяти SD (*Secure Digital Memory Card*). В ассоциацию с этими компаниями входят такие гиганты, как «Intel» и «IBM». Выпускает SD-память фирма «Panasonic», входящая в концерн «Matsushita». SD-память снабжена защитой.

Миниатюризация карт флэш-памяти продолжается. Компании «Olympus» и «FujiFilm» начали выпуск самых миниатюрных карт флэш-памяти *xD-Picture* (*xD – extreme digital*). Размер этих носителей составляет 20х25х1,7 мм, масса – 2 г. Носитель нового формата *xD-Picture* должен прийти на смену морально устаревшим картам *SmartMedia*. В настоящее время уже выпущены подобные носители объемом 1 Тбайт. Столь значительный рост емкости миниатюрного носителя стал возможен благодаря использованию многослойной технологии.

В условиях жесткой конкуренции, существующей сегодня на рынке сменных карт флэш-памяти, необходимо обеспечивать совместимость новых носителей с уже имеющимся у пользователей оборудованием, рассчитанным на другие форматы флэш-памяти. Поэтому одновременно с картами флэш-памяти осуществляется выпуск адаптеров-переходников и внешних считывающих устройств, так называемых *карт-ридеров*, подключаемых ко входу USB персонального компьютера. Выпускаются индивидуальные (для определенного типа карт флэш-памяти, а также универсальные карт-ридеры на 3, 4, 5 и более различных типов карт флэш-памяти. Они представляют собой миниатюрную коробочку, в которой имеются слоты для одного или сразу для нескольких типов карт, и разъем для присоединения ко входу USB персонального компьютера.

Устройства вывода информации

Очень важную роль в составе ПК играет *видеоподсистема.* Видеосистема служит для вывода на экран изображений текстов, рисунков и видеофрагментов и фильмов. Она состоит из монитора (дисплея) с экраном, на который выводятся изображения; видеоплаты, т.е. платы управления вывода изображения на экран монитора; набора специальных программ – драйверов.

Основными параметрами видеоподсистемы являются:

• разрешающая способность – количество точек на экране монитора;

• цветовое разрешение – количество цветов, которое иметь отдельная точка;

• частота развертки – скорость обновления изображения экрана.

Видеоплата (или *видеокарта, видеоадаптер*) служит для хранения видео-изображений, преобразования их из цифровой в аналоговую форму для вывода на экран монитора. Она способна поддерживать текстовый и графический режимы работы. Аппаратно видеоадаптер чаще всего бывает выполнен в виде отдельной платы, вставляемой в разъем расширения материнской платы.

В текстовом режиме на экран можно вывести символы букв, цифр и специальных знаков из определенного набора, хранящегося в памяти ПК. В графическом режиме на экран можно вывести и текст и любые неподвижные и подвижные изображения. Современная видеоплата должна обеспечивать максимальное разрешение 1024x768, а рекомендовать можно разрешение 1280x1024 при отображении 16,8 миллиона цветов. Для этого ПК должен иметь не менее 2 Мбайт видеопамяти.

Видеоадаптеры бывают следующих типов:

• MDA – монохромный адаптер, работает в текстовом режиме, 25 строк по 80 символов в строке, с разрешением 720x0350 точек, с двумя градациями яркости (черный- белый);

• VGA (Video Graphics Array) – видеографическая матрица, графический режим 640x480 точек, 16 цветов, 4096 оттенков или 320x200 точек, 256 цветов;

• SVGA (Super VGA) – до 1280x1024 точек при 16 Мбайт цветов и выше.

Базовые параметры основных типов видеоадаптеров приведены в таблице 2.3.

Следует заметить, что развитию графической подсистемы персональных компьютеров уделяется очень большое внимание. Это связано с постоянно возрастающими требованиями к разрешающей способности и цветовому разрешению видеоподсистемы ПК. Так, например, для работы с текстовыми документами формата А4 необходимо экранное разрешение не менее 1024x768 при размере экрана монитора 17 дюймов. При работе с компьютерной графикой и компьютерной верстской соответствующие параметры должны быть больше 1280x1024 и 19 дюймов.

Требования, предъявляемые к видеоподсистеме персонального компьютера, становятся еще более критичными при работе со ставшими в настоящее время стандартными мультимедийными приложениями и программами обработки трехмерной графики. В этом случае требуется введение в состав видеоадаптера специальных микросхем видеоускорителя (акселераторов), основная задача которых – освободить центральный процессор компьютера от работы по построению трехмерных изображений, которая связана с большим количеством вычислений с числами с плавающей запятой.

Мониторы используют: с жидкокристаллическим экраном и плазменные.

Действие жидкокристаллического *LCD (Liquid Crystal Display)* монитора основано на использовании вещества, находящегося в жидком состоянии, но при этом обладающего некоторыми свойствами кристаллических

тел. Молекулы таких жидких кристаллов под действием электрического поля способны изменять свою ориентацию и свойства проходящего сквозь них светового луча. Пользуясь этим свойством, в жидкокристаллических индикаторах, изменяя электрическое напряжение и ориентацию молекул, создают изображение.

LCD-монитор имеет несколько слоев, содержащих между собой тонкие слои жидких кристаллов. Панель монитора подсвечивается источником света. В зависимости от его расположения панели работают или на отражение, или на прохождение света. В цветных мониторах цвет получается с помощью трех фильтров.

В компьютерных LCD-мониторах используются так называемые нематические или супернематические жидкие кристаллы. Нематические элементы способны поворачивать плоскость поляризации на угол до 90 градусов, а супернематические – до 270 градусов. Супернематические кристаллы обладают высоким быстродействием и контрастностью. Они применяются для пассивных индикаторов. Нематические кристаллы используются в высококачественных цветных мониторах.

В пассивных индикаторах элементы располагаются на пересечениях сетки проводников, к которым подводится электрическое поле путем переключения транзисторов, подключенных к этим проводникам. Такие элементы имеют эффект последействия, поэтому движущиеся предметы на них расплываются.

В активных жидкокристаллических TFT-экранах (*Thin Film Transistor* – тонкопленочный транзистор) каждый элемент снабжается транзистором. Эти транзисторы управляют приложенным напряжением и быстрее переключаются.

В цветных жидкокристаллических экранах элементы группируют по три (в вертикальный ряд). Каждые такие три элемента образуют пиксель. Каждый элемент имеет светофильтр. Транзисторы управляют количеством проходящего света, образуя нужную смесь цветов.

Недостатком пассивных мониторов является возможность смотреть на них только во фронтальной позиции, а экран с активной матрицей имеет угол обзора 120–160 градусов и обладает хорошей яркостью и контрастностью изображения. Первые LCD-дисплеи выпускались только для портативных ПК с диагональю экрана 8 дюймов.

LCD-мониторы являются полностью цифровыми приборами.

Несомненным преимуществом LCD-мониторов является почти полное отсутствие вредного излучения, которому подвергается человек, работающий перед экраном.

Стандарты безопасности, которым должны отвечать мониторы, – это TCO или MPRII, разработанные в Швеции. При покупке монитора нужно обратить внимание на знаки этих стандартов в паспорте или на корпусе монитора.

Работа плазменного (*Plasma Display Panels*, PDP) монитора похожа на работу неоновой лампы. Он выполнен в виде плоской стеклянной трубки,

заполненной инертным газом под низким давлением. Внутри трубки помещены два электрода. При подаче напряжения между ними зажигается электрический (так называемый тлеющий) разряд и возникает свечение. В плазменных экранах пространство между двумя стеклянными поверхностями заполняется, как и в неоновой лампе, инертным газом (аргоном или неоном). На стеклянную поверхность помещают маленькие прозрачные электроды, на которые подается высокочастотное напряжение: образуется поле миниатюрных точечных неоновых ламп. Под действием напряжения в газовой области, прилегающей к электроду, возникает электрический разряд. Плазма этого разряда излучает свет в ультрафиолетовом диапазоне спектра, а он, в свою очередь, вызывает свечение частиц люминофора в видимой человеком части спектра, т.е. каждый пиксель на экране работает подобно лампе дневного света.

Преимуществами плазменных экранов являются высокая яркость, контрастность и очень большой угол обзора – до 180 градусов. У них отсутствует дрожание картинки, так как она выводится не по строчкам, а прямо в цифровом виде.

Вывод информации из компьютера *на бумагу* осуществляется электромеханическими устройствами вывода информации – *принтерами*. Существуют принтеры монохромные (черно-белые) и цветные, ударного (*impact*) и безударного (*non-impact*) действия. Последовательные принтеры печатают на бумаге символ за символом, *строчные* – сразу всю строку, а *страничные* – целую страницу. В зависимости от технологии печати различают матричные, струйные, лазерные, светодиодные, сублимационные принтеры, принтеры на твердых красителях.

В 1970–1980-х гг. самыми распространенными были *матричные принтеры*, наиболее простые и дешевые. Они печатают с помощью набора миниатюрных игл, которые ударяют по красящей ленте. В этом они похожи на обыкновенную пишущую машинку и, подобно ей, позволяют печатать под копирку. Они являются монохромными, т.е. способны печатать только черно-белое изображение. Последовательные ударные матричные печатающие устройства (*impact dot matrix*) снабжены печатающей головкой с одним или двумя вертикальными рядами игл. Головка движется вдоль печатаемой строки, и в нужный момент иголки ударяют по бумаге через красящую ленту, формируя последовательно символ за символом. Для матричных принтеров можно использовать и форматную, и рулонную бумагу. Головка принтера оснащается 9, 18 или 24 иголками. Существуют модели принтеров с широкой (формата А3) и узкой (формата А4) каретками.

Матричные принтеры ударного действия дают невысокое качество печати, невысокую производительность и сильно шумят при работе. В последние годы они практически вытеснены более совершенными принтерами безударного действия, обеспечивающими монохромную и цветную печать высокого качества.

Более совершенные *струйные принтеры* относятся к устройствам безударного действия. Они печатают, разбрызгивая на бумагу микроско-

пические капельки специальных чернил, выбрасываемых на бумагу через сопла печатающей головки. Перед разбрызгиванием этим микрокапелькам дается электрический заряд, а после разбрызгивания они направляются в нужные точки бумаги с помощью электростатического поля. Количество сопел у разных моделей струйных принтеров – от 12 до 256, а максимальная разрешающая способность массовых моделей – 1440 точек на дюйм. В отличие от матричных, струйные принтеры обеспечивают лучшее качество печати и работают с гораздо меньшим шумом.

В *лазерных принтерах*, подобно ксероксу, используется электрографический принцип: изображение переносится на бумагу с барабана, к которому с помощью электростатического потенциала притягиваются частички краски (тонера). В отличие от копировального аппарата, в лазерном принтере печатающий барабан электризуется с помощью полупроводникового лазера по командам компьютера. В состав лазерного принтера входят: фотопроводящий цилиндр (печатающий барабан), полупроводниковый лазер и прецизионная оптико-механическая система, которая перемещает лазерный луч.

Лазерные принтеры обеспечивают наилучшую, близкую к типографской монохромную и цветную печать. Они обеспечивают самую высокую среди принтеров скорость печати и не требуют специальной бумаги.

В *светодиодных принтерах* (*Light Emitting Diode*, LED) вместо полупроводникового лазера используют «гребенку» мельчайших светодиодов. Для них не требуется сложная оптическая система вращающихся зеркал и линз, поэтому светодиодный принтер дешевле, чем лазерный.

Сублимационные (dye sublimation) принтеры применяются для получения цветных изображений сверхвысокого качества. В них красящие ленты нагреваются примерно до 400°С, при этом краситель испаряется и переносится на специальную бумагу. В принтерах на твердых красителях (*solid ink*) бруски краски каждого из четырех цветов, похожие на мыло или цветной воск, заправляются в принтер отдельно. В процессе разогрева в течение 10–15 мин эти краски-чернила частично расплавляются и подготавливаются к работе.

Плоттер (plotter), графопостроитель, – это устройство для автоматического вычерчивания рисунков, схем, чертежей, карт на бумаге. Первыми появились и традиционно широко используются перьевые плоттеры. Более современную технологию обеспечивают струйные плоттеры.

Перьевые плоттеры можно разделить на три группы: плоттеры, использующие фрикционный прижим для перемещения бумаги в направлении одной оси и движения пера по другой; барабанные (или рулонные) плоттеры; планшетные плоттеры, в которых бумага неподвижна, а перо перемещается по обеим осям.

Различные модели плоттеров имеют одно или несколько перьев различного цвета (обычно 4–8). Перья бывают трех различных типов: фитильные (заправляемые чернилами), шариковые (аналог шариковой ручки) и с трубчатым пишущим узлом (инкографы). Связь с компьютером плоттеры, как

правило, осуществляют через последовательный и параллельный порты.

В 1990-х гг. перьевые плоттеры начинают вытесняться струйными, которые работают в 4–5 раз быстрее. Используя два чернильных картриджа, струйный плоттер обеспечивает разрешение не менее 300 dpi и имеет два режима работы: чистовой и эскизный. При работе в эскизном режиме почти вдвое сокращается расход чернил.

Для ввода и вывода звуковых сигналов служит ***звуковая система***, состоящая из звуковой платы (или карты), встроенного динамика в системном блоке ПК и внешней звуковой системы. Ввод звука в систему осуществляется через микрофон, линейный выход магнитофона, радиоприемника или CD-проигрывателя. Простейшая внешняя система состоит из наушников или пассивных динамиков, а более сложная и качественная – из активных динамиков, имеющих собственное питание и снабженных усилителями.

Звуковые карты условно делятся на 8- и 16-разрядные. 8-разрядная звуковая карта (*SoundBlaster*) способна обеспечить качество звучания кассетного магнитофона, а 16-разрядная – более высокое качество, соответствующее CD-проигрывателю. Новые звуковые карты обеспечивают трехмерный, т.е. объемный звук. Для технологии DVD, в которой звуковое сопровождение фильмов поддерживает технологию *Dolby Digital*, звуковая карта должна уметь раскодировать DVD-звук с диска и иметь 6 каналов.

2.3. Тенденции развития цифровых аппаратных средств ИТ

Цифровые технологии дали возможность создать ряд современных аппаратных средств, которые оказывают существенную помощь работе правоохранительных органов. К ним относятся *мобильная сотовая связь, цифровые диктофоны, цифровые фото- и видеокамеры.*

Связь называют *мобильной*, если источник информации или ее получатель (или оба) перемещаются в пространстве. Сущность *сотовой связи* заключается в разделении пространства на небольшие участки – *соты* (или ячейки радиусом 1–5 км) и отделении радиосвязи в пределах одной ячейки от связи между ячейками. Это позволяет использовать в разных сотах *одни и те же частоты*. В центре каждой ячейки располагается базовая (приемно-передающая) радиостанция для обеспечения радиосвязи в пределах ячейки со всеми абонентами. У каждого абонента своя микрорадиостанция – мобильный телефон – комбинация телефона, приемопередатчика и мини-компьютера. Абоненты связываются между собой через базовые станции, соединенные друг с другом и с городской телефонной сетью. Каждая сота обслуживается базовым радиопередатчиком с ограниченным радиусом действия и фиксированной частотой. Это дает возможность повторно использовать ту же частоту в других сотах. Во время разговора сотовый радиотелефон соединен с базовой станцией радиоканалом, по которому передается телефонный разговор. Размеры соты определяются максимальной дальностью связи радиотелефонного аппарата с базовой станцией. Эта максимальная дальность является радиусом соты.

Идея ***мобильной сотовой связи*** состоит в том, что, еще не выйдя из зоны действия одной базовой станции, мобильный телефон попадает в зону действия любой соседней вплоть до наружной границы всей зоны сети.

Для этого созданы системы антенн-ретрансляторов, перекрывающих свою соту – область поверхности Земли. Для обеспечения надежности связи расстояние между двумя соседними антеннами должно быть меньше радиуса их действия. Мобильный телефон может принимать сигналы сразу от нескольких антенн-ретрансляторов, но настраивается он всегда на самый мощный сигнал.

Идея мобильной сотовой связи заключается еще и в применении компьютерного контроля за телефонным сигналом от абонента, когда он переходит от одной сотовой ячейки к другой. Именно компьютерный контроль позволил в течение всего лишь тысячной доли секунды переключать мобильный телефон с одного промежуточного передатчика на другой. Все происходит так быстро, что абонент просто этого не замечает.

Центральной частью системы сотовой мобильной связи являются компьютеры. Они отыскивают абонента, находящегося в любой из сот и подключают его к телефонной сети. Когда абонент перемещается из одной ячейки в другую, они передают абонента с одной базовой станции на другую.

Важным преимуществом мобильной сотовой связи является возможность пользоваться ею вне общей зоны своего оператора – *роуминг*. Для этого различные операторы договариваются между собой о взаимной возможности пользования своими зонами для пользователей. При этом пользователь, покидая общую зону своего оператора, автоматически переключается на зоны других операторов даже при перемещении из одной страны в другую, например из России в Германию или во Францию. Либо, находясь в России, пользователь может звонить по сотовой связи в любую страну. Таким образом, сотовая связь обеспечивает пользователю возможность связываться по телефону с любой страной, где бы он ни находился. Ведущие компании-производители сотовых телефонов ориентируются на единый европейский стандарт – GSM.

Диктофон (от лат. *dido* – говорю, диктую) – это разновидность магнитофона для записи речи с целью, например, последующего печатания ее текста. Диктофоны делятся на механические, в которых в качестве накопителя информации используются стандартные кассеты или микрокассеты с магнитной пленкой, и цифровые.

Цифровые диктофоны отличаются от механических полным отсутствием подвижных деталей. В них в качестве накопителя информации вместо магнитной пленки используется твердотельная флэш-память.

Цифровая фотография позволяет оперативно и без использования дорогостоящих, длительных и вредных для здоровья химических процессов получать в цифровой форме качественные фотографии.

Принцип работы цифровой фотокамеры заключается в том, что ее оптическая система (объектив) проецирует уменьшенное изображение фото-

графируемого объекта на миниатюрную полупроводниковую матрицу из светочувствительных элементов, так называемый прибор с зарядовой связью ПЗС (CCD). ПЗС-матрица – это аналоговое устройство: электрический ток возникает в пикселе изображения в прямом соотношении с интенсивностью падающего света. Чем выше плотность пикселей в ПЗС-матрице, тем более высокое разрешение будет давать фотокамера. Далее полученный аналоговый сигнал с помощью цифрового процессора преобразуется в оцифрованное изображение, которое сжимается в формат JPEG (или аналогичный ему) и затем записывается в память камеры. Емкостью этой памяти определяется количество снимков. В качестве памяти цифровых фотокамер используются различные накопители – дискеты, карточки флэш-памяти, оптические диски CD-RW и др. Запомненные электрические сигналы в виде картинки можно вывести на экран компьютера, телевизора, напечатать на бумаге с помощью принтера или передать по электронной почте в любую страну. Чем больше пикселей содержит ПЗС-матрица, тем больше четкость цифрового фотоизображения. В матрицах современных цифровых фотоаппаратов число пикселей – от 2 до 6 миллионов и более.

Цифровой фотоаппарат снабжен миниатюрным жидкокристаллическим дисплеем, на котором сделанный снимок появляется сразу же после нажатия кнопки. Никакого проявления и закрепления изображения (как в традиционной фотографии) при этом не требуется. Если снимок не понравился, его можно «стереть» и на его место поместить новый. Единственное, что в цифровом фотоаппарате осталось от традиционной фотографии – это объектив.

В цифровой фотографии полностью исключено использование светочувствительных материалов с солями дефицитного серебра. По сравнению с традиционными, цифровые фотокамеры содержат значительно меньшее количество механических подвижных деталей, что обеспечивает их высокую надежность и долговечность.

Во многих цифровых фотокамерах используются вариообъективы с переменным фокусным расстоянием – трансфокаторы или ZOOM-объективы), обеспечивающие оптическое (чаще всего трехкратное) увеличение. Это означает, что при фотосъемке можно, не сходя с места, приблизить или отдалить снимаемый объект, причем это можно делать постепенно. Кроме того, применяется и цифровое увеличение, при котором фрагмент изображения растягивается на весь экран.

Еще одно преимущество цифровых фотокамер – возможность делать не только фотографии, но и снимать короткие видеосюжеты длительностью до нескольких минут. В наиболее совершенных цифровых фотокамерах имеется встроенный микрофон, позволяющий снимать видеосюжеты со звуком.

Введенные в компьютер цифровые фотографии могут быть подвергнуты обработке, например кадрированию (выделению отдельных участков с увеличением), изменению яркости и контрастности, цветового баланса, ретуши и т.д. В компьютере можно создавать альбомы цифровых фотографий, которые можно просматривать либо последовательно, либо в режиме слайд-фильма.

Качество цифровых фотоснимков уже сегодня не уступает качеству обычных. Можно предположить, что в ближайшие годы цифровая фотография полностью вытеснит традиционную.

Видеокамеры позволяют записывать движущееся изображение со звуком. В современных видеокамерах оптическое изображение, так же как в цифровых фотокамерах, преобразуется в электрическое с помощью ПЗС-матрицы. В них также не нужна кинопленка, не требуется проявление и закрепление. Изображение в них записывается на магнитную видеопленку. Однако для записи вдоль магнитной ленты (как это осуществляется при записи звука) потребовалась бы очень высокая скорость ее движения – более 200 км/ч (приблизительно в 10 000 раз большая, чем при записи звука): человек слышит звуки в диапазоне частот от 20 до 20 000 Гц. Качественная запись звука осуществляется в этом диапазоне. Для записи видеоизображения требуются гораздо более высокие частоты – свыше 6 МГц.

Вместо того, чтобы увеличивать скорость движения магнитной ленты при записи и воспроизведении изображения, магнитные головки в видеокамере и видеомагнитофоне закреплены на вращающемся с высокой скоростью барабане, а сигналы записываются не вдоль, а поперек ленты. Ось вращения барабана наклонена к ленте, а его магнитная головка при каждом обороте записывает на ленте наклонную строчку. При этом плотность записи значительно увеличивается, а магнитная лента должна двигаться сравнительно медленно – со скоростью всего 2 мм/с. Они записывают цветное изображение и звук (с помощью встроенного микрофона), обладают высочайшей чувствительностью. Измерение яркости изображения, установка диафрагмы и наводка на резкость полностью автоматизированы. Результат видеосъемки можно просмотреть сразу же, ведь никакой проявки пленки (как при киносъемке) не требуется.

Видеокамеры снабжаются высококачественными объективами. В наиболее дорогих видеокамерах используются вариообъективы с переменным фокусным расстоянием, обеспечивающие оптическое х-кратное увеличение. Это означает, что при видеосъемке можно, не сходя с места, приблизить или отдалить снимаемый объект, причем это можно делать постепенно. Кроме того, применяется и цифровое увеличение, при котором фрагмент изображения растягивается на весь экран. Применяется также система стабилизации изображения, которая корректирует дрожание камеры с большой точностью и в широких пределах. Применение ПЗС-матриц обеспечивает видеокамерам высочайшую чувствительность, дающую возможность снимать почти в полной темноте (при свете костра или свечи).

В видеофильме, как и в звуковом кинофильме, движущееся изображение и звук записываются на один и тот же носитель информации – магнитную видеопленку. Наиболее распространенный бытовой стандарт видеозаписи – VHS (*Video Home System* – домашнее видео). Ширина магнитной пленки в этом стандарте – 12,5 мм. Для портативных видеокамер применяется уменьшенная кассета с пленкой той же ширины – *VHS Compact.*

Фирма «Sony» разработала и выпускает миниатюрные видеокассеты стандарта *Video-S* (Hi8). Ширина пленки в них равна 8 мм. Это позволило уменьшить габариты портативных бытовых видеокамер. Наиболее совершенные из них для контроля изображения во время видеосъемки помимо видоискателя снабжены миниатюрным цветным жидкокристаллическим дисплеем. С их помощью можно просмотреть только что отснятый видеофильм прямо на съемочной видеокамере. Другой способ просмотра – на экране телевизора. Для этого выход видеокамеры соединяют со входом телевизора.

Переход на цифровой метод записи позволяет избежать потери качества даже при многократной перезаписи. В 1995 г. консорциум 55 ведущих производителей электроники, в том числе «Sony», «Philips», «Hitachi», «Panasonic» и «JVC», приняли цифровой формат видеозаписи на магнитную пленку DVC (*Digital Video Cassette*) или DV (*Digital Video*). Уже в конце 1995 г. «Sony» представила первую DV-видеокамеру. Теперь цифровой видеофильм можно перенести с видеокамеры на винчестер компьютера и обратно непосредственно, без всяких сложных преобразований.

Каждому кадру на магнитной ленте соответствуют 12 наклонных строк-дорожек шириной 10 мкм. На каждой из них, кроме записи аудио- и видеоинформации, часа, минуты, секунды и порядкового номера кадра, есть возможность записать дополнительную информацию о видеосъемке. Все DV-камеры могут работать в режиме фотосъемки и фиксировать отдельные изображения со звуковым сопровождением в течение 6–7 с. Они превращаются в цифровые фотоаппараты с емкостью 500–600 кадров. Создан уже и DV-видеомагнитофон.

Наряду с цифровым форматом DV фирма «Sony» разработала новую цифровую технологию *Digital 8*, которая призвана стереть границу между аналоговыми и цифровыми форматами. Она позволяет использовать цифровую запись DV на обычной кассете Hi8, применявшейся для аналоговой записи.

Выпускаются цифровые видеокамеры без видеокассеты. Изображение в них записывается на жесткий съемный диск (винчестер). Записанный в цифровом формате видеофильм можно просмотреть на персональнрм компьютере или преобразовать его в аналоговый сигнал и посмотреть по телевизору. Запись ведется со сжатием информации в формате MPEG/JPEG, стандартном для компьютеров, поэтому ее можно просматривать и даже редактировать на мониторе персонального компьютера.

В новейших видеокамерах вместо магнитной ленты для записи видеоизображения применены перезаписываемые оптические DVD-RW-диски. Записанный на них диск можно сразу же вставить в DVD-плеер для просмотра. Благодаря малому диаметру диска (8 см) габариты видеокамеры такие же, как и у обычных – с использованием кассет с магнитной пленкой. Время записи на DVD-диске составляет 30 мин, а в «режиме экономии» – 60 мин с некоторым понижением качества видеоизображения.

Цифровым видеокамерам, фотокамерам, диктофонам без подвижных узлов и деталей принадлежит будущее. Они более надежны, долговечны, легки и миниатюрны, не боятся встрясок при ходьбе, ударов.

Контрольные вопросы

1. Что понимается под аппаратным и программным обеспечением компьютера?
2. Назовите отличительные особенности ПК типа IBM PC.
3. Рассмотрите историю клона IBM PC по типу используемого микропроцессора.
4. Каковы основные устройства входят в аппаратное обеспечение ПК?
5. Каково назначение системной шины и разъемов расширения ПК.
6. Как связаны быстродействие микропроцессора и быстродействие ПК?
7. Как влияют характеристики МП и памяти на производительность ПК?
8. Объясните назначение адаптеров и контроллеров.
9. Что такое аналого-цифровой (АЦП) и цифро-налоговый (ЦАП) преобразователи?
10. В чем различие между носителями и накопителями информации?
11. Назовите основные виды носителей и накопителей информации в компьютере?
12. В чем различие между оперативной и долговременной памятью компьютера?
13. Назовите основные типы оптических компакт-дисков?
14. Что такое флэш-память?
15. В чем заключается разница между принтером и плоттером?

Глава 3. Информационное и программное обеспечение информационных технологий

3.1. Информационные ресурсы, продукты и услуги

Информационные ресурсы (ИР) – *это отдельные документы, массивы документов, документы и массивы документов в информационных системах (библиотеках, архивных фондах, банках данных и других информационных системах).*

Информационные ресурсы следует понимать как *знания, которые материализовались в виде документов, баз данных, баз знаний, программ, алгоритмов и т.д.,* поэтому ИР следует рассматривать как стратегические ресурсы общества. Методологии количественной и качественной оценки ИР не разработано. ИР являются базой для создания информационных продуктов.

Информационный продукт (ИП) – *совокупность данных, сформированная производителем для распространения в вещественной или невещественной формах. ИП распространяется с помощью информационных услуг.*

Информационная услуга (ИУ) – *предоставление в распоряжение пользователя ИП.*

В настоящее время оказание информационных услуг практически невозможно без создания и ведения **баз данных (БД)**.

Виды информационных услуг классифицируются в зависимости от вида ИП:

1. Выпуск информационных изданий;
2. Ретроспективный поиск информации – целенаправленный поиск по заявке и пересылка результатов;
3. Предоставление первоисточника или копии;
4. Традиционные услуги научно-технической информации:
- обзоры;
- переводы;
5. Дистанционный доступ:
- непосредственный доступ;
- косвенный доступ (бюллетени, справочная служба);
- Down loading: часть центральной БД (результат отбора по критериям поиска) загружается на ПК пользователя для дальнейшей работы;
- регулярный поиск;
6. Оказание информационных услуг:
- связь;
- программное обеспечение;
- создание информационных систем;
- обработка данных на вычислительном центре и т.д.

Рынок информационных продуктов и информационных услуг

Рынок ИП и ИУ – *система экономических, правовых, организационных отношений по торговле продуктами интеллектуального труда на коммерческой основе.* На этом рынке действуют:

• поставщики ИП и ИУ;
• потребители ИП и ИУ.

История развития рынка ИП и ИУ может быть представлена следующим образом:

• 50-е гг. – научные учреждения, гос. учреждения;
• 60-е гг. – электронные средства обработки и передачи информации; **важнейшая форма представления данных – базы данных;**
• 70-е гг. – глобальные сети передачи данных; д**иалоговый поиск информации в удаленной БД;**
• 80-е гг. – **всемирные сети передачи данных** (Internet), WWW, космическая и сотовая связь.

В *структуре рынка* ИП и ИУ можно выделить следующие компоненты:

1. Технологическая составляющая;
2. Нормативно-правовая составляющая;
3. Информационная составляющая;
4. Организационная составляющая.

В результате развития рынка ИП и ИУ формируется **инфраструктура информационного рынка – совокупность секторов**, *каждый из которых объединяет группы, предлагающие однородные информационные продукты и услуги.*

Подходы к определению инфраструктуры рынка ИП и ИУ различны. Например, можно предложить инфраструктуру из 5-ти секторов:

• научно-техническая информация (И);
• объекты художественной культуры;
• услуги образования;
• управленческие данные и сообщения;
• бытовая информация.

Другой пример инфраструктуры приведен на рис. 3.1. и также включает пять секторов:

1. Деловая информация:
• биржевая информация;
• статистическая информация;
• коммерческая информация.

2. Информация специалистов:
• профессиональная информация;
• научно-техническая информация;
• доступ к первоисточникам.

3. Потребительская информация:
• новости и литература;
• расписание, заказы;
• развлекательная: игры и т.д.

4. Обеспечивающие информационные системы и средства:
• программные продукты;
• технические средства;

Рис. 3.1. Сектора рынка информационных продуктов и услуг

- разработка и сопровождение информационных систем и технологий;
- консультирование по аспектам информационной технологии;
- подготовка источников информации: баз данных, баз знаний и т.п.

5. Услуги образования: обучение по дополнительным образовательным программам, преподавание специальных курсов и циклов дисциплин, репетиторство, занятия с обучающимися углубленным изучением предметов и другие услуги.

3.2. Классификация пакетов прикладных программ

Пакеты прикладных программ (ППП) являются наиболее динамично развивающейся частью рынка ИП и ИУ. Совершенствование ППП способствует внедрению компьютеров во все сферы деятельности. Развитие ППП и аппаратного обеспечения идет рука об руку – появление мощных по своим функциональным возможностям компьютеров способствует созданию улучшенных ППП, и наоборот, требования к улучшению ППП стимулируют развитие аппаратной базы.

Структура и принципы построения ППП определяются типом компьютера и операционной системы. В настоящий момент среди пользователей наиболее распространены ППП для IBM PC совместимых компьютеров с ОС MS DOS и Windows. В целом классификация ППП приведена на рис. 3.2.

Проблемно-ориентированные ППП – наиболее развитая и многочисленная по количеству пакетов часть ППП. Разберем подробнее некоторые продукты.

Особенности построения и области применения ППП

Текстовые процессоры (ТП) – предназначены для работы с документами (текстами). Позволяют компоновать, форматировать, редактировать тексты, обладают функциями по работе с блоками текста, объектами. При-

Рис. 3.2. Классификация пакетов прикладных программ

мерами ТП для ПК являются MS Word, Лексикон, Chiwriter и т.д. Работа с текстовыми данными будет рассмотрена в отдельном разделе.

Настольные издательские системы (НИС) – программы профессиональной издательской деятельности, позволяющие осуществлять электронную верстку основных типов документов. Средства НИС позволяют:

• верстать текст, используя эталонные страницы, создавать колонки текста, работать с длинными документами как с единым целым;

• осуществлять полиграфическое оформление путем настройки базовой линии, поворотов текста и т.п.;

• импортировать разнообразные данные и собирать текст;

• обрабатывать графические изображения, начиная от возможности импорта и кончая возможностью редактирования графических объектов, поддерживать полиграфические цветовые модели типа CMYK;

• обеспечивать вывод документов полиграфического качества, реализуя функции цветоделения, преобразования дополнительных цветов в CMYK, надпечатки, печати негативов;

• работать в сетях на разных платформах.

Графические редакторы – пакеты, предназначенные для обработки графической информации. Делятся на ППП обработки **растровой** и **векторной** графики.

Пакеты прикладных программ растровой графики предназначены для работы с фотографическими изображениями. Они включают средства по кодированию изображений в цифровую форму, обработки и редактирования изображений (насыщенность, контрастность, цветовая гамма). Предусмотрены средства преобразования в изображения с разными степенями разрешения и разными форматами данных – BMP, GIF,PCX и т.д., а также средства вывода готовых изображений в виде твердых копий. Лидером среди растровых пакетов является Adobe Photoshop. Среди других следует упомянуть Aldus Photostyler, Picture Publisher, Photo Works Plus. Все программы рассчитаны на работу в среде Windows.

ППП векторной графики – профессиональные пакеты для работы, связанной с художественной и технической иллюстрацией, дизайном и занимают промежуточное положение между САПР и НИС. Они включают в себя:

• инструментарий создания графических иллюстраций – дуги, окружности, эллипсы, ломаные и многоугольники и т.д.;

• средства разбиения и объединения объектов, копирования, штриховки, перспективы;

• средства обработки текста – различные шрифты, выравнивание, параграфы и т.д.;

• средства импорта и экспорта графических объектов разных графических форматов – BMP, CDR, PCX, WMF и т.д.;

• средства вывода на печать в *полиграфическом исполнении экранного образа;*

• сложные средства настройки цвета – оттенки серого вместо цветов, замещение цвета подслоя, компенсация размеров точки при печати и т.д.

Стандартом является пакет Coreldraw. Среди других можно выделить Adobe Illustrator, Aldus Freehand, Professional Draw.

Электронные таблицы (табличные процессоры) – пакеты программ, предназначенные для обработки табличным образом организованных данных. Наиболее распространены и популярны в настоящее время Excel, Quattro Pro, Supercalc. Использование электронных таблиц рассматривается в отдельном разделе.

Организаторы работ – ППП, предназначенные для автоматизации процедур планирования использования ресурсов (времени, денег, материалов) и имеют две разновидности: 1) управление проектами и 2) организация деятельности отдельного человека.

Пакеты первого типа предназначены для сетевого планирования и управления проектами. Средства этих пакетов позволяют:

• манипулировать данными на уровне графических объектов;

• управлять множеством задач (>1000) и ресурсов в рамках одного проекта;

• планировать с точностью до минут;

• использовать индивидуальные графики ресурсов;

• использовать задачи на опережение с фиксированной длительностью и задержкой;

• работать с изменяющейся величиной загрузки персонала и стоимостью ресурса;

• использовать библиотеку типовых решений;

• генерировать отчеты с графиками и инструкции;

• осуществлять экспорт и импорт в электронные таблицы.

К пакетам первого типа относятся: MS Project, Time Line, CA-Superproject.

Пакеты второго типа представляют собой электронный помощник делового человека. По своей сути они выполняют функции электронных секретарей и предназначены для управления деловыми контактами. Основные функции следующие:

• формирование графика деловой активности с автоматическим контролем за его выполнением;

• ведение электронной картотеки;

• хранение произвольного объема данных в большом количестве баз данных;

• наличие полнофункционального текстового процессора, включающего все необходимые средства для создания деловых документов;

• генерация типовых документов по базе данных;

• обеспечение безопасности и конфиденциальности данных;

• работа с телефонной линией (автонабор, автодозвон и т.д.);

• работа с E-mail и Fax.

Самыми известными пакетами являются Lotus Organizer, Microsoft Shedule и ACTI.

Системы управления базами данных (СУБД) предназначены для создания, хранения и ведения баз данных. СУБД разработано великое множество, для различных классов компьютеров и операционных систем. Они отличаются способами организации данных, форматом данных, языком формирования запросов. Самыми популярными являются *реляционные СУБД* для IBM PC совместимых ПК: dBase, Paradox, MS Access, FoxPro. Для серверов и сетей популярны продукты Oracle. Использование баз данных в правоохранительной деятельности рассмотрено в отдельном разделе.

Пакеты демонстрационной графики – конструкторы графических образов деловой информации, т.е. *средства создания презентаций*, дающие возможность в наглядной и динамичной форме представить результаты аналитического исследования.

Работа с пакетом строится по следующему плану:

• разработка плана представления;

• выбор шаблона для оформления элементов;

• формирование и импорт текстов, графиков, таблиц, диаграмм, звуковых эффектов.

Соответственно, в состав пакета входят:

1) планировщик, который позволяет составить план и отформатировать его для печати;

2) шаблоны для создания слайдов, наполнения их текстовыми и графическими объектами;

3) средства для вывода на принтер, печать на прозрачную пленку для диапозитивов;

4) средства управления скоростью, порядком следования слайдов, импорта диаграмм и данных для графиков из табличных процессоров, баз данных.

Среди пакетов данного типа следует выделить MS PowerPoint, Harvard Graphics, WordPerfect presentations и т.д.

Пакеты программ мультимедиа – средства обработки аудио и видео информации. Их использование требует *дополнительного аппаратного обеспечения* – аудиоплат и видеоплат, колонок, CD-ROM и т.д.

Суть мультимедиа пакетов можно обозначить как преобразование самых разнообразных видов аналоговой информации в цифровую. Мультимедиа требует значительных вычислительных затрат компьютера.

Мультимедиа программы можно разделить на *две большие группы*. **Первая** включает пакеты для образования и досуга.

Вторая группа включает средства подготовки видеоматериалов, демонстрационных дисков, стендовых материалов, анимации. В данную группу включаются различные инструментальные средства.

К пакетам второй группы относятся Director for Windows, Multimedia ViewKit, Nec MultiSpin.

Системы автоматизации проектирования предназначены для автоматизации проектно-конструкторских работ в машиностроении, строительстве и т.п. Они включают большой набор инструментальных средств, позволяющих реализовать следующие основные функции:

• масштабирование объектов;

• группировка, передвижение с растяжкой, поворот, разрезание, изменение размеров;

• работа со слоями;

• перерисовка (фоновая, ручная, прерываемая);

• управление файлами в части каталога библиотек и каталогов чертежей;

• использование большого количества разнообразных чертежных инструментов; использование библиотеки символов, выполнение надписей;

• автоматизация процедур с использованием встроенного макроязыка;

• работа с цветом;

• коллективная работа в сети;

• экспорт-импорт файлов различных форматов.

Стандартом среди пакетов данного класса является AutoCAD фирмы Autodesk. Следует отметить также программы DesignCAD, Drawbase, Microstation, TurboCAD, TopoMaster (для рисования топографических изображений).

Программы распознавания символов предназначены для перевода графического изображения текста (буквы и цифры) в ASCII коды символов. Основные продукты данного типа поставляются *совместно со сканерами.* В программах данного типа стараются реализовать следующие возможности:

- настройку на различные кегли шрифтов;
- устойчивое распознавание символов при наклоне;
- множественную фрагментацию – распознавание многоколонных текстов, нескольких шрифтов одновременно;
- отделение текста от графики;
- ввод многостраничных документов;
- настройку на тип шрифта (полиграфия, машинопись и т.д.);
- подбор яркости;
- импорт графических изображений разных форматов;
- встроенные словари для проверки орфографии;
- автоматический перевод текста документа по мере ввода.

К пакетам данного типа относятся FineReader, CunieForm, Tigertm, OmniPage.

Финансовые программы предназначены для ведения личных финансов, автоматизации бухгалтерского учета фирм и предприятий, анализа инвестиционных проектов, экономического обоснования финансовых сделок и т.п. Особую популярность приобрели *программы планирования личных денежных ресурсов*, например, MS Money, MoneyCounts, MECA Software. В таких программах предусмотрены средства ведения деловых записей в виде записной книжки и расчета финансовых операций.

Круг специализированных бухгалтерских программ необычайно велик. Среди наиболее популярных отечественных разработок следует назвать Турбобухгалтер, 1С:Бухгалтерия.

Аналитические ППП – программы для проведения статистических расчетов. Они значительно перекрывают по возможностям статистического анализа электронные таблицы. К пакетам данного типа относятся популярные зарубежные программы StatGraphics, SPSS, Statistika. Применение и аналитические возможности статистических пакетов рассмотрены в отдельном разделе.

Интегрированные пакеты прикладных программ

Наиболее мощная и динамично развивающаяся часть программного обеспечения. В рамках этого ПО можно выделить две наиболее значимые группы: 1) **полносвязанные пакеты** и 2) **объектно-связанные пакеты**.

Полносвязанные пакеты представляют собой многофункциональный автономный пакет, в котором *в одно целое соединены функции и возможности специализированных (проблемно-ориентированных) пакетов, родственных по технологии обработки данных.* По сути, в таких программах происходит интеграция функций редактора текстов, СУБД и табличного процессора. Пакеты обеспечивают связь между данными, однако за счет сужения возможностей каждого компонента в отдельности. Представите-

лями данного класса пакетов являются: для ОС MS DOS – ***FrameWork***, ***Symphony***, для Windows – ***Microsoft Works***, ***Lotus Works***.

Объектно-связанные интегрированные пакеты – последнее слово в технологии программного обеспечения. *Подход к интеграции программных средств заключается в объединении специализированных пакетов в рамках единой ресурсной базы и обеспечении взаимодействия приложений, т.е. программ пакета, на уровне объектов и единого упрощенного центра – переключателя между приложениями.*

Наиболее мощные пакеты данного типа: ***Microsoft Office, Lotus SmartSute, Borland Office***. В **профессиональной версии** пакетов присутствуют четыре приложения: текстовый редактор, СУБД, табличный процессор, пакет демонстрационной графики. В **пользовательском варианте** СУБД отсутствует. В объектно-ориентированных пакетах **эффект интеграции не сводится** к простой сумме составляющих компонентов – дополнительные возможности получаются за счет взаимодействия компонентов пакета в процессе работы. В полносвязанных пакетах преимущества интеграции часто сводятся на нет ввиду отсутствия той или иной функции, имеющейся в специализированном пакете.

Объектно-связанный подход к интеграции предполагает придание компонентам единообразного согласованного интерфейса: пиктограмм и меню, диалоговых окон, макроязыка и т.п. **Главной особенностью** является использование общих ресурсов. Выделяются ***четыре основных вида*** совместного доступа к ресурсам:

1. использование общих утилит для всех программ комплекса (например, утилита проверки орфографии);
2. применение объектов, которые могут находиться в совместном использовании программ комплекса;
3. простой переход или запуск одного приложения из другого;
4. единый макроязык как средство автоматизации работы с приложениями, что позволяет организовать комплексную обработку информации, поскольку программирование ведется на едином языке макроопределений.

Совместное использование объектов – краеугольный камень *современной технологии интеграции*. На данный момент существуют ***два стандарта***:

• Object Linking and Embedding OLE2.0 динамической компоновки и встраивания объектов фирмы Microsoft.

• OpenDoc (открытый документ) фирм Apple, Borland, IBM, Novell.

OLE2.0 дает возможность помещать информацию, созданную одной прикладной программой, в другую, при этом имеется возможность редактировать информацию в новом документе средствами того продукта, с помощью которого объект ранее был создан.

OLE2.0 позволяет переносить объекты из окна одной прикладной программы в окно другой.

OLE2.0 предусматривает возможность общего использования функциональных ресурсов программ: например, модуль построения графиков ЭТ

может быть использован в текстовом редакторе.

Основной недостаток OLE2.0 – ограничение на размер объекта размером одной страницы.

OpenDoc – объектно-ориентированная система, использующая в качестве модели объекта распределенную модель системных объектов (DSOM – Distributed System Object Model), разработанную фирмой IBM для операционной системы OS/2. Предполагается наличие совместимости между OLE и OpenDoc.

Контрольные вопросы

1. Что понимается под информационными продуктами?
2. Что понимается под информационными услугами?
3. Назовите основные виды информационных услуг.
4. Перечислите основные услуги образования.
5. Охарактеризуйте структуру и принципы построения ППП.
6. Назовите основные составляющие проблемно-ориентированных ППП.
7. Что включают в себя ППП векторной графики?
8. Какие задачи решаются с помощью ППП организаторов работ?
9. Для чего предназначены ППП демонстрационной графики?
10. Какие задачи можно решать с помощью ППП мультимедиа?
11. Какие возможности реализованы в ППП распознавания символов?
12. Каковы функции аналитических ППП?
13. Что понимается под интегрированными ППП?
14. Дайте классификацию интегрированных ППП.
15. Назовите основные преимущества объектно-связанных интегрированных пакетов.

Глава 4. Информационно-вычислительные сети

4.1. Понятие информационно-вычислительной сети. Классификация ИВС

Информационно-вычислительная сеть (ИВС) – два или более компьютеров, соединенных посредством каналов передачи данных (линий проводной или радиосвязи, линий оптической связи) с целью объединения ресурсов и обмена информацией. Под *ресурсами* понимаются аппаратные средства и программные средства.

Соединение компьютеров в сеть обеспечивает следующие основные возможности:

• **объединение ресурсов** – возможность резервировать вычислительные мощности и средства передачи данных на случай выхода из строя отдельных из них с целью быстрого восстановления нормальной работы сети;

• **разделение ресурсов** – возможность стабилизировать и повысить уровень загрузки компьютеров и дорогостоящего **периферийного** оборудования, управлять периферийными устройствами;

• **разделение данных** – возможность создавать распределенные **базы данных**, размещаемые в памяти отдельных компьютеров, и управлять ими с периферийных рабочих мест;

• **разделение программных средств** – возможность совместного **использования** программных средств;

• **разделение вычислительных ресурсов** – возможность организовать **параллельную** обработку данных, используя для этой цели другие системы, входящие в сеть;

• **многопользовательский режим**.

В целом, как показала практика, *стоимость обработки данных в вычислительных сетях* за счет расширения возможностей обработки данных, лучшей загрузки ресурсов и повышения надежности функционирования системы не менее чем в полтора раза ниже по сравнению с обработкой аналогичных данных на автономных компьютерах.

При объединении компьютеров в сеть система должна сохранять *надежность*, т.е. отказ какого-либо компьютера не должен приводить к остановке работы системы, и, более того, должна обеспечиваться передача функций отказавшего компьютера на другой компьютер сети.

На сегодняшний день более 130 миллионов компьютеров, т.е. более 80%, объединены в информационно-вычислительные сети, начиная от малых локальных сетей до глобальных сетей типа Internet. Тенденция к объединению компьютеров в сети обусловлена рядом причин, таких, как:

• необходимость получения и передачи сообщений не отходя от рабочего места;

• необходимость быстрого обмена информацией между пользователями;

• возможность быстрого получения разнообразной информации, вне зависимости от ее местонахождения.

Бурное развитие компьютерных сетей и подключение все большего числа персональных компьютеров к глобальным сетям привело в последнее десятилетие к формированию основ концепции *сетевого компьютера*. Суть ее заключается в том, что персональный компьютер, работающий в сети, получает определенные преимущества перед автономным персональным компьютером:

• программы загружаются непосредственно из сети;

• нет необходимости иметь на ПК жесткий диск;

• экономятся время и средства на покупку и обновление ПО, т.к. оно устанавливается и обновляется через сеть;

• имеется доступ к электронной почте и ресурсам Internet.

Все функции по установке и обновлению программного обеспечения сетевого компьютера, наряду с другими функциями по поддержке функционирования сети, берут на себя *провайдеры*, обслуживающие сеть за небольшую абонентскую плату.

4.2. Классификация ИВС

Вычислительные сети классифицируют по различным признакам:

а) по территории:

Локальные вычислительные сети (ЛВС) охватывают небольшие территории диаметром до 5–10 км внутри отдельных контор (офисов), бирж, банков, учреждений, вузов, научно-исследовательских организаций и т.п. При помощи общего канала связи ЛВС может объединять от десятков до сотен абонентских узлов, включающих персональные компьютеры, внешние запоминающие устройства, дисплеи и др.

Современная стадия развития ЛВС характеризуется почти повсеместным переходом от отдельных сетей к сетям, которые охватывают все предприятие (фирму, компанию), объединяют разнородные вычислительные ресурсы в единой среде. Такие сети получили название **корпоративных**;

Региональные и глобальные ИВС образуются путем объединения локальных ИВС на отдельных территориях или по всей планете. Наиболее крупной глобальной компьютерной сетью является сеть Internet;

б) по способу управления:

Сети с *централизованным управлением*, в которых выделяются одна или несколько машин, управляющих процессом обмена данных по сети. Эти машины называются *серверами*. Остальные компьютеры называются *рабочими станциями*. Рабочие станции имеют доступ к дискам сервера и совместно используемым принтерам, однако с рабочей станции нельзя работать с дисками других рабочих станций и для обмена данными пользователи вынуждены использовать диски сервера.

Примером сети с централизованным управлением может служить *сеть Novell NetWare*. Выделенный компьютер-сервер поддерживает и отвечает за все сетевые ресурсы, в то время как любой клиент имеет доступ к этим ресурсам только через сетевую оболочку, имеющуюся на каждой рабочей станции.

Децентрализованные (одноранговые) сети не содержат в своем составе выделенных серверов. Функции управления сетью передаются по очереди от одной рабочей станции к другой. Как правило, рабочие станции имеют доступ к дискам и принтерам других рабочих станций. Пример одноранговой сети – сеть Windows, в которой нажатием на кнопку мыши Вы можете предоставить свой диск или принтер в коллективное пользование.

в) по характеру выполняемых функций:

• вычислительные;

• информационные;

г) по составу вычислительных средств:

• однородные – объединяют однородные вычислительные средства;

• неоднородные – объединяют различные вычислительные средства;

д) по типу организации передачи данных:

• коммутация каналов;

• коммутация сообщений;

• коммутация пакетов.

4.3. Модель взаимодействия открытых систем. Организация работы сети

Процесс передачи данных в сети требует единого представления данных в линиях связи, по которым передается информация. Все сети работают в одном принятом для компьютерных сетей стандарте – *стандарте взаимодействия открытых систем* (Open Systems Interconnection (**OSI**)).

Базовая модель взаимодействия открытых систем разработана Международной организацией по стандартизации (International Standards Organization (ISO)). Эта модель является международным стандартом для передачи данных.

Модель содержит ***семь уровней***:

1. **физический** – битовые протоколы передачи информации;
2. **канальный** – управление доступом к среде, формирование кадров;
3. **сетевой** – маршрутизация, управление потоками данных;
4. **транспортный** – обеспечение взаимодействия удаленных процессов;
5. **сеансовый** – поддержание диалога между удаленными процессами;
6. **представительский** – интерпретация передаваемых данных;
7. **прикладной** – пользовательское управление данными.

Основная идея базовой модели заключается в том, что каждому уровню отводится конкретное место в процессе передачи данных в сети, т.е. общая задача передачи данных расчленяется на отдельные легко обозримые задачи. В результате вычислительная сеть представляется как комплексная система, которая координирует взаимодействие задач пользователей.

Протоколами называются соглашения, необходимые для связи одного уровня модели с выше- и нижерасположенными уровнями.

Уровни базовой модели проходятся в направлении вверх от источника данных (от уровня 1 к уровню 7) и в направлении вниз от приемника данных (от уровня 7 к уровню 1). В первом случае на каждом уровне поступающие

данные анализируются и, по мере надобности, передаются далее в вышерасположенный уровень, пока информация не будет передана в пользовательский прикладной уровень. Во втором случае пользовательские данные передаются в нижерасположенный уровень вместе со специфическим для уровня заголовком до тех пор, пока не будет достигнут последний уровень.

Далее мы подробнее рассмотрим функции каждого уровня.

Физический уровень. На этом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в сетевых системах. Установление физической связи является основной функцией первого уровня. *Протоколы физического уровня* включают рекомендации V.24 МККТТ (CCITT), EIA RS232 и X.21. В будущем определяющую роль для функций передачи данных будет играть стандарт ISDN (*Integrated Services Digital Network*).

Канальный уровень. Канальный уровень организует канал для передачи данных и формирует из данных, передаваемых физическим уровнем, так называемые последовательности кадров. На этом уровне осуществляются управление доступом к передающей среде, используемой несколькими компьютерами, синхронизация, обнаружение и исправление ошибок.

Сетевой уровень. На сетевом уровне устанавливается связь в вы-числительной сети между двумя абонентами. Соединение происходит благодаря функциям маршрутизации, которые требуют наличия сетевого адреса в пакете. Сетевой уровень должен обеспечивать обработку ошибок, мультиплексирование, управление потоками данных. Самый известный протокол этого уровня – рекомендация X.25 МККТТ для сетей общего пользования с коммутацией пакетов.

Транспортный уровень. Транспортный уровень поддерживает не-прерывную передачу данных между двумя взаимодействующими друг с другом пользовательскими процессами. Качество транспортировки, безошибочность передачи, независимость вычислительных сетей, сервис транспортировки из конца в конец, минимизация затрат и адресация связи гарантируют непрерывную и безошибочную передачу данных.

Сеансовый уровень. Сеансовый уровень координирует прием, передачу и организацию одного сеанса связи. Для координации необходимы контроль рабочих параметров сети, управление потоками данных промежуточных накопителей и диалоговый контроль, гарантирующий передачу имеющихся в распоряжении данных. Сеансовый уровень содержит функции управления паролями, подсчета платы за пользование ресурсами сети, управления диалогом, синхронизации и отмены связи в сеансе передачи в случае возникновения сбоя вследствие ошибок в нижерасположенных уровнях.

Представительский уровень. Уровень представления данных предназначен для интерпретации данных, а также подготовки данных для пользовательского прикладного уровня. На этом уровне происходит преобразование данных из кадров, используемых для передачи данных, в экранный формат или формат для печатающих устройств.

Прикладной уровень. На прикладном уровне необходимо предоставить в распоряжение пользователей переработанную информацию, что является задачей системного и прикладного программного обеспечения пользователя.

Организация работы сети

Для передачи информации по коммуникационным линиям данные преобразуются в цепочку следующих друг за другом битов. Алфавитно-цифровые символы представляются с помощью битовых комбинаций. Существуют специальные кодовые таблицы, содержащие 4-, 5-, 6-, 7- или 8-битовые коды символов.

При передаче информации в сетях на практике применяют следующие кодировки:

ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) – передача символьной информации с помощью 7-битового кодирования, позволяющего закодировать заглавные и строчные буквы английского алфавита, а также некоторые спецсимволы;

8-битовые коды (напр. КОИ-8 и др.) – для представления символов национальных алфавитов и специальных знаков (напр. символов псевдографики).

Для обмена информацией в сетях используется *принцип пакетной коммутации*. При этом информация перед передачей разбивается на *блоки*, которые представляются в виде *пакетов* определенной длины, содержащих, кроме информации пользователя, некоторую служебную информацию, позволяющую различать пакеты и выявлять возникающие при передаче ошибки.

Для правильной, т.е. полной и безошибочной передачи блоков данных необходимо придерживаться согласованных и установленных правил, которые называются ***протоколами передачи данных***.

Протоколами передачи данных оговариваются следующие моменты:

• *Синхронизация* – механизм распознавания начала и конца блока данных;

• *Инициализация* – механизм установления соединения между взаимодействующими партнерами;

• *Пакетирование* – механизм разбиения передаваемой информации на блоки определенной длины, включая опознавательные знаки начала блока и его конца;

• *Адресация* – способ формирования адреса, что обеспечивает идентификацию компьютера в сети для установления взаимодействия;

• *Обнаружение ошибок* – установка битов четности и вычисление контрольных сумм;

• *Нумерация* – механизм присвоения номеров последовательным блокам с целью сборки сообщения;

• *Управление потоком* – механизм распределения и синхронизации информационных потоков в сети;

• *Восстановление* – способ восстановления процесса передачи данных в сети после его прерывания.

Для доставки пакетов используются *коммутируемые и некоммутируемые каналы*. Для понимания принципов коммутации можно привлечь ана-

логию с телефонной и почтовой связью.

Компьютер пользователя может работать в режиме, когда он непосредственно присоединен к сети (режим ON LINE). Однако часто приходится обращаться к сетевым ресурсам по коммутируемым каналам (режим OFF LINE). В этом случае помогают *серверы доступа*. Серверы доступа обеспечивают удаленную связь пользователя с удаленной ЛВС с помощью программы дистанционного управления. Каждый сервер доступа соединен с ЛВС и может извлекать прикладные программы с жесткого диска сетевого сервера и загружать их для выполнения. В результате удаленные пользователи имеют возможность работать с этими программами, т.е. проверять сообщения электронной почты, передавать файлы, распечатывать информацию на принтере и т.п.

Обязанность поддержания функционирования сети возлагается на *администратора* или *супервизора*. Он обеспечивает контроль работы с любой рабочей станции, а также сохранение информации от несанкционированного доступа. Высокая степень конфиденциальности достигается за счет ограниченного доступа к определенным файлам, рабочим станциям, ограничения времени доступа, а также системы паролей и приоритетов.

Соединение компьютера через телефонную линию осуществляется с помощью *модема*. Телефонная линия предназначена для передачи только аналоговых звуковых сигналов. Чтобы передать по ней цифровые импульсы, их нужно промодулировать, то есть преобразовать в колебания звуковой частоты.

Еще один метод доступа к сети основан на использовании *электронных досок объявлений*. При вызове электронной доски объявлений на экране появляется меню сообщений и функции. Пользователь может прочитать нужное сообщение, отправить свое сообщение, загрузить или выгрузить файл.

Электронная почта. При установке специального программного обеспечения любой персональный компьютер может обмениваться сообщениями с любым компьютером сети.

4.4. Локальные вычислительные сети. Операционные системы ЛВС

Локальной вычислительной сетью (ЛВС) называют совместное подключение нескольких отдельных компьютеров к единому каналу передачи данных. Понятие ЛВС (англ. LAN – Lokal Area Network) относится к географически ограниченным (территориально или производственно) аппаратно-программным комплексам, в которых несколько компьютерных систем связаны между собой с помощью соответствующих средств коммуникаций.

ЛВС предоставляет возможность одновременного использования программ и баз данных несколькими пользователями, а также возможность взаимодействия с другими рабочими станциями, подключенными к сети. Посредством ЛВС в систему объединяются персональные компьютеры, расположенные на многих удаленных рабочих местах, которые используют совместно оборудование, программные средства и информацию. Рабочие места сотруд-

ников перестают быть изолированными и объединяются в единую систему.

Важнейшей характеристикой ЛВС является скорость передачи информации. В идеале, при посылке и получении данных через сеть время отклика должно быть почти таким же, как если бы они были получены от ПК пользователя, а не из другого места сети. Это требует передачи данных со скоростью 10 Мбит/с и выше. Реально достигаются следующие скорости:

• Коаксиальный кабель – 10 ÷ 50 Мбод;
• Витая пара – до 10 Мбод;
• Специальная витая пара 5 категории – до 100 Мбод;
• Оптическое волокно – до 1Гбод;
• Телефонная линия – от 2400 бод до 56 кбод;
• Спутник – 10000 компьютеров одновременно и скорость около 1 Мбод.

Компоненты ЛВС: сетевые устройства и средства коммуникаций.

В ЛВС реализуется принцип модульной организации, который позволяет строить сети различной конфигурации с различными функциональными возможностями. Основными компонентами, из которых строится сеть, являются следующие:

- ***серверы*** – отдельные компьютеры с программным обеспечением, выполняющие функции управления сетевыми ресурсами общего доступа;
- ***передающая среда*** – коаксиальный кабель, телефонный кабель, витая пара, оптоволоконный кабель, радиоэфир и др.;
- ***рабочие станции*** – ПК, АРМ или собственно сетевая станция. Если рабочая станция подключена к сети, для нее могут не потребоваться ни винчестер, ни флоппи-диски. Однако в этом случае необходим сетевой адаптер – специальное устройство для дистанционной загрузки операционной системы из сети;
- ***платы интерфейса*** – сетевые платы для организации взаимодействия рабочих станций с сетью;
- ***сетевое программное обеспечение***.

Рассмотрим некоторые из перечисленных компонентов сети более подробно.

Серверы. Сеть может иметь один или несколько серверов. Различные серверы могут использоваться для управления работой сети (*серверы сети*), хранения информации в виде файлов (*файл-серверы*), поиска и извлечения информации из баз данных (*серверы баз данных*), рассылки информации (*почтовые серверы*), сетевой печати (*серверы печати*) и др. Диски серверов доступны со всех остальных рабочих станций сети, если у пользователей есть соответствующие полномочия.

Взаимодействие сервера с рабочими станциями происходит примерно по следующей схеме. По мере необходимости рабочая станция отправляет серверу запрос на выполнение каких-либо действий: прочитать данные, напечатать документ, передать электронное письмо и т.п. Сервер выполняет затребованное действие и выдает подтверждение.

Передающая среда. Передающие среды характеризуются скоростью и

дальностью передачи информации и надежностью.

В качестве средств коммуникации в ЛВС чаще всего используются витая пара, коаксиальный кабель, оптоволоконные линии. При выборе передающей среды необходимо учитывать следующие показатели:

- скорость передачи информации;
- дальность передачи информации;
- защищенность передачи информации;
- надежность передачи информации;
- стоимость монтажа и эксплуатации.

Одновременное выполнение требований, предъявляемых к передающей среде, является трудно разрешимой задачей. Так, например, большая скорость передачи данных часто ограничена предельно допустимым расстоянием надежной передачи данных, при обеспечении необходимого уровня защиты передаваемых данных. Стоимость средств коммуникации сказывается на возможности наращивания и расширения сети.

Характеристики типовых передающих сред приведены в таблице 4.1.

Рассмотрим свойства некоторых передающих сред подробнее.

Витая пара. Витое двухжильное проводное соединение (twisted pair), наиболее дешевое среди передающих сред. Позволяет передавать информацию со скоростью до 10 Мбит/с, легко наращивается, помехозащищенность низкая. Длина кабеля не превышает 1000 м при скорости передачи 1 Мбит/с. Для повышения помехозащищенности информации используют экранированную витую пару, помещенную в оболочку, аналогичную экрану коаксиального кабеля. Цена такой пары близка к цене коаксиального кабеля.

Коаксиальный кабель. Коаксиальный кабель применяется для связи на расстояния до нескольких километров, имеет хорошую помехозащищенность при средней цене. Скорость передачи информации от 1 до 10 Мбит/с, в некоторых случаях достигает 50 Мбит/с. Коаксиальный кабель может использоваться для широкополосной передачи информации.

Широкополосный коаксиальный кабель. Такой коаксиальный кабель слабо восприимчив к помехам, легко наращивается, однако имеет высокую цену. Скорость передачи информации достигает 500 Мбит/с. Для передачи информации на расстояние более 1,5 км в базисной полосе частот необходим ***репитер*** (усилитель сигнала), при этом расстояние устойчивой передачи увеличивается до 10 км.

Ethernet кабель. Толстый Ethernet – коаксиальный кабель с волновым сопротивлением 50 Ом (thick Ethernet. или желтый кабель – yellow cable). Максимально допустимое расстояние передачи без репитера не превышает 500 м, а общая длина сети Ethernet – 3000 м.

Тонкий Ethernet – коаксиальный кабель с волновым сопротивлением 50 ом (thin Ethernet) и скоростью передачи информации 107 бит/с, более дешевый, чем толстый Ethernet. ЛВС с кабелем thin Ethernet характеризуются низкой стоимостью, минимальными затратами при наращивании и не требуют дополнительного экранирования. При соединении сегментов thin

Таблица 4.1.

Характеристики типовых передающих сред

Показатели	Передающая среда		
	Витая пара	Коаксиальный кабель	Оптоволоконный кабель
Цена	Невысокая	Средняя	Высокая
Наращивание	Очень простое	Проблематично	Проблематично
Защита от прослушивания	Плохая	Хорошая	Очень хорошая
Заземление	Нет	Требуется	Нет
Помехозащищенность	Низкая	Высокая	Очень высокая

Ethernet требуются репитеры. Расстояние между рабочими станциями без репитеров не может превышать 300 м, а общая длина сети – 1000 м.

Оптоволоконный кабель. Наиболее дорогостоящей передающей средой для ЛВС является оптоволоконный кабель, называемый также стекловолоконным кабелем. Скорость передачи информации по нему достигает нескольких гигабит в секунду при допустимой длине более 50 км. Помехозащищенность оптоволоконного кабеля очень высокая, поэтому ЛВС на его основе применяются там, где возникают электромагнитные помехи и требуется передача информации на большие расстояния без использования репитеров. Сети устойчивы против подслушивания, так как техника ответвлений в оптоволоконных кабелях очень сложна. Обычно ЛВС на основе оптоволоконного кабеля строятся по звездообразной топологии.

Топология ИВС. Топология, т.е. конфигурация соединения элементов в ЛВС, привлекает к себе внимание в большей степени, чем другие характеристики сети. Это связано с тем, что именно топология во многом определяет самые важные свойства сети, такие, например, как *надежность* и *производительность*.

Существуют разные подходы к классификации топологий ЛВС. Согласно одному из них, конфигурации локальных сетей делят на два основных класса: ***широковещательные*** и ***последовательные***.

В *широковещательных конфигурациях* каждый ПК передает сигналы, которые могут быть восприняты остальными ПК. К таким конфигурациям относятся общая шина, дерево (соединение нескольких общих шин с помощью репитеров), звезда с пассивным центром. Главное преимущество конфигураций этого класса – простота технической организации работы сети. В широковещательных ЛВС рабочие станции получают частоту, на которой они могут отправлять и получать информацию. Пересылаемые данные модулируются на соответствующих несущих частотах. Такая техника позволяет одновременно транспортировать в коммуникационной среде довольно большой объем данных.

В *последовательных конфигурациях* каждый физический подуровень передает информацию только одному ПК. К таким конфигурациям относятся звезда с интеллектуальным центром, кольцо, иерархическое соединение, снежинка. Основное достоинство – простота программной реализации работы сети. Для предотвращения коллизий при передаче информации применяется *временной метод разделения*, согласно которому каждой подключенной рабочей станции в определенные моменты времени предоставляется исключительное право на использование канала передачи информации.

В различных топологиях реализуются различные *принципы передачи информации*. В широковещательных это *селекция информации*, в последовательных – *маршрутизация информации*.

Звездообразная топология. Топология сети в виде *звезды с активным центром* унаследована из области *мэйнфреймов*, где головная машина получает и обрабатывает все данные с терминальных устройств как активный узел обработки данных. Вся информация между периферийными рабочими станциями проходит через центральный узел вычислительной сети (рис. 4.1.).

Пропускная способность сети определяется вычислительной мощностью центрального узла и гарантируется для каждой рабочей станции. Коллизий, т.е. столкновений в передаче данных не возникает.

Кабельное соединение топологии относительно простое, поскольку каждая рабочая станция связана с центральным узлом, однако затраты на прокладку линий связи высокие, особенно когда центральный узел географически расположен не в центре топологии. При расширении ЛВС к новой рабочей станции необходимо прокладывать отдельный кабель от центрального узла сети.

Производительность ЛВС звездообразной топологии в первую очередь определяется параметрами центрального узла, который выступает в качестве сервера сети. Он может оказаться узким местом сети. В случае выхода из строя центрального узла нарушается работа сети в целом.

При хорошей производительности центрального узла топология *является одной из наиболее быстродействующих топологий* ЛВС. Частота запросов на передачу информации от одной станции к другой невысокая по сравнению с другими топологиями. Также важно, что в ЛВС с центральным узлом управления можно реализовать оптимальный механизм защиты от несанкционированного доступа к информации.

Кольцевая топология. В кольцевой топологии сети рабочие станции ЛВС связаны между собой по кругу. Последняя рабочая станция связана с первой, т.е. коммуникационная связь замыкается в кольцо (рис. 4.2.).

Прокладка линий связи между рабочими станциями может оказаться довольно дорогостоящей, особенно если территориально рабочие станции расположены далеко от основного кольца.

Сообщения в кольце ЛВС циркулируют по кругу. Рабочая станция посылает по определенному адресу информацию, предварительно получив из кольца запрос. Передача информации оказывается достаточно эффек-

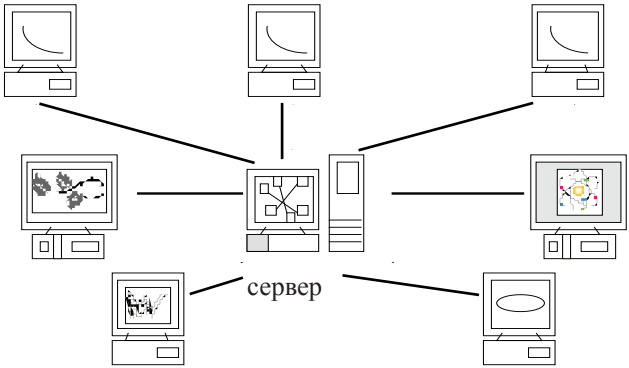

Рис. 4.1. Топология сети в виде звезды

тивной, так как сообщения можно отправлять одно за другим. Так, например, можно сделать кольцевой запрос на все станции. Продолжительность передачи информации увеличивается пропорционально количеству рабочих станций, входящих в ЛВС.

Главная проблема кольцевой топологии состоит в том, что каждая рабочая станция должна участвовать в передаче информации, и в случае выхода из строя хотя бы одной из них вся сеть парализуется. Неисправности в кабельной системе локализуются легко.

Расширение сети с кольцевой топологией требует остановки работы сети, так как кольцо должно быть разорвано. Специальных ограничений на размер ЛВС не существует.

Особой формой кольцевой топологии является логическое кольцо.

Физически оно монтируется как соединение звездных топологий. Отдельные звезды включаются с помощью специальных коммутаторов (англ. Hub – концентратор), которые по-русски также иногда называют “хаб”. В зависимости от числа рабочих станций и длины кабеля между рабочими станциями применяют активные или пассивные концентраторы. Активные концентраторы дополнительно содержат усилитель для подключения от 4-х до 16-ти рабочих станций. Пассивный концентратор является исключительно разветвительным устройством (максимум на три рабочие станции). Управление отдельной рабочей станцией в логической кольцевой сети происходит так же, как и в обычной кольцевой сети.

Шинная топология. В ЛВС с шинной топологией основная передающая среда (*шина*) – общая для всех рабочих станций. Функционирование ЛВС не зависит от состояния отдельной рабочей станции, т.е. рабочие станции в любое время могут быть подключены к шине или отключены от нее без нарушения работы сети в целом (рис. 4.3.).

Поскольку расширение ЛВС с шинной топологией можно проводить без прерывания сетевых процессов и разрыва коммуникационной среды,

отвод информации из ЛВС и, соответственно, прослушивание информации осуществляются достаточно легко, вследствие чего защищенность такой ЛВС низкая.

Характеристики топологий вычислительных сетей приведены в таблице 4.2.

Древовидная топология. Образуется путем различных комбинаций рассмотренных выше топологий ЛВС. Основание дерева (корень) располагается в точке, в которой собираются коммуникационные линии (ветви дерева).

Сети с древовидной структурой применяются там, где невозможно непосредственное применение базовых сетевых структур. Для подключения рабочих станций применяют устройства, называемые *концентраторами*.

Существует две разновидности таких устройств. Устройства, к которым можно подключить максимум три станции, называют *пассивными концентраторами*. Для подключения большего количества устройств необходимы *активные концентраторы* с возможностью усиления сигнала.

Операционные системы ЛВС

Для сетей с централизованным управлением важным компонентом является *сетевая операционная система*, которая устанавливается на сервере сети, и *клиентские* части, устанавливаемые на рабочих станциях.

Основное направление развития современных сетевых операционных систем (Network Operation System) – поддержка систем с распределенной обработкой данных и перенос операций обработки на рабочие станции. Это в основном связано с ростом вычислительных возможностей ПК и внедрением многозадачных операционных систем. Внедрение объектно-ориентированных технологий обработки данных (OLE, DCE, IDAPI) также позволяет упростить организацию распределенной обработки данных. В такой ситуации основной задачей сетевой операционной системы становится объединение разнородных операционных систем рабочих станций и поддержка протоколов транспортного уровня для широкого круга задач:

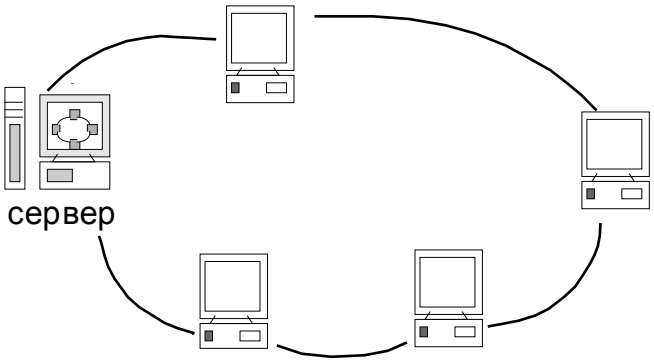

Рис. 4.2. Кольцевая топология

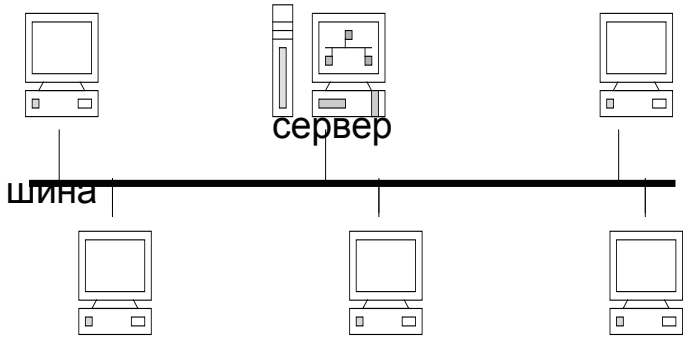

Рис. 4.3. Шинная топология

обработка баз данных, передача сообщений, управление распределенными ресурсами сети (Directory Name Service).

В современных сетевых операционных системах применяются три подхода к организации управления ресурсами сети.

Таблицы Объектов (Bindery). Таблицы находятся на каждом файловом сервере сети. Они содержат информацию о пользователях, группах, их правах доступа к ресурсам сети (данным, сервисным услугам и т.п.). Такая организация работы удобна, если в сети имеется только один сервер. В этом случае требуется определить и контролировать только одну информационную базу. При расширении сети, добавлении новых серверов объем задач по управлению ресурсами сети резко возрастает. Администратор системы вынужден на каждом сервере сети определять и контролировать работу пользователей. Абоненты сети, в свою очередь, должны знать, где расположены те или иные ресурсы сети, и для получения доступа к этим ресурсам регистрироваться на выбранном сервере. Для информационных систем, состоящих из большого количества серверов, такая организация работы сети неэффективна.

Структура Доменов (Domain). Все ресурсы сети и пользователи объединены в группы. Домен можно рассматривать как аналог таблиц объектов (bindery), только в данном случае такая таблица является общей для нескольких серверов, а ресурсы серверов являются общими для всего домена. Поэтому пользователю, для того чтобы получить доступ к сети, достаточно подключиться к домену (зарегистрироваться), после чего ему становятся доступны все ресурсы домена, т.е. ресурсы всех серверов и устройств, входящих в состав домена. Однако и при использовании этого подхода также возникают проблемы при построении информационной системы с большим количеством пользователей, серверов и доменов, например, сети масштаба предприятия. Проблемы связаны с организацией управления несколькими доменами.

Служба Каталогов (Directory Name Service). Все ресурсы сети: серверы, пользователи, сетевая печать, хранение данных и т.п. рассматриваются

Таблица 4.2.

Характеристики топологий вычислительных сетей

Характеристика	Топология		
	Звезда	Кольцо	Шина
Стоимость расширения	Низкая	Средняя	Средняя
Присоединение абонентов	Пассивное	Активное	Пассивное
Защита от отказов	Низкая	Низкая	Высокая
Защита от прослушивания	Хорошая	Хорошая	Плохая
Поведение при высоких нагрузках	Хорошее	Плохое	Плохое
Работа в режиме реального времени	Хорошая	Хорошая	Плохая
Разводка кабеля	Хорошая	Плохая	Хорошая

как ветви или директории одной общей информационной системы. Таблицы, определяющие DNS, находятся на каждом сервере. Это, *во-первых*, повышает надежность операционной системы и, *во-вторых*, упрощает обращение к ресурсам сети. После регистрации на одном сервере пользователю становятся доступны все ресурсы сети. Управление такой системой проще, чем при использовании доменов, так как существует одна таблица, характеризующая все ресурсы сети, в то время как при доменной организации необходимо определять ресурсы, пользователей, их права доступа отдельно для каждого домена.

4.5. Глобальная компьютерная сеть Интернет

История создания Интернет. В 1969 году Министерство Обороны США создало сеть, которая явилась прародительницей Интернет – она называлась ARPAnet. ARPAnet создавалась для поддержки научных исследований в военно-промышленной сфере, в частности, для исследования методов построения сетей, устойчивых к частичным повреждениям и способных в критических условиях продолжать нормальное функционирование. Основной принцип состоял в том, что любой компьютер мог связаться как равный с равным с любым другим компьютером.

Передача данных в сети была организована на основе ***протокола Internet*** **(IP)**. Протокол IP – это свод правил по работе сети. Сеть задумывалась и проектировалась так, чтобы от пользователей не требовалось никакой информации о конкретной структуре сети.

Примерно 10 лет спустя после появления ARPAnet появились локальные вычислительные сети, такие как Ethernet и др. На большинстве рабочих станций ЛВС была установлена операционная система UNIX, которая имела возможность работы в сети с протоколом Internet (IP). Появились организации, которые начали создавать свои собственные сети, использующие протокол IP. Возникла потребность подключения ЛВС к ARPAnet.

Одной из сетей была NSFNET, разработанная по инициативе Национального научного фонда (NSF) США. NSF построил собственную сеть, основанную на IP технологии. В конце 80-х NSF создал пять суперкомпьютерных центров, сделав их доступными для использования в любых научных учреждениях. Центры были соединены специальными телефонными линиями с пропускной способностью 56 Kbps.

Началом становления мировой компьютерной сети Интернет принято считать 1986 г., когда Национальный научный фонд создал научную компьютерную сеть и объединил ее с АРПАНЕТ. В 1987 г. контракт на управление и развитие сети был передан компании Merit Network Inc., которая занималась образовательной сетью Мичигана совместно с IBM и MCI. Старая физически сеть была заменена более быстрыми (примерно в 20 раз) телефонными линиями. Были заменены на более быстрые и управляющие суперкомпьютеры. С тех пор ее популярность постоянно растет, а рост количества пользователей составляет, по некоторым оценкам, более 10% в месяц. Из средства передачи электронных посланий Интернет превратился в место для встреч, полное людей и идей, стал киберпространством, миром коммуникаций, информации и развлечений, в котором не существует понятия «расстояние».

Потребности пользователей Интернет продолжают расти. Большинство высших учебных заведений США и Западной Европы уже подсоединено к Интернет, предпринимаются попытки подключить к этому процессу средние и начальные школы. Пользователи сети прекрасно понимают преимущества, которые дает Интернет. Вся это приводит к непрерывному росту сети, развитию технологий и системы безопасности сети.

Основы устройства и функционирования Интернет. Сеть Интернет предоставляет следующие *информационные услуги*:

• передача и распространение информации;

• удаленный доступ к огромным массивам накопленных информационных ресурсов;

• общение между пользователями компьютерных сетей в различных странах мира.

Интернет представляет собой *всемирное объединение взаимосвязанных компьютерных сетей*. Использование общих протоколов семейства TCP/IP и единого адресного пространства позволяет говорить об Интернет как о единой глобальной «метасети», или «сети сетей». При работе на компьютере, имеющем подключение к Интернет, можно установит связь с любым другим подключенным к Сети компьютером и реализовать обмен информацией с помощью того или иного *прикладного сервиса* (службы) Интернет (WWW, FTP, E-mail и др.).

Число пользователей Интернет в мире строго подсчитать невозможно, однако по приблизительным оценкам оно составляет более трех миллиардов человек.

Домашний компьютер или рабочая станция локальной сети получает доступ к глобальной сети Интернет благодаря установлению соединения

(постоянного или сеансового) с компьютером *сервис-провайдера* – организации, сеть которой имеет постоянное подключение к Интернет и представляет услуги другим организациям и отдельным пользователям. Региональный сервис-провайдер, работающий с конечными пользователями, подключается, в свою очередь, к более крупному сервис-провайдеру – сети национального масштаба, имеющей узлы в различных городах страны или даже в нескольких странах. Национальные сети получают доступ в глобальный Интернет благодаря подключению к международным сервис-провайдерам – сетям, входящим в мировую магистральную инфраструктуру Интернет. Кроме того, региональные и национальные сервис-провайдеры, как правило, устанавливают соединения между собой и организуют обмен трафиком между своими сетями, чтобы снизить загрузку внешних каналов.

Темпы развития Интернет в той или иной стране во многом определяются развитием национальной инфраструктуры IP-сетей (компьютерных сетей, построенных на основе протоколов TCP/IP), включающей магистральные каналы передачи данных внутри страны, внешние каналы связи с зарубежными сетями и узлы в различных регионах страны. Степень развитости этой инфраструктуры, характеристики каналов передачи данных, наличие достаточного количества местных сервис-провайдеров определяют условия работы конечных пользователей Интернет и оказывают существенное влияние на качество предоставляемых услуг.

Пользователь, получивший полный доступ в Интернет, становится равноправным членом этого мирового сообщества и, вообще говоря, может не интересоваться тем, какие региональные и национальные сервис-провайдеры предоставляют этот доступ.

Интернет – организация с полностью добровольным участием. Высшая власть принадлежит ISOC (Internet Society). ISOC – общество с добровольным членством. Его цель – способствовать глобальному обмену информацией через Интернет. ISOC назначает совет старейшин, который отвечает за техническую политику, поддержку и управление Интернет.

Совет старейшин представляет собой группу приглашенных добровольцев, называемую IAB (Совет по архитектуре Интернет.). IAB регулярно собирается, чтобы утвердить стандарты и распределить ресурсы, такие, например, как сетевые адреса.

За Интернет никто централизовано не платит: каждая сеть или пользователь платит за свою часть. Так, например, NSF платит за содержание NSFNET, а NASA платит за Научную сеть NASA (NASA Science Интернет). Организации платят за подключение к некоторой региональной сети, которая в свою очередь платит за свой доступ сетевому владельцу государственного масштаба и т.д.

Каждая сеть имеет свой собственный сетевой эксплуатационный центр (NOC). Такой центр связан с другими и знает, как разрешить различные возможные проблемы.

Архитектура сетевых протоколов TCP/IP, на базе которых построена

Интернет, предназначена специально для объединенной сети. Сеть может состоять из совершенно разнородных *подсетей*, соединенных друг с другом *шлюзами*. В качестве подсетей могут выступать самые разные локальные сети (Token Ring, Ethernet, пакетные радиосети и т.п.), различные национальные, региональные и специализированные сети (например, HELPnet), а также другие глобальные сети, такие, например, как Sprint. К этим сетям могут подключаться машины совершенно разных типов. Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу связи.

Доступ в Интернет, как уже упоминалось выше, получают через поставщиков услуг (сервис-провайдеров). Поставщики эти продают различные виды услуг, каждый из них имеет свои преимущества и недостатки.

Персональный доступ в Интернет, особенно в России, пока что достаточно дорогое удовольствие, однако многие организации, особенно институты, уже имеют доступ в Интернет. В этом случае пользователю не надо платить денег из своего кармана, не надо иметь дело с поставщиками услуг и т.д.

Уровни сети Интернет. Пересылка битов в Интернет происходит на *физическом* уровне схемы ISO OSI. Попытка дать краткое и доступное описание затруднительна. Потребуется введение большого количества специальных терминов, понятий, описаний процессов на физическом уровне и т.д. Для понимания работы сети это необязательно. Можно считать, что просто имеется канал, по которому из конца в конец перекачиваются биты.

Организация блочной, символьной передачи, обеспечение надежной пересылки происходит на других уровнях модели ISO OSI. Функции *канального* уровня в Интернет распределены по другим уровням, но не выше транспортного. В этом смысле Интернет не совсем соответствует стандарту ISO. Канальный уровень Интернет занимается только разбиением потока битов на символы и кадры и передачей полученных данных на следующий уровень.

Сеть Интернет состоит, в основном, из выделенных телефонных линий. Однако модель телефонной сети не отражает адекватно ее структуру и работу. Телефонная сеть – это сеть с *коммутацией каналов*, т.е. на все время сеанса связи имеется физическое соединение с абонентом. При этом пользователю выделяется часть сети, которая для других уже недоступна. Это приводит к нерациональному использованию линий сети. Интернет является сетью с *коммутацией пакетов*, что принципиально отличается от сети с коммутацией каналов.

Наглядным примером сети с коммутацией пакетов является почта. Модель почты достаточно точно отражает суть работы и структуры Интернет, и ею часто пользуются. Компьютерные сети, которые в концептуальном плане наследуют принцип организации почтовой связи, называются *дейтаграммными сетями*.

Протоколы Internet (IP). Интернет аккуратно передает данные в различные точки, разбросанные по всему миру. Забота об этом возложена на *сетевой уровень* в эталонной модели ISO OSI.

Различные части Интернет соединяются между собой посредством компьютеров, которые называются узлами. Узлы – аналоги почтовых отделений, где принимается решение, как перемещать пакеты по сети, точно так же, как в почтовом узле намечается дальнейший путь почтового конверта. Каждый узел не имеет непосредственных прямых связей со всеми остальными узлами.

Для работы такой системы требуется, чтобы каждый узел знал об имеющихся связях и о том, на какой из ближайших узлов оптимально следует передать адресованный пакет. В Интернет узлы выясняют, куда следует пакет данных, решают, куда его дальше отправить и отправляют. Такой процесс называется *маршрутизацией*.

Для осуществления маршрутизации составляются таблицы маршрутизации. В Интернет составление и модификация таблиц маршрутизации определяются соответствующими протоколами: ICMP (Internet Control Message Protocol), RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First). Узлы, занимающиеся маршрутизацией, называются *маршрутизаторами*.

Основой организации передачи данных по сети являются протоколы IP и TCP. ***Протокол Интернет (IP)*** – это набор формализованных правил, которые применяются для транспортировки и адресации передаваемых пакетов данных. В начало каждого передаваемого пакета помещается заголовок, несущий информацию об адресате сети. Длина информации внутри пакета имеет ограниченный размер, который обычно составляет от 1 до 1500 байт. При таком подходе всем пользователям предоставляются примерно равные права. Поэтому, чем больше пользователей одновременно пользуется сетью, тем медленнее она работает с каждым пользователем.

Протокола IP вполне достаточно для работы в Интернет. Данные, помещенные в оболочку IP, содержат всю необходимую информацию для передачи их с компьютера пользователя получателю. Однако при пересылке информации с использованием протокола IP имеет место ряд проблем, которые необходимо решать:

• большинство сообщений превышает длину в 1500 символов, т.е. допустимый размер одного пакета;

• пакеты в сообщении могут следовать в последовательности, отличной от их исходного порядка;

• возможны ошибки в передаче пакетов.

Протокол управления передачей TCP обеспечивает способ пересылки больших массивов информации и исправляет искажения, которые могут возникать по вине сети. Этот протокол разбивает всю исходную информацию на пакеты, передаваемые посредством протокола IP, и проверяет правильность сборки пакетов на приёмной стороне, а также управляет соединением абонентов. Таким образом, протокол TCP занимается проблемой пересылки больших объемов информации, основываясь на возможностях протокола IP.

Следующие уровни сети Интернет должны обеспечить пересылку больших массивов информации и устранить ошибки, которые возникают

в процессе передачи.

Для этого создается программное обеспечение, которое понимает язык команд, выдает сообщения об ошибках, подсказки, использует для адресации сетевых компьютеров при общении с пользователем обычные имена, а не числа и т.д., т.е. повышает уровень удобства работы в сети. В модели ISO OSI над этим работают уровни выше *транспортного*, т.е. *сеансовый, представления данных* и *прикладной*.

Адресация в Интернет. Адрес в Интернет состоит из 4 байт. При записи байты отделяются друг от друга точками: 111.22.345.99 или 3.33.33.3. По сути, адрес состоит из нескольких частей. Начало адреса говорит о том, частью какой из сетей является отправитель. Правый конец адреса говорит о том, какой компьютер или хост должен получить пакет. Каждый компьютер в Интернет имеет в этой схеме уникальный адрес, аналогично обычному почтовому адресу. Существует несколько типов адресов Интернет, которые по-разному делят адрес на поля номера сети и номера узла, и от типа такого деления зависит количество возможных различных сетей и машин в таких сетях.

Остановимся несколько подробнее на адресации в Интернете. IP -адрес – это число, строго определяющее узел (компьютер) в Интернете или внутренней сети. IP-адрес представляется в двоичном, или в двоично-десятичном виде. Длина адреса установлена 32 бита, что равно 4 байтам. Таким образом, адресное пространство позволяет использовать 2^{32} *(примерно 4,3 миллиарда)* различных адресов. Для удобства восприятия, IP-адресация принята в двоично-десятичном (десятичноточечном) виде, например, *128.121.188.201*. За распределение и присвоение адресов в Интернете отвечает неправительственная организация InterNIC (Сетевой информационный центр Интернета).

IP-адрес содержит идентификатор сети и идентификатор узла. Первый из них обозначает конкретную сеть (или сегмент сети), в которой физически находится узел, второй – определяет конкретный узел в данной сети. Например, в адресе 128.121.188.201 идентификатором сети являются первые два октета – 128.121., а идентификатором узла – 188.201.

Знание принципов адресации в Интернете и структуры адреса необходимо не только для специалистов в этой области, но, например, и для сотрудников ОВД. Это объясняется тем, что в последнее время Интернет используется для совершения различных противозаконных деяний и, зачастую, бывает очень важно определить местоположение (Интернет – адрес) злоумышленника.

Как известно, у Интернета нет владельца, но кто-то все-таки должен устанавливать правила, принимать протоколы и т.д. Этим занимаются некоммерческие организации. Организация RIPE отвечает за распределение IP-адресов и имеет огромную базу данных, которая содержит информацию о тех, за кем числятся все распределенные IP-адреса. Она содержит название организации, диапазон выделенных ей IP адресов, почтовый адрес организации, IP-адреса маршрутизаторов и некоторую информацию о контактных лицах. Эта база данных является публичной, т.е. любой желающий может

сделать к ней запрос с помощью специальной ***службы Whois***, обратиться к которой можно по нескольким Web-адресам, например, по адресу http://www.ripe.net/perl/whois/. Таким образом, при желании всегда можно узнать какому провайдеру принадлежат интересующие вас IP-адреса. По определенным координатам провайдера можно вычислить и злоумышленника.

Службы Интернет. *Приложения Интернет* – это составляющие части программного обеспечения. Их создают на основе сервиса TCP или UDP. Приложения позволяют пользователю достаточно просто справиться с возникшей проблемой, не вдаваясь в подробности технического устройства сети, протоколов и т.п.

Существует несколько стандартных приложений, или *служб* Интернет: удаленный доступ (telnet), передача файлов, электронная почта (E-mail) и т.д., которые далее будут рассмотрены подробнее. Наряду с ними используются и другие, нестандартные приложения.

Удаленный доступ (telnet) – работа на удаленном компьютере в режиме, когда компьютер пользователя эмулирует терминал удаленного компьютера, т.е. на своем рабочем месте можно делать то же, что и с обычного терминала удаленной машины. Находясь, например, в России, можно работать на суперкомпьютере в США так, как если бы он стоял рядом.

Начать сеанс удаленного доступа можно, подав соответствующую команду и указав имя машины, с которой хотят работать. Сеанс обеспечивается совместной работой программного обеспечения удаленного компьютера и компьютера пользователя. Они устанавливают TCP-связь и общаются через TCP и UDP пакеты.

Для пользования службой telnet необходимо иметь доступ в Интернет класса не ниже dial-up.

Электронная почта (E-mail) – одна из самых популярных на сегодняшний день Интернет-служб. По разным оценкам, в мире насчитывается более 50 миллионов пользователей электронной почты. В то же время мировой трафик электронной почты занимает только около 5% всего сетевого. Популярность E-mail в России объясняется как тем, что большинство подключений имеют класс dial-up(с модема), так и тем, что E-mail доступна при любом виде доступа к Интернет.

E-mail (Electronic mail) – электронный аналог обычной почты. С ее помощью можно посылать сообщения, получать их в свой электронный почтовый ящик, автоматически отвечать на письма корреспондентов, используя их адреса, рассылать копии писем нескольким получателям, переправлять полученное письмо по другому адресу, включать в письма файлы разных типов, вести подобие дискуссий с группой корреспондентов и т.д. Можно также посылать почту через шлюзы в сопредельные сети. Посредством электронной почты осуществляется фактически мгновенная пересылка сообщений независимо от расстояния. Применение этой важной составляющей сетевых информационных технологий актуально в том числе и в деятельности ОВД.

Принципы организации электронной почты достаточно просты. Каж-

дый абонент имеет свой индивидуальный почтовый адрес. Причем, структура адреса электронной почты базируется на принятых при доменной адресации принципах, рассмотренных выше. То есть, у каждого абонента должно быть уникальное имя, а доменное имя должно соответствовать принятому при URL – адресации. Например, типичный адрес электронной почты user@mail.ru. Также как в обычной почте, в отправляемом электронном сообщении необходимо указать адрес получателя.

После отправки почтовое сообщение попадает не сразу на компьютер получателя, а сначала отправляется на почтовый сервер поставщика почтовых услуг. Для получения сообщения адресату необходимо доставить его с сервера на свой компьютер. Для обеспечения электронной почты предназначены специальные почтовые службы и программное обеспечение, называемое почтовыми клиентами. Почтовые клиенты устанавливаются на компьютеры пользователей электронной почты и обеспечивают создание, отправку и получение почтовых сообщений.

Необходимо отметить недостаточную защищенность применяемых в Интернете почтовых служб, которая заключается в возможности перехвата, фальсификации почтовых сообщений, пересылке с такими сообщениями вредоносных программ и т.д. Поэтому, для защиты и обеспечения конфиденциальности электронной почты в ОВД применяются дополнительные меры. Одной из таких мер является применение в ОВД ведомственной электронной почты «Дионис», которая обеспечивает шифрование передаваемых сообщений и защиту адресов абонентов.

Служба E-mail позволяет получить доступ к услугам других служб, например ftp, Whois, WWW и т.п. Существует множество серверов, поддерживающих такие услуги. В адрес такой службы посылается E-mail, содержащий команды этой службы, а в ответ по E-mail приходит необходимый файл. В таком режиме возможно использование почти всего набора команд службы ftp.

E-mail дает возможность проводить телеконференции и дискуссии. Для этого используется специальное программное обеспечение – *рефлекторы почты* – установленное на некоторых узловых машинах сети. Рефлектор почты по получении электронных писем рассылает их копии всем подписчикам.

Доски объявлений (USENET news). Эта служба дает возможность читать и посылать сообщения в открытые дискуссионные группы. По сути она представляет собой сетевой вариант досок объявлений (BBS: Bulletin Board System), изначально работавших на машинах с модемным доступом. Сообщения адресуются широкой публике, а не конкретному адресату и могут иметь совершенно разный характер.

Узлы сети, занимающиеся обслуживанием системы новостей, по получении пакета новостей рассылают его своим соседям, так что получается широковещание, обеспечивающее быструю рассылку новостей по всей сети.

После установки клиентской программы службы Usenet на компьютере пользователя создается список дискуссионных групп, в которых он хочет участвовать и чьи бюллетени новостей он будет получать постоянно.

World Wide Web (WWW или Мировая Паутина) – это объединение глобально распространяемых текстовых и мультимедийных документов и файлов, а также других сетевых сервисов, связанных друг с другом таким образом, что поиск и получение информации, а также интерактивное взаимодействие между пользователями осуществляется быстрыми и интуитивно понятными способами.

Основной службой доступа к ресурсам Интернета является **служба Web**, которая представляет собой графический интерфейс к Интернету, позволяющий доставлять и обрабатывать информацию, содержащуюся в специально отформатированных документах, и включает в себя *три основных компонента*:

- язык разметки гипертекста – HTML,
- протокол передачи гипертекста – HTTP,
- универсальный указатель ресурса – URL.

Гипертекст – способ организации документов или баз данных, при котором соответствующие фрагменты документов или информации связываются друг с другом ссылками, позволяющими пользователю переходить по ним к соответствующим документам или информации, следуя по ассоциативному пути. Ссылки могут быть представлены в текстовом, графическом, аудио- или видео-формате.

Имея редактор гипертекстов, который поддерживает язык HTML, можно создать любую структуру рабочей среды, включая документацию, файлы, данные, рисунки, программное обеспечение и т.д. Создание гипертекстовых редакторов с дружественным интерфейсом является одной из основных проблем WWW.

При просмотре гипертекста в *программе-браузере*, которая обрабатывает ссылки и выполняет соответствующие действия, в тексте видны выделенные подсветкой слова. Если навести на них курсор и нажать на клавишу ввода или на кнопку мыши, то высветится содержимое ссылки.

В WWW документ может иметь гипертекстовую структуру любой степени сложности. Пользователь может сам организовать структуры типа меню в гипертексте.

Язык HTML включает в себя программные коды разметки файла или тэги, которые определяют шрифты, слои, графику и ссылки на другие Web-документы.

HTTP определяет набор стандартов по передаче Web-страниц через Интернет.

URL представляет собой стандарт для определения местонахождения (адреса) файла или другого ресурса в Интернете. Тип ресурса зависит от используемого протокола. В случае Web, протоколом является HTTP, ресурсом может быть HTML-страница, графический файл, программа, выполняемая на удаленном компьютере.

URL содержит название протокола, требующегося для доступа к ресурсу, доменное имя, определяющее конкретный компьютер в Интернете

и иерархическое описание местоположения файла на этом компьютере. Доменное имя – это, фактически, многоуровневый адрес ресурса в сети. Например, URL официального сайта министерства внутренних дел России в Интернете, выглядит так: http://www.mvd.ru. Причем, «http:» – название протокола, «www» – обозначает используемую службу Web, домен второго уровня «mvd.ru» идентифицирует административного владельца ресурса – МВД России, домен первого (верхнего) уровня «.ru» в данном случае указывает на географическую принадлежность сети – RU (Russia). Домены второго уровня могут быть иерархически разделены на домены третьего и т.д. уровней. Домены верхнего уровня указывают как на географическую принадлежность, так и на тип домена:

.com – коммерческий,
.edu – образовательный,
.gov – правительственный,
.org – некоммерческие организации,
.net – сети и сервис – провайдеры,
.mil – вооруженные силы.

URL, использующий доменные имена, применяется для наглядного, удобного для восприятия человеком отображения *адреса ресурса Интернет*. Но на уровне организации функционирования сети за адресацию сетевых ресурсов отвечает протокол Интернета **IP**. То есть, каждому доменному имени однозначно соответствует конкретный IP-адрес.

Для работы с Web – ресурсами предназначены специальные средства Web – серверы и Web – браузеры.

Web-сервер – это компьютерная программа, которая обслуживает запросы на HTML-страницы или файлы. Она устанавливается и работает на аппаратуре, представляющей доступ к Интернет – ресурсу, то есть находится у владельца ресурса (сайта или портала). Запросы к серверу поступают со стороны программы-клиента, находящейся на компьютере или любом другом возможном Интернет – терминале пользователя. Такая программа называется браузером (программа просмотра) или ***Web-браузером***. Наиболее распространенными браузерами в настоящее время являются графические браузеры *Microsoft Internet Explorer, FireFox* и *Opera*.

С понятием Web-сервера напрямую связаны понятия ***Web-сайт*** и ***портал***. Как правило, по адресу, указываемому URL, располагается Web-сайт. ***Web-сайт*** – это тесно связанная совокупность World Wide Web файлов, которая включает стартовый файл (стартовую или главную страницу), именуемую домашней страницей. Как правило, в качестве адреса сайта используется адрес домашней страницы. С домашней страницы можно получить доступ к любой другой странице на сайте.

Web-сайты делятся по типам на десятки категорий и сотни подкатегорий в зависимости от системы классификации. Наиболее посещаемые пользователями сайты – это ***поисковые машины, каталоги*** и ***Web-магазины***.

Для крупнейших сайтов в настоящее время происходит слияние в одну

категорию порталов с последующей классификацией на их типы. ***Порталом*** называют определяющий Web-сайт как постоянный стартовый сайт Интернет-пользователя при доступе к World Wide Web. Порталы подразделяются на две крупные подкатегории: порталы общего назначения и специализированные тематические порталы. По сути, современный портал может выполнять функции и поисковой машины, и каталога товаров и услуг, и виртуального магазина.

Контрольные вопросы

1. Поясните назначение и принципы конструирования информационных компьютерных сетей.
2. Раскройте понятие сетевого протокола.
3. Чем локальная вычислительная сеть отличается от глобальной? Поясните на примерах.
4. Назовите основные типы сетевых структур (способы объединения компьютеров в сеть).
5. Поясните назначение сервера и сетевой рабочей станции. Какие требования предъявляются к компьютерам данного класса?
6. Поясните принцип работы сети, построенной по принципу клиент-сервер.
7. В чем заключается принцип распределения ресурсов в ЛВС? Назовите его основные преимущества и недостатки.
8. Что такое права доступа в сети? Приведите примеры разграничения прав доступа для различных категорий пользователей.
9. Что понимается под администрированием сети? Назовите основные функции сетевого администратора.
10. Объясните иерархию протоколов в сети Интернет.
11. Как формируется универсальный адрес сетевого ресурса в Интернет?
12. Назовите основные службы сети Интернет.
13. Что представляет собой гипертекстовая структура?
14. Объясните назначение таких программ, как Web – серверы и Web – браузеры.
15. Каковы основные достоинства и недостатки технологий доступа к информации в сети Интернет.

Часть II.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Глава 5. Информационные технологии документирования и документооборота

5.1. Основы технологии подготовки текстовых документов

Структура текстовых документов

Структуру любого текстового документа можно рассматривать в трех аспектах: *изобразительном, операционном* и *внутримашинном*.

Изобразительная структура характеризует логику построения документа.

Операционная структура характеризует человеко-машинный аспект. Она отражает возможности, предоставляемые для манипуляции основными элементами текста.

Внутримашинная структура отражает способ хранения текста в памяти ЭВМ.

Три наиболее известных вида текста: **прозаический, табличный, программный.**

Прозаический текст наиболее распространен. Важнейшие элементы изобразительной структуры: символ (буква, цифра, знак препинания. специальный знак), слово, предложение, абзац, раздел и т.д. Элементы операционной структуры: символ, слово, строка, фрагмент и т.п. Внутри-машинная структура представляет собой цепочку символов, среди которых и управляющие.

В общем виде прозаический текст состоит из *страниц*, страницы – из *строк*, строки – из *символов*. Символ в тексте может быть однозначно определен номером страницы, номером строки и номером позиции символа в строке. Строки состоят из подстрок, что характерно для записи формул, содержащих *надстрочные* и *подстрочные* элементы типа индекса, степени и т.д.

Табличный текст. Элементами его изобразительной структуры являются *символ, строка, столбец, клетка.* Элементы операционной структуры: *строка, столбец, клетка.* Внутримашинная структура сложная.

Программный текст – исторически первый; он представляет исходные программы на алгоритмических языках.

Существуют и другие виды текста: *поэтический, графический, формульный* и др. Редакторы прозаических текстов позволяют создавать другие виды текстов. *Символы псевдографики* образуют несложный графический текст.

Этапы подготовки текстовых документов

Основными этапами подготовки текстовых документов являются:

- набор текста;
- редактирование текста;
- ведение архива текстов;
- печать текста.

Рис. 5.1. Этапы обработки текста на компьютере

Каждый этап состоит из выполнения операций. Последовательность всех четырех этапов подготовки текстового документа приведена на рис. 5.1.

Не все операции можно четко отнести к конкретному этапу подготовки документа. Если присутствует этап набора и редактирования, то лучше перед печатью выполнить этап записи текста на внешнее запоминающее устройство.

Набор текста. Очередной символ отображается на экране в позиции курсора, а курсор перемещается на одну позицию вправо. Большинство редакторов хранит весь вводимый текст в оперативной памяти.

Возможности редактора при наборе текста определяются используемой *таблицей кодировки*. Стандартная кодовая таблица состоит из 256 символов. Первая половина таблицы с кодами от 0 до127 соответствует стандартному коду ASCII. Символы с кодами от 0 до 32 являются управляющими и для набора текста не используются. Символы с кодами от 32 до 127 используются для представления знаков пунктуации, арифметических операций, цифр, прописных и строчных букв латинского алфавита.

Вторая половина таблицы является расширением стандарта ASCII.

Дисплей используется либо в *текстовом*, либо в *графическом* режиме. В текстовом режиме – 25 строк по 80 прямоугольников в каждой. В графическом режиме экран из отдельных точек. Каждый символ отображается с помощью матрицы, например 8x8 точек.

Редактор избавляет от необходимости осуществлять действия по переводу курсора на следующую строку и автоматически выравнивает правые границы строк. Создается специальная *направляющая линия*, на которой специальными знаками отмечены *левая, правая граница* строки и *метки табуляции*. Метки табуляции используются при нажатии клавиши TAB.

В конце строки добавляется признак *конца строки*, он не индицируется на экране. Существуют «*мягкие*» и «*жесткие*» признаки конца строки. «*Мягкие*» создаются автоматически при переносе текста, в процессе достижения правой границы экрана. «*Жесткие*» создаются при нажатии клавиши «Enter». Признак конца строки называют *разделителем строк*.

Редактор для выравнивания строк автоматически вставляет «*мягкие*» пробелы, в отличие от «*жестких*», вносимых при нажатии клавиши «Пробел».

Признаком отделения слова от слова является пробел, а после знака препинания надо ставить пробел.

При заполнении экрана дисплея текстом происходит скроллинг или прокрутка строк.

Множество символов редактора всегда шире множества символов на клавиатуре. Существует *два способа* ввода этих символов.

Первый способ – ALT-ввод. Нажимается клавиша «ALT» и, не отпуская ее, код на малой цифровой клавиатуре.

Второй способ – специальные команды редактора для смены шрифтов.

Редактирование текста. При использовании ПК и текстовых редакторов этап *печати* документа отделен от этапов *набора* и *редактирования*.

Этап редактирования состоит из операций:

• перемещения курсора;
• просмотра текста;
• вставки символов, строк, фрагментов;
• замены символов, строк, фрагментов;
• удаления символов, строк, фрагментов;
• перемещения символов, строк, фрагментов;
• поиска по образцу или по месту;
• контекстной замены;
• форматирования абзацев.

Операции редактирования делятся на:

• операции редактирования над символами;
• операции редактирования над строками;
• операции редактирования над фрагментами;
• операции поиска и замены;
• операции форматирования.

Печать текста. Этап печати состоит из операций подготовки текста к печати и собственно печати.

К операциям подготовки текста к печати относятся:

• разделение на страницы;
• нумерация страниц;
• изменение шрифта;
• выделение элементов текста при печати;
• задание заголовка и подножия страницы.

Существуют «мягкие» и «жесткие» разделители страниц.

Всегда перед распечаткой вновь подготовленного текста желательно сделать пробную распечатку текста на экране дисплея.

Собственно печать является самой заключительной стадией.

5.2. Текстовые редакторы и процессоры

При *вводе информации* в компьютер каждый символ превращается в двоичный код. При *выводе информации* код каждого символа преобразуется во внешнее представление этого символа на экране или принтере.

За основу кодирования символов взят код ASCII – American Standard Code for Information Interchange. Каждому символу соответствует се-

мизначный двоичный код – всего

27 = 128 символов.

Этого мало, поэтому применяют расширенный стандарт ASCII

28 = 128 ASCII + 128= 256 символов.

Один из альтернативных вариантов – расширение за счет включения символов кириллицы.

Текстовый файл (файл ASCII) – файл, содержимое которого без преобразования может быть выведено на экран или монитор и воспринято человеком, он содержит строки произвольной длины и состоит из семиразрядных или восьмиразрядных двоичных символов. В текстовом файле встречаются специальные символы, которые не выводятся на экран и имеют специальные названия:

EOL – конец строки;

CR – возврат каретки;

LF – перевод строки;

EOF – конец файла.

В текстовом файле строки при просмотре имеют произвольную длину. В двоичном файле строки фиксированной длины.

Редакторы текстов (Word Processor). Всего их насчитывается несколько сотен.

Основные возможности ТП:

• набор текста с контролем на экране;

• создание жесткой копии (распечатка);

• использование ASCII.

Основные возможности совпадают практически с возможностями печатной машинки.

Дополнительные возможности текстовых процессоров, общие для файлов любого формата:

• хранение копии на магнитном носителе;

• внесение изменений в текст до распечатки(вставка, удаление);

• создание резервных копий;

• организация поиска по имени и последовательности символов и т.д.

Специальные возможности текстовых редакторов:

А. Редактирование текста.

• Работа с участком текста:

- выделение;
- удаление;
- запись в буфер;
- копирование;
- запись в виде отдельного файла и т.д.

• Выравнивание текста:

- по краю (правому, левому, ширине);
- по центру;
- по ширине.

• Автоперенос слов:
- целиком;
- по правилам переноса.
• Организация колонок.

B. Создание резервных копий через равные промежутки времени.

C. Работа с таблицами.
• Разметка.
• Удаление и добавление столбцов и строк.
• Выравнивание текста в ячейках.
• Оформление рамок.

D. Отказ от последних действий и отказ от отказа.

E. Операции над рисунками.
• Вставка в текст.
• Масштабирование и растяжка по осям.
• Обтекание рисунка текстом и т.д.

F. Разбиение на страницы.
• Автоматическое, путем задания числа строк на странице.
• Жесткое, принудительное.
• Нумерация страниц (сверху, снизу).

G. Использование шаблонов документов.

H. Использование набора шрифтов.
• **true type (ttf)** – пропорциональные шрифты.
• шрифты с произвольно изменяемыми размерами.
• различные способы выделения шрифтов – подчеркивание, курсив и т.д.

I. Контекстный поиск и замена заданной последовательности слов в тексте.

J. Проверка орфографии с использованием встроенного словаря.

K. Подсказка синонимов и антонимов.

L. Проверка грамматики – анализ предложения как целого.

M. Построение оглавлений, индексов, сносок.

N. Набор сложных формул – математических и физических.

O. Использование в тексте данных из СУБД и ЭТ.

Классификация текстовых редакторов

1. По возможностям.

A. *Качество печатной машинки,* небольшой набор возможностей по работе с текстом:
• Norton Editor;
• Фотон;
• Лексикон;
• MultiEdit
• Chiwriter.

Список составлен в порядке возрастания возможностей. Редакторы реализуются на компьютерах типа IBM PC, XT, AT

В. *Издательское качество (**текстовые процессоры**)*. Реализация принципа WYSIWYG – What You See Is What You Get.

• Microsoft Word
• Ventura Publishers
• Aldus Page Maker

С. *Технические редакторы* – Tex, Latex и т.д.

2. По типу файлов, с которыми работают ТП.

• текстовые файлы;
• графический набор.

Возможны и другие варианты классификации текстовых редакторов, например, редакторы печатных текстов и редакторы электронных документов и т.д.

В большинстве случаев для создания деловых документов достаточно качества печатной машинки. Поэтому в 90-е годы широкое распространение получил редактор текстов Лексикон.

В общем случае *для оценки удобства работы с ТП* могут служить следующие ***параметры***:

• количество необходимых нажатий клавиш для выполнения конкретной операции (колеблется от 1–2 до 20–30);

• скорость отображения измененного текста на экране при загрузке, перемещениях по тексту, редактировании-вставке, копировании и удалении фрагментов, смене шрифтов и т.д.;

• удобство работы с помощью, т.е. скорость вызова подсказок, их полнота и структура;

• возможность реализации WYSIWYG, т.е. получение на экране точной копии будущего печатного документа – текста без управляющих и разметочных символов;

• ограничения на длину файлов;

• количество одновременно обрабатываемых текстовых файлов;

• возможности использования новых шрифтов и алфавитов, их расширения и дополнения;

• требования к аппаратному обеспечению – например, к объему оперативной памяти ПК.

5.3. Технология работы с текстовыми документами в процессоре Microsoft Word

История развития ТП Word

Одним из наиболее мощных текстовых процессоров считается Word – программный продукт фирмы Microsoft. В России Word начал приобретать популярность начиная с версии Word 5.0. На смену ему пришел Word 5.5, более удобный в работе: в Word 5.5 использовались «выпадающие» меню и развитая система помощи.

Начиная с версии Word 6.0 текстовый процессор изменился функционально. Фактически возможности текстового процессора вышли за рамки

собственно работы с текстом документов и приблизились к возможностям настольных издательских систем: подготовка текстов с графическими фрагментами, таблицами, диаграммами, колонками и т.д. Кроме того, процессор поддерживает работу в многозадачных объектно-ориентированных средах (Windows и т.п.), используя при этом все их возможности. Начиная с этой же версии, текстовый процессор входит в состав объектно-связанного интегрированного пакета Microsoft Office. Данный программный продукт предназначен для работы на современных производительных персональных компьютерах, с процессорами Pentium MMX и выше и объемом оперативной памяти более 16 Мб.

Контрольные вопросы

1. Назовите основные этапы и операции подготовки текстовых документов на компьютере.
2. Назовите основные элементы текста, подлежащие автоматизированной обработке.
3. Перечислите основные функции систем обработки текстов.
4. Чем отличаются текстовые редакторы, текстовые процессоры и издательские системы?

Глава 6. Технологии подготовки презентаций

6.1. Презентация как средство представления идей

У термина *презентация* два значения – широкое и узкое. В широком смысле слова презентация – это выступление, доклад, защита законченного или перспективного проекта, представление на обсуждение бизнес-плана, технического предложения, эскизного или рабочего проекта, готового товара и услуги, результатов внедрения, контроля, испытаний и многое другое. В этом смысле защита курсовой или дипломной работы – это тоже презентация. Ее цель – убедить экзаменационную комиссию в том, что докладчик получил за время подготовки необходимый уровень знаний, владеет терминами, понятиями, методами и приемами в той научной области, в пределах которой он претендует на получение квалификации.

С экономической точки зрения презентации являются очень дорогостоящими мероприятиями. Одно совещание совета директоров международного автомобильного концерна может стоить акционерам больше, чем выпуск десятков дополнительных автомобилей, но оно может и дать больше, чем выпуск сотен и тысяч изделий. Это вопрос эффективности. Презентации должны быть эффективными в том смысле, что при оптимальных затратах всех видов ресурсов они должны давать максимальную результативность.

Наиболее очевидными техническими средствами сопровождения презентаций являются наглядные пособия (плакаты с графиками, диаграммами, фотоматериалами). Если технические условия позволяют и это уместно по характеру презентации, то в ней могут использоваться проекторы различных типов (кино-, видео- и диапозитивные), средства воспроизведения звукового ряда, а также средства дистанционного управления. Функционально компьютер способен заменить любые технические средства проведения презентаций и, более того, дополняет их свойства интерактивностью и автоматизацией. Широкое внедрение компьютеров в этой сфере началось после 1993–1994 гг., когда они обрели надлежащие мультимедийные функции. Начиная с 1995 г. вычислительную технику начали использовать при подготовке и проведении произвольных презентаций[1].

Развитие Интернета тоже внесло свой вклад в расширение технологий проведения презентаций. Изменения происходили в основном в двух направлениях. Во-первых, Интернет стал удобным средством проведения дистанционных презентаций и, во-вторых, способствовал их полной автоматизации. Сегодня в Интернете можно найти множество презентаций, работающих в автоматическом режиме. Их создателям нет необходимости разъезжать по миру, готовить доклады и выступать перед большими аудиториями – автоматизированные системы доносят авторские идеи и проекты до потенциальных инвесторов.

В узком смысле слова *презентации* – это электронные документы особого рода. Они отличаются комплексным мультимедийным содержанием и

[1] Информатика для юристов и экономистов / Симонович С.В. и др. – СПб.: Питер, 2001.С.565.

особыми возможностями управления воспроизведением. Воспроизведение может быть автоматическим или интерактивным, в том числе и дистанционным. Документы такого типа готовят с помощью специальных программных средств, но при этом широко используют и традиционные универсальные средства, такие, как текстовые и табличные процессоры, графические редакторы, средства обработки звуковой и видеоинформации и другие[1].

6.2. Microsoft PowerPoint – средство создания презентаций

В презентации основой успеха является оптимальный баланс между содержанием и средствами его представления. Выбор темы и подбор материала остаются творческими процессами автора и не автоматизируются. Автоматизации подлежат лишь процессы воплощения авторских идей в готовый продукт и процессы его публичного воспроизведения[2].

Одним из средств автоматизации создания служит приложение Microsoft PowerPoint, входящее в состав пакета Microsoft Office. Это универсальное средство, предназначенное для создания и оформления *электронных презентаций*. С помощью инструментов PowerPoint можно представить работу на любом из ее этапов: от концепции до итогов практической реализации. Для этого в программе имеются все необходимые средства, которые позволяют эффективно продемонстрировать как вполне материальные объекты (например машины и механизмы), так и нематериальные идеи, мысли, концепции и прочее.

Неочевидным, но, тем не менее, полезным свойством PowerPoint является необходимость в процессе подготовки презентации четко структурировать свои мысли и подводить промежуточные итоги этапов проделанной работы. Часто это помогает своевременно увидеть проблемы и недостатки, после чего найти новые направления развития проекта. Из практического опыта следует, что основное содержание работы с PowerPoint составляет не освоение интерфейса и инструментария программы, а осмысление целей презентации, выявление и представление преимуществ своего проекта и другие действия творческого характера. Однако, не стоит преуменьшать и значения детального овладения средствами PowerPoint.

Применение нестандартных эффектов, оригинальных элементов, созданных своими руками, воспринимается аудиторией как признак уважения к ее вниманию, как свидетельство значимости проделанной работы. Такой подход существенно повышает шансы на успех проекта.

Интеграция PowerPoint с Microsoft Office и другими программами

Благодаря тесной интеграции с другими компонентами пакета Microsoft Office исполнитель имеет возможность применять уже наработанные материалы. Например, текст может быть подготовлен в текстовом процессоре Word, формулы – в приложении Microsoft Equation, таблицы – в табличном процессоре Microsoft Excel, диаграммы – в приложении Microsoft Graph,

[1] Информатика для юристов и экономистов / Симонович С.В. и др. СПб.: Питер, 2001.С.565.
[2] Там же.

художественные заголовки – в приложении Microsoft Word Art и так далее. Кроме того, вся работа над проектом может быть организована с помощью приложения Microsoft Outlook[1].

Сказанное отнюдь не означает, что при подготовке объектов для презентации PowerPoint нельзя использовать другие программы. Напротив, некоторые специализированные приложения позволяют создать более качественные объекты, чем стандартные средства Microsoft Office. Например, растровую графику лучше готовить в графическом редакторе Adobe Photoshop, а векторную – в векторном редакторе Corel Draw. Однако именно приложения, входящие в состав Microsoft Office, являются наиболее тесно интегрированными и могут обмениваться данными без риска потерь и искажений[2].

Копирование и вставка. Объект создается в родительском приложении, копируется в Буфер обмена и вставляется в документ PowerPoint. Этот способ обычно применим к относительно простым объектам: текстам, растровой и векторной графике стандартных форматов, таблицам. При необходимости задать особые свойства объекта следует применять пункт ***Специальная вставка*** меню ***Правка***, присутствующий во всех приложениях Microsoft Office.

Перетаскивание. Объект перемещается (копируется или переносится) между родительским приложением и PowerPoint методом перетаскивания с помощью мыши. Обе программы должны быть в этот момент открыты.

Импорт (экспорт). Объект вставляется в документ PowerPoint в качестве файла, созданного в родительском приложении. В этом случае имеются ограничения как на формат поддерживаемых типов файлов, так и на их содержание. Кроме того, существуют ограничения на тип данных, содержащихся в файле. Например, в файлах векторной графики CorelDraw (расширение имени файла .car) не воспроизводится градиентная заливка[3].

Гиперссылка (ярлык). Этот способ заключается в указании перехода к содержимому файла другого приложения. Как правило, применяется в документах, рассчитанных на публикацию в Интернете (в формате HTML) или на представление на экране компьютера (с использованием формата PDF).

Гиперссылка является, прежде всего, средством перехода к другому документу (или другому месту в том же документе). Ярлык в основном применяют для запуска внешнего приложения, способного корректно обрабатывать данные определенного типа (например, воспроизведение музыки осуществляется стандартной программой Media Player).

Связывание. Это специальное свойство объекта, указывающее на его взаимодействие с исходным файлом и родительским приложением. Как правило, таким свойством обладают объекты, созданные в программах с полной поддержкой технологии OLE. В большинстве случаев наличие связи необходимо указывать явно. Связанный объект является клоном исход-

[1] Хэлворсон М., Янг М. Эффективная работа с MS Office 2000. СПб.: Питер, 2000. С. 116.
[2] Сагман С. Эффективная работа с PowerPoint 7.0. СПб.: Питер, 1997. С. 212.
[3] Сагман С. Эффективная работа с PowerPoint 7.0. СПб.: Питер, 1997. С. 217.

ного файла и меняется в той же мере, что и исходный файл.

Внедрение. Это свойство указывает на то, что в документ встроена копия исходного файла, после операции вставки никак с ним не связанная. Однако при поддержке родительским приложением технологии OLE возможно редактирование внедренного объекта средствами программы-источника.

Основные возможности PowerPoint

Существуют отдельные виды презентаций, где средствами PowerPoint создается практически законченный продукт. Прежде всего, это презентации, рассчитанные на публикацию в сетях Интернет/интранет[1] или предназначенные для автономного просмотра на компьютере. Имеется вариант рассылки презентации в виде печатного документа, который тоже можно считать законченным продуктом. Близким по характеру является вариант создания презентации для рассылки средствами электронной почты с целью дальнейшего просмотра адресатами на собственных компьютерах. Во всех перечисленных случаях презентации являются, скорее, «виртуальными», так как автор не видит реальной аудитории и уже не может управлять ходом презентации.

Остальные виды презентаций относятся либо к реальным, происходящим перед конкретной аудиторией, либо к псевдовиртуальным, когда документ представляется в сети (локальной, Интернет, интранет) в режиме реального времени. Характерным свойством таких типов презентаций является возможность управления их ходом со стороны докладчика.

В сфере подготовки презентаций PowerPoint является одним из наиболее мощных приложений и обеспечивает разработку следующих документов:

• вспомогательные материалы (как правило, цветные) презентации, рассчитанные на распечатку на прозрачной пленке с целью их демонстрации через оптический проектор;

• вспомогательные материалы (как правило, цветные) презентации, рассчитанные на распечатку на 35-мм диапозитивной фотопленке с целью их демонстрации через оптический слайд-проектор;

• вспомогательные материалы презентации, рассчитанные на воспроизведение через компьютерный проектор или на демонстрационной панели (светодиодной, плазменной, LCD);

• материалы презентации для автономного показа на экране компьютера или демонстрационной панели;

• материалы презентации для воспроизведения в сетевом окружении в режиме реального времени;

• материалы презентации для публикации в сетевом окружении с последующим автономным просмотром пользователями;

• материалы презентации для рассылки по электронной почте с последующим автономным просмотром адресатами;

• материалы презентации (как правило, черно-белые) для распечатки на бумаге (именуются в PowerPoint выдачами) с целью последующей раздачи заинтересованным лицам.

[1] Информатика для юристов и экономистов / Симонович С.В. и др. – СПб.: Питер, 2001.С.569.

Идеальным вариантом при разработке документов в PowerPoint является тот случай, когда тип презентации однозначно определен. Однако столь однозначный вариант встречается редко. Чаще необходимо готовить презентацию для основного типа представления, имея в виду два-три вспомогательных. Если необходимые типы существенно различаются по характеру, приходится готовить отдельные варианты для каждого из них.

Самый простой пример – создание презентации в вариантах для публикации в World Wide Web и для распечатки на 35-мм слайдах. Эти варианты существенно различаются по требованиям к цветовым схемам оформления, формату и разрешению графики, используемым шрифтам. Получается, что при одинаковом содержании придется затратить много времени на адаптацию презентации к специфическим требованиям типа представления.

Структура документов PowerPoint

Любой документ PowerPoint представляет собой набор отдельных, но взаимосвязанных кадров (страниц, по аналогии с книгой), называемых слайдами. Таких слайдов в презентации может быть сколь угодно много (в разумных пределах). Каждый слайд в документе имеет собственный уникальный номер, присваиваемый по умолчанию в зависимости от его места.

Последовательность слайдов (а следовательно и их связь, и нумерация) в документе линейная. Удаление, вставка, перемещение, скрытие или показ слайдов не нарушают линейной структуры документа. Таким образом, в PowerPoint невозможно построить иерархическую структуру документа или организовать между слайдами иные виды связи (например, с помощью логических операций), кроме линейной.

Слайды содержат объекты самого разного типа, их сочетание призвано наиболее полно выразить содержание данного кадра презентации. На каждом слайде присутствует, как минимум, один объект – фон кадра. Полностью пустого слайда существовать не может и под «пустым» понимается слайд с объектом типа «фон».

К объектам, размещаемым на слайде, относятся:

- фон (обязательный элемент любого слайда);
- текст;
- гиперссылки (как особый вид текста);
- колонтитулы (как особый вид текста);
- таблицы;
- графические изображения;
- надписи (как особый вид графики);
- диаграммы (как особый вид графики);
- фильмы (видеоклип);
- звук;
- значок (ярлык);
- цветовое оформление, в совокупности представляющее цветовую схему слайда.

Все объекты, размещаемые на слайде, могут быть созданы или оформ-

лены внутренними средствами PowerPoint, внешними приложениями или одновременно и теми, и другими.

Фон может быть представлен как обычное цветовое заполнение (в том числе градиентное, с использованием текстур или узора) или иметь в качестве основы рисунок (графический файл).

Текст может иметь различное форматирование, то есть в нем могут использоваться разные элементы шрифтового оформления, методы выделения цветом и выравнивания, приемы создания абзацных отступов.

Таблицы представляют собой специальным образом отформатированный текст, размещаемый в ячейках, разделенных вертикальными и горизонтальными границами. При этом границы могут быть скрыты или выделены линиями, а ячейки иметь цветовое оформление фона.

Графическое изображение (рисунок) может использоваться в качестве фона или быть отдельным объектом на слайде. Для полноценного отображения графики необходимо знать особенности форматов графических файлов, поддерживаемых PowerPoint. В первую очередь, это относится к предпочтительной области их применения и ограничениям, накладываемым при импорте файлов некоторых форматов. Графическое изображение может иметь только внешний источник.

Фильм – это объект PowerPoint, содержащий последовательность кадров, хранящихся в одном файле. Фильм обязательно имеет внешний источник и воспроизводится внешними средствами.

Звук является объектом, внешним по отношению к документу PowerPoint, и поэтому всегда требует указания названия источника. Небольшая коллекция звуков входит в стандартную поставку Microsoft Office. Воспроизведение звука осуществляется внешними средствами.

Значок (ярлык) представляет собой ссылку одновременно и на внешний объект, и на приложение, способное корректно его обработать в соответствии с расширением имени файла объекта.

Цветовая схема устанавливает заданное соотношение цветового оформления некоторых объектов, которое можно сохранить и использовать в дальнейшем.

Свойства объектов PowerPoint

Анимация. Анимация в PowerPoint является особым видом демонстрации объектов и содержит последовательность появления объекта в кадре при демонстрации слайда. Анимация относится к свойствам объекта, специфичным для PowerPoint, и воспроизводится встроенными средствами. Настройка параметров анимации слайда выполняется средствами диалогового окна **Дизайн слайда**, которое открывается пунктом **Эффекты анимации** из раздела **Показ слайдов** основного меню (рис. 6.1.). Настройка параметров анимации отдельного объекта выполняется средствами диалогового окна **Настройка анимации**, которое открывается пунктом **Настройка анимации** контекстного меню объекта.

Действие. Объектам PowerPoint может быть присвоено особое свой-

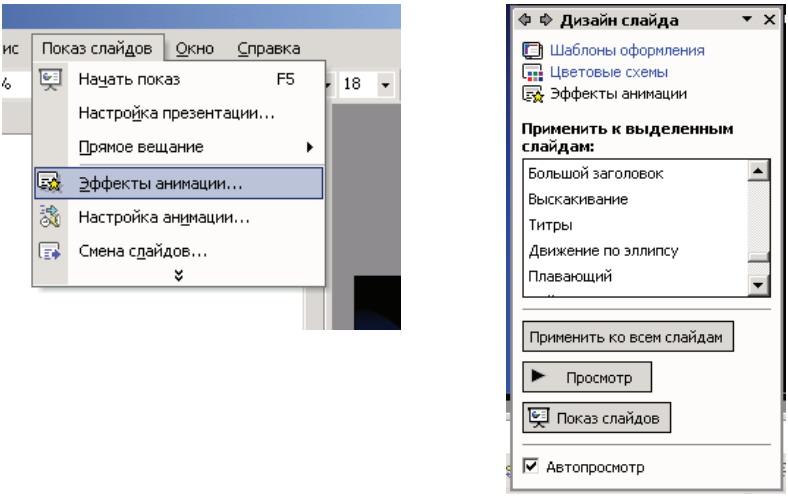

Рис. 6.1. Средства настройки параметров анимации объекта PowerPoint

ство, называемое действием. Оно определяет, что именно происходит при щелчке мышью или при наведении указателя на данный объект. Параметры действия устанавливаются в диалоговом окне ***Настройка действия*** (Показ слайдов > Настройка действия) (рис. 6.2.).

Свойства слайдов и свойства презентации. Каждый слайд презентации обладает набором свойств, к которым относятся параметры страницы (то есть размер и ориентация слайда) и эффекты при смене слайдов. Документ целиком (то есть презентация) имеет свой набор свойств, определяющий параметры его демонстрации (публикации) или правила совместной работы над содержанием.

Основные элементы интерфейса PowerPoint

Основное отличие интерфейса PowerPoint заключается в специфических режимах отображения документа на рабочем поле. Предусмотрено три основных режима отображения:

- обычный;
- сортировщика слайдов.
- показ слайдов;

В каждом режиме имеются специфичные для него наборы панелей инструментов. В зависимости от принятого режима меняется и состав контекстного меню, открываемого при щелчке на объекте (слайде) правой кнопкой мыши (рис. 6.3.).

В ***обычном режиме*** рабочее окно имеет три панели. На левой панели отображается структура презентации. Правая панель занимает большую часть поля, и в ней отображается слайд со всеми размещенными объектами. Третья панель небольшой высоты располагается в нижней части рабочего поля и предназначена для внесения заметок разработчиком презентации.

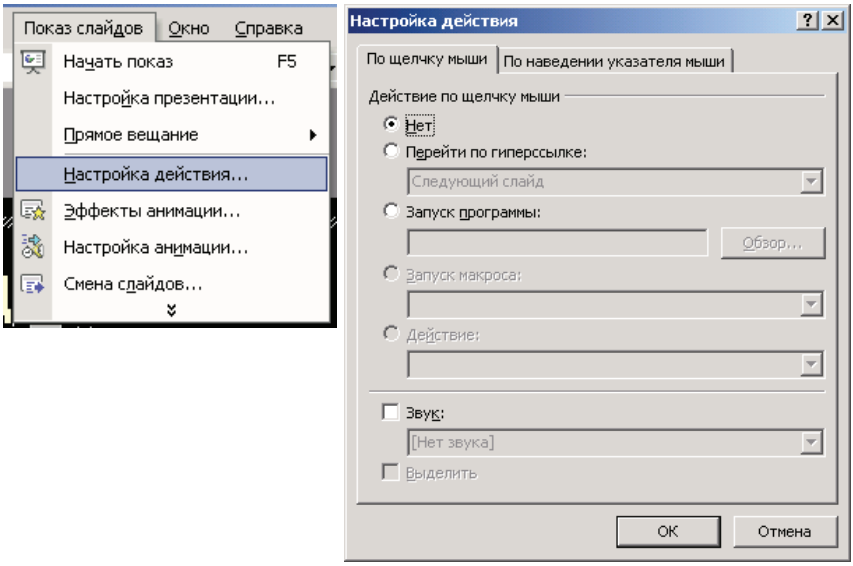

Рис. 6.2. Настройка действия объекта PowerPoint

В *режиме структуры* (вкладка структура обычного режима) размер панели с отображаемой структурой увеличен. Именно в режиме структуры удобно вводить и форматировать текст.

Следует иметь в виду следующие особенности, которые могут ввести в заблуждение пользователя, привыкшего работать с текстовым процессором Microsoft Word. При начале ввода текста на пустом слайде ему автоматически присваивается формат заголовка первого уровня (то есть уровня названия слайда). Попытка создания следующего абзаца нажатием клавиши ENTER приводит к появлению нового слайда. Понижение уровня текста уничтожает созданный слайд и переносит текст на предыдущий.

В *режиме слайдов* обычного режима каждый кадр занимает основную часть рабочего окна, а структура презентации отображается на узкой панели слева, где представлены символы слайдов и их номера. В этом режиме удобно работать с объектами, размещенными на слайде, особенно мелкими.

В ***режиме сортировщика*** слайдов кадры представлены эскизами, занимающими все рабочее поле, под каждым из которых размещаются значки, указывающие на параметры смены слайдов, анимации, времени экспозиции кадра. Соответственно меняется и панель инструментов, где появляются необходимые элементы управления, и контекстное меню, открываемое щелчком правой кнопкой мыши на эскизе слайда. Двойной щелчок на эскизе автоматически переводит программу в режим слайдов.

При переходе в ***режим показа слайдов*** автоматически запускается полноэкранная демонстрация с параметрами, выставленными в режиме со-

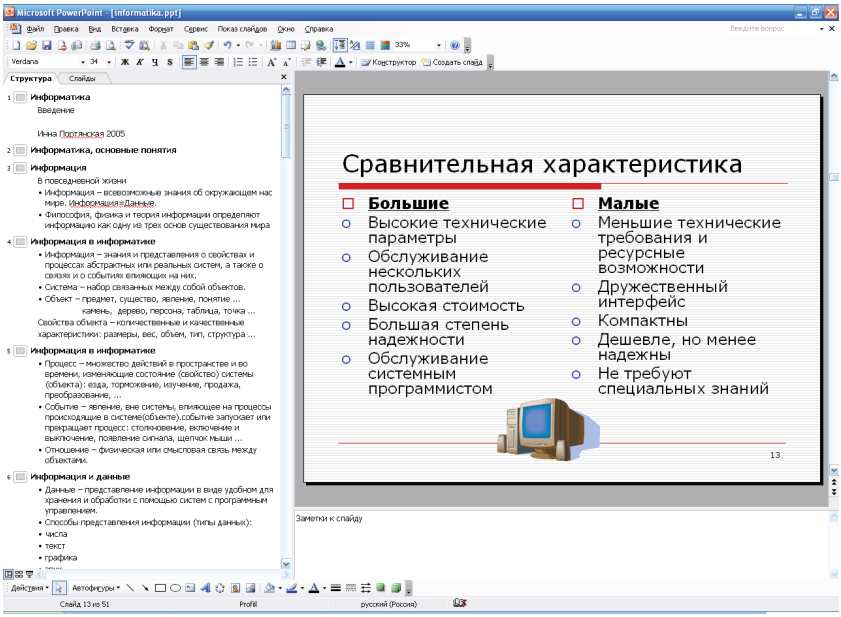

Рис. 6.3. Окно PowerPoint в обычном режиме

ртировщика слайдов. Демонстрация начинается с текущего (выбранного) слайда. Завершить ее можно в любой момент нажатием клавиши ESC. При этом происходит возврат в режим, который был текущим перед запуском демонстрации.

Содержание конкретных операций над объектом зависит от его типа, однако некоторые операции могут быть общими для всех типов объектов. Например, все объекты можно анимировать различными способами путем настройки параметров в диалоговом окне **Настройка анимации**. Таким способом добиваются динамичного «роста» диаграмм, «выпадающих» или вращающихся надписей и прочих эффектов оформления, оживляющих презентацию.

Важным элементом интерфейса служит пункт основного меню **Справка**. Там можно найти ответы на большую часть вопросов, возникающих при работе с программой PowerPoint.

6.3. Этапы разработки презентаций

Разработка презентационных документов, как и любых других, выполняется в несколько этапов.

Планирование презентации

Содержание презентации должно зависеть от целей докладчика, заинтересованности и подготовленности аудитории. Прежде всего необходимо

определить, на кого ориентирована презентация, каковы знания потенциальных слушателей по данной теме. Следует оценить потребности и предпочтения аудитории. Очень важно правильно сформулировать цель презентации и установить, как она соотносится с ожидаемыми результатами. Сформулируйте задачи презентации в следующей последовательности:

- что необходимо довести до аудитории;
- в чем следует убедить слушателей;
- чему нужно научить аудиторию;
- как мотивировать свои тезисы.

Когда цель и задачи точно сформулированы, можно приступать к отбору средств для их реализации.

Подготовка структуры презентации

Подготовьте эффектное начало презентации, сразу привлекающее внимание. При расчете времени на вводную часть отводится не более 10% от общей продолжительности презентации.

Далее формируются главные идеи доклада, с обоснованием их статистикой, документами, аналогиями или наглядными примерами. Все идеи и тезисы должны быть неразрывно связаны с темой доклада. Основная часть доклада должна занимать 80–85% отводимого времени.

Правильное завершение презентации, соответствующее цели доклада и создающее надолго запоминающееся впечатление, является важной частью успеха. Завершение презентации должно занимать не более 10% времени.

Работа с мастером автосодержания

Перейти к работе с мастером можно, открыв диалоговое окно **Создать презентацию** командой **Файл/Создать** и выбрав в нем пункт **Мастер автосодержания**. В диалоговом окне **Мастер автосодержания** переход к следующему этапу осуществляется щелчком на кнопке **Далее**.

Определение вида и стиля презентации

Автору необходимо определить, каким образом состоится публикация презентации. Например, при защите дипломной работы публиковать ее в Интернете нет смысла.

Важным параметром является определение формата страниц презентации. Следует помнить, что при распечатке слайдов надо указывать реальные размеры печатного листа. В случае вывода на экран компьютера в режиме создания презентации используется то разрешение и тот цветовой охват, которые установлены по умолчанию в операционной системе.

Работа с текстовым содержанием

В нижнем колонтитуле на каждом слайде следует указать заголовок презентации. Он должен совпадать с темой презентации. На левой панели структуры презентации показаны значки всех слайдов и весь текст, размещенный на них. Если использованы шаблоны, предлагаемые PowerPoint, то их текст следует заменить собственным содержанием.

Иногда полезно изменить принятый по умолчанию размер шрифта заголовка, если он занимает более двух строк и выглядит неопрятно. Часто

для лучшего представления следует изменить тип выравнивания заголовка. Обычно заголовки выравнивают по центру.

Ниже заголовка обычно размещен текстовый блок, в который автоматически заносятся сведения об авторе, взятые программой из данных операционной системы. При необходимости надо подставить данные о реальном авторе презентации.

На следующем этапе полезно выровнять положение текстовых блоков на слайде, для чего их можно выделить (при этом границы блока должны обозначаться серым цветом) и с помощью клавиш управления курсором разместить в нужном месте.

Текстовое содержание на слайдах можно создавать, ориентируясь на советы, имеющиеся в тексте самого шаблона. Любая часть текста на слайдах может быть отформатирована согласно предпочтениям автора. Для этого служат кнопки управления параметрами форматирования на панели инструментов и средства, предоставляемые диалоговыми окнами Шрифт и Список.

Важным инструментом PowerPoint при работе с текстом являются средства проверки орфографии. При этом не следует забывать, что ответственность за правописание лежит на авторе, а не на программе.

Работа с таблицами

Таблицы, размещаемые на слайдах презентации, должны быть простыми и понятными. Недопустимо применение таблиц со сложной структурой, так как времени на их изучение у аудитории нет. Назначение и характер данных в таблице должны быть понятны с первого взгляда.

Размещая таблицу на слайде, сделайте ее ячейки крупными, чтобы все данные в них читались ясно. Следует избегать размещения в ячейках текста длиной более одного-двух слов. Лучше всего таблицы выглядят, когда в ячейках размещаются только цифры и специальные значки.

Для привлечения внимания к таблице используются следующие элементы оформления: разделительные линии разной толщины и цвета; фоновый цвет для отдельных ячеек, столбцов, строк или таблицы в целом; эффекты анимации.

Таблица в PowerPoint может быть создана несколькими способами.

1. Рисованием непосредственно в поле слайда с помощью инструмента **Таблицы и Границы** панели инструментов.

2. Интерактивным указанием числа строк и столбцов (протягиванием мыши в рабочем поле) инструмента **Добавить таблицу** панели инструментов.

3. Копированием и вставкой таблиц через буфер обмена из внешних приложений (например Microsoft Word, Microsoft Excel и других).

4. Вставкой из внешних приложений (с внедрением или связыванием) средствами меню Вставка.

У каждого из описанных способов есть свои преимущества и недостатки. При рисовании таблицы в PowerPoint обеспечены наглядность и интерактивность, простые методы редактирования. При вставке таблицы из внешнего приложения можно использовать уже готовые наработки, а

связав таблицу с файлом, быть всегда уверенным, что на слайде отражены последние изменения в данных.

Работа с диаграммами

Программа PowerPoint поддерживает некоторые специальные средства для создания и анимации диаграмм. Непосредственно на слайде диаграмму создают с помощью внешнего приложения **Microsoft Graph**, запускающая кнопка которого находится на панели инструментов PowerPoint. Такой способ удобен благодаря простому, интуитивно понятному интерфейсу и доступу к многочисленным инструментам редактирования диаграммы. К тому же, к диаграммам в формате Microsoft Graph может быть применена особая анимация, позволяющая выводить элементы диаграммы по частям.

Другим способом размещения диаграммы на слайде является вставка объекта **Диаграмма Microsoft Excel**. В этом случае редактирование содержания возможно только средствами Excel. Однако такой объект может автоматически отслеживать изменения в файле-родителе (при их связывании) и тем самым приобретает свойство автоматического обеспечения актуальности. Это особенно важно при групповой разработке проекта, когда согласованность данных, используемых разными исполнителями, имеет ключевое значение.

Работа с иллюстрациями

Под иллюстрацией мы понимаем графическое изображение, созданное во внешних по отношению к PowerPoint приложениях. Выразительные, правильно подобранные иллюстрации способны существенно улучшить привлекательность презентации любого стиля. В некоторых случаях иллюстрации могут играть ключевую роль, стать основной темой доклада.

Простые иллюстрации можно взять из библиотек готовых элементов (клипартов), входящих в пакет поставки Microsoft Office. Существуют также библиотеки изображений самой разной тематики, распространяемые на CD-ROM. Многие из них отличаются хорошим качеством и вполне могут быть использованы в презентации. Важным источником иллюстраций является Интернет, хотя в каждом конкретном случае следует выяснить у их публикатора, как обстоит дело с правами на их использование.

Профессионалы предпочитают создавать собственные иллюстрации в таких программах, как Adobe Photoshop, Adobe Illustrator, CorelDraw, Painter и других. Хотя такая работа отличается трудоемкостью, индивидуальный подбор иллюстраций позволяет добиться высочайшего качества презентаций, что будет по достоинству оценено аудиторией.

У готовых изображений, взятых из свободно распространяемых коллекций, есть существенный недостаток – они широко известны. Слушатели могут по-думать, что докладчик либо готовил материалы в спешке, либо посчитал, что для данной темы этого достаточно. Особенно негативную реакцию такой подход вызовет в среде профессионалов компьютерной графики, рекламного дизайна, средств массовой информации. Если презентация рассчитана на аудиторию, разбирающуюся в компьютерах и графике, особенно при открытой публикации ее в Интернете, следует са-

мым серьезным образом подойти к вопросу создания иллюстраций.

Использование графических файлов в PowerPoint имеет свои особенности. Надо четко представлять, что при публикации в Интернете невозможно просмотреть иллюстрацию из-за ее огромного размера, а при печати на принтере невозможно получить качественный оттиск из-за низкого разрешения изображения.

В PowerPoint допустимо использовать графические файлы следующих форматов[1]:

• .BMP (BitMap) – формат хранения растровых изображений, ориентированный на операционную систему Windows. Такие изображения удобно переносить через буфер обмена. Рекомендуется использовать для снимков экрана, значков и других элементов Windows.

• .CDR (CorelDraw) – формат хранения векторных изображений программы CorelDraw. Рекомендуется использовать для векторной графики, рассчитан-ной на печатное устройство.

• .CGM (Computer Graphics Metafile) – универсальный формат хранения векторных изображений, принятый для систем автоматизированного проектирования. Используется для представления чертежей.

• .EPS (Encapsulated PostScript) – формат хранения векторных и растровых изображений, разработанный компанией Adobe Systems. Рекомендуется использовать при печати презентации на принтерах, совместимых со стандартом PostScript.

• .PPX (FlashPix) – формат обмена данными, используемый многими цифровыми фотокамерами. Рекомендуется использовать для электронной публикации презентации.

• .GIF (Graphics Interchange Format) – формат хранения сжатых изображений с фиксированным (256) количеством цветов. Позволяет выполнять чересстрочную загрузку изображений, создавать рисунки с прозрачным фоном и встроенной анимацией. Рекомендуется применять при публикации в Интернете.

• .JPG (Joint Photographic experts Group) – средство хранения растровых изображений с возможностью управления степенью сжатия. Рекомендуется использовать только для электронной публикации, в том числе в Интернете.

• .PCD (PhotoCD) – формат хранения графических изображений высокого качества, позволяющий хранить изображение с фиксированными величинами разрешений. Рекомендуется использовать для печати презентации на 35-мм слайдах.

• .PCT (Macintosh PICT) – формат рисунков операционной системы компьютеров Apple Macintosh.

• .PNG (Portable Network Graphics) – формат хранения изображений, ориентированных на публикацию в Интернете. Поддерживает глубину цвета до 24 бит. Рекомендуется использовать для электронных публикаций.

• .TIF (Tagged Image File format) – средство хранения растровых изобра-

[1] Информатика для юристов и экономистов / Симонович С.В. и др. – СПб.: Питер, 2001.С.569.

жений высокого качества. Диапазон глубины цвета до 32 бит. Рекомендуется применять при выводе презентации на печатное устройство.

• .WMF (Windows MetaFile) – формат хранения векторных изображений операционной системы Windows.

Перечисленные выше форматы графических файлов поддерживаются либо напрямую (их можно вставлять через буфер обмена и обрабатывать в PowerPoint), либо через собственные фильтры импорта PowerPoint. Однако допустимо использовать графику других форматов, если родительское приложение соответствует спецификации OLE. Так, например, на слайды можно вставлять файлы изображений высокого качества программы Adobe Photoshop (расширение .psd). В этом случае они могут редактироваться средствами родительской программы.

Работа с эффектами анимации

Напомним, что под анимацией в PowerPoint понимается порядок появления объекта на слайде, его представления и, при необходимости, скрытия. Анимация является свойством, которое может быть присвоено любому объекту презентации, кроме фона. Параметры анимации настраиваются индивидуально для каждого объекта на слайде. Сгруппированные объекты воспринимаются и анимируются как одно целое. Существуют некоторые виды объектов, к которым может быть применена эксклюзивная анимация, невозможная для объектов иного типа.

В текстовом объекте могут отдельно анимироваться абзацы, слова и даже отдельные буквы. Однако характер эффекта анимации применим только к текстовому объекту целиком. То есть нельзя, к примеру, одному абзацу назначить Вылет слева, а другому – Вылет сверху. Важной особенностью является возможность анимации текста, импортированного из других приложений.

Другим объектом с эксклюзивными свойствами анимации выступают диаграммы. Элементы диаграммы можно анимировать отдельно, по категориям. Следует иметь в виду, что импортируемые диаграммы (например, из программы Excel) воспринимаются как обычные объекты и анимируются только целиком.

Особым эффектом анимации служит **Действие после анимации**, то есть характер преобразования объекта по завершении анимации. Например, объект можно скрыть или перекрасить в другой цвет.

Принимая решение об анимации объекта, важно соблюдать меру и художественный вкус. Анимация должна служить привлечению внимания слушателей, но не его отвлечению или рассеиванию. Поэтому на одном слайде не рекомендуется анимировать более одного-двух объектов, иначе эффекты оформления могут отвлечь внимание от содержания презентации.

Работа со звуком и видео

Если презентация предназначена для представления в Интернете, автономного просмотра на компьютере и других видов электронной публикации, ее можно сопровождать звуковым оформлением. Это могут быть музыка, речь, звуковые эффекты. Обычно звуковые эффекты используют как элемен-

ты для привлечения внимания к отдельным слайдам, а музыка выступает самостоятельным элементом доклада при представлении творческой темы.

Речь используют для комментирования презентации, ориентированной на автономный просмотр. Вместе с тем, запись речи можно применять и для подготовки аудиторного доклада. Например, посредством звукозаписи можно представить обращение известного лица, привести цитату из речи исторического деятеля.

Звуковые эффекты вставляют для привлечения внимания аудитории либо к слайду в целом, либо к его объектам. Например, демонстрируя фотографию автомобиля, уместно в качестве звукового фона использовать звукозапись работы его двигателя. Если надо привлечь внимание к очередному слайду, можно вставить звук фанфар.

Надо иметь в виду, что передача звука в Интернете связана с определенными трудностями, так как объемы звуковых файлов могут быть весьма велики. Рекомендуется применять специальные форматы звуковых файлов, обеспечивающие высокую степень сжатия с возможностью управления качеством, например формат MP3.

Если требуется передавать речь и звуковые эффекты, вполне достаточно оцифровки со средним качеством, чтобы получить файлы небольших размеров. В случае передачи музыки следует опытным путем подобрать наиболее эффективное соотношение между качеством звучания и размером файлов.

Видеоклипы включают в презентацию обычно в том случае, если она демонстрируется на достаточно мощном компьютере или в локальной сети. Для публикации в Интернете видеоклипы использовать не рекомендуется, так как качество получается низким и ухудшает восприятие презентации. Чтобы гарантировать верное воспроизведение видеоклипов, лучше применять стандартные форматы, например файлы .avi или .mov.

Настройка действия

Специфическим средством программы PowerPoint является возможность настройки действия при щелчке или наведении указателя мыши на объект. К числу таких действий относятся: переход к другому слайду, документу, файлу, завершение показа, запуск макрокоманды или внешней программы, воспроизведение звука и так далее. Таким образом, реакция объекта на манипуляции с мышью становится его свойством.

Настройку действия рекомендуется применять при разработке и демонстрации сложных презентаций, которые состоят из разных частей, хранящихся на разных компьютерах сети. Полезно применять настройку действия для объектов, по которым могут понадобиться дополнительные разъяснения.

Замечание: Предположим, что по требованиям наглядности на слайде отображена таблица с данными только за отчетный период. У слушателей могут возникнуть вопросы по предшествующим периодам. В этом случае можно настроить такое действие, чтобы по щелчку мыши открывался файл таблицы Excel, содержащий полную информацию.

Средства оформления документов PowerPoint позволяют сделать элек-

тронную презентацию цельной и привлекательной. Управляя сменой слайдов, временем их показа, демонстрируя видеоклипы, воспроизводя звук, применяя анимацию, используя гиперссылки, можно существенно разнообразить презентацию.

6.4. Воспроизведение презентаций

Презентация перед аудиторией. Если презентация PowerPoint проходит в помещении с использованием монитора или проектора, с помощью **Мастера проекторов** можно регулировать разрешение экрана, соответствующее используемой проекционной системе.

Автономная презентация. В большинстве случаев автономная презентация применяется для автоматического показа на стенде фирмы во время выставки или конференции. При этом средства управления недоступны для зрителей, что необходимо для защиты от несанкционированного доступа. Обычно после завершения автономная презентация запускается повторно.

Сетевая конференция. Интеграция программ Microsoft позволяет в режиме реального времени совместно использовать презентацию и обмениваться сведениями с людьми, даже находящимися в других городах и странах. В ходе сетевой конференции совместно используются программы и документы, происходит обмен файлами, а также голосовыми и текстовыми сообщениями.

При совместной работе участники могут просматривать и изменять презентацию. Если во время сетевой конференции режим совместной работы отключен, в каждый момент времени только один человек может изменять презентацию, но в общении и в работе на общей электронной доске могут одновременно участвовать несколько пользователей.

Вещание презентации. Вещание презентации, включая видеоклипы и звук, может осуществляться через Интернет. Вещание обычно применяют на собрании акционеров фирмы или для проведения презентаций перед виртуальной аудиторией. С помощью приложения Microsoft Outlook или другой почтовой программы назначают начало вещания так же, как любой другой сетевой конференции. Презентация транслируется в формате HTML, поэтому все, что нужно пользователям для ее просмотра, – это браузер Microsoft Internet Explorer. Если какой-либо пользователь пропустил вещание или если вещание требуется заархивировать, презентацию можно записать и сохранить на Web-сервере с возможностью последующего воспроизведения.

Презентации в Интернете

Новую презентацию можно создать специально для использования в Интернете, а затем опубликовать, сохранив как Web-страницу. Опубликование презентации заключается в создании ее копии в формате HTML и размещении полученного файла на одном из Web-серверов Интернета. Копии одной презентации можно публиковать в разных местах. При этом по выбору автора публикуется презентация целиком, произвольная часть показа, один или несколько слайдов.

Просматривать презентацию можно в браузере Internet Explorer. В любом случае показ презентации осуществляется в полноэкранном режиме без отображения элементов окна браузера. Поскольку переход между слайдами является важным элементом презентации, автоматически включается панель перехода, отображающая область структуры.

Презентацию можно подготовить с таким расчетом, чтобы она одинаково хорошо смотрелась в цвете на экране и на распечатках (в оттенках серого или в черно-белом режиме), сделанных на лазерном принтере. Перед печатью в черно-белом режиме можно посмотреть, как будут выглядеть распечатки.

Заметки, выдачи и структуры

Для улучшения восприятия презентации аудитории можно раздавать так называемые выдачи – два, три или шесть уменьшенных эскизов слайдов, распечатанных на одной странице. В некоторых случаях можно распечатать заметки докладчика. При работе над презентацией можно распечатать ее структуру, включая заголовки слайдов и основные пункты. Кроме того, можно отправить слайды и заметки в Microsoft Word, чтобы подготовить их к печати средствами текстового процессора.

Средства управления показом презентации

Презентация запускается либо непосредственно из PowerPoint, либо с Рабочего стола стандартными для интерфейса Windows способами. Для автономного просмотра используются: специальное средство просмотра, поставляемое в комплекте PowerPoint.

Любому слайду презентации может быть присвоено свойство «скрытый», то есть запрет на показ во время данного просмотра. Это свойство можно изменить в ходе презентации с помощью меню управления переходом.

В ходе презентации с помощью средства Перо можно рисовать знаки и писать текстовые заметки на слайдах. Если во время сетевой конференции включен доступ всех участников, любой из них может воспользоваться данным средством.

Указатель мыши может быть скрыт во время демонстрации слайдов. По умолчанию он отображается, но автоматически скрывается, если мышь не задействована в течение 15 секунд.

В процессе показа слайдов можно создать отдельный список действий для каждого слайда, который по окончании презентации помещается на автоматически создаваемый последний слайд. Такое средство позволяет учитывать изменения, вносимые докладчиком или рекомендованные аудиторией. Также в ходе презентации можно вводить заметки и замечания докладчика, которые автоматически присоединяются к нужному слайду.

Во время показа слайдов в полноэкранном режиме рекомендуется использовать сочетания клавиш, управляющих демонстрацией. Полный список команд управления отображается после нажатия клавиши F1 во время показа.

Средства просмотра презентаций

Средством просмотра называется программа, используемая для по-

каза слайдов на компьютерах, где не установлено приложение Microsoft PowerPoint. С помощью Мастера упаковки средство просмотра помещается на диск с презентацией. Затем на другом компьютере презентация распаковывается вместе со средством просмотра и запускается показ слайдов. Кроме того, можно создавать список воспроизведения, используемый средством просмотра для последовательного показа нескольких презентаций.

Такой список создается в любом текстовом редакторе и представляет собой обычный текстовый файл с расширением .1st, где в отдельных строках которого указывается полный путь и имя каждого файла, предназначенного для показа. Некоторыми свойствами показа презентации можно управлять, используя параметры командной строки при запуске средства просмотра.

Контрольные вопросы

1. Какие значения имеет термин «презентация»?
2. С какими программами наиболее тесно интегрирован Power Point?
3. Назовите основные элементы структуры документа Power Point.
4. Опишите основные элементы интерфейса Power Point.
5. Охарактеризуйте основные этапы разработки презентации.
6. Как происходит презентация в сети Интернет?

Глава 7. Информационная технология баз данных

7.1. Банки данных

Понятие банка данных

Банк данных (БнД) – информационная система, комплекс специальных методов и средств для поддержания динамической информационной модели предметной области (ПО) с целью обеспечения информационных потребностей пользователей.

БнД может рассматриваться как специальная обеспечивающая подсистема в составе старшей по иерархии АИС.

Поддержание *динамической информационной модели* предусматривает не только хранение информации о ней и своевременное внесение изменений в соответствии с реальным состоянием объектов, но и обеспечение возможности учета изменений состава этих объектов (в том; числе появление новых) и связей между ними (т.е. изменений самой структуры хранимой информации).

Обеспечение *информационных потребностей* (запросов) пользователей имеет два аспекта:

• определение границ конкретной предметной области и поддержание соответствующей информационной модели;

• разработка БнД, ориентированного на эффективное обслуживание запросов различных категорий пользователей.

С точки зрения целевой направленности профессиональной деятельности принято выделять пять основных категорий пользователей:

• аналитики;

• системные программисты;

• прикладные программисты;

• администраторы;

• конечные пользователи.

По типу работы с БнД различают пользователей *постоянных* и *разовых*; пользователей-людей и пользователей-задачи; пользователей с различным *уровнем компетентности* (приоритетом). Каждый класс пользователей предъявляет специфические требования к своему обслуживанию (с точки зрения организации диалога «запрос – ответ»). Постоянные пользователи обращаются в БнД с фиксированными по форме (типовыми) запросами; пользователи-задачи должны иметь возможность получать информацию из БнД в согласованной форме в указанные области памяти; пользователи с низким приоритетом могут получать ограниченную часть информации из БнД и т.д.

Основные требования к БнД

Уровень сложности и важности задач информационного обеспечения ИТ баз данных определяет ряд ***основных требований*** к БнД:

• адекватность информации состоянию предметной области;

• быстродействие и производительность;

• простота и удобство использования;

• массовость использования;
• защита информации;
• возможность расширения круга решаемых задач.

Централизованное управление данными в БнД имеет *ряд важных преимуществ*:

• сокращение избыточности хранимых данных;
• устранение противоречивости хранимых данных;
• многоаспектное использование данных (при однократном вводе);
• обеспечение возможности стандартизации данных;
• обеспечение возможности санкционированного доступа к данным и др.

Все названные преимущества по существу связаны с такими основополагающими принципами концепции БнД, как интеграция данных, централизация управления ими и обеспечение независимости данных от прикладных программ их обработки.

Состав банка данных

БД (БД)– совокупность специальным образом организованных (структурированных) данных и связей между ними, датологическое (от англ. data – данные) представление информации о предметной области.

Если в состав БнД входит одна БД, банк принято называть *локальным*; если БД несколько – *интегрированным*.

СУБД – специальный комплекс программ и языков, посредством которого организуется централизованное управление базами данных и обеспечивается доступ к ним.

В состав любой СУБД входят языки двух типов:

язык *описания данных* (с его помощью описываются типы данных, их структура и связи);

язык *манипулирования данными* (его часто называют языком запросов к БД), предназначенный для организации работы сданными в интересах всех типов пользователей.

Наличие разнообразного состава потребителей информации потребовало включения в БнД специального элемента – *словаря данных*.

Словарь данных предназначен для хранения единообразной и централизованной информации обо всех ресурсах данных конкретного банка:

• об объектах, их свойствах и отношениях предметной области;
• данных, хранимых в БД (наименование, смысловое описание, структура, связи и т.п.);
• форматах представления данных;
• кодах защиты и разграничении доступа пользователей к данным и т.п.

Администратор баз данных – лицо (группа лиц), реализующее управление БД.

Функции администратора являются долгосрочными: он координирует все виды работ на этапах создания и применения БнД. На стадии проектирования АБД выступает как идеолог и главный конструктор системы; на стадии эксплуатации отвечает за нормальное функционирование БнД,

управляет режимом его работы и обеспечивает безопасность данных.

Основные ***функции*** администратора следующие:

• решать вопросы организации данных в БД;

• согласовывать представления пользователей, учитывать текущие и перспективные требования пользователей;

• следить, чтобы БД удовлетворяли актуальным потребностям пользователей;

• решать вопросы, связанные с расширением БД в связи с изменением границ предметной области;

• разрабатывать и реализовывать меры по обеспечению защиты данных, сбоев технических средств, обеспечивать секретность определенной части данных и разграничение доступа к ним;

• выполнять работы по ведению словаря данных; контролировать избыточность и противоречивость данных, их достоверность; и т.п.

7.2. Базы данных информационных систем

Процесс проектирования баз данных (БД) является весьма сложным. По сути, он заключается в определении перечня данных, хранимых на физических носителях (магнитных дисках и лентах), которые достаточно полно отражают информационные потребности потенциальных пользователей в конкретной ПО. Проектирование БД начинается с анализа предметной области и возможных запросов пользователей. В результате этого анализа определяется перечень данных и связей между ними, которые адекватно (с точки зрения будущих потребителей) отражают ПО. Завершается проектирование БД определением форм и способов хранения необходимых данных на физическом уровне.

В процессе разработки ***модели данных*** необходимо выделить информационные объекты, соответствующие требованиям нормализации данных, и определить связи между ними. Эта модель позволяет создать реляционную базу данных без дублирования, в которой обеспечивается однократный ввод данных при первоначальной загрузке и корректировках, а также целостность данных при внесении изменений.

При разработке модели данных могут использоваться ***два подхода***. В первом подходе сначала определяются основные задачи, для решения которых строится база, выявляются потребности задач в данных и соответственно определяются состав и структура информационных объектов. При втором подходе сразу устанавливаются типовые объекты предметной области. Наиболее рационально сочетание обоих подходов.

Процесс выделения информационных объектов предметной области, отвечающих требованиям нормализации, может производиться на основе *интуитивного* или *формального* подхода. Теоретические основы формального подхода были разработаны и полно изложены в монографиях по организации баз данных известного американского ученого Дж. Мартина.

При **интуитивном подходе** легко могут быть выявлены информаци-

онные объекты, соответствующие реальным объектам. Однако получаемая при этом информационно-логическая модель, как правило, требует дальнейших преобразований, в частности преобразования многозначных связей между объектами. При таком подходе возможны существенные ошибки, если отсутствует достаточный опыт. Последующая проверка выполнения требований нормализации обычно показывает необходимость уточнения информационных объектов.

При **формальном подходе** для выделения информационных объектов следует использовать следующие основные правила:

• на основе описания предметной области выявить документы и их атрибуты, подлежащие хранению в базе данных;

• определить функциональные зависимости между атрибутами;

• выбрать все зависимые атрибуты и указать для каждого все его ключевые атрибуты, т.е. те, от которых он зависит;

• сгруппировать атрибуты, одинаково зависимые от ключевых атрибутов. Полученные группы зависимых атрибутов вместе с их ключевыми атрибутами образуют ***информационные объекты***.

При определении ***логической структуры*** реляционной базы данных на основе модели каждый информационный объект адекватно отображается реляционной таблицей, а связи между таблицами соответствуют связям между информационными объектами.

В процессе создания сначала конструируются таблицы базы данных, соответствующие информационным объектам построенной модели данных. Далее может создаваться схема данных, в которой фиксируются существующие логические связи между таблицами. Эти связи соответствуют связям информационных объектов. В схеме данных могут быть заданы параметры поддержания целостности базы данных, если модель данных была разработана в соответствии с требованиями нормализации. Целостность данных означает, что в БД установлены и корректно поддерживаются взаимосвязи между записями разных таблиц при загрузке, добавлении и удалении записей в связанных таблицах, а также при изменении значений ключевых полей.

После формирования схемы данных осуществляется ввод непротиворечивых данных из документов предметной области.

На основе созданной базы данных формируются необходимые запросы, формы, макросы, модули, отчеты, производящие требуемую обработку данных базы и их представление.

7.3. Системы управления базами данных

Понятие и состав СУБД

В общем случае под СУБД можно понимать любой программный продукт, поддерживающий процессы создания, ведения и использования БД. К СУБД относятся следующие основные виды программ:

• полнофункциональные СУБД;

• серверы БД;

• клиенты БД;
• средства разработки программ работы с БД.

Полнофункциональные СУБД (ПФ СУБД) представляют собой традиционные СУБД, которые сначала появились для больших машин, а затем и для ПЭВМ. Из числа всех СУБД современные ПФ СУБД являются наиболее многочисленными и мощными по своим возможностям. К ПФ СУБД относятся, например, такие пакеты, как Clarion Database Developer, DataEase, DataFlex, dBase IV, Microsoft Access, Microsoft FoxPro и Paradox R:BASE.

Обычно ПФ СУБД имеют развитый интерфейс, позволяющий с помощью команд меню выполнять основные действия с БД: создавать и модифицировать структуры таблиц, вводить данные, формировать запросы, разрабатывать отчеты, выводить их на печать. Для создания запросов и отчетов удобно пользоваться языком QBE (Query By Example – формулировки запросов по образцу). Многие ПФСУБД включают средства программирования для профессиональных разработчиков.

Некоторые системы имеют в качестве вспомогательных и дополнительные средства проектирования схем БД или CASE-подсистемы. Для обеспечения доступа к данным SQL-серверов полнофункциональные СУБД имеют факультативные модули.

Серверы БД предназначены для организации центров обработки данных в сетях ЭВМ. Эта группа БД в настоящее время менее многочисленна, но их количество постепенно растет. Серверы БД реализуют функции управления базами данных, запрашиваемые другими (клиентскими) программами с помощью операторов SQL.

Примерами серверов БД являются следующие программы: NetWare SQL (Novell), MS SQL Server (Microsoft), InterBase (Borland), SQLBase Server (Gupta), Intelligent Database (Ingress).

В роли ***клиентских программ*** для серверов БД в общем случае могут использоваться различные программы: ПФ СУБД, электронные таблицы, текстовые процессоры, программы электронной почты и т. д. При этом элементы пары «клиент – сервер» могут принадлежать одному или разным производителям программного обеспечения.

В случае, когда клиентская и серверная части выполнены одной фирмой, естественно ожидать, что распределение функций между ними выполнено рационально. В остальных случаях обычно преследуется цель обеспечения доступа к данным «любой ценой». Примером такого соединения является случай, когда одна из полнофункциональных СУБД играет роль сервера, а вторая СУБД (другого производителя) – роль клиента. Так, для сервера БД SQL Server (Microsoft) в роли клиентских (фронтальных) программ могут выступать многие СУБД, такие как dBASE IV, Blyth Software, Paradox, DataEase, Focus, 1-2-3, MDBS III, Revelation и другие.

Модели данных в СУБД

СУБД зависит от модели, которая положена в основу базы. В наше время стали наиболее распространенными две модели: реляционная (модель

отношений) и объектно-ориентированная (модель объектов).

Реляционная модель. В 1969 году американский математик доктор Э.Ф. Кодд (E.F. Codd) проанализировал сложившуюся к тому времени ситуацию по базам данных. Во всех имевшихся в то время моделях были существенные недостатки: избыточность данных, сложность обработки и отсутствие безопасности хранения информации и т.п. Кодд решил создать свою модель – реляционную (relation – англ. "отношение" или просто "таблица"). Он реализовал хранение данных в табличной форме, то есть организовал такие "хранилища" в виде логических структур (физические методы хранения могут быть любыми). Тем самым Кодд сумел добиться наглядности представления информации и удобства ее обработки.

Для формирования таблицы данных стало достаточно выполнить определенный логический запрос, подчиняющийся законам булевой алгебры. Среди операторов манипуляции данными существуют минимум три операции: извлечение строк (SELECT), извлечение столбцов (PROJECT) и объединение таблиц (JOIN). В результате этих действий мы получаем таблицу.

Результатом любой операции в модели является объект того же рода, что и объект, над которым осуществлялось действие. Это и есть основное свойство описываемой модели.

Основные понятия, применимые к реляционной модели, следующие: тип данных, атрибут, кортеж, отношение и первичный ключ.

Тип данных –понятие, которое соответствует понятию типа в языках программирования. Для реляционной модели можно отметить такие основные типы, как "целые числа", "символы", "числа с плавающей запятой", "дата" и "финансы".

Атрибут – это столбец в таблице с данными. Например, если на экране имеется информация о хакерских течениях, эксплойтах и стаже деятельности, то все эти столбцы являются атрибутами.

Кортеж – строка в таблице с данными.

Отношение – таблица в целом. Описание типов данных, применяемых в таблице, называется заголовком отношения, а все остальное (собственно данные) – телом отношения.

Первичный ключ – минимальный набор атрибутов (столбцов), которые будут определять однозначную уникальность каждого кортежа (строки) в отношении (таблице). При создании базы следует очень внимательно отнестись к заданию первичного ключа. Иногда для аутентификации вводится дополнительное поле с порядковым номером, который будет однозначно разным для каждой строки. Но не запрещается выбирать для первичного ключа два или три атрибута – главное, чтобы это действие было логически обоснованным (подобный ряд атрибутов будет называться составным первичным ключом).

Чтобы добиться эффективного управления базой, необходимо обеспечить связанность данных. Для этого был придуман так называемый "внешний ключ", который представляет собой атрибут (или набор атрибутов) в

одной таблице, совпадающий по типу с первичным ключом другой. Следует соблюдать условие, согласно которому каждое значение в столбце одной таблицы должно совпадать с каким-либо значением в другой.

В теории СУБД выделяется три вида связей: один-к-одному, один-ко-многим и многие-ко-многим.

1. Один-к-одному. Этот вид связи применяется в том случае, когда первичный ключ одной таблицы ссылается на ключ другой.

2. Один-ко-многим. Наиболее типичная связь. Реализуется при копировании первичного ключа одной таблицы в другую. В этом случае во второй таблице этот ключ называется уже внешним.

3. Многие-ко-многим. Суть этого типа связи в том, что ключ в одной таблице связывается с ключом другой и наоборот. Эту связь напрямую вообще никак не реализовать. Чтобы обойти этот недостаток, используется классическое решение: добавляется промежуточное отношение, которое будет связано типом "один-ко-многим" как с первой, так и со второй таблицей. Многие СУБД построены именно на ее основе.

Средства разработки программ работы с БД

Средства разработки программ работы с БД могут использоваться для создания разновидностей следующих программ:

- клиентских программ;
- серверов БД и их отдельных компонентов;
- пользовательских приложений.

Программы первого и второго вида довольно малочисленны, так как предназначены, главным образом, для системных программистов. Пакетов третьего вида гораздо больше, но меньше, чем полнофункциональных СУБД.

К средствам разработки пользовательских приложений относятся системы программирования, например Clipper, разнообразные библиотеки программ для различных языков программирования, а также пакеты автоматизации разработок (в том числе систем типа клиент-сервер). В числе наиболее распространенных можно назвать следующие инструментальные системы: Delphi и Power Builder (Borland), Visual Basic (Microsoft), SILVERRUN (Computer Advisers Inc.), S-Designor (SDP и Powersoft) и ERwin (LogicWorks).

Кроме перечисленных средств, для управления данными и организации обслуживания БД используются различные дополнительные средства, к примеру мониторы транзакций.

Классификация СУБД

По характеру использования СУБД делят на *персональные* и *многопользовательские*.

Персональные СУБД обычно обеспечивают возможность создания персональных БД и недорогих приложений, работающих с ними. Персональные СУБД или разработанные с их помощью приложения зачастую могут выступать в роли клиентской части многопользовательской СУБД. К персональным СУБД, например, относятся Visual FoxPro, Paradox, Clipper, dBase, Access и др.

Многопользовательские СУБД включают в себя сервер БД и клиентскую часть и, как правило, могут работать в неоднородной вычислительной среде (с разными типами ЭВМ и операционными системами). К многопользовательским СУБД относятся, например, СУБД Oracle и Informix.

По используемой модели данных СУБД (как и БД), разделяют на иерархические, сетевые, реляционные, объектно-ориентированные и другие типы. Некоторые СУБД могут одновременно поддерживать несколько моделей данных.

Функции и языки СУБД

С точки зрения пользователя, СУБД реализует ***функции*** хранения, изменения (пополнения, редактирования и удаления) и обработки информации, а также разработки и получения различных выходных документов.

Для работы с хранящейся в базе данных информацией СУБД предоставляет программам и пользователям следующие два типа языков:

• язык описания данных – высокоуровневый непроцедурный язык декларативного типа, предназначенный для описания логической структуры данных;

• язык манипулирования данными – совокупность конструкций, обеспечивающих выполнение основных операций по работе с данными: ввод, модификацию и выборку данных по запросам.

Названные языки в различных СУБД могут иметь отличия. Наибольшее распространение получили два стандартизованных языка: QBE (Query By Example) – язык запросов по образцу и SQL (Structured Query Language) – структурированный язык запросов. QBE в основном обладает свойствами языка *манипулирования* данными, SQL сочетает в себе свойства языков обоих типов – *описания* и *манипулирования* данными.

Перечисленные выше функции СУБД, в свою очередь, используют следующие основные функции более низкого уровня, которые назовем ***низкоуровневыми***:

• управление данными во внешней памяти;
• управление буферами оперативной памяти;
• управление транзакциями;
• ведение журнала изменений в БД;
• обеспечение целостности и безопасности БД.

Реализация функции *управления данными во внешней памяти* в разных системах может различаться и на уровне управления ресурсами (используя файловые системы ОС или непосредственное управление устройствами ПЭВМ), и по логике самих алгоритмов управления данными. В основном методы и алгоритмы управления данными являются «внутренним делом» СУБД и прямого отношения к пользователю не имеют. Качество реализации этой функции наиболее сильно влияет на эффективность работы специфических ИС, например, с огромными БД, со сложными запросами, большим объемом обработки данных.

Необходимость буферизации данных и как следствие реализации функ-

ции *управления буферами* оперативной памяти обусловлено тем, что объем оперативной памяти меньше объема внешней памяти.

Механизм транзакций

Механизм транзакций используется в СУБД для поддержания целостности данных в базе. ***Транзакцией*** называется некоторая неделимая последовательность операций над данными БД, которая отслеживается СУБД от начала и до завершения. Если по каким-либо причинам (сбои и отказы оборудования, ошибки в программном обеспечении, включая приложение) транзакция остается незавершенной, то она отменяется.

Транзакции присущи три основных свойства:

• атомарность (выполняются все входящие в транзакцию операции или ни одна);

• сериализуемость (отсутствует взаимное влияние выполняемых в одно и то же время транзакций);

• долговечность (даже крах системы не приводит к утрате результатов зафиксированной транзакции).

Примером транзакции является операция перевода денег с одного счета на другой в банковской системе. Здесь необходим, по крайней мере, двухшаговый процесс. Сначала снимают деньги с одного счета, затем добавляют их к другому счету. Если хотя бы одно из действий не выполнится успешно, результат операции окажется неверным и будет нарушен баланс между счетами.

Контроль транзакций важен в однопользовательских и в многопользовательских СУБД, где транзакции могут быть запущены параллельно. В последнем случае говорят о сериализуемости транзакций. Под *сериализацией* параллельно выполняемых транзакций понимается составление такого плана их выполнения (сериального плана), при котором суммарный эффект реализации транзакций эквивалентен эффекту их последовательного выполнения.

При параллельном выполнении смеси транзакций возможно возникновение конфликтов (блокировок), разрешение которых является функцией СУБД. При обнаружении таких случаев обычно производится «откат» путем отмены изменений, произведенных одной или несколькими транзакциями.

Ведение журнала изменений в БД (журнализация изменений) выполняется СУБД для обеспечения надежности хранения данных в базе при наличии аппаратных сбоев и отказов, а также ошибок в программном обеспечении.

Журнал СУБД – это особая БД или часть основной БД, непосредственно недоступная пользователю и используемая для записи информации обо всех изменениях базы данных. В различных СУБД в журнал могут заноситься записи, соответствующие изменениям в СУБД на разных уровнях: от минимальной внутренней операции модификации страницы внешней памяти до логической операции модификации БД (например, вставки записи, удаления столбца, изменения значения в поле) и даже транзакции.

Для эффективной реализации функции ведения журнала изменений в БД необходимо обеспечить повышенную надежность хранения и поддер-

жания в рабочем состоянии самого журнала. Иногда для этого в системе хранят несколько копий журнала.

Обеспечение целостности БД составляет необходимое условие успешного функционирования БД, особенно для случая использования БД в сетях.

Целостность БД есть свойство базы данных, означающее, что в ней содержится полная, непротиворечивая и адекватно отражающая предметную область информация. Поддержание целостности БД включает проверку целостности и ее восстановление в случае обнаружения противоречий в базе данных. Целостное состояние БД описывается с помощью *ограничений целостности* в виде условий, которым должны удовлетворять хранимые в базе данные. Примером таких условий может служить ограничение диапазонов возможных значений атрибутов объектов, сведения о которых хранятся в БД, или отсутствие повторяющихся записей в таблицах реляционных БД.

Обеспечение безопасности достигается в СУБД шифрованием прикладных программ, данных, защиты паролем, поддержкой уровней доступа к базе данных и к отдельным ее элементам (таблицам, формам, отчетам и т.д.).

7.4. Распределенные банки данных

Следует выделить ***два класса*** систем распределенной обработки и систем распределенных данных:

1. системы распределенной обработки, которые в основном отражают структуру и свойства многопользовательских операционных систем с базой данных, размещенной на центральном компьютере;

2. системы распределенных данных, которые обеспечивают обработку распределенных запросов, используя информационные ресурсы, размещенные на различных ЭВМ сети.

Для распределенных баз данных свойственны следующие характеристики:

• база данных – это логически связанные, разделяемые на некоторое количество фрагментов данные;

• фрагменты распределяются по разным узлам, которые связаны между собой сетевыми соединениями;

• может быть предусмотрена репликация фрагментов;

• доступ к данным на каждом узле происходит под управлением СУБД, которая на каждом узле должна поддерживать работу как локальных приложений, так и глобальных.

Требования к распределенной обработке данных

Основные *условия и требования* к распределенной обработке данных:

• прозрачность относительно расположения данных (СУБД должна представлять все данные так, как если бы они были локальными);

• гетерогенность системы (СУБД должна работать с данными, которые хранятся в системах с различной архитектурой и производительностью);

• прозрачность относительно сети (СУБД должна одинаково работать в условиях разнородных сетей);

• поддержка распределенных запросов (пользователь должен иметь возможность объединять данные из любых баз, даже если они размещены в разных системах);

• поддержка распределенных изменений (пользователь должен иметь возможность изменять данные в любых базах, на доступ к которым у него есть права, даже если эти базы размещены в разных системах);

• поддержка распределенных транзакций (СУБД должна выполнять транзакции, выходящие за рамки одной вычислительной системы, и поддерживать целостность распределенной БД даже при возникновении отказов как в отдельных системах, так и в сети);

• безопасность (СУБД должна обеспечивать защиту всей распределенной БД от несанкционированного доступа);

• универсальность доступа (СУБД должна обеспечивать единую методику доступа ко всем данным).

Любой пользователь или любая прикладная программа оперирует с одной или несколькими базами данных. В том случае, когда прикладная программа и сервер БД выполняются на одном и том же узле, проблемы расположения не возникает. Однако в том случае, когда прикладная программа запускается на локальном узле, а база данных находится на удаленном, возникает проблема идентификации удаленного узла. Для того чтобы получить доступ к базе данных на удаленном узле, необходимо указать имя удаленного узла и имя базы данных. Если использовать жестко фиксированное имя узла в паре «имя_узла, имя_БД», то прикладная программа становится зависимой от расположения БД. Например, обращение к БД «host: stock», где первый компонент – имя узла, будет зависимым от расположения.

Одно из возможных решений этой проблемы состоит в использовании виртуальных имен узлов. Управление ими обеспечивается специальным программным компонентом СУБД – сервером имен (Name Server), который адресует запросы клиентов к серверам.

Ни один из существующих Бнд не удовлетворяет всем указанным требованиям вследствие следующих практических *проблем*:

• низкая и несбалансированная производительность сетей передачи данных;

• в разных системах используются разные физические форматы и кодировки;

• трудности выбора схемы размещения системных каталогов;

• необходимость обеспечить совместимость СУБД разных типов и поставщиков;

• увеличение потребностей в ресурсах для координации работы приложений с целью обнаружения и устранения тупиковых ситуаций в распределенных транзакциях.

Распределенные СУБД

Распределенные СУБД подразделяются на *однородные* и *разнородные.*

В *однородных системах* все узлы используют один и тот же тип СУБД.

Однородные системы значительно проще проектировать и сопровождать, добавляя новые узлы к уже существующей распределенной системе и повышая производительность системы за счет параллельной обработки информации.

Разнородные системы обычно возникают в тех случаях, когда узлы, уже эксплуатирующие свои собственные системы с базами данных, со временем интегрируются в распределенную систему. В разнородных системах на узлах могут функционировать различные типы СУБД, использующие разные модели данных. В разнородных системах для организации взаимодействия между различными типами СУБД требуется обеспечить преобразование передаваемых сообщений.

Распределенная СУБД должна иметь следующий набор функциональных возможностей:

• расширенные службы установки соединений должны обеспечивать доступ к удаленным узлам и позволять передавать запросы и данные между узлами, входящими в сеть;

• расширенные средства ведения каталога, позволяющие сохранять сведения о распределении данных в сети;

• средства обработки распределенных запросов;

• расширенные функции управления защитой, позволяющие обеспечить соблюдение правил авторизации и прав доступа к распределенным данным;

• расширенные функции управления параллельным выполнением, позволяющие поддерживать целостность копируемых данных;

• расширенные функции восстановления, учитывающие вероятность отказов в работе отдельных узлов и отказов линий связи.

Соответственно, программные средства, обеспечивающие целевую (функциональную) обработку данных, должны быть организованы таким образом, чтобы обеспечить более эффективное использование совокупных вычислительных ресурсов за счет специализированного разделения функций обработки между центральным процессом СУБД и клиентскими функционально-ориентированными процедурами.

Процедуры базы данных

В различных СУБД они носят название хранимых (stored), присоединенных, разделяемых и т.д.

Использование процедур базы данных преследует ***четыре цели***:

• обеспечивается новый независимый уровень централизованного контроля доступа к данным, осуществляемый администратором базы данных;

• одна и та же процедура может использоваться несколькими прикладными программами – это позволяет существенно сократить время написания программ за счет оформления их общих частей в виде процедур базы данных. Процедура компилируется и помещается в базу данных, становясь доступной для многократных вызовов;

• значительное снижение трафика сети в системах с архитектурой «клиент-сервер». Прикладная программа, вызывающая процедуру, передает

серверу лишь ее имя и параметры;

• процедуры базы данных в сочетании с правилами предоставляют администратору мощные средства поддержки целостности базы данных.

Процедуры обычно хранятся непосредственно в базе данных и контролируются ее администратором.

Правила

Механизм правил (триггеров) позволяет программировать обработку ситуаций, возникающих при любых изменениях в базе данных.

Правило придается таблице базы данных и применяется при выполнении над таблицей операций включения, удаления или обновления строк.

Одна из целей механизма правил — отражение некоторых внешних правил деятельности организации. Пусть, например, в базе данных Склад содержится таблица Деталь, хранящая сведения о наличии деталей на складе завода. Одно из правил деятельности завода заключается в том, что недопустима ситуация, когда на складе число деталей любого типа становится меньше некоторого числа (например, 1000).

Таким образом, если возникает ситуация, когда на складе количество деталей какого-либо типа становиться меньше требуемого, запускается процедура базы данных, которая заказывает недостающее количество деталей этого типа. Заказ сводится к посылке письма (например, по электронной почте), на завод или в цех, который изготавливает данные детали. Все это происходит автоматически, без вмешательства пользователя.

Важнейшая цель механизма правил – обеспечение целостности базы данных. Один из аспектов целостности – целостность по ссылкам (referential integrity) – относится к связи двух таблиц между собой.

Размещение данных в распределенных БД

Размещение данных в распределенных БД характеризуется следующими понятиями:

• **фрагментация**. Любая запись (отношение в случае реляционных моделей данных) может быть разделено на некоторое количество частей, называемых фрагментами, которые затем могут распределяться по различным узлам. Как отмечалось ранее, существуют два основных типа фрагментации: горизонтальная и вертикальная. В первом случае фрагменты представляют собой подмножества строк, а во втором — подмножества столбцов (атрибутов);

• **размещение**. Каждый фрагмент сохраняется на узле, выбранном с учетом оптимальной схемы доступа;

• **репликация**. Распределенная СУБД может поддерживать актуальную копию некоторого фрагмента на нескольких различных узлах.

Определение и размещение фрагментов должно проводиться с учетом особенностей использования базы данных (в частности, на основе анализа транзакций).

Существуют **четыре стратегии** размещения данных в системе:

1. ***Централизованное размещение***. Данная стратегия предусматривает

создание на одном из узлов единственной базы данных под управлением СУБД, доступ к которой будут иметь все пользователи сети.

2. ***Фрагментированное размещение***. В этом случае база данных разбивается на непересекающиеся фрагменты, каждый из которых размещается на одном из узлов системы.

3. ***Размещение с полной репликацией***. Эта стратегия предусматривает размещение полной копии всей базы данных на каждом из узлов системы. Стоимость устройств хранения данных и уровень затрат на передачу информации об обновлениях в этом случае также будут самыми высокими. Для преодоления части этих проблем в некоторых случаях используется технология снимков. Снимок представляет собой копию базы данных в определенный момент времени. Эти копии обновляются через некоторый установленный интервал времени, например 1 раз в час или в сутки.

4. ***Размещение с избирательной репликацией***. Данная стратегия представляет собой комбинацию методов фрагментации, репликации и централизации. Одни массивы данных разделяются на фрагменты, что позволяет добиться для них высокой локализации ссылок, тогда как другие, используемые на многих узлах, но не подверженные частым обновлениям, подвергаются репликации. Все остальные данные хранятся централизованно.

Доступ к данным в распределенных БД

Мобильный интерфейс к базам данных на платформе Java – JDBC (Java Data Base Connectivity) – это интерфейс прикладного программирования (API) для выполнения SQL-запросов к базам данных из программ, написанных на платформенно-независимом языке Java, позволяющем создавать как самостоятельные приложения, так и аплеты, встраиваемые в Web-страницы.

JDBC имеет ряд следующих отличий;

• приложения загружают JDBC-драйвер динамически, появляется возможность переключаться на работу с другой СУБД без перенастройки клиентского рабочего места;

• JDBC, как и Java в целом, не привязан к конкретной аппаратной платформе, следовательно проблемы с переносимостью приложений практически снимаются;

• использование Java-приложений и связанной с ними идеологии «тонких клиентов» обещает снизить требования к оборудованию клиентских рабочих мест.

Прикладные интерфейсы OLE DB и ADO – это прикладные интерфейсы доступа к данным с использованием SQL.

OLE DB (Object Linking and Embedding Data Base) специфицирует взаимодействие, обеспечивая единый интерфейс доступа к данным через провайдеров – поставщиков данных не только из реляционных БД. OLE DB предоставляет приложениям общее решение обеспечения доступа к информации независимо от типа источника данных.

OLE DB включает два базовых компонента: провайдер данных и потре-

битель данных. Потребитель (клиент) – это приложение или компонент, обращающийся к OLE DB. Провайдер (сервер) – это приложение, отвечающее на вызовы OLE DB и возвращающее запрашиваемый объект – обычно данные в табличном виде.

ADO (Active Data Object) – это универсальный интерфейс высокого уровня. Модель объекта ADO не содержит таблиц, среды или машины БД. Здесь основными объектами являются следующие: объект Соединение, создающий связь с провайдером данных; объект Набор данных и объект Команда – выполнение процедуры, SQL-строки. В общем случае ADO можно рассматривать как язык программирования, позволяющий выбирать, модифицировать и удалять записи.

7.5. Разработка и реализация информационной модели предметной области в СУБД Access

Эффективность функционирования любой информационной системы в юридической сфере во многом определяется уровнем разработки информационного обеспечения, ведущим направлением которого является технология создания и эксплуатации баз данных. В связи с этим актуальным является освоение принципов создания и эксплуатации баз данных. Изучение технологии баз данных дает необходимые знания в области создания и проектирования организованных массивов информации.

Процесс проектирования БД представляет собой последовательность переходов от неформального словесного описания информационной структуры предметной области к формализованному описанию объектов предметной области в терминах некоторой модели. Можно выделить следующие этапы проектирования.

1. ***Системный анализ*** и словесное описание информационных объектов предметной области.

2. Проектирование ***инфологической модели*** предметной области – частично формализованное описание объектов предметной области в терминах некой инфологической, например, ER-модели.

3. ***Даталогическое*** (или логическое) проектирование БД, то есть описание БД в терминах принятой даталогической модели.

4. ***Физическое проектирование*** БД, то есть выбор способа размещения БД на внешних носителях.

Системный анализ должен заканчиваться подробным описанием информации об объектах, формулировкой задач с кратким описанием алгоритмов их решения, описанием входных и выходных документов.

Инфологическая модель должна выражать информацию в виде, не зависящем от используемой системы управления базами данных (далее – СУБД). Обычно эта модель отражает описание объектов, их свойства и взаимосвязи в виде схем. В настоящий момент наиболее широкое распространение получила модель Чена (Chen), которая называется «сущность-связь» или ER-модель (Entity Relationship). В ее основе лежат следующие базовые понятия.

Сущность – это класс однотипных объектов. Сущность имеет уникальное имя. Объект имеет свой набор *атрибутов* – свойств объекта. Атрибут, однозначно идентифицирующий конкретный экземпляр сущности, называется ключевым.

Между сущностями могут быть установлены связи. По множественности связи делятся на три типа: *один-к-одному* (один экземпляр одной сущности связан только с одним экземпляром другой сущности), *один-ко-многим* (один экземпляр одной сущности связан с несколькими экземплярами другой сущности), *многие-ко-многим* (один экземпляр одной сущности связан с несколькими экземплярами другой сущности и наоборот). Связь любого типа может быть обязательной, если в данной связи должен участвовать каждый экземпляр, и необязательной. Связь может быть обязательной с одной стороны и необязательной с другой.

Для реализации проекта в конкретной СУБД следует разработать даталогическую модель. На настоящий момент для этой цели используется *реляционная модель данных.*

Существует *алгоритм* преобразования ER-модели в реляционную модель данных:

1. Каждой сущности ставится в соответствие отношение реляционной модели данных.

2. Каждый атрибут сущности становится атрибутом соответствующего отношения, задается тип данных и обязательность или необязательность данного атрибута.

3. Первичный ключ сущности становится ключевым полем соответствующего отношения.

4. В каждое отношение, соответствующее подчиненной сущности, добавляется атрибут основной сущности, и этот атрибут становится *внешним ключом.*

5. Для определения необязательного типа связи у атрибута, соответствующего внешнему ключу, устанавливается необязательность данного атрибута. При обязательном типе связи устанавливается его обязательность.

6. Если в ER-модели присутствуют связи «многие-ко-многим», то для перехода к реляционной модели данных (где такие связи не поддерживаются) вводится дополнительное связующее отношение. Оно связано с каждым исходным связью «один-ко-многим», а его атрибутами служат первичные ключи связываемых отношений.

В результате выполнения даталогического проектирования должна быть разработана схема БД, то есть совокупность отношений, которые моделируют объекты БД и связи между ними.

Пример разработки БД СУД

Необходимо разработать БД СУД согласно следующему описанию предметной области.

Описание предметной области. В каждом районе города имеется свой *районный суд.* В каждом суде имеются *судьи*, которые занимаются рассмо-

трением гражданских и уголовных *дел* и *помощники судей*, которые занимаются судебным делопроизводством. Каждый судья может иметь несколько помощников, но каждый помощник может работать только с одним судьей.

При разработке БД требуется отразить следующую информацию:

для дел – номер, название, дату открытия, дату закрытия, количество томов, кто рассматривает дело;

для судей – код, фамилия, имя, отчество, место работы (районный суд), коллегия;

для районных судов – код, район, адрес;

для помощников судей – табельный номер, фамилия, контактный телефон, чьи поручения исполняет (код судьи).

1. Разработка ER-модели (модель «сущность-связь»).

Согласно описанию предметной области можно выделить следующие сущности: ***районные суды, судьи, дела, помощники судей.***

При разработке модели «сущность – связь» каждая сущность изображается в виде прямоугольника, в верхней части которого отражается имя сущности, а в нижней – атрибуты данной сущности, ключевой атрибут подчеркнут.

В каждом районном суде могут работать несколько судей, но каждый судья может работать только в одном районном суде. Таким образом, между сущностями ***районные суды*** и ***судьи*** устанавливается связь один ко многим.

Каждый судья может вести несколько дел, но каждое дело ведет только один судья. Таким образом, между сущностями ***судьи*** и ***дела*** устанавливается связь один ко многим.

Каждый судья может иметь несколько помощников, но каждый помощник может работать только с одним судьей. Таким образом, между сущностями ***судьи*** и ***помощники судей*** устанавливается связь один ко многим.

Тогда ER-модель будет выглядеть следующим образом (рис. 7.1.):

2. Разработка даталогической модели БД.

Согласно алгоритму преобразования ER-модели в реляционную модель данных каждой сущности будет соответствовать одноименное отношение с соответствующими атрибутами. Какие поля будут полями внешнего ключа? Зачем они нужны? Атрибуты между которыми устанавливается связь должны иметь одинаковый тип и свойства. На рис. 7.2. показана реляционная модель «Суд», с указанием типов данных.

3. Реализация разработанной информационной модели в системе управления базами данных (СУБД) Access.

Формирование базы данных (далее – БД) в Access состоит из ряда последовательных этапов. Первый этап этого процесса – *создание таблиц*. Таблицы в Access являются теми первичными, исходными файлами, на основе которых в дальнейшем строится все здание БД. Каждой сущности модели соответствует своя таблица. Имя таблицы совпадает с именем сущности.

Данные в таблице организованы в столбцы (называемые *полями*) и строки (*записи*). Каждому атрибуту сущности соответствует поле в таблице.

Наиболее детальным и основательным методом формирования таблиц

является режим конструктора. В режиме конструктора задаются имена полей и типы данных. В зависимости от характера данных необходимо задать свойства полей.

Каждая таблица должна содержать одно или несколько полей, однозначно идентифицирующих каждую запись в таблице. Такое поле называется ключевым полем таблицы. Если поле содержит уникальные значения, такие как коды или инвентарные номера, то это поле можно определить как ключевое. Ключевой атрибут сущности становится ключевым полем таблицы.

3.1. Создание новой базы данных **Суд**.

Запустить программу Access и создать новую базу данных. Для этого воспользоваться пиктограммой на рабочем столе, либо выполнить **Пуск – Программы – Microsoft Access**. В диалоговом окне **Создание файла** (справа) выбрать пункт **Новая база данных**. Присвоить имя **Суд** (в папке своей группы). Завершить создание БД. В результате будет создан файл новой БД. На экране будет отображено **Окно базы данных**.

3.2. Создание таблицы ***районные суды*** в режиме конструктора.

В **Окне базы данных** выбрать вкладку **Таблицы**. Нажать кнопку **Создать**. В диалоговом окне **Новая таблица** выбрать **Конструктор**, нажать кнопку **ОК**.

При конструировании таблицы необходимо задать имена полей и тип данных. **Имя поля** – это заголовки столбцов таблицы. В разделе **Тип данных** можно задать, какие данные и в каком формате будут введены в таблицу (числовой, текстовый, денежный и т.п.). **Описание** поля является необязательным параметром при конструировании таблицы.

В первой строке в разделе **Имя поля** набрать ***код суда***. Мышкой переключиться в раздел **Тип данных**. Справа от указателя мыши появится стрелка раскрывающегося списка. Развернуть список и выбрать из него тип *Числовой*. Переключиться на следующую строку.

В разделе **Имя поля** набрать ***район***, в разделе **Тип данных** выбрать *Текстовый*. В нижней половине окна конструктора расположен раздел *Свойства поля*. Его вид зависит от выбранного типа данных (текстовый, числовой, денежный и т.д.). Заполнить свойства для поля ***район***. В разделе **Размер** поля указать 25 (символов), в разделе **Обязательное** поле указать *Да*, в разделе **Пустые строки** – *нет*.

В следующей строке раздела **Имя поля** ввести ***адрес***, в разделе тип данных выбрать *Текстовый*. В разделе **Размер** поля указать 50 (символов), в разделе **Обязательное** поле указать *Нет*, в разделе **Пустые строки** – *да*.

Задание ключевого поля. Каждая таблица должна содержать одно или несколько полей, однозначно идентифицирующих каждую запись в таблице. Такое поле называется ключевым. Ключ служит для установления связей между таблицами и для предотвращения ввода повторяющихся данных. В данной таблице в качестве ключевого следует использовать поле ***код суда***. Для того чтобы обозначить поле как ключевое, необходимо в режиме конструктора выделить поле и нажать кнопку  на панели инструментов.

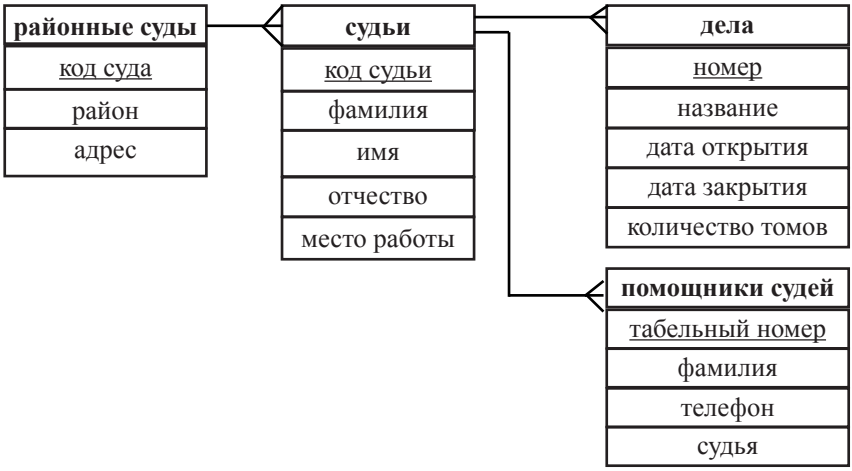

Рис. 7.1. ER-модель Базы данных «Суд»

Сохранение таблицы. Все объекты в Access, в том числе таблицы, сохраняются стандартным для Windows способом. Сохранить таблицу под именем ***Районные суды***. Закрыть таблицу.

3.3. Аналогично в режиме конструктора создаются таблицы ***Судьи***, ***Дела*** и ***Помощники судей***. Тип данных выбирается в соответствии с разработанной реляционной моделью (см. рис. 7.2.). Атрибуты, между которыми устанавливается связь, должны иметь одинаковый тип и свойства.

3.4. Создание связи между полями таблиц.

Когда между двумя таблицами устанавливается связь, это означает, что *величины из одной таблицы ставятся в соответствие величинам другой таблицы*. Обычно связывают *ключевое поле родительской таблицы* с соответствующим ему полем в *дочерней таблице* (внешним ключом).

Установить связи между таблицами согласно разработанной реляционной модели (рис. 7.2.). Перед созданием связей закрыть все таблицы! В меню **Сервис** выбрать **Схема данных**. В диалоговом окне **Добавление таблицы** отметить все четыре таблицы и нажать кнопку **Добавить**. Закрыть окно **Добавление таблицы**.

В окне **Схема данных** установить связь между соответствующими полями таблиц ***Судьи*** и ***Дела***. Для этого щелкнуть мышью по полю ***код судьи*** таблицы ***Судьи*** и, удерживая ее, перетащить указатель мыши на поле ***Судья*** таблицы ***Дела***. На экране появится диалоговое окно **Связи**. В левой части этого окна указано связываемое поле родительской таблицы, а в правой – дочерней. Поставить флажки на пунктах **Обеспечение целостности данных** и **Каскадное обновление**, нажать **Создать**. В окне **Схемы данных** появится линия связи между таблицами *Судьи* и *Дела*. Следует обратить внимание, что на одном конце линии связи стоит знак **1**, а на другом ∞. Этот тип связи называется *«один-ко-многим»*. Связь с отношени-

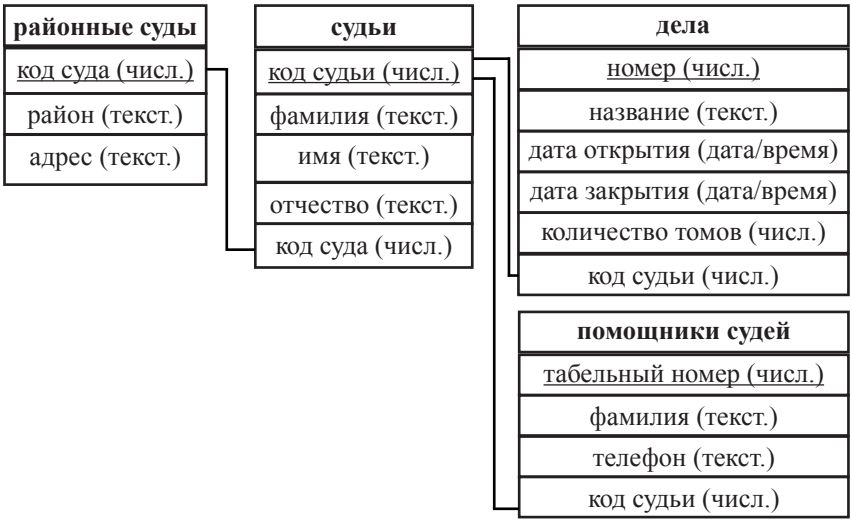

Рис. 7.2. Реляционная модель «Суд»

ем *«один-ко-многим»* является наиболее часто используемым типом связи между таблицами. В такой связи *каждой записи* в таблице *Судьи* могут соответствовать несколько записей в таблице *Дела*, а запись в таблице *Дела* не может иметь *более одной* соответствующей ей записи в таблице *Судьи*. Аналогично установить остальные связи.

3.5. Заполнить таблицы произвольными данными в режиме Таблица. Сначала заполнить таблицу ***Районные суды*** (3 записи), затем – ***Судьи*** (5 записей), а далее – ***Дела*** (7 записей) и ***Помощники судьи*** (8 записей). Для этого открыть нужную таблицу в режиме Таблица и ввести данные.

3.6. Дочерняя таблица в поле внешнего ключа может содержать только те значения, которые содержатся в ключевом поле родительской таблицы. Например, в поле ***место работы*** таблицы ***Судьи*** могут содержаться только те значения, которые ранее были внесены в поле ***код суда*** таблицы ***районные суды***.

Контрольные вопросы

1. Что такое реляционная база данных? Приведите примеры.
2. Что такое запись в базе данных?
3. Данные какого типа могут размещаться в полях базы данных? В чем их отличие?
4. Что называется ключевым полем (ключом) базы данных?
5. Приведите пример простого и сложного ключа.
6. Что такое индексное поле и как его используют в базах данных?
7. Для какого класса прикладных задач ОВД целесообразно использовать СУБД?
8. Назовите основные функции СУБД.
9. Дайте определение автоматизированного рабочего места (АРМ).
10. Укажите необходимый состав программно-аппаратных средств для АРМ сотрудника конкретной специализации (следственной, экспертной и т.д.).

Глава 8. Справочные правовые системы

Обеспечение юристов актуальной, полной и достоверной законодательной информацией, сведениями об изменениях и дополнениях, вносимых в нормативно-правовые документы, является одной из первоочередных задач. Сложность ее решения состоит хотя бы в том, что ежедневно только органами высшей государственной власти России принимается в среднем несколько десятков нормативных актов. Если учесть, что для эффективной работы часто требуется наличие нормативных актов, принимаемых субъектами РФ, а также *ведомственных документов*, то трудности и, вместе с тем, необходимость решения возникающих проблем становятся очевидными.

Пользователям нормативно-правовой информации приходится искать ответы сразу на несколько вопросов, основными из которых являются следующие:

• как поддерживать информационную базу в актуальном состоянии;

• как обеспечить быстрый поиск необходимого документа, особенно если нет полной информации о нем или необходимо обеспечить тематическую выборку;

• как хранить и каким образом систематизировать огромный объем нормативной документации.

Важнейшими требованиями при работе с нормативно-правовой информацией являются обеспечение *полноты информационной базы* и *поддержание ее в актуальном состоянии*. Выполнение этих требований приводит к необходимости решения задачи о включении в информационную базу множества ведомственных документов, которые часто не являются нормативными и получить которые достаточно сложно. Наиболее трудным моментом является пополнение и изменение базы, поскольку далеко не все документы публикуются. Более того, публикуется обычно изменившаяся часть документа, поэтому при работе с документом приходится одновременно просматривать несколько текстов: исходный и все изменения и дополнения. Часто окончательную редакцию документа приходится создавать самому пользователю, что может привести к появлению неточностей.

Традиционные методы получения информации, такие, как использование периодических печатных изданий или других печатных источников, не в состоянии адекватно решить поставленные задачи. Практика показала, что наиболее полное и последовательное решение как указанных выше вопросов, так и ряда других, находится на пути внедрения *компьютерных справочных правовых систем* (СПС).

8.1. История создания и тенденции развития СПС

Правовые базы данных впервые начали появляться за рубежом в конце 60-х, одновременно с развитием компьютерных информационных технологий. Первоначально они представляли собой электронные каталоги-картотеки, содержащие подробные реквизиты печатных изданий, содержащих

правовую информацию (система CREDOC, Бельгия). Фактически такие системы были призваны автоматизировать работу библиографов и облегчить поиск необходимой информации, не предоставляя доступ к текстам документов. Со временем появилась возможность диалогового терминального доступа к каталогам через библиотечные сети. Полнотекстовые системы, позволяющие не только найти документ, но и работать с его текстом впервые появились в конце 60-х годов в США, несколько раньше чем в Европе. Наиболее известна американская компьютерная правовая система LEXIS (DATA Corp.), впервые предоставившая не только тексты документов, но и дополнительную информацию к ним, а так же давшая возможность поиска информации по контексту и датам. Оказалось, что спрос на подобные системы огромен, и к середине 70-х, появилась система Westlaw. После включения в LEXIS британского законодательства и судебных прецедентов система получила название LEXIS-NEXIS, и доступна потребителям правовой информации в том числе через Интернет.

В настоящее время справочные правовые системы существуют во всем мире (США – WRU, LEXIS, WESTLAW, JURIS, Великобритания – INFOLEX, PRESTEL, POLIS, Германия – JURIS, Франция – IRETIV, Финляндия – FINLEX, и др.).

В юридическую практику Великобритании и США давно и эффективно внедрены целый ряд так называемых «экспертных» систем, содержащих толкование сложных правовых ситуаций, формы документов и договоров, методики и консультации экспертов.

Работы по созданию правовых баз данных в нашей стране начались в середине 70-х годов прошлого века, вначале – в рамках ведомственных информационных систем и для использования во властных структурах. Интерес к использованию компьютерных правовых систем начался с ростом потребности в правовой информации в конце 80-х годов, но из-за несовершенства наполнения и программных оболочек широкого распространения они не получили.

Появление массовых общедоступных правовых баз данных в нашей стране относится к началу 90-х годов. Большинство из них были созданы на базе стандартных (универсальных) СУБД, и затем, с учетом потребностей пользователей, переписаны с использованием языков высокого уровня.

В настоящее время в области правовой информатизации в России работают как государственные, так и коммерческие структуры. На рынке присутствуют около двадцати компаний – разработчиков правовых систем.

В последнее время обозначились два лидера правовых услуг: «ГАРАНТ» (НПП «Гарант-Сервис») и “Консультант Плюс” (НПО “ВМИ”), распространяющие свои программы в большинстве регионов РФ.

Разработка научно-производственного предприятия “Гарант-Сервис” – компьютерная справочная правовая система ГАРАНТ появилась в конце 1990 года. В системе ГАРАНТ впервые была применена гипертекстовая технология представления правовой информации в компьютерной форме и реа-

лизован поиск документов по словосочетаниям, встречающимися в текстах, ускоренный контекстовый поиск, позволяющий находить документы по словам, произвольно вводимым с клавиатуры, с возможностью прямого вхождения в текст документа в месте нахождения искомого слова (словосочетания).

НПО "ВМИ" осуществляет управление и координацию работы Сети КонсультантПлюс. Основной деятельностью Сети является распространение правовой информации. Координационным центром Сети разрабатываются программные продукты (СПС по федеральному и региональному законодательству, международному праву, и так называемые аналитические системы поддержки принятия решений) и планируется стратегия их распространения.

Предприятие "Центр компьютерных разработок" осуществляет разработку и сопровождение автоматизированных информационных систем «Кодекс» для Администрации и Законодательного собрания Санкт-Петербурга. Кроме того, разрабатываются и распространяются юридические системы по законодательству России и субъектов федерации, по международному праву, по налогам и особенностям бухгалтерского учета, по судебной, арбитражной и иной правоприменительной практике, база образцов правовых документов, специализированные (отраслевые) системы (например, «СтройЭксперт») и электронные правовые справочники. Оболочка систем позволяет работать с различными продуктами «Кодекс»; развивается интеграция продуктов, как приложений офисных систем.

Система «Эталон» (разработчик – НЦПИ при Министерстве Юстиции РФ), и база данных Научно-технического центра правовой информации "Система" ФСО РФ активно используются органами государственной власти и практически не распространяются коммерчески.

Научный центр правовой информации при Министерстве юстиции Российской Федерации (НЦПИ) проводит научные исследования по проблемам создания, внедрения и эксплуатации информационно – телекоммуникационных систем, а также осуществляет сбор и обработку правовой информации, создает и поддерживает в контрольном состоянии правовые базы данных, осуществляет обмен правовой информацией с государствами-участниками СНГ. Хранящаяся в НЦПИ информация может предоставляться на основе договоров органам государственной власти, юридическим и физическим лицам. На базе документов, поступающих из федеральных органов государственной власти, НЦПИ сформированы полнотекстовые базы данных правовых актов "Фонд" и "Эталон".

База данных "Фонд" – архив Министерства юстиции Российской Федерации, содержащий документы с 1917 года. Это правовые акты СССР, государств-участников СНГ, Российской Федерации. "Фонд" содержит не только документы бывшего СССР и России, но и акты субъектов РФ, прошедшие экспертизу в Минюсте.

"Эталон 5.0" – это полнотекстовая база данных по действующему российскому законодательству, в которую входят тексты действующих нормативных актов – законов, указов и постановлений органов государственной

власти, приказов и инструкций министерств и ведомств, судебная, нотариальная, арбитражная практика и т.п. Нормативные акты в базе данных "Эталон 5.0" поддерживаются в актуальном состоянии, пользователям предлагается последняя редакция документа, а также информация об актах, изменивших его первоначальный вариант.

Научно-технический центр правовой информации "Система" поддерживает эталонный банк данных правовых актов и распространяет базу данных правовых актов федерального уровня и электронные версии официальных бюллетеней: "Собрание законодательства Российской Федерации" и "Бюллетень нормативных актов федеральных органов исполнительной власти". Эталонный банк данных содержит правовые документы с 1992 года по текущий момент.

Тексты Федеральных законов и правовых актов Президента и Правительства Российской Федерации, распространяемые НТЦ "Система", в соответствии с Указами Президента Российской Федерации от 5 апреля 1994 года № 662 и от 23 мая 1996 года № 763, являются официальными.

Существуют так же ведомственные информационные системы правоохранительных органов, системы законопроектной и нормотворческой деятельности, о которых можно прочитать в специальной литературе.

Существует ряд менее распространенных правовых систем – «ЮСИС» («Интралекс»), «Законодательство России» («АРБТ»), «Референт» («Референт-Сервис»), «Юрисконсульт», «Ваше Право» («Информационные системы и технологии»), «Юридический мир» («Дело и право»), и др.

К такого рода продуктам можно отнести также отдельные базы данных и подборки документов, представленные в сетях Интернет.

Вначале считалось, что СПС создают лишь дополнительное удобства при работе с информацией и без их использования вполне можно обойтись. Однако, когда начались масштабные пересмотр и перестройка всего российского законодательства, уследить за огромным потоком вновь принятых нормативных актов стало невозможно. Поэтому к середине 1994 г. число потенциальных покупателей пакетов юридических программ значительно возросло.

Компьютерные справочные правовые системы обладают рядом важнейших свойств, делающих их практически незаменимыми при работе с нормативно-правовой информацией.

Во-первых, это возможность работы с *огромными массивами текстовой* информации. Объем информации в базе практически не ограничен, что позволяет вносить в нее ежедневно несколько десятков документов, одновременно хранить базы архивных документов и т.д.

Во-вторых, это использование в СПС специальных *поисковых программных средств*, что позволяет осуществлять поиск в режиме реального времени по всей информационной базе.

В-третьих, это возможность работы СПС с *использованием телекоммуникационных средств*, т.е. с применением электронной почты или сети Интернет. Такому подходу способствует развитие компьютерных сетей. В

этом случае можно избавиться от задержки обновления информационной базы, если работать в режиме on-line с базой данных, хранящейся на удаленном компьютере. В то же время не расходуется дисковое пространство на компьютере пользователя.

Следует, однако, отметить, что наибольшим спросом пока пользуются модификации СПС с локализованными базами данных. Объяснить это обстоятельство можно несколькими причинами. Во-первых, качество телефонных линий в России оставляет желать лучшего. Во-вторых, при обращении к базе данных в режиме on-line пользователь должен заплатить либо за междугородную телефонную связь, либо за трафик сети. В-третьих, справочные правовые системы, хранящиеся на компьютере пользователя, часто имеют больше сервисных возможностей. Тем не менее, если обращение к базе данных производится не чаще одного раза в месяц, работа в режиме on-line является предпочтительной.

Широкое признание пользователей получили коммерческие справочные правовые системы, такие как “КонсультантПлюс” (АО “Консультант Плюс”), “Гарант” (НПП “Гарант-сервис”). Фирмы-разработчики таких систем уделяли основное внимание во-первых, разработке и совершенствованию программных технологий и возможностей оболочек и, во-вторых, развитию сервисных центров поддержки СПС.

В результате проводимой политики коммерческие СПС завоевали широкое признание, что отражается, прежде всего, в количестве пользователей. Так, если в 1991–1992 в России было установлено около 4000 СПС, то в 1995–1996 уже более 100 000 таких систем, а в 2015 – более 5 млн. Работа со справочными правовыми системами становится нормой для специалистов различных уровней.

8.2. Структура справочно-правовых систем

Справочно-правовые системы в настоящее время включают в себя универсальные и специализированные базы данных, выпущенные различными эмитентами, относящимися к высшим органам государственной власти и управления.

Процесс классификации (рубрикации) документов заключается в определении предмета регулирования акта, соотнесении его с рубриками классификатора (рубрикатора) и присвоении обрабатываемому документу индексов соответствующих рубрик. Цель классификации документов состоит в том, чтобы обеспечить пользователю возможность поиска документов по определенной, интересующей его теме, вопросу. Для эффективной предметной классификации информации важно использовать в работе качественный и юридически обоснованный классификатор. Производители СПС и отделы кодификации в государственных органах используют в своей работе классификаторы, созданные на основе общеправового классификатора правовых актов, утвержденного Указом Президента РФ «О классификаторе правовых актов» от 15 марта 2000 г. № 511.

Рассмотрим ***структуру справочно-правовых систем*** на примере СПС «Гарант». Основные ***классы законодательства*** в СПС:

- основы государственно-правового устройства;
- гражданское право;
- налоги и сборы;
- бухгалтерский учет и аудит, статистическая отчетность;
- банковская деятельность;
- валютное регулирование и валютный контроль;
- таможенное право, внешнеэкономическая деятельность;
- ценные бумаги;
- жилые и нежилые помещения, коммунальное хозяйство;
- земельное право, природоохранная деятельность, природные ресурсы;
- общие вопросы хозяйственной и предпринимательской деятельности;
- гражданский и арбитражный процесс, исполнительное производство;
- труд, трудоустройство, занятость населения;
- социальная защита, пенсии, компенсации;
- семейное право, акты гражданского состояния;
- здравоохранение, образование, наука, культура, спорт и туризм;
- оборона, воинская обязанность и военная служба;
- охрана правопорядка, безопасность, правоохранительные органы;
- суд и судоустройство, адвокатура, нотариат;
- уголовное, уголовно-процессуальное, уголовно-исполнительное право;
- административные правонарушения, административная ответственность;
- международное право, международные отношения.

Классификатор законодательства имеет иерархическое строение – список классов дробится на подклассы и т.д. и в режиме ветвления можно выбрать подборку документов по интересующей узкой тематике или все документы данного класса.

Документы в СПС классифицируются ***по виду правовой информации:***

- Документы
- Судебная и арбитражная практика
- Международные договоры
- Разъяснения, комментарии и схемы
- Проекты законов
- Формы документов

По территории регулирования:

- Федеральные
- Региональные
- Международные

По статусу:

- Действующие
- Утратившие силу
- Не вступившие в силу

Рассмотрим подробнее виды правовой и экономической информации.

Документы

В данном разделе содержатся документы, относящиеся ко всем видам правовой информации, кроме проектов. Здесь находятся правовые акты, включая нормативные (Кодексы, Федеральные законы, Указы Президента Российской Федерации, постановления Правительства Российской Федерации, приказы и инструкции органов исполнительной власти, акты органов власти субъектов Российской Федерации и др.), а также судебную практику, международные соглашения. Все виды правовой информации систематизированы в данном разделе с помощью единого классификатора правовой информации.

Судебная и арбитражная практика

Раздел судебной и арбитражной практики включает в себя документы Конституционного Суда, Высшего Арбитражного Суда РФ, Верховного Суда РФ, федеральных арбитражных судов округов и федеральных судов общей юрисдикции. Эта информация нужна не только профессиональным юристам, но и всем, кто участвует в заключении договоров и урегулировании споров. Зачастую нормативные акты бывают сформулированы так, что невозможно однозначно определить порядок их применения и толкования. Именно в таких ситуациях незаменима подборка практики высших судебных инстанций, которая является ориентиром в применении норм права.

Международные договоры

Этот раздел включает в себя конвенции, декларации, международные пакты, многосторонние и двусторонние договоры России с другими странами, включая страны Содружества Независимых Государств. Международные соглашения, ратифицированные законами Российской Федерации, являются составной частью ее правовой системы. Согласно Конституции РФ, нормы международного права имеют приоритет по отношению к нормам внутреннего законодательства. Например, при изучении бухгалтером вопросов налогообложения иностранных компаний ему потребуются тексты российских нормативных актов, но и соответствующие документы международного права.

Разъяснения, комментарии, схемы

Особую важность для пользователей СПС представляет наличие в ней такого вида правовой информации, как консультационные материалы. Эти материалы помогают разобраться во всех тонкостях интересующего вопроса: получить не только необходимые для изучения нормативные акты, но и подробные компетентные разъяснения по их правильному применению. При изучении консультационных материалов следует учитывать, что взгляды различных специалистов могу различаться, особенно если изучаемый вопрос не находит однозначного регулирования в нормативных актах. Поэтому важно изучить разные мнения.

Проекты законов

Этот раздел содержит проекты кодексов и федеральных законов. Гра-

мотному юристу необходимо знать не только нынешнее законодательство но и прогнозировать свою деятельность в будущем. Все законопроекты в этом разделе сопровождаются пояснительными записками их авторов, из которых можно определить, что хочет получить законодатель в результате принятия того или иного закона. Кроме того, в системе отслеживается судьба каждого законопроекта от момента его внесения на рассмотрение Государственной Думы до момента подписания Президентом России.

Формы документов

Этот раздел представляет образцы деловых бумаг, формы бухгалтерской и статистической отчетности.

Кроме правовой информации в СПС представлен еще один полезный вид информации – справочная информация экономического характера, включающая в себя бизнес-справки, мониторинг законодательства и Календарь бухгалтера.

В разделе **Бизнес-справки** содержится наиболее часто используемая информация, которая целиком находится в информационном банке, но для ее поиска требуется определенное время, иногда весьма продолжительное. Например, минимальная заработная плата менялась со времен СССР два десятка раз. Соответственно, для ее изменения принималось такое же количество нормативных актов. Для того, чтобы отследить динамику изменения минимальной заработной платы, нужно найти и изучить все эти документы. Благодаря наличию в СПС соответствующей бизнес-справки, Вы можете сэкономить свое время.

Мониторинг законодательства – это обзор наиболее важных документов за последние версии системы. Имеется возможность быстрого перехода к ежедневно обновляемым информационным разделам сайта – мониторингу федеральных документов и разделу «Горячие документы».

Календарь бухгалтера (Налоговый календарь) представляет собой электронный календарь налоговых платежей, обязательных к уплате в тот или иной день, а также сроков предоставления налоговой отчетности о количестве рабочих дней в отчетных периодах. По ссылкам можно осуществлять переход непосредственно в текст нормативного документа, где регламентируется тот или иной платеж.

Каждый документ, находящийся в СПС, имеет определенные ***реквизиты***:

- тип документа,
- принявший орган, источник опубликования,
- раздел законодательства,
- номер и дату принятия,
- номер и дату регистрации в Министерстве юстиции.

По теме (предмету регулирования) нового документа, выделяются из информационного банка все документы по этой теме, а затем сопоставляют содержание нового документа с содержанием каждого из выделенных документов, выявляя взаимосвязи между документами. При этом необходимо отследить не только официально устанавливаемые взаимосвязи, но

реальные взаимосвязи документов, при которых новый документ определенным образом взаимодействует с документами, изданными ранее, но в новом документе не указывается ни характер взаимодействия, ни реквизиты документов, с которыми взаимодействует новый документ.

Между документами существуют ***ссылки***, которые можно разделить на два основных вида: *смысловые* и *формальные*. Ссылки являются гипертекстовыми, то есть в тексте документа они выделены цветом, и можно нажатием одной клавиши на клавиатуре (или щелчком мыши) перейти по этой ссылке в текст соответствующего документа.

Формальные ссылки, не определяя характера взаимосвязи, позволяют, тем не менее, перейти из текста просматриваемого документа в упоминаемый в нем документ.

В примечаниях и справочных сведениях к документу содержится информация о состоянии документа: о его соотношении с другими документами, о его действии или утрате силы, то есть та информация, которая необходима пользователю при применении документа, но которая не доведена до его сведения компетентным органом.

Для решения юридических вопросов нормативной информации бывает недостаточно. Многие нормативно-правовые акты отличаются сложностью, запутанностью и противоречивостью. Поэтому их применение зачастую требует дополнительных разъяснений, комментариев, консультаций и схем. СПС содержат десятки тысяч дополнительных справочных материалов по экономическим, социальным, финансовым, страховым и другим вопросам. Для того, чтобы неспециалист мог решать правовые вопросы с эффективностью юриста в СПС разработаны дополнительные справочные и обучающие информационные разделы: законодательство в схемах, практические библиотеки, энциклопедии, бераторы, толковый словарь и календарь бухгалтера.

8.3. Поисковые и сервисные возможности юридических пакетов

В настоящее время растет конкуренция между фирмами-производителями справочных правовых систем. Повышаются запросы пользователей СПС. Если еще недавно было достаточно лишь найти нужный документ, то сегодня зачастую необходимо еще и проследить все возможные связи между документами, получить разъяснения, подготовить обзор по интересующей теме, создать свою пользовательскую базу данных.

Как следствие, в развитии коммерческих СПС проявляются сходные тенденции – расширение спектра хранящихся в системе документов, улучшение программной оболочки систем, введение новых технологических возможностей. Фирмы-разработчики вводят в свои технологии то лучшее, что используется конкурентами, уделяют больше внимания развитию сбытовых структур. Вместе с тем, между существующими правовыми системами сохраняется много отличий, связанных с различными подходами к построению баз, к принципам их пополнения.

Существует множество параметров, по которым можно сравнивать и

оценивать справочные правовые системы. К ним относятся:

- объем информационного банка;
- скорость поиска документов по базе;
- актуальность информации и оперативность поступления документов;
- степень аутентичности документов оригиналу;
- юридическая обработка документов;
- формирование пользовательской базы;
- возможность удаленного доступа к базе через телекоммуникационные линии и ряд других важных характеристик.

Особо следует отметить возможность использования гипертекста. Гипертекст – это такая организация текста, при которой отображение и доступ к информационным блокам представлены в виде логических связей и явно указанных переходов.

Сегодня все распространенные системы осуществляют поиск по тематическому рубрикатору, названию принимающего документ органа, названию документа, дате принятия, типу документа и предусматривают вывод текста необходимого документа на печать или в текстовый файл.

Полнотекстный поиск по всему тексту информационной базы осуществляют программы “Кодекс”, “Юсис”, “Юрисконсульт”. Полнотекстный поиск из слов своего словаря предлагают пользователю СПС “Гарант” и “Консультант Плюс”.

При поиске по слову в названии документа в большинстве систем пользователю самому необходимо ограничить длину слова. Однако, например, СПС “Гарант” и “Консультант Плюс” найдут нужные слова, даже если они в другом падеже.

Очень помогает пользователям в работе *встроенный редактор* или возможность подключения внешнего редактора, как, например, в пакете “Кодекс”. Проследить связи между документами позволяют или *гипертекстовые* средства, как в СПС “КонсультантПлюс” и “Гарант”, или *система ссылок на документы* с возможностью просмотра их текста, внедренная в пакете “Кодекс”.

Возможность ведения *собственной базы* данных пользователя реализована в СПС “КонсультантПлюс” и “Кодекс”. *Многооконный режим* работы предусмотрен в системах “КонсультантПлюс”, “Кодекс”.

Глубокой *юридической обработке* подвергаются документы, поступающие перед подключением в систему “Гарант”. Анализируются нормативные акты в целом, выявляются прямые и косвенные связи между документами и правовыми нормами. В результате документы в СПС связаны перекрестными ссылками, не ограничивающимися случаями очевидных упоминаний одного документа в другом. Комментарии, вносимые в тексты документов юристами, подробно разъясняют, как применять данную правовую норму и значительно облегчают работу с документами, содержащими противоречивые формулировки.

Интеллектуальные черты СПС проявляются наличием базы знаний, с

чертами внутренней интерпретируемости, структурированности, связанности и активности. Объективно существование интеллектуальных черт может быть продемонстрировано на примере связи двух и более норм права (две правовые нормы связаны, если они содержат одинаковые термины и понятия и относятся к одной и той же сфере правового регулирования). Характерен так же пример, связанный с поиском латентной информации, то есть норм или понятий сходных или близких по смыслу, но выраженных в различной языковой форме. (Например – Строительная организация, С. предприятие, С. трест, С. объединение). Получение информации лишь по одному термину (например, при поиске по контексту), приводит к тому, что остальная информация остается невостребованной, скрытой – т.е. латентной. Латентная информация может быть исследована средствами гипертекста, найти свое отражение в комментариях к тексту документа, в системе респондентов\ корреспондентов для нормативного акта. Теоретически проблема решается созданием тезауруса – юридического словаря терминов и ключевых слов, отражающего логические связи между понятиями, реализованным в системе классификации нормативных актов системы, системе респондентов-корреспондентов для нормативного акта и в виде Энциклопедии ситуаций.

Применение гипертекстовых технологий позволяет отображать, наряду с текстом основного акта, иные тексты – систему ссылок, комментарии, разные редакции (ретроспективу), информацию о противоречиях, разъяснения и т.п.

Гипертекстовая структура базы позволяет проследить все виды взаимосвязей правовых актов законодательства РФ. Формирование базы нормативных документов происходит на основе использования логических и семантических средств, а также данных общей теории права. Логический анализ дополняется семантическим.

Интеллектуальные технологии работы с информацией предназначены для использования, прежде всего, в информационно-аналитических службах различных сфер деятельности (государственного управления, СМИ, и т.д.). Развитие подобных систем происходит на стыке нескольких направлений: семантические сети, гипертекст, лингвистические процессоры.

Специальные методы индексации данных в современных СПС позволяют выявить неслучайную устойчивую связь документов, связанных с рассматриваемой проблемой, а также получить информацию, раскрывающую характер и содержание интересующих пользователя связей. Таким образом, можно получить информацию по любому аспекту проблемы, выстроить аргументации в поддержку той или иной гипотезы, проследить связь между не связанными на первый взгляд фактами, обстоятельствами, вопросами. При сравнении директивных документов и проектов выявляются тесно взаимосвязанные позиции, обозначаются некоторые неочевидные или неявные взаимосвязи в рамках исследуемой проблемы или ситуации. Анализ дает возможность «заметить» эти связи, зафиксировать их, получить достаточно полную и систематизированную картину этих связей.

Некоторые справочные правовые системы предоставляют пользователю уже не только все необходимые документы, но и целые базы консультаций по применению законодательства. Пользователю предоставляются разъяснения и консультации, подборки документов по бухгалтерскому учету и аудиту, описывается порядок действий при аудиторских проверках, предоставляются электронные версии энциклопедий.

Далее мы подробнее рассмотрим возможности, принципы функционирования, состав и систему поддержки некоторых наиболее популярных справочных правовых систем.

КонсультантПлюс. Системы КонсультантПлюс появились на российском рынке более пятнадцати лет назад и в настоящее время их пользователями являются более 500 000 человек. На всей территории России действует около 300 сервисных центров более чем в 150 городах, которые образуют Общероссийскую сеть распространения правовой информации КонсультантПлюс. Центры сети обеспечивают оперативное, вплоть до ежедневного, обновление информационной базы СПС.

Наличие прямых договоров между фирмой-разработчиком КонсультантПлюс и более чем 100 основными законодательными органами об обмене правовой информацией, обеспечивает полное и оперативное включение правовых документов в базу системы. Среди партнеров – Аппарат Правительства РФ, Аппарат Государственной Думы Федерального Собрания РФ, Центральный Банк РФ и др. Тройная проверка документов перед внесением в базу СПС гарантирует отсутствие ошибок в текстах документов. Возможна ситуация, когда в базе СПС документ отсутствует. В этом случае АО “КонсультантПлюс” может заказать нужный документ в виде ксерокопии или текстового файла.

Популярность систем КонсультантПлюс объясняется их мощными технологическими возможностями. СПС КонсультантПлюс созданы на базе технологии, разработанной в Координационном Центре сети КонсультантПлюс, включающей в себя две взаимосвязанные компоненты: и*нформационно-поисковую систему* и *систему передачи информации*.

Информационно-поисковая оболочка системы КонсультантПлюс имеет ряд особенностей. Это вызвано тем обстоятельством, что большинство стандартных СУБД предназначены для работы с числовыми данными и не содержат средств поиска по текстовым полям большого размера, тогда как нормативные документы, составляющие Информационный Банк СПС КонсультантПлюс, представляют собой преимущественно текстовые поля.

Все программные модули СПС КонсультантПлюс реализованы на языке С++ с использованием специально разработанного оригинального *формата базы данных* и *способа индексации*. В версии КонсультантПлюс 6.0 реализована автоматическая корректировка индексных файлов и гипертекстовых связей при добавлении и изменении документов. Специальные алгоритмы автоматической корректировки индексов по всем словам в тексте документов позволяют избежать полной переиндексации базы данных системы.

В основу алгоритма поиска положен принцип построения "инвертированных данных", широко применяемый в полнотекстовых информационно-поисковых системах, дающий возможность независимо от объема информационной базы практически мгновенно осуществлять сложные поисковые операции.

В СПС КонсультантПлюс реализованы процедуры поиска по:

- виду документа;
- его регистрационному номеру;
- названию органа, принявшего документ;
- названию документа;
- словарю терминов;
- рубрикам;
- дате принятия;
- дате и номеру регистрации в Минюсте;
- статусу документа;
- словам и словосочетаниям, встречающимся в тексте документа.

Возможность использования логических условий при формировании поискового запроса позволяет:

- работать только с последними редакциями документов;
- отбирать документы, полученные с очередным пополнением;
- отбирать документы, поступившие в Информационный Банк пользователя за определенный промежуток времени.

Особенность систем КонсультантПлюс – оперативность доставки информации пользователю.

Специфика российских условий – отсутствие разветвленных информационных сетей и техническое несовершенство существующих линий связи. Это послужило причиной разработки *оригинальной схемы передачи информации* по Сети Консультант Плюс: *АО "Консультант Плюс" – региональные информационные центры – пользователи.* Алгоритмы и форматы обмена данными между эталонным информационным банком и абонентами сети КонсультантПлюс обеспечивают полную автоматизацию процедуры поддержания эквивалентности, достигающуюся передачей только новых и измененных документов. Такой способ называется "кусочным" пополнением, его реализация крайне важна для оперативности информационного обмена с помощью телекоммуникационных сетей в режиме OFF-LINE. Системы КонсультантПлюс доступны также в режиме ON-LINE через сеть Интернет.

Схема информационного обмена СПС позволяет пользователю формировать свой собственный информационный банк и держать на компьютере тексты только непосредственно необходимых документов. Наличие у пользователя постоянно актуализируемого полного каталога эталонного информационного банка дает возможность в любой момент заказать тексты отсутствующих документов.

СПС КонсультантПлюс характеризуются также:

- высокой степенью сжатия информации;

• быстродействием;

• простотой и удобством работы с программной оболочкой.

Такие преимущества достигнуты в результате внедрения ряда оригинальных разработок.

Во-первых, это *многоуровневый рубрикатор*, базирующийся на ***Общеправовом классификаторе отраслей законодательства***. Для рубрикатора с большим числом рубрик и уровней вложенности были разработаны необходимые средства отображения, которые позволяют:

• использовать преимущества "древовидной" структуры рубрикатора;

• формировать сложные поисковые запросы, объединяя по разным логическим условиям произвольное число рубрик.

Во-вторых, это *режим гипертекста*, т.е. переходы из текста одного документа в другой по системе перекрестных ссылок. Главная особенность работы с нормативно-правовой информацией состоит в необходимости учета существующей связи между документами и отслеживании изменений, а также возможности получить для каждого документа из информационного банка списки прямых и обратных ссылок и в случае необходимости быстро перейти в текст документа по этим ссылкам.

Прямые ссылки – это документы, на которые действует просматриваемый. *Обратные ссылки* – документы, которые действуют на просматриваемый. Ссылки четко классифицированы по *типам*, упорядочены по *важности* и *хронологии* происходящих с документом изменений.

Введение гипертекста не повлияло на "кусочный" способ пополнения информационного банка. Это достигнуто за счет специально разработанных алгоритмов динамической настройки перекрестных ссылок.

В-третьих, разработан режим *"папок" документов*, т.е. возможность сохранять сформированные подборки документов по некоторым тематикам, производить их объединение или пересечение. Становится возможной коллективная работа нескольких пользователей над одной проблемой.

Встроенный редактор СПС КонсультантПлюс позволяет использовать фрагменты текстов документов из информационного банка системы, закладки, расставляемые пользователем в текстах документов, истории выполненных пользователем запросов.

СПС КонсультантПлюс представляет собой семейство самостоятельных систем, каждая из которых предназначена для специалистов определенного уровня.

Система КонсультантПлюс: ВерсияПроф. Это уникальная справочная система по российскому законодательству. Содержит законы и подзаконные акты, принятые на федеральном уровне. Дает возможность пользователям иметь у себя на компьютере специализированные документы, документы общеправового характера, документы смежных специализаций. Позволяет организовать тематическую базу, убрав тексты ненужных документов.

КонсультантПлюс: ЭкспертПриложение – справочная система, содержащая все законодательные и нормативные акты РФ, а также документы

свыше 80 министерств и ведомств. Включает в себя документы, содержащиеся в системе КонсультантПлюс:ВерсияПроф, а также ведомственные документы либо тематические с разноплановой правовой информацией узкоспециального характера.

Система КонсультантСудебнаяПрактика – справочная система, содержащая документы Высшего Арбитражного Суда РФ, Верховного Суда РФ, обзоры дел, слушавшихся в разных судах, обзоры адвокатской и арбитражной практики.

КонсультантПлюс: Региональные выпуски. Содержит документы местного законодательства регионов: Москва, Санкт-Петербург, Астрахань, Екатеринбург, Омск, Тюмень, Нижний Новгород и т.д.

КонсультантПлюс: Регионльное законодательство. Первая в России свободная база нормативных актов органов местной власти и органов управления.

КонсультантПлюс:Международноеправо. Содержит многосторонние документы СНГ, двусторонние договоры России.

Еще одна СПС семейства КонсультантПлюс: ДеловыеБумаги. Эта система представляет собой универсальную “мини-канцелярию”, содержащую формы большинства стандартных деловых документов.

Системы семейства КонсультантПлюс работают на любых IBM-совместимых компьютерах, в локальных сетях, доступны в сети Интернет в режиме ON-LINE.

Обновление баз СПС производится курьером, по сети Интернет (возможно ежедневное обновление). Имеется возможность ведения собственной базы данных.

СПС КонсультантПлюс прошла тестирование в США и признана полностью совместимой с операционными системами Windows. Учитывая, что справочные правовые системы стали неотъемлемой частью информационного обеспечения всех крупных компаний, банков и государственных органов Российской Федерации, корректная работа правовых баз данных в операционных системах Microsoft имеет принципиальное значение для этих организаций.

В СПС КонсультантПлюс достигнут крупнейший в России объем информационного банка. Это документы федерального, регионального и международного права, а также аналитические, справочные и консультационные материалы по применению законодательства в судебной практике, в области бухучета, налогообложения, финансов и кредита. Новые документы передаются в систему ежедневно.

Гарант. Система ГАРАНТ разработана в 1990 году в научно-производственном предприятии “Гарант-Сервис”. Разработчики ставили перед собой задачу создания эффективной программной оболочки, позволяющей пользователям различной квалификации быстро получать необходимую информацию.

В настоящее время НПП “Гарант-Сервис” имеет более 300 представительств в регионах России и СНГ.

Постоянными партнерами компании являются органы власти и управ-

ления федерального и регионального уровней: Государственная Дума РФ, Администрация Президента РФ, Министерство финансов, Высший Арбитражный Суд РФ, мэрии Москвы, Санкт-Петербурга и других городов России. Двусторонние договоры предусматривают обмен информацией и ведение совместных проектов. Новые документы поступают в базы ГАРАНТа практически сразу после утверждения, еженедельно производится обновление информационного банка.

В системе ГАРАНТ применена *гипертекстовая технология* представления правовой информации. Открыт доступ к российскому законодательству через Интернет.

Новые версии СПС разработаны на основе результатов анализа особенностей российского законодательства с использованием передовых компьютерных технологий. Система обеспечивает *правовую поддержку принятия решения* с учетом современных требований.

Система ГАРАНТ имеет отличные показатели по аутентичности электронных копий документов официальным.

Кодекс. С документами любой выбранной базы данных выполняются все операции, доступные в системе. Команда *Все документы* позволяет отобразить на экране полный перечень документов, содержащихся в выбранной базе данных. Команда *Выборка* служит для поиска и выборки документов по заданным признакам. В окне *Условия выборки* можно: добавить новый признак, изменить значения уже выбранного признака, отказаться от ранее выбранного признака.

Два поля окна *Документы* содержат: в верхней части – список наименований документов, в нижней – полное название и атрибуты текущего документа. По умолчанию документы выстроены по алфавиту. *Сортировка* позволяет перестроить список по дате принятия, виду, номеру документа. Можно также сузить поиск уже среди найденных документов, вернувшись в окно *Условия выборки* и уточнив признаки.

В окне *Текст документа* доступны все функции просмотра и обработки текста, а также режимы просмотра и редактирования карточки документа, тематик и связей.

СПС Кодекс позволяет просмотреть перечень документов, связанных с данным, а также создать *собственную базу данных.* СПС Кодекс имеет полный набор средств для создания и ведения произвольного числа пользовательских баз данных.

Полнота и достоверность правовых баз данных

Подборкой документов, составляющих информационные базы коммерческих СПС, занимаются сами разработчики, заключая с органами власти договора о предоставлении документов. Централизованного информационного канала не существует.

Во всем мире юридическая информация на магнитных носителях *не имеет юридической силы.* И в этом Россия не является исключением. Поэтому в базах данных обычно есть ссылка на печатное издание.

Информация в базах данных СПС носит *исключительно справочный характер* и на нее нельзя ссылаться в суде. Что же касается возмещения материальных убытков из-за неточных или неполных сведений, то каждый разработчик решает этот вопрос по-своему.

Приобретение справочной правовой системы имеет смысл только при условии регулярного ее обновления и добавления документов по индивидуальному заказу.

Использование справочных правовых пакетов существенно облегчает работу, однако пользователю не следует ждать фантастических эффектов от использования юридической базы данных – она лишь хороший помощник в работе.

Следует также заметить, что широкий спектр юридических компьютерных систем – уникальное явление российского рынка делового программного обеспечения.

Контрольные вопросы

1. Определение СПС, основные параметры, характеризующие СПС.
2. Источники поступления информации в СПС.
3. Основные задачи, решаемые с помощью СПС. Ограничения в использовании СПС.
4. Понятие полноты информационного банка СПС. Критерии оценки полноты предоставляемой СПС информации.
5. Правовая информация. Подходы к разбиению массива правовой информации на отдельные базы.
6. Способы актуализации информационных банков СПС.
7. Справочные правовые системы КонсультантПлюс. Состав и характеристика систем по федеральному законодательству.
8. Справочные правовые системы КонсультантПлюс. Состав и характеристика систем поддержки принятия решений.
9. Цель и основные элементы юридической обработки документов в СПС.
10. Дайте определение гипертекста. Характеристика и использование гипертекста в СПС.
11. Документ как единица информационного банка СПС.
12. Охарактеризуйте основные виды поиска документов в СПС.
13. Опишите методику поиска документов в СПС при известных реквизитах.
14. Опишите методику поиска документов в СПС в случае, когда реквизиты неизвестны.
15. Дайте сравнительную характеристику справочных правовых систем (Гарант, Консультант Плюс, ЮСИС и т.д.).

Глава 9. Правовые ресурсы Интернета

9.1. Классификация правовых ресурсов

Правовые информационные ресурсы Интернета можно классифицировать по следующим основаниям:

1. По видам владельцев сайта – государственные организации, коммерческие организации, общественные объединения, образовательные учреждения, частные лица и т.п.

2. По отраслям права – теория государства и права, гражданское право, авторское право, информационное право и т.д.

3. По характеру содержания (контента) – каталоги правовых ссылок, научные публикации, правовые базы данных, сборники нормативных документов, предложение юридических услуг и пр.

4. По национально-территориальному признаку.

5. По охвату предполагаемой аудитории – международные, обще-российские, региональные и местные ресурсы.

Многие сайты трудно отнести к той или иной категории, так как они содержат комбинацию различных вариантов. Сайты могут содержать подборку нормативных документов, статьи, форум т.д.. Один и тот же сайт может попадать одновременно в несколько категорий классификации.

Как было отмечено ранее, пользуясь *поисковыми системами,* можно получить списки ссылок на правовые ресурсы. В многочисленных поисковых *каталогах* обычно есть соответствующие разделы правовой тематики. Они могут называться по-разному. Так, например, в каталоге ***Яндекс*** есть раздел «Общество», внутри которого есть подраздел «Власть». В каталоге поисковой системы ***Google*** также есть раздел «Общество», а в нем подразделы «Политика» и «Право». В поисковой системе ***АПОРТ*** есть раздел «Общество», в котором представлены следующие подразделы:

- Армия и вооружение
- Государственная власть
- Катастрофы, безопасность
- Люди
- Международные отношения
- Национальные отношения
- Миграция
- Общественные объединения
- Политика
- Право и законодательство
- Преступность, криминал
- Религия и духовность
- Социальные группы
- Публикации и аналитика
- Справочная информация

Имеются правовые разделы и на других ресурсах. В каталоге ресурсов

Russia on the Net (www.ru) есть раздел «Политика и право», содержащий три подраздела: Право, Политика и Официальные сайты, Разное. В справочном ресурсе *Желтые страницы Интернет* (http://yp.piter.com) юридическая тематика представлена разделом «Юридические услуги».

Правовая тематика представлена и на зарубежных каталогах.. На главной странице зарубежного каталога ***Yahoo!*** есть категория ***Government***, в которой есть раздел ***Law@***. Список каталога Yahoo! является конкретным примером возможного варианта классификации зарубежных правовых ресурсов.

9.2. Поиск правовых ресурсов

Многие правовые сайты и правовые порталы содержат собственные подборки ссылок юридической тематики. Например, сайт «Право России»[1] (http://www.e-pravo.ru) содержит каталог сайтов юридической тематики, а также статьи по законодательству и праву.

Для более полного или более конкретного поиска правовой информации в той или иной области права следует пользоваться поисковыми машинами. Оценить эффективность различных поисковых машин, можно, если использовать разные поисковики для одного и того же запроса. Это вызвано тем обстоятельством, что со временем происходит модернизация программного обеспечения поисковых машин, появляются новые поисковые сервисы, и в лидеры по качеству поиска могут выходить разные поисковые системы.

Можно сопоставить поиск по запросу «Правовые ресурсы интернет» в различных поисковых системах и сравнить полученные результаты.

Google (www.google.ru)

Поисковая машина Google в последнее время заслужила популярность во всем мире, в том числе и в России. Система ориентирована на поддержку русского языка, поэтому результаты отображаются корректно и удобно. Поисковая система использует механизм ранжирования информации, поэтому в начало списка попадают наиболее популярные ресурсы, удовлетворяющее запросу.

Яндекс (www/yandex.ru)

Один из лучших российских поисковиков. Страницы отсортированы по релевантности, что облегчает использование результатов поиска.

Rambler (www.rambler.ru)

Ссылки могут быть отсортированы по релевантности и по дате, и сгруппированы по сайтам и по документам. В остальном принципиальных отличий от других поисковых систем у Rambler нет.

Yahoo! по русски (ru.yahoo.com)

Параметры поиска поддаются корректировке в специальном окне «Настройки».

Иностранные поисковые машины дали в ответ на запрос «Правовые ресурсы интернет» следующие результаты:

AltaVista (www.altavista.com)

Найдено 1 млн. 970 тыс. результатов поиска. Результат поиска, несмо-

тря на англоязычный интерфейс, удобен для дальнейшей работы.

Fast Search (www.alltheweb.com)

Поисковая система дает в списке 1 млн. 960 тыс. результатов – примерно столько же, сколько и AltaVista.

В ответ на введенный запрос, как видно из рассмотренных примеров, поисковые системы выдали очень большое количество ссылок. Если провести анализ релевантности, то есть соответствия результата поставленной задаче, то качество результата почти всех систем нельзя признать удовлетворительным.

При большом количестве ссылок приходится сначала анализировать их аннотацию, заголовки сайтов, фрагменты, содержащие ключевые слова. Уже на этом, первом этапе исключается, как правило, больше половины ссылок. На втором этапе приходится конкретно просматривать содержимое найденных сайтов. При этом также выясняется, что большая часть сайтов не содержит нужной информации. Наконец, в целом ряде случаев приходится повторять запрос, задавая другое сочетание ключевых слов. Часто приходится включать расширенный поиск – либо применяя язык запросов, либо используя форму для задания дополнительных условий поиска.

9.3. Зарубежные правовые ресурсы

В зарубежных сегментах Интернет существуют специальные поисковые правовые системы – каталоги. Перечислим некоторые из них:

Catalaw: Metaindex of Law and Government (http://www.catalaw.com)

Это предметный указатель, содержащий законодательство различных стран, имеющий специализированный поиск.

Internet Legal Resource Guide (http://www.ilrg.com)

Это каталог, содержащий периодические издания, учебные заведения, профессиональные объединения, законодательство различных стран

FindLaw (http://www.findlaw.com) (рис. 9.1.).

Справочник ресурсов Интернет юридической тематики, учитывающий учебные заведения, правовые организации, судебные процессы и прочие ресурсы правовой направленности. В числе прочих отражены российские сайты, однако их общее число не превышает несколько десятков. Гораздо полнее учтены источники в США, Канаде и странах Западной Европы, поэтому FindLaw может служить надежной отправной точкой при обращении к правовым ресурсам западных стран. FindLaw обладает логичной внутренней структурой, включающей 14 основных категорий. Можно осуществлять поиск по заданной тематике в электронной библиотеке документов или в текущих сообщениях новостных агентств, включая Reuters, а также получать толкование юридического термина с помощью специального электронного словаря.

Law.com (http://www.law.com)

Каталог профессиональных объединений, учебных заведений, имеется юридический словарь.

Hieros Gamos (http://www.hg.org)

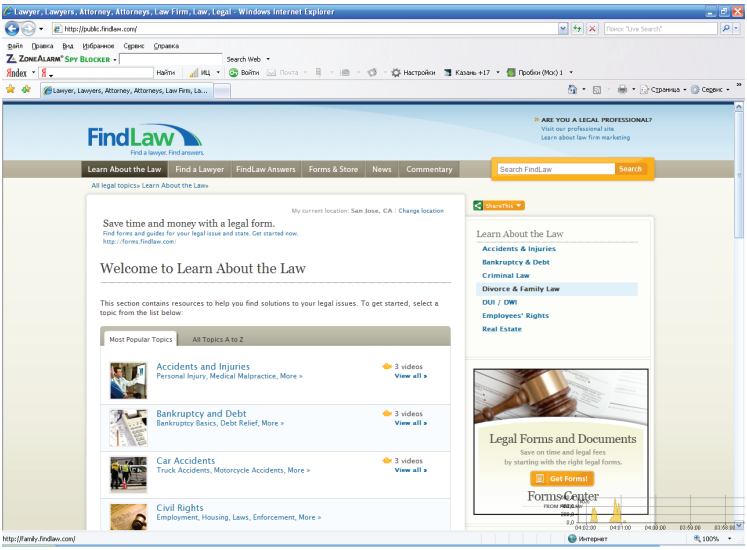

Рис. 9.1. Главная страница правового каталога FindLaw

Справочник юридической тематики, предлагает посетителям большой объем правовой информации, а также много дополнительных видов обслуживания – обращение к последним юридическим новостям, аналитическим обзорам, аудио семинарам, получение сведений об имеющихся вакансиях для юристов и т.д.

Law central – The Portal of Legal Portals (http://www.lawcentral.com)

Крупнейший юридический портал-каталог

LexisNexis (http://www.lexisnexis.com)

Говоря о зарубежных правовых ресурсах, необходимо отметить именно эту электронную библиотеку. LexisNexis – крупнейшая полнотекстовая политематическая электронная библиотека, поисковые возможности и информационные ресурсы которой способны решить самые сложные задачи, стоящие перед компаниями, организациями, вузами, правительственными учреждениями.

Информационными ресурсами LexisNexis пользуются более 2 миллионов клиентов по всему миру. Среди них консалтинговые фирмы, юридические и коммерческие организации, банки, брокерские конторы, правительственные учреждения, библиотеки, рекламные агентства, академические институты, газеты и журналы, тысячи университетов и т.д.

Система баз данных LexisNexis, основанная в 1968 году, в настоящее время содержит более чем 33000 информационных источников, свыше 150 информационных агентств, содержащих в совокупности более 4 миллиардов документов с глубоким архивом до 30 лет по бизнес информации и более 600 лет по юридической информации. Каждую неделю к ним добав-

ляются 18 миллионов документов. Общий объем информации, находящейся в LexisNexis, составляет около 30 Тбайт.

9.4. Российские правовые ресурсы

Приведенный ниже перечень сайтов правовой тематики не является полным и всеобъемлющим, однако дает примеры правовых ресурсов,относящихся к разным категориям. Пользуясь стандартными методами поиска, читатель легко сможет найти интересующий его конкретный ресурс.

Государственные органы Российской Федерации

• Сервер государственных органов России (http://www.gov.ru) (см. рис. 9.2.). На главной странице сайта размещены ссылки на другие официальные правовые ресурсы Российской Федерации.

• Сайт Президента Российской Федерации (http://kremlin.ru) (рис. 9.3.). Официальный информационный ресурс, выполняющий оперативное и всестороннее освещение деятельности Президента РФ; формирование и обновление банка данных о статусе Президента РФ, институтах власти, посредством которых реализуются конституционные полномочия Президента, о реформах и инициативах Президента, документах, подписанных Президентом. Представлена познавательная и образовательная информация об институте президентства в России, политическом устройстве, государственной символике и т.д. Имеется персональная информация о Президенте России Путине В.В..

• Правительство Российской Федерации (http://www.government.ru) – официальный интернет-портал.

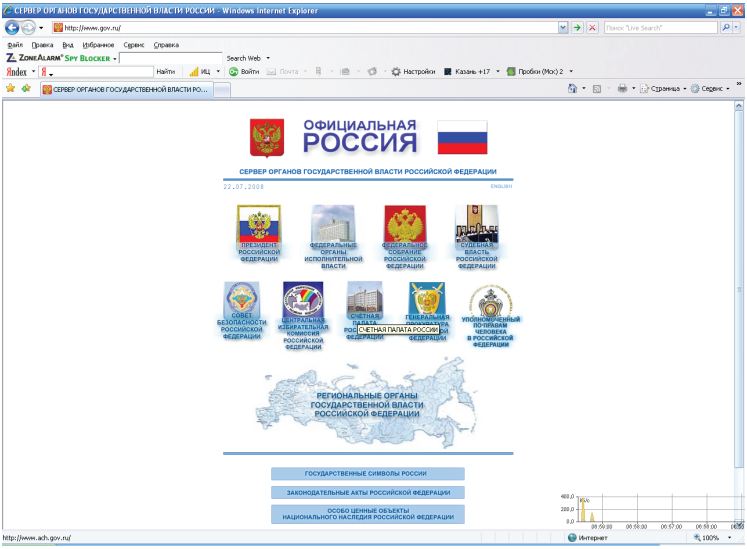

Рис. 9.2. Главная страница сервера органов государственной власти России

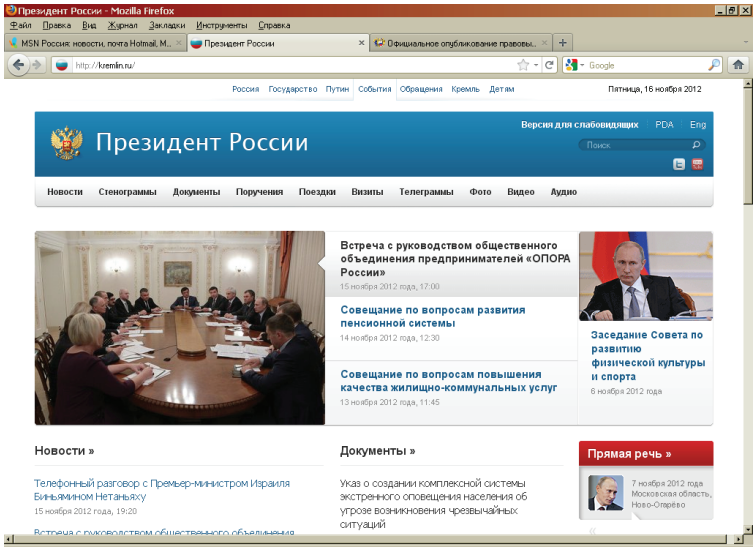

Рис. 9.3. Главная страница сайта Президента России

• Государственная Дума Федерального Собрания Российской Федерации (http://www.duma.gov.ru) – официальный сайт Государственной Думы.

• Совет Федерации Федерального Собрания Российской Федерации (http://www.council.gov.ru) – официальный сайт Совета Федерации/

Судебные органы

Судебные органы РФ также представлены в сети Интернет. Основные ресурсы следующие:

• Конституционный Суд РФ (http://ks.rfnet.ru/).

• Верховный Суд РФ (http://www.supcourt.ru).

• Высший Арбитражный Суд РФ (http://www.arbitr.ru).

Базы правовой информации

Все ведущие организации – разработчики справочно-правовых систем имеют свои сайты в Интернет. Эти сайты предоставляют множество полезной информации и дополнительных услуг, на основании чего их полноправно можно называть порталами. Многие фирмы предоставляют доступ через Интернет к своим правовым базам. Этот доступ осуществляется как на платной, так и на бесплатной основе. Бесплатный доступ предоставляется или в определенное время (например, в выходные дни), или к отдельным правовым базам, или к отдельным, обычно самым свежим, документам.

• КонсультантПлюс (http://www.consultant.ru). Сервер содержит информацию о кампании, выпускаемых продуктах, новые поступления документов, обзоры законодательства и много другой полезной информации. Помимо прочего, содержатся полные online-версии систем. Бесплатный доступ к своей основной базе «КонсультантПлюс:ВерсияПроф» Консультант Плюс

предоставляет в вечернее время (с 20 до 24 часов) и по выходным дням.

• СПС ГАРАНТ (http://www.garant.ru) – сайт системы «Гарант».

• ГАРАНТ On-Line (http://www.garant.park.ru). Интернет-версия системы ГАРАНТ (поиск по реквизитам, ситуации, источнику).

• Информационно-правовой Сервер «Кодекс» (http://www.kodeks.ru). Является Интернет-версией профессиональных юридических и специализированных систем «Кодекс». Содержит огромный банк данных по нормативно-правовой, нормативно-технической и специализированной информации для всех сфер деятельности, включающий более чем 500 000 документов. На сайте представлены образцы правовых и деловых документов, консультации юристов и аудиторов, словари юридических и бухгалтерских терминов, ежедневные обзоры законодательства России, Москвы, Санкт-Петербурга. Основная задача сервера – предоставить оперативный доступ граждан и организаций к постоянно обновляемой полнотекстовой базе данных. Поиск конкретного документа (списка документов) обеспечивается развитой и гибкой системой поиска.

• Правовая система «Референт» (http://www.referent.ru). On-line доступ к информационным модулям системы «Референт».

• Юридическое информационное агентство «Intralex» (http://www.intralex.ru). Информация о правовом органайзере АРМ “ЮРИСТ” (Юридическая информационная система). Мониторинг законодательства, описание услуг для вузов.

• Научно-технический центр правовой информации «Система» (http://www.systema.ru). Научно-технический центр правовой информации «Система» Федеральной службы охраны Российской Федерации. Сайт предоставляет доступ к правовой базе данных, содержит электронные версии официальных изданий.

Общеюридические ресурсы и правовые каталоги.

• InterLaw – юридический портал (http://www.interlaw.dax.ru). Юридический портал InterLaw имеет целью объединить все юридические сайты в одну большую сеть.

• Бесплатные ресурсы для юриста (http://antitax.ru). Сайт содержит законы, формы документов, налоговые схемы, много полезных ссылок на правовые ресурсы Интернета.

• Юрцентр (http://jurcenter.ru). Информационно-юридический портал, включающий правовую конференцию, виртуальную юридическую консультацию, поиск в правовых базах данных, вакансии для юристов, сборник типовых документов и т.п. Включает подписку на рассылки: «Новинки юридической литературы на ЮрЦентре» и «Новые публикации на ЮрЦентре».

• Каталог юридических ресурсов (http://www.e-pravo.ru). В каталоге можно зарегистрировать сайт, представляющий предприятие или личный проект в сети Интернет. На сайте ведется мониторинг рейтинга юридических ресурсов Интернета.

• ЮрКлуб – Виртуальный Клуб Юристов (http://www.yurclub.ru). Соз-

дан для обмена опытом людей, связанных с юриспруденцией, оперативного обсуждения возникающих вопросов. Имеются конференция, Чат, статьи. Содержит большое количество On-Line – публикаций правовой тематики. Имеется список рассылки, извещающей об обновлениях сайта.

• АКДИ (агентство консультаций и деловой информации) «Экономика и жизнь». Раздел «Право» (http://www.akdi.ru/pravo/akdi.htm). Оперативная экономико-правовая информация, новые документы и комментарии к ним, хроника законодательной деятельности российского парламента, налоговые и правовые консультации и статьи, арбитражная практика и др.

• Российская национальная библиотека, ссылки на правовые ресурсы (http://www.nlr.ru/lawcenter/lres/links.htm).

Тематические правовые сайты

• Коллекция ссылок на правовые ресурсы в области мировой торговли (http://www.miripravo.ru/links/links.htm).

• Налоговая помощь (http://www.taxhelp.ru). Сайт "Налоговая помощь" посвящен российскому налоговому праву. Помощь в решении вопросов налогообложения. На сайте есть статьи, рефераты, форум и многое другое.

• Право и средства массовой информации (http://www.medialaw.ru).

Правовое регулирование Интернет

• Интернет и Право (www.internet-law.ru). Авторский проект Антона Серго. Сайт посвящен юридическим аспектам компьютерной индустрии, интеллектуальной собственности в Интернете. Содержит большую подборку материалов по Интернет-правовой тематике, материалы Судебной палаты по информационным спорам и многое другое.

• Право и Интернет (http://www.russianlaw.net). Персональный ресурс Виктора Наумова, исследователя из Санкт-Петербурга. Проблемы правового регулирования Интернета: право телекоммуникаций, информационное право, интеллектуальная собственность. Семинар, статьи, иностранные прецеденты, предметная арбитражная практика и законопроекты, ссылки.

Сайты некоторых юридических ВУЗов

• Московская Государственная Юридическая Академия (www.msal.ru).

• Московский государственный институт международных отношений (Университет) (http://www.mgimo.ru).

•РоссийскаяЭкономическаяАкадемияим.Г.В.Плеханова(http://www.rea.ru).

• Академия государственной службы (http://www.rags.ru).

• Институт международной торговли и права (ИМТП). (http://www.iitl.ru).

• Институт экономики и права (http://www.stelecom.ru/iep).

Юридические библиотеки

• Юридическое издательство СПАРК и юридическая научная библиотека (http://www.lawlibrary.ru).

Контрольные вопросы и задания:

1. Назовите наиболее известные зарубежные правовые каталоги.
2. Какие правовые системы позволяют искать и получать правовые документы че-

рез Интернет?
3. Как подписаться на какие-либо правовые рассылки?
4. Приведите пример сайтов органов законодательной, исполнительной и судебной власти.

Задания. Поиск информации в интернет-версиях СПС

1. Пользуясь одним из серверов Гарант, Консультант, Кодекс (по указанию преподавателя), найдите:
• один из самых последних принятых Федеральных законов
• одно из самых последних Постановлений Правительства РФ
• одно из последних Постановлений Правительства Москвы
2. Определите, какие документы и в какое время доступны для бесплатного доступа в онлайн-версии системы Консультант.
3. Пользуясь сервером Научно-технического центра правовой информации «Система» найдите (по указанию преподавателя):
• Доктрину информационной безопасности Российской Федерации
• Арбитражный процессуальный кодекс Российской Федерации
• Гражданский процессуальный кодекс Российской Федерации

Часть III.
ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глава 10. Основы правового обеспечения информационной безопасности

10.1. Законодательство РФ в области информационной безопасности и защиты информации

Информация как объект правового регулирования

Развитие информационных технологий и их широкое внедрение в различные сферы человеческой деятельности вызвало рост числа противозаконных действий, объектом или орудием совершения которых являются компьютеры. Путем различного рода манипуляций, т. е. внесения изменений в информацию на различных этапах ее обработки, в программное обеспечение, овладения конфиденциальной информацией нередко удается получать значительные денежные суммы, уклоняться от налогообложения, заниматься промышленным шпионажем, уничтожать программы конкурентов и т.д.

Информационная среда – сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Как сфера правового регулирования информационная сфера представляет собой совокупность ***субъектов права***, осуществляющих такую деятельность, ***объектов права***, по отношению к которым, или в связи с которыми эта деятельность осуществляется, и ***социальных отношений***, регулируемых правом или подлежащих правовому регулированию.

В соответствии с действующим законодательством информационные правоотношения – это отношения, возникающие при:

• осуществлении права на поиск, получение, передачу, производство и распространение информации;

• применении информационных технологий;

• обеспечении защиты информации (Федеральный закон «Об информации, информационных технологиях и о защите информации»).

Основным **объектом** правоотношений в информационной сфере является информация. При рассмотрении информации в качестве предмета правоотношений в правовой системе, предмета отношений государства, юридических и физических лиц, приходится возвращаться к определению информации в его исходном смысле: **под информацией понимается содержание сообщений, сведений и сигналов**.

Это верно постольку, поскольку при движении информации в процессе ее создания, распространения, преобразования и потребления подавляющее *большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений.* Такой подход к определению понятия “информация” получил название **антропоцентрический**.

Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет информацию как «сведения (сооб-

щения, данные) независимо от формы их представления». Учитывая социальный аспект, добавим: включаемые в оборот в виде, понятном для восприятия человеком.

Закон вводит также термин «**документированная информация**» и определяет ее как «зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель».

Понятие «документированная информация» основано на **двуединстве информации** – *сведений* и *материального носителя*, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений. Информация "закрепляется" на материальном носителе, "привязывается" к нему и тем самым обособляется от своего создателя. В итоге, в качестве документированной информации мы получаем книгу, статью в журнале, сборник статей, фонд документов, банк данных или иной массив документов (данных) на бумажном, машиночитаемом или иных носителях. По сути, документированная информация представляет собой обыкновенные **данные**, а подход, отождествляющий информацию и данные, носит название **техноцентрический**.

Согласно приведенному определению, *документированная информация есть по сути дела объект материальный*, что дает основание относить ее также и к категории вещей. На нее распространяется право вещной собственности. Следует, однако, отметить, что документированная информация относится к вещам особого рода. Главное отличие заключается в единстве информации и материального носителя, что предопределяет специфику требований, касающихся ее правового режима.

С правовой точки зрения двуединство информации и материального носителя дает возможность защищать документированную информацию с использованием одновременно *двух институтов*: института интеллектуальной собственности и института вещной собственности.

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения следующих ее свойств:

- целостности;
- доступности;
- конфиденциальности.

Целостность информации заключается в ее существовании в неискаженном виде, неизменном по отношению к некоторому ее исходному состоянию.

Доступность информации – это свойство, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность – это свойство информации, указывающее на необходимость введения ограничений на доступ к ней определенного круга

пользователей.

Все известные на настоящий момент методы защиты информации можно разделить на следующие виды:

• правовые;

• организационные;

• технические.

Какое место занимают правовые методы в системе комплексной защиты информации?

В большинстве отечественных работ правовые методы защиты информации принято рассматривать в рамках организационно-правового обеспечения защиты информации. Правовые аспекты организационно-правового обеспечения защиты информации направлены на достижение следующих целей[1]:

• формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;

• определение мер ответственности за нарушение правил защиты информации;

• придание юридической силы технико-математическим решениям вопросов организационно-правового обеспечения защиты информации;

• придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

В современной юриспруденции организационный и правовой подходы не объединяют. Поэтому, на наш взгляд, не следует ограничиваться рассмотрением вопросов правовой защиты информации в рамках правовых аспектов комплексной защиты информации.

К правовым методам относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включается:

• законодательство об интеллектуальной собственности;

• законодательство о средствах массовой информации;

• законодательство о формировании информационных ресурсов и представлении информации из них;

• законодательство о реализации права на поиск, получение и использование информации;

• законодательство о создании и применении информационных технологий и средств их обеспечения.

В отрасли права, акты которых включают информационно-правовые

[1] Основы информационной безопасности: учебник / В.А.Минаев, С.В.Скрыль, А.П.Фисун, В.Е.Потанин, С.В.Дворянкин. – Воронеж: Воронежский институт МВД России, 2000. – 464 с.

нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

Законодательство Российской Федерации в сфере информации

«Информационная революция» застигла Россию в сложный экономический и политический период и потребовала срочного регулирования возникающих на ее пути проблем. Между тем, как известно, правовые механизмы могут быть включены и становятся эффективными лишь тогда, когда общественные отношения, подлежащие урегулированию, достаточно стабилизировались.

Необходимость срочной разработки юридических основ информационных отношений привела к поспешному и не всегда корректному формированию ряда базовых правовых понятий в этой области с их уточнением в каждом следующем нормативном акте. Понятно, что, отойдя от главенствующего ранее тезиса о том, что «право – это возведенная в закон воля господствующего класса», нынешний законодатель, стремясь удовлетворить потребности всех слоев общества, не был слишком внимателен к правилам законодательной техники, что привело к разноголосице в российских законах начала 90-х годов.

Законодательство России в области информационных правоотношений начало формироваться начиная с 1991 года.

Федеральный закон «Об информации, информационных технологиях и о защите информации» был принят Государственной Думой Федерального собрания Российской Федерации 8 июля 2006 г. Закон был подписан Президентом Российской Федерации 27 июля 2006 г., официально опубликован в «Российской газете» за 29 июля 2006 г. № 165. и вступил в силу с 9 августа 2006 г.

Закон об информации регулирует *три группы* отношений, достаточно емкие по содержанию:

• отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации (ст. 29 Конституции РФ);

• отношения, возникающие при применении информационных технологий и средств их обеспечения (например, правоотношения по созданию информационных сетей);

• отношения, возникающие при защите информации (например, связанные с правом на защиту личной жизни, защиты информации от несанкционированного доступа).

Сущность и характер общественных отношений, возникающих между различными субъектами в информационной сфере, во многом определяются особенностями и юридическими свойствами информации – основного объекта, по поводу которого и возникают эти отношения.

Объект информационных отношений обладает несомненными специфическими свойствами. Данная специфика предопределена многоаспектностью и многогранностью самого понятия «информация». Соответствен-

но информационные отношения, как правило, не выступают в чистом виде. Чаще всего они сопровождают другие отношения в сфере управления, государственного строительства, международного сотрудничества, в области экономики, жизни граждан и т.д. Процессы этого сопровождения все чаще и чаще регламентируются законодательными и иными нормативными актами: устанавливаются обязательность предоставления соответствующих видов информации, порядок ее распространения, правила доступа к ней и ограничения, ответственность за определенные правонарушения, обеспечение информационной безопасности и т.д.

В ст. 2 Закона «Об информации ...» определен ряд важнейших понятий:

информация – сведения (сообщения, данные) независимо от формы их представления;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации – возможность получения информации и ее использования;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной си-

стемы, в том числе по обработке информации, содержащейся в ее базах данных.

В ст. 3 Закона говорится, что правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

• свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

• установление ограничений доступа к информации только федеральными законами;

• открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

• равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

• обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

• достоверность информации и своевременность ее предоставления;

• неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

• недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

В ст. 5 Закона «Об информации…» записано, что в зависимости от категории доступа к ней она подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

• информацию, свободно распространяемую;

• информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

• информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

• информацию, распространение которой в Российской Федерации ограничивается или запрещается.

К общедоступной информации, в соответствии со ст. 7, относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Из ст. 8 следует, что не может быть ограничен доступ к:

• нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

• информации о состоянии окружающей среды;

• информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

• информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

• иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Бесплатно предоставляется информация:

• о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

• затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

• иная установленная законом информация.

Ст. 9 Федерального Закона содержит ограничения на доступ к информации. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и

(или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В ст. 11 по вопросу документирования информации записано, что электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В ст. 16, посвященной защите информации, записано, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

• обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

• соблюдение конфиденциальности информации ограниченного доступа;

• реализацию права на доступ к информации.

Согласно ст. 17, нарушение требований Федерального закона «Об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Следует особо отметить, что Российское законодательство последовательно рассматривает информацию в качестве самостоятельного объекта регулирования лишь в том случае, если она является документом. Объектом собственности выступает документированная информация, входящая в состав информационных ресурсов и информационных систем. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Президентом Российской Федерации утверждена **Доктрина информационной безопасности Российской Федерации** (09.09.2000 №. Пр-1895), которая опубликована в «Российской газете» от 28.09.2000 №. 187.

Доктрина информационной безопасности Российской Федерации (Доктрина) представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Особую значимость представляют следующие положения Доктрины[1]:

1. Информационная безопасность Российской Федерации понимается в Доктрине как состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Определяется содержание интересов личности, общества и государства в информационной сфере. При этом в качестве составляющей части этих интересов называется обеспечение права на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности (пункт 1 раздела I).

2. В Доктрине выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

- соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
- информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным и информационным ресурсам;
- развитие современных информационных технологий, отечественной индустрии информации и т.п.;
- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем (пункт 1 раздела I).

3. Доктрина называет в числе угроз информационной безопасности Российской Федерации угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, среди которых, в частности, выделяются:

- создание монополий на формирование, получение и распространение информации в Российской Федерации;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- неисполнение требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти, органов местного самоуправления, к открытым архивным материалам, к другой открытой

[1] О Доктрине информационной безопасности Российской Федерации. ПИСЬМО ВАС РФ No. С1-7/УЗ-1121 от 31.10.2000.

социально значимой информации;

- манипулирование информацией (дезинформация, сокрытие или искажение информации) и др. (пункт 2 раздела I).

Среди источников угроз информационной безопасности называется и отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти и других органов и сфер деятельности (пункт 3 раздела I).

4. Особое место в Доктрине отводится особенностям обеспечения информационной безопасности в сфере экономики, играющего ключевую роль в обеспечении национальной безопасности Российской Федерации (пункт 6 раздела II).

Отмечается, что недостаточность нормативной базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну.

5. В Доктрине определяются и некоторые особенности обеспечения информационной безопасности в судебной сфере (пункт 6 раздела II).

К наиболее важным объектам обеспечения такой безопасности относятся информационные ресурсы судебных органов, содержащие специальные сведения и оперативные данные служебного характера.

При этом среди специфических методов и средств обеспечения информационной безопасности в судебной сфере называются в качестве главных создание защищенной многоуровневой системы интегрированных банков данных справочного и статистического характера, а также повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

6. В Доктрине сформулированы основные положения государственной политики обеспечения информационной безопасности Российской Федерации (пункт 8 раздела III).

В качестве приоритетного направления такой политики называется правовое обеспечение информационной безопасности, которое должно базироваться, прежде всего, на соблюдении принципов законности и баланса интересов граждан, общества и государства в информационной сфере.

7. Органы судебной власти, как это предусмотрено в Доктрине, являются одним из основных элементов организационной основы системы обеспечения информационной безопасности Российской Федерации. В их задачи входит осуществление правосудия и обеспечение судебной защиты граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации (пункт 11 раздела III).

Уголовный кодекс РФ, вступивший в действие в 1997 году, установил нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие ответственность за их совершение. Такие нормы появились в российском законодательстве впервые.

Таким образом, мы видим, что информационные отношения получили и уголовно-правовую защиту. Из этого следует, что *информация*, в том числе *конфиденциальная* и *документированная*, стала новым *объектом преступления*.

Сейчас, когда ряд базовых нормативных актов в области информационных отношений создан и принят, наступило время для их применения на практике. Однако на этом пути неизбежны пробы и ошибки, обычные для претворения в жизнь решений, принятых с поспешностью. Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а следовательно, и негативные последствия. И если такие ошибки, допущенные в области хозяйственных отношений, могут быть тем или иным образом эффективно исправлены, ошибки в области уголовно-репрессивной отражаются на конституционных правах и свободах конкретных граждан и носят необратимый характер.

Поэтому очевидно, что настоящее время законодательная база обеспечения защиты информации в стране находится в состоянии становления. Продолжается процесс ее создания и совершенствования.

10.2. Понятие и виды защищаемой по законодательству РФ информации

Статья 5 Федерального Закона «Об информации, информационных технологиях и защите информации» устанавливает две группы информационных ресурсов по категориям доступа: открытые информационные ресурсы и информационные ресурсы, доступ к которым ограничен в соответствии с законом.

Все государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет информация, отнесенная законом к категории ограниченного доступа.

В соответствии с законом «Об информации ...», защите подлежат сведения ограниченного доступа, а степень защиты определяет их собственник. Ответственность за выполнение мер по защите информации возлагается не только на собственника информации, но и на ее пользователя.

Информация с ограниченным доступом, в свою очередь, подразделяется на сведения, составляющие государственную тайну и конфиденциальную информацию (ФЗ «Об информации ...»). Классификация информации по категориям доступа приведена в таблице 8.1.

В таблице 8.1 приведен перечень видов информации с ограниченным доступом и соответствующая нормативная база.

Следует отметить, что из всех многочисленных видов конфиденци-

альной информации в законе «Об информации, информационных технологиях и защите информации» упомянуты коммерческая, служебная, профессиональная, личная и семейная тайны, а также персональные данные. Наличие в п. 4 ст. 9 слов «иную тайну» подразумевает расширение списка конфиденциальной информации.

В Указе Президента России от 06.03.97 г. № 188 «Об утверждении перечня сведений конфиденциального характера» была предпринята попытка упорядочить состав конфиденциальной информации. Указом утвержден перечень сведений конфиденциального характера, в котором перечислены шесть видов информации:

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, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации.

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.

Наличие в п. 4 перечня, касающемся профессиональной тайны, слов «и так далее» предполагает его продолжение.

Федеральный закон “Об информации, информационных технологиях и защите информации” в ст. 8 закрепляет перечень сведений, которые не разрешается относить к информации с ограниченным доступом.

Таким образом, *анализ действующего законодательства показывает*, что:

1. Информацией является совокупность формализованных знаний (сообщений, данных) и сведений независимо от формы их представления (Федеральный закон «Об информации …»).

2. Правовой защите подлежит любая информация, (Федеральный закон «Об информации … «).

3. Информация является объектом гражданских прав и имеет собственника.

4. Информация может быть ограниченного доступа, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, и общедоступной, предназначенной для неограниченного круга лиц (Федеральный закон «Об информации … «).

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют степень (уровень) ее конфиденциальности.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

- содержащая государственную тайну (Закон РФ «О государственной тайне» ст. 275, 276, 283, 284 УК РФ);

- передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ, ст. 138 УК РФ); касающаяся тайны усыновления (ст. 155 УК РФ);

- содержащая служебную тайну (ст. 139 ГК РФ), коммерческую тайну (ст. 139 ГК РФ и ст. 183 УК РФ), банковскую тайну (ст. 183 УК РФ), личную тайну (ст. 137 УК РФ), семейную тайну (ст. 137 УК РФ), информация, являющаяся объектом авторских и смежных прав (Гражданский Кодекс РФ, ч. IV).

- информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Федеральный закон «Об информации, информационных технологиях и о защите информации», Закон « О персональных данных», ст. 140 УК РФ) и др.

6. Любая форма завладения и пользования конфиденциальной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является нарушением его прав, т.е. неправомерной.

7. Неправомерное использование информации наказуемо. Нарушение требований закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

8. Документирование не следует считать условием, обязательным для отнесения информации к категории с ограниченным доступом, поскольку в качестве материального носителя могут выступать и *физические поля*, не имеющие реквизитов[1].

Главной чертой настоящего этапа развития информационных отношений в области обеспечения информационной безопасности является переход от ведомственных, преимущественно технократических подходов

[1] Карпычев В.Ю. Основы информационной безопасности: учебное пособие. М.: ГУ НПО «Специальная техника и связь» МВД России, 2001. 174 с.

к защите информационных ресурсов, к комплексному государственному регулированию вопросов защиты информации.

С развитием информационного общества проблемы, связанные с защитой конфиденциальной информации, приобретают все большее значение. Далее мы рассмотрим более подробно некоторые виды конфиденциальной информации, которые закреплены упомянутыми выше нормативными актами.

Коммерческая тайна

В соответствии с Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» информация, составляющая коммерческую тайну, – это научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Иными словами, режим коммерческой тайны вводится в целях сохранения конфиденциальности информации, что позволит ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Законодателем в ст. 5 Федерального закона «О коммерческой тайне» дан также перечень сведений, которые не могут составлять коммерческую тайну и, следовательно, не подлежат засекречиванию.

Режим коммерческой тайны считается введенным после принятия обладателем мер по охране конфиденциальности информации, которые должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Таким образом, меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Коммерческая деятельность организации тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразной информации. В связи с этим возникают следующие вопросы:

• вся ли информация подлежит защите или следует выделять отдельные ее группы?

• если для защиты выделяется определенная группа информации, то какие критерии для этого существуют?

Отвечая на поставленные вопросы, следует подчеркнуть, что защите подлежит не вся информация, а только та, которая представляет ценность для организации. При определении ценности коммерческой информации необходимо руководствоваться такими ее свойствами, как полезность, своевременность и достоверность.

Полезность информации состоит в том, что она создает субъекту выгодные условия для принятия оперативного решения и получения эффективного результата. В свою очередь, полезность информации зависит от своевременного ее получения и доведения до исполнителя. Из-за несвоевременного поступления важных по своему содержанию сведений часто упускается возможность заключить выгодную торговую или иную сделку.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности информации. Причины возникновения недостоверных сведений различны: неправильное восприятие (в силу заблуждения, недостаточного опыта или профессиональных знаний) фактов или умышленное, предпринятое с определенной целью их искажение. Поэтому, как правило, сведения, представляющие коммерческий интерес, а также источник их поступления должны подвергаться перепроверке.

Собственник коммерческой информации на основании совокупности перечисленных критериев определяет ее ценность для своей хозяйственной деятельности и принимает соответствующее оперативное решение.

В зарубежной экономической литературе коммерческая информация рассматривается не в качестве средства извлечения прибыли, а прежде всего условие, способствующее или препятствующего ее получению. Особо подчеркивается наличие стоимостного фактора коммерческой информации, т.е. возможность выступать в качестве предмета купли-продажи. Поэтому важное значение в условиях развития многообразных форм собственности имеет вопрос об определении принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге наличия у него прав на ее защиту.

В совокупности *под служебной или коммерческой тайной* негосударственной организации следует понимать сведения, не являющие-

ся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб ее интересам.

Закон РФ, регламентирующий коммерческую деятельность, предусматривает, что владельцами (собственниками) коммерческой информации могут быть граждане России, граждане иностранных государств, а также объединения граждан – коллективных предпринимателей.

Обширны и направления коммерческой деятельности. Это внутренние и внешние экономические сферы производственной, посреднической, коммерческой, научно-технической, инвестиционной, сервисной деятельности.

Обеспечение защиты государственной тайны не имеет прямого отношения к защите коммерческой тайны. Однако следует указать на некоторые возможные исключения. Под защиту государства может быть взята коммерческая информация, оцененная как особо важная не только для ее собственника, но и для государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимателем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних.

Что касается собственно коммерческой тайны, то она специальной уголовно-правовой и режимной защитой не обладает.

Определение и вопросы гражданско-правовой охраны служебной и коммерческой тайны рассмотрены в статье 139 части первой Гражданского кодекса Российской Федерации, называющейся “Служебная и коммерческая тайна”:

“1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору”.

Подводя итог, можно выделить основные признаки информации, составляющей коммерческую и служебную тайну и подлежащей защите:

• действительная или потенциальная ценность информации в силу не-

известности ее третьим лицам,

• доступ к информации закрыт на законном основании,

• обладатель информации принимает надлежащие меры по ее охране;

Действительная или потенциальная коммерческая ценность информации во многом носит субъективный характер и позволяет предпринимателю ограничивать доступ к практически любым сведениям, используемым в предпринимательской деятельности, за исключением сведений, определяемых нормативно-правовыми актами.

Коммерческая информация, циркулирующая в организации, подразделяется на техническую, организационную, финансовую, рекламную, информацию о спросе-предложении, конкурентах, криминальной обстановке и т.д. Прежде чем принимать меры к защите определенной информации, необходимо ответить на следующие вопросы:

1. Какие сведения не могут составлять коммерческую тайну предприятия и предпринимателя, т.е. какие сведения нельзя скрывать и ограничивать доступ к ним?

2. Какие сведения невыгодно скрывать?

3. Какие сведения подлежат защите?

В соответствии со ст. 5 ФЗ « О коммерческой тайне» режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Этот перечень является исчерпывающим. Он заменил и отменил аналогичный перечень сведений, утвержденный Постановлением Правительства РФ от 5 декабря 1991 г. № 35 (с изменениями и дополнениями от 3 октября 2002 г. № 731). Ранее действовавший перечень тех сведений, которые не могут составлять коммерческую тайну, значительно сужен. Прежде те сведения, которые в обязательном порядке должны были сообщаться в налоговые, финансовые и иные контролирующие органы, не могли относиться к коммерческой тайне. Теперь же они могут быть отнесены к коммерческой тайне, если обладатель этих сведений сделает о том особое указание (см. части 3 и 4 ст. 6 Закона).

Статья 5 Закона перечисляет отдельные категории сведений, которые не могут составлять коммерческую тайну, и заканчивает это перечисление указанием на то, что иные федеральные законы могут определить дополнительные категории сведений, которые не должны составлять коммерческую тайну лиц, осуществляющих предпринимательскую деятельность. В то же время ст. 139 ГК устанавливает, что «сведения, которые не могут составлять служебную или коммерческую тайну, определяются» не только «законом», но и «иными правовыми актами».

Предприятия и лица, занимающиеся предпринимательской деятельностью, руководители государственных и муниципальных предприятий обязаны представлять перечисленные выше сведения по требованию органов власти, управления, контролирующих и правоохранительных органов, других юридических лиц, имеющих на это право в соответствии с законодательством, а также трудового коллектива предприятия.

Можно задаться вопросом о том, кому конкретно предприниматель обязан предъявлять по требованию перечисленные сведения. Исходя из характеристики информации, следует предполагать, что претендовать на это могут в пределах своей компетенции:

- прокурор в порядке надзора и в других случаях, предоставленных ему законом;
- правоохранительные органы по возбужденному уголовному делу;
- налоговые службы (управления);
- аудиторские фирмы (по просьбе самого владельца);
- профсоюзы;

• государственные предприятия (учреждения);
• санэпидемстанции;
• экологические организации;
• коммерческие предприятия и частные лица, вступающие в сделку с организацией.

Данный перечень не является исчерпывающим и может быть продолжен.

Ответ на вопрос о том, какие сведения невыгодно скрывать, касается коммерческой информации, которую невыгодно скрывать самой организации или предпринимателю. Это прежде всего рекламная информация. Без рекламы трудно добиться эффективного результата в хозяйственной деятельности, особенно в условиях жесткой конкуренции. Реклама широко начинает входить в нашу жизнь. Однако широкое распространение рекламы имеет как положительную, так и отрицательную стороны. Рекламная информация становится достоянием не только законопослушных граждан, на которых она и рассчитана, но и преступных элементов. Коммерческая информация, содержащаяся в рекламе в газетах, журналах, по телевидению и радио помогает преступникам определиться с объектом будущего посягательства, изучить его слабые стороны.

Предприниматель, рекламирующий свою деятельность, должен знать, с какими препятствиями он может столкнуться, и как он может их преодолеть в конкретной ситуации. Не является выходом конспирация коммерческой деятельности, как пытаются это делать некоторые фирмы. Очевидно, что обеспечить свою безопасность можно путем применения соответствующих форм, методов и способов защиты.

К группе коммерческих сведений, которые следует защищать, относятся те, которые представляют хозяйственную ценность для предпринимателя, и на которые не распространяется законный доступ третьих лиц, т.е. прежде всего сведения, составляющие коммерческую тайну.

Нарушение закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Следует отметить, что ограничения, вводимые на использование сведений, составляющих коммерческую тайну, направлены на защиту интеллектуальной , материальной, финансовой собственности и других интересов, возникающих при организации трудовой деятельности организации, персонала ее подразделений, а также при их сотрудничестве с работниками других организаций.

Целью таких ограничений является предотвращение разглашения, утечки или несанкционированного доступа к конфиденциальной информации. Ограничения должны быть целесообразными и обоснованными с точки зрения необходимости обеспечения информационной безопасности. Не допускается использование ограничений для сокрытия ошибок и некомпетентности руководства организации, бесхозяйственности, расточительства, недобросовестной конкуренции и других негативных явлений в

Таблица 8.1.

Классификация информации ограниченного доступа

Информация с ограниченным доступом	Нормативные и законодательные акты
Государственная тайна	ФЗ «О государственной тайне», ст. 275, 276, 283, 284 УК Российской Федерации
Конфиденциальная информация	ФЗ «Об информации, информационных технологиях и о защите информации»
Персональные данные	ФЗ «Об информации, информационных технологиях и о защите информации»
Личная и семейная тайна	Ст. 23 Конституции Российской Федерации, ФЗ «Об информации, информационных технологиях и о защите информации», ст. 150 Гражданского кодекса Российской Федерации
Служебная тайна	ст. 139 Гражданского кодекса Российской Федерации, ФЗ «Об информации …»
Служебная информация	Ст. 31 ФЗ «О рынке ценных бумаг»
Коммерческая тайна	ФЗ «О коммерческой тайне», Ст. 139 Гражданского кодекса Российской Федерации
Сведения о сущности изобретения ... (“ноу-хау”)	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна следствия и судопроизводства	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна связи	ФЗ «О связи»
Тайна страхования	Ст. 946 Гражданского кодекса Российской Федерации
Тайна усыновления	Ст. 139 Семейного кодекса Российской Федерации, с. 155 УК Российской Федерации
Тайна исповеди	Ст. 3 ФЗ «О свободе совести и религиозных объединениях»
Банковская тайна	Ст. 857 Гражданского кодекса Российской Федерации, ст. 183 УК Российской Федерации
Нотариальная тайна	Ст. 16, 28 Основ законодательства Российской Федерации о нотариате
Адвокатская тайна	Ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре в РФ»
Врачебная тайна	Ст. 61 Основ законодательства Российской Федерации «Об охране здоровья граждан», ст. 14 закона Российской Федерации «О трансплантации органов и (или) тканей человека»

деятельности организации, а также уклонения от выполнения договорных обязательств и уплаты налогов.

Служебная тайна

Сформулируем критерий разграничения понятий коммерческой и служебной тайны организации. Если основной целью обеспечения конфиденциальности информации, составляющей коммерческую тайну, является обеспечение конкурентного превосходства, то охрана конфиденциальности служебной тайны, хотя и может затрагивать коммерческие интересы организации, главной задачей имеет обеспечение интересов клиентов либо собственных интересов, непосредственно не связанных с коммерческой деятельностью.

Так, к служебной, а не к коммерческой тайне следует отнести сведения, касающиеся мер по обеспечению безопасности сотрудников организации, охране складских и иных помещений и др., прямо не связанные с осуществлением предметной деятельности.

В настоящее время институт служебной тайны в отечественном праве является наименее разработанным. В этой проблеме можно выделить три аспекта[1].

На законодательном уровне требуют урегулирования вопросы «пограничных» и производных сведений. «Пограничная» информация – это такая служебная информация в любой отрасли науки, техники, производства и управления, которая при определенном обобщении и интеграции становится государственной тайной. Производные сведения – служебная информация, полученная в результате дробления сведений, составляющих государственную тайну, на отдельные компоненты, каждый из которых не может к ней отнесен.

Особого правового регулирования требует защита сведений, образующихся в деятельности органов государственной власти и управления. Для формирования административно-правового института служебной тайны следует принять специальный закон, действие которого должно распространяться на все уровни системы государственного управления.

Требует защиты определенная категория значимых сведений субъектов гражданско-правовых отношений. Здесь имеется в виду правовая защита сведений, которые в деятельности организаций не могут быть отнесены к коммерческой тайне несмотря на то, что в ГК РФ понятие служебной тайны напрямую связано с действительной или потенциальной коммерческой ценностью информации.

Следует заметить, что практикуется упрощенный подход, при котором любые сведения о предпринимательской деятельности организации, доступ к которым ограничен, относятся к коммерческой тайне. Однако при таком подходе могут возникнуть трудности в части определения материального ущерба и упущенной выгоды при неправомерном распространении конфиденциальной информации, например, сведений о режиме охраны организации или других аспектах ее функционирования, напрямую не

[1] Фатьянов А. А. Тайна и право. М.: МИФИ, 1999. 299 с.

связанных с осуществлением предметной деятельности. Вместе с тем, указанные сведения необходимо защищать, так как от ограничения доступа к ним в значительной степени зависит коммерческий успех организации.

Профессиональные тайны

Профессиональная тайна как правовой институт чаще всего имеет дело с информацией, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций. При этом в качестве субъекта может выступать как юридическое, так и физическое лицо.

В соответствии с действующим законодательством, к профессиональной тайне относится информация, связанная со служебной деятельностью медицинских работников, нотариусов, адвокатов, частных детективов, священнослужителей, работников банков, ЗАГСов, учреждений страхования. Сохранение в тайне сведений, полученных в связи с выполнением профессиональных функций, вызвано в первую очередь нормами профессиональной этики, а не собственными коммерческими интересами предпринимателя или организации. Соответствующий правовой статус рассматриваемым нормам придает их законодательное закрепление.

Банковская тайна. Понятие банковской тайны, в соответствии с ст. 857 ГК Российской Федерации, охватывает сведения о банковском счете, вкладе, операциях по счету, а также сведения о клиентах банка.

Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

Федеральный закон "О банках и банковской деятельности" определяет обязанности субъектов, категории информации и основания, по которым сведения предоставляются заинтересованным органам государственной власти, организациям и лицам. Кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к банковской тайне любые сведения, за исключением прямо указанных в Законе.

Нотариальная тайна. Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 "Основ законодательства Российской Федерации о нотариате", нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им

известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий, или увольнения, за исключением случаев, предусмотренных Основами.

Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

Врачебная тайна. Согласно ст. 61 "Основ законодательства Российской Федерации об охране здоровья граждан", информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

Адвокатская тайна. Особенностью адвокатской деятельности является возможность получения конфиденциальных сведений как в документированном, так и недокументированном виде.

Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю (ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре в РФ».

Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.

Полученные в ходе оперативно-розыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей. Указанные ограничения не распространяются на орудия преступления, а также на предметы, которые запрещены к обращению или оборот которых ограничен в соответствии с законодательством Российской Федерации.

Аудиторская тайна. Аудиторские организации и индивидуальные аудиторы обязаны хранить тайну об операциях аудируемых лиц и лиц, которым оказывались сопутствующие аудиту услуги.

Аудиторские организации и индивидуальные аудиторы обязаны обеспечивать сохранность сведений и документов, получаемых и (или) составляемых ими при осуществлении аудиторской деятельности, и не вправе передавать указанные сведения и документы или их копии третьим лицам либо разглашать их без письменного согласия организаций и (или) индивидуальных предпринимателей, в отношении которых осуществлялся аудит и оказывались сопутствующие аудиту услуги, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами.

В случае разглашения сведений, составляющих аудиторскую тайну, ау-

диторской организацией, индивидуальным аудитором, уполномоченным федеральным органом, а также иными лицами, получившими доступ к сведениям, составляющим аудиторскую тайну, на основании настоящего Федерального закона и иных нормативных правовых актов Российской Федерации, аудируемое лицо или лицо, которому оказывались сопутствующие аудиту услуги, а также аудиторские организации и индивидуальные аудиторы вправе потребовать от виновного лица возмещения причиненных убытков.

Тайна страхования. Институт страховой тайны во многих отношениях схож с институтом банковской тайны.

Тайну страхования, в соответствии со ст. 946 ГК Российской Федерации, составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц.

За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 ГК.

Согласно ст. 8 закона «Об организации страхового дела в Российской Федерации», в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица – страховые агенты и страховые брокеры.

Кроме того, в соответствии со ст. 33 Закона, должностные лица федерального органа исполнительной власти по надзору за страховой деятельностью не вправе использовать в корыстных целях и разглашать в какой-либо форме сведения, составляющие коммерческую тайну страховщика.

Тайна завещания (ст. 1123 ГК РФ). Нотариус, другое удостоверяющее завещание лицо, переводчик, исполнитель завещания, свидетели, а также гражданин, подписывающий завещание вместо завещателя, не вправе до открытия наследства разглашать сведения, касающиеся содержания завещания, его совершения, изменения или отмены.

В случае нарушения тайны завещания завещатель вправе потребовать компенсацию морального вреда, а также воспользоваться другими способами защиты гражданских прав, предусмотренными настоящим Кодексом.

Тайна связи (ФЗ «О связи»). На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений,

осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами.

Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

Тайна усыновления. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения).

Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка. Согласно ст. 155 УК тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну (судьи, работники местных администраций, органов опеки и попечительства и прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй – все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

Тайна исповеди. Обеспечение тайны исповеди является внутренним делом священника; юридической ответственности за ее разглашение он не несет. Согласно ч. 2. ст. 51 Конституции РФ и ч. 7 ст. 3 ФЗ «О свободе совести и религиозных объединениях», священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Процессуальные тайны

Тайна следствия. Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам (ст. 310 УК «Разглашение данных предварительного расследования»).

К тайне предварительного расследования следует отнести информацию о результатах оценки доказательств, полученных при производстве следственных и иных процессуальных действий, о следственных версиях, о мерах безопасности, принятых в отношении участников уголовного судопроизводства, о данных оперативно-розыскной деятельности, находящейся в распоряжении следователя в соответствии со ст. 89 УПК РФ.

Сведения о ходе предварительного расследования могут быть преданы гласности только с разрешения прокурора, следователя или лица, производящего дознание. Такая информация может касаться как характера производимых следственных действий, так и доказательственной базы, перспектив расследования, круга лиц, участвующих в расследовании. Важно

отметить, законодательно не закреплен перечень сведений, составляющих следственную тайну. Это означает, что прокурор, следователь или лицо, производящее дознание, могут по своему усмотрению устанавливать, какая информация о предварительном расследовании может быть специально охраняемой, а какая – нет.

Тайна совещания судей. Видом профессиональной тайны в соответствии со ст. 298 УПК следует считать тайну совещания судей. Для всех четырех видов существующих в отечественном судопроизводстве процессов предусмотрена определенная процедура обеспечения независимости и объективности вынесения решения по делу. Эта процедура имеет одной из целей запрет на разглашение информации о дискуссиях, суждениях, результатах голосования, которые имели место во время совещания судей. Обеспечение тайны совещания судей устанавливается ст. 193 ГПК России, ст. 70 ФЗ О конституционном суде Российской Федерации, ст. 11 Арбитражного процессуального кодекса Российской Федерации.

Персональные данные

Федеральным законом «О персональных данных» регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Целью Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В России нормы, регулирующие вопросы защиты персональных данных, были впервые включены в Конституцию Российской Федерации 1993 г. Согласно ст. ст. 23 и 24 Конституции, каждый гражданин России имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение , использование и распространение информации о частной жизни лица без его согласия не допускаются.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Конституционное положение о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица является одной из гарантий закрепленного в ст. 23 Конституции права на неприкосновенность частной жизни. Оно призвано защитить частную жизнь,

личную и семейную тайну от какого бы то ни было проникновения в нее со стороны как государственных органов, органов местного самоуправления, так и негосударственных предприятий, учреждений, организаций, а также отдельных граждан.

Особое значение запрет собирать, хранить, использовать и распространять информацию о частной жизни лица приобретает в связи с созданием информационных систем на основе использования средств вычислительной техники и связи, позволяющих накапливать и определенным образом обрабатывать значительные массивы информации.

Можно определить достаточно четкий круг сведений, которые могут быть отнесены к персональным данным. Такими сведениями могут быть:

- идентификационные данные;
- биографические данные;
- личные характеристики;
- сведения о семейном положении;
- сведения о социальном положении;
- сведения о состоянии здоровья;
- особенности половой жизни гражданина и его половая ориентация;
- политические взгляды и религиозные убеждения.

Ряд проблем, связанных с оборотом персональных данных, решен на законодательном уровне. В Уголовный кодекс Российской Федерации введены ст. 137 и 140, устанавливающие ответственность за нарушение неприкосновенности частной жизни. Вместе с тем, следует отметить, что в законодательной базе имеется ряд противоречий и пробелов, которые позволяют произвольно толковать положения закона «Об информации ...» и других нормативных актов.

10.3. Правовые аспекты защиты информации с использованием технических средств

Технико-математические аспекты правового обеспечения представляют совокупность технических средств, математических методов, моделей, алгоритмов и программ, обеспечивающих условия, необходимые для юридического разграничения прав и ответственности относительно регламентов обращения с защищаемой информацией.

При этом основными условиями являются:

1) фиксация на документе персональных идентификаторов («подписей») лиц, изготовивших документ и (или) несущих ответственность за него;

2) фиксация (при любой необходимости) на документе персональных идентификаторов (подписей) лиц, ознакомившихся с содержанием соответствующей информации;

3) фиксация фактов несанкционированного доступа с любой целью к конфиденциальной информации и средствам ее защиты;

4) невозможность незаметного (без оставления следов) изменения содержания информации даже лицами, имеющими к нему санкции на доступ;

5)применение криптографических методов и специальных средств защиты, что позволяет ограничить круг лиц, производящих обработку конфиденциальной информации.

Реализация рассмотренных технико-математических средств защиты информации также требует правового обеспечения. Решение этой задачи осуществляется в рамках существующего информационного законодательства.

Электронная цифровая подпись.

Документ выполняет две основные функции: информационную и доказательственную. С точки зрения информационной безопасности определяющей является доказательственная функция – именно она обеспечивает защиту документа от подделки и фальсификации.

В последнее время значительные массивы данных передаются, обрабатываются и хранятся в электронной форме в автоматизированных информационных системах. Поэтому важное значение имеет определение правового статуса электронного документа с точки зрения возможности его применения наряду с традиционным бумажным документом.

Определение электронного документа в Российском законодательстве впервые введено в Федеральном Законе «Об электронной цифровой подписи». *Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.* Следовательно, к электронному документу предъявляются те же требования , что и к традиционному документу на бумажном носителе. В частности, это касается соблюдения требований, обеспечивающих доказательственную функцию документа, т.е. придающих ему юридическую силу.

Для электронного документа, в силу особой природы машинных носителей информации, неприемлемы такие способы идентификации, как собственноручная подпись лица, печать организации, специальный тип бумаги и т.д. Существует по крайней мере два пути для решения данной проблемы. Первый – уточнить понятие электронного документа с учетом необходимости его преобразования в письменный акт установленной формы. Так, например, электронный документ можно определить как набор данных, записанных в электронно-цифровой форме, для которых выполнено следующее условие: существует признанная участниками и утвержденная процедура, позволяющая однозначно преобразовать эти данные в традиционный документ, причем указанная процедура подтверждена посредством традиционного бумажного документа. В Законе «Об информации» об этом говорится следующим образом: документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

Другой путь – использовать для подтверждения подлинности электронного документа электронную цифровую подпись (ЭЦП). Такая процедура придания юридической силы документу в электронно-цифровой форме была предложена во второй половине 1970-х годов американскими мате-

матиками У. Диффи и М. Хеллмэном.

Возможность использования ЭЦП прописана в Законе «Об информации, информационных технологиях и о защите информации»: электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Электронная цифровая подпись (ЭЦП) – набор знаков и символов для подтверждения подлинности электронных документов. В основе создания и использования ЭЦП лежат математические принципы. В России в 1994 году были приняты государственные стандарты функций, образующих систему ЭЦП: ГОСТ Р 34.11-94 «Функция хэширования» и ГОСТ Р 34.10-94 «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

Первый ГОСТ определяет функцию преобразования конечной последовательности двоичных бит электронного документа в двоичное число фиксированной длины (256 бит). Второй ГОСТ определяет функцию и алгоритм вычисления ЭЦП документа, а также алгоритм проверки подлинности цифровой подписи.

Система ЭЦП содержит три алгоритма:

1. хэширования (преобразование документа в двоичное число оп-ределенной длины);

2. выработки ЭЦП под документом;

3. проверки подписи.

Цифровую подпись практически невозможно подделать. Проверить подлинность подписи может любой участник ЭДО, знающий открытый ключ. Подписанное сообщение можно, не опасаясь фальсификаций, передавать по любым открытым каналам связи. Если сообщение будет искажено, то подпись окажется недействительной.

Цифровая подпись обеспечивает высокий уровень защиты документа от несанкционированных изменений. Единственный ее недостаток, по сравнению с обычной подписью – по ней нельзя определить, кто именно подписал документ. Физические характеристики обычной подписи неповторимы, а о секретном ключе человек может умышленно либо случайно кому-то рассказать, ключ могут подсмотреть или украсть, если его записали. Данное свойство цифровой подписи не является непреодолимым препятствием для ее использования. Достаточно, чтобы каждый из участников электронного документооборота объявил о признании своих обязательств по всем документам, заверенным его цифровой подписью.

Однако для того, чтобы ЭЦП вошла в оборот, необходимо выполнение нескольких важных условий. Во-первых, субъекты гражданского документооборота должны оценить удобство и выгодность ее использования. Во-вторых, способ подтверждения подлинности электронных документов с помощью ЭЦП должен доказать свою надежность на практике. В-третьих, требуется законодательное закрепление следующих положений:

• определения электронно-цифровой подписи;

• возможности и сферы применения электронных документов и цифровой подписи;

• допустимости использования электронных документов в качестве доказательств в суде.

Последние условия были во многом выполнены с принятием Федерального закона «Об электронной цифровой подписи». В частности, ст. 1 данного Закона гласит:

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

В соответствии со ст. 3 закона «электронная 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».

Следует заметить, что попытки разработать ***правовой режим электронного документа*** предпринимались в нашей стране с середины 70-х годов. Приказом № 158 от 29 декабря 1980 г. Государственный комитет СССР по делам изобретений и открытий утвердил положение о всесоюзной магнитно-ленточной службе патентной информации. 20апреля 1981 г. Государственный комитет по науке и технике СССР постановлением №100 утвердил «Временные общеотраслевые руководящие указания о придании юридической силы документам, создаваемым средствами вычислительной техники». При заключении договора об обмене документами на магнитных носителях предписывалось устанавливать дополнительные реквизиты, которые должны были отражаться на бумажных копиях магнитных документов.

Государственный комитет СССР по стандартам 9 октября 1984 г. ввел ГОСТ 6.10.4-84 «Придание юридической силы документам на машинной носителе и машинограмме, создаваемым средствами вычислительной техники». Данный стандарт определял требования к составу и содержанию

реквизитов, придающих юридическую силу документам на машинных носителях информации, создаваемым средствами вычислительной техники. В соответствии с ГОСТом регламентировались следующие положения:

• допускалось «транспортирование (передача, пересылка) документа на магнитном носителе». При этом требовались сопроводительное письмо на бланке с личной подписью, что ставило вне ГОСТа передачу электронных документов по телекоммуникационным каналам;

• перечислялись обязательные реквизиты, т.е. устанавливались требования к форме документа;

• вводилось понятие подлинника, дубликата, копии документа на машинном носителе.

Подлинник определялся как «первая во времени запись документа, содержащая технико-математические аспекты организационно-правового обеспечения, представляющие указания, что этот документ является подлинником». Дубликаты (копии) определялись как более позднее по времени, аутентичные по содержанию записи документа с указанием на то, что эти документы являются дубликатами. С учетом технических средств и способов копирования информации на машинных носителях целесообразнее было бы считать полностью аутентичные копии документа подлинниками, т.е. признать, что электронный документ может иметь сколько угодно много подлинников. Вполне возможна также и ситуация, когда может понадобиться электронная копия электронного документа. Поэтому важным моментом является то, что стандарт признавал за подлинниками, копиями, дубликатами документов на машинном носителе, равно как и за машинограммой (копией электронного документа на бумажном носителе) одинаковую юридическую силу при соблюдении установленных к ним требований.

В ГОСТе был установлен порядок внесения изменений в документы на машинных носителях. Производить изменения разрешалось только организации-создателю документа. Однако ГОСТ не предусматривал никаких средств для проверки того, кто внес изменения в документ, в случае если возникали разногласия в различных его экземплярах.

Широкого применения в гражданском обороте электронные документы тогда не нашли, и тому было несколько причин. Так, необходимость использования вместе с электронным документом сопроводительного письма лишало его основного преимущества – скорости обмена. Но главная причина состояла в экономической нецелесообразности использования ЭДО.

Необходимо, чтобы законодательно было определено, в каких случаях может быть использован электронный документ, заверенный электронно-цифровой подписью. Закон “Об информации, информационных технологиях и о защите информации”, говорит следующее:

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными

нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Принципиально новая ситуация сложилась после принятия закона «Об информации … « и нового Гражданского Кодекса (ГК) РФ. Ряд основных положений закона, касающихся ЭЦП и электронного документа, рассматривался выше.

Таким образом, новый ГК разрешил использование электронных документов, заверенных электронно-цифровой подписью, во всех случаях, когда требуется письменная форма сделки, за исключением тех, при которых установлены специальные требования к форме документа.

Ограничением на использование электронных документов является ситуация, когда для оформлении сделки требуется участие третьих лиц. Для некоторых таких сделок ГК предусматривает их государственную регистрацию.

Еще одна группа ограничений на ЭДО связана с тем, что деятельность по разработке систем ЭЦП подлежит лицензированию. Лицензирование такого рода деятельности связано с шифровальными средствами и предоставлением услуг по шифрованию информации.

Запрещена деятельность юридических и физических лиц в области шифровании информации без лицензии. Государственным организациям запрещено использовать не имеющие сертификата средства криптографической защиты информации.

Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация»?
3. Что выступает в качестве основного объекта правовой защиты информации?
4. В чем заключается двуединство информации с правовой точки зрения?
5. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Что понимается под угрозой безопасности информации?
9. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
10. Какие существуют противоправные действия в отношении компьютерной информации?

11. Какие меры необходимо применять для защиты компьютерной информации?
12. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
13. Назовите основные цели государства в области обеспечения информационной безопасности.
14. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
15. В тексте какого закона приведена классификация средств защиты информации?
16. Какой закон определяет понятие «официального документа»?
17. В тексте какого закона определены нормы, устанавливающие правовой режим информационных ресурсов?
18. Что в соответствии с законодательством понимается под защитой информации?
19. Поясните содержание термина «информационная безопасность».
20. Какой закон определяет понятие электронного документа?
21. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
22. Назовите основные положения Доктрины информационной безопасности Российской Федерации.
23. Что входит в понятие профессиональной тайны?
24. Что представляют собой технико-математические аспекты организационно-правового обеспечения информации?
25. Дайте определение электронного документа.
26. Как можно придать юридическую силу электронному документу?
27. Что представляет собой электронно-цифровая подпись?
28. Какие алгоритмы содержит система электронно-цифровой подписи?
29. Назовите основные условия, необходимые для введения ЭЦП в гражданский документооборот.
30. Каковы основные особенности правового режима электронного документа?
31. Назовите основные ограничения на использование электронных документов.
32. Какие условия необходимо выполнить с целью использования электронного документа в качестве доказательства?
33. Какие задачи в области законодательства следует отнести к первоочередным в области лицензирования и сертификации?
34. Можно ли в использовать несертифицированные средства защиты информации?
35. Рассмотрите структуру основных руководящих документов ФСТЭК РФ в области защиты информации от несанкционированного доступа.

Глава 11. Организационно-технические методы защиты информации в компьютерных системах

Защита информации вызывает необходимость системного подхода, т.е. здесь нельзя ограничиваться отдельными мероприятиями. Системный подход к защите информации требует, чтобы средства и действия, используемые для обеспечения информационной безопасности – *организационные, физические* и *программно-технические* – рассматривались как единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер. Один из основных принципов системного подхода к безопасности информации – принцип «разумной достаточности», суть которого: стопроцентной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы.

11.1. Организационные методы защиты информации

Организационные методы защиты информации состоят из совокупности мероприятий по подбору, проверке и инструктажу персонала; обеспечению программно-технического обслуживания; назначению лиц, ответственных за конкретное оборудование; осуществлению режима секретности; обеспечению физической охраны объектов; оборудованию помещений металлическими дверями, решетками и т.д.

Организационные методы обычно включают в себя три следующие большие составляющие:

- ограничение доступа;
- разграничение доступа;
- контроль доступа.

Ограничение доступа – это создание некоторых замкнутых рубежей вокруг объекта защиты. Доступ любых лиц к объекту осуществляется в контролируемых условиях и лишь для выполнения ими функциональных обязанностей. Ограничение доступа в отношении компьютерной системы заключается в такой организации ее работы, чтобы был исключен доступ к ней посторонних лиц. Для этого в особо ответственных случаях следует разместить компьютеризированное рабочее место в отдельном изолированном помещении. Дверь в это помещение должна быть оборудована механическим или электромеханическим замком. В период длительного отсутствия пользователя системный блок и носители информации могут быть изолированы в сейфе.

Разграничение доступа в компьютерной системе заключается в разделении информации на части и организации доступа к ней в соответствии с функциональными обязанностями и полномочиями пользователя. Задача разграничения доступа состоит в защите информации от нарушителя, который входит в круг лиц, допущенных к работе в компьютерной системе.

При этом деление информации может выполняться в соответствии с различными критериями: по степени важности, секретности, функциональному назначению и т.д. Обычно при организации разграничения доступа следует придерживаться следующих правил: техническое обслуживание оборудования в процессе эксплуатации должно выполняться специальным персоналом без доступа к информации, подлежащей защите; любое изменение программного обеспечения должен выполнять выделенный специально для этой цели специалист.

Контроль доступа – это определение подлинности субъекта и фиксация факта доступа. При этом вначале каждому субъекту, который может быть допущен к информации, присваивается уникальный образ, имя или число.

Присвоение субъекту уникального образа, имени или числа называется *идентификацией.*

Установление подлинности субъекта, то есть процесс проверки, является ли субъект тем, за кого себя выдает, называется *аутентификацией.*

Субъектами идентификации и аутентификации в компьютерной системе могут быть: человек (оператор, пользователь и т.д.), техническое средство (компьютер, устройство), документ. Соответственно, и аутентификация может производиться в отношении человека, технических средств, документов.

При аутентификации человека обычно базируются на антропологических и физиологических данных и используют достаточно устойчивые признаки или их сочетание: отпечатки пальцев и очертание ладоней рук, тембр голоса, личную подпись, рисунок радужной оболочки глаза и т.д. В настоящее время в этом направлении ведутся поиски технических решений и достигнуты определенные успехи. Однако широкого распространения такие методы пока еще не получили.

Наиболее распространенный метод – присвоение пароля и запрос его при входе в систему. При этом для большей надежности пароль может быть разделен, например, на две части: одну из них пользователь вводит вручную, а вторая размещается на специальном носителе (например, магнитной карточке). Еще один метод аутентификации называется «Запрос-ответ». Он заключается в том, что при попытке пользователя включиться в работу ему задаются некоторые вопросы, на которые он должен правильно ответить.

Примером аутентификации технических средств может служить установление подлинности терминала, с которого входит в систему пользователь. Данная процедура может осуществляется также с помощью пароля.

Аутентификация документов применяется для защиты от следующих преднамеренных несанкционированных действий: отказ отправителя от переданного документа; фальсификация (подделка) документа получателем; маскировка отправителя под другого абонента; изменение получателем документа. Обеспечение защиты с каждой стороны, участвующей в обмене, осуществляется с помощью ведения специальных протоколов, одним из элементов которых служит цифровая подпись. Цифровая подпись – это некоторая дополнительная информация, зависящая от передаваемых данных,

имени получателя и некоторой закрытой информации, которой обладает только отправитель. Фактически подпись также является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения.

11.2. Защита информации от потери и разрушения

В настоящем разделе мы рассмотрим преимущественно моменты, связанные с защитой информации на персональном компьютере, не интегрированном в сеть. *Потеря информации* при работе на ПК может про-изойти, например, по следующим причинам:

1. нарушение работы компьютера;
2. отключение или сбои питания;
3. повреждение носителей информации;
4. ошибочные действия пользователя;
5. действие компьютерных вирусов;
6. несанкционированные умышленные действия других лиц.

Защита от компьютерных вирусов и несанкционированного доступа будут рассматриваться в отдельных разделах. Предотвратить причины 1-4 можно *резервированием данных*, что является наиболее общим и простым выходом. Средства резервирования таковы:

• программные средства, входящие в состав большинства комплектов утилит, для создания резервных копий – MS Backup, Norton Backup;

• создание архивов на внешних носителях информации.

Резервирование рекомендуется делать регулярно – раз в день, месяц, после окончания работы с использованием соответствующих программных средств и устройств. Так, для резервирования больших массивов информации по стоимости на единицу хранения наиболее выгодны магнитные ленты. Они также отличаются повышенной надежностью.

В случае потери информации она может быть восстановлена:

1. с использованием резервных данных;
2. без использования резервных данных.

Во втором случае применяются следующие особенности удаления файлов и каталогов:

• при удалении стирается только первая буква в имени файла;

• из FAT стирается информация о занятых секторах (сложности возникают, если файл фрагментирован).

Для успешного восстановления данных необходимо чтобы:

• после удаления файла на освободившееся место не была записана новая информация;

• файл не был фрагментирован (для этого необходимо регулярно выполнять операцию дефрагментации с помощью, например, утилиты Speedisk из пакета Norton Utilites).

Восстановление производится следующими программными средствами:

• Undelete из пакета утилит DOS;

• Unerase из комплекта утилит Norton Utilites.

Если данные представляют особую ценность для пользователя, то можно применять *защиту от уничтожения*:

1. присвоить файлам атрибут Read Only;

2. использовать специальные программные средства для сохранения файлов после удаления его пользователем, имитирующие удаление, например утилиту SmartCan из пакета Norton Utilites. В этом случае при удалении файлы переписываются в скрытый каталог, где и хранятся определенное число дней, которое пользователь может установить сам. Размер каталога ограничен, и при заполнении его наиболее старые файлы стираются и замещаются вновь удаленными.

Необходимо отметить, что большую угрозу для сохранности данных представляют *нарушения в системе подачи питания* – отключение напряжения, всплески и падения напряжения, импульсные помехи и т.д.. Практически полностью избежать потерь информации в таких случаях можно применяя источники бесперебойного питания, на рынке которых лидирует американская фирма APC. Источники бесперебойного питания выпускаются в трех основных модификациях: offline, line-interactive и online. Устройства offline – это недорогие устройства для массового пользователя, устраняющие основные виды сетевых помех и обеспечивающие переход на питание от аккумуляторных батарей при отключении питания. Модификация line-interactive подразумевает устройства, анализирующие параметры входного питания и принимающие решения о переходе на батарейное питание в случае превышения заданных допустимых значений. В устройствах online применяется двойное или тройное преобразование: переменного входного напряжения в постоянное (одно или два) с последующим преобразованием в переменное. Как результат, на выходе получается идеально отфильтрованное питание, полностью безопасное для нагрузки, а при отключении электроэнергии не происходит даже кратковременного перерыва в подаче питания на выход. Устройства очень дороги, поэтому применяются для питания серверов и другого критичного оборудования.

11.3. Защита информации от несанкционированного доступа

Несанкционированный доступ – это чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Проблема несанкционированного доступа к информации обострилась и приобрела особую значимость в связи с развитием компьютерных сетей, прежде всего глобальной сети Интернет. Однако несанкционированный доступ в компьютерные сети имеет ряд характерных особенностей, поэтому его имеет смысл рассматривать отдельно.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.

Для успешной защиты своей информации пользователь должен иметь абсолютно ясное представление о возможных *путях несанкционированного доступа* к компьютерной системе. Перечислим основные типовые пути несанкционированного получения информации:

• хищение носителей информации и производственных отходов;

• копирование носителей информации с преодолением мер защиты;

• маскировка под зарегистрированного пользователя;

• мистификация (маскировка под запросы системы);

• использование недостатков операционных систем и языков программирования;

• использование программных закладок и программных блоков типа "троянский конь";

• перехват электронных излучений;

• перехват акустических излучений;

• дистанционное фотографирование;

• применение подслушивающих устройств;

• злоумышленный вывод из строя механизмов защиты и т.д..

Для защиты информации от несанкционированного доступа применяются:

1. Организационные методы
2. Технические методы;
3. Программные методы;
4. Криптографические методы.

Организационные методы включают в себя:

• пропускной режим;

• хранение носителей и устройств в сейфе (дискеты, монитор, клавиатура и т.д.);

• ограничение доступа лиц в компьютерные помещения и т.д.

Под *техническими методами* защиты информации от НСД понимаются методы, использующие различные технические (аппаратные) средства защиты информации. Технические средства включают в себя:

• фильтры, экраны на аппаратуру;

• ключ для блокировки клавиатуры;

• устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;

• электронные ключи на микросхемах и т.д.

Под *программными методами* защиты информации понимается разработка специального программного обеспечения (программных средств), которое бы не позволяло постороннему человеку, не знакомому с этим видом защиты, получать информацию из системы. Программные средства включают в себя:

• парольный доступ – задание полномочий пользователя;

• блокировка экрана и клавиатуры, например, с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;

• использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т.д.

Одна из простых мер ограничения доступа – использование встроенного пароля, который блокирует загрузку и работу компьютера. Такая защита предусмотрена изготовителями персональных компьютеров. Пароль хранится в специальной памяти – CMOS, работоспособность которой поддерживается за счет энергии встроенного в материнскую плату аккумулятора. Для его изменения следует нажать клавишу Delete (иногда некоторую комбинацию клавиш) после включения питания или перезапуска и удерживать ее до тех пор, пока не высветится специальное окно для работы с CMOS-памятью. Однако следует помнить, что такой пароль может быть нейтрализован перемычками на материнской плате, либо путем изъятия или замыкания аккумулятора. Поэтому такая мера защиты может быть использована с соответствующими ограничениями (например, от нарушителя-непрофессионала).

Под *криптографическими методами* защиты информации подразумевается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. Криптографические методы обеспечивают самую надежную защиту информации от несанкционированного доступа, т.к. если даже произойдет перехват на линиях связи или будет украден машинный носитель, зашифрованная информация все равно не будет доступна преступнику.

Криптографическая защита информации может быть реализована с помощью *методов криптографического преобразования* информации. В зависимости от *вида воздействия на исходную информацию* методы криптографической защиты делят на четыре группы:

• шифрование;
• стеганография;
• кодирование;
• сжатие.

Шифрование заключается в проведениии обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых она представляется хаотическим набором символов – букв, цифр и двоичных кодов. Защита информации методом шифрования заключается в преобразовании ее составных частей с помощью специальных алгоритмов. Алгоритм шифрования может быть известен широкому кругу лиц.

Управление процессом шифрования осуществляется с помощью ключа. Ключ – это секретное состояние некоторых параметров алгоритма преобразования, обеспечивающее выбор одного варианта из всех возможных. Ключ необходимо иметь и для расшифровки информации, чтобы с его помощью преобразовать зашифрованную информацию к исходному виду.

Методы шифрования можно разделить на четыре большие группы: методы перестановки; методы замены; аддитивные методы; комбинирован-

ные методы.

Идея *методов перестановки* состоит в том, что исходная информация (например, текст) делится на блоки, в каждом из которых выполняется перестановка символов. В классическом варианте перестановки получаются в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры. Простейший пример – запись исходного текста по строкам некоторой матрицы и чтение его по столбцам, или наоборот. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Приведем пример метода перестановки.

Исходный текст: «Пример перестановки».

Шифрование: матрица из 5 столбцов. Запись по строкам, чтение по столбцам.

1	2	3	4	5
П	Р	И	М	Е
Р	П	Е	Р	Е
С	Т	А	Н	О
В	К	И	Ъ	Х

Результат кодирования: ПРСВ РПТК ИЕАИ МРНЪ ЕЕОХ

Для методов перестановки характерны простота алгоритма и низкая защищенность, так как при большой длине исходного текста в зашифрованном тексте проявляются статистические закономерности ключа, что позволяет быстро его раскрыть.

Методы замены заключаются в том, что символы исходного текста, записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым ключом преобразования. Одним из простейших методов является прямая замена исходных символов их эквивалентом согласно вектору замен. Для очередного символа исходного текста отыскивается его местоположение в исходном алфавите. Эквивалент из вектора замены выбирается как отстоящий на полученное смещение от начала алфавита.

Аддитивные методы в качестве ключа используют некоторую последовательность того же алфавита и такой же длины, что и в исходном тексте. Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Примером аддитивного метода является гаммирование – наложение на исходный текст некоторой последовательности кодов, называемой гаммой. При этом ключ шифрования может выбираться случайным образом, например, с помощью генератора псевдослучайных чисел.

И, наконец, комбинированные методы – это методы, представляющие собой некоторое сочетание всех вышеописанных. Полученный в результате шифр называется производным шифром.

Одним из наиболее распространенных криптографических стандартов шифрования информации является стандарт DES (Data Encryption

Standard), применяемый в США. Он используется федеральными департаментами и агентствами для защиты всех достаточно важных данных. Стандарт DES применяют многие негосударственные институты, в том числе большинство банков и служб обращения денег. Оговоренный в стандарте алгоритм (комбинированный, использующий перестановки, замены и гаммирование) опубликован для того, чтобы большинство пользователей могли использовать проверенный алгоритм с хорошей криптостойкостью.

Стойкость любого алгоритма шифрования не абсолютна. Это многократно доказано теоретически и практически. Криптостойкость алгоритма DES в современных условиях недостаточна. В США регулярно проводятся конкурсы на вскрытие зашифрованных с его помощью сообщений. Это своего рода соревнование для специалистов и энтузиастов. Так, 19 января 1999 г. зашифрованное с помощью алгоритма DES сообщение было взломано за рекордно короткое время – 22 часа 15 минут. Над взломом трудились около 100 тыс. энтузиастов, которые были объединены распределенной сетью Distributed.Net и использовали специально созданный суперкомпьютер Deep Crack. Скорость перебора составила 245 млрд ключей в секунду.

История взломов алгоритма DES такова: в январе 1997 г. на успешный взлом потребовалось 96 дней, в 1998 г. было проведено два конкурса (в феврале и июле), завершившихся за 41 день и 56 часов. Таким образом, установленный во время предыдущей атаки рекорд превышен более чем вдвое.

Противостояние правительства США и криптографических компаний в основном касается вопроса о достаточной для гарантий безопасности длине ключа, которым шифруется сообщение. В алгоритме DES длина ключа равна 56 битам. Принятый федеральным правительством еще в 1977 г., 56-разрядный DES все еще широко используется финансовыми и другими отраслями промышленности во всем мире, несмотря на имеющиеся основания считать такую длину ключа недостаточной.

В России установлен единый алгоритм криптографического преобразования информации, который определяется ГОСТ 28147-89. Это комбинированный алгоритм, использующий перестановки, замены и гаммирование.

В настоящее время наиболее перспективны алгоритмы шифрования с открытым ключом. В системах с открытым ключом для шифрования данных используется один ключ (открытый), а для расшифровки – другой (закрытый). Открытый ключ не является секретным и может быть опубликован для употребления всеми пользователями системы. Для расшифровки же используется закрытый (секретный) ключ.

Ни один алгоритм шифрования не обладает абсолютной криптостойкостью. На практике этого и не требуется. Главные критерий практической секретности – время, в течение которого можно по перехваченному сообщению получить криптографический ключ. Если время сравнимо с несколькими годами, то для практического использования это вполне приемлемо.

Средства реализации шифрования бывают аппаратные и программные. В серьезных применениях преобладают аппаратные средства. Они облада-

ют следующими преимуществами: высокая скорость; большая защищенность (программу, установленную на компьютере, легче вскрыть); легкая установка на месте (такое средство не требует обычно никакой адаптации).

Основными *видами несанкционированного доступа* к данным являются следующие:

• чтение;

• запись,

и соответственно требуется защита данных:

• от чтения;

• от записи.

Защита данных от чтения автоматически подразумевает и защиту от записи, ибо возможность записи при отсутствии возможности чтения практически бессмысленна.

Защита от чтения осуществляется:

• наиболее просто – на уровне DOS введением атрибута Hidden для файлов;

• наиболее эффективно – шифрованием.

Защита от записи осуществляется:

• установкой атрибута Read Only для файлов;

• запрещением записи на дискету – рычажок или наклейка);

• запрещением записи через установки BIOS – дисковод не установлен.

При защите данных от чтения возникают две основные проблемы:

1. Как надежно зашифровать данные;

2. Как надежно уничтожить данные.

Проблемы надежного уничтожения данных заключаются в следующем:

• при удалении файла информация не стирается полностью;

• даже после форматирования дискеты и диска данные могут быть восстановлены с помощью специальных технических и программных средств по остаточному магнитному полю.

Для надежного удаления используют, например, утилиту Wipeinfo из пакета Norton Utilites. Данные стираются путем выполнения нескольких циклов (не меньше трех) записи на место удаляемых данных случайной последовательности нулей и единиц.

Для шифрования данных можно использовать утилиту Diskreet из пакета Norton Utilites. Используются два метода шифрования:

• быстрый собственный метод;

• медленный стандартный метод.

Для шифрования нужно выбрать требуемые файлы и набрать пароль. Исходные данные уничтожаются. При расшифровке данных используется исходный пароль.

Более общий подход состоит в создании секретного диска. Он создается средствами Diskreet. При введении пароля диск раскрывается и с ним можно работать как с обычным логическим диском. При этом все данные расшифровываются. В любой момент диск можно закрыть, при этом все

данные вновь окажутся зашифрованными.

Для персональных компьютеров созданы программно-аппаратные комплексы, позволяющие шифровать информацию, передаваемую на диски или в порты. Например, программно-аппаратный комплекс «КРИПТОН» представляет собой электронную плату с программным обеспечением, устанавливаемую в свободный слот компьютера. Комплекс позволяет: обеспечить секретность информации на жестком диске; разграничить доступ к информации; защитить компьютер от несанкционированного включения; проверить целостность программ в момент запуска; запретить запуск посторонних программ.

На практике обычно используются комбинированные способы защиты информации от несанкционированного доступа.

11.4. Защита информации от компьютерных вирусов

Очевидна аналогия понятий компьютерного и биологического вирусов.

Компьютерным вирусом называется способная к самовоспроизводству и размножению программа.

Однако не всякая могущая саморазмножаться программа является компьютерным вирусом. С программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к другим программам (“заражать” их). При запуске последних вирус может выполнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), модификацию и уничтожение данных, переполнение машинной памяти, создание помех в работе ЭВМ и т.п. Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий.

После того как вирус выполнит нужные ему действия, он передает управление той зараженной программе, в которой он находится в момент ее запуска, и она работает также как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Исторически появление компьютерных вирусов связано с идеей создания самовоспроизводящихся механизмов, в частности программ, которая возникла в 50-х гг. Джон фон Нейман еще в 1951 г. предложил метод создания таких механизмов, и его соображения получили дальнейшее развитие в работах других исследователей. Первыми появились игровые программы, использующие элементы будущей вирусной технологии, а затем уже на базе накопленных научных и практических результатов некоторые лица стали разрабатывать самовоспроизводящиеся программы с целью нанесения ущерба пользователям компьютера.

Первые случаи массового заражения ПК вирусами были отмечены в 1987 г., когда появился так называемый Пакистанский вирус, созданный братьями Амджатом и Базитом Алви. Таким образом они решили наказать американцев, покупавших дешевые незаконные копии программного

обеспечения в Пакистане, которые братья стали инфицировать разработанным вирусом. Вирус заразил в США более 18 тыс. компьютеров и, проделав кругосветное путешествие, попал в тогда СССР. Следующим широко известным вирусом стал вирус Lehigh (Лехайский вирус), распространившийся в одноименном университете США. В течение нескольких недель он уничтожил содержимое нескольких сот дискет из библиотеки вычислительного цента университета и личных дискет студентов. К февралю 1989 года в США этим вирусом было поражено около 4 тысяч ПК.

Вирусы *всегда наносят ущерб* – они препятствуют нормальной работе ПК, разрушают файловую структуру и т.д., поэтому их относят к разряду так называемых вредоносных программ. Многие разновидности вирусов устроены так, что при запуске зараженной программы *вирус остается резидентно* в оперативной памяти, вследствие чего до перезагрузки операционной системы он время от времени заражает программы и выполняет вредные действия на компьютере.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Многие резидентные вирусы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают сведения о них в исходном (неискаженном) виде. Разумеется, этот эффект наблюдается только на зараженном компьютере – на «чистом» компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения – модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью программ-дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, затрудняет нахождение таких вирусов программами-детекторами.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски – испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по локальной сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

• общие средства защиты информации – страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

• профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

• специализированные программы для защиты от вирусов.

Общие средства защиты информации необходимы не только для защиты от вирусов. Имеются две основные разновидности этих средств:

• средства резервного копирования информации – создание копий файлов и системных областей дисков;

• средства разграничения доступа – предотвращают несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами, а также ошибочные действия пользователей.

Несмотря на то, что общие средства защиты информации очень важны, их одних для защиты от вирусов все же недостаточно. Поэтому для защиты от вирусов необходимо применение специализированных программ.

В настоящие время имеется большое количество антивирусных средств. Однако все они не обладают свойствами универсальности: каждое рассчитано на конкретные вирусы, либо перекрывает некоторые каналы заражения ПК или распространения вирусов. В связи с этим перспективной областью исследований можно считать применение методов искусственного интеллекта к проблеме создания антивирусных средств.

Антивирусным средством называют программный продукт, выполняющий одну или несколько из следующих функций:

1. защиту файловой структуры от разрушения;
2. обнаружение вирусов;
3. нейтрализацию вирусов.

Антивирусные программы можно разделить на несколько видов: де-

текторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Детектором называется программа, осуществляющая поиск вирусов как на внешних носителях информации, так и в ОЗУ. Результатом работы детектора является список инфицированных файлов и/или областей, возможно, с указанием конкретных вирусов, их заразивших.

Детекторы делятся на универсальные и специализированные. *Универсальные детекторы* проверяют целостность файлов путем подсчета их контрольной суммы и ее сравнения с эталоном. Эталон либо указывается в документации на программный продукт, либо может быть определен в самом начале его эксплуатации.

Специализированные детекторы настроены на конкретные вирусы, один или несколько. Если детектор способен обнаруживать несколько различных вирусов, то его называют *полидетектором*. Работа специализированного детектора основывается на поиске строки кода, принадлежащей тому или иному вирусу, возможно заданной регулярным выражением. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение.

Детектор не способен обнаружить все возможные вирусы. Следует особо подчеркнуть, что программы-детекторы могут выявлять только те вирусы, которые им известны. Некоторые программы-детекторы могут настраиваться на новые типы вирусов, для этого им лишь необходимо указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Очевидно поэтому, что из того, что программа не опознается детекторами как зараженная, не следует, что она здорова – в ней может находиться какой-нибудь новый вирус или даже слегка модифицированная версия старого вируса, неизвестные детекторам.

Многие программы-детекторы не умеют обнаруживать заражение «невидимыми» вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции операционной системы, которые перехватываются вирусом. Ряд детекторов пытается выявить вирус путем просмотра оперативной памяти, но против некоторых «хитрых» вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке ОС с «чистой», защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с загрузочной дискеты.

Некоторые детекторы умеют ловить «невидимые» вирусы, даже когда они активны. Для этого они читают диск, не используя команды ОС. Правда, этот метод работает не на всех дисководах.

Большинство программ-детекторов имеют функцию «доктора» или фага, т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние. ***Дезинфектором*** *(доктором, фагом)* называется программа, осуществляющая удаление вируса как с восстановлением, так

и без восстановления среды обитания.

Ряд вирусов искажает среду обитания таким образом, что ее исходное состояние не может быть восстановлено. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются программой-фагом.

Наиболее известными полидетекторами-фагами являются программные пакеты Antiviral Toolkit Pro Евгения Касперского и DrWeb фирмы «ДиалогНаука». Большинство программ-докторов умеют «лечить» только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов. К таким программам относится, например, AVSP фирмы «ДиалогНаука».

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

Многие программы-ревизоры являются довольно «интеллектуальными» – они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать заражение «невидимыми» вирусами, если такой вирус активен в памяти компьютера. Но некоторые программы-ревизоры, например ADinf фирмы «ДиалогНаука», все же умеют делать и это, не используя вызовы операционной системы для чтения диска (правда, она работают не на всех дисководах). Другие программы часто используют различные полумеры – пытаются обнаружить вирус в оперативной памяти, требуют вызова из первой строки файла AUTOEXEC.BAT, надеясь работать на «чистом» компьютере, и т.д. Увы, против некоторых «хитрых» вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизо-

ры проверяют длину файла. Но одна такая проверка недостаточна – некоторые вирусы не изменяют длину зараженных файлов. Более надежная проверка – прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. *доктора-ревизоры*. Это такие программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но даже такие программы, как доктора-ревизоры, могут лечить не от всех вирусов, а только от тех, которые используют «стандартные», известные на момент написания программы, механизмы заражения файлов.

Вирус-фильтром *(монитором, сторожем)* называется резидентная программа, обеспечивающая контроль выполнения характерных для вирусов действий и требующая от пользователя подтверждения на производство действий. Контроль осуществляется путем подмены обработчиков соответствующих прерываний. В качестве контролируемых действий могут выступать:

- обновление программных файлов;
- прямая запись на диск (по физическому адресу);
- форматирование диска;
- резидентное размещение программы в ОЗУ.

Программы-фильтры располагаются резидентно в оперативной памяти компьютера, перехватывают обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-мониторы не отслеживают подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера. Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Иммунизатором *(вакциной)* называют программу, предотвращающую заражение среды обитания или памяти конкретными вирусами. Иммунизаторы решают проблему нейтрализации вируса не посредством его уничтожения, а путем блокирования его способности к размножению.

Программы-вакцины или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или

диски уже зараженными. Эти программы малоэффективны, поэтому в настоящее время практически не используются.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, «эшелонированная» оборона. Опишем структуру этой обороны. Это неформальное описание позволит лучше понять методику применения антивирусных средств.

Средствам разведки в «обороне» от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны – это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

В «стратегическом резерве» находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать четыре правила:

1. Прежде всего не надо торопиться и принимать опрометчивых решений. Непродуманные действия могут привести не только к потере части файлов, но к повторному заражению компьютера.

2. Надо немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.

3. Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС (обязательное правило).

4. Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь более опытных коллег.

При защите от компьютерных вирусов как никогда важна комплексность проводимых мероприятий как организационного, так и технического характера. На переднем ее крае “обороны” целесообразно разместить средства защиты данных от разрушения, за ними – средства обнаружения вирусов и, наконец, средства нейтрализации вирусов.

Средства защиты данных от возможной потери и разрушения должны использоваться всегда и регулярно. Дополнительно к этому следует придерживаться следующих рекомендаций организационного характера, чтобы избавиться от заражения вирусами:

• гибкие диски использовать всегда, когда это возможно, с заклеенной прорезью защиты от записи;

• без крайней необходимости не пользоваться неизвестными дискетами;

• не передавать свои дискеты другим лицам;

• не запускать на выполнение программы, назначение которых не понятно;

• использовать только лицензионные программные продукты;

• ограничить доступ к ПК посторонних лиц.

При необходимости использования программного продукта, полученного из неизвестного источника, рекомендуется:

• протестировать программный продукт специализированными детекторами на предмет наличия известных вирусов. Нежелательно размещать детекторы на жестком диске – для этого нужно использовать защищенную от записи дискету;

• осуществить резервирование файлов нового программного продукта;

• провести резервирование тех своих файлов, наличие которых требуется для работы нового программного обеспечения;

• организовать опытную эксплуатацию нового программного продукта на фоне вирус-фильтра с обдуманными ответами на его сообщения.

Защита от компьютерных вирусов должна стать частью комплекса мер по защите информации как в отдельных компьютерах, так и в автоматизированных информационных системах в целом.

11.5. Обеспечение защиты информации в компьютерных сетях

Опасность злоумышленных несанкционированных действий над информацией приняла особенно угрожающий характер с развитием компьютерных сетей. Большинство систем обработки информации создавалось как обособленные объекты: рабочие станции, ЛВС, большие универсальные компьютеры и т.д. Каждая система использует свою рабочую платформу (Windows, Linux), а также разные сетевые протоколы (TCP/IP). Сложная организация сетей создает благоприятные предпосылки для совершения различного рода правонарушений, связанных с несанкционированным доступом к конфиденциальной информации. Большинство операционных систем, как автономных, так и сетевых, не содержат надежных механизмов защиты информации.

Следствием опасности сетевых систем стали постоянно увеличивающиеся расходы и усилия на защиту информации, доступ к которой можно осуществить через сетевые каналы связи. Сохранить целостность данных можно только при условии принятия специальных мер контроля доступа к данным и шифрования передаваемой информации. Разные системы нуждаются в разных степенях защиты. Актуальной стала задача объединения систем с различными степенями защищенности (например, на платформах Unix и Windows).

Необходимо иметь четкое представление о возможных каналах утечки информации и путях несанкционированного доступа к защищаемой информации. Только в этом случае возможно построение эффективных механизмов защиты информации в компьютерных сетях[1].

[1] Локальные вычислительные сети: справочник: в 3-х кн. / под ред. С.В. Назарова. М.: Фи-

Угрозы безопасности сети

Пути утечки информации и несанкционированного доступа в компьютерных сетях в основной своей массе совпадают с таковыми в автономных системах (см. выше). Дополнительные возможности возникают за счет существования каналов связи и возможности удаленного доступа к информации. К ним относятся:

- электромагнитная подсветка линий связи;
- незаконное подключение к линиям связи;
- дистанционное преодоление систем защиты;
- ошибки в коммутации каналов;
- нарушение работы линий связи и сетевого оборудования.

Вопросы безопасности сетей решаются в рамках архитектуры безопасности, в структуре которой различают:

- угрозы безопасности;
- службы (услуги) безопасности;
- механизмы обеспечения безопасности.

Под *угрозой безопасности* понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Угрозы принято делить на:

1. непреднамеренные, или случайные;
2. умышленные.

Случайные угрозы возникают как результат ошибок в программном обеспечении, выхода из строя аппаратных средств, неправильных действий пользователей или администратора сети и т.п.

Умышленные угрозы преследуют цель нанесения ущерба пользователям и абонентам сети и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы направлены на несанкционированное использование информационных ресурсов сети, но при этом не оказывают влияния на ее функционирование. Примером пассивной угрозы является получение информации, циркулирующей в каналах сети, посредством прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования сети *посредством целенаправленного воздействия* на ее аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы, искажение сведений в пользовательских базах данных или системной информации и т.п.

К основным угрозам безопасности информации в сети относятся:

- раскрытие конфиденциальной информации;
- компроментация информации;

нансы и статистика, 1994. Кн. 1: Принципы построения, архитектура, коммуникационные средства. 208 с.

• несанкционированный обмен информацией;
• отказ от информации;
• отказ в обслуживании;
• несанкционированное использование ресурсов сети;
• ошибочное использование ресурсов сети.

Угрозы раскрытия конфиденциальной информации реализуются путем несанкционированного доступа к базам данных.

Компрометация информации реализуется посредством внесения несанкционированных изменений в базы данных.

Несанкционированное использование ресурсов сети является средством раскрытия или компрометации информации, а также наносит ущерб пользователям и администрации сети.

Ошибочное использование ресурсов является следствием ошибок, имеющихся в программном обеспечении ЛВС.

Несанкционированный обмен информацией между абонентами сети дает возможность получать сведения, доступ к которым запрещен, т.е., по сути, приводит к раскрытию информации.

Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки.

Отказ в обслуживании представляет собой весьма распространенную угрозу, источником которой является сама сеть. Подобный отказ особенно опасен в случаях, когда задержка с предоставлением ресурсов сети может привести к тяжелым для абонента последствиям.

Службы безопасности сети

Службы безопасности сети указывают направления нейтрализации возможных угроз безопасности. Службы безопасности находят свою практическую реализацию в различных механизмах безопасности. Одна и та же служба безопасности может быть реализована с использованием разных механизмов безопасности или их совокупности.

Различия в составе и особенностях служб безопасности. Протоколы информационного обмена в сетях делятся на две большие группы: типа *виртуального соединения* и *дейтаграммные*, в соответствии с которыми сети также принято делить на *виртуальные* и *дейтаграммные.*

В первых, виртуальных, передача информации между абонентами организуется по так называемому *виртуальному каналу* и происходит в три этапа: создание канала (соединение), собственно передача, уничтожение канала (разъединение). Сообщения разбиваются на блоки, которые передаются в порядке их следования в сообщении.

В дейтаграммных сетях пакеты (*дейтаграммы*) сообщения передаются от отправителя к получателю независимо друг от друга по различным маршрутам, в связи с чем порядок доставки пакетов может не соответствовать порядку их следования в сообщении. Виртуальная сеть в концептуальном плане реализует принцип организации телефонной связи, тогда как дейтаграммная – почтовой.

Международная организация стандартизации (МОС) определяет следующие службы безопасности:

1. аутентификация (подтверждение подлинности);
2. обеспечение целостности;
3. засекречивание данных;
4. контроль доступа;
5. защита от отказов.

Две последние службы едины для дейтаграммных и виртуальных сетей. Первые три характеризуются определенными отличиями, обусловленными особенностями используемых в сетях протоколов.

Служба аутентификации. Данная служба применительно к виртуальным сетям называется *службой аутентификации объекта (одноуровневого)* и обеспечивает подтверждение того факта, что отправитель информации является именно тем, за кого он себя выдает. Применительно к дейтаграммным сетям служба аутентификации называется *службой аутентификации источника данных.*

Службы целостности. Под *целостностью* понимается точное соответствие отправленных и полученных данных между собой. Службы целостности для рассматриваемых сетей выглядят следующим образом:

виртуальные сети:

• служба целостности соединения с восстановлением;
• служба целостности соединения без восстановления;
• служба целостности выборочных полей соединения;

дейтаграммные сети:

• служба целостности без соединения;
• служба целостности выборочных полей без соединения.

Под *полями* понимаются отдельные определенные элементы блоков или пакетов передаваемых данных. Под восстановлением понимаются процедуры восстановления данных, уничтоженных или потерянных в результате обнаружения искажений, вставок или повторов в блоках или дейтаграммах. В службах целостности дейтаграммных сетей наличие процедур восстановления не предусматривается.

Службы засекречивания данных:

• *служба засекречивания соединения* – обеспечивает секретность всех данных, пересылаемых объектами по виртуальному каналу;

• *служба засекречивания без соединения* – обеспечивает секретность данных, содержащихся в каждой отдельной дейтаграмме;

• служба засекречивания отдельных полей соединения;

• служба засекречивания трафика – нейтрализует возможность получения сведений об абонентах сети и характере использования сети.

Механизмы безопасности

Среди механизмов безопасности сетей, предусмотренных МОС, обычно выделяют следующие *основные:*

• шифрование;

• контроль доступа;
• цифровая подпись.

Шифрование применяется для реализации служб засекречивания и используется в ряде других служб.

Механизмы контроля доступа обеспечивают реализацию одноименной службы безопасности, осуществляют проверку полномочий объектов сети, т.е. программ и пользователей, на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется в точке инициализации связи, в промежуточных точках, а также в конечной точке.

Механизмы контроля доступа делятся на *две основные группы:*

• *аутентификация объектов,* требующих ресурса, с последующей проверкой допустимости доступа, для которой используется специальная информационная база контроля доступа;

• *использование меток безопасности,* связываемых с объектами; наличие у объекта соответствующего мандата дает право на доступ к ресурсу.

Самым распространенным и одновременно самым ненадежным методом аутентификации является *парольный доступ.* Более совершенными являются пластиковые карточки и электронные жетоны. Наиболее надежными считаются методы аутентификации по особым приметам личности, так называемые *биометрические методы.*

Цифровая подпись используется для реализации *служб аутентификации и защиты от отказов.* По своей сути она призвана служить электронным аналогом реквизита «подпись», используемого на бумажных документах. Механизм цифровой подписи базируется на использовании способа шифрования с открытым ключом. Знание соответствующего открытого ключа дает возможность получателю электронного сообщения однозначно опознать его отправителя.

Дополнительными механизмами безопасности являются следующие:

• обеспечение целостности данных;
• аутентификация;
• подстановка трафика;
• управление маршрутизацией;
• арбитраж.

Механизмы обеспечения целостности данных направлены на реализацию одноименной службы как применительно к отдельному блоку данных, так и к потоку данных. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Возможны и более простые методы контроля целостности потока данных, например нумерация блоков, дополнение их меткой времени и т.д.

Механизмы обеспечения аутентификации используются для реализации одноименной службы, при этом различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов одного уровня проверяет подлинность другого, тогда как во втором проверка является взаимной. На практике механизмы аутентификации,

как правило, совмещаются с контролем доступа, шифрованием, цифровой подписью и арбитражем.

Механизмы подстановки трафика используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами сети фиктивных блоков, их шифровании и организации их передачи по каналам сети.

Механизмы управления маршрутизацией используются для реализации служб засекречивания. Эти механизмы обеспечивают выбор маршрутов движения информации по сети.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами сети, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтвердить упомянутые характеристики. В общем случае *для реализации одной службы безопасности может использоваться комбинация нескольких механизмов безопасности.*

Защита сетевых операционных систем

Операционная система и аппаратных средства сети обеспечивают защиту ресурсов сети, одним из которых является сама ОС, т.е. входящие в нее программы и системная информация. Поэтому в сетевой ОС ЛВС должны быть так или иначе реализованы механизмы безопасности.

Принято различать:

• пассивные объекты защиты (файлы, прикладные программы, терминалы, области оперативной памяти и т.п.);

• активные субъекты (процессы), которые могут выполнять над объектами определенные операции.

Защита объектов реализуется операционной системой посредством контроля за выполнением субъектами совокупности правил, регламентирующих указанные операции. Указанную совокупность иногда называют *статусом защиты.* Операции, которые могут выполняться над защищенными объектами, принято называть *правами доступа,* а права доступа субъекта по отношению к конкретному объекту – *возможностями.* В качестве *формальной модели статуса защиты* в ОС чаще всего используется так называемая *матрица контроля доступа.*

Достаточно простым в реализации средством разграничения доступа к защищаемым объектам является *механизм колец безопасности.*

Защита файлов в ОС организована следующим образом. С каждым файлом связывается множество *прав доступа:* чтение, обновление и (или) выполнение (для исполняемых файлов). Владелец файла, т.е. создавшее его лицо, пользуется но отношению к файлу всеми правами. Часть этих прав он может передать членам группы –лицам, которым он доверяет сведения, имеющиеся в файле.

Доступ к ресурсам ОС чаще всего ограничен средствами защиты по паролям. Пароль может быть использован и в качестве ключа для шифрования-дешифрования информации в пользовательских файлах. Сами па-

роли также хранятся в зашифрованном виде, что затрудняет их выявление и использование злоумышленниками. Пароль может быть изменен пользователем, администратором системы либо самой системой по истечении установленного интервала времени.

Защита распределенных баз данных

Обеспечение безопасности распределенных баз данных (РБД) косвенно реализуется сетевой ОС. Однако все указанные механизмы и средства инвариантны конкретным способам представления информации в БД. Подобная инвариантность приводит к тому, что в случае непринятия специальных мер все пользователи СУБД имеют равные права по использованию и обновлению всей информации, имеющейся в базе данных. В тоже время указанная информация, как и при ее неавтоматизированном накоплении и использовании, должна быть разбита на категории по грифу секретности, группам пользователей, которым она доступна, а также по операциям над нею, которые разрешены указанным группам. Реализация этого процесса требует разработки и включения в состав СУБД специальных механизмов защиты.

Принятие решения о доступе к той или иной информации, имеющейся в РБД, может зависеть от следующих факторов:

- времени и точки доступа;
- наличия в БД определенных сведений;
- текучесть состояния СУБД;
- полномочий пользователя;
- предыстории обращения к данным.

В первом случае доступ к БД с каждог о терминала ЛВС может быть ограничен некоторым фиксированным отрезком времени.

Во втором случае пользователь может получить из БД интересующие его сведения только при условии, что база данных содержит некоторую взаимосвязанную с ними информацию определенного содержания.

В третьем случае обновление информации в некоторой БД может быть разрешено пользователю только в те моменты времени, когда она не обновляется другими пользователями.

В четвертом случае для каждого пользователя прикладной программы устанавливаются индивидуальные права на доступ к различным элементам базы данных. Эти нрава регламентируют операции, которые пользователь может выполнять над указанными элементами. Например, пользователю может быть разрешен отбор элементов БД, содержащих информацию о товарах, предлагаемых на бирже, но запрещено обновление этих сведений.

В основе ***пятого*** из перечисленных факторов лежит то обстоятельство, что интересующую его информацию пользователь может получить не непосредственным отбором тех или иных элементов БД, а косвенным путем, т.е. посредством анализа и сопоставления ответов СУБД на последовательно вводимые запросы (команды на обновление данных). В связи с этим для обеспечения безопасности информации в БД в общем случае необходимо учитывать предысторию обращения к данным.

11.6. Организация защиты информации в автоматизированных информационных системах

Обеспечение безопасности информации в крупных **автоматизированных системах** является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить.

Объектом защиты в современных АИС выступает территориально распределенная гетерогенная сеть со сложной структурой, предназначенная для распределенной обработки данных, которая часто называется ***корпоративной сетью***. Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных.

Решение проблем безопасности АИС заключается в построении целостной системы защиты информации. При этом защита от физических угроз, например доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов **политики безопасности**, решение которых обеспечит надежное и бесперебойное функционирование информационной системы. Главными этапами построения политики безопасности являются следующие:

• обследование информационной системы на предмет установления ее организационной и информационной структуры и угроз безопасности информации;

• выбор и установка средств защиты;

• подготовка персонала работе со средствами защиты;

• организация обслуживания по вопросам информационной безопасности;

• создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается **Концепция информационной безопасности ИС**, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

• организация сети организации;

• существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;

• организация хранения информации в ИС;

• организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);

• регламентация допуска персонала к той или иной информации;

• ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается **схема безопасности**, структура которой должна удовлетворять следующим условиям:

1. Защита от несанкционированного проникновения в корпоративную

сеть и возможности утечки информации по каналам связи.

2. Разграничение потоков информации между сегментами сети.

3. Защита критичных ресурсов сети.

4. Защита рабочих мест и ресурсов от несанкционированного доступа (НСД).

5. Криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10 – 15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Защита от несанкционированного проникновения и утечки информации

Основным источником угрозы несанкционированного проникновения в АИС является канал подключения к внешней сети, например, к Интернет. Вероятность реализации угрозы зависит от множества факторов, поэтому говорить о едином способе защиты в каждом конкретном случае не представляется возможным. Распространенным вариантом защиты является применение **межсетевых экранов** или **брандмауэров**.

Брандмауэр – *барьер между двумя сетями: внутренней и внешней, обеспечивает прохождение входящих и исходящих пакетов в соответствии с правилами, определенными администратором сети.* Брандмауэр устанавливается у входа в корпоративную сеть и все коммуникации проходят через него. Возможности межсетевых экранов позволяют определить и реализовать правила разграничения доступа как для внешних, так и для внутренних пользователей корпоративной сети, скрыть, при необходимости, структуру сети от внешнего пользователя, блокировать отправку информации по «запретным» адресам, контролировать использование сети и т.д. Вход в корпоративную сеть становится узким местом, прежде всего для злоумышленника.

Выбор брандмауэров достаточно широк. В качестве рекомендации необходимо отметить, что желательно ориентироваться на продукты, сертифицированные Гостехкомиссией России. Несмотря на более высокую стоимость (сертифицированный экран стоит в среднем на 10-15% дороже несертифицированного), применение сертифицированных межсетевых экранов дает ряд преимуществ в решении юридических аспектов организации защиты конфиденциальной информации, а также некоторую гарантию качества реализации защитных механизмов в соответствии с руководящими документами, действующими в нашей стране.

Разграничение потоков информации между сегментами сети

В зависимости от характера информации, обрабатываемой в том или

ином сегменте сети, и от способа взаимодействия между сегментами реализуют один из следующих вариантов.

В первом варианте не устанавливается никакого разграничения информационных потоков, т.е. защита практически отсутствует. Такой вариант оправдан в случаях, когда ни в одном из взаимодействующих сегментов не хранится и не обрабатывается критичная информация или когда сегменты сетевой информационной системы содержат информацию одинаковой важности и находятся в одном здании, в пределах контролируемой зоны.

Во втором варианте разграничение достигается средствами коммуникационного оборудования (маршрутизаторы, переключатели и т.п.). Такое разграничение не позволяет реализовать защитные функции в полном объеме поскольку, во-первых, коммуникационное оборудование изначально не рассматривается как средство защиты и, во-вторых, требуется детальное представление о структуры сети и циркулирующих в ней информационных потоков.

В третьем варианте предполагается применение брандмауэров. Данный способ применяется, как правило, при организации взаимодействия между сегментами через сеть Интернет, когда уже установлены брандмауэры, предназначенные для контроля за потоками информации между информационной системой и сетью Интернет.

Защита критичных ресурсов АИС

Наиболее критичными ресурсами корпоративной сети являются серверы, а основным способом вмешательства в нормальный процесс их функционирования является проведение атак с использованием уязвимых мест в аппаратном и программном обеспечении. Атака может быть реализована как из внешней сети, так и из внутренней. Основная задача заключается не столько в своевременном обнаружении и регистрации атаки, сколько в противодействии ей.

Наиболее мощными инструментами защиты, предназначенными для оперативного реагирования на подобные нападения, являются специальные системы, наподобие системы RealSecure, производимой американской корпорацией Internet Security Systems, Inc., которые позволяют своевременно обнаружить и предотвратить наиболее известные атаки, проводимые по сети.

Защита рабочих мест и ресурсов от НСД

До настоящего времени большинство автоматизированных систем ориентируется только на *встроенные защитные механизмы сетевых операционных систем*. При правильном администрировании такие механизмы обеспечивают достаточную защиту информации на серверах корпоративной сети.

Однако обработка информации, подлежащей защите, производится рабочих станциях, подавляющее большинство которых (более 90%) работает под управлением ОС Windows и не имеет средств обеспечения безопасности, так как эти операционные системы не содержат встроенных механизмов защиты. Как следствие, на незащищенном рабочем месте может обрабатываться критичная информация, доступ к которой ничем не ограничен.

Для рабочих станций рекомендуется применять дополнительные средства защиты, часть из которых описана в предыдущем разделе.

Криптографическая защита информационных ресурсов

Шифрование является одним из самых надежных способов защиты данных от несанкционированного ознакомления. Особенностью применения подобных средств в России является жесткая законодательная регламентация. Для защиты конфиденциальной информации разрешается применять только сертифицированные продукты. В настоящее время в корпоративных сетях они устанавливаются только на тех рабочих местах, где хранится информация, имеющая очень высокую степень важности.

Этапы построения политики безопасности

По окончании работ ***первого этапа*** – обследования информационной системы – необходимо иметь полное представление о том, в каком состоянии находится корпоративная сеть и о том, что нужно сделать, чтобы обеспечить в ней защиту информации.

На основе данных обследования можно перейти ко ***второму этапу*** – выбору, приобретению, установке, настройке и эксплуатации систем защиты в соответствии с разработанными рекомендациями.

Любое средство защиты создает дополнительные неудобства в работе пользователя, при этом препятствий тем больше, чем меньше времени уделяется настройке систем защиты. Администратор безопасности должен ежедневно обрабатывать данные регистрации, чтобы своевременно корректировать настройки, обеспечивающие адаптацию к изменениям в технологии обработки информации. Без этого любая система защиты, какой бы хорошей она ни была, обречена на медленное вымирание.

Третий этап – обучение администраторов безопасности работе со средствами защиты. В процессе обучения администратор получает базовые знания о технологии обеспечения информационной безопасности, об имеющихся в операционных системах подсистемах безопасности и о возможностях систем защиты, о технологических приемах, используемых при их настройке и эксплуатации.

Четвертый этап – информационное обслуживание по вопросам безопасности. Наличие своевременной информации об уязвимых местах и способах защиты способствует принятию адекватных мер обеспечения безопасности. Источники подобных сведений – книги, журналы, Web-серверы и т.п. Однако администратор безопасности не всегда имеет достаточное количество времени для поиска необходимых сведений в этом море информации. Поэтому при выборе системы защиты необходимо учитывать возможности обеспечения последующей информационной поддержки.

Пятый этап – периодический аудит системы информационной безопасности. Корпоративная сеть является постоянно изменяющейся структурой: появляются новые серверы и рабочие станции, меняется программное обеспечение и его настройки, состав информации, персонал, работающий в организации, и т.д. Все это приводит к тому, что степень защищенности

системы постоянно изменяется и, что наиболее опасно, снижается.

Чтобы адаптировать систему информационной безопасности к новым условиям работы, необходимо отслеживать изменения и своевременно реагировать на них. Многие работы по анализу состояния защищенности корпоративной сети могут быть выполнены при помощи специальных программных средств, например Internet Scanner и System Security Scanner из семейства SAFESUITE корпорации Internet Security Systems Inc. Такие программные средства существенно облегчают работу администратора безопасности по поиску ошибок в настройках и выявлению критичного программного обеспечения, а также позволяют в автоматизированном режиме отслеживать состояние корпоративной сети, своевременно обнаруживать и устранять возможные источники проблем.

Составной частью работ пятого этапа является корректировка Плана защиты в соответствии с реальным состоянием корпоративной сети, поскольку самая совершенная схема рано или поздно устаревает и становится препятствием на пути совершенствования технологии обработки данных.

Следует помнить, что не существует стандартных решений, одинаково хорошо работающих в разных условиях. Всегда возможны и необходимы дополнения к рассмотренному общему плану организации защиты корпоративной сети, учитывающие особые условия той или иной организации. Однако реализация комплекса рассмотренных мероприятий с учетом возможных дополнений способна обеспечить достаточный уровень защищенности информации в корпоративной сети.

Контрольные вопросы

1. В чем заключается системный подход к защите информации?
2. Дайте общую характеристику организационным методам защиты информации.
3. Какие виды мероприятий необходимо проводить для защиты компьютерной информации?
4. Охарактеризуйте сущность понятий и терминов, используемых в законодательстве: неправомерный доступ, вредоносные программы, уничтожение, модификация, блокирование информации.
5. Дайте определение несанкционированного доступа (НСД) к компьютерным ресурсам.
6. Перечислите наиболее типичные способы несанкционированного доступа к информации.
7. Какие технические средства используются для защиты компьютерной информации?
8. Что такое идентификация и аутентификация пользователя?
9. Назовите основные субъекты идентификации и аутентификации.
10. С помощью каких программных средств обеспечивается защита информации от НСД на рабочей станции?
11. С помощью каких программных средств обеспечивается защита информации от НСД в информационной сети?
12. Дайте определение криптографических методов защиты информации.
13. Перечислите основные методы шифрования информации.

14. Поясните основные принципы работы криптографических программ.
15. Назовите программные средства восстановления удаленной либо испорченной компьютерной информации.
16. В каких случаях удаленный файл может быть полностью и успешно восстановлен?
17. Как обнаружить появление вируса на компьютере до периода его активизации?
18. Какие профилактические меры необходимо применять для защиты от вирусной атаки?
19. Каковы преимущества антивирусных программ-ревизоров перед анти-вирусными программами-детекторами Вы могли бы назвать?
20. Перечислите основные службы безопасности сети.
21. Какие механизмы безопасности сети считаются основными?
22. Назовите основные вопросы политики безопасности при построении защиты информации в корпоративной автоматизированной системе.
23. Назовите возможные способы защиты информации в корпоративной сети от шпионажа и диверсий.

ЗАКЛЮЧЕНИЕ

В современных условиях персональный компьютер стал для юриста «орудием производства», сейчас без знания персонального компьютера и соответствующего программного обеспечения уже невозможно представить работу сотрудника правоохранительных органов – следствия, криминалиста, а тем более сотрудника штаба или информационного подразделения. Поэтому эти категории работников должны иметь навыки работы на персональном компьютере, знать и применять в повседневной практике методы обработки деловой и аналитической информации с использованием ПК.

Очевидно, что в рамках одной книги сколько-нибудь детально ответить на все поставленные вопросы не представляется возможным. Так, не были описаны подробно методы работы с пакетами прикладных программ общего назначения, такими как системы управления базами данных, электронные таблицы, издательские системы, программы для работы в локальных и глобальных сетях, вопросы, касающиеся моделирования, алгоритмизации и программирования профессиональных задач и т.д. Существует несколько причин, по которым была выбрана стратегия изложения материала, реализованная в учебном пособии:

• ряд вопросов подробно изложен в широко доступной учебной литературе, в том числе, предназначенной для юристов (работа с текстовыми редакторами, электронными таблицами, архивирование информации);

• некоторые затронутые вопросы требуют отдельного подробного изложения, и их включение неизбежно потребовало бы значительного увеличения объема книги (системные утилиты, алгоритмизация, базы данных и системы управления базами данных, организация работы в глобальных сетях);

• знание некоторых вопросов не потребуется большинству пользователей в повседневной работе (работа с графическими пакетами, программирование);

• существуют вопросы, которые следует детально рассматривать в рамках отдельных спецкурсов(моделирование задач, системы искусственного интеллекта и базы знаний, криптография);

• сведения, которые можно почерпнуть в настоящей книге, должны стимулировать более глубокое и всестороннее самостоятельное изучение материала.

В целом, книга представляет собой базовый курс, рассчитанный на пользователей начального и среднего уровня квалификации.

За время написания и подготовки книги к изданию происходили серьезные изменения в области компьютерных информационных технологий – менялись поколения микропроцессоров (Pentium III, Pentium IV, Core 2 Duo, Core 2 Extreme), значительно, до 4 Ггц; возросла тактовая частота микропроцессоров, появились двух ядерные и четырех ядерные микропроцессоры. Появились новые типы микросхем оперативной и кэш памяти, на порядок, возрос их объем. Увеличились быстродействие и емкость накопителей на жестких магнитных дисках (до 1 Тбайт); на смену накопителям

DVD ROM пришли накопители Blue Ray, способные хранить до 50 Гбайт информации; появились новые типы видеоадаптеров и мониторов; сменилось несколько поколений операционных систем (Windows XP, Windows Vista), появилось большое количество мультимедийных программных продуктов и офисных приложений (MSOffice XP, MSOffice 2007). Громадный шаг вперед был сделан в развитии глобальных компьютерных сетей, прежде всего сети Интернет, а персональный компьютер все больше и больше трансформировался в часть общемировой информационной сети.

Вместе с тем, характер работы пользователя на персональном компьютере во многом остался прежним и даже упростился за счет применения все более дружественного интерфейса и объектно-ориентированных приемов работы. Это обстоятельство позволяет надеяться, что материал книги окажется полезным потенциальным читателям, поможет в освоении не только описанных в книге технических и программных средств, но и новых, более удобных и совершенных, предназначенных как для грамотной работы на компьютере, так и для компетентного выполнения профессиональных функций. Мы надеемся, что материал книги послужит для читателей стартовой базой для движения вперед, ибо совершенству нет предела.

Авторы будут признательны за замечания по содержанию и оформлению книги.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Згадзай О.Э. Информационные технологии в юридической деятельности : учебное пособие / О.Э. Згадзай, Н.Р. Шевко; под ред. С.Я. Казанцева. - Казань : КЮИ МВД России, 2012.
2. Информатика для юристов и экономистов / Симоновича С.В. и др. – СПб: Питер, 2013. – 688 с.
3. Информатика и вычислительная техника в деятельности органов внутренних дел. Информационно-вычислительные сети в органах внутренних дел: учебное пособие / под ред. В.А. Минаева. – М.: ГУК МВД РФ, 1997.
4. Информатика и математика для юристов. Краткий курс в таблицах и схемах: учебное пособие / под ред. В.А. Минаева.– М.: Приор, 1998. – 224 с.
5. Информатика: учебник / под ред. Н.В. Макаровой. – М.: Финансы и статистика, 2007.
6. Информационные технологии управления в органах внутренних дел / под ред. проф. В.А. Минаева. – М.: Академия управления МВД РФ, 1997. – 705 с.
7. Компьютерные технологии в юридической деятельности: учебное и практиче-ское пособие / под ред. проф. Н. Полевого, канд. юрид. наук. В. Крылова. – М.: БЕК, 1994. – 304 с.
8. Мельников В.П. Информационные технологии: учебник / В.П. Мельников. – М.: Академия, 2009.
9. Острейковский В.А. Информатика: учебник для вузов / В.А. Острейковский. – М.: Высшая школа, 2009.
10. Першиков В.И. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков. – 2-е изд., доп. – М.: Финансы и статистика, 1995.
11. Советов Б.Я. Информационные технологии: учебник для вузов / Б.Я. Советов, В.В. Целиховский. – М.: Высшая школа, 2009.
12. Степанов А.Н. Информатика. Базовый курс для студентов гуманитарных специ-альностей высших учебных заведений / А.Н. Степанов. – СПб.: Питер, 2011.
13. Уткин В.Б. Информационные технологии управления: учебник / В.Б. Уткин, К.В. Балдин. – М.: Академия, 2008.
14. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ.
15. Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ.
16. Гаврилов, М.В. Информатика и информационные технологии: учебник / М.В. Гаврилов, В.А. Климов. – 3-е изд., перераб. и доп. – М. : Юрайт, 2013.
17. Симонович, С.В. Информатика. Базовый курс: учебник для вузов / С.В. Симонович. – 3-е изд. - СПб: Питер, 2011.
18. Голицына О.Л. Информационные технологии: учебник / О.Л. Голицына, Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – М.: Форум, ИНФРА-М, 2013.
19. Гришин В.Н. Информационные технологии в профессиональной деятельности: учебник / В.Н. Гришин, Е.Е. Панфилова. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013.
20. Смелянский Р.Л. Компьютерные сети: В 2 т.: учебник / Р.Л. Смелянский. – М., Академия, 2011. – Т. 1: Системы передачи данных.
21. Кузин А.В. Базы данных: учебное пособие / А.В. Кузин, С.В. Левонисова. – М., Академия, 2010.
22. Таненбаум Э.С. Современные операционные системы: учебное пособие / Э.С. Таненбаум. – СПб., Питер, 2010.
23. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации: учебник для вузов / В.Л. Бройдо, О.П. Ильина. – СПб., Питер, 2011.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ALU	Arithmetic Logical Unit	арифметическое логическое устройство
ASCII	American Standard Code for Information Interchange	американский стандартный код для обмена информацией
BIOS	Basic Input/Output System	базовая система ввода/вывода информации
BSA	Business Software Alliance	Ассоциация производителей коммерческого ПО
CD-ROM	Compact Disk ROM	компакт диск
CD WORM	Compact Disk Write Once Read Many	записываемый компакт диск
CISK	Complex Information System Command	процессор с полной системой команд
CPU	Central Processing Unit	центральный процессор
CU	Control unit	устройство управления
DNS	Directory Name Service	служба каталогов
DVD	Digital Versatile Disk	цифровой диск общего назначения
FAT	File Allocation Table	таблица размещения файлов
FDD	Floppy Disk Drive	НГМД, накопитель на гибком магнитном диске
HDD	Hard Disk Drive	НЖМД, накопитель на жест-ком магнитном диске
IBM	International Business Machines Corporation	Международная корпорация машин для бизнеса
IP	Internet Protocol	межсетевой протокол Интернет
ISO	Integrated Standart Organization	Международная организация стандартизации
LAN	Local Area Network	локальная компьютерная сеть
MS DOS	Microsoft Disk Operation System	дисковая операционная система фирмы Microsoft
MSD	Mass Storage Device	ВЗУ, внешнее запоминающее устройство
OLE	Object Linking and Embedding	связывание и внедрение объектов
OSI	Open System Interconnection	взаимодействие открытых систем
PC	Personal Computer	персональный компьютер
RAM	Random Access Memory	ОЗУ, оперативно запоминающее устройство

RISK	Reduced Information System Command	процессор с сокращенной системой команд
ROM	Read-Only Memory	ПЗУ, постоянно запоминающее устройство
TCP	Transmission Control Protocol	протокол управления передачей
UPS	Uninterruptable Power Supply	источник бесперебойного электропитания
VGA	Video Graphics Array	видеографическая матрица
WWW	World Wide Web	всемирная компьютерная сеть (Интернет)

СЛОВАРЬ КОМПЬЮТЕРНЫХ ТЕРМИНОВ

BIOS: Базовая система ввода/вывода, которая является частью операционной системы, постоянно хранящейся в постоянном запоминающем устройстве машины.

COM: Тип исполняемого файла, в котором привязка уже выполнена и поэтому все адреса уже правильно записаны в файле перед его загрузкой.

EXE: Исполняемый файл, который требует привязки при загрузке. Не все адреса программы могут быть установлены до тех пор, пока неизвестно ее положение в памяти. EXE-файлы имеют заголовок, который содержит информацию об этой привязке. Эти файлы загружаются немного дольше и требуют больше места на диске, чем файлы типа COM.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ (АСУ): Организованная совокупность правил работы, баз данных и пакетов прикладных программ, обеспечивающая с помощью ЭВМ рациональное управление деятельностью.

АЛГОРИТМ: Последовательность команд (инструкций) для выполнения поставленной задачи. В данном случае команд компьютера.

АЛФАВИТНО-ЦИФРОВОЕ ПЕЧАТАЮЩЕЕ УСТРОЙСТВО (АЦПУ): Внешнее устройство ЭВМ, служащее для представления выводимой из нее информации в виде букв и цифр на бумажном носителе.

АРХИТЕКТУРА ЭВМ: Общее описание структуры и функций ЭВМ на уровне, достаточном для понимания принципов работы и системы команд ЭВМ.

БАЗА ДАННЫХ: Организованная совокупность данных во внешней памяти ЭВМ, предназначенная для длительного хранения и постоянного использования.

БАЙТ: Единица измерения количества информации, равная 8 битам. Набор из 8 двоичных разрядов, обрабатываемых как единое целое.

БАНК ДАННЫХ: Совокупность баз данных, объединенных общностью применения.

ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ: См. РЕЗЕРВНЫЕ ИСТОЧНИКИ ПИТАНИЯ.

БИБЛИОТЕКА: Организованная совокупность программ или алгоритмов, хранящаяся обычно во внешней памяти ЭВМ.

БИТ: Единица измерения количества информации и объема памяти. Может принимать значения 1 или 0.

ВОССТАНОВЛЕНИЕ ДАННЫХ: Процесс восстановления потерянной (поврежденной, случайно стертой и др.) информации на магнитных носителях с помощью специального программного обеспечения.

ВРЕМЕННЫЕ ФАЙЛЫ: Специальные файлы, в которых во время работы программы хранятся промежуточные данные. При корректном завершении программы эти файлы автоматически уничтожаются.

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА: Ассортимент вычислительных машин, вычислительных устройств и приборов, используемых для ускорения решения задач, связанных с обработкой информации, путем частичной или полной автоматизации вычислительного процесса.

ГИБКИЙ МАГНИТНЫЙ ДИСК (ГМД): См. ДИСКЕТА.

ГРАФОПОСТРОИТЕЛЬ: Внешнее устройство ЭВМ для вычерчивания контурных, графических изображений.

ДАННЫЕ: Информация, представленная в формальном виде, который обеспечивает возможность ее хранения, обработки или передачи.

ДЕРЕВО КАТАЛОГОВ: Система подкаталогов, организованная как ветви дерева, в которой на каталоги первого уровня имеются ссылки в корневом каталоге, а те, в свою очередь, содержат ссылки на каталоги более низкого уровня.

ДЕФЕКТНЫЕ СЕКТОРЫ: Место на магнитном носителе информации с поврежденным покрытием, где невозможно хранение данных.

ДЖОЙСТИК: Внешнее устройство ЭВМ в виде рычага на шаровом шарнире, позволяющее пользователю вручную перемещать курсор по экрану дисплея.

ДИСК МАГНИТНЫЙ: Вид внешней памяти, в котором носителем информации является вращающийся металлический или пластмассовый диск, покрытый слоем магнитного материала.

ДИСКЕТА: Гибкий магнитный диск внешней памяти ЭВМ, представляющий собой тонкий упругий диск, покрытый слоем магнитного материала в пластмассовом или пленочном корпусе.

ДИСКОВОД: Внешнее устройство ЭВМ, предназначенное для ввода-вывода информации с магнитных дисков в память ЭВМ.

ДИСПЛЕЙ: Внешнее устройство ЭВМ для отображения графической и текстовой информации.

ЕМКОСТЬ: Количество информации, содержащейся в запоминающем устройстве.

ИГРА КОМПЬЮТЕРНАЯ: Техническая игра, в которой игровое поле находится под управлением компьютера и воспроизводится обычно на экране дисплея.

ИНТЕРФЕЙС: Средства и способы установления и поддержания информационного обмена между исполнительными устройствами автоматической системы или системы человек-машина.

КАНАЛ СВЯЗИ: Техническое устройство, в котором сигналы, содержащие информацию, распространяются от передатчика к приемнику.

КЛАВИАТУРА: Внешнее устройство ЭВМ и других технических средств, служащие для ручного ввода информации как при передаче сообщений, так и в целях управления.

КОД: Набор выполняемых инструкций, составляющих программу, в отличие от данных, над которыми выполняются операции. Иначе говоря, кодом называется последовательность машинных инструкций, которые производит транслятор или ассемблер из текста программы.

КОДИРОВАНИЕ: Процесс записи или преобразования информации в соответствии с правилами, заданными некоторым кодом.

КОМАНДА: Типовое предписание, записанное на языке машины, определяющее действия ЭВМ при выполнении отдельной операции или части вычислительного процесса.

КОМАНДНАЯ СТРОКА: Строка на экране дисплея, принимающая управляющую информацию, такая, как строка, начинающаяся с запроса операционной системы.

КОМПЬЮТЕРНЫЕ ВИРУСЫ: Небольшие программы, внедренные в программное обеспечение, обладающие возможностью к самотиражированию (распространению, заражению других программ). Обычно обладают враждебными функциями, которые влекут задержку работы, уничтожение данных и др.

КОМПЬЮТЕР: То же, что ЭВМ. Чаще употребляется в применении к персональным ЭВМ.

КОРНЕВОЙ КАТАЛОГ: Центральный каталог диска. Он расположен в фик-

сированном месте на диске. Он может содержать список файлов, метку тома и указатели на подкаталоги.

КУРСОР: Особый подвижный знак, воспроизводимый на экране дисплея и отмечающий рабочую точку экрана.

ЛАЗЕРНЫЙ ДИСК (CD-ROM): Носитель информации, принцип работы которого основывается на отражении и рассеивании света от различных поверхностей. Источником света служит лазер. Запись информации на данный диск происходит, в основном, в заводских условиях. В персональном компьютере происходит только считывание информации (при отсутствии специального записывающего дисковода).

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ: Объединение компьютеров с помощью специальных устройств (СЕТЕВОГО ОБОРУДОВАНИЯ) с целью взаимного использования вычислительных ресурсов, обмена информацией и использования одной базы данных.

МАШИННЫЙ ЯЗЫК: Инструкции в специальных компьютерных кодах, непосредственно используемых процессором (самый сложный уровень программирования).

МИКРОПРОЦЕССОР: Процессор, выполненный в виде одной большой интегральной схемы и используемый в средствах вычислительной техники для решения широкого круга разнотипных задач.

МОДЕМ: Устройство сопряжения, преобразующее цифровые сигналы в аналоговую форму и обратно для передачи их по телефонной или выделенной линии связи.

МОНИТОР: См. ДИСПЛЕЙ.

НОСИТЕЛЬ ИНФОРМАЦИИ: Физическое тело или среда для записи, хранения и воспроизведения информации.

ОПЕРАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ: Программные операции, которые должны выполняться в определенный момент, а не тогда, когда компьютер окажется способным их выполнить. Мультипликация, сигналы тревоги и роботы используют работу в реальном времени.

ОПЕРАЦИОННАЯ СИСТЕМА: Комплекс программ, постоянно находящихся в памяти ЭВМ, позволяющих организовать управление устройствами машины и ее взаимодействие с пользователями.

ПАКЕТ ПРИКЛАДНЫХ ПРОГРАММ: Организованная совокупность программ постоянного применения для решения некоторых классов однотипных задач.

ПАМЯТЬ: Устройство ЭВМ, предназначенное для хранения обрабатываемой информации.

ПАМЯТЬ ВИРТУАЛЬНАЯ: Способ управления памятью ЭВМ, позволяющий программе использовать объем оперативной памяти, существенно превышающей емкость микросхем оперативной памяти ЭВМ.

ПАМЯТЬ ВНЕШНЯЯ: Память ЭВМ, организуемая внешними запоминающими устройствами (жесткие и гибкие магнитные диски, магнитные ленты, перфокарты и т.д.).

ПАМЯТЬ ВНУТРЕННЯЯ: Память ЭВМ, реализуемая через запоминающее устройство, непосредственно связанное с процессором и содержащее данные, непосредственно участвующие в его операциях.

ПАМЯТЬ ОПЕРАТИВНАЯ: Часть внутренней памяти ЭВМ, реализуемая оперативным запоминающим устройством (ОЗУ) и предназначенная для

временного хранения команд, данных, результатов в процессе выполнения арифметических и логических операций. После отключения питания ЭВМ информация, хранящаяся в оперативной памяти, автоматически удаляется.

ПАМЯТЬ ПОСТОЯННАЯ: Часть внутренней памяти ЭВМ, предназначенная для хранения стандартных программ и данных для управления ЭВМ и решения типовых задач, реализуемая обычно на базе специальных микросхем.

ПАРОЛЬ: Специальная комбинация клавиш, без набора которой невозможно получить доступ к информации и ресурсам вычислительной системы.

ПЕРФОКАРТА: Носитель информации в виде прямоугольной карточки (из тонкого эластичного картона или пластмассы) стандартной формы и размера, служащий для записи информации посредством пробивки отверстий (перфораций) по определенной системе.

ПЛАТА: Пластина определенного размера из электроизоляционного материала, обычно прямоугольной формы, применяемая в электронной аппаратуре в качестве основания для установки и механического закрепления электро- и радиоэлементов.

ПОДКАТАЛОГ: Каталог, который ничем не отличается от корневого каталога, за исключением того, что он хранится на диске как файл, а не в абсолютных секторах диска. Корневой каталог может содержать элементы, указывающие на подкаталоги, а они, в свою очередь, могут содержать элементы, описывающие другие подкаталоги.

ПОЛЬЗОВАТЕЛЬ: Человек, работающий на ЭВМ.

ПОРТ: Путь, по которому происходит обмен данными между процессором и внешними устройствами.

ПРИНТЕР: То же, что АЛФАВИТНО-ЦИФРОВОЕ ПЕЧАТАЮЩЕЕ УСТРОЙСТВО.

ПРОГРАММА: Упорядоченная последовательность действий для ЭВМ, реализующая алгоритм решения какой-либо задачи.

ПРОГРАММИРОВАНИЕ: Процесс разработки программы в соответствии с алгоритмом решения задачи, ее отладки и дальнейшего развития программы в ходе ее применения.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ: Совокупность программных средств управления работой вычислительной машины и совокупность инструментальных программных средств, используемых для создания новых программ.

ПРОЦЕССОР: Основное устройство вычислительных машин, выполняющее заданные программы преобразования информации и осуществляющее управление всем вычислительным процессом в ЭВМ.

РАЗДЕЛ: Область жесткого диска. Жесткий диск может быть разбит на разделы, с тем, чтобы он использовался несколькими операционными системами.

РАСПЕЧАТКА: Лист или рулон бумаги, на котором напечатана выведенная из ЭВМ информация.

РЕГИСТР: Часть микросхемы, в которой данные хранятся и над ними производятся операции.

РЕЗЕРВНОЕ КОПИРОВАНИЕ: Процесс создания специальных (резервных) копий с информации по окончании работы или для долговременного хранения.

РЕЗЕРВНЫЕ ИСТОЧНИКИ ПИТАНИЯ (UPS): Источники питания, способные обеспечить кратковременную работу вычислительной системы при полном отключении электропитания.

РЕЗИДЕНТНАЯ ПРОГРАММА: Программа, остающаяся в памяти после за-

вершения. Система предохраняет ее от порчи другими загружаемыми программами, которые могут иметь доступ к содержащимся в данной программе процедурам через вектора прерывания.

СИСТЕМА ЗАЩИТЫ: Комплекс программно-аппаратных средств, ограничивающих доступ пользователей к определенной информации или ресурсам вычислительной системы.

СИСТЕМА ОПЕРАЦИОННАЯ: См. ОПЕРАЦИОННАЯ СИСТЕМА.

СКАНЕР: Устройство ЭВМ, предназначенное для ввода графической информации (рисунков, фотографий и др.)

СКРЫТЫЙ ФАЙЛ: Статус, который может быть присвоен файлу установкой его байта атрибутов. Скрытые файлы не выводятся при выводе каталога файлов.

ТЕКСТ ПРОГРАММЫ: Исходный вариант программы, в том виде, как она выглядит до того, как она была переведена в машинный язык.

ТЕКУЩИЙ КАТАЛОГ: Каталог, являющийся частью дерева каталогов, к которому автоматически адресуются все файловые операции, до тех пор, пока строка пути в полном имени файла не указывает другого.

УСТРОЙСТВО: Устройством называется любое оборудование, которое хранит, выводит или обрабатывает информацию, такое как дисковый накопитель, видеодисплей или принтер.

ФАЙЛ: Последовательность записей, размещаемая на внешних запоминающих устройствах и рассматриваемая в процессе пересылки и обработки как единое целое.

ФЛОППИ-ДИСК: См. ДИСКЕТА.

ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНАЯ МАШИНА (ЭВМ): Устройство, преобразующее величины в виде набора цифр, предназначенное для обработки информации, в том числе для вычислений, решения прикладных задач, управления производством или какой либо сферой деятельности.

ЯЗЫК АССЕМБЛЕРА: Язык программирования самого низкого уровня, в котором программист пишет инструкции, непосредственно управляющие работой процессора.

ЯЗЫК ПРОГРАММИРОВАНИЯ: Формальный язык описания данных (информации) с целью их обработки на вычислительной машине.

ОГЛАВЛЕНИЕ

Учебное издание

Шевко Наиля Рашидовна
Казанцев Сергей Яковлевич
Згадзай Олег Эдуардович

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

под редакцией заслуженного юриста России,
профессора С.Я. Казанцева

Корректоры О.Н. Хрусталева,
Н.А. Климанова

Компьютерная верстка Л.А. Ризванова

Формат 60x90 1/16 Подписано в печать 08.06.2016
Усл. печ. л. 14,4 Тираж 100 экз.
Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 35

Отпечатано с готового оригинал-макета
в ООО «Центр инновационных технологий»
420108, г. Казань, ул. Портовая, 25а
Тел./факс (843) 231-05-46, 231-05-61
E-mail: citlogos@mail.ru
www.logos-press.ru