ИНФОРМАТИКА МАТЕМАТИКА для ЮРИСТОВ

учебник
второе издание

ИНФОРМАТИКА и МАТЕМАТИКА для ЮРИСТОВ

Под редакцией *С.Я. Казанцева, Н.М. Дубининой*

Второе издание,
переработанное и дополненное

Рекомендовано Министерством образования Российской Федерации в качестве ***учебника*** *для студентов высших учебных заведений, обучающихся по специальности «Юриспруденция» (021100)*

Допущено Министерством внутренних дел Российской Федерации в качестве ***учебника*** *для образовательных учреждений высшего профессионального образования МВД России*

ЮНИТИ
UNITY
Москва • 2010

УДК 34:[004+51](075.8)
ББК 22.1я73-1+32.81я73-1
И74

Рекомендовано Учебно-методическим центром
«Профессиональный учебник» в качестве ***учебника***
для студентов вузов, обучающихся по специальности «Юриспруденция»

Р е ц е н з е н т ы:
кафедра высшей математики Всероссийского
заочного финансово-экономического института
*(*зав. кафедрой проф. *Н.Ш. Кремер);*
д-р физ.-мат. наук, проф. *Л.А. Муравей*

Главный редактор издательства *Н.Д. Эриашвили*,
кандидат юридических наук, доктор экономических наук, профессор,
лауреат премии Правительства РФ в области науки и техники

И74 **Информатика** и математика для юристов: учебник для студентов вузов, обучающихся по юридическим специальностям / [С.Я. Казанцев и др.]; под ред. С.Я. Казанцева, Н.М. Дубининой. — 2-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2010. — 560 с.

I. Казанцев, Сергей Яковлевич.

ISBN 978-5-238-00928-5
Агентство CIP РГБ

Рассматривается аппаратное и программное обеспечение современной информационной технологии применительно к юридической деятельности. Освещены современные компьютерные и информационные технологии, используемые в правоприменительной деятельности. Показаны роль и место математики в ней. Представлены необходимые для юриста понятия и методы математической логики, теории вероятностей и математической статистики. Особое внимание уделено стандартному программному обеспечению юридической деятельности.

Для студентов и преподавателей юридических факультетов вузов. Может быть полезно студентам других специальностей и лицам, интересующимся информационными технологиями.

ББК 22.1я73-1+32.81я73-1

ISBN 978-5-238-00928-5

ВВЕДЕНИЕ

Интенсификация информационного обеспечения правоохранительной деятельности

Систематическое накопление достоверной, характеризующей оперативную обстановку информации, ее своевременный и качественный анализ являются одними из важнейших условий организации борьбы с преступностью в современных условиях. Информация стала стратегическим продуктом, а использование средств ее обработки, важнейшим из которых является компьютерная техника, сделалось жизненно важной потребностью при решении управленческих задач. Общество, которое не сумеет решить задачи интенсификации информационного обеспечения управления, рискует безнадежно отстать от развитых стран.

Наряду с определенными достижениями, в области информационного обеспечения правоохранительной деятельности остается много нерешенных вопросов. Одними из главных являются обоснованная децентрализация оперативного управления и информационного обеспечения, устранение противоречия между необходимостью сокращения количества учетных показателей и объективными потребностями в них, эффективность использования статистической информации, улучшение качественных аспектов информации — ее агрегированности и достоверности.

Подходы к решению указанных вопросов должны учитывать, очевидно, два аспекта — организационный и технический. В рамках организационного подхода следует добиваться того, чтобы информационные показатели, требующиеся в аппаратах МВД, УВД, прокуратуры, суда и т.д., были немногочисленными, но информационно емкими. При большом количестве информации следует так ее систематизировать, чтобы исключить повторное фиксирование и механическое объединение. Следует приводить информацию в стройную систему с логической связью позиций и показателей, четко определять объем и содержание необходимых сведений. Достаточная степень обобщения и специальный отбор данных являются необходимой предпосылкой автоматизации информационных процессов,

поскольку без четкого установления связей, позиций, видов и показателей информации автоматизированные системы работать не могут. Технический аспект улучшения информационного обеспечения правоохранительной деятельности предусматривает, прежде всего, оснащение всех структур управления средствами современной компьютерной техники, включая средства компьютерной связи, а также соответствующее программное обеспечение — операционные системы (ОС), системы управления базами данных (СУБД), программные средства защиты и кодирования информации.

Таким образом, автоматизация информационных процессов непосредственно связана с внедрением компьютерной техники и созданием автоматизированных систем сбора, хранения, обработки и выдачи информации на ее основе. При этом необходимо учитывать то важнейшее обстоятельство, что компьютер — мощное вычислительное средство — превратился в устройство для обработки и хранения любых видов информации, что позволяет применять его для моделирования и принятия управленческих решений, в системах автоматизированного проектирования, а также как средство связи в сложных системах коммуникации. Решение проблем информатизации видится в создании автоматизированных информационных сетей на разных уровнях управления. Особенно актуально создание локальных сетей на уровне подразделений, что обеспечило бы рациональное использование данных, поступающих в информационные центры (ИЦ) МВД и УВД. Функционирование таких сетей способствует организации бездокументного обмена информацией руководителей служб и подразделений МВД, УВД и использованию автоматизированных рабочих мест. При этом решается задача децентрализации обработки информации, основная часть которой до сих пор проводится в информационных центрах МВД и не оправдывает себя в силу технических сложностей. Формирование информационных массивов и концентрацию данных с созданием сетей также можно будет организовать на уровне ГРОВД, тем самым обеспечив рациональное использование информации и своевременный анализ оперативной обстановки.

Успешное решение задачи интенсификации информационного обеспечения правоохранительной деятельности требует коренного улучшения информационной подготовки кадров. Только глубокие специальные знания могут обеспечить высокий уровень информационной культуры. В этом направлении намечаются два основных пути решения проблемы: 1) обучение всего личного состава современным информационным методам; 2) целевая переподготовка работников информационно-аналитических служб МВД, УВД, прокуратуры, суда, налоговой полиции в соответствующих центрах. Для от-

дельных категорий целесообразна организация специальных курсов и стажировок в соответствующих вузах. Однако, поскольку информационная работа по обеспечению управления осуществляется во всех подразделениях, одним из основных направлений следует считать корректировку учебных программ и тематических планов учебных заведений с внесением в них вопросов, касающихся интенсификации информационного обеспечения.

В основу совершенствования подготовки специалистов в системе образования должна быть положена общая концепция информатизации образования. Повышение научно-технического уровня информационного обеспечения управления требует комплексного подхода к решению стоящих проблем, консолидации деятельности ученых — юристов, управленцев, математиков, программистов.

КОЛЛЕКТИВ АВТОРОВ:

С.Я. Казанцев, *В.Н. Калинина*, *О.Э. Згадзай*, *В.И. Левин*, *А.В. Филиппов*, *А.А. Дорошин*, *Н.М. Дубинина*

ПРЕДИСЛОВИЕ

История компьютера

Во все времена, начиная с древности, людям необходимо было считать. Сначала для счета использовали пальцы собственных рук или камешки. Однако даже простые арифметические операции с большими числами трудны для мозга человека. Поэтому уже в древности был придуман простейший инструмент для счета — абак, изобретенный более 15 веков назад в странах Средиземноморья. Этот прообраз счетов представлял собой набор косточек, нанизанных на стержни, и использовался купцами для счета.

Стержни абака в арифметическом смысле представляют собой десятичные разряды. Каждая косточка на первом стержне имеет достоинство, равное единице, на втором стержне — 10, на третьем стержне — 100 и т.д. До XVII века счеты оставались практически единственным счетным инструментом.

В России так называемые русские счеты появились в XVI веке. Они основаны на десятичной системе счисления и позволяют быстро выполнять арифметические действия

В 1614 г. математик Джон Непер (1550—1617) ввел понятие логарифма.

Логарифм — это показатель степени, в которую нужно возвести число (основание логарифма), чтобы получить другое заданное число. Открытие Непера состояло в том, что *таким способом* можно выразить любое число и что сумма логарифмов двух любых чисел равна логарифму произведения этих чисел. Это дало возможность действие умножения свести к более простому действию сложения. Непер создал таблицы логарифмов. Для того, чтобы перемножить два числа, нужно посмотреть в этой таблице их логарифмы, сложить их и отыскать число, соответствующее этой сумме, в обратной таблице — антилогарифмов. На основе этих таблиц в 1654 г. Р. Биссакар и в 1657 г. независимо от него С. Партридж разработали прямоугольную логарифмическую линейку — основной счетный инструмент инженера до середины XX века.

В 1642 г. Блез Паскаль (1623—1662) изобрел механическую суммирующую машину, использующую десятичную систему счисления.

Каждый десятичный разряд представляло небольшое колесо с десятью зубцами, обозначавшими цифры от 0 до 9. Всего колес было 8, т.е. машина Паскаля была 8-разрядной.

В 1673 г. Готфрид Лейбниц (1646—1716) построил механический арифмометр, выполнявший все четыре арифметических действия. В нем использовалась двоичная система счисления.

В 1804—1808 гг. Жозеф Мари Жаккар (1752—1834) создал приспособление для выработки крупноузорчатых тканей (машина Жаккара). Узор программировался с помощью колоды перфокарт — прямоугольных карточек из картона. На них информация об узоре записывалась посредством пробивки отверстий (перфораций[1]), расположенных в определенном порядке. При работе машины эти перфокарты ощупывались с помощью специальных штырей. Именно так с них считывалась информация для плетения запрограммированного узора ткани. Машина Жаккара явилась прообразом машин с программным управлением, созданных в XX веке.

В 1820 г. Тома де Кольмар разработал первый коммерческий арифмометр, способный умножать и делить. Начиная с XIX века арифмометры получили широкое распространение при выполнении сложных расчетов.

В 1830 г. Чарльз Бэббидж попытался создать универсальную аналитическую машину, которая должна была выполнять вычисления без участия человека. Для этого в нее вводились программы на перфокартах из плотной бумаги, заранее записанные с помощью отверстий, сделанных на них в определенном порядке. Принципы программирования для аналитической машины Бэббиджа разработала в 1843 г. Ада Лавлейс.

Аналитическая машина умела запоминать данные и промежуточные результаты вычислений, т.е. имела память. Эта машина содержала три основных части: устройство для хранения чисел, набиравшихся с помощью зубчатых колес (*память*), устройство для операций над числами (*арифметическое устройство*) и устройство для операций над числами с помощью перфокарт (*устройство программного управления*). Работа по созданию аналитической машины не была завершена, но заложенные в ней идеи помогли построить в XX веке первые компьютеры (в переводе с английского это слово означает «вычислитель»).

В 1880 г. В.Т. Однер в России создал механический арифмометр с зубчатыми колесами и в 1890 г. наладил его массовый выпуск. В дальнейшем под названием «Феликс» он выпускался до 50-х годов XX века.

---

[1] Перфорация — пробивка отверстий в бумаге или картоне.

В 1888 г. Герман Холлерит создал первую электромеханическую счетную машину — табулятор, в котором нанесенная на перфокарты информация считывалась с помощью электрического тока. Эта машина позволила в несколько раз сократить время подсчетов при переписи населения в США. В 1890 г. изобретение Холлерита было впервые использовано в одиннадцатой американской переписи населения. Работа, которую 500 сотрудников раньше выполняли в течение 7 лет, под руководством Холлерита 43 помощника на 43 табуляторах выполнили эту работу всего за один месяц.

В 1896 г. Холлерит основал фирму «Tabulating Machine Co». В 1911 г. эта компания была объединена с двумя другими фирмами, специализировавшимися на автоматизации обработки статистических данных, а свое современное название «IBM» (*International Business Machines*) получила в 1924 г. Она стала электронной корпорацией, одним из крупнейших мировых производителей всех видов компьютеров и программного обеспечения провайдеров глобальных информационных сетей. С середины 1950-х годов «IBM» заняла ведущее положение на мировом компьютерном рынке. В 1981 г. компания создала свой первый персональный компьютер, который стал стандартом в своей отрасли. К середине 1980-х годов «IBM» контролировала около 60% мирового производства электронно-вычислительных машин.

В конце XIX века была изобретена *перфолента* — бумажная или целлулоидная пленка, на которую информация наносилась перфоратором в виде совокупности отверстий.

Широкая бумажная перфолента была применена в монотипе — наборной машине, изобретенной Т. Ланстоном в 1892 г. Монотип состоял из двух самостоятельных аппаратов — клавиатуры и отливного аппарата. Клавиатура служила для составления программы набора на перфоленте, а отливной аппарат изготавливал набор (из специального типографского сплава — гарта) в соответствии с ранее составленной на клавиатуре программой.

Наборщик садился за клавиатурный аппарат, смотрел в стоящий перед ним на пюпитре текст и нажимал на соответствующие клавиши. При ударе по одной из буквенных клавиш иглы перфорирующего механизма с помощью сжатого воздуха пробивают в бумажной ленте кодовую комбинацию из горизонтального ряда отверстий. Эта комбинация соответствует данной букве, знаку или пробелу. После каждого удара по клавише бумажная лента передвигается на один шаг (3 мм). Готовую (пробитую) катушку перфоленты переносят в отливной аппарат, в котором также с помощью сжатого воздуха считывается с перфоленты закодированная на ней информация и автоматически изготавливается набор из литер. Таким образом, монотип является одной из первых в истории техники машин с программным управлением. Он относился к машинам горячего набора; со временем он уступил свое место сначала фотонабору, а затем электронному набору.

Несколько ранее монотипа, в 1881 г., была изобретена пианола (или фонола) — инструмент для автоматической игры на фортепиано. Действовала она также с помощью сжатого воздуха. В пианоле каждой клавише обыкновенного пианино или рояля соответствует молоточек, ударяющий но ней. Все молоточки вместе составляют контрклавиатуру, приставляемую к клавиатуре пианино. В пианолу вставляется широкая бумажная перфолента, намотанная на валик. Отверстия на перфоленте проделаны заранее во время игры пианиста — это своеобразные «ноты». При работе пианолы перфолента перематывается с одного валика на другой. Считывание записанной на ней информации производится с помощью пневматического механизма. Он приводит в действие молоточки, соответствующие отверстиям на перфоленте, заставляет их ударять по клавишам и воспроизводить игру пианиста. Таким образом, пианола также являлась машиной с программным управлением. Благодаря сохранившимся перфолентам пианол удалось получить некоторое представление об игре таких замечательных пианистов прошлого, как композитор А.Н. Скрябин. Пианолой пользовались известные композиторы и пианисты Рубинштейн, Падеревский, Бузони.

Позднее было применено считывание информации с перфоленты и перфокарт с помощью электрических контактов — металлических щеточек, которые при попадании на отверстие замыкали электрическую цепь. Затем щеточки заменили на фотоэлементы и считывание информации стало оптическим, бесконтактным. Так записывалась и считывалась информация в первых цифровых вычислительных машинах.

В 1937 г. Джордж Стибиц создал из обыкновенных электромеханических реле двоичный сумматор — устройство, способное выполнять операцию сложения чисел в двоичном коде. И теперь двоичный сумматор по-прежнему является одним из основных компонентов любого компьютера, основой его арифметического устройства.

В 1937—1942 гг. Джон Атанасофф создавал модели первой вычислительной машины, работавшей на вакуумных электронных лампах. В ней использовалась двоичная система счисления. Для ввода данных и вывода результатов вычислений использовались перфокарты. Работа над этой машиной в 1942 г. была практически завершена, но из-за войны дальнейшее финансирование было прекращено.

В 1937 г. Конрад Цузе создал свою первую вычислительную машину «Z1» на основе электромеханических реле. Исходные данные вводились в нее с помощью клавиатуры, а результат вычислений высвечивался на панели с множеством электрических лампочек. В 1938 г. К. Цузе создал усовершенствованную модель «Z2» своей машины. Программы в нее вводились с помощью перфоленты, которую изготавливали, пробивая отверстия в использованной 35-миллиметровой фотопленке. В 1941 г. К. Цузе построил действующий компьютер «Z3», а позднее и «Z4», основанные на двоичной системе

счисления. Они использовались для расчетов при создании самолетов и ракет. В 1942 г. Конрад Цузе и Хельмут Шрайер задумали перевести «Z3» с электромеханических реле на вакуумные электронные лампы. Такая машина должна была работать в 1000 раз быстрее, но создать ее не удалось — помешала война.

В 1943—1944 гг. на одном из предприятий «IBM» в сотрудничестве с учеными Гарвардского университета во главе с Говардом Эйкеном была создана вычислительная машина «Марк-1». Ее масса составляла около 35 тонн. Машина «Марк-1» была основана на использовании электромеханических реле и оперировала числами, закодированными на перфоленте. При ее создании использовались идеи, заложенные Ч. Бэббиджем в его аналитической машине. В отличие от Стибица и Цузе, Эйкен не осознал преимуществ двоичной системы счисления и в своей машине использовал десятичную систему. Машина могла манипулировать числами, имеющими до 23 разрядов. Для перемножения двух таких чисел ей было необходимо затратить 4 секунды. В 1947 г. была создана машина «Марк-2», в которой уже использовалась двоичная система счисления. В этой машине операции сложения и вычитания занимали в среднем 0,125, а умножение — 0,25 секунды.

Использование двоичной системы счисления позволяет сделать устройство компьютера максимально простым. Впервые принцип двоичного счисления был сформулирован в XVII веке немецким математиком Готфридом Лейбницем (1646—1716).

Электромеханические реле работали слишком медленно. Поэтому уже в 1943 г. американские ученые начали разработку вычислительной машины на основе электронных ламп. В 1946 г. Преспер Эккерт и Джон Мочли построили первую электронную цифровую вычислительную машину ENIAC. Ее масса составляла 30 т, она занимала 170 м^2. Вместо тысяч электромеханических реле ENIAC содержал 18 000 электронных ламп. Считала машина в двоичной системе и производила 5000 операций сложения или 300 операций умножения в секунду. На электронных лампах в этой машине было построено не только арифметическое, но и запоминающее устройство. Ввод числовых данных осуществлялся с помощью перфокарт. Программы же вводились в эту машину с помощью штекеров и наборных полей, т.е. приходилось соединять для каждой новой программы тысячи контактов. Поэтому для подготовки к решению новой задачи требовалось до нескольких дней, хотя сама задача решалась за несколько минут. Это было одним из основных недостатков такой машины.

Работы трех выдающихся ученых — Клода Шеннона, Алана Тьюринга и Джона фон Неймана явились основой для создания структуры современных компьютеров.

Клод Шеннон (1916—2000) — американский инженер и математик, основоположник математической теории информации, в 1948 г.

опубликовал работу «Математическая теория связи» со своей теорией передачи и обработки информации, которая включала все виды сообщений, в том числе передаваемых по нервным волокнам в живых организмах. Шеннон ввел понятие количества информации как меры неопределенности состояния системы, снимаемой при получении информации. Он назвал эту меру неопределенности *энтропией* по аналогии с подобным понятием в статистической механике. При получении наблюдателем информации энтропия, т.е. степень его неосведомленности о состоянии системы, уменьшается

Алан Тьюринг (1912—1954) — английский математик. Основные труды — по математической логике и вычислительной математике. В 1936—1937 гг. написал основополагающую работу «О вычислимых числах», в которой ввел понятие абстрактного устройства, названного впоследствии «машиной Тьюринга». В этом устройстве он предвосхитил основные свойства современного компьютера. Тьюринг назвал свое изобретение «универсальной машиной»: она должна была решать любую допустимую (теоретически разрешимую) математическую или логическую задачу. Данные в нее вводили с бумажной ленты, поделенной на ячейки — клетки. В каждой такой клетке либо содержался символ, либо не содержался. Машина Тьюринга могла обрабатывать вводимые с ленты символы и изменять их, т.е. стирать их и записывать новые по инструкциям, хранимым в ее внутренней *памяти*.

Джон фон Нейман (1903—1957) — американский математик и физик, участник работ по созданию атомного и водородного оружия. Родился в Будапеште, с 1930 г. жил и работал в США. В своем докладе, опубликованном в 1945 г. (ставшем первой работой по цифровым электронным компьютерам), выделил и описал «архитектуру» современного компьютера. В машине EDVAC более вместительная внутренняя память способна была хранить не только исходные данные, но и программу вычислений. Эту идею — хранить в памяти машины программы — Дж. фон Нейман выдвинул наряду с Мочли и Эккертом. Он впервые описал структуру универсального компьютера (так называемую «архитектуру фон Неймана» современного компьютера). Для универсальности и эффективной работы, по мнению фон Неймана, компьютер должен содержать центральное арифметико-логическое устройство, центральное устройство управления всеми операциями, запоминающее устройство (память) и устройство ввода-вывода информации. Фон Нейман считал, что компьютер должен работать на основе двоичной системы счисления, быть электронным и выполнять все операции последовательно, одну за другой. Эти принципы заложены в основу всех современных компьютеров.

Машина на электронных лампах работала значительно быстрее, чем на электромеханических реле, но сами электронные лампы были ненадежны. Они часто выходили из строя. Для их замены в 1947 г.

Джон Бардин, Уолтер Браттейн и Уильям Шокли предложили использовать изобретенные ими переключающие полупроводниковые элементы — транзисторы.

Джон Бардин (1908—1991) — американский физик, один из создателей первого транзистора (Нобелевская премия 1956 г. по физике совместно с У. Браттейном и У. Шокли за открытие транзисторного эффекта). Один из авторов микроскопической теории сверхпроводимости (вторая Нобелевская премия 1957 г. совместно с Л. Купером и Д. Шриффеном).

Уолтер Браттейн (1902—1987) — американский физик, один из создателей первого транзистора, лауреат Нобелевской премии по физике 1956 г.

Уильям Шокли (1910—1989) — американский физик, один из создателей первого транзистора, лауреат Нобелевской премии по физике 1956 г.

Совершенствование первых образцов вычислительных машин привело в 1951 г. к созданию компьютера UNIVAC, предназначенного для коммерческого использования. Он стал первым серийно выпускаемым компьютером.

Первая в СССР Малая электронная счетная машина (МЭСМ) на электронных лампах была построена в 1949—1951 гг. под руководством академика С.А. Лебедева. В 1952—1954 гг. под его руководством была разработана Быстродействующая Электронная Счетная Машина (БЭСМ), выполнявшая 8000 операций в секунду.

Созданием электронных вычислительных машин руководили крупнейшие советские ученые и инженеры: И.С. Брук, В.М. Глушков, Ю.А. Базилевский, Б.И. Рамеев, Л.И. Гутенмахер, Н.П. Брусенцов.

К первому поколению советских компьютеров относятся ламповые ЭВМ «БЭСМ-2», «Стрела», «М-2», «М-3», «Минск», «Урал-1», «Урал-2», «М-20».

Ко второму поколению советских компьютеров относятся полупроводниковые малые ЭВМ «Наири» и «Мир», средние ЭВМ для научных расчетов и обработки информации со скоростью 5—30 тысяч операций в секунду «Минск-2», «Минск-22», «Минск-32», «Урал-14», «Раздан-2», «Раздан-3», «БЭСМ-4», «М-220» и управляющие ЭВМ «Днепр», «ВНИИЭМ-3», а также сверхбыстродействующая «БЭСМ-6» с производительностью 1 млн операций в секунду.

Родоначальниками советской микроэлектроники были ученые, эмигрировавшие из США в СССР, Ф.Г. Старос (Альфред Сарант) и И.В. Берг. Они были инициаторами, организаторами и руководителями центра микроэлектроники в Зеленограде под Москвой.

ЭВМ третьего поколения на интегральных микросхемах появились в СССР во второй половине 1960-х годов. Были разработаны Единая Система ЭВМ (ЕС ЭВМ) и Система Малых ЭВМ (СМ ЭВМ) и организовано их серийное производство.

Четвертое поколение советских компьютеров реализовано на основе больших (БИС) и сверхбольших (СБИС) интегральных микросхем.

Примером крупных вычислительных систем четвертого поколения стал многопроцессорный комплекс «Эльбрус-2» с быстродействием до 100 млн операций в секунду.

В 1950-х годах было создано второе поколение компьютеров, выполненных на транзисторах. В результате быстродействие машин возросло в 10 раз, размеры и масса значительно уменьшились. Стали применять запоминающие устройства на магнитных ферритовых сердечниках, способные хранить информацию неограниченное время даже при отключении компьютеров. Их разработал Джой Форрестер в 1951—1953 гг. Большие объемы информации хранились на внешнем носителе, например на магнитной ленте или на магнитном барабане.

В 1959 г. Д. Килби, Д. Херни, К. Леховец и Р. Нойс изобрели интегральные микросхемы (чипы), в которых все электронные компоненты вместе с проводниками помещались внутри кремниевой пластинки. Применение чипов в компьютерах позволило сократить пути прохождения тока при переключениях. Скорость вычислений при этом увеличилась в десятки раз. Существенно уменьшились и габариты машин. Появление чипа позволило создать третье поколение компьютеров. В 1964 г. фирма «IBM» начинает выпуск компьютеров «IBM-360» на интегральных микросхемах.

В 1965 г. Дуглас Энгелбарт создал первую «мышь» — компьютерный ручной манипулятор. Впервые она была применена в персональном компьютере «Apple» фирмы «Macintosh», созданном позднее (в 1976 г.).

В 1967 г. компания «IBM» начала производить дискету для компьютера, изобретенную Йосиро Накамацу — съемный гибкий магнитный диск (флоппи-диск) для постоянного хранения информации. Первоначально дискета была гибкой, имела диаметр 8 дюймов, затем — 5 дюймов и емкость 80 Кбайт. Современная дискета емкостью 1,44 Мбайт, выпущенная фирмой «Sony» в 1982 г., заключена в жесткий пластмассовый корпус и имеет диаметр 3,5 дюйма.

В 1969 г. в США началось создание оборонной компьютерной сети — прародителя современной всемирной сети Internet.

В 1970-е годы были разработаны матричные принтеры, предназначенные для распечатки информации на выходе из компьютеров.

В 1971 г. сотрудник компании «Intel» Эдвард Хофф создал первый микропроцессор 4004, разместив несколько интегральных микросхем на одном кремниевом кристалле. Этот микропроцессор первоначально предназначался для использования в калькуляторах, но по существу представлял собой законченный микрокомпьютер. Это революционное изобретение кардинально изменило представление о компьютерах как о громоздких, тяжеловесных монстрах. Микропроцессор дал возможность создать компьютеры четвертого поко-

ления. Такой компьютер можно было разместить на письменном столе пользователя.

«Intel Corporation» (сокращение от *Integrated Electronics*) — крупнейшая американская компания по производству полупроводниковых интегральных схем и устройств — микропроцессоров, чипов памяти и др. Она основана в 1968 г. Робертом Нойсом и Гордоном Муром, разработавшими первые полупроводниковые интегральные схемы. В середине 1990-х годов компанию возглавлял Эндрю Гроув (родился в Венгрии в 1936 г.). «Intel Corporation» находится в Калифорнии (США) в Силиконовой долине, производит микропроцессоры для 90% всех персональных компьютеров.

В середине 1970-х годов начинают предприниматься попытки создания персонального компьютера (ПК) — вычислительной машины, предназначенной для частного пользователя.

В 1974 г. — Эдвард Робертс создал первый персональный компьютер «Altair» на основе микропроцессора «8080» фирмы «Intel». Без программного обеспечения он был неработоспособен — ведь дома у частного пользователя нет «под рукой» своего программиста. В 1975 г. о создании ПК «Altair» узнали два студента Гарвардского университета Билл Гейтс и Пол Аллен. Они первыми поняли насущную необходимость создания программного обеспечения для персональных компьютеров и в течение месяца создали его для ПК «Altair» на основе языка Бейсик. В том же году они создали компанию «Microsoft», быстро завоевавшую лидерство в создании программного обеспечения для персональных компьютеров и ставшую богатейшей компанией во всем мире.

В 1973 г. фирмой «IBM» был разработан жесткий магнитный диск (винчестер) для компьютера. Это изобретение дало возможность создать долговременную память большого объема, которая сохраняется при выключении компьютера.

Первые микрокомпьютеры «Altair-8800» представляли собой только набор деталей, которые нужно было собирать. Кроме того, пользоваться ими было крайне неудобно: они не имели ни монитора, ни клавиатуры, ни мыши. Ввод информации в них осуществлялся с помощью переключателей на передней панели, а результаты отображались с помощью светодиодных индикаторов. Позднее стали выводить результаты с помощью телетайпа — телеграфного аппарата с клавиатурой.

В 1976 г. инженер Стив Возняк из компании «Hewlett—Packard» создал принципиально новый микрокомпьютер. Он впервые применил для ввода данных клавиатуру, подобную клавиатуре пишущей машинки, а для отображения информации — обыкновенный телевизор. Символы выводились на его экран в 24 строки по 40 символов в каждой. Компьютер имел 8 Кбайт памяти, половину из которых занимал встроенный язык Бейсик, а половину пользователь мог использовать для введения своих программ. Этот компьютер

значительно превосходил «Altair-8800», имевший всего 256 байт памяти. С. Возняк предусмотрел для своего нового компьютера разъем (так называемый «слот») для подсоединения дополнительных устройств. Первым понял и оценил перспективы этого компьютера Стив Джобс. Он предложил организовать фирму для его серийного изготовления. И 1 апреля 1976 г. они основали компанию «Apple». Новый компьютер они назвали «Apple-I». В течение 10 месяцев им удалось собрать и продать около 200 компьютеров «Apple-I». В это время Возняк уже работал над его усовершенствованием. Новая версия называлась «Apple-II». Компьютер был выполнен в пластмассовом корпусе, он обладал графическим режимом, функциями звука, цвета, расширенной памятью, имел 8 разъемов расширения (слотов) вместо одного. Для сохранения программ в нем использовался кассетный магнитофон. Основу первой модели «Apple-II» составлял, как и в «Apple-I», микропроцессор 6502 фирмы «MOS Technology» с тактовой частотой 1 МГц. В постоянной памяти был записан Бейсик. Объем оперативной памяти в 4 Кбайт расширялся до 48 Кбайт. Информация выводилась на цветной или черно-белый телевизор, работающий в стандартной для США системе NTSC. В текстовом режиме отображались 24 строки, по 40 символов в каждой, а в графическом — разрешение составляло 280 на 192 точки (шесть цветов). Основное достоинство «Apple-II» заключалось в возможности расширения его оперативной памяти до 48 Кбайт и использования 8 разъемов для подключения дополнительных устройств. Благодаря использованию цветной графики его можно было использовать для различных игр.

Благодаря своим возможностям «Apple-II» завоевал популярность среди людей самых различных профессий. От его пользователей не требовалось знания электроники и языков программирования. «Apple-II» стал первым по-настоящему персональным компьютером для ученых, инженеров, юристов, бизнесменов, домохозяек и школьников.

В июле 1978 г. «Apple-II» был дополнен дисководом Disk II, значительно расширившим его возможности. Для него была создана дисковая операционная система Apple-DOS. В конце 1978 г. компьютер снова усовершенствовали под именем «Apple-II Plus». Теперь его можно было использовать в деловой сфере для хранения информации, ведения дел, помощи в принятии решений. Началось создание таких прикладных программ, как текстовые редакторы, органайзеры, электронные таблицы.

В 1979 г. Дэн Бриклин и Боб Фрэнкстон создали программу VisiCalc — первую в мире электронную таблицу. Этот инструмент лучше всего подходил для бухгалтерских расчетов. Первая его версия была написана для «Apple-II», который зачастую покупали только для того, чтобы работать с VisiCalc.

Таким образом, за несколько лет микрокомпьютер во многом благодаря фирме «Apple» и ее основателям Стивену Джобсу и Стиву Возняку превратился в персональный компьютер для людей самых различных профессий.

В 1981 г. появился персональный компьютер «IBM PC», который вскоре стал стандартом компьютерной индустрии и вытеснил с рынка почти все конкурирующие модели персональных компьютеров. Исключение составил только компьютер «Apple». В 1984 г. был создан «Apple Macintosh» — первый компьютер с графическим интерфейсом, управляемый мышью. Благодаря его преимуществам фирме «Apple» удалось удержаться на рынке персональных компьютеров. Она завоевала рынок в области образования, издательского дела, где используются их выдающиеся графические возможности для верстки и обработки изображений.

Сегодня фирма «Apple» контролирует 8—10% мирового рынка персональных компьютеров. Большая часть компьютеров «Macintosh» находится у пользователей США.

В 1979 г. появился оптический компакт-диск (CD), разработанный фирмой «Philips» и предназначенный только для прослушивания музыкальных записей.

В 1979 г. фирма «Intel» разработала микропроцессор «8088» для персональных компьютеров.

Широкое распространение персональные компьютеры получили с созданием в 1981 г. фирмой «IBM» модели «IBM PC» на базе микропроцессора «8088».

В IBM PC был применен принцип открытой архитектуры, позволивший вносить усовершенствования и дополнения в существующие конструкции ПК. Этот принцип означает применение в конструкции при сборке компьютера готовых блоков и устройств, а также стандартизацию способов соединения компьютерных устройств.

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 микрокомпьютеры и оснащать их дополнительными устройствами сотен производителей.

В конце 1990-х годов IBM PC-совместимые компьютеры составили 90% рынка персональных компьютеров.

За последние десятилетия XX века компьютеры многократно увеличили свое быстродействие и объемы перерабатываемой и запоминаемой информации.

В 1965 г. Гордон Мур, один из основателей корпорации «Intel», лидирующей в области компьютерных интегральных схем — чипов, высказал предположение, что число транзисторов в них будет ежегодно удваиваться. В течение последующих 10 лет это предсказание сбылось; и тогда он предположил, что теперь это число будет уд-

ваиваться каждые два года. Действительно, число транзисторов в микропроцессорах удваивается каждые 18 месяцев. Теперь специалисты по компьютерной технике называют эту тенденцию *законом Мура*. Похожая закономерность наблюдается и в области разработки и производства устройств оперативной памяти и накопителей информации.

Не отставало и развитие программного обеспечения, без которого вообще невозможно пользование персональным компьютером, и прежде всего операционных систем, обеспечивающих взаимодействие между пользователем и ПК.

В 1981 г. фирма «Microsoft» разработала операционную систему MS-DOS для своих персональных компьютеров.

В 1983 г. был создан усовершенствованный персональный компьютер «IBM PC/XT» фирмы «IBM».

В 1980-х годах были созданы черно-белые и цветные струйные и лазерные принтеры для распечатки информации на выходе из компьютеров. Они значительно превосходят матричные принтеры по качеству и скорости печати.

В 1983—1993 годах происходило создание глобальной компьютерной сети «Internet» и электронной почты «E-mail», которыми смогли воспользоваться миллионы пользователей во всем мире.

Мощный толчок к популяризации и развитию Internet дало появление Всемирной паутины (*World Wide Web*, WWW) — системы гипертекста (*hypertext*), которая сделала путешествие по сети Internet быстрым и понятным.

Идея связывания документов через гипертекст впервые была предложена Тедом Нельсоном в 1960-е годы, однако уровень существующих в то время компьютерных технологий не позволял воплотить ее в жизнь.

Основы WWW заложил Тим Бернерс—Ли с сотрудниками в процессе работ по созданию системы гипертекста в Европейской лаборатории физики элементарных частиц (*European Laboratary for Particle Physics*, Европейский центр ядерных исследований).

В январе 1991 г. они создали протокол передачи, т.е. язык описания документов — HTML (*Hypertext Markup Language*), в результате чего родилась служба *World Wide Web* (WWW) или сокращенно Web.

Служба WWW позволила объединять в одном документе текстовые и графические данные, а позднее и другие мультимедиаэлементы (например, звук), и обмениваться ими между компьютерами самых различных типов на общем «языке». С этой целью был разработан ряд правил, названных протоколами.

Для обмена HTML-документами между клиентами и серверами используется интернет-протокол HTTP (*Hypertext Transfer Protocol*).

Тим Бернерс—Ли подарил свои изобретения всему человечеству. Это сделало Internet общественным достоянием. Эта дата — январь 1991 г. — может считаться днем рождения Internet.

В 1992 г. фирма «Microsoft» выпустила операционную систему «Windows-3.1» для IBM PC-совместимых компьютеров. Слово «*windows*» в переводе с английского означает «окна». Эта «оконная» операционная система позволяет работать сразу с несколькими документами. Она представляет собой так называемый «графический интерфейс». Это система взаимодействия с ПК, при которой пользователь имеет дело с так называемыми «иконками» — картинками, которыми он может управлять с помощью компьютерной мыши. Такой графический интерфейс и система окон был впервые создан в исследовательском центре фирмы «Xerox» в 1975 г. и применен для ПК «Apple».

В 1995 г. фирма «Microsoft» выпустила операционную систему «Windows-95» для IBM PC-совместимых компьютеров, более совершенную по сравнению с «Windows-3.1», в 1998 г. — ее модификацию — «Windows-98», а в 2000 г. — «Windows-2000», а затем «Windows-XP». В их состав входит ряд прикладных программ: текстовый редактор Word, электронные таблицы Excel, программа для пользования системой Internet и электронной почтой E-mail — Internet Explorer, графический редактор Paint, стандартные прикладные программы (калькулятор, часы, номеронабиратель), дневник, универсальный проигрыватель, фонограф и лазерный проигрыватель.

За последние годы стало возможным объединить на персональном компьютере текст и графику со звуком и движущимися изображениями. Такая технология получила название «мультимедиа». В качестве носителей информации в таких мультимедийных компьютерах используются оптические компакт-диски CD-ROM (*Compact Disk Read Only Memory*, т.е. память на компакт-диске «только для чтения»). Внешне они не отличаются от звуковых компакт-дисков, используемых в проигрывателях и музыкальных центрах.

Емкость одного CD-ROM достигает 650 Мбайт, по емкости он занимает промежуточное положение между дискетами и винчестером. Для чтения компакт-дисков используется CD-дисковод. Информация на компакт-диск записывается только один раз в промышленных условиях, а на ПК ее можно только читать. На CD-ROM издаются самые различные игры, энциклопедии, художественные альбомы, карты, атласы, словари и справочники. Все они снабжаются удобными поисковыми системами, позволяющими быстро найти нужный материал. Объема памяти трех компакт-дисков CD-ROM достаточно для размещения энциклопедии, превышающей по объему Большую Советскую энциклопедию.

В конце 1990-х гг. были созданы однократно записываемые CD-R и многократно перезаписываемые CD-RW оптические компакт-диски и дисководы для них, позволяющие пользователю делать любые записи звука и изображения по своему вкусу.

В 1990—2000 гг. помимо настольных персональных компьютеров были созданы ПК «ноутбук» в виде портативного чемоданчика

и еще более миниатюрные карманные «палмтоп» («наладонники»), помещающиеся в кармане и на ладони. Ноутбуки снабжены жидкокристаллическим экраном — дисплеем, размещенным в откидной крышке, а палмтопы — на передней панели корпуса.

В 1998—2000 гг. была создана миниатюрная твердотельная флэш-память (без подвижных деталей). Габариты ее не превышают размеров почтовой марки, а емкость достигает 1 Гбайт.

Кроме портативных персональных компьютеров создаются суперкомпьютеры для решения сложных задач в науке и технике — прогнозов погоды и землетрясений, расчетов ракет и самолетов, ядерных реакций, расшифровки генетического кода человека.

Изобретателем суперкомпьютера стал Сеймур Крей (1925—1996 гг.). Он разработал мультипроцессорные компьютеры, способные осуществлять одновременную (параллельную) обработку данных с высокой операционной скоростью. Первым суперкомпьютером стал выпущенный в 1976 г. «Крей-1». Он мог осуществлять 240 миллионов вычислений в секунду и применялся для научных исследований, таких как моделирование сложных физических явлений.

В 2002 г. в Японии был построен суперкомпьютер «NEC Earth Simulator», выполняющий 35,6 триллионов операций в секунду. На сегодня это самый быстродействующий в мире суперкомпьютер.

Компания «IBM» разработала суперкомпьютер «Blue Gene» производительностью свыше 30 триллионов операций в секунду (2005 г.). Он содержит 12 000 процессоров. В отличие от персональных компьютеров, содержащих всего один микропроцессор и совершающих все операции последовательно, в суперкомпьютерах операции совершаются параллельно, что многократно увеличивает их быстродействие.

В 2001 г. персональным компьютерам исполнилось 20 лет. Посмотрим, как они изменились за эти годы. Первые из них, оборудованные микропроцессором «Intel», работали с тактовой частотой всего 4,77 МГц и имели оперативную память 16 Кбайт. Современные ПК, оборудованные микропроцессором «Pentium 4», созданном в 2001 г., имеют тактовую частоту 2—3 ГГц, оперативную память 128—512 Мбайт и более и долговременную память (винчестер) емкостью 20—80 Гбайт и более. Такого гигантского прогресса не наблюдается ни в одной отрасли техники, кроме цифровой вычислительной.

Компьютеры создавались для численных расчетов, но они могут обрабатывать и другие виды информации, так как практически все виды информации могут быть представлены в цифровой форме. Для обработки различной информации компьютеры снабжаются средствами для ее преобразования в цифровую форму и обратно. Поэтому с помощью компьютера можно производить не только численные расчеты, но и работать с текстами, рисунками, фотографиями, видео, звуком, управлять производством и транспортом, осуществлять различные виды связи. Компьютеры превратились в универсальные средства обра-

ботки всех видов информации, используемых человеком. Миллионы компьютеров используются практически во всех отраслях экономики, промышленности, науки, техники, педагогики, медицины.

Основные причины такого прогресса — необычайно высокие темпы микроминиатюризации устройств цифровой электроники и успехи программирования, сделавшие «общение» рядовых пользователей с персональными компьютерами простым и удобным.

Все современные компьютеры делятся на *классы* — микрокомпьютеры и мини-компьютеры, мейнфреймы, суперкомпьютеры.

Микрокомпьютер, настольный или портативный компьютер, использует микропроцессор в качестве единственного центрального процессора, выполняющего все логические и арифметические операции. К микропроцессорам относятся настольные персональные компьютеры, портативные персональные компьютеры — ноутбуки и карманные компьютеры — палмтопы.

Мини-компьютер занимает промежуточное положение между большими вычислительными машинами — мейнфреймами и микрокомпьютерами; они играют роль серверов, к которым подключаются десятки и сотни терминалов или микрокомпьютеров. Персональные компьютеры предназначены для работы с персональным пользователем.

Мини-компьютеры используются в крупных фирмах, государственных и научных учреждениях, учебных заведениях, компьютерных центрах для решения задач, с которыми не способны справиться микрокомпьютеры, и для централизованного хранения и переработки больших объемов информации.

Мейнфрейм — это универсальный, большой компьютер высокого уровня, предназначенный для решения задач, связанных с интенсивными вычислениями и обработкой больших объемов информации.

Суперкомпьютер — это компьютер, способный производить как минимум сотни миллиардов операций в секунду. Такие громадные объемы вычислений нужны для решения задач в аэродинамике, метеорологии, физике высоких энергий, геофизике, генетике. Суперкомпьютеры нашли свое применение и в финансовой сфере.

Таким образом, компьютеры всего за полвека превратились из многотонных гигантов в миниатюрные быстродействующие устройства, позволяющие решать самые разнообразные задачи во всех видах человеческой деятельности.

Часть I

ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАТИКИ. ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР: УСТРОЙСТВО И ПРИНЦИПЫ РАБОТЫ

Глава 1

ИНФОРМАТИКА КАК НАУКА. ИНФОРМАЦИЯ И ЕЕ ХАРАКТЕРИСТИКИ. АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

1.1. Основные понятия и определения информатики

Процесс информатизации общества, охвативший большинство сфер человеческой деятельности, не обошел стороной и правоохранительные органы. Компьютер стал средством, «орудием труда» сотрудника ОВД. Вместе с тем появились и новые виды преступности, связанные по своей сути с незаконным хищением, копированием и распространением информации, так называемые *компьютерные преступления*. Очевидно, все это требует соответствующей подготовки в области современных информационных технологий, соответствующей информационной культуры. Квалификация современного специалиста в области юридической и правоохранительной деятельности включает в себя понимание устройства и основных принципов работы персонального компьютера (ПК), необходимые навыки алгоритмизации и программирования задач, знание современных принципов сбора, хранения и переработки информации, в том числе с использованием телекоммуникаций (компьютерных сетей), понимание основ искусственного интеллекта.

Программа курса «Информатика и математика» охватывает материал, по крайней мере, пяти дисциплин: 1) основы информатики и вычислительной техники; 2) основы управления; 3) правовая статистика; 4) правовая информатика и кибернетика; 5) криминология.

В курсе «Информатика и математика» осуществляется базовая подготовка, т.е. изучаются основы информатики, вычислительной техники, математики и статистики. Информационные аспекты управления в целом рассматриваются в курсе социального управления. С юридической статистикой слушатели знакомятся дополнительно в курсах правовой статистики, социологии и криминологии.

Предметом курса «Информатика и математика» являются информационные отношения, складывающиеся в процессе деятельности по сбору, переработке, передаче, хранению и выдаче информации.

Задачи курса: изучить основные понятия и определения информатики, устройство персонального компьютера, основные виды системного и прикладного программного обеспечения, математические методы и приемы обработки и анализа данных; освоить работу на ПК в объеме, достаточном для осуществления дальнейшей профессиональной деятельности; ознакомиться с новейшими информационными технологиями, применяемыми в деятельности правоохранительных органов.

Система курса определяется содержанием информационной деятельности в условиях информатизации общества, в том числе его правоохранительной деятельности.

Информация, ее свойства и характеристики

Деятельность органов внутренних дел — это по своей сути управленческая деятельность. В научной литературе встречается следующее определение: «*Управление* — это процесс восприятия и переработки *информации*».

Таким образом, *информация является субстратом* (основой) *управления*. В общем виде управление может быть представлено как воздействие управляющей системы на управляемую. От субъекта управления к объекту (исполнителю) поступает управляющая информация — команды управления, обратно, по обратной связи — осведомляющая информация. В правильно функционирующей системе управления низший уровень предстает перед высшим как «черный ящик», информирующий о результатах своей деятельности; информация о способах и механизмах ее реализации на верхний уровень не передается. Таким образом, осуществление управления неотделимо от переработки информации, а эффективность управления — от правильной организации информационных процессов.

Слово «информация» перешло из латинского во многие другие языки, стало обиходным, и кажется, что дать ему определение несложно. Однако и в настоящее время термин «информация» не имеет устоявшегося определения.

В переводе с латинского «информация» — сообщение о каком-либо факте, событии, объекте, явлении и т.п., т.е. информация тождественна сообщению. Но возникает вопрос, что такое «сообщение»?

Ф.Л. Бауэр в своей фундаментальной книге «Информатика» пишет так: «“Сообщение” и “информация” — основные понятия информатики, значение которых не вполне соответствует их употреблению в обиходной речи. Поэтому мы вводим “сообщение” и “информация” как неопределяемые, основные понятия». Все остальные понятия информатики являются производными от основных.

Винер дает такое определение: «Информация — это обозначение содержания сообщения, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде».

В статистической теории информации информация понимается как содержание сообщения и как *мера сложности объекта* (алгоритмический подход Колмогорова).

Существуют попытки использования понятия «информация» в точно определенном смысле: информация — *мера зависимости случайных переменных* или *мера организации системы*.

Наиболее распространенным является так называемый «содержательный подход» к определению понятия «информация». Так, можно определить информацию как совокупность отобранных данных, являющихся содержательным выходом системы. В рамках содержательного подхода можно дать два самых общих определения понятия «информация»:

1. Информация — это сведения, которые снимают *неопределенность*, существовавшую до их получения.

2. Информация — это сведения, которые уменьшают или снимают *неразличимость* вещей или явлений.

Однако существенно не всякое снятие неопределенности, а лишь то, в результате которого возникает знание; также важно лишь значимое разнообразие.

Информацию можно трактовать и как *отраженное разнообразие*. Это согласуется с философской теорией отражения и с представлением об информации как о сведениях или сообщениях, которые всегда что-то отражают — события, явления и т.п.

Справедливо ли утверждение: информация тождественна сообщению? Очевидно, что в повседневной жизни под информацией мы понимаем лишь такое сообщение, которое содержит неизвестные его получателю факты. Поэтому сообщение может либо нести, либо не нести информацию, а сам объем информации зависит от того, кто воспринимает данное сообщение. Если сообщение не несет никакой информации, оно называется *тривиальным*.

В качестве примера приведем два сообщения:

1) $2 \times 2 = 4$;

2) сообщение о совершенной неизвестным преступником краже.

Для определенности договоримся временно пользоваться следующим определением: «***Информация*** *— это содержание сообщения, сигнала, памяти*».

Во все времена существования человеческого общества информация оказывала определяющее влияние на все сферы человече-

ской деятельности: сельское хозяйство, промышленность, политику, культуру и т.д.

Насколько важным является владение информацией видно уже из того, что каждый из этапов развития человечества обусловлен овладением определенной информацией. Поэтому можно сказать, что все усилия общества направлены на получение и обработку информации. Информация получается в результате творческой деятельности человека. В дальнейшем она может передаваться, храниться, шифроваться, уничтожаться.

В целом в жизни общества информация выступает и как продукт его жизнедеятельности, и как один из основных его ресурсов, наряду с такими ресурсами, как природные и энергетические ресурсы. Однако в отличие от материальных ресурсов, *количество информации в процессе развития общества* не уменьшается, а *увеличивается*. Если с материальными ресурсами проблема состоит в том, откуда их получить, то с информацией — все наоборот.

Основная проблема — *как эффективно хранить и обрабатывать информацию*; ее решение становится все актуальнее с развитием общества:

«Объем литературы в любой области огромен. Дело становится все хуже и хуже, ибо не проходит и дня, чтобы новые статьи не добавлялись к тому, что уже сейчас представляет собой целую гору материалов. Слишком мало времени и слишком много нужно прочесть» (Плуае, 1793 г.);

«Люди науки должны испытывать чувство, близкое к политической тревоге, когда они созерцают поток новых знаний, который приносит с собой каждый год. Каждое, любое новое, сколько-нибудь значительное добавление к уже существующей к этому времени информации сделает этот объем почти не переносимым» (Релей, 1974 г.).

Такая реакция понятна психологически. В определенный момент времени наступает *информационное насыщение* — состояние, при котором человек не способен воспринимать и обрабатывать новую информацию. Возникает оно не только в результате перенапряжения, но и в тех случаях, когда требуется воспринять большие объемы данных и принять ответственное решение в ограниченное время.

Это рано или поздно должно было привести к становлению науки, которая должна была заняться специфическими проблемами, связанными с переработкой информации, что и произошло в 50-х годах XX века.

В XX веке произошел *информационный взрыв* — резкое увеличение объема информации, которую должен воспринимать, хранить и использовать человек в процессе своей трудовой деятельности. Это является следствием научно-технической революции. Наблюдается

тенденция к росту объема воспринимаемой информации за каждый очередной промежуток времени (например, за 10 лет). Считается, что XIX век был веком механики, XX — веком энергии, а XXI — будет веком информации, т.е. основная трудовая деятельность человека будет связана с ее переработкой («информационное общество»).

Информационное общество — новая историческая фаза развития цивилизации, жизнь и деятельность человека в которой прежде всего связаны с созданием, переработкой и использованием информации. В качестве средств информационное общество широко использует компьютеры, телекоммуникационные сети, электронные библиотеки, банки данных, автоматизированные информационные системы, системы искусственного интеллекта.

То, что информация представляет собой один из основных ресурсов общества, означает, что обладание информацией позволяет получить или экономить материальные ресурсы. В настоящее время научная и производственная технологии настолько обогнали информационную, что часто бывает выгоднее повторить изобретение или заново сделать разработку, чем отыскать ее описание в литературных источниках.

Этим же обусловлено и то, что информационные технологии все больше становятся орудием преступления. Появился специальный термин — «информационная преступность». Большая часть преступлений в сфере информации связана с попытками проникновения в банковские сети с целью модификации кодов и извлечением выгоды. Другая часть относится к разрушению информации, например, с помощью *компьютерных вирусов*.

Все многообразие информации можно сгруппировать по различным п р и з н а к а м.

По способу передачи и восприятия:

- зрительная;
- слуховая;
- тактильная;
- вкусовая;
- машинно-ориентированная.

Каждый вид воспринимается только определенным устройством. Для того чтобы информация могла быть воспринята, например, компьютером, она должна быть формализована.

По формам отображения информация бывает:

- символьная;
- текстовая;
- графическая.

Данные — это информация, представленная в формализованном виде. Справедливо и такое определение: ***данные*** — это зарегистрированные сигналы.

Для машинно-ориентированной информации характерны следующие *формы представления*:

- двоичная;
- текстовая;
- графическая;
- электронные таблицы;
- базы данных.

По содержанию информация подразделяется по виду обслуживаемой человеческой деятельности:

- научная;
- производственная;
- управленческая;
- правовая и т.п.

Виды представления информации

По виду представления информация подразделяется на одномерную и многомерную.

Одномерная информация — сообщение, в котором передаваемая информация имеет вид последовательности символов, каждый из которых несет только один признак:

- электрические импульсы — компьютеры, живые существа;
- звуковые символы — речь;
- знаки алфавита — тексты.

Многомерная информация — сообщение, в котором информацию несут не один, а множество признаков символов:

- текст — значение, цвет и шрифт написания знаков алфавита;
- голос — амплитуда, тембр, значение звука.

Переработка и передача многомерной информации часто требуют преобразования многомерной информации в одномерную путем кодирования.

Характеристики информации

Характеристиками информации являются целевое назначение, полнота, надежность, ценность, достоверность, избыточность, скорость передачи и обработки.

Целевое назначение — для кого или для чего предназначена информация.

Примеры.

1. Патрульная машина №2 — проследовать к перекрестку улиц Восстания и Декабристов;

2. Пропал человек, приметы: ... Всем, кто видел его, просьба сообщить по телефону 02.

Полнота — количество информации, необходимое для принятия решения.

Пример.

Свидетель сообщил, что видел гр-на *N* вблизи места преступления. Однако эта информация недостаточна, чтобы произвести арест (*информация неполная*). Экспертиза обнаружила отпечатки пальцев гр-на *N* на орудии, которым было совершено убийство. Под давлением улик гр-н *N* сознался (*информация полная*).

Надежность — степень доверия к содержанию информации.

Примеры.

1. Фотография представляет не очень надежную информацию для опознания преступника, так как облик человека изменяется со временем и может быть легко изменен умышленно. Более надежную информацию предоставляют дактокарты.

2. Способ передачи информации в виде цифрового кода более надежен, чем в виде аналогового сигнала.

Ценность — пригодность информации к практическому использованию.

Пример.

Похищено произведение искусства, которое было уничтожено преступником. Информация о художнике, создавшем картину, может не представлять ценности для розыска преступника.

Достоверность — свойство информации быть правильно воспринятой, вероятность отсутствия ошибок.

Пример.

В записной книжке обнаружен адрес, в котором номер дома записан неразборчиво (1 или 4). Интерпретация неразборчивой цифры как 1 представляется недостоверной.

Избыточность — наличие в сообщении дублирующих данных, которые можно удалить без ущерба для содержания и принимаемого решения.

Примеры.

1. В сообщении указано, что преступнику 30 лет и он родился в 1969 г.

2. По ненадежной линии телефонной или радиосвязи передают сообщения, кодируя каждую букву словом, это повышает достоверность полученной информации.

Скорость передачи и обработки — эта характеристика часто зависит от вида информации и определяет ее ценность.

Примеры.

1. По номеру двигателя устанавливают, находится ли машина в поиске. Обработка информации по угнанным машинам производится с помощью компьютера.

2. Передача информации об угнанном транспортном средстве по радиосвязи. При отказе средства связи теряется оперативность и в результате ценность информации.

Для измерения объема или количества информации используются энтропийный и технический способы.

Измерение информации. Математическое понятие информации

Математическое понятие информации связано с ее измерением. В теории информации принят *энтропийный подход*, который устанавливает ценность информации, содержащейся в сообщении для его получателя, и исходит из следующей модели. Получатель сообщения имеет представление о возможности наступления некоторых событий. Эти представления в общем случае недостоверны и выражаются вероятностями, с которыми он ожидает то или иное событие. Общая мера неопределенности, называемая энтропией, характеризуется некоторой математической зависимостью от совокупности этих вероятностей:

$$S = \ln W,$$

где W — число всех возможных комбинаций, которыми может быть выражено некоторое состояние.

Количество информации в сообщении определяется тем, насколько уменьшается энтропия после получения сообщения. Тривиальное сообщение не несет информации. Сообщение несет полную информацию о некотором событии, если оно снимает всю неопределенность.

Примеры.

1. Бросание монеты: до падения монеты вероятность выпадения одной из сторон равна 0,5 и возможны две комбинации; после падения — реализована единственная комбинация.

2. Одним из жителей города, деликтоспособное население которого составляет примерно 1 млн человек, совершено преступление.

Неопределенность относительно лица, совершившего это преступление, определяется энтропией

$$S_0 = \log_2 1\ 000\ 000 \approx 20 \text{ бит}.$$

Получено сообщение, что преступник — мужчина. Информация, содержащаяся в этом сообщении,

$$I_1 = \log_2 2 = 1 \text{ бит}.$$

В результате энтропия стала

$$S_1 = S_0 - I_1 \approx 19 \text{ бит}.$$

Получено сообщение о возрасте преступника. При деликтоспособном интервале возраста в 78 − 14 = 64 года информация, содержащаяся в этом сообщении, будет равна

$$I_2 = \log_2 64 = 6 \text{ бит.}$$

В результате после получения второго сообщения энтропия

$$S_2 = S_1 - I_2 \approx 13 \text{ бит.}$$

Получено сообщение о районе проживания преступника. Информация, содержащаяся в этом сообщении, если в городе всего около 500 улиц,

$$I_3 = \log_2 512 = 9 \text{ бит.}$$

В результате энтропия станет

$$S_3 = S_2 - I_3 \approx 4 \text{ бит.}$$

Могут прийти сообщения об образовании, месте рождения и др., которые также уменьшат энтропию и неопределенность.

В технике часто используют более простой и грубый *объемный способ* измерения информации. Он основан на подсчете числа символов в сообщении, т.е. связан с длиной сообщения и не учитывает его содержания. При объемном способе применяют две стандартные единицы измерения информации: *бит* и *байт*.

Бит — это один символ двоичного алфавита. С его помощью можно полностью передать информацию о реализации события, которое может иметь два исхода. Например, бросание монеты.

Байт — это количество информации, которое можно передать с помощью 8 двоичных символов, восьмиразрядного двоичного кода. С помощью байта можно полностью передать информацию о реализации события, которое может иметь $2^8 = 256$ исходов. Например, нажатие на одну из клавиш компьютера.

Производные единицы измерения информации: *килобайт* (1 Кбайт = 1024 байт), *мегабайт* (1 Мбайт = 1024 Кбайт); *гигабайт* (1 Гбайт = 1024 Мбайт).

Шеннон — единица измерения количества информации, равная количеству информации, содержащейся в сообщении, выраженном одним из двух равновероятных, взаимоисключающих и исчерпывающих состояний.

Дит — единица количества информации, содержащейся в сообщении о состоянии системы, имеющей десять равновероятных состояний; количество информации, равное единице, при выборе основания логарифма, равного десяти.

Результаты, полученные двумя рассмотренными способами измерения информации, как правило, не совпадают. Энтропийное количество информации никогда не превосходит объемного.

При измерении информации, циркулирующей в ЭВМ, используют в основном технический подход.

Информационные процессы

Информация может быть не только воспринята познающим субъектом или техническим устройством, но и отделена от ее первоисточника. В результате информация может быть подвергнута операциям, совокупность которых называют информационными процессами.

Информационные процессы — это процессы восприятия, накопления, обработки и передачи информации.

Проявляется информация всегда в материально-энергетической форме, в частности в виде сигналов. *Сигнал* может иметь самую различную физическую природу, и в информационном процессе он выполняет функцию переносчика информации от источника к приемнику и далее к адресату. Этот процесс показан на рис. 1.1 в виде блок-схемы.

Рис. 1.1. **Сигнал в информационном процессе**

Процесс передачи информации — многоступенчатый, сигнал может на каждом из промежуточных этапов менять свою физическую природу. При этом возникают вопросы о взаимной однозначности (изоморфности) информации и сигнала, полноте и объективности передачи, возможности восприятия сигнала принимающим субъектом.

Передача информации — это лишь одна фаза информационного процесса. Общая структура информационного процесса представлена на рис. 1.2.

Собственно информационный процесс начинается с *восприятия и фиксации* информации, содержащейся в том или ином источнике. Информация отделяется от шумов. Завершается процесс *формированием сигнала*, с помощью которого информация передается. Сигнал обладает определенной структурой, которую можно выразить в дискретной форме. На принципах передачи сигналов, подвергшихся дискретизации, основана работа компьютера, который способен выполнять формально-логические операции. Машина обучена воспринимать введенный в нее класс объектов, признаки которых за-

кодированы. Имеется существенная разница между компьютером и человеком. Человек субъективно воспринимает образ объекта, а машина — коды различных признаков объекта.

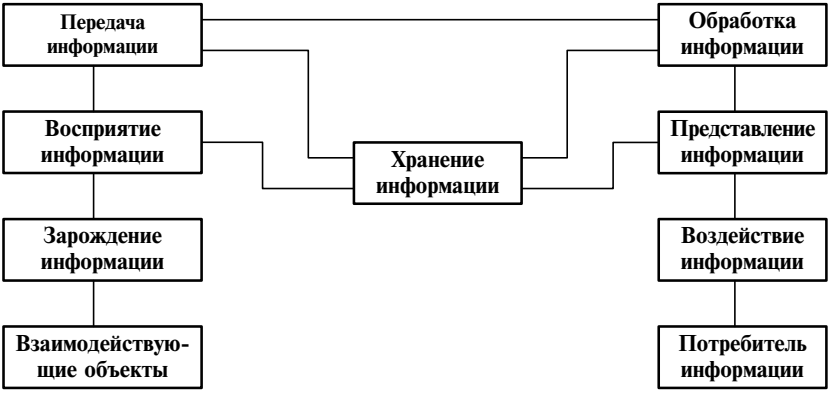


Рис. 1.2. **Структура информационного процесса**

Независимо от принципиального различия в восприятии информации человеком и компьютером информационный процесс всегда начинается с восприятия и выделения информации. Сама информация — это содержание сигнала, который удобен для передачи по физическим каналам связи — электрическим, акустическим, оптическим и т.д.

Прием информации — вторичное ее восприятие другим субъектом или принимающим устройством.

Обработка информации осуществляется человеком или техническим устройством, в частности компьютером. Сущность обработки информации компьютером — аналоговое или цифровое преобразование поступающих данных по жесткой программе или алгоритму обработки. Для успешной обработки информации и решения задачи ЭВМ должна иметь небольшой набор переменных. Человек, в отличие от компьютера, способен проводить смысловую и логическую обработку информации.

Завершается информационный процесс *представлением информации* потребителю, т.е. демонстрацией на индикаторах различного вида изображений и принятием решения.

Особая стадия информационного процесса — *хранение информации*. Она занимает промежуточное положение между другими стадиями и может реализовываться на любом этапе информационного процесса.

Таким образом, *компьютер может быть использован на любой стадии информационного процесса, начиная от восприятия и кончая воздействием информации, в чем и состоит его ключевая роль и значение.*

Конкретное содержание каждого информационного процесса определяется той областью деятельности, где обрабатывается информация.

Информационные процессы отличаются по степени сложности. Пример достаточно простого информационного процесса — копирование информации. К наиболее сложным относятся процессы управления.

Управление — это информационный процесс, изменение состояния системы, ведущее к достижению поставленной цели. При этом реализуются принципы прямой и обратной связи, что позволяет не только получать желаемые результаты, но и вести учет и контроль за действительным ходом процесса и воздействовать на него в направлении желательных изменений с целью получения наименьших отклонений системы от расчетных параметров.

Оперирование информацией влечет за собой множество проблем: поиск, кодирование, защита, хранение и т.п.

Реальные системы управления отличаются большой сложностью и большим разнообразием (рис. 1.3). Они могут содержать несколько каналов управляющей информации и обратной связи.

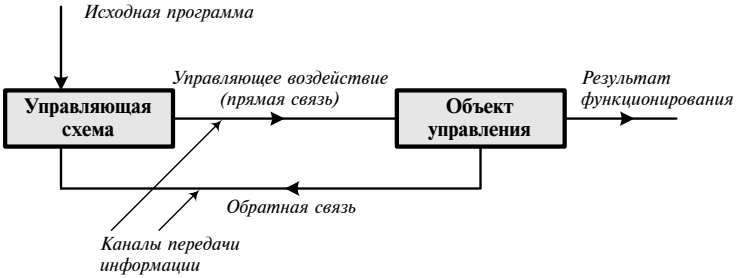


Рис 1.3. **Общая схема управления (кибернетическая схема)**

Примеры.

1. Управление автомобилем;

2. Планирование развития хозяйства страны.

Изучением общих свойств процессов управления в неживой природе, живых организмах и обществе занимается *кибернетика*, которая является предшественницей *информатики*.

Информатика как наука

Информатика — фундаментальная естественная наука, изучающая все аспекты получения, хранения, переработки и использования информации с помощью ЭВМ и других технических средств.

Информатика — научное направление, занимающееся изучением законов, методов и способов накапливания, обработки и передачи информации с помощью ЭВМ и других технических средств; группа дисциплин, занимающихся различными аспектами применения и разработки ЭВМ: прикладная математика, программирование, программное обеспечение, искусственный интеллект, архитектура ЭВМ, вычислительные сети (толковый словарь по информатике).

Важно отметить, что:

1) информатика занимается изучением наиболее общих вопросов обработки информации, информации вообще, в то время как другие науки занимаются обработкой информации, которая составляет содержание лишь данных наук;

2) информатика имеет дело лишь с машинной обработкой информации.

Само название «информатика» произошло от немецкого и французского (*Informatik*, *informatique*), так на этих языках называется эта наука. По-английски название науки «*Computer Science*» ясно указывает на компьютерный способ обработки информации. Наука информатика начала свое становление лишь с 50-х годов XX в., когда появились первые компьютеры. До того времени методы обработки информации, конечно, существовали (вспомним, например, библиотечные или больничные каталоги), но они не имели общей серьезной научной основы. Та основа, которая использовалась ими, могла быть описана в популярной статье в журнале «Наука и жизнь» в разделе «Научная организация умственного труда». По-настоящему научная основа для обработки информации появилась лишь при использовании компьютеров.

Как и другие науки, которые принято делить на теоретические и прикладные (например, физику, биологию), информатика тоже состоит из научных направлений, которые можно назвать теоретической и прикладной информатикой. Каждый из этих разделов в свою очередь можно делить и дальше. Рассмотрим основные направления информатики.

Основные направления информатики

1. *Теоретическая информатика.* Это математическая дисциплина, она использует методы математики для построения и изучения моделей обработки, передачи и использования информации, создает тот теоретический фундамент, на котором строится все здание информатики. Она распадается на ряд самостоятельных дисциплин. Их можно разделить на пять классов.

➤ *Дисциплины, опирающиеся на математическую логику.* В них разрабатываются методы, позволяющие использовать достижения логики

для анализа процессов переработки информации с помощью компьютеров.

➤ *Дисциплины, лежащие на границе между дискретной математикой и теоретической информатикой* (вычислительная математика и вычислительная геометрия). Эти науки направлены на создание методов, ориентированных на реализацию в компьютерах.

➤ *Теория информации* и *теория кодирования* занимаются выявлением общих свойств информации и изучением тех форм, в которых содержатся конкретные информационные единицы. Специальный раздел занимается теоретическими вопросами передачи информации по каналам связи.

➤ *Системный анализ* изучает структуру реальных объектов и дает способы их формализованного описания. Системный анализ занимает пограничное положение между теоретической информатикой и кибернетикой. Такое же положение занимают *имитационное моделирование* (воспроизведение процессов, протекающих в реальных объектах, в тех моделях объектов, которые реализуются на ЭВМ) и *системы массового обслуживания*.

➤ Дисциплины, ориентированные на использование информации для принятия решений в самых различных ситуациях (*теория принятия решений, теория игр*). При организации поведения, ведущего к нужной цели, принимать решения приходится многократно. Поэтому выбор отдельных решений должен подчиняться общему плану. Этим занимается *исследование операций*.

2. *Кибернетика.* Наука об управлении в живых, неживых и искусственных системах. Кибернетика может рассматриваться как прикладная информатика в области создания и использования автоматических или автоматизированных систем управления разной степени сложности, от управления отдельным объектом (станком, промышленной установкой, автомобилем и т.п.) до сложнейших систем управления целыми отраслями промышленности, банковскими системами, системами связи и даже сообществами людей. Наиболее активно развивается техническая кибернетика, результаты которой используются для целей управления в промышленности и науке.

3. *Программирование.* Эта дисциплина полностью связана с вычислительными машинами. Включает создание отдельных программ и пакетов прикладных программ, разработку языков программирования, создание операционных систем, организацию взаимодействия компьютеров с помощью протоколов связи.

4. *Искусственный интеллект* (ИИ)**.** Основная цель работ в области ИИ — стремление проникнуть в тайны творческой деятельности людей, их способности к овладению навыками, знаниями и умениями. Для этого необходимо раскрыть те глубинные механизмы, с помощью

которых человек способен научиться практически любому виду деятельности. Если суть этих механизмов будет разгадана, то удастся реализовать их подобие в искусственных системах. Искусственный интелект — наука не чисто теоретическая, она занимается и прикладными вопросами, например робототехникой (создание роботов), созданием баз знаний и экспертных систем на основе этих баз знаний. Некоторые из экспертных систем находят применение в юридической деятельности («Маньяк», «Блок» — раскрытие хищений в строительстве и т.п.).

5. ***Информационные системы*** (ИС). Человеко-машинные системы, предназначенные для хранения, поиска и выдачи информации по запросам пользователей.

Современное состояние развития информационных систем и технологий в США, странах Западной Европы и Японии характеризуется, в частности, следующими тенденциями:

1) созданием большого количества банков данных большого объема, содержащих информацию практически по всем видам деятельности общества;

2) созданием локальных, многофункциональных проблемно-ориентированных информационных систем различного назначения.

В России наблюдаются аналогичные тенденции. Созданы банки данных, содержащие научную, технологическую и другую информацию, в том числе правовую (системы «Кодекс», «Гарант», «КонсультантПлюс» и др.). В органах внутренних дел информация хранится в форме различных учетов (дактилоскопический, пофамильный, учеты похищенных и обнаруженных вещей, пулегильзотеки и др.). Часть из них переведена в электронную форму, однако это лишь относительно небольшая часть. Задача перевода всех учетов в электронную форму и организация доступа к ним через вычислительную сеть является одной из наиболее актуальных.

Для организации доступа к централизованно или распределенно хранящейся информации создаются информационно-вычислительные сети разного уровня. Для этого необходима разработка специфического оборудования, программного обеспечения, развитие средств связи и коммуникации (последнее особенно актуально для России с ее большими расстояниями и традиционно плохим качеством линий связи).

6. ***Вычислительная техника.*** Развитие вычислительной техники — это самостоятельное направление, в котором часть задач не имеет прямого отношения к информатике (микроэлектроника). Однако при разработке, проектировании и производстве компьютерной техники наиболее широко используются достижения информатики (рис. 1.4).

Рис. 1.4. **Информатика в Юридическом институте**

1.2. Принципы устройства и работы ЭВМ

Структурная организация ЭВМ. Принципы Неймана

Обобщенная структурная схема ЭВМ включает пять основных функциональных блоков: устройство ввода (УВв), запоминающее устройство (ЗУ), арифметико-логическое устройство (АЛУ), устройство управления (УУ) и устройство вывода информации (УВыв).

Чтобы понять назначение и взаимосвязь основных устройств ЭВМ, необходимо рассмотреть последовательность прохождения информации при ее обработке (рис. 1.5).

В основе организации вычислительного процесса на машине лежит принцип программного управления. Для решения задачи на ЭВМ необходимо составить программу.

Программа *— определенная последовательность команд* (*инструкций*), *которая обеспечивает выполнение задачи.*

Пользователь записывает программу на каком-либо алгоритмическом языке. Однако компьютер работает под управлением программы, переведенной с алгоритмического на машинный язык, который является собственным языком программирования машины.

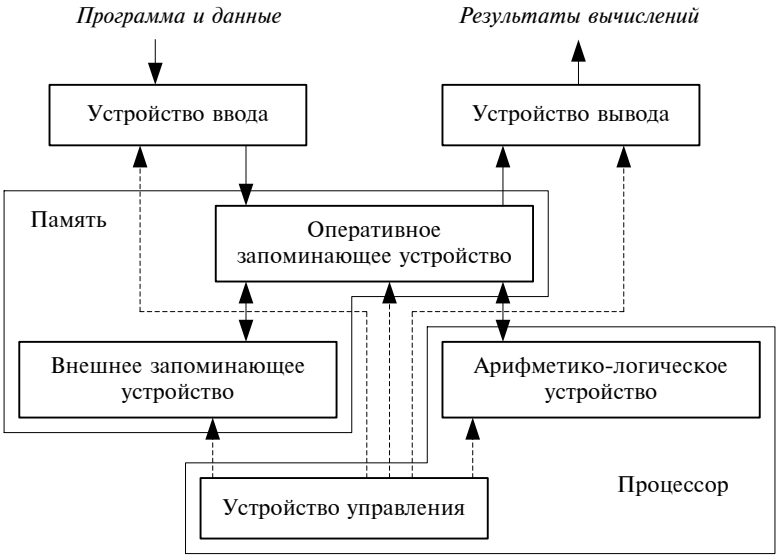


Рис. 1.5. **Обобщенная структурная схема ЭВМ неймановского типа**

Программа, а также исходная информация вводятся с промежуточного машинного носителя (например, с магнитной ленты, перфокарты и т.п.) или напрямую с клавиатуры.

Информация, зафиксированная на машинных носителях, вводится в ЭВМ через ***устройство ввода***, с помощью которого закодированная на носителе информация преобразуется в электрические сигналы и передается в запоминающее устройство.

Основной функцией запоминающих устройств (памяти ЭВМ) является хранение программ и данных, необходимых для решения задачи, а также промежуточных и окончательных результатов вычислений.

Пользователя ЭВМ интересуют прежде всего такие характеристики, как емкость памяти и ее быстродействие.

Емкость памяти определяется максимально возможным количеством кодов чисел и команд определенной разрядности, которые могут одновременно храниться в запоминающем устройстве.

Быстродействие памяти характеризуется временем, которое необходимо для поиска (выборки), записи или считывания данных (*время доступа к памяти*).

Эти две характеристики взаимопротиворечивы (увеличение емкости может привести к снижению быстродействия), поэтому для удовлетворения требований высокого быстродействия и большой емкости памяти в ЭВМ включается набор запоминающих устройств, построенных на различных физических принципах.

В ЭВМ всегда имеется не менее двух типов ЗУ: оперативное запоминающее устройство (ОЗУ) и внешнее запоминающее устройство (ВЗУ).

Оперативное запоминающее устройство используется непосредственно при выполнении операций вычислительного процесса и имеет сравнительно небольшую емкость. Его главное достоинство — высокое быстродействие (время доступа — десятки и сотни наносекунд), которое достигается за счет *прямого доступа к регистрам* памяти. Это реализуется чисто электронным способом. Недостатки — относительно высокая стоимость и *энергозависимость*: при выключении ЭВМ все данные, хранящиеся в ОЗУ, пропадают.

Внешнее запоминающее устройство предназначено для хранения промежуточных результатов, участков программ и массивов, исходных данных, не уместившихся в ОЗУ; ВЗУ обладает сравнительно невысокой скоростью работы (время доступа — микросекунды, десятые доли секунды и даже десятки секунд). При этом емкость памяти практически не ограничена. Этот вид памяти может обеспечивать *прямой доступ* (магнитный диск) или *последовательный доступ* (магнитная лента) к данным. В любом случае реализация доступа является не чисто электронной, а электронно-механической, поэтому быстродействие во много раз ниже, чем у ОЗУ; ВЗУ является энергонезависимым устройством.

Кроме ОЗУ и ВЗУ в ЭВМ используются и другие виды памяти, в частности ***постоянная память*** (ПЗУ) — часть *основной памяти*[1], размещаемая в электронном устройстве, обеспечивающем постоянное хранение данных. В этом случае вместе с преимуществами оперативной памяти (быстродействие, прямой доступ), обеспечивается одно из важнейших преимуществ внешней памяти — энергонезависимость.

Преобразование информации происходит в ***арифметико-логическом устройстве*** (АЛУ), которое выполняет арифметические операции (например, сложение и умножение) и логические операции (сравнение, инверсия).

---

[1] Основная память включает ОЗУ, ПЗУ и разновидности кэш-памяти.

Устройства вывода представляют результаты обработки данных либо в удобной форме для визуального восприятия человеком — печатают на бумаге или отображают на дисплее, либо в форме, удобной для передачи на другие устройства, — на машинных носителях, по линиям связи. Результаты решения задачи передаются в УВыв из оперативной памяти.

Часто совокупность устройств ввода и вывода принято называть ***устройствами ввода-вывода*** (УВвВыв). Это связано с тем, что некоторые устройства, например дисплеи, телетайпы, могут применяться как для ввода, так и для вывода данных.

Согласование работы описанных устройств осуществляет ***устройство управления*** (УУ). Оно реализует программный принцип управления на основе хранимой в памяти машины программы, контролирует взаимодействие между различными устройствами и блоками вычислительной машины, определяет последовательность операций в соответствии с заданным преобразованием данных в процессе решения задачи.

Совокупность устройств ЭВМ, включающая устройство управления, арифметико-логическое устройство, внутреннюю регистровую память, принято называть ***центральным процессором***.

Упрощенная *схема вычислительного процесса* может быть описана следующим образом (см. рис. 1.5). По указанию УУ управляющая информация (команда) считывается из оперативного запоминающего устройства, передается в УУ и расшифровывается. Она определяет, какая операция и над какими данными должна выполняться в АЛУ. Получив соответствующие числа и адреса, ОЗУ выдает требуемые числа в АЛУ, где они преобразуются. Результаты обработки пересылаются в ОЗУ на хранение. Окончательная результатная информация из ОЗУ с помощью устройств вывода поступает на дисплей, печатающее устройство, на машинный носитель или для передачи по линиям связи.

Принципы устройства и работы вычислительных машин описанного выше типа были впервые описаны группой американских ученых — разработчиков одной из первых в мире ЭВМ «ЭНИАК» — на основе критического анализа результатов функционирования машины. Главным теоретиком проекта был Джон фон Нейман, поэтому такой тип ЭВМ получил название «***машины с неймановской архитектурой***». Эти п р и н ц и п ы следующие:

1. ЭВМ должна создаваться на *электронной основе* и работать в *двоичной системе счисления*.

2. В *состав ЭВМ* должны входить АЛУ, центральное устройство управления, запоминающие устройства (в том числе ОЗУ для данных и команд и связанное с ним ВЗУ большой емкости), устройства ввода данных и вывода результатов.

3. Программа для ЭВМ хранится в оперативной памяти машины вместе с данными (*принцип хранимой программы*).

4. Время доступа к ячейке памяти не зависит от ее номера (*принцип прямого доступа к памяти*).

5. *В системе команд* должны быть команды условной и безусловной передачи управления.

Рассмотренные принципы были реализованы практически во всех компьютерах 60-х — 80-х годов. И в настоящее время большинство компьютеров, в том числе и персональные, имеет «неймановскую» архитектуру.

Представление данных в ЭВМ

Информация, участвующая в процессе обработки в ЭВМ, может быть разбита на т р и г р у п п ы.

➤ ***Системные данные*** содержат сведения о состоянии ЭВМ, отдельных устройств и выполняемой программе. Они входят в состав системного программного обеспечения, являются постоянными и разрабатываются одновременно с аппаратной частью ЭВМ.

➤ ***Обрабатываемые данные*** — это данные, которые преобразуются в вычислительном процессе. Они включают исходные данные и результаты. Данные могут быть числовыми, логическими и текстовыми.

➤ ***Программные данные*** представляют собой набор команд программ, которые обеспечивают решение задач на ЭВМ. Они формируются программистом для каждой конкретной задачи.

Для кодирования любой информации в ЭВМ используется двоичная система счисления, так как вычислительные машины выполнены на двухпозиционных электронных элементах. Двухпозиционные элементы в каждый момент времени находятся в одном из двух устойчивых состояний, которые соответствуют знакам двоичной системы счисления: единице или нулю.

Во внешней памяти ЭВМ данные хранятся в виде файлов. ***Файл*** — целостная поименованная совокупность данных на внешнем носителе информации (например, в виде участка намагниченности на магнитном диске или на магнитной ленте). Файл может представлять собой программу, текст, рисунок, базу данных и т.п. Поэтому файлы называют программными, текстовыми, графическими, файлами баз данных и др.

Этапы подготовки и решения задач на ЭВМ

Решение любой задачи на ЭВМ представляет собой процесс обработки данных с помощью программы. Создание такой программы предполагает выполнение ряда последовательных этапов (рис. 1.6).

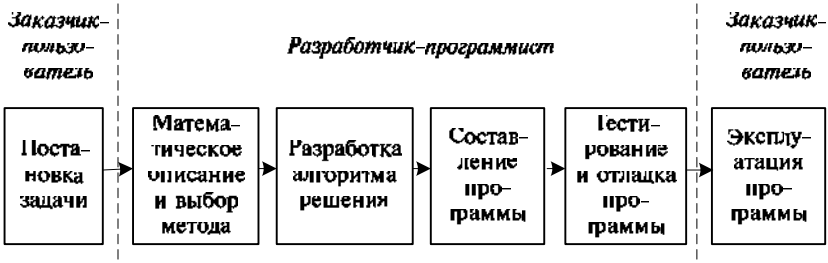


Рис. 1.6. **Этапы подготовки и решения задач на ЭВМ**

➤ *Первый этап* представляет собой ***постановку задачи***. На этом этапе формулируется цель задачи, определяется взаимосвязь с другими задачами, раскрывается состав и форма представления входной, промежуточной и результатной информации, характеризуются формы и методы контроля достоверности информации на ключевых этапах решения задачи, определяются формы взаимодействия пользователя с ЭВМ в ходе решения задачи и т.п.

➤ *Второй этап* — ***формализованное описание задачи***, т.е. устанавливаются и формулируются средствами языка математики логико-математические зависимости между исходными и результатными данными. Для задач, допускающих возможность математического описания, необходимо выбрать численный метод решения, а для нечисловых задач — принципиальную схему решения в виде однозначно понимаемой последовательности выполнения элементарных математических и логических операций.

➤ *Третий этап* — ***алгоритмизация*** решения задачи, т.е. разработка оригинального или адаптация известного алгоритма. Алгоритмизация — это сложный процесс, носящий в значительной степени творческий характер. Постановка задачи и ее алгоритмизация составляют до 20—30% общего времени на разработку программы. Сложность и ответственность реализации данного этапа объясняется тем, что для решения одной и той же задачи, как правило, существует множество различных алгоритмов, отличающихся друг от друга уровнем сложности, объемами вычислительных работ и другими факторами.

Алгоритм — это точное предписание, определяющее вычислительный процесс, ведущий от варьируемых начальных данных к искомому результату. Это конечный набор правил, однозначно раскрывающих содержание и последовательность выполнения операций для систематического решения определенного класса задач за конечное число шагов.

➤ *Четвертый этап* — ***составление программы***. На этом этапе производится перевод описания алгоритма на один из доступных для ЭВМ языков программирования.

➤ *Заключительный этап* разработки программы решения задачи на ЭВМ — ***тестирование и отладка***. Оба эти процесса функционально связаны между собой, хотя их цели несколько отличаются друг от друга.

Тестирование — совокупность действий, предназначенных для демонстрации правильной работы программы. Цель тестирования заключается в выявлении возможных ошибок в разработанных программах путем их проверки на наборе заранее подготовленных контрольных примеров.

Процессу тестирования сопутствует процесс *отладки*, который подразумевает совокупность действий, направленных на устранение ошибок в программе. Действия по отладке начинаются с момента обнаружения фактов ошибочной работы программы и завершаются устранением причин, порождающих ошибки.

По своему характеру о ш и б к и в программах делятся на синтаксические и логические.

Синтаксические ошибки представляют собой некорректную запись отдельных языковых конструкций с точки зрения правил их представления на выбранном языке программирования.

Логические ошибки представляют собой неверное представление логики вычислений.

Процесс тестирования и отладки программ носит итерационный характер и считается одним из наиболее трудоемких этапов процесса разработки программ. Он может составлять 30—50% и более в общей структуре временных затрат и зависит от объема и сложности разрабатываемой программы.

После завершения процессов тестирования и отладки программные средства вместе с сопроводительной документацией передаются пользователю для ***эксплуатации***. Основное назначение сопроводительной документации — обеспечить пользователя необходимыми инструктивными материалами по работе с программой. Как правило, это документы, регламентирующие работу пользователя при эксплуатации программных средств, а также содержащие информацию о программе, необходимую для внесения в нее изменений и дополнений.

Понятие алгоритма, его свойства. Формы записи алгоритмов

Алгоритмы встречаются не только в вычислительной технике, но и в обыденной жизни. Понятие алгоритма было введено выше.

Приведем примеры алгоритмов из обыденной жизни:

а) поездка в институт;

б) ремонт телевизора (по инструкции);

в) поиск пропавшей вещи;

г) выращивание растений на участке и т.п.

Не все задачи могут быть решены с использованием алгоритмов. Например, написание музыки, написание стихов, научное открытие.

Компьютер используется для решения лишь тех задач, для которых может быть составлен алгоритм.

Любой алгоритм обладает следующими свойствами: детерминированностью, массовостью, результативностью и дискретностью.

Детерминированность (определенность) означает, что набор указаний алгоритма должен быть однозначно и точно понят любым исполнителем. Это свойство определяет однозначность результата работы алгоритма при заданных исходных данных.

Массовость алгоритма предполагает возможность варьирования исходных данных в некоторых пределах. Это свойство определяет пригодность использования алгоритма для решения множества конкретных задач определенного класса.

Результативность алгоритма означает, что для любых допустимых исходных данных он должен через конечное число шагов (или итераций) завершить свою работу.

Дискретность алгоритма означает возможность разбиения определенного алгоритмического процесса на отдельные элементарные этапы, возможность реализации которых человеком или компьютером не вызывает сомнения, а результат выполнения каждого элементарного этапа вполне определен и понятен.

Таким образом, алгоритм дает возможность чисто механически решать любую конкретную задачу из некоторого класса однотипных задач. Существует несколько способов описания алгоритмов: словесный, формально-словесный, графический и др.

Словесный способ описания алгоритма отражает содержание выполняемых действий средствами естественного языка. К достоинствам этого способа описания следует отнести его общедоступность, а также возможность описывать алгоритм с любой степенью детализации. К главным недостаткам этого способа следует отнести достаточно громоздкое описание, отсутствие строгой формализации в силу неоднозначности восприятия естественного языка.

Формально-словесный способ описания алгоритма основан на записи содержания выполняемых действий с использованием изобразительных возможностей языка математики, дополненного с целью указания необходимых пояснений средствами естественного языка. Данный способ, обладая всеми достоинствами словесного способа, вместе с тем более лаконичен, а значит, и более нагляден, имеет

большую формализацию, однако также не является строго формальным.

Графический способ описания алгоритмов представляет собой изображение логико-математической структуры алгоритма, при котором все этапы процесса обработки данных представляются с помощью определенного набора геометрических фигур (блоков), имеющих строго определенную конфигурацию в соответствии с характером выполняемых действий.

Для облегчения процесса разработки и восприятия графического изображения алгоритмов их составление осуществляется в соответствии с требованиями ГОСТ 19701—90 «Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения» и ГОСТ 19.003—80 «Схемы алгоритмов и программ. Обозначения условно-графические».

Изображение схем алгоритмов осуществляется по определенным правилам. В соответствии с этими правилами каждая схема должна начинаться и кончаться соответствующими символами, обозначающими начало и окончание алгоритма.

Все блоки в схеме располагаются в последовательности сверху вниз и слева направо, объединяясь между собой *линиями потока.* В этом случае направление линий потока не идентифицируется с помощью стрелок, в отличие от других направлений.

С целью повышения наглядности графические схемы алгоритмов могут сопровождаться кратким формально-словесным описанием внутри условного изображения блоков, раскрывающим содержание выполняемой операции. Для обозначения условной передачи управления от блоков логических операций над соответствующими линиями потока могут записываться специальные знаки операций отношения (<, >, = и другие) или слова «Да» либо «Нет».

Основные виды алгоритмических структур

При всем разнообразии решаемых задач в них можно выделить *три основных* (*канонических*) *вида алгоритмических структур*: линейную, разветвленную и циклическую. С помощью этих трех видов структур можно построить алгоритм любой сложности.

Линейным процессом называется такой алгоритмический процесс, при котором все этапы решения задачи выполняются в естественном порядке следования этих этапов. Для линейной структуры характерно, что порядок выполнения этапов не зависит ни от исходных данных, ни от результатов выполнения предыдущих этапов.

Разветвленным процессом называется такой алгоритмический процесс, в котором выбор направления, а значит, и характера обработки информации зависит от результатов проверки выполнения

какого-либо условия. В зависимости от характера логического условия процесс может состоять из двух и более ветвей. В любой конкретный момент реализации данной структуры осуществляется обработка только по одной из ветвей, а выполнение операций по другим ветвям исключается.

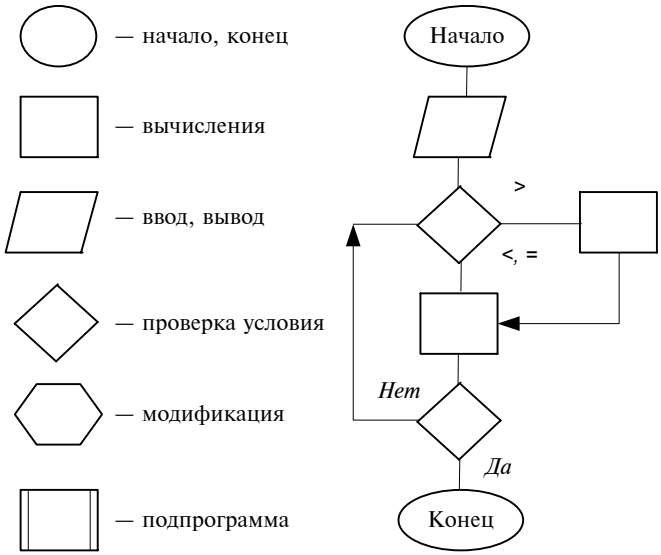


Рис. 1.7. **Основные графические обозначения блоков и программ (*а*) и пример записи схемы алгоритма (*б*)**

Циклический процесс представляет собой алгоритмическую структуру, реализующую многократно повторяющиеся однотипные этапы обработки данных. Многократно повторяющийся участок алгоритма, входящий в циклическую структуру (за исключением этапа проверки условия окончания цикла), называется *телом цикла*. В качестве тела цикла могут выступать линейные, разветвленные или другие циклические структуры, а также сочетания этих структур.

Циклы, не содержащие внутри себя других циклов, называются простыми. Сложные циклы содержат внутри себя, по крайней мере, хотя бы еще одну циклическую структуру. При этом циклы, охватывающие другие циклы, называются внешними, а циклы, входящие в тело внешних, — внутренними.

В зависимости от способа организации числа повторений цикла различают: циклы с заранее заданным количеством повторений; циклы с заранее неизвестным числом повторений (итерационные циклы).

По способу организации порядка исполнения проверки условия окончания цикла различают две разновидности циклических структур: с проверкой условия окончания цикла до и после реализации цикла.

Примеры алгоритмических структур:

1) линейный алгоритм: ввод x, y; вывод $z = x + y$;
2) разветвленный алгоритм: ввод x; вывод $z = |x|$;
3) циклические алгоритмы:
   а) с известным числом повторений: ввод n — целое положительное число; вывод $S = 1 + 2 + ... + (n - 1) + n$;
   б) с неизвестным числом повторений: решение уравнения $y(x) = 0$ численным методом деления отрезка пополам с заданной точностью.

1.3. Структурная схема персонального компьютера

В настоящее время основная работа по информационному обслуживанию управления ведется на персональных ЭВМ, называемых также персональными компьютерами (ПК), *программно и аппаратно совместимыми* с ПК фирмы «IBM». Такие ПК обычно называют IBM PC совместимыми. При работе с такими ПК используется английская терминология, поэтому представляется целесообразным дать ее перевод на русский язык.

- IBM (International Business Machines Corporation) — международная корпорация машин для бизнеса;
- PC (Personel Computer) — персональный компьютер (ПК).

Первые модели IBM PC появились в августе 1981 г. Сейчас эти ПК наиболее распространены во всем мире. В правоохранительных органах IBM PC-совместимыми компьютерами оснащаются все структуры: от центральных аппаратов до отделов на местах. На их базе создаются автоматизированные рабочие места сотрудников.

IBM PC, как и все ЭВМ, включает в себя два основных компонента: оборудование, или аппаратную часть, называемую *hardware*, и программы, или программное обеспечение, называемое *software*; к последнему относятся операционные системы, трансляторы с алгоритмических языков (BASIC, PASCAL, СИ и т.д.), различные прикладные программные системы. Основной операционной системой, используемой в IBM PC-совместимых ПК, до середины 90-х гг. являлась MS DOS (MicroSoft Disk Operating System) — *дисковая операционная система* фирмы «Майкрософт».

В последнее время более широкое распространение на PC-совместимых компьютерах получили операционные системы семейства Windows с графическим интерфейсом работы пользователя.

Операционная система обеспечивает решение двух главных задач:

- предоставление пользователям возможности общего управления компьютером;
- поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой.

К *hardware* относятся следующие устройства:

- CPU (*Central Proceccing Unit*) — центральное процессорное устройство (ЦПУ), выполненное на основе микропроцессора фирмы *Intel Corporation*, называемое также *Central processor* — Центральный процессор (ЦП);
- ALU (*Arithmetic Logical Unit*) — арифметико-логическое устройство (АЛУ);
- CU (*Control Unit*) — устройство управления (УУ);
- *Controller* — контроллер (УУ подсистемами ПК);
- ROM (*Read Only Memory*) — постоянное запоминающее устройство (ПЗУ);
- устройства ввода-вывода:
  monitor — монитор (дисплей, экран);
  printer — принтер (печатающее устройство);
  keyboard — клавиатура.
- MSD (*Mass Storage Device*) — устройство массового хранения (память на накопителях, внешнее запоминающее устройство);
- *disk drive* — дисковод (устройство для считывания и записи информации на магнитные диски);
- *hard disk drive, winchester disk* — накопитель на жестком магнитном диске (НМД), винчестерский диск (винчестер);
- *floppy disk drive* — накопитель на гибком магнитном диске (НГМД), на дискете, флоппи-диске.

Большинство из перечисленных компонентов IBM PC объединены в ***системный блок*** (*system unit*).

Основным блоком IBM PC является центральное процессорное устройство (CPU), состоящее из арифметико-логического устройства (ALU) и устройства управления (CU):

- ALU осуществляет с данными операции сложения, вычитания, умножения, деления, сравнения и т.д.;
- CU устанавливает очередность выполнения операций, управляет потоками данных внутри и между блоками IBM PC.

Память ПК состоит из ОЗУ (RAM) и ПЗУ (ROM), а также памяти на накопителях (MSD) (рис. 1.8):

➤ ROM реализован на микросхемах, информация с которых может только считываться, не изменяясь при этом. ROM ПК содержит BIOS (*basic input/output system*) — *базовую систему ввода/вывода*, являющуюся первым основным компонентом операционной системы MS DOS.

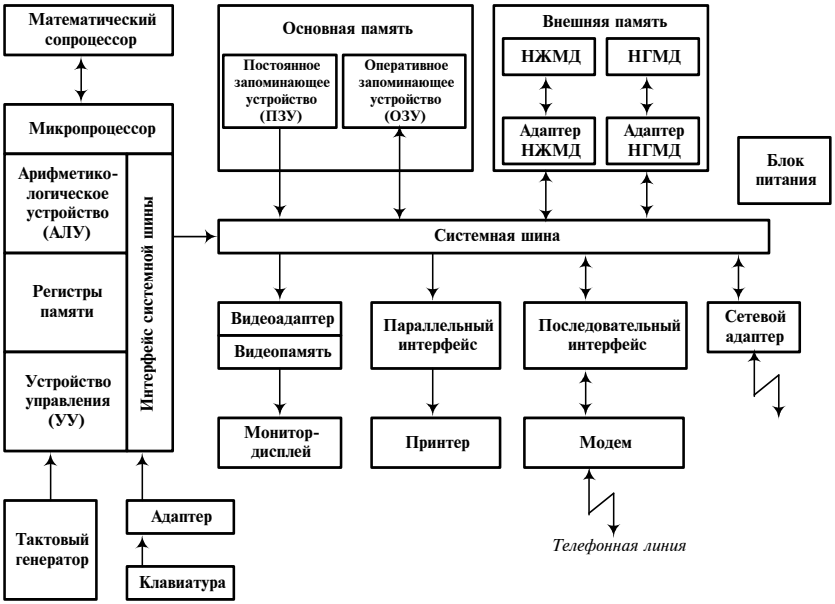


Рис. 1.8. **Структурная схема ПК**

BIOS выполняет следующие ф у н к ц и и:

- устанавливает, какие устройства подключены к ПК, т.е. выясняет конфигурацию системы;
- организует взаимосвязь между устройствами;
- определяет местоположение загрузочной части операционной системы и передает ей управление.

➤ RAM состоит из микросхем, которые временно хранят информацию. При отключении питания компьютера информация из RAM пропадает.

В MS DOS RAM делится на к а т е г о р и и:

- *базовую память* — объемом 640 Кбайт, доступную всем программам, работающим под управлением MS DOS;
- *наращенную память* — за пределами 1 Мбайт, для использования которой нужны особые программные средства в MS DOS или другие ОС (например, OS/2);
- *расширенную память* — выход в нее осуществляется из верхней области памяти (от 640 Кбайт до 1 Мбайт).

Сигналы и данные между блоками ПК объединяются в потоки и передаются по шинам. В IBM PC — совместимых ПК имеются т р и с т а н д а р т н ы е ш и н ы:

- *шина данных,* по которой передаются собственно данные («что передавать»);

- *шина адреса,* по которой передаются адреса данных («куда и откуда передавать»);
- *шина управления,* по которой передаются команды управления данными («как передавать»).

Таблица 1.1. ***Логическая структура основной памяти***

Основная память (*Base Memory*)		*Расширенная память* (EMA)	**Всего памяти**
Стандартная память	Верхняя память (UMB)	Высокая память (HMA)	
640 Кбайт	384 Кбайт	64 Кбайт	**1024 Кбайт**

Большинство устройств ввода-вывода IBM PC содержат устройства сопряжения сигналов и данных между блоками и собственные CU, называемые *адаптерами* и *контроллерами*, а также собственную память для хранения данных при обмене (такую память имеют, например, монитор и принтер).

Дисководы НГМД считывают и записывают информацию на дискеты. До последнего времени использовались дискеты двух типов: диаметрами 5,25 и 3,5 дюйма (1 дюйм = 2,54 см). На дискетах обычно указывается следующая маркировка:

- DS,2S (*Double Side*) — двусторонние;
- DD,2D (*Double Density*) — двойной плотности;
- HD (*High Density*) — высокой плотности.

Перед записью информации на дискету она должна быть отформатирована. Максимальный объем информации на дискетах двух указанных выше типов при различном форматировании приведен в табл. 1.2.

Таблица 1.2. ***Возможность использования дисководов при работе с дискетами различных типов***

Дисководы / *Дискеты*	5,25″ DD	5,25″ HD	3,5″ DD	3,5″ HD
5,25″ DD	360	360		
5,25″ HD	360	1200		
3,5″ DD			720	720
3,5″ HD			720	1440

➤ *Устройства памяти на дисковых накопителях* — основные устройства ПК для долговременного хранения больших объемов данных и программ. К ним относятся накопители на жестких маг-

нитных дисках (НЖМД), накопители на основе компакт-дисков (CD-ROM), накопители на магнитооптических дисках (НМОД).

Основными параметрами устройств памяти на накопителях являются *емкость* и *производительность*. Емкость определяется физическими принципами чтения/записи данных на носители и зависит от технологии их изготовления. Производительность дисковых накопителей напрямую зависит от таких параметров, как *среднее время доступа* к данным (определяется временем поиска сектора данных на диске и скоростью вращения диска) и *скорость передачи данных* (определяется в первую очередь характеристиками интерфейса контроллера накопителя).

Характеристики основных дисковых накопителей приведены в табл. 1.3.

Таблица 1.3. ***Характеристики дисковых накопителей***

Тип накопителя	*Емкость,* Мбайт	*Время доступа*, мс	*Скорость передачи**, Кбайт/с	*Вид доступа***
НГМД	1,2; 1,44	65—100	150	Ч/З
НЖМД	250—8000	8—20	500—5000	Ч/З
CD-ROM	250—1500	15—300	150—1500	Ч
НМОД	100—1300	15—150	300—2000	Ч/З
Бернулли	20—230	20	500—2000	Ч/З
CD-WORM	120—1000	15—150	150—1500	Ч/З***
DVD	4000—16000			Ч

* Средние скорости передачи в режимах «чтение/запись».

** Ч — чтение; З — запись.

*** Запись однократная.

Важнейший принцип построения IBM PC-совместимых ПК — ***открытая архитектура*** — означает модульный принцип построения и возможность замены блоков на новые по мере развития. В IBM PC имеются специальные разъемы расширения для подключения дополнительных устройств, таких как дополнительная память, сопроцессор, джойстик (координатная ручка), мышь (устройство ввода координат), плоттер (графопостроитель), сканер (устройство ввода изображений), стример (запоминающее устройство на магнитной ленте), модем (устройство для подключения к телефонной линии связи и обмена информацией с другими компьютерами).

При разработке *hardware* и *software* для IBM PC-совместимых 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 IBM PC, привели к созданию семейства IBM-совместимых ПК, которое называется «клоном» IBM. Первая модель этого семейства появилась в 1982 г. и называлась IBM PCjr. Родословное дерево PC представлено на рис. 1.9.

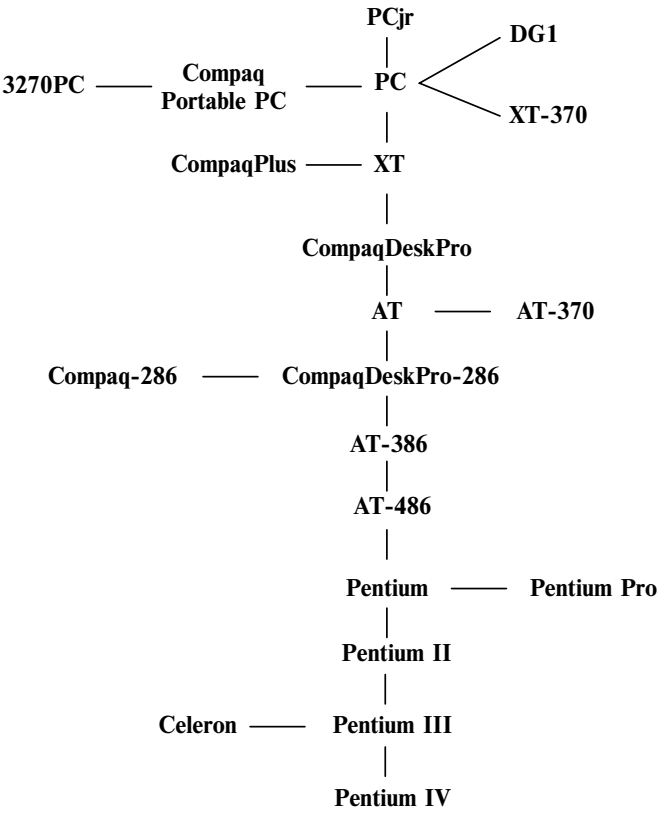


Рис. 1.9. **Семейство IBM PC-совместимых ПК**

Центральная линия обозначает главную ветвь семейства, на которой модели располагаются в соответствии с их мощностями — от наименее мощной PCjr до наиболее мощной AT/486; ветви — 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 80 286;

- IBM PC/AT/386 и IBM PC/AT/486 — на микропроцессорах Intel 80 386 и Intel 80 486, 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 главным образом именно типом используемого микропроцессора.

Intel 8088 разработан в 1979 г., имел 8-разрядную шину данных и 20-разрядную адресную шину, т.е. адресуемый RAM до 1 Мбайт. Intel 80 286, 1982 г. создания, имел 16-разрядную шину данных и 24-разрядную адресную шину, т.е. адресовался к RAM до 16 Мбайт. Intel 80 386 и 80 486 имели 32-битные шины данных и адреса, т.е. доступный RAM до 4 Гбайт.

Микропроцессор (МП) конструктивно представляет собой кристалл кремния, в котором в результате технологического процесса создана электронная схема. Количество электронных компонентов (транзисторов) в этой схеме: от десятков тысяч до нескольких миллионов. Кристалл помещен в пластиковый корпус, а выводы выходят наружу, как у типичной микросхемы широкого применения.

Стоимость компьютера в значительной степени определяется стоимостью МП, однако себестоимость производства одного экземпляра очень мала. Основная доля затрат приходится на разработку технологии производства.

Основные характеристики микропроцессора:

- максимальная тактовая частота;
- разрядность;
- тип архитектуры.

➤ ***Тактовая частота.*** Вычислительный процесс представляет собой последовательность элементарных действий, выполнение которых синхронизируется тактовым генератором. Превышение тактовой частоты выше некоторого предела может привести к срыву вычислений или перегреву МП. Таким образом, максимальная тактовая частота определяет быстродействие процессора (но она не равна быстродействию МП и тем более быстродействию компьютера).

➤ ***Разрядность процессора.*** Этим термином обозначается максимальное количество разрядов двоичного кода, которое может вырабатываться и передаваться одновременно.

Разрядность определяется тремя параметрами: *m*/*n*/*k*:

- *m* — разрядность внутренних регистров, т.е. количество разрядов, с помощью которых обмениваются информацией внутренние устройства МП;
- *n* — разрядность шины данных, которая представляет собой часть системной шины, показывает количество разрядов, че-

рез которые МП обменивается данными с различными устройствами;

- *k* — разрядность шины адреса, определяет объем доступной для МП части ОП.

Основные типы и характеристики микропроцессоров фирмы «Intel», являющейся лидером по производству микропроцессоров для IBM PC-совместимых ПК, приведены в табл. 1.4.

Таблица 1.4. ***Типы и характеристики МП*** **(Intel)**

Тип МП	*Марка ПК*	*m*	*n*	*k*	*Максимальная тактовая частота, МГц*	*Максимальный объем ОЗУ, Мбайт*	*Год создания*
8086	PC	16	16	20	4,77	1	1976
8088	PC XT	16	8	20	10	1	1977
80 286	AT-286	16	16	24	10—33	16	1982
80 386	AT-386	32	32	32	33	4000	1985
80 486	AT-486	32	32	32	33—100	4000	1989
Pentium	Pentium	64	64	32	66—150	4000	1993
Pentium II	Pentium	64	64	32	200—400	4000	1998
Pentium III	Pentium III	64	64	32	500—1000	4000	2000
Pentium IV	Pentium IV	64	64	32	1,5—2000	4000	2001

➤ ***Тип архитектуры МП.*** Микропроцессор представляет собой довольно сложное электронное устройство, в котором отдельные части связаны информационными каналами. Часть этих каналов фиксирована при создании МП, другая часть может изменяться при программировании — в целом это образует архитектуру МП.

Более широкое представление об архитектуре МП — организация МП с точки зрения пользователя. Она включает в себя пользовательские возможности программирования, а именно: состав регистров, систему команд, способы адресации, организацию памяти, средства ввода-вывода и типы обрабатываемых данных.

К наиболее важным аспектам архитектуры относятся:

- система команд и способы адресации;
- возможность выполнения тех или иных команд во времени;
- наличие дополнительных узлов и устройств в составе МП (например, интегрированной *кэш-памяти*, устройства для работы с числами с плавающей точкой — *сопроцессора математики*);
- режим работы.

Другие критерии классификации МП.

➤ ***По системе команд.*** CISC (*complex information system command*, сложная система команд), RISC (*reduced information system command*, сокращенная система команд). При использовании первых число встроенных в МП команд очень велико, например для 8086 и 8088 оно составляет 134, а для МП Pentium — 240. Число встроенных в CISC МП команд увеличивается за счет добавления команд обработки графики и звука. Сложные команды выполняются за несколько тактов, вырабатываемых тактовым генератором, так же как и набор простых команд. При использовании RISK МП количество встроенных команд невелико, каждая команда выполняется за один или два такта. Сложные команды программируются на машинном языке. В целом быстродействие МП, при прочих одинаковых характеристиках, увеличивается.

➤ ***По универсальности.*** *Универсальные МП* выполняют все действия, в то время как *специализированные* предназначены для выполнения только определенного класса задач, при этом их быстродействие намного превышает быстродействие универсальных МП. Очень часто используют математические процессоры, которые могут дополнять соответствующие универсальные и поэтому называются *сопроцессорами*:

- 8088 — 8087;
- 80 286 — 80 287.

В МП фирмы «Intel», начиная с 80 486, математические сопроцессоры встраиваются в один блок с центральным процессором.

Очень важную роль в составе ПК играет *видеоподсистема,* состоящая из монитора и видеокарты. В настоящее время большинство функций построения изображения в ПК выполняет отдельный блок, получивший название *видеоадаптер.* Аппаратно чаще всего он бывает выполнен в виде отдельной платы, вставляемой в разъем расширения материнской платы.

Основными параметрами видеоподсистемы являются:

- разрешающая способность — количество точек на экране монитора;
- цветовое разрешение — количество цветов, которое может иметь отдельная точка;
- частота развертки — скорость обновления изображения экрана.

Графические адаптеры (видеоадаптеры), которые используются в ПК, бывают следующих типов:

- MDA — монохромный адаптер, работает в текстовом режиме, 25 строк по 80 символов в строке, с разрешением 720 × 350 точек, с двумя градациями яркости (черный — белый);
- EGA (*Enhanced Graphics Adapter*) — улучшенный графический адаптер, работающий в режимах: 1) *текстовом* (25 или 43 строки на экране по 80 символов в строке, 16 цветов), 2) *графи-*

ческом (640 точек по горизонтали, 350 по вертикали, 16 цветов и 64 оттенка каждого цвета);

- VGA (*Video Graphics Array*) — видеографическая матрица, графический режим 640 × 480 точек, 16 цветов, 4096 оттенков или 320 × 200 точек, 256 цветов;
- SVGA (*Super VGA*) — до 1280 × 1024 точек при 16 Мбайт цветов и выше.

Таблица 1.5. ***Характеристики видеоадаптеров***

Характеристика	*MDA*	*CGA*	*EGA*	*VGA*	*SVGA*
Разрешающая способность — количество пикселей (по горизонтали × × по вертикали)	720×350	640×200 320×200	640×350 720×350	720×350 640×480	800×600 1024×768
Количество цветов		2 16	16	16 256	16 256
Число символов (строка×столбец*)	80×25	80×25	80×25	80×25 80×50	80×25 80×50
Видеопамять, Кбайт	64	128	128/512	256/512	512/1024
Емкость видеопамяти**	1	4	4—8	8	8
Матрица символа (пикселей по горизонтали × по вертикали)	14×9	8×8	8×8 14×8	8×8 14×8	8×8 14×8
Частота развертки, Гц	50	60	60	60	75

* Текстовый режим.

** Число страниц в текстовом режиме.

Следует заметить, что развитию графической подсистемы персональных компьютеров уделяется 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 1024 × 768 при размере экрана монитора 17 дюймов. При работе с компьютерной графикой и компьютерной верстkой соответствующие параметры должны быть больше: 1280 × 1024 и 19 дюймов. Нормальным цветовым разрешением в настоящий момент считается 65 тысяч цветов (режим High Color), а наиболее эргономичным — 16,7 млн цветов (режим True Color).

Для работы с такими параметрами требуются значительные объемы видеопамяти. Так, для работы в режиме True Color с разрешением 1280 × 1024 на экране 19 дюймов требуется 8 Мбайт видеопамяти.

Требования, предъявляемые к видеоподсистеме ПК, 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, основная задача которых — освободить центральный процессор компьютера от работы по построению трехмерных изображений, которая связана с большим количеством вычислений с числами с плавающей запятой.

Контрольные вопросы и задания

1. Объясните основные свойства информации: *а*) количество информации зависит от того, кто ее получает; *б*) количество информации постоянно увеличивается.
2. Что такое *информационный взрыв*, насколько велики его возможные угрозы и как его предотвратить?
3. Что такое *информационное общество*?
4. Что понимается под информационной преступностью и компьютерными преступлениями?
5. Назовите основные виды представления информации.
6. Дайте математическое понятие информации.
7. Назовите основные направления информатики.
8. Назовите перспективы и тенденции развития ЭВМ.
9. Назовите основные виды и характеристики устройств памяти.
10. Назовите составные части и характеристики процессора.
11. Назовите этапы подготовки и решения задач на ЭВМ.
12. Дайте понятие алгоритма, приведите примеры алгоритмов.
13. Назовите основные свойства алгоритма.
14. Назовите способы описания алгоритмов, приведите примеры.
15. Что такое *блок-схема программы*?
16. Назовите основные виды алгоритмических структур.
17. Составьте словесные, формально-словесные и графические алгоритмы (блок-схемы) для заданий 1—3 из параграфа 1.2.
18. Назовите признаки классификации ЭВМ.
19. Что относится к аппаратным средствам ЭВМ?
20. Назовите отличительные особенности ПК типа IBM PC.
21. Каково назначение системной шины и разъемов расширения ПК.
22. Дайте классификацию ПК IBM PC по типу используемого микропроцессора.
23. Как связаны быстродействие микропроцессора и быстродействие ПК?
24. Как влияют характеристики МП и памяти на производительность ПК?
25. Объясните назначение адаптеров и контроллеров.

Глава 2

СИСТЕМНОЕ И СЕРВИСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

2.1. Представление информации

Информация в ЭВМ хранится в двоичном виде, и объем памяти ЭВМ измеряется в двоичной системе. Основные единицы измерения информации в ЭВМ:

бит — количество информации, которую можно передать, используя одно двоичное число, принимающее значения 0 и 1;

байт — количество информации, которую можно передать, используя 8 двоичных разрядов, равно $2^8 = 256$. Информация, имеющая объем 1 байт, может быть записана одним из 256 двоичных чисел:

0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1
0 0 0 0 0 0 1 0
0 0 0 0 0 0 1 1
.....
1 1 1 1 1 1 1 0
1 1 1 1 1 1 1 1

1 Килобайт (Кбайт, К) = 2^{10} байт = 1024 байт;
1 Мегабайт (Мбайт, М) = 2^{20} байт = 1 048 576 байт;
1 Гигабайт (Гбайт, Г) = 2^{30} байт и т.д.

В стандартном коде обмена информацией (ASCII) любой символ кодируется одним байтом, что дает возможность использовать 256 различных символов (буквы латинского и русского алфавитов, цифры, знаки препинания и некоторые специальные символы).

Информация на IBM PC хранится на дисках. Считывание и запись производятся дисководами, которые обозначаются буквой латинского алфавита с двоеточием. Первый накопитель на ГМД обозначается «A:», второй «B:». Жесткий диск обычно разбивается на несколько разделов, называемых логическими дисками, которые обозначаются как «C:», «D:», «E:» и т.д.

Информация на дисках хранится в виде файлов. ***Файлом*** называется поименованная область памяти на диске, в которой хранятся программы, данные, тексты, графическая информация и т.д.

Полное имя файла содержит собственно имя файла — от одного до восьми символов, за которым может следовать расширение.

Расширение имени начинается после точки и может либо отсутствовать, либо включает от одного до трех символов. В качестве символов в полном имени файла могут выступать: латинские буквы: A, B, ..., Z, цифры 0, 1, ..., 9 и некоторые специальные символы «!», «@», «#», «$», «%», «^», «&», «(», «)», «—», «{», «}», «'». Заглавные и строчные буквы в имени не различаются между собой. Русские буквы в именах файлов использовать не рекомендуется, как и символы «"», «/», «\», «[», «]», «:», «=», «+», «;», «,» с кодами, меньшими 20H.

Запрещены и не могут использоваться в качестве имен или типов файлов некоторые трехбуквенные имена, зарезервированные в MS DOS как имена устройств. К ним относятся:

AUX — имя дополнительного устройства ввода-вывода;
CON — имя клавиатуры при вводе или дисплея при выводе;
LPT1, ..., LPT3 — имена параллельных принтеров;
COM1, ..., COM3 — имена последовательных адаптеров;
PRN — имя печатающего устройства;
NUL — имя фиктивного устройства, эмулирующего выводные операции без реального вывода.

Расширение имени файла обычно обозначает тип файла. В MS DOS общеприняты следующие стандартные расширения:

ASM — программа на языке Ассемблера;
BAK — копия файла, сделанная перед его изменением;
BAS — программа на языке Бейсик;
BAT — командный (batch) файл пакетной обработки;
C — программа на языке СИ;
COM — выполняемая программа;
DAT — файл данных;
DOC — файл документов;
EXE — выполняемая программа;
FOR — программа на языке Фортран;
PAS — программа на языке Паскаль;
TXT — текстовый файл.

Команды MS DOS могут оперировать сразу с группами файлов, для обозначения которых используются *шаблоны имен файлов*, называемые также *глобальными* или *групповыми именами файлов*. В шаблонах используются символы «*» и «?». Символ «*» обозначает любое число любых символов в имени или расширении файла. Например:

*.BAS — обозначает все файлы с расширением BAS;
POPOV.* — обозначает все файлы с именем POPOV;
. — обозначает все файлы с любыми именами и расширениями.

Символ «?» в шаблонах обозначает один произвольный символ или его отсутствие, если «?» находится после значащих символов.

Шаблон PETR??.TXT обозначает все файлы с расширением TXT, именем, начинающимся на PETR и содержащим от 4 до 6 символов.

Важным при работе в MS DOS является понятие «*спецификация файла*». Этот термин используется для обозначения имени файла в формате:

[имя диска:] имя файла [.тип файла]

В квадратных скобках обозначены необязательные элементы. На дисках файлы объединяются в *каталоги* (*директории*). Главный или корневой каталог на каждом диске обозначается наклонной чертой «\». Этот каталог создается автоматически при форматировании диска. В корневом каталоге могут находиться файлы и другие каталоги. Имена каталогов не содержат расширений и образуются по тем же правилам, что и имена файлов. Каждый каталог может содержать файлы и другие каталоги, называемые *подкаталогами*. Тот каталог, который содержит подкаталоги, называется *надкаталогом* или *родительским каталогом*. Такой способ организации информации называется *иерархической файловой структурой*, которая представляет собой как бы «дерево» (рис. 2.1).

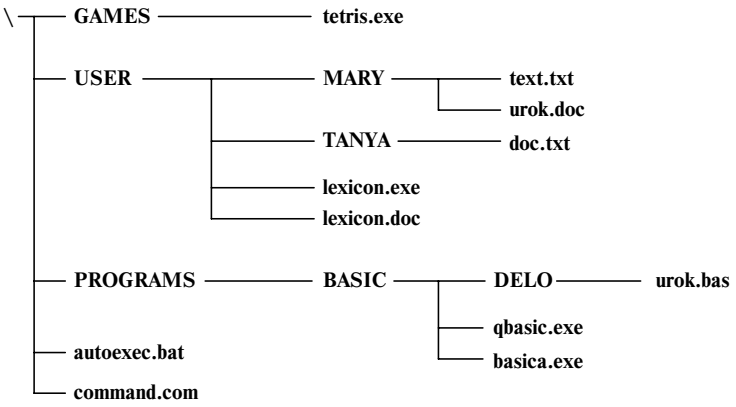


Рис. 2.1. **Пример древовидной файловой структуры**

В древовидной файловой структуре принято заглавными буквами записывать имена каталогов, а строчными — имена файлов.

При использовании иерархической структуры MS DOS необходимо указывать местоположение файлов в этой структуре. Для этого файлу дается *подымя*, или *полная спецификация файла*.

Формат подымени:

[имя диска:][имя каталога]\[имя подкаталога]\имя файла[.тип]

Здесь необязательные элементы указаны в скобках «[ ]».

Для некоторых файлов из приведенного выше дерева укажем их подымена:

Имя файла	Подымя
doc.txt	C:\USER\TANYA\doc.txt
basica.exe	C:\PROGRAMS\BASIC\basica.exe

Каталогу в иерархической структуре дается полное имя каталога, которое содержит имена всех надкаталогов с указанием имени диска.

О каждом файле хранится информация не только о его имени, но и о его размере в байтах, о дате и времени создания.

Таким образом, с каждым файлом в DOS связываются:

1) составное имя файла;
2) дополнительные атрибуты файла;
3) дата создания или изменения файла;
4) время создания или изменения файла;
5) длина файла.

Эти характеристики файла называются *атрибутами файла.*

Дата создания и время создания файла при создании или обновлении файла берутся из системных часов. Для изменения показания системных часов используются команды DOS: Date и Time. Размер (size) файла указывается в байтах. У каждого файла имеются также *дополнительные атрибуты файла:*

R (*read only*) — только для чтения;
A (*archive*) — архивный;
H (*hidden*) — скрытый;
S (*system*) — системный.

Файловая структура усложняется по мере создания новых каталогов. В каждый новый каталог могут быть добавлены файлы, а также новые подкаталоги. Любой файл можно найти путем перемещения по какой-либо ветви дерева, начиная от корня, или, наоборот, поднятием по ветви дерева по направлению к корню. Существуют определенные *правила формирования файловой структуры*:

1. Каталог или файл может входить только в один каталог.

2. На порядок следования файлов в каталоге никаких ограничений не налагается.

3. Допускается вхождение в разные каталоги файлов с одинаковыми именами.

4. Глубина вложенности каталогов не ограничивается.

При работе с каталогами используют следующую терминологию:

Текущий каталог — каталог, с которым в данный момент работает пользователь. DOS хранит информацию о текущем каталоге для каждого дисковода компьютера. При запуске (включении ПК) в качестве текущего каталога устанавливается корневой каталог.

Текущий дисковод — дисковод, с которым в данный момент работает пользователь.

Рабочий каталог — текущий каталог на текущем дисководе.

Дочерний и ***родительский каталоги*** — если первый каталог входит во второй, то первый — дочерний, а второй — родительский.

Создать новый файл можно только в рабочем каталоге. Для создания файла в другом каталоге нужны специальные действия.

Доступ к файлу в иерархической структуре осуществляется с помощью маршрута. ***Полным маршрутом*** (*путем*) ***к файлу*** называется последовательность каталогов, ведущих от корневого каталога к этому файлу. Полный маршрут представляется перечислением имен каталогов, разделенных символом «\», причем корневой каталог от его дочернего символом «\» не отделяется.

Пример:

\PROGRAMS\BASIC\DELO

Указание полных маршрутов на жестком диске с разветвленной файловой структурой утомительно, поэтому существуют дополнительные возможности доступа к файлам с помощью относительного маршрута. *Относительный маршрут* отличается от полного тем, что:

1) начинается от текущего каталога;
2) перечисление имен каталогов может идти как от корневого каталога, так и по направлению к нему;
3) для обозначения родительского каталога используется символ.

Пример:

..\..\GAMES

С использованием маршрута полную спецификацию файла можно представить в виде:

[имя диска:] [маршрут\] имя файла.[расширение]

Если необязательные элементы отсутствуют, то действуют *правила умолчания*:

- не задано имя диска — выбирается текущий привод;
- маршрут начинается с корневого каталога — пишется полный маршрут;
- маршрут начинается не с символа «\» — поиск начинается с текущего каталога;
- маршрут не задан — считается, что файл находится в текущем каталоге на выбранном дисководе;
- расширение не задано — считается, что его нет.

Примеры:

1. C:\GAMES\tetris.exe — определяет местонахождение файла tetris.exe в каталоге GAMES, который находится в корневом каталоге диска C.

2. \command.com — файл command.com расположен в корневом каталоге текущего диска.

3. Пусть текущий каталог USER, тогда MARY\urok.doc определяет местонахождение файла urok.doc в текущем каталоге текущего дисковода.

2.2. Операционные системы

Операционная система — группа взаимосвязанных программ, выступающая посредником между аппаратными средствами ЭВМ и пользователем, обеспечивающая управление ресурсами ЭВМ и процессами, использующая эти ресурсы при вычислении.

В качестве ресурсов ЭВМ выступают:

- микропроцессор (МП);
- основная память (ОП);
- периферийные устройства (ПУ).

➤ ***Назначение операционной системы*:** обеспечение удобства управления компьютером, позволяет освободить пользователя от выполнения большого числа рутинных операций.

Операционная система обеспечивает *выполнение двух главных задач*:

1. Поддержка работы всех программ и обеспечивающих их взаимодействие с аппаратными средствами. ОС обеспечивает взаимодействие программ с внешними устройствами и друг с другом, расширение оперативной памяти, выявление различных событий (например, связанных с аварийными ситуациями и ошибками) и реакцию на них.

2. Возможность общего управления машиной, которое осуществляется на основе командного языка ОС (системы команд — директив). С помощью этих команд человек может выполнять такие операции, как разметка диска, копирование файлов, распечатка каталогов на экране, запуск программ, установка режимов работы периферийных устройств и другие действия.

Выполнение самых простых действий на аппаратном уровне описывается большим числом машинных команд. Например, программа копирования содержит около 30 действий, каждое из которых, в зависимости от состояния компьютера, может иметь различные исходы. Задача ОС состоит в том, чтобы скрыть от пользователя ненужные ему подробности. Это удобство, без которого пользователь практически не смог бы работать.

➤ ***Основные компоненты операционной системы*:**

1) базовая система ввода-вывода;
2) системный загрузчик;
3) командный процессор или интерпретатор команд;
4) драйверы внешних устройств;
5) файловая система;
6) утилиты.

Базовая система ввода-вывода (BIOS) является одновременно частью компьютера и компонентом данной операционной системы, при

установке на компьютер другой операционной системы BIOS автоматически становится ее частью. BIOS, скрывая архитектурные особенности конкретной модели компьютера, реализует наиболее простые и универсальные услуги операционной системы по управлению основными периферийными устройствами, в частности по организации ввода-вывода информации.

Системный загрузчик предварительно производит тестирование устройств компьютера, затем, при положительном результате тестирования, выполняет загрузку ОС из внешней памяти.

Командный процессор — производит анализ и исполнение команд пользователя, включая загрузку готовых программ из файлов в операционную память ПК и их запуск.

Драйверы — программы специального вида, ориентированные на управление внешними устройствами (ПУ). Каждому типу внешнего устройства соответствует драйвер (клавиатура, НЖМД, НГМД и др.)

Файловая система — хранилище программ, данных и функциональная часть, обеспечивающая выполнение операций над файлами.

Утилиты — программы, расширяющие возможности ОС, предоставляя пользователю набор дополнительных услуг по контролю и управлению за компонентами ОС и устройствами компьютера.

Операционная система MS DOS

Для работы с файлами на компьютере создано множество операционных систем. Наиболее широкое распространение среди них получила операционная система MS DOS (дисковая операционная система фирмы «Microsoft»), разработанная в 1981 г. для работы на 16-разрядных IBM-совместимых персональных компьютерах. В последующие годы эта ОС прошла путь развития, который выразился в появлении новых версий. Каждая новая версия появлялась почти одновременно с разработкой новых аппаратных средств: микропроцессоров, внешних устройств и др. Вместе с тем каждая новая версия содержала все возможности предыдущей и обладала новыми. Поэтому при перенесении старых программ в среду новой версии проблем не возникало. В силу своего широкого распространения MS DOS приобрела статус фактического стандарта для IBM PC-совместимых персональных компьютеров. Операционная система Windows 95, появившаяся в 1995 г., сохранила совместимость с MS DOS. Отличительные особенности этой системы будут рассмотрены ниже.

Операционные системы *классифицируются по следующим признакам*:

1. Число пользователей, одновременно обслуживаемых системой (однопользовательская или многопользовательская).

2. Число задач, которые одновременно могут выполняться под управлением ОС (однозадачная или многозадачная).

3. Тип доступа пользователя к ЭВМ (сетевая или несетевая).

4. Тип организации вычислительного процесса (однопроцессорная или многопроцессорная).

Согласно этим критериям, MS DOS является:

- однопользовательской;
- однозадачной с элементами многозадачности;
- несетевой;
- однопроцессорной.

Команды MS DOS

Посредством команд происходит общение пользователя с компьютером. Вводя команды MS DOS с клавиатуры, пользователь передает системе задания.

С помощью команд MS DOS выполняются следующие основные действия:

- сравнение, копирование, распечатка, удаление и переименование файлов;
- анализ и распечатка каталогов;
- копирование и форматирование дисков;
- выполнение системных программ и программ пользователей;
- ввод даты, времени и комментариев;
- установка функций экрана и режимов печати;
- копирование системных файлов MS DOS на другой диск;
- перевод MS DOS в режим ожидания реакции пользователя.

Существуют два типа команд MS DOS — встроенные (внутренние) и загружаемые (внешние). *Встроенные команды* — простейшие, наиболее часто употребляемые. Пользователь не видит их в каталогах диска MS DOS, они являются частью процессора команд. Введенные пользователем команды выполняются немедленно. *Загружаемые команды* существуют на диске как программные файлы. Прежде чем начать выполняться, они должны быть считаны с диска. Любое имя файла с типом .com, .exe или .bat рассматривается как загружаемая команда. Пользователь может создавать свои загружаемые команды и добавлять их к системе. При вводе таких команд можно не вводить их тип.

В зависимости от характера выполняемых функций команды MS DOS разделяются на семь классов:

1) общие команды;
2) команды сравнения;
3) команды — фильтры;
4) команды — функции;
5) команды для организации пакетных файлов;

6) команды конфигурирования системы;
7) команды настройки системы.

Наиболее употребляемыми пользователями являются общие команды, к которым относятся:

1) команды для работы с файлами;
2) команды для работы с каталогами;
3) команды для работы с дисками, объектами которых выступают внешние запоминающие устройства в целом.

Формат команд MS DOS

Формат команд MS DOS имеет вид:

команда [параметры]

где команда — имя команды MS DOS, а параметрами, в зависимости от типа команды, могут быть:

1) имя диска;
2) маршрут;
3) имя файла;
4) подымя;
5) ключи команд, перед которыми ставится знак «/», например «/p», разделенные пробелами.

Основные команды для работы с файлами

1. ***Создание текстового файла*****:**

copy con подымя

Здесь con — имя устройства, откуда копируется файл (клавиатура). Символ обозначает обязательный пробел между параметрами в командной строке. По такой команде copy будет создан файл с заданным именем в указанном каталоге. При вводе текста в файл в конце строк нажимать Enter, после ввода всего текста нажать F6 или Ctrl+Z и Enter.

Пример:

C:\PROGRAMS>copy con new.txt — создание файла new.txt в текущем каталоге PROGRAMS и ввод в него текста.

2. ***Копирование файлов*****:**

copy подымя1 подымя2

Подымя1 — «кого и откуда» копируем, подымя2 — «куда копируем и как называем». Если подымя2 отсутствует, то копирование производится в текущий каталог с именем файла1.

Примеры:

1. C:\USER\MARY>copy text.txt doc.txt — копируется файл text.txt из текущего каталога MARY, создается файл doc.txt в этом же каталоге.

2. C:\GAMES>copy C:\PROGRAMS\BASIC*.exe A:*.com — копируются все файлы с расширением .exe из каталога BASIC, создаются файлы под теми же именами в корневом каталоге диска A:, но с расширением .com.

Копирование всегда удобнее проводить из текущего каталога, так как в этом случае не надо указывать маршрут к копируемым файлам.

3. ***Удаление файлов*:**

del подымя

Пример:

C:\>del USER\TANYA\doc.txt — удаление файла doc.txt из каталога TANYA.

4. ***Переименование файла*:**

ren подымя1 подымя2

Пример:

C:\USER>ren MARY\urok.doc igra.doc — переименовывается файл urok.doc из каталога MARY в файл igra.doc.

5. ***Вывод на экран содержимого файла*:**

type подымя

Pause/Enter — приостанов/продолжение процесса вывода, Ctrl+C — прекращение вывода

6. ***Вывод содержимого файла на принтер*:**

copy подымя prn

Здесь prn — имя устройства вывода (принтер), которое стоит вместо имени файла.

Во всех случаях действуют правила умолчания: если указано только имя файла, то действия производятся в рабочем каталоге.

Основные команды для работы с каталогами

1. ***Просмотр каталога*:**

dir [имя диска][маршрут\][/p][/w]

При подаче этой команды будут выданы имена подкаталогов просматриваемого каталога, а также полная информация о файлах, т.е. имена с расширениями, размер в байтах, дата и время создания. Как видно из формата команды, все параметры могут быть опущены — в этом случае просматривается рабочий каталог.

Примеры:

1. C:\PROGRAMS\BASIC>dir .. — просмотр надкаталога PROGRAMS каталога BASIC.

2. C:\PROGRAMS\BASIC>dir DELO — просмотр подкаталога DELO каталога BASIC.
3. C:\PROGRAMS\BASIC>dir \ — просмотр корневого каталога.
4. C:\PROGRAMS\BASIC>dir — просмотр текущего каталога BASIC.

В команде, как видно из ее формата, могут быть использованы ключи:

/p — просмотр содержимого каталога будет производиться постранично, что очень удобно, если список файлов и подкаталогов просматриваемого каталога очень большой;

/w — на экран при просмотре выводится лишь краткая информация о файлах и каталогах (без указания их размера, даты и времени создания).

Примеры:

1. C:\PROGRAMS\BASIC>dir ..\..\USER/p — постраничный просмотр каталога USER.
2. C:\PROGRAMS\BASIC>dir/w — выдача содержания текущего каталога в краткой форме.

2. *Смена рабочего каталога* (change directory):

cd [имя диска][маршрут\]

По этой команде рабочим каталогом становится каталог, путь к которому указан в команде.

Примеры:

1. C:\USER>cd \PROGRAMS\BASIC — переход в рабочий каталог BASIC.
2. C:\PROGRAMS\BASIC>cd DELO — переход в подкаталог DELO каталога BASIC с назначением его рабочим каталогом.
3. C:\PROGRAMS\BASIC\DELO>cd \ — назначение в качестве рабочего корневого каталога диска C:.

3. *Создание каталога* (make directory):

md [имя диска][маршрут\]

Пример:

C:\PROGRAMS\BASIC>md IGRA — создание подкаталога IGRA в текущем каталоге BASIC.

4. *Удаление каталога* (remove directory):

rd [имя диска][маршрут\]

Пример:

C:\PROGRAMS\BASIC>rd IGRA — удаление подкаталога IGRA из рабочего каталога BASIC.

Команды для работы с магнитными дисками

Эти команды работают с магнитными дисками на уровне устройства, а не файла. Целесообразно классифицировать команды по группам в соответствии со схемой, приведенной на рис. 2.2.

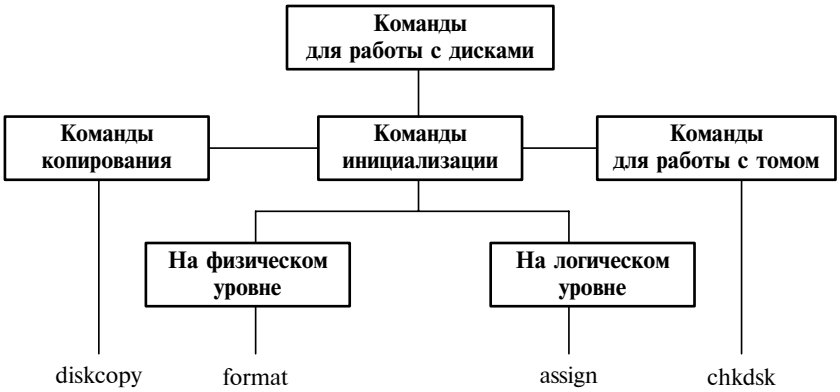


Рис. 2.2. **Классификация команд работы с дисками**

1. ***Копирование магнитных дисков*** **(DISKCOPY):**

DISKCOPY [источник] [приемник][/1]

Параметр «источник» — имя диска с дискетой, которую нужно скопировать. Параметр «приемник» — имя диска с целевой дискетой.

Ключ /1 позволяет копировать только первую сторону исходной дискеты.

Команда перезаписывает гибкие магнитные диски на физическом уровне, при этом целевая и исходная дискеты получаются неразличимыми. Копирование производится через оперативную память, поэтому возможно на машинах с одним и двумя дисководами. Копия системной дискеты будет также системной дискетой.

Неформатированные дискеты DISKCOPY автоматически форматирует. Дискеты копируются «дорожка в дорожку». Если дискеты или дисководы не соответствуют друг другу по формату, то копирование не выполняется. Команда внешняя, загрузочный модуль содержится в файле DISKCOPY.COM.

Пример:

C:\> diskcopy a: a:

2. ***Форматирование магнитных дисков*** **(FORMAT).**

Команда форматирования выполняет следующие операции:

1) форматирование диска;
2) проверка нанесенных секторов и пометка дефектных блоков;
3) запись блока начальной загрузки (BOOT RECORD, БНЗ) в первый сектор нулевой дорожки;

4) создание и запись в первых секторах магнитного диска (после БНЗ) таблицы распределения информационного пространства диска (FAT) и ее копии;
5) создание и запись на магнитный диск (МД) корневого каталога (ROOT DIRECTORY).

Рассмотрим каждую из вышеупомянутых операций отдельно.

1. *Форматирование диска* заключается в разметке поверхности магнитного диска на отдельные дорожки и сектора, что позволяет в дальнейшем реализовать секторный поиск при обмене данными с магнитными дисками. При секторном поиске для считывания одного сектора требуется в N раз меньше оперативной памяти и, соответственно, времени, чем для считывания одной дорожки (N представляет частное от деления размера дорожки на размер сектора). Секторная разметка прочно вошла в обиход. При любом типе секторной разметки форматирование приводит к однозначной идентификации каждого сектора на поверхности магнитного диска. Команда FORMAT размещает в каждом секторе уникальные коды, считывание которых служит обратной связью при выполнении операций позиционирования магнитных головок в процессе обмена данными с МД. Рассматриваемая операция называется также *низкоуровневым форматированием*, поскольку после ее завершения МД готов к выполнению физических операций ввода-вывода, но не имеет файловой структуры DOS и не может быть использован операционной системой для записи файлов.

2. *Проверка отформатированных секторов и пометка дефектных блоков.* Операция заключается в проверке возможности считывания каждого физического сектора МД, она совмещена во времени с операцией форматирования. В случае обнаружения ошибки соответствующие сектора помечаются как дефектные, а остальные — как бездефектные, которые и составляют полезное пространство МД. Здесь следует отметить, что минимальная область памяти МД, рассматриваемая MS DOS при распределении дискового пространства под файлы, называется ***кластером*** или ***блоком***. Если хотя бы один сектор в кластере помечен как дефектный, то данный кластер не используется MS DOS при распределении полезного пространства МД.

3. *Запись блока начальной загрузки.* Операция записывает блок начальной загрузки в первый сектор нулевой дорожки МД. Основа БНЗ — загрузочный модуль программы, инициирующей загрузку ОС. Запись БНЗ производится вне зависимости от того, будет ли на диск записана MS DOS или нет.

4. *Создание таблицы распределения информационного пространства диска* (FAT) *и ее копии.* Таблица FAT — важнейший элемент файловой структуры DOS. Потеря содержащихся в ней данных мо-

жет привести к потере больших объемов информации пользователя, поэтому в файловую систему DOS заложена возможность формирования и сохранения резервных копий FAT (обычно их две). Размер FAT прямо пропорционален количеству кластеров МД.

5. *Создание и запись корневого каталога* завершает процедуру инициализации магнитного диска. Размер ROOT DIRECTORY при росте емкости диска растет нелинейно, он составляет 7 секторов для DS/DD диска и 14 секторов для DS/HD диска. Корневой каталог размещается сразу же за таблицей FAT. Корневой каталог и таблицу размещения файлов нельзя удалить с диска средствами операционной системы, так как использование МД без этих структур невозможно.

Формат команды FORMAT следующий:

FORMAT имя диска [/S] [/4] [/8] [V:метка] [/B] [/N:XX] [T:YY]

Ключ /S	— форматирование с созданием системного диска.
Ключ /4	— форматирование дискеты 360 Кбайт в дисководе на 1,2 Мбайт.
Ключ /8	— восьмисекторное форматирование.
Ключ /V:метка	— вызов запроса на ввод имени метки тома по окончании форматирования.
Ключ /B	— резервирование при форматировании места для системных файлов.
Ключ /N:XX	— произвольное форматирование с размещением XX секторов на дорожке.
Ключ /T:YY	— произвольное форматирование с размещением YY дорожек на каждой магнитной поверхности диска.

Пример:

C:\FORMAT A:/4 — форматирование дискеты на 360 Кбайт в дисководе на 1,2 Мбайт.

При форматировании вся информация, записанная на магнитном диске, уничтожается. Рекомендуется всегда форматировать новые дискеты на дисководах того компьютера, где их предполагается использовать. При этом желательно применять стандартные варианты разметки, указанные в табл. 1.2. Команда FORMAT — внешняя, загрузочный модуль содержится в файле FORMAT.COM.

3. *Переназначение накопителей на магнитных дисках* (ASSIGN).

Команда ASSIGN переадресует запросы ввода-вывода с одного накопителя на магнитных дисках к другому. Например, если программа требует вывода данных на накопитель B:, а в системе он отсутствует, можно переназначить операции ввода-вывода с B: на C:.

ASSIGN [источник = целевое устройство] [...]

Параметр «источник» — накопитель, запросы к которому должны быть переназначены. Имя накопителя задается без двоеточия.

Параметр «целевое устройство» — имя накопителя, который будет обрабатывать переадресованные запросы.

Пример:

1. ASSIGN B=C — переадресация ввода-вывода с накопителя B: на C:.

2. ASSIGN без параметров устраняет все текущие назначения. Команда ASSIGN внешняя, содержится в модуле ASSIGN.COM.

4. *Контроль файловой структуры* (CHKDSK).

Команда CHKDSK — основное средство контроля корректности файловой структуры магнитного диска в рамках ОС MS DOS. Она выполняет проверку логической структуры томов внешней памяти (дисков). CHKDSK работает в двух режимах: 1) индикации ошибок и 2) их корректировки. В режиме 2 существует вероятность искажения данных, поэтому перед запуском CHKDSK необходимо сделать резервную копию корректируемой информации.

В процессе работы CHKDSK проверяет файловую структуру на наличие следующих логических дефектов:

- потерянных кластеров в таблице размещения файлов FAT;
- перекрестных ссылок на кластеры;
- ссылок на несуществующие кластеры (ошибок размещения);
- нарушений непрерывности файлов и их фрагментации.

Потерянные блоки — это участки магнитного носителя, не включенные ни в одну цепочку кластеров, описывающую файлы. Они могут образоваться при аварийном завершении работы с дисками, например при выключении питания ПК при наличии открытых файлов. CHKDSK формирует из таких кластеров файлы с именем FILEnnnn.CHK, где nnnn — порядковый номер файла. Таким образом, можно проанализировать содержимое потерянных блоков, использовать его для восстановления испорченной информации или удалить.

Перекрестные ссылки возникают тогда, когда один и тот же кластер включается в две или более независимые цепочки, каждая из которых соответствует отдельному файлу. Они могут возникнуть после принудительного прерывания операции записи на магнитный диск. Обнаружив перекрестные ссылки, CHKDSK выдает сообщение. Можно переписать и проверить каждый файл, после чего для полной гарантии восстановления файловой структуры диск желательно переформатировать.

Ошибки размещения возникают достаточно редко и бывают вызваны в большинстве случаев некорректным программированием операций обмена с магнитными дисками, при этом появляются

ссылки на «мнимый», несуществующий кластер магнитного диска. CHKDSK оставляет только правильно размещенные части файлов, а остальные данные теряются.

Нарушение непрерывности файлов (фрагментация), вообще говоря, не является сбойной ситуацией и допускается MS DOS. Она позволяет повысить эффективность использования дискового пространства, а фрагментированные файлы называются списковыми. Однако появление фрагментации файлов увеличивает число физических обращений к дискам и время поиска информации при обмене с устройствами внешней памяти. CHKDSK выявляет все случаи фрагментации. Устранить фрагментацию можно, перезаписав файлы на переформатированный диск командами COPY, XCOPY или BACKUP.

Формат команды CHKDSK:

CHKDSK [спец. файла] CHKDSK [/F] [/V]

Ключ [/F] позволяет проводить корректировку найденных ошибок по ходу выполнения программы CHKDSK.

Ключ [/V] обеспечивает вывод на дисплей имен проверяемых файлов с маршрутами.

Пример:

C:\USER\MARY> CHKDSK a:*.* — проверка всех файлов диска a: на наличие логических дефектов.

Операционные системы Windows

Первое принципиально важное с точки зрения технологии обработки информации отличие операционных систем Windows заключается в их *реальной многозадачности* и *режиме разделения времени*. Это значит, что на компьютере одновременно можно запускать на выполнение несколько задач. Например, одновременно производить расчеты, редактировать текст и получать данные через канал связи. Второе отличие — стандартизация всех форм представления информации. Теперь данные из текстового редактора можно передавать в базу данных, электронную таблицу, другие программы и обратно. Системы Windows имеют возможность работы в локальной информационной сети и глобальной сети Internet.

Операционные системы Windows намного превосходят MS DOS в простоте общения и в удобстве интерфейса. Windows является *графической* операционной системой для компьютеров платформы IBM PC. Если раньше запустить программы было непросто, то теперь все «точки входа в программы» обозначены на рабочем столе — экране монитора — значками-пиктограммами. Чтобы запустить программу на исполнение, нужно подвести курсор к нужному значку и

дважды щелкнуть по кнопке манипулятора «мышь». Пользователь компьютера с Windows не нуждается в услугах программ-оболочек, столь необходимых пользователю, работающему с MS DOS. Для эффективной работы в Windows необходимо знать основные объекты операционной системы, базовые принципы и приемы управления. Их можно разобрать на примере версий Windows 95 и Windows 98.

Принцип Рабочего стола **(Desktop).**

Это основная идея операционной системы. Создатели новой ОС стремились показать, что не только внешний вид Рабочего стола напоминает письменный стол, на котором разложены все необходимые для работы предметы (папки, документы, даже часы и др.), но и основные приемы работы пользователя в Windows 95 аналогичны приемам работы за письменным столом.

Панель задач (Taskbar) — горизонтальная линейка, расположенная в нижней части Рабочего стола.

Основное предназначение Панели задач: найти важную кнопку Пуск (Start), кнопки активных приложений, индикатор кодировки клавиатуры (языка), часы и некоторые другие элементы. Кнопка Пуск (Start) открывает доступ к Главному меню (Start Menu) и ко всем основным рабочим программам. Чрезвычайно удобным и полезным оказалось размещение на Панели задач кнопок активных приложений. Это позволяет не только всегда видеть, какие приложения запущены, но также значительно облегчает переключение между ними: достаточно щелкнуть на кнопку нужного приложения.

Мой компьютер (My Computer) представляет собой средство доступа ко всем ресурсам компьютера пользователя, а также дискам других компьютеров, подсоединенных к сети. Кроме того, применяя Мой компьютер, пользователь:

- получает доступ к содержимому всех дисков и может выполнять все файловые операции, а также запускать все необходимые приложения;
- имеет возможность использования *Панели управления* (Control Panel) для изменения установок операционной среды;
- способен управлять всеми локальными и сетевыми принтерами.

Сетевое окружение (Network Neighborhood) — средство для работы с ресурсами в том случае, если компьютер включен в локальную компьютерную сеть.

Глобальная сеть (Microsoft Network) — средство для работы с ресурсами глобальной сети.

Входящие (Inbox) — комплекс средств предназначен для работы с электронной почтой. Почтовая система — Microsoft Exchange.

Корзина (Recycle Bin). В Windows борьба за восстановление уничтоженных файлов ведется кардинальным способом: удаленные пользователем файлы на самом деле не уничтожаются, а аккуратно

складываются в специальную папку-корзину. Щелкнув дважды по значку «корзина» можно получить доступ к списку всех сохраненных в ней файлов. При необходимости можно восстановить удаленный файл. Очевидно, что платой за предоставляемые операционной системой удобства являются дополнительные затраты места на жестком диске. Если объем свободного дискового пространства становится недостаточным для эффективной работы Windows, то пользователь всегда может очистить корзину. Очистка может быть произведена одновременно для всех файлов, сохраненных в корзине, или выборочно. Однако после очистки корзины никаких гарантий относительно восстановления файлов средствами операционной системы никто уже не даст. Кроме того, корзина бесполезна при работе с дискетой.

Портфель (My Briefcase). Это средство применяется в тех случаях, когда пользователю приходится работать то на одном, то на другом компьютере. Обычно один из этих компьютеров установлен стационарно, а другой — является переносным (Notebook). При работе в таком режиме периодически возникает необходимость обновления файлов (Update) на основном, стационарном компьютере, что и выполняется с помощью портфеля.

Значки (Icon). Значки являются *графическими представителями различных объектов* Windows — документов, программ, отдельных групп объектов, например папок (Folders). Рабочий стол тоже имеет свой собственный значок. *Значки позволяют не только видеть, с каким объектом приходится иметь дело, но и выполнять многие операции с самими объектами.* То, что делается со значком, на самом деле выполняется с самим объектом. Например, удаление значка приводит к удалению самого объекта, копирование значка приводит к копированию объекта и т.д. Значки (Icons), как правило, сопровождаются метками (Icons Labels) с именем того объекта, который они представляют. Операционная система включает в себя средства для изменения размеров значков, шрифта, применяемого в метке значка, создания оригинальных значков самим пользователем.

Папки (Folders) в Windows обозначают каталоги, по которым распределены все аппаратные и программные компоненты компьютера: диски, принтеры, документы, ярлыки, приложения (Applications), другие папки. Все папки образуют единую иерархическую систему. Для ее просмотра может быть использован Мой компьютер (My computer) или приложение, называемое Проводник (Explorer). Для доступа внутрь папки нужно использовать двойной щелчок мышью на значке (Icon), соответствующем нужной папке. Папки можно открывать и закрывать, копировать и перемещать, создавать и удалять.

Ярлыки (Shortcuts). Некоторый нужный объект (папка, документ или приложение) может находиться в любом месте файловой системы. Пользователю достаточно видеть перед собой только ярлык (Shortcut) объекта. *Ярлык является указателем на объект.* Например, сам объект может быть спрятан где-нибудь в глубине файловой структуры, а его ярлык помещен непосредственно на Рабочий стол. Это дает возможность начинать работу с объектом без долгих поисков его самого. Достаточно дважды щелкнуть на ярлыки, и при этом произойдет вызов соответствующего объекта.

Ярлыки существенно ускоряют и облегчают доступ к часто используемым приложениям и документам. Ярлык — это *ссылка* на документ. Для одного объекта может использоваться несколько ярлыков, расположенных в самых разных частях файловой системы. Удаление не приводит к уничтожению самого объекта. Ярлыки могут указывать на любые объекты, включая папки, диски, компьютеры и принтеры. С ними можно выполнять все те же операции, что и с обычными значками. Значок ярлыка повторяет значок того объекта, на который этот ярлык ссылается, но к нему в нижней левой части добавлен маркер в виде стрелки.

Документно-ориентированный принцип Windows. Этот принцип базируется *на двух основных положениях*:

1. Под документом в Windows 95 и 98 понимают не только текстовые файлы (как это было при работе в MS DOS и прежних версиях Windows), а практически любой файл, содержащий данные: текст, графическое изображение, электронную таблицу, звук, видеофильм.

2. Документ является *первичным по отношению к приложению* (Application), в котором он был создан или может быть использован. Если дважды нажать левой кнопкой мыши на значке нужного документа или на значке его ярлыка (Shortcut), то это приведет к вызову соответствующего приложения и последующей загрузке в него выбранного документа.

Мышь в Windows. Можно ли работать без мыши в Windows? Да, можно, но это очень неудобно. При работе в этой операционной системе мышь играет значительно более важную роль, чем в MS DOS и предыдущих версиях Windows. В Windows 95 и 98 указатель мыши изменяет свой вид в зависимости от того, какая операция с использованием мыши выполняется. Чаще всего с помощью мыши выполняются следующие типовые операции:

- выделение объектов и вызов приложений;
- перемещение объектов методом «перетащить и оставить» (Drag & Drop).

Клавиатура (Keyboard) — является наиболее важным инструментом оператора при работе на ПК. Но пользователя Windows, как правило, в первую очередь интересуют *клавиши быстрого доступа.*

Такие клавиши, называемые также «горячими клавишами» (Hot Key), служат для выполнения команд без использования мыши и без вызова их через меню.

Окна. Существуют следующие типы окон Windows: *окна папок*, *окна диалога*, *окна подсказки*, *рабочие окна приложений* и другие.

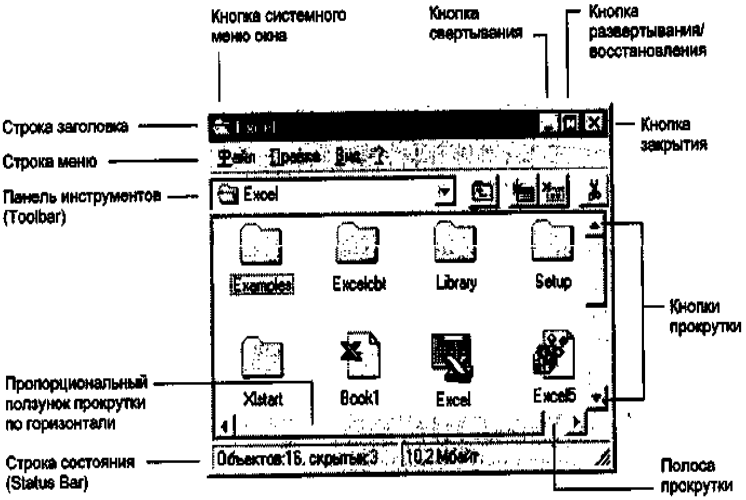


Рис. 2.3. **Окно папки «Excel и его элементы»**

Типы окон выделяются по наличию в них однородных элементов управления и оформления. Структура окна папки и его элементы показаны на рис. 2.3. Элементы окна диалога приведены на рис. 2.4.

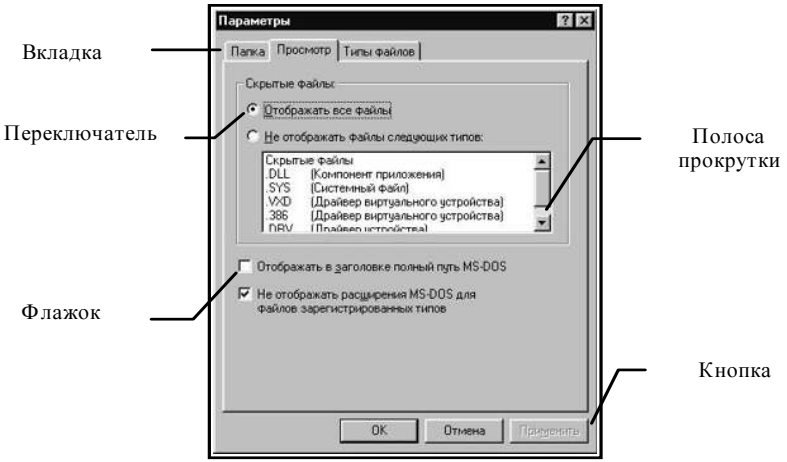


Рис. 2.4. **Окно диалога «Параметры и его элементы»**

Работа с документами, файлами, папками, дисками.

Файл — это массив информации, сохраненный на диске и имеющий собственное имя. Файл, например, может быть программой, набором данных, текстовым документом.

Документом называют файл, содержащий данные, например текст, графическое изображение, электронную таблицу.

Папка — это каталог, в котором могут быть размещены файлы документов и программ, другие папки.

Диск — это одно из устройств, на котором могут храниться файлы.

Файлы и папки. Одним из наиболее заметных отличий Windows 95 и 98 является возможность использования длинных имен файлов и папок.

Правила образования имен в Windows следующие:

- предельная длина имени файла составляет 255 символов, включая пробелы;
- имя файла может содержать буквы, цифры, пробелы, а также следующие символы: «(», «!», «)», «@», «#», «$», «%», «&», «_», «–», «[», «+», «]», «=», «`», «,», «;», «:», «{», «}», «,», «~»;
- все папки, находящиеся внутри одной общей папки, должны иметь уникальное имя, т.е. не может быть двух папок с одинаковыми именами;
- то же самое относится и к файлам: внутри одной папки не может быть двух файлов с одинаковыми именами;
- имена могут содержать как большие, так и маленькие буквы, но Windows 95 расценивает их как одинаковые.

Наиболее важные операции с объектами Windows 95 и Windows 98:

1) создание (Creating) новых объектов;
2) выделение (Selecting) объектов (одного, нескольких или всех сразу);
3) копирование (Coping) и перемещение объектов (Moving) с использованием команд, меню, мыши и буфера обмена (Clipboard) Windows;
4) переименование (Renaming) объектов;
5) удаление (Deleting) объектов с предварительным помещением их в корзину и без такового;
6) восстановление (Restoring, Undeleting) объектов;
7) просмотр (Preview) документов без их редактирования;
8) поиск (Finding) файлов и папок;
9) запуск программ.

Создание новых объектов

➤ *Создание папки.*

1. Установить указатель мыши на свободной части Рабочего стола и вызвать контекстное меню, выполнив щелчок правой кнопки или нажав клавиши Shift+F10.

2. Открыть меню команды «Создать» (New), выбрать в нем и исполнить команду «Папка» (Folder).

3. В поле метки значка выписать название папки.

Создать папку можно также следующим образом:

- Создать папку можно в любом окне, имеющем в меню команды «Файл» (File) пункт «Создать» (New).
- Создать папку можно в любом окне, предназначенном для сохранения файлов на Панели инструментов. В таких окнах всегда присутствует кнопка создания новой папки.

➤ *Создание документа.*

1. Открыть папку, в которой планируется создать новый документ.

2. Открыть контекстное меню (правая кнопка мыши или Shift+F10).

3. Открыть меню команды «Создать» (New) и в нем выбрать тип нужного документа.

4. В поле метки значка документа указать нужное имя.

Создать документ можно также следующим образом:

- Создать документ можно в любом окне, имеющем в меню команды «Файл» (File) пункт «Создать» (New).
- Создать документ можно непосредственно из приложения.

➤ *Создание ярлыка.*

Ярлыки создаются так же, как папки и документы. Но если для папок и документов надо вводить их имена, то для ярлыка нужно предварительно указать объект, на который он ссылается, после чего Windows сама предложит имя для ярлыка. При желании это имя можно изменить. Для создания ярлыков нужно выполнить следующие действия:

1. Открыть папку, в которой планируется создать ярлык.

2. Открыть контекстное меню нажатием правой кнопкой мыши или нажатием клавиши Shift+F10.

3. Открыть меню команды «Создать» (New), в нем выбрать команду «Ярлык» (Shortcut) и нажать ENTER.

Создать ярлык можно также следующим образом:

- Создать ярлык можно в любом окне, имеющем в меню команды «Файл» (File) пункт «Создать» (New).
- Создать ярлык можно с помощью метода «перетащить и оставить». Для этого необходимо, чтобы на экране были одновременно видны обе папки — та, в которой находится исходный объект, и та, в которую будет помещен ярлык этого объекта. Нажав правую кнопку мыши, следует перетащить объект из одной папки в другую. В контекстном меню, ко-

торое появляется после завершения этой операции, нужно щелкнуть на строке с командой «Создать ярлык» (Create Shortcut).

➤ *Выделение объекта.*

Любой объект, перед тем как с ним будет выполнено какое-либо действие, должен быть выделен.

Для выделения одного объекта следует щелкнуть на нем мышью. Чтобы выделить несколько объектов, расположенных в произвольном порядке, надо нажать клавишу Ctrl и, не отпуская ее, щелкнуть мышью на каждом объекте. Если нужно выбрать несколько объектов, расположенных последовательно, следует сделать так: установить указатель мыши рядом с первым из выделяемых объектов, нажать левую кнопку и, не отпуская ее, тащить указатель мыши по экрану. Все объекты, попадающие при этом в раздвигающуюся прямоугольную область, окажутся выделенными.

Сразу все объекты в папке выделить еще проще: надо открыть папку и выполнить команду «Правка»/«Выделить все» (Edit/Select All) или нажать Ctrl+A.

Несколько расположенных подряд объектов можно выделить еще и другим способом: пометить первый из них, затем нажать клавишу Shift и щелкнуть мышью на последнем из выделяемых объектов.

➤ *Копирование и перемещение.*

Для копирования объекта (или группы выделенных объектов) нужно нажать клавишу Ctrl и, зацепив объект указателем мыши, переместить его к месту назначения при нажатой левой кнопке. При перемещении объекта (или группы выделенных объектов) вместо клавиши Ctrl нужно нажать Alt.

Другие способы выполнения этой операции:

- Если вы перетаскиваете объект в другую папку на том же диске, не нажимая при этом клавиши, то объект будет перемещен.
- Если вы перемещаете объект в другую папку на другом диске, не нажимая при этом клавиши, то объект будет скопирован.
- Если при перемещении объекта удерживать правую кнопку мыши, то после ее освобождения появится контекстное меню, из которого можно выбрать одну из команд: «Копировать» (Copy) или «Переместить» (Move).

➤ *Копирование и перемещение с использованием буфера обмена Windows.*

Буфер обмена (Clipboard) — место для временного хранения информации. Он расположен в памяти компьютера, поэтому его

содержимое при отключении питания или при перезагрузке компьютера пропадает. Хранить в нем можно: папки, документы, фрагменты текста, изображений. Используется буфер обмена для того, чтобы временно сохраненную в нем информацию можно было вставить (Paste) в другой объект.

Для работы с буфером обмена предназначено несколько специальных команд. Их можно выполнять практически во всех окнах из меню команды «Правка» (Edit).

Основные команды работы с буфером обмена:

1. «Вырезать» (Cut) — команды для переименования выделенного объекта в буфер (Ctrl+X).

2. «Копировать» (Copy) — команда для переноса копии выделенного объекта в буфер с сохранением оригинала на прежнем месте (Ctrl+C).

3. «Вставить» (Paste) — для копирования содержимого буфера обмена в позицию размещения указателя мыши или курсора (Ctrl+V).

4. «Вставить ярлык» (Paste Shortcut) — команда для размещения ярлыка со ссылкой на объект, помещенный в буфер обмена.

➤ *Переименование* (Renaming) *объекта.*

Для переименования объекта необходимо:

- выделить объект, имя которого предполагается изменить;
- выполнить команду «Файл»/«Переименовать» (File/Rename);
- ввести новое имя объекта непосредственно в поле метки значка.

➤ *Удаление* (Deleting) *объекта.*

Удаление объекта в корзину можно выполнить несколькими способами:

- с помощью команды «Файл»/«Удалить» из меню окна;
- с помощью командной кнопки  на Панели инструментов;
- воспользовавшись пунктом контекстного меню «Удалить», щелкнув правой кнопкой мыши на удаляемом объекте;
- с помощью клавиши DELETE клавиатуры, предварительно выделив объект.

➤ *Восстановление объекта.*

Восстановление объекта возможно с помощью команды меню окна «Правка»/«Отменить удаление» (Edit/Undo Delete) при оперативном восстановлении ошибочно удаленных объектов.

Возврат удаленных ранее объектов можно произвести из корзины до момента ее очистки.

➤ *Поиск* (Find) *объекта.*

Поиск объекта — операция автоматического просмотра файловой структуры, позволяющая найти некоторый объект по его характеристикам.

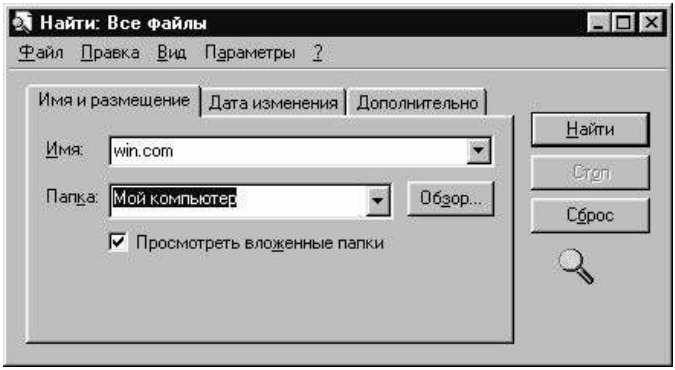


Рис. 2.5. **Окно поиска объекта в Windows**

2.3. Программы-оболочки операционной системы

Программы-оболочки предназначены для облегчения работы пользователя с операционной системой (ОС). Они позволяют пользователю наглядно представлять общее состояние информационных записей на компьютере, быстро, удобно и наглядно производить стандартные операции и выполнять команды ОС. Наиболее популярной программой-оболочкой с символьным интерфейсом много лет является Norton Commander. Несколько позже появились программы-оболочки с графическим интерфейсом, среди которых наибольшей популярностью пользуются Windows 3.*.

Norton Commander. Работа с файловой системой средствами операционной системы MS DOS достаточно неудобна. Необходимо помнить названия команд, параметров и ключей, маршруты по дереву каталогов, имена файлов и каталогов и т.д., и при этом работать лишь с одной командной строкой ОС. Программы-оболочки, одной из которых является Norton Commander (NC), облегчают работу в MS DOS, позволяют работать с программами DOS в диалоговом режиме и делают работу наглядной. NC предназначен для работы с ОС MS DOS и служит для:

- создания, переименования, копирования, удаления, пересылки и изображения дерева каталогов;
- создания, переименования, копирования, удаления, пересылки и просмотра файлов;

- редактирования файлов;
- выполнения команд MS DOS.

Принцип работы с Norton Commander. Norton Commander вызывается командой NC. При загрузке NC на экране высвечиваются два окна со списком файлов и нижняя полоса меню. Цифры 1, 2, ..., 10 нижней полосы меню соответствуют функциональным клавишам F1, F2, ..., F10. Выполнение команды происходит при нажатии на соответствующую клавишу. Переход из одного окна в другое осуществляется нажатием клавиши Tab или Ctrl-I. Для запуска исполняемого файла необходимо перевести указатель (выделенный другим цветом прямоугольник) на этот файл и нажать клавишу ENTER. Существует несколько версий программы-оболочки. Ниже мы рассмотрим русифицированную версию NC 4.

Назначение функциональных клавиш:

F1 — вызывает на экран меню помощи.

F2 — меню пользователя. Предоставляет возможность назначать функциональные клавиши и определять наиболее часто употребляемые команды.

F3 — просмотр файла. При нажатии этой клавиши происходит просмотр выбранного файла.

F4 — режим редактирования файла. Данный режим предоставляет возможность просмотра и редактирования выбранного файла посредством встроенного или внешнего редактора файлов. Если размер файла больше 32 Кбайт, то файл можно только просмотреть.

F5 — копирование файлов. Производит копирование файлов или группы файлов, выделенных клавишей Ins или «Серый+».

F6 — переименование или пересылка файлов и каталогов. Каталоги можно только переименовывать.

F7 — создание нового каталога.

F8 — удаление файлов или каталогов.

F9 — вызов верхней полосы меню (меню NC).

F10 — конец работы.

Команды меню Norton Commander:

- *Верхняя полоса меню* вызывается нажатием клавиши F9.
- *Движение вдоль полосы* производится при помощи клавиш «←» и «→».
- *Выход в подменю* производится нажатием клавиши ENTER.

- *Подменю ПРАВ.* — вызывает список параметров правого окна.
- *Подменю ЛЕВ.* — вызывает список параметров левого окна.

Параметры окна:

- Крат. — высвечивает краткую информацию (без указания размера файла, времени и даты).
- Полн. — полная информация (с указанием размера, времени и даты).
- Инф. — информация состояния текущего диска (количество байт свободной и занятой памяти и т.д.).
- Дерев. — вызывает в окно «дерево каталогов», т.е. список каталогов с текущего диска.
- Вк/Вык — производит включение и гашение окна (альтернативная команда Ctrl-F1 (Ctrl-F2)).
- Имя — устанавливает сортировку файлов окна по имени.
- Расширен. — сортировка файлов по расширению.
- Время — сортировка файлов по времени создания.
- Разм. — сортировка файлов по размеру.
- Не сорт. — отмена любой сортировки файлов.
- Считать — производит повторное считывание директории с диска (например, после смены дискеты).
- Привод — производит считывание директории с диска при задании нового имени привода (альтернативная команда — Alt-F1 (Alt-F2)).

Команды Подменю КОМАНДЫ:

- NCD дерев. — быстрая смена каталогов (команда Alt-F10).
- Иск. файл — поиск заданного файла (команда Alt-F7). Данный режим позволяет искать файл(ы) по всем директориям на данном диске.
- История — выводит на экран команды, введенные ранее в процессе работы и дает возможность их повторного выполнения (команда Alt-F8).
- Режим EGA — переключение в режим 43 строк (необходим монитор EGA) (команда Alt-F9).
- Помен. окно — меняет окна местами (команда — Ctrl-U).
- Окна вк/вык — показать/убрать окна (команда — Ctrl-O).
- Сравнить директории — сравнение директорий двух окон. Несовпадающие имена файлов выделяются другим цветом.
- Ред. файла меню — редактирование файла меню пользователя.
- Ред. файла расширения — редактирование файла расширения: при нажатии на клавишу ENTER на выделенном имени файла его обработка происходит в зависимости от расширения.

Подменю ОПЦИИ:

- Цвет — устанавливает цвет экрана.
- Ч/Б — черно-белый.
- Цветн. — цветной.
- Компакт — цвет на ЖК экране.
- Авто меню — если ВКЛ., то при первоначальной загрузке NC на экране появляется меню пользователя.
- Подсказка — если ВКЛ., то высвечивается имя текущего привода и директории, если ВЫКЛ., то только имя привода.
- Ключи — включает/выключает нижнюю полосу меню.
- Сжать окно — сжимает окно до половины или расширяет на весь экран.
- Мини статус — включает/выключает справочную информацию в последней строке окна о файле, на котором стоит указатель.
- INS (сдвиг вниз) — включает/выключает режим сдвига вниз при нажатии клавиши INS.
- Часы — высвечивает в правом верхнем углу экрана текущее время.
- Редактор. — предоставляет возможность установить внутренний или любой внешний редактор.
- Зап. устан — записывает установленные пользователем параметры NC в файл NC.INI (альтернативная команда Shift-F9).

Редактирование файлов меню и расширения. NC позволяет выполнять команду или группы команд MS DOS, используя меню, в котором перечислены действия пользователя. Формат файла меню пользователя следующий:

- Строка комментария — в первой колонке должен стоять апостроф « ‘ »;
- m: Метка меню — при нажатии на клавишу «m» последовательно выполняются команды из файла меню пользователя;
- первая команда (любая команда MS DOS);
- следующие команды MS DOS.

Пример:

1. F1: Запуск редактора ЛЕКСИКОН
c:\lex\lexicon
Проверка диска с помощью программы ДОС chkdsk.com
2. F2: Проверка диска
Chkdsk /f
del *.chk
3. F3: Просмотр архивных файлов
Pkxarc — v * и т.д.

При нажатии клавиши F2 появится меню пользователя:
F1: Запуск редактора ЛЕКСИКОН

F2: Проверка диска

F3: Просмотр архивных файлов

Можно выбрать один из трех пунктов меню при помощи курсора или непосредственно, нажав нужную функциональную клавишу. В результате произойдет выполнение выбранной команды.

Если в NC перевести указатель на нужный файл и нажать клавишу ENTER (ВВОД), то действие произойдет в зависимости от расширения файла. Если файл имеет расширение COM, EXE или BAT, то файл запускается на выполнение. Для других расширений действие не определено и можно установить любое действие. Например, для файлов с расширением TXT можно определить действие вызов редактора текстов. Для этого надо создать файл NC.EXT. Формат файла расширения следующий — каждая его строка имеет вид:

расширение: *команда* [параметры],

причем в расширении можно использовать символы «*» и «?».

В команду можно передать следующие параметры:

! — имя файла без расширения;

!.! — имя файла с расширением;

!\ — путь к текущему каталогу;

!: — имя текущего устройства;

!! — символ «!».

Пример:

```
txt: lexicon !.!   txt — расширение файла, lexicon — команда DOS.
arc: d:\exe\pkxarc — v !
asm: masm !
*: rem Этот файл нельзя обработать.
```

Расширение «*» в последней строке примера означает, что действие для остальных расширений не определено.

Быстрый поиск по имени файла. Если надо найти нужный файл среди множества других с похожими именами в текущей директории, нажимают клавишу Alt и, не отпуская ее, набирают имя этого файла. NC будет находить и выделять то имя файла, начальные буквы которого совпадают с набираемыми. То же правило применимо и к директориям.

Поиск заданного файла по всем директориям на выбранных дисках позволяет осуществить команда Alt-F7.

Быстрое передвижение по директориям. Если надо быстро перейти в предыдущую директорию, нажимают сочетание клавиш Ctrl-PgUp. Для перехода в корневую директорию текущего диска нажимают Ctrl-\.

2.4. Алгоритмические языки для персонального компьютера

Алгоритмические языки представляют собой средства описания данных и алгоритмов решения задач, они разработаны для составления программы пользователем. В настоящее время разработано большое количество языков программирования. Они отличаются друг от друга различными свойствами и областью применения.

Класс машинно-зависимых языков представлен ассемблером. Язык ассемблера делает доступными все программно-управляемые компоненты компьютера, поэтому он применяется для написания программ, использующих специфику конкретной аппаратуры. Ассемблер — это наиболее трудоемкий язык программирования, и из-за его низкого уровня не удается построить средства отладки, которые существенно снизили бы трудоемкость разработки программ. Программирование на ассемблере требует от программиста детальных знаний технических компонентов ПК. Ассемблер используется в основном для системного программирования (компоненты ОС, драйверы и др.).

Класс машинно-ориентированных языков представляют языки группы С − С, C^{++}, Турбо С. Эти языки являются результатом попытки объединить возможности ассемблера со встроенными структурами данных.

Класс универсальных языков программирования представлен наиболее широко (Бейсик, Паскаль, Фортран и др.).

Исторически одним из самых распространенных языков стал Бейсик. Он прост в освоении и использовании. Написать на этом языке программу в 20—30 строк и получить результат можно за несколько минут. Для различных типов ПК разработаны различные версии языка Бейсик.

Паскаль также является одним из самых распространенных языков программирования, хотя он и создавался как учебный. Использование в структуре языка специального кода позволило уменьшить в 4—5 раз длину текста программы и в 4—5 раз увеличить быстродействие программы. Версия Паскаля для ПК — Турбо-Паскаль — характеризуется такими важными особенностями, как полноэкранное редактирование и управление, графика, звуковое сопровождение и развитые связи с DOS. Система программирования на Турбо-Паскале является резидентной программой. Это позволяет пользователю вводить тексты программ и немедленно их выполнять, не тратя время на компилирование.

Язык Кобол был разработан специально для решения экономических задач. Он дает возможность составлять наиболее удобочитаемые программы, которые понятны и непрограммисту. В обработке данных сложной структуры Кобол бывает эффективнее Паскаля.

Фирмой «IBM» в развитие идей Фортрана, Алгола и Кобола был предложен язык PL/1, который получил наибольшее распространение на больших машинах. PL/1 разрабатывался как универсальный язык программирования, поэтому он располагает большим набором средств обработки цифровой и текстовой информации. Однако эти достоинства делают его весьма сложным для обучения и использования.

Класс проблемно-ориентированных языков программирования представлен языками Лого, РПГ и системой программирования GPSS. Язык Лого был создан с целью обучения школьников основам алгоритмического мышления и программирования. Лого – диалоговый процедурный язык, реализованный на основе интерпретатора с возможностью работы со списками и на их основе с текстами, оснащенный развитыми графическими средствами, которые доступны для детского восприятия. Этот язык реализован в большинстве ПК, применяемых в школах.

РПГ, или генератор отчетов, представляет собой язык, включающий многие понятия и выражения, которые связаны с машинными методами составления отчетов и проектирования форм выходных документов. Язык используется главным образом для печати отчетов, записанных в одном или нескольких файлах баз данных.

Система программирования GPSS ориентирована на моделирование систем с помощью событий. В терминах этого языка легко описывается и исследуется класс моделей массового обслуживания и другие системы, работающие в реальном масштабе времени.

В последние годы развивается ***объектно-ориентированный*** подход к программированию. Наиболее полно он реализован в языках Форт и СМОЛТОК. Форт сочетает в себе свойства операционной системы, интерпретатора и компилятора одновременно. Основной чертой языка является его открытость. Программист может легко добавлять новые операции, типы данных и определения основного языка. Форт позволяет поддерживать многозадачный режим работы, использует принцип одновременного доступа программ.

Класс функциональных языков программирования представлен языками Лисп, Пролог и Снобол. Лисп является инструментальным средством для построения программ с использованием методов искусственного интеллекта. Особенность этого языка заключается в удобстве динамического создания новых объектов. В качестве объектов могут выступать и сами исходные объекты. В настоящее время

для Лиспа определились две сферы активного применения: проектирование систем искусственного интеллекта и анализ текстов на естественном языке.

Нетрудно заметить, что языка идеального для всех случаев не существует. Какой язык является лучшим, надо определять в каждой конкретной ситуации. Поэтому перед разработкой программы следует установить:

а) назначение разрабатываемой программы;
б) время выполнения программы;
в) ожидаемый размер программы (хватит ли объема памяти);
г) необходимость сопряжения программы с другими пакетами или программами;
д) возможность и необходимость переноса программы на другие типы компьютеров;
е) основные типы данных, с которыми будет работать программа;
ж) характер и уровень использования в программе аппаратных средств (дисплея, клавиатуры; НМД и др.);
з) возможность и целесообразность использования стандартных библиотек программ.

Контрольные вопросы и задания

1. Как представляется информация в компьютере?
2. Каково назначение основных компонентов ОС MS DOS?
3. Что такое *каталог-отец*, *дочерний*, *подчиненный* каталог?
4. Что такое *файл данных*?
5. Сколько символов содержит имя файла? Из каких символов может состоять имя?
6. Для чего используется расширение имени файла? Из скольких символов оно может состоять, с чего начинается?
7. Назовите основные запрещенные имена файлов.
8. Назовите основные общепринятые расширения имен файлов.
9. Что такое спецификация файла? Приведите примеры спецификации файлов.
10. Что такое маршрут или путь в файловой структуре?
11. Объясните разницу между понятиями абсолютного и относительного маршрутов?
12. Что такое полная спецификация файла?
13. Для чего используются шаблоны или групповые имена файлов? Поясните следующие шаблоны имен: *.exe, a*.com, ??b.bas, *.*, prg1.*, a*.*, b??.bas
14. Приведите примеры имен файлов, отвечающих шаблонам petr??.txt, petr?.???, petrov.t??

15. Что такое *корневой каталог диска* и как он обозначается? Ограничен ли размер корневого каталога?
16. Какой каталог называется рабочим? С каким количеством рабочих каталогов постоянно работает пользователь?
17. Как обозначается каталог-отец в командах MS DOS?
18. Какие возможности дает использование на дисках каталогов древовидной структуры?
19. Какой диск называется текущим?
20. Какое устройство дисковой памяти обозначается идентификатором C: ?
21. Что такое *полное имя файла*, *полное имя каталога*?
22. Какая информация о файлах, кроме имени, хранится в компьютере? По какой команде ее можно получить?
23. Что такое *приглашение операционной системы*? Как оно выглядит? Какой стандартный вид приглашения? Какая команда изменяет вид приглашения?
24. Какие виды команд MS DOS вы знаете? Приведите примеры команд каждого вида.

Часть II

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Глава 3

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ОСНОВНЫЕ ПОНЯТИЯ, КРАТКАЯ ИСТОРИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Своим формированием человеческое общество обязано общественному труду и информационным процессам и технологиям, которым столько тысячелетий, сколько существует человеческое общество.

Информационные технологии — это система приемов, способов, методов осуществления информационных процессов.

Часто под информационными технологиями понимают также 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 новый термин — *информационно-коммуникационные технологии* (ИКТ).

Потребность человека общаться с окружавшими его людьми, т.е. выразить и передать информацию, привела к появлению языка и речи — древнейшей информационной технологии.

Речь — это язык в действии. Она участвует не только в передаче сведений от одного человека собеседникам, но и во всех сознательных процессах самого человека. 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. Воспринимаемые нами предметы в своем сознании мы называем словами-понятиями: «дождь», «снег», «небо», «земля» и т.д. Считаем «в уме» мы тоже с помощью слов, обозначающих числа и арифметические действия: «один», «два», «три», «четыре», «сложить», «вычесть», «умножить», «разделить». Например: «Шесть умножить на восемь равно сорока восьми», — говорим мы «в уме».

Зрительные, звуковые и другие впечатления человек запоминает в виде образов, а смысловую информацию — в виде слов.

Речь представляет собой самую древнюю *природную информационную технологию*, 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*.

Дальнейшие этапы развития информационных технологий — это изобретение книгопечатания, почты, телеграфа, телефона, радио, телевидения, космической связи и, наконец, компьютеров.

Информационные технологии следует делить по принципу — до появления компьютеров и после их появления. Появление компьютеров — это новая эра информационных технологий (цифровая).

Однако не следует забывать, что эра компьютеров не могла наступить без основополагающих открытий в области электричества, и, прежде всего, без работ Л. Гальвани, А. Вольта, А.М. Ампера, М. Фарадея, Д. Максвелла, Г. Герца, А.И. Попова.

Появление и широкое распространение компьютеров обеспечило человеку совершенно новые возможности поиска, получения, накопления, передачи и, главное, обработки информации.

К информационным технологиям относятся средства записи, хранения, обработки, передачи на расстояния (средства связи — сигнализация, почта, телеграф, телефон, радио, телевидение) и воспроизведения информации.

Человек живет в пространстве и времени. В пространстве он может перемещаться, в том числе с помощью различных видов транспорта — от телеги до космического корабля. Но во времени он перемещаться не может — ни в прошлое, ни в будущее.

Существуют два способа получения информации — *синхронный* и *асинхронный*. При синхронном способе ее получатель должен присутствовать при самом событии — разговоре (неважно каком — устном или телефонном), показе телефильма или радиопередаче. Если он в этот момент отсутствовал, то он эту информацию не получит. Для ее получения он должен синхронизироваться по времени с ее передачей. Это всегда вызывает массу неудобств. Поэтому человек всегда, с момента изобретения письменности, старался «законсервировать информацию» — о событиях, при которых он не присутствовал лично, либо о событиях, при которых он присутствовал, но хотел бы сохранить их в памяти, чтобы снова узнать о них в любое удобное для него время. Это и есть асинхронный способ получения информации, обеспечивающий свободу выбора.

Уже давно проигрыватель, магнитофон, автоответчик и видеомагнитофон обеспечивают асинхронный способ: информацию с их помощью можно получить в любое время.

Информационные технологии дают возможность человеку получать информацию о событиях не только в данном месте и настоящем времени, но и в других местах и прошлом времени. Информацию о событиях в других местах обеспечивают средства связи, информа-

цию о событиях в прошлом времени — физические тела — *носители информации* или *устройства памяти* (камень, бумага, книга, грампластинка, фотография, кинопленка, магнитная пленка, компакт-диск, дискета, карта флэш-памяти и др.), в которые эта информация вносится и 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.

Поток информации, который получал древний человек, был ограничен. Информация помогла древнему человеку выжить среди опасностей дикой природы.

Современный человек получает большой объем разнообразной информации: знания, приобретенные при общении с другими людьми, результаты наблюдений за животными; содержание книг, газет, журналов; сообщения по радио и телевидению; реклама; впечатления от посещения кино, театров, музеев и концертов, прослушивания звукозаписей, туристических поездок и многое другое.

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.

За последние годы появилось понятие «Пи-Ар» (пиар) (от англ. *public relations* (PR) — общественные отношения), особый вид деятельности, направленный на формирование общественного мнения по широкому спектру вопросов (политическая акция, избирательная кампания, бизнес, производство, благотворительность, реклама и т.д.). Связь с общественностью осуществляется специалистами в области пиар (так называемыми «пиарщиками») посредством рекламы, паблисити, постоянных контактов со СМИ и др.

Существуют также специальные информационные технологии для общения со слепыми (воспринимаемый наощупь шрифт Брайля в книгах для слепых) и глухими: дактилология — своеобразная форма речи, воспроизводящая слова пальцами рук, и дактилография — письмо пальцем на любой удобной для письма поверхности. *Дактилология* — азбука для глухонемых — используется как заменитель устной речи для общения слышащих с глухими, глухих между собой и как средство обучения глухих, а также для сурдоперевода в телевидении. *Дактилография* используется как вспомогательное средство общения с глухим или слепоглухим (слова пишутся на его ладони пальцем).

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.

Появление компьютеров — машин для переработки информации — это новая эра информационных технологий — *цифровая*, открывающая спектр возможностей. В связи с их появлением и стремительным внедрением практически во все стороны нашей жизни и стал применяться термин «информационные технологии», хотя они, начиная с освоения языка и речи, существовали с самого начала формирования человеческого общества.

Особенность современных информационных технологий по сравнению с промышленными технологиями заключается в том, что в ней и предметом, и продуктом труда является информация, а орудиями труда служат средства вычислительной техники и связи.

Информационные технологии делятся на аналоговые и цифровые.

Аналоговые технологии основаны на способе представления информации в виде какой-либо непрерывной (аналоговой) физической величины, например напряжения или силы электрического тока, значение которых (сигнал) является носителем информации.

Цифровые технологии основаны на дискретном способе представления информации в виде чисел (обычно с использованием двоичной системы счисления), значение которых является носителем информации.

Простота цифровых сигналов обеспечивает (по сравнению с аналоговыми сигналами) их несоизмеримо бóльшую 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. В этом состоит главное преимущество цифровых вычислительных устройств по сравнению с аналоговыми. Современные персональные компьютеры оперируют с 32-разрядными двоичными числами. В ближайшем будущем предстоит переход на 64-разрядную структуру.

Цифровые технологии, имеющие столь очевидные преимущества, не могли появиться раньше аналоговых. Причина в том, что аналоговые технологии значительно проще цифровых, и поэтому именно они могли быть осуществлены на уровне техники прежних времен.

Органы чувств человека (и прежде всего органы слуха) способны воспринимать в основном аналоговые сигналы. Поэтому для применения цифровых технологий нужны достаточно сложные устройства (компьютеры, аналого-цифровые и цифроаналоговые преобразователи), массовое использование которых стало возможным только

в последние десятилетия в результате стремительного развития микроэлектроники.

Цифровое представление информации дало возможность создать мультимедиа (англ. *multimedia*, от *multi* — много и *media* — средство), компьютерную технологию, которая обеспечивает соединение нескольких видов связанной между собой информации (текст, звук, фото, рисунок, анимация, видео и др.) в единый носитель такой информации. Таким мультимедийным носителем является, например, оптический компакт-диск CD-ROM.

XXI век будет «цифровым». Сегодня происходит непрерывная конкурентная борьба между новейшими, например, магнитными и оптическими методами записи, хранения и воспроизведения различных видов информации, а также их комбинированное использование. Эти методы обеспечивают гораздо более высокую плотность и долговечность записи информации по сравнению с записью на бумаге, фото- и кинопленке и поэтому вытесняют эти традиционные носители информации и связанные с ними информационные технологии. На наших глазах за последние годы магнитная пленка, так же как кино- и фотопленка, отживает свой недолгий (по сравнению с бумагой) век и уступает свое место оптическим дискам, жестким магнитным дискам и твердотельной флэш-памяти. Миниатюрные карточки флэш-памяти, в отличие от магнитной и оптической памяти, не требуют применения дисководов с использованием сложной высокоточной механики и не содержат ни одной подвижной детали, поэтому за ними будущее.

Областями применения информационных технологий стали практически все сферы жизни: государственное и муниципальное управление, экономика, хозяйственная деятельность, промышленность, строительство, транспорт, связь, оборона, научные исследования, образование, медицина, сфера развлечений и досуга.

Наиболее важные цифровые информационные технологии нашего времени — сотовая мобильная связь, Internet, электронная почта, волоконно-оптические линии связи, цифровые фотография и видеосъемка, цифровые кино и телевидение, оптическая цифровая запись звука и изображения, 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 засекречивания информации в криптографии, цифровые методы идентификации личности, система беспроводной передачи данных *Bluetooth* («Синий зуб») и *Hand 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, построенных на базе бурно прогрессирующей микроэлектроники.

В США услугами сотовой телефонной связи пользуются примерно 81 млн чел., что составляет более 31% от общей численности населения страны.

В странах Европы, включая Россию, этот показатель выше — примерно 33,8% всего населения. Максимальный в мире показатель — в Финляндии: 63,5% населения страны владеют сотовыми телефонами.

Число пользователей сотовой связи в России в 2000 г. составляло 3,3 млн чел., в 2001 г. — 7,8 млн чел., в 2002 г. — 17,7 млн чел., в 2003 г. — 32 млн чел. При этом уровень обеспеченности сотовой связью на конец октября 2003 г. в Москве и Московской области составляет 63%, в Петербурге и Ленинградской области — 51%, а в других регионах России — 22%. Особой популярностью сотовая связь пользуется у молодежи.

Создание информационной сети Internet и электронной почты (E-mail) позволило любому владельцу персонального компьютера приобщиться к информационным ресурсам всего человечества и даже внести в них свою долю. Ведь при объединении множества компьютеров с помощью средств связи в Сеть происходит объединение носителей информации каждого из них в один общий банк информации для всех пользователей этой сети, а это открывает поистине неограниченные возможности для получения любой информации.

Особую часть сети Internet составляет *электронная почта* (E-mail). Значительная часть пользователей сети Internet подключается к ней ради пользования E-mail. Для этого каждый ее пользователь снабжается специальным электронным адресом.

Главное преимущество электронной почты — скорость доставки независимо от географического положения отправителя письма и получателя. Но и отправитель, и получатель для этого должны иметь компьютеры и доступ к электронной почте.

Число пользователей сети Internet стремительно возрастает с каждым годом. 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. К концу 2000 г. в России уже было 7,8 млн пользователей, в 2001 г. — 11 млн, в 2002 г. — около 12 млн (из них в Москве — 19%). В 2003 г. с лета до осени их число возросло на 1 млн (а ведь еще в 1996 г. их число составляло всего 0,4 млн чел.).

Предполагается, что в мире число пользователей Internet в 2005 г. возрастет до 1 млрд чел. (15% населения Земли).

Технологии Internet — это еще одна экономическая и техническая революция в конце XX века с переходом в третье тысячелетие. До настоящего времени информационные технологии только об-

служивали экономику, а теперь они начинают создавать ее. По прогнозам аналитиков объем интернет-экономики в начале XXI века достигнет десятков триллионов долларов.

Цифровые технологии серьезно изменили фотографию и видеосъемку. Вместо традиционной фотопленки используются полупроводниковые матрицы, которые состоят из множества микроскопических светочувствительных элементов (пикселей), — приборы с зарядовой связью (ПЗС). Объектив цифрового фотоаппарата фокусирует оптическое изображение на миниатюрной ПЗС-матрице, которая превращает его в электрические сигналы — заряды на каждом пикселе. Эти сигналы в цифровой форме записываются на дискету или полупроводниковые носители — миниатюрные флэш-карты. А дальше эти 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.

Качество цветных цифровых фотографий уже превзошло качество традиционных. Цифровой фотоаппарат снабжен жидкокристаллическим дисплеем, на котором сделанный снимок появляется сразу же после нажатия кнопки. Никакого проявления и закрепления изображения при этом не требуется. Если снимок не понравился, его можно «стереть» и на его место поместить новый. В цифровой фотографии полностью исключается использование светочувствительных материалов с солями дефицитного серебра. В видеосъемке цифровые технологии обеспечивают возможность многократной переписи изображений без потери качества и значительно большие возможности при монтаже видеофильмов.

Серийно выпускаются сотовые телефоны, в которые встроена цифровая видеокамера или фотокамера.

Существуют системы идентификации личности по радужной оболочке глаза. Сравнение рисунка считанного образца и идентификация личности занимают всего несколько секунд. Распознавание по радужной оболочке устраняет необходимость в паролях и пропусках. При этом отпадают проблемы, связанные с их потерей, повреждением или кражей, а также с забыванием пароля. Большую помощь распознавание по радужной оболочке может оказать в борьбе с терроризмом.

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, не выходя из дома.

Информационная сеть будет играть главную роль в процессе образования. Она способна объединить труды и способности лучших

преподавателей и лекторов. Школьные учителя и преподаватели высших учебных заведений смогут использовать их материалы в своей работе, а школьники и студенты смогут изучать их в интерактивном режиме.

Информационная сеть создаст *равные возможности* в получении образования всем желающим учиться.

Информационная сеть Internet создает условия для домашней работы пенсионеров, инвалидов, беременных женщин и кормящих матерей, которые могут с помощью домашних компьютеров выполнять задания, не выходя из дома (при этом разгружается транспорт).

Все это — *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 бóльшая 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. Значительно ускорилось его создание 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.

В России реализуется Федеральная целевая программа «Электронная Россия». Эта программа информатизации России рассчитана на 9 лет. В нее будут произведены инвестиции на сумму около 2,4 млрд долл. Согласно программе к 2007 г. доля продукции индустрии информационных технологий (ИТ) в российском ВВП должна возрасти с нынешних 0,5% до 2%, а объем экспорта высоких технологий увеличится в 15—20 раз (до 2,5 млрд долл.). Программа предусматривает внедрение новых информационных технологий в государственных органах и частном секторе, создание образовательных программ, призванных повысить уровень компьютерной грамотности россиян, и построение масштабной сети коммуникаций. В результате реализации программы будут подключены к Internet все российские вузы и больше половины школ, созданы электронные библиотеки, внедрены системы телемедицины и т.д.

Появилось понятие «электронное правительство» — *Electronic government* (e-Government) — система государственного управления

на основе электронных средств обработки, передачи и распространения информации. Одна из главных задач этой системы — перенос общения каждого отдельного гражданина с государственными чиновниками в электронную почту. Прозрачность этого общения должна снизить уровень коррупции чиновников и значительно ускорить решение любых вопросов, касающихся отношений граждан с государством.

Таким образом, информационное общество — это концепция постиндустриального общества, новая историческая фаза развития цивилизации, в которой главными продуктами производства являются информация и знания.

Основные этапы в развитии информационных технологий:

1. *Появление языка и устной речи.* 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.

2. *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.

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

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

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

6. *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.

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

8. *Изобретение всемирной сети Internet и электронной почты*, позволяющих отдельным людям пользоваться информационными ресурсами всего человечества, вносить свой личный вклад в эти ресурсы и общаться между собой, с частными и государственными организациями.

Знание работниками правоохранительных органов современных информационных технологий и оснащение их передовой цифровой вычислительной техникой окажет серьезную помощь в борьбе с преступностью и международным терроризмом. При этом следует

учитывать, что преступный мир уже хорошо знаком с передовыми информационными технологиями и владеет современными средствами вычислительной техники.

Контрольные вопросы и задания

1. Дайте определение понятия «информационные технологии».
2. Способы получения «синхронной» и «асинхронной» информации.
3. Что такое «*носители информации*»?
4. В чем различие между аналоговыми и цифровыми технологиями?
5. Что такое «*мультимедийные компьютерные технологии*»?
6. Перечислите основные области применения информационных технологий.
7. Назовите наиболее важные информационные цифровые технологии.
8. В чем состоят основные признаки информационного общества?
9. Назовите основные этапы развития информационных технологий.
10. В чем состоит идея мобильной сотовой связи?
11. Чем отличается цифровой фотоаппарат от традиционного пленочного?

Глава 4

АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Современные информационные технологии включают в себя две обязательные составляющие — аппаратное (*hardware*) и программное (*software*) обеспечение, дополняющие друг друга.

К аппаратному обеспечению относятся:

- 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;
- световое перо;
- графические планшеты;
- внешние запоминающие устройства (дискеты, жесткие диски, стримеры, оптические диски, магнитооптические диски, флэш-память и др.);
- клавиатура;
- компьютерная мышь;
- трекбол;
- тачпад;
- трекпойнт;
- джойстик;
- системный блок компьютера;
- мониторы;
- акустические системы;
- принтеры;
- плоттеры и др.

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. Такая операция называется квантованием. Такая последовательность 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 2^{16}, равное 65 536 уровням 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.

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. Ведь человек способен слышать только аналоговые сигналы звукового давления. Для улучшения качества звука при этом используются специальные фильтры.

Цифроаналоговый преобразователь превращает последовательность двоичных чисел в ступенчатый аналоговый сигнал, значения ступеней которого равны значениям этих двоичных чисел. Для превращения этого ступенчатого сигнала в «гладкий» аналоговый сигнал его пропускают через фильтр нижних частот с верхней границей полосы пропускания, равной 20 кГц. Этот «гладкий» аналоговый сигнал почти полностью соответствует аналоговому сигналу, который был подан на вход аналого-цифрового преобразователя (рис. 4.1).

Подобное преобразование с помощью АЦП и ЦАП происходит и в ***модеме*** (*модуляторе-демодуляторе*) персонального компьютера. Модем [от англ. *mo*(*dulator*) и *de*(*modulator*], 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.

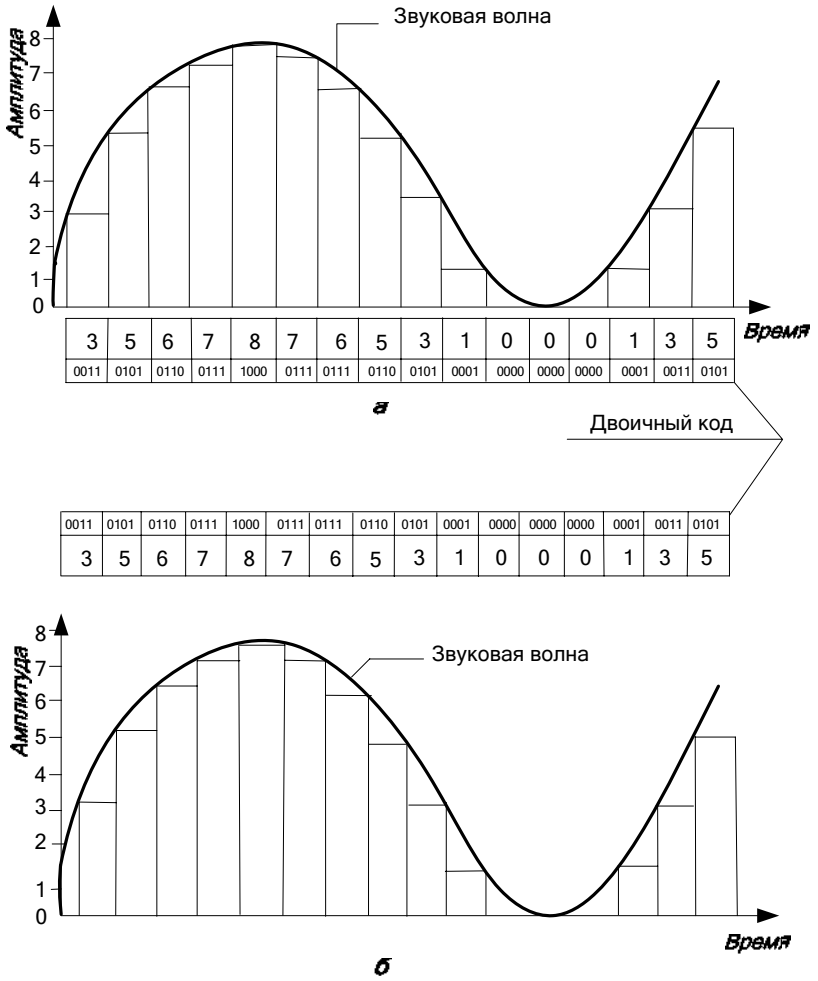


Рис. 4.1. **Аналого-цифровой (*а*) и цифроаналоговый (*б*) преобразователи звука**

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 из которых 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 происхо-

дит 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. Датчики, представляющие собой оптические пары (светодиод — фотодиод), располагаются по разные стороны дисков с прорезями. Порядок, в котором освещаются фоточувствительные элементы, определяет направление перемещения мыши, а частота приходящих от них импульсов — скорость. Хороший механический контакт с поверхностью обеспечивает специальный коврик. Мышь имеет две кнопки (правую и левую), а некоторые — еще и колесико «скроллер» для прокрутки текста на экране компьютера. Более точного позиционирования курсора позволяет добиться оптическая мышь.

Кроме подачи команд с помощью мыши можно создавать и 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. Собственный контроллер посылает импульсы по расположенной под поверхностью планшета сетке проводников. Получив два таких сигнала, контроллер преобразует их в координаты, передаваемые в персональный компьютер, который переводит эту информацию в координаты точки на экране монитора, соответствующие положению указателя на планшете. Планшеты, предназначенные для рисования, обладают чувствительностью к силе нажатия пера, преобразуя эти данные в толщину или оттенок линии.

Графический планшет по сравнению с компьютерной мышью дает возможность сделать гораздо более качественные рисунки. Обычно в комплект планшета кроме пера входит и мышь, что позволяет использовать их совместно при создании рисунков.

Трекбол (*trackball*) — шаровой манипулятор, является разновидностью мыши, применяемой в портативных ПК — ноутбуках (*notebook*). Рука приводит в движение не корпус мыши, а сам шарик, поэтому он занимает меньше места, что важно при малых габаритах ноутбука. Обычно шарик трекбола встроен в клавиатуру. Большого

распространения в ноутбуках трекболы не получили из-за своего недостатка — постепенного загрязнения поверхности шара и направляющих роликов, которые трудно очищать. Впоследствии их заменили тачпады и трекпойнты.

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 переменными резисторами, изменяющими свое сопротивление при ее перемещении. Один резистор определяет перемещение по координате *X*, а 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. В ней сопоставляется время появления сигнала с синхросигналом развертки изображения. В результате определяется положение светового пера на экране. 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.

Внешние запоминающие устройства делятся на *носители* и *накопители*. ***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, так как информация на них записывается только один раз, а затем

хранится. Дискета и стример представляют собой накопители, так как информация может на них записываться, храниться и стираться, а затем многократно записываться и храниться новая информация.

Дискета — это кассета с гибким магнитным диском (флоппи-диском), устройство для записи, хранения информации и для ее перемещения с одного персонального компьютера на другой. Современная дискета представляет собой гибкий флоппи-диск диаметром 3,5 дюйма из искусственной пленки — майлара с магнитным покрытием, заключенный в жесткий пластмассовый футляр. Емкость ее памяти — 1,44 Мбайт. Для чтения и записи информации дискета помещается в специальное электронно-механическое устройство — дисковод. Дискета имеет центральное отверстие под шпиндель привода дисковода, а в футляре сделано отверстие для доступа магнитных головок чтения и записи. Оно закрыто металлической шторкой. Гибкий диск разбит на концентрические дорожки, а они, в свою очередь, разбиты на секторы. Чтение и запись производятся с помощью блока магнитных головок дисковода. Они перемещаются с помощью привода позиционирования дисковода по радиусу гибкого диска для доступа к различным дорожкам. Доступ к различным секторам внутри каждой дорожки происходит за счет вращения гибкого диска с помощью привода дисковода.

Основные внутренние узлы дисковода — дискетная рама, шпиндельный двигатель, блок магнитных головок со своим приводом и плата управляющей электроники.

Плоский шпиндельный двигатель обеспечивает вращение дискеты с постоянной скоростью 300 об/мин. Двигатель привода магнитных головок обеспечивает их движение с помощью зубчатой, червячной или ленточной передачи.

Информацию на флоппи-диск можно записывать неоднократно, поэтому дискеты широко используются, несмотря на недостаточную надежность и сравнительно небольшую емкость. На корпусе дискеты имеется переключатель, разрешающий или запрещающий запись информации на флоппи-диск. Запись разрешена, если отверстие в корпусе дискеты перекрыто переключателем, и запрещена, если это отверстие открыто. Запись производится на обе стороны поверхности флоппи-диска.

Перед первым использованием дискеты ее необходимо отформатировать. Эту операцию проводит компьютер с помощью специальной программы. При форматировании проверяется пригодность к записи поверхности флоппи-диска. Дефектные участки помечаются и в дальнейшем запись информации на них не производится. Бóльшая часть выпускаемых дискет продается заранее отформатированными. Скорость чтения или записи для современного 3,5-дюй-

мового дисковода составляет около 63 Кбайт/с, среднее время поиска информации — примерно 80 мс.

Дисковод располагает двумя двигателями: один вращает флоппи-диск (в зависимости от типа дискеты со скоростью от 300 до 360 об/мин), а второй перемещает головки записи и чтения по радиусу флоппи-диска от края диска к центру. Работой всех узлов дисковода управляет специальный контроллер.

***Жесткий диск* (*винчестер*)** — устройство для постоянного хранения информации, используемой при работе персонального компьютера. Свое название жесткий диск получил благодаря конструктивным отличиям от накопителей информации на гибких магнитных лентах и гибких дисках.

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, укрепленными на поворотных рычагах-позиционерах. Головки не касаются поверхностей дисков, а перемещаются над ними на расстоянии долей микрометра.

Головки записи/считывания перемещаются над поверхностью дисков на расстоянии не более 0,07 мкм. Зазор между ними создается воздушным потоком, а сам поток — непрерывным вращением пакета дисков.

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.

Под пакетом дисков со шпинделем размещается двигатель. При вращении пакета дисков создается сильный поток воздуха, который циркулирует по периметру гермоблока и непрерывно очищается фильтром.

Емкость винчестеров современных персональных компьютеров достигает более 80 Гбайт, а в настоящее время приближается к 1 Тбайт (терабайт).

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. Современные винчестеры обеспечивают доступ к информации за 8—10 мс.

Другой характеристикой винчестера является скорость чтения и записи, но она зависит не только от самого диска, но и его контроллера, шины, быстродействия процессора. У стандартных современных жестких дисков эта скорость составляет 15—17 Мбайт/с.

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. Стримеры представляют собой кассеты — картриджи с двумя или с одной бобиной. При этом используется два способа записи: линейно-серпантинный или способ с наклонными дорожками (как в видеомагнитофонах). В первом случае магнитная головка неподвижна относительно ленты. Во втором случае магнитные головки устанавливаются на вращающемся барабане, который охватывается магнитной лентой. Способ записи с наклонными дорожками сложнее линейно-серпантинного. Линейно-серпантинным способ называется потому, что запись производится от начала до конца одной из параллельных дорожек, после чего продолжается на соседней дорожке в обратную сторону. Емкость магнитной ленты в одном картридже может составлять до 40 Гбайт.

Магнитная лента не обеспечивает, в отличие от дисков, возможности прямого доступа к записанной на ней информации, так как ее сначала нужно перемотать на нужное место. Это существенно увеличивает время считывания информации с ленты. Но у нее по сравнению с диском есть и бесспорное преимущество — гораздо бóльшая поверхность магнитного слоя, ограниченная только длиной ленты, а, следовательно, и бóльшая емкость. Это ее свойство используется для резервного копирования информации, в котором скорость считывания не так важна.

Разные типы стримеров отличаются по емкости (от 20 Мбайт до 40 Гбайт), интерфейсу, скорости чтения и записи данных (от 100 Кбайт/с до 5 Мбайт/с и более).

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. Однако следует указать, что оптические диски боятся глубоких царапин и прямых солнечных лучей.

Основной возможностью увеличения емкости оптических дисков является уменьшение расстояний между дорожками и размеров пит за счет уменьшения длины волны лазерных диодов.

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. Время просмотра видеофильмов на мониторе персонального компьютера в стандарте VideoCD составляло также 74 мин. Поэтому для размещения фильма стандартной длительности требовалось два диска. Однако теперь разработана технология сжатия информации MPEG, с помощью которой обеспечивается коэффициент сжатия до 200:1. Это позволяет разместить фильм на одном диске, а длительность музыкальной записи доходит до 11 ч. К оптическим дискам относятся и диски нового стандарта DVD.

Кроме дисков «только для чтения информации» существуют и диски как для однократной CD-R, так и многократной CD-RW записи информации.

CD-ROM (только для чтения). 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* — т.е. 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, т.е. по емкости он занимает промежуточное положение между дискетами и винчестером. 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. Поэтому такие диски легко повредить. Информация на диске кодируется чередованием пит и промежутков между ними, расположенными вдоль дорожки.

В состав дисковода или привода CD-ROM входят плата электроники, шпиндельный двигатель, устройство загрузки диска и система считывающей оптической головки. Шпиндельный двигатель приводит диск во вращение. В состав системы считывающей головки входят сама оптическая головка и система ее перемещения. В головке находятся лазерный излучатель (на основе лазерного инфракрасного светодиода), система фокусировки лазерного луча, фотоприемник и предварительный усилитель. Система перемещения головки содержит собственный двигатель, который приводит в движение каретку с оптической считывающей головкой при помощи червячной или зубчатой передачи.

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. Иногда вместо лотка применяется специальный футляр для диска (*caddy*). Система загрузки содержит двигатель, который обеспечивает движение лотка (или футляра) и механизма перемещения рамы. На передней панели дисковода размещаются: кнопка Eject загрузки/выгрузки оптического диска, индикатор обращения к дисководу и гнездо для подключения наушников с регулятором громкости. Обычно на передней панели имеется отверстие для аварийного извлечения диска. При выходе из строя лотка или всего дисковода, при исчезновении питания необходимо вставить в это отверстие шпильку или распрямленную скрепку и осторожно нажать. При этом снимается механическая блокировка лотка и его можно выдвинуть вручную.

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. В двух- и более скоростных CD-ROM диск вращается с пропорционально большей скоростью. При этом пропорционально повышается скорость передачи информации.

Как уже отмечалось, на дисководе CD-ROM можно проигрывать и звуковые диски, но эта функция для них является побочной. Обычно в них применяются простейшие цифроаналоговый преобразователь (ЦАП) и выходной усилитель. Поэтому они значительно уступают по качеству передачи звука музыкальным центрам и приближаются только к недорогим переносным проигрывателям.

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-1 (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 MP3 (до 11 ч звука).

Кроме дисков CD-ROM диаметром 12 см выпускаются «урезанные» CD-визитки с размерами стандартной визитной карточки 8 × 5,5 см и емкостью до 100 Мбайт. Их размеры: внешний диаметр 5,65 см и внутренний (полезный) диаметр 2,35 см. Укладываются такие CD-визитки в углубление лотка привода CD-ROM диаметром 8 см.

На смену существующим компакт-дискам приходит новый стандарт носителей информации — **DVD** (*Digital Versatil 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. К ним можно обращаться, регулируя положение лазерной головки.

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.

Новый стандарт DVD определен таким образом, что будущие модели устройств считывания будут разрабатываться с учетом возможности воспроизведения всех предыдущих поколений компакт-дисков, т.е. с соблюдением принципа «обратной совместимости». Стандарт DVD позволяет значительно увеличить время и улучшить качество воспроизведения видеофильмов по сравнению с существующими CD-ROM и видеокомпакт-дисками LD. Дисководы DVD представляют собой усовершенствованные дисководы CD-ROM.

Кроме оптических дисков CD-ROM и DVD существуют записываемые и перезаписываемые оптические диски.

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 и фиксируется это изменение отражательной способности. Записываемый CD-R, начиная с обратной (блестящей) стороны, состоит из пяти слоев: прозрачной пластиковой подложки, слоя краски (синей, зеленой или красной — в зависимости от типа применяемого красителя), серебряного или золотого отражающего слоя, защитного слоя и верхнего слоя лака, обладающего высокой механической прочностью. Во время записи луч лазера проходит сквозь прозрачную подложку и выжигает питы (метки) на поверхности слоя краски. При считывании другой луч лазера проходит вдоль дорожки с питами, реагирует на их отражательную способность и преобразует их в цифровые последовательности. На нагревание красочного слоя требуется некоторое время, и поэтому скорость записи не превышает 8^x.

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. Записывающий слой состоит из специального металлопластика, обладающего обратимой отражающей способностью. Этот эффект называется *phase change* (т.е. изменение фазы). Он позволяет с помощью луча лазера записывать новую информацию взамен старой. Питы при записи на перезаписываемый диск CD-RW имеют значительно меньшую глубину, чем при записи на диск CD-R. Поэтому для их чтения требуются более чувствительные дисководы CD-ROM, поддерживающие режим *Multi-Read*. Следует заметить, что почти все выпущенные за последние годы дисководы CD-ROM этот режим поддерживают. 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. Стоимость хранения 1 Мбайт на нем составляет менее 0,4 цента — это в 35 раз дешевле, чем на флоппи-диске. Емкость CD-R равна 650 Мбайт, что равно емкости 451 дискеты. Записывать на CD-R можно со скоростью 600 Кбайт/с (для скорости 4^x) и 1,2 Мбайт/с (для скорости 8^x). Скорость считывания — до 24^x (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, цена которых составляет 0,5—1,5 долл. Для оперативного хранения информации больше подходят перезаписываемые диски CD-RW. Цена их выше, однако они быстро окупаются всего за несколько циклов записи.

Наряду с CD-R и CD-RW — дисками стандартного диаметра 120 мм, выпускаются диски «миньон» диаметром 80 мм. Для них в приемном лотке CD-дисковода персонального компьютера, музыкального центра или CD-проигрывателя предусмотрено специальное углубление диаметром 80 мм (3 дюйма). Максимальное время звучания таких аудиодисков составляет 21 мин, а емкость 185—211 Мбайт. Считать их можно на любом компьютере с приводом CD-ROM. Применяются они в аудиоплеерах и цифровых фотокамерах. Главное их преимущество по сравнению с флэш-памятью — гораздо меньшая стоимость. Диск «миньон» CD-R стоит около 1,5 долл., а CD-RW — около 2 долл.

Для записи выпускаются только дисководы CD-RW. Их можно использовать как для однократной записи на диски CD-R, так и для многократной 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 4^x, а чтения — 20^x.

Формат DVD-RAM с возможностью перезаписи был создан для записи видео- и компьютерной информации. Этот формат допускает работу с четырьмя типами дисков:

- двухсторонними дисками диаметром 12 см (емкостью 9,4 Гбайт);
- односторонними дисками диаметром 12 см (емкостью 4,7 Гбайт);
- двухсторонними дисками диаметром 8 см (емкостью 2,8 Гбайт);
- односторонними дисками диаметром 8 см (емкостью 1,4 Гбайт).

Формат DVD-RAM обеспечивает быстрое преобразование информации и быстрый прямой доступ к ней. Это позволяет одновременно производить запись и воспроизведение информации, что до сих пор было возможно только в системах с жестким диском (винчестером). DVD-RAM можно переписывать 100 000 раз. Для их записи разработаны DVD-RAM — рекордеры. Диски DVD-RAM все шире используются в самых различных устройствах. Например, созданы видеокамеры, в которых они применяются для записи видео- и аудиоинформации вместо магнитной пленки.

В магнитооптических **(MO)** ***дисках*** используют комбинацию магнитных и оптических методов. В них 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. При считывании различают значения записанных данных — 0 и 1, так как плоскость поляризации отраженного лазерного луча отклоняется в различных направлениях в зависимости от того, что записано — 0 или 1. На таком магнитооптическом диске процесс перезаписи информации может быть повторен до 1 миллиона раз. Огромным 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 MO-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 MO-носителях.

Недостаток стандартной MO-технологии — малая скорость перезаписи — из-за цикла стирания перед записью новых данных на диск. Обычно MO-диски требуют процесса с тремя проходами — сначала стирания, а затем записи и проверки.

Все MO-диски стандартизированы. Существуют два типоразмера MO-накопителей: 5,25 и 3,5 дюйма. Магнитооптические диски

5,25 дюйма бывают емкостью 650 Мбайт, 1,3 Гбайт, 2,6 Гбайт, 4,6 Гбайт. Так как диски этого формата двухсторонние, то общая емкость складывается из емкостей двух поверхностей, т.е. 1300 Мбайт = 650 Мбайт + + 650 Мбайт. Магнитооптические диски 3,5 дюйма выпускаются емкостью — 128 Мбайт, 230 Мбайт, 540 Мбайт, 640 Мбайт. Диски этого формата — только односторонние.

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 и поэтому будущее — за ней.

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. MP3-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 еще не выработан.

К твердотельной флэш-памяти относится память *Memory Stick* фирмы «Sony». Она представляет собой универсальный носитель для самых различных приложений. Масса ее — всего 4 г, а габариты — не больше пластины жевательной резинки (21,5 × 50 × 2,8 мм).

Предусмотрена возможность ее подключения к миниатюрным MP3-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.

Емкости памяти носителя *Magic Gate Memory Stick* (64 Мбайт) достаточно для 80 мин музыкальных записей.

В 2003 г. «Sony» выпустила карту *Memory Stick* емкостью 1 Гбайт.

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». Масса карты флэш-памяти равна 2 г, габариты — 24 × 32 × 2,1 мм, емкость памяти 32 и 64 Мбайт, скорость записи — 2 Мбайт/с. Этой емкости памяти достаточно для записи музыкального произведения длительностью 1 ч. В 2001 г. емкость памяти доведена до 256 Мбайт, в 2002 г. — до 512 Мбайт, в 2003 г. — до 1—2 Гбайт, в 2004 г. емкость доведена до 4 Гбайт, а скорость записи — до 20 Мбайт/с. Этой емкости памяти будет достаточно для 16 ч музыкальной записи или 36 мин видеозаписи. SD-память снабжена защитой записей.

В 2003 г. фирма «Sony» выпустила новейшую версию флэш-памяти *Memory Stick Duo Pro*, уменьшенную по размеру по сравнению с *Memory Stick*. Ее габариты составляют всего 20 × 31 × 1,6 мм (без адаптера) и 21,5 × 50 × 2,8 мм (с адаптером), а масса — 2 и 4 г соответственно, объем памяти — до 512 Мбайт, а теоретический объем памяти — 32 Гбайт. 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 20 × 25 × 1,7 мм, масса — 2 г. Носитель нового формата *xD-Picture* должен прийти на смену морально устаревшим картам *SmartMedia*, максимальная емкость которых 128 Мбайт. Выпускаются карты *xD-Picture* емкостью 16, 32, 64, 128, 256 и 512 Мбайт, а в дальнейшем 1 Гбайт. В перспективе предусмотрено увеличение емкости этого носителя до 8 Гбайт. Столь значительный рост емкости миниатюрного носителя стал возможен благодаря использованию многослойной технологии. Основные технические характеристики карт *xD-Picture*: максимальная скорость чтения данных с карт *xD-Picture* составляет 5 Мбайт/с, а скорость записи — 3 Мбайт/с; напряжение питания — 3,3 В; потребляемая при работе мощность — 25 мВт. Карты *xD-Picture* используются, в частности, в новых моделях цифровых фотокамер компании «Olympus».

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 опреде-

ленного типа карт флэш-памяти, а также универсальные картридеры на 3, 4, 5 и даже 8 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.

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 содержит корпус и находящиеся в нем источник питания, материнскую (системную, или основную) плату с процессором и оперативной памятью, платы расширения (видеокарту, звуковую карту), различные накопители (жесткий диск, дисководы, приводы CD-ROM), дополнительные устройства.

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 входные и выходные устройства.

В состав системного блока входят:

- блок питания;
- процессор (микропроцессор), который выполняет поступающие на его вход команды, проводит вычисления и управляет работой остальных 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);

- накопители — дисководы для чтения-записи дискет (флоппи-дисководы);
- накопители на жестких дисках — винчестеры;
- дисководы оптических дисков CD-ROM и CD;
- могут входить дисководы — накопители записываемых CD-R и перезаписываемых CD-RW, DVD, DVD-RW оптических дисков;
- может входить внутренний модем — устройство для ввода и вывода с использованием телефонной сети для связи, например, с сетью Internet.

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.

Создание микропроцессора стало возможным только благодаря миниатюризации в современной электронной технике второй половины XX века. Это миниатюрное вычислительное устройство (или микрочип) состоит из сотен тысяч и миллионов микроскопических электронных схем, нанесенных на поверхность миниатюрного кремниевого кристалла. Его возможности определяются размерами этого кристалла и количеством реализованных в нем транзисторов.

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).

Работой микропроцессора управляют электрические импульсы: наличие импульса соответствует единице, отсутствие импульса — нулю. 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. В нем имеется генератор тактовых импульсов, служащих метками времени («тактами») для синхронизации работы его устройств. *Тактовая частота*, измеряемая в герцах (МГц—ГГц), в основном определяет производительность (или быстродействие) компьютера.

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.

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. Для работы монитора необходима видеокарта (контроллер монитора). Остальные платы можно добавлять: звуковую карту — для ввода и воспроизведения речи и музыки; видеокарту — для вывода видеоизображения; плату внутреннего модема — для соединения через телефонную линию с другими компьютерами и сетью Интернет (используются также внешние модемы в виде отдельных устройств, подключаемые к компьютеру кабелем) и др. В корпус системного блока ПК устанавливаются и устройства внешней памяти — винчестеры, дисководы гибких дисков (дискет), приводы CD-ROM, CD-RW, DVD, DVD-RW и др.

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 «Pentium» составляет 32—512 Мбайт 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 медленно 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 промежуточная 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.

Оперативная память реализуется в виде твердотельных микросхем и поэтому вообще не содержит подвижных деталей.

В компьютере есть еще и ***постоянная память*** (ПЗУ), хранящая информацию даже при отключении питания. В ней содержится наиболее важная информация — 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-Semicondactor*) или CMOS RAM — служит для сохранения некоторых характеристик ПК и среды. Эта микросхема питается от аккумуляторов и поэтому энергонезависима. Это дает возможность постоянно сохранять важные характеристики, используемые при загрузке операционной системы.

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.

Носители служат для постоянного хранения цифровой информации. Это магнитные диски (дискеты, жесткие диски — винчестеры), магнитооптические диски, оптические диски. Они использу-

ются совместно с соответствующими приводами (дисководами). Исключение составляет новейший вид носителей — твердотельная полупроводниковая флэш-память. Она не содержит подвижных деталей и не требует использования приводов.

Накопители — это устройства, способные осуществлять запись, перезапись и считывание цифровой информации. Они представляют собой совокупность носителя и соответствующего привода, служащего для записи и последующего считывания информации. К ним относятся, в частности, дисководы гибких дисков (дискет), жесткие диски (винчестеры), дисководы *Zip*, записываемых оптических дисков CD-R и CD-RW, ленточные накопители. В то же время дисковод CD-ROM к накопителям не принадлежит, так как предназначен только для считывания цифровой информации, а запись ее осуществлять не может.

По сравнению с оперативной памятью носители и накопители имеют значительно большую емкость памяти, однако быстродействие их на несколько порядков меньше.

Магнитные 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. Лишь ленточные накопители имеют последовательный доступ: данные, содержащиеся в произвольном участке ленты, могут быть считаны только после ее перемотки к этому участку. Это существенно увеличивает время обращения к нужному месту записи по сравнению с прямым доступом.

Магнитные диски, в отличие от оперативной памяти, служат для постоянного хранения информации. Физический смысл записи и считывания цифровой информации в виде байтов на магнитный диск аналогичен записи звука на магнитную ленту, и даже проще ее — ведь для записи байтов нужно запоминать только две цифры двоичного кода 0 и 1. Поэтому постепенное размагничивание с течением времени при цифровой записи (в отличие от аналоговой) как на дисках, так и на ленте *не приводит к появлению помех и искажению записанной информации.*

В персональном компьютере используются два типа магнитных дисков: *жесткий диск* (винчестер) и сменные *гибкие диски* (дискеты, Zip, суперфлоппи LS-120 и другие). Винчестер используется для постоянного хранения информации, которая часто используется в работе (программы, текстовые документы, базы данных). Дискеты используются для обмена программами и данными между компьютерами, для хранения запасных копий данных. Жесткий диск значительно превосходит дискеты по скорости доступа и емкости. Его емкость доходит до нескольких десятков гигабайт. В последних мо-

делях она составляет 20—120 Гбайт и более. К тому же в ПК может быть не один винчестер, а несколько.

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-диску. Новые звуковые карты обеспечивают трехмерный (т.е. объемный) звук. Для технологии DVD, в которой звуковое сопровождение фильмов *Dolby Digital*, звуковая карта должна уметь раскодировать DVD-звук с диска и иметь 6 каналов.

Видеосистема ПК 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.

Видеоплата (или *видеокарта*, *видеоадаптер*) служит для хранения видеоизображений, преобразования их из цифровой в аналоговую форму для вывода на экран монитора. Она способна поддерживать текстовый и графический режимы работы.

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 1024 × 768, а рекомендовать можно разрешение 1280 × 1024 при отображении 16,8 миллиона цветов. Для этого ПК должен иметь не менее 2 Мбайт видеопамяти.

В IBM-совместимых компьютерах при использовании программ Windows видеоплаты используются вместе с акселераторами — микросхемами, позволяющими перемещать фрагменты изображений по экрану ПК, рисовать линии и различные фигуры, закрашивать замкнутые контуры, удалять части изображений, отображать шрифты, перемещать по экрану курсор и т.д.

Мониторы используются трех типов: с электронно-лучевой трубкой, с жидкокристаллическим экраном и плазменные.

Монитор с электронно-лучевой трубкой CRT(*Cathode Ray Tube*) состоит из самой CRT-трубки и электронного блока управления лу-

чом. Изображение на цветном экране формируется с помощью точек — пикселей, каждая из комбинации трех цветов — красного, зеленого и синего.

Выпускаются 15, 17—21-дюймовые (по диагонали экрана) мониторы.

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. Сегодня LCD-панели имеют по диагонали 15 дюймов, а для настольных ПК — 17—19 дюймов и более.

LCD-мониторы являются полностью цифровыми приборами. Однако приходится обеспечивать их совместимость с аналоговыми CRT-мониторами. Для этого цифровой сигнал от системного блока компьютера сначала преобразуется в видеокарте в аналоговый сигнал, а затем снова в цифровой — уже в самом LCD-мониторе. Для преодоления этого неестественного положения уже созданы первые цифровые видеокарты.

Несомненным преимуществом LCD-мониторов по сравнению с CRT-мониторами является почти полное отсутствие вредного излучения, которому подвергается человек, работающий перед экраном электронно-лучевой трубки, а недостатком — большая цена, которая, однако, довольно быстро снижается по мере увеличения выпуска LCD-мониторов.

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. Размер плазменных экранов достигает 100 см при толщине всего 8,5—9,0 см.

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 микроскопические 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.

Существует необходимость многократного копирования всевозможных бумаг — президентских указов, правительственных и парламентских постановлений, учрежденческих приказов, научно-технических отчетов и статей, рисунков, рукописей новых статей и книг. Наиболее распространенным способом копирования является ***ксерография*** (ксерографическое копирование) (от греч. *xeros* — сухой и *graphein* — графия, в отличие от «мокрой» фотографии). Это способ оперативного копирования документов в черно-белом или цветном изображении методами электрофотографии, в котором применяется сухое проявление с помощью окрашенных частиц порошка.

В традиционной фотографии изображения предметов запечатлеваются на светочувствительных слоях, в которых под действием света происходят необратимые химические изменения. В ксерографии свет воздействует не на химические, а на электрические свойства светочувствительного слоя. В качестве такого слоя используются электрические свойства фотополупроводников, зависящие от освещения. На свету они являются проводниками, а в темноте — диэлектриками. Фотополупроводниками являются сера, селен, оксид цинка. Ими покрывают металлическую подложку, а затем в темноте электризуют ее и проецируют на нее изображение какого-либо предмета. При этом засвеченные участки слоя становятся проводниками, и электрические заряды с них уходят в металлическую подложку, а незасвеченные участки становятся диэлектриками, и заряды на них сохраняются. Так образуется скрытое электростатическое изображение. Чтобы проявить его, пластину посыпают мелкораздробленным порошком красителя. При этом частицы этого порошка прилипают только к участкам полупроводникового слоя, на котором сохраняются электрические заряды. Так скрытое изображение становится видимым. Аппарат ксерокс позволяет быстро получить любое количество копий с листа текста, рисунка, страницы газеты, журнала или книги.

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. В городах оно составляет около 500 м, а в сельской местности — 2—3 км. 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. *dicto* — 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.

Во всех механических кассетных диктофонах содержится более 100 деталей, часть из которых — подвижные. Записывающая головка и электрические контакты изнашиваются за несколько лет. Откидная крышка также легко ломается. В кассетных диктофонах используется электрический двигатель, который протягивает магнитную пленку мимо головок записи.

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 фотографируемого 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.

Съемочные 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 бóльшая, 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 10-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 до 400 и более раз, 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*. Для воспроизведения в видеомагнитофоне ее помещают в специальный адаптер, имеющий внешние размеры стандартной *видеокассеты* VHS. Выпускаются видеокассеты VHS с временем записи 120, 180, 195 и 240 мин. Запись на эти кассеты (в отличие от звуковых или аудиокассет) — односторонняя.

Современные видеомагнитофоны кроме основной скорости записи (SP) и воспроизведения имеют уменьшенную вдвое скорость — *long play* (LP). Это позволяет удвоить время записи и воспроизведе-

ния стандартной кассеты (правда, с небольшой потерей качества записи). Так, например, время записи наиболее распространенной кассеты на 180 мин при этом увеличивается до 360.

Фирма «Sony» разработала и выпускает миниатюрные видеокассеты стандарта *Video*-8 (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. Однако вставить миниатюрную видеокассету стандарта *Video*-8 в видеомагнитофон нельзя. Предварительно ее нужно переписать на обычную видеокассету стандарта VHS. При перезаписи видеокассет происходит потеря качества — значительно большая, чем у аудиокассет. Ведь на кассеты VHS и Hi8 видеозапись осуществляется по аналоговому методу.

Переход на цифровой метод записи, осуществленный в наиболее современных видеокамерах, 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. Кассета Hi8 значительно дешевле цифровой кассеты DV, однако несколько больше ее по габаритам.

Цифровая запись на кассеты Hi8 осуществлена с помощью видеокамер «Digital 8». Эти камеры можно подсоединять к компьютеру или другому DV-устройству, что дает возможность перезаписывать без потери качества и обеспечивает удобство монтажа записей. Кроме того, с помощью видеокамер «Digital 8» можно перевести ранее сделанные аналоговые записи в цифровую форму и даже воспроизводить смешанную запись — и аналоговую, и цифровую. Более широкая лента Hi8 дает возможность записывать ту же информацию, что и в формате DV, но при этом информация о каждом кадре записывается на вдвое меньшем числе дорожек (6 вместо 12). Однако скорость движения ленты при этом увеличена в полтора раза, поэтому на двухчасовую кассету Hi8 помещается только 1 ч 40 мин цифровой записи.

Выпускаются цифровые видеокамеры без видеокассеты. Изображение в них записывается на жесткий съемный диск (винчестер). Записанный в цифровом формате видеофильм можно просмотреть на персональном компьютере или преобразовать его в аналоговый сигнал и посмотреть по телевизору. Но эту камеру можно использовать и в качестве цифрового фотоаппарата. Тогда этого объема памяти хватает на несколько тысяч цветных фотоснимков или даже на большое число цветных фотоснимков с закадровым звуковым комментарием. Запись ведется со сжатием информации в формате MPEG/JPEG, стандартном для компьютеров, поэтому ее можно просматривать и даже редактировать на мониторе персонального компьютера. Главная особенность этой камеры — возможность комбинировать видеофрагменты и фотографии.

Во многих современных видеокамерах есть фоторежим, дающий возможность записывать стоп-кадры на видеоленту, а в самых новых — на флэш-карту.

До недавнего времени самой компактной кассетой была miniDV. Но ей на смену приходит новый формат MICRO MV Sony. Эта фирма впервые использовала в бытовых видеокамерах более эффективный метод сжатия информации. Благодаря этому размер новой видеокассеты втрое меньше, чем у miniDV.

Особенностью этих миникамер является возможность снимать на карты флэш-памяти Memory Stick, правда, только с ленты на флэш-карту для дальнейшей переброски на компьютер.

При этом на карту Memory Stick емкостью 8 Мбайт входит 5 мин видеозаписи, а на карту емкостью 128 Мбайт — 82 мин видеозаписи.

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 использова-

нием кассет с магнитной пленкой. Время записи на DVD-диске составляет 30 мин, а в «режиме экономии» — 60 мин с некоторым понижением качества видеоизображения. На таком диске емкостью 4,7 Гбайт помещается до 2000 фотографий высокого качества. DVD-технология обеспечивает мгновенный доступ к любому кадру в отличие от пленочных камер, в которых для просмотра нужного кадра магнитную пленку нужно предварительно перемотать. С помощью специальных программ DVD-видеокамеры обеспечивают удобный компьютерный монтаж видеофильмов. Снимать рекомендуется на перезаписываемый диск DVD-RW, а хранить записи — на обычных записываемых дисках DVD-R.

Все перечисленные модели видеокамер содержат сложные механизмы лентопротяжки или привода DVD-дисков.

Наиболее революционной моделью в настоящее время является сверхминиатюрная видеокамера «Panasonic», вообще не содержащая механических подвижных узлов. Запись видео и фотоснимков в ней осуществляется на карту флэш-памяти SD. Форматы записи MPEG2 или MPEG4. В режиме максимального разрешения MPEG2 (705 × 576 точек) картинка сопоставима по качеству с записью на DVD-диск. Камера оснащена жидкокристаллическим дисплеем с диагональю 2,5 дюйма. Карта флэш-памяти SD емкостью 512 Мбайт обеспечивает время видеосъемки, равное 10 мин, с максимальным разрешением. При съемке в формате MPEG4 с заметно пониженным разрешением этой карты хватает на 10 ч записи. Габариты видеокамеры — всего 33 × 90 × 65 мм, а масса — 156 г.

Именно таким 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 и задания

1. Что такое *аппаратное* и *программное обеспечение компьютера*?
2. Каковы основные устройства аппаратного обеспечения компьютера?
3. Что такое *аналого-цифровой* (АЦП) и *цифроаналоговый* (ЦАП) преобразователи?
4. Что такое *архитектура фон Неймана*?
5. В чем различие между носителями и накопителями информации?
6. Назовите основные виды носителей и накопителей информации в компьютере?
7. В чем различие между оперативной и долговременной памятью компьютера?
8. Назовите основные типы оптических компакт-дисков.
9. Что такое *флэш-память*?
10. В чем разница между принтером и плоттером?

Глава 5

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ

5.1. Информационные продукты и услуги

В Федеральном законе «Об информации, информатизации и защите информации» введено понятие информационных ресурсов.

Информационные ресурсы (ИР) — это отдельные документы, массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, 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.

Информационные услуги ≠ Компьютерные услуги (например, библиотека), однако все больше и больше к этому равенству приближаются. 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:
- 1950-е гг. — научные учреждения, государственные учреждения;
- 1960-е гг. — электронные средства обработки и передачи информации; *важнейшая форма представления данных — базы данных*;
- 1970-е гг. — глобальные сети передачи данных; *диалоговый поиск информации в удаленной БД*;
- 1980-е гг. — *Всемирная сеть передачи данных* (Internet), WWW, космическая и сотовая связь.

Структура рынка информационных продуктов и информационных услуг

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, каж-

дый из которых объединяет группы, предлагающие однородные информационные продукты и услуги.

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

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

Другой пример инфраструктуры приведен на рис. 5.1, он также включает пять секторов:

Рис. 5.1. **Секторы рынка информационных продуктов и информационных услуг**

1. *Деловая информация:*
- биржевая информация;
- статистическая информация;
- коммерческая информация.

2. *Потребительская информация:*
- новости и литература;
- расписание, заказы;
- развлекательная: игры и т.д.

3. *Информация специалистов:*
- профессиональная информация;

- научно-техническая информация;
- доступ к первоисточникам.

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

5.2. Классификация пакетов прикладных программ

Пакеты прикладных программ (ППП) являются наиболее динамично развивающейся частью рынка ИП и ИУ программного обеспечения. 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. 5.2.

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. Примерами ТП для ПК являются MS Word, Лексикон, Chiwriter и т.д. Работа с текстовыми данными будет рассмотрена отдельно.

Настольные издательские системы (НИС) — программы профессиональной издательской деятельности, позволяющие осуществ-

лять 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.

Рис. 5.2. **Классификация ППП**

Лучшими программами НИС для ПК являются Corel Ventura, PageMaker, QuarkXPress. Последние два пакета созданы в стандарте Windows.

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

➢ *ППП растровой графики* предназначены для работы с фотографическими изображениями. Они включают средства по кодированию изображений в цифровую форму, обработке и редактированию 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, 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;

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 погрешностью 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* являются электронным помощником 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. Разработано множество СУБД 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 рассмотрено отдельно.

Пакеты демонстрационной графики — конструкторы графических образов деловой информации, т.е. средства создания подобия

видеошоу, 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 видеоинформации. Их использование требует *дополнительного аппаратного обеспечения* — аудио- и видеоплат, колонок, CD-ROM и т.д.

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

Мультимедиапрограммы можно разделить на две большие группы.

Первая группа — включает пакеты для образования и досуга. Они поставляются в основном на CD-ROM объемом 500—700 Мбайт.

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 в себя 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, Tiger^{tm}, 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 Турбо бухгалтер, 1С:Бухгалтерия.

Аналитические ППП — программы статистических расчетов. 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 ППП

Наиболее мощная и динамично развивающаяся часть программного обеспечения. В рамках этого ПО можно выделить две наиболее значимые группы:

1) полносвязанные пакеты;

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. Представителями 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 присутствует 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 осо-*

бенностью является использование общих ресурсов. Выделяется 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 существует два стандарта:

➢ Object Linking and Embedding OLE 2.0 динамической компоновки и встраивания объектов фирмы «Microsoft».

➢ OpenDoc (открытый документ) фирм «Apple», «Borland», «IBM», «Novell».

OLE 2.0 позволяет:

- 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;
- переносить объекты из окна одной прикладной программы в окно другой;
- предусматривает возможность общего использования функциональных ресурсов программ: например, модуль построения графиков ЭТ может быть использован в текстовом редакторе.

Основной недостаток OLE 2.0 — 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 ОС OS/2.

Предполагается совместимость OLE и OpenDoc.

5.3. Виды и 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. Внутримашинная 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 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.

Каждый этап состоит из выполнения операций. Последовательность подготовки текстового документа показана на рис. 5.3.

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 МД.

Рис. 5.3. **Этапы подготовки текстовых документов**

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 до 127 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 8 × 8 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; после знака препинания следует 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 заключительной стадией.

5.4. Текстовые 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 семизначный двоичный код — всего:

$$2^7 = 128 \text{ символов.}$$

Этого мало, поэтому применяют расширенный стандарт ASCII:

$$2^8 = 256 \text{ символов} = 128 \text{ ASCII} + 128.$$

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 (практически совпадают с возможностями печатной машинки):

- набор текста с контролем на экране;
- создание жесткой копии (распечатка);
- использование ASCII.

Дополнительные возможности, 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:

A. ***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);
  - 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, физических).***

O. ***Использование в тексте информации 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.

B. *Издательское качество.* Реализация принципа WYSIWYG — What You See Is What You Get:

- Microsoft Word;
- Ventura Publishers;
- Aldus Page Maker.

Для работы с такими редакторами требуется ПК не ниже AT 486 DX с 8 Мбайт оперативной памяти.

C. 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 широкое распространение получил редактор текстов «Лексикон» для MS DOS.

В общем случае для оценки удобства работы с ТП могут служить следующие п а р а м е т р ы:

- 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.

5.5. Технология работы с текстовыми документами в процессоре Microsoft Word для Windows

В настоящее время получили распространение несколько десятков текстовых процессоров. Примерами являются Word Perfect, MultiEdit, Lotus Word Pro, Ultra Edit, Wordstar, Word, XY Write, Ami Pro и др.

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 Мбайт. Одна только справочная система с примерами занимает, в зависимости от версии пакета, от 5 до 25 Мбайт памяти на жестком диске ПК.

В настоящее время наиболее широко используется версия процессора Word 97, входящая в состав пакета Microsoft Office 97, с расширенными возможностями редактирования текста, в том числе в формате HTML.

Начало работы с Word

Запуск текстового процессора. Прежде чем пользователь сможет работать с Word, необходимо вызвать его для работы одним из возможных способов, используя: или кнопку «Пуск» панели задач, или пиктокнопку  на панели Microsoft Office, или предварительно созданный ярлык на рабочем столе.

При запуске Word автоматически выводит на экран окно нового документа с именем Документ 1. Каждый документ имеет свое собственное окно, и, чтобы работать с несколькими документами, нужно открыть их или вызвать из памяти. Одновременно можно работать не более чем с девятью документами.

Осваивать работу с редактором лучше всего, выполняя практические задания на компьютере. Далее по тексту такие задания будут отмечаться значком ☑.

☑ **Задание.**

Запустите Word.

Элементы экрана Word. Верхняя строка экрана называется **Строкой заголовка**, которая содержит название программы Microsoft Word и имя файла документа (первоначально Документ 1).

Следующей строкой является **Главное меню** (активизируется нажатием клавиши ALT), в которой перечислены группы команд: **Файл**, **Правка**, **Вид**, **Вставка**, **Формат**, **Сервис**, **Таблица**, **Окно**, **Справка**. Каждая группа объединяет команды одной функциональной направленности.

Ниже **Главного меню** по умолчанию находятся ***панели инструментов*,** включающие две группы ***пиктокнопок*** со значками: **Стандартная** и **Форматирование** (рис. 5.4). Это кнопки команд, которые можно найти и в меню, однако с помощью пиктокнопок и мыши работа значительно ускоряется. Если указатель мыши подвести к какой-нибудь пиктокнопке, Word выдаст ее краткое описание в небольшом желтом окошке.

Под панелями инструментов расположена управляющая **Линейка**, с помощью которой легко контролировать размеры полей и абзацных отступов на странице документа.

Внизу, под окном документа, расположена **Статусная строка**, которая выдает ряд сведений, полезных при редактировании документа. Из нее можно узнать номер текущей страницы, число страниц в тексте документа, расположение курсора и задействованные режимы клавиатуры.

По умолчанию Word размещает на экране две ***полосы прокрутки*** текста: *вертикальную* — у правого края экрана и *горизонтальную* — у

нижнего края. *Движок* или *лифт*, установленные на каждой из полос, позволяет перемещаться по тексту с помощью мыши. В левой части горизонтальной полосы находятся три пиктокнопки ***режимов просмотра документа***: *обычного* режима, режима *разметки страницы* и режима *структуры документа*. Ввод текста, как правило, осуществляется в обычном режиме просмотра.

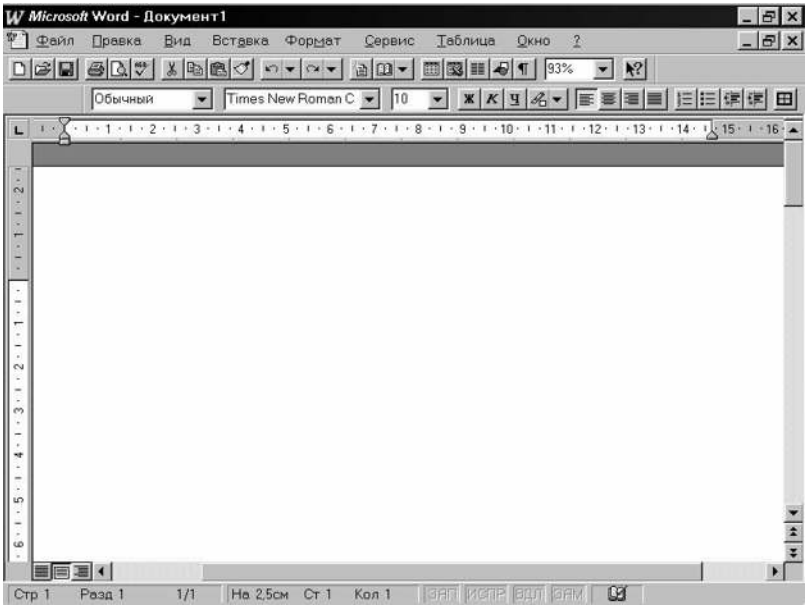


Рис. 5.4. **Экран редактора Word**

Рабочая область находится в центре экрана. На ней располагаются все элементы создаваемого документа, а также курсор клавиатуры и маркер конца текста.

☑ **Задание.**
Найдите все рассмотренные выше элементы экрана.

Меню и окна. Окна и меню Word имеют стандартный вид для программ, работающих под управлением Windows. Команды можно выполнять с помощью соответствующих пунктов главного меню, контекстных меню, вызываемых нажатием правой кнопки мыши, пиктокнопок на панелях инструментов окон документов, а также диалоговых окон.

Каждая группа команд главного меню представляет собой набор команд, объединенных в ниспадающее меню. Если некоторые из

команд отображаются не в черном, а в сером свете, это означает, что они в данный момент недоступны по причине невыполнения необходимых предварительных условий. Например, нельзя вырезать фрагмент, если он не выделен.

Слова «выполнить команду» в самом общем смысле означают активизацию соответствующего пункта главного меню. Наиболее употребительные команды выполняются с использованием пиктокнопок на панелях инструментов или с помощью команд контекстных меню, вызываемых нажатием правой кнопки мыши.

У ряда команд меню после названия стоит многоточие. Это означает, что для выполнения команды необходимо ввести дополнительную информацию. При активизации такой команды на экране открывается *диалоговое окно* (ДО) с соответствующим названием. Внутри ДО находятся различные элементы: ***кнопки*** (например, нажатие на кнопку **OK** приводит к выполнению команды, а нажатие на кнопку **Отмена** — к отказу от выполнения команды), ***флажки*** (квадратные окошки, устанавливающие определенный режим; он считается включенным, если в окошке находится крестик); ***переключатели*** (круглые кнопки для выбора одной опции из нескольких); выпадающие ***списки*** (перечень вариантов, из которых нужно выбрать один), ***строки ввода*** (для ввода текстовой или числовой информации). После заполнения ДО и нажатия на кнопку **OK** происходит выполнение команды.

Переключение между окнами различных документов осуществляется с помощью пункта главного меню **Окно**. Для удобства просмотра и редактирования документа окно можно разделить на две части горизонтальной полосой, воспользовавшись командой **Разделить** меню **Окно**.

☑ **Задание.**

Выведите на экран панель инструментов **Обрамление**. Для этого:

- выполните команду **Вид/Панели инструментов**;
- установите флажок для панели **Обрамление**.

☑ **Задание.**

Уберите панель инструментов **Обрамление** с экрана.

Использование справки. При работе с Word всегда можно получить подсказку по интересующему вопросу от встроенной справочной подсистемы программы, оказывающей всестороннюю помощь во время сеанса работы. Можно получить на экране любые справки о выполняемом в данный момент действии. Для работы со справочной подсистемой используется пункт главного меню со знаком вопроса **?**.

Наиболее сложные темы рассматриваются в справке на основе примеров, снабженных иллюстрациями. Окно справки имеет также

команду **Поиск**, которая позволяет на основе введенного критерия найти нужный раздел.

☑ **Задание.**

С помощью справочной подсистемы найдите информацию о непечатаемых элементах таблицы. Для этого:

- выполните команду **?/Вывод справки**;
- в открывшемся диалоговом окне выберите вкладку **Поиск**;
- наберите слово «непечатаемые» в окне поиска;
- в открывшемся списке выберите раздел Непечатаемые элементы таблицы и нажмите на кнопку **Вывести**;
- закройте окно справки.

Этап создания нового документа

Окно документа при запуске текстового процессора настроено на *стандартный* **шаблон** ввода документа (как правило, шаблон *Normal — Нормальный*). В шаблоны документов входят специальные **стили** оформления, определяющие внешний вид символов и абзацев посредством инструкций форматирования.

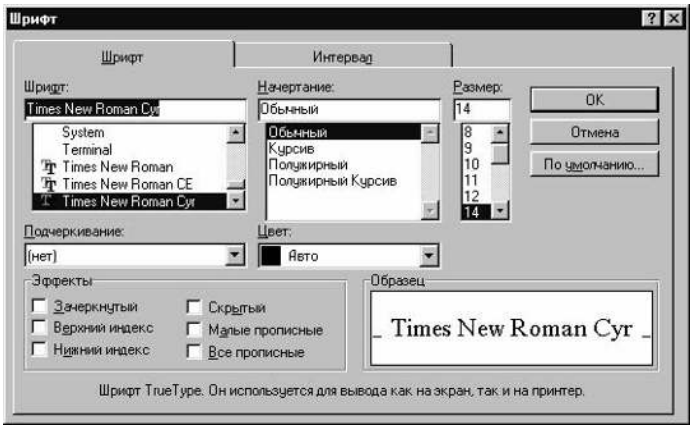


Рис. 5.5. **Диалоговое окно Шрифт**

Перед вводом текста следует установить параметры шрифта, которым должен отображаться текст. Для этого необходимо выполнить следующие действия:

- открыть меню **Формат**;
- выбрать команду **Шрифт**. Появится диалоговое окно **Шрифт**;
- выбрать вкладку **Шрифт** в верхней части диалогового окна;
- выбрать тип шрифта в окне списка **Шрифт**;

- выбрать стиль шрифта в окне списка **Начертание** (например: обычный; *курсив*; **полужирный;** ***полужирный курсив***);
- выбрать нужный размер шрифта в окне списка **Размер**;
- выбрать вид подчеркивания в раскрывающемся списке:

Подчеркивание, например:

обычное, только слова, двойное, пунктир.

- нажать на кнопку **По умолчанию.**

☑ **Задание.**

Установите по умолчанию шрифт Times New Roman Cyr с размером 14, обычным начертанием, без подчеркивания.

Информационная технология создания текстового документа состоит из ряда последовательных этапов и операций. Начальные этапы — набор текста, редактирование текста — выполняются, как правило, в *обычном режиме* (подробнее о режимах работы см. далее). Операции *форматирования* текста выполняются в режиме *разметки страницы.*

Для создания нового документа нужно:

- Открыть меню **Файл.**
- Выбрать команду **Создать.**
- Выбрать в списке **С шаблоном** имя шаблона для документа. В поле **Описание** появится характеристика выбранного шаблона. *По умолчанию* выбирается шаблон **Normal.**
- Нажать на кнопку **OK**. На экране появится пустое окно документа.

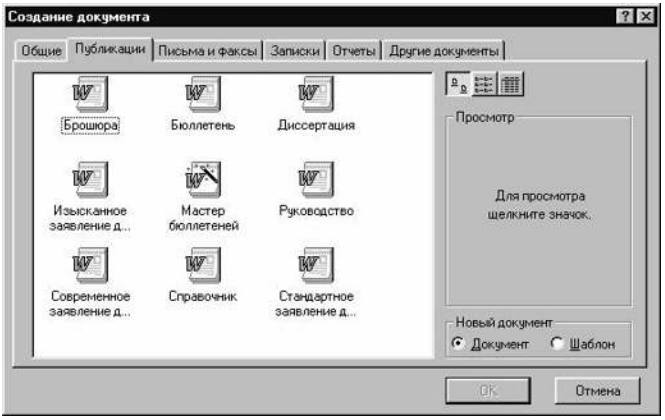


Рис. 5.6. **Диалоговое окно Создать**

☑ **Задание.**

Самостоятельно создайте новый документ с шаблоном Normal. Введите следующий текст:

Использование компьютерных технологий в деятельности милиции

Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы, проводимой органами внутренних дел. В свою очередь, результаты этой работы зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации. Именно эти функции и призвана обеспечить система информационного обеспечения органов внутренних дел, которая в настоящее время поддерживает обработку и хранение значительных объемов информации.

В течение значительного периода времени компьютеризация ОВД сводилась к поставке персональных компьютеров и созданию на их базе простейших автономных систем — дорогостоящих автоматизированных «пишущих машинок» и «записных книжек». Практика показала, что с помощью одних только персональных компьютеров невозможно решить проблемы информатизации, необходимы прежде всего крупные хранилища колоссальных картотек — интегрированные банки данных. В них вся информация, по всем категориям учета систематизируется, хранится и поддерживается в актуальном состоянии в одном месте, с обеспечением межрегионального обмена, а также прямого доступа к ней практических работников с мест в пределах своей компетенции. Эти функции обеспечивают мощные базовые ЭВМ и специализированные сетевые компьютерные средства. Крупнейшим банком криминальной информации является ФБКИ.

В целом в органах внутренних дел России в автоматизированном режиме с помощью компьютерной техники обслуживаются задачи оперативно-розыскного и справочного назначения с количеством обрабатываемых запросов примерно 10 млн в год, а также задачи учетно-статистического, управленческого и производственно-экономического назначения. Всего в машинном контуре ежегодно обрабатывается свыше 150 млн документов.

Планируется объединение на логическом уровне региональных банков данных нескольких МВД, УВД близлежащих областей, находящихся в зоне экономического района. Такие зональные центры призваны обеспечивать требуемый уровень интеграции информационных ресурсов и способствовать реальному формированию единого информационного пространства подразделений ОВД.

Этап редактирования и форматирования документов

Работа с абзацами текста. Под **абзацем** в Word понимается часть документа, за которой следует ***маркер абзаца*** ¶, образующийся на-

жатием клавиши **Enter**. Абзац является элементом текста, который Word рассматривает как ***объект***. Такими объектами являются не только абзацы, но и рисунки, таблицы, звуки.

Поскольку в Word используются ***масштабируемые шрифты***, при изменении их размеров текстовый процессор сразу же изменяет число строк абзаца, поэтому число строк и их длина при определении абзаца не используются.

Стили абзаца определяют внешний вид абзаца: тип и размер шрифта, величину межстрочного интервала, выравнивание текста, отступ первой строки абзаца, расстояние между абзацами, контроль положения абзаца на странице — запрет висячих строк, запрет нумерации строк и т.п. Все параметры, определяющие стиль абзаца, задаются в диалоговом окне **Абзац**, вызываемом командой главного меню **Формат/Абзац**. Стили хранятся под определенным именем в виде ***таблицы стилей*** в специальном файле.

☑ **Задание.**

В набранном тексте:

- установите выравнивание первого абзаца по ширине, второго — по правому краю, третьего — по левому краю, четвертого — по центру;
- для первого абзаца установите отступ: слева — 2 см, справа — 0,5 см;
- измените межстрочный интервал во втором абзаце на полуторный.

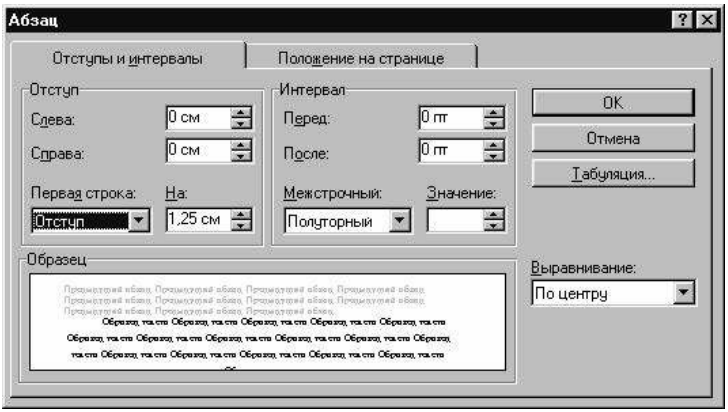


Рис. 5.7. **Диалоговое окно Абзац**

Использование стилей. Если пользователя не устраивают некоторые стили абзаца, он может их изменить и создать на основе стандартного новый стиль оформления, добавив его в таблицу стилей.

Удобство использования стилей состоит в том, что созданный документ можно переформатировать, задав ему соответствующий

стиль. Например, чтобы изменить шрифт и расположение у заголовков разделов документа, не требуется искать в тексте эти заголовки и вручную менять их форматирование. Достаточно исправить стиль абзаца этих заголовков, после чего они автоматически примут нужное оформление.

При записи документа на диск сохраняется и таблица стилей, используемых в нем.

Для того чтобы применить соответствующий стиль для форматирования текста, нужно:

- выделить текст, к которому нужно применить стиль;
- открыть меню **Формат**;
- выбрать команду **Стиль**. Появится диалоговое окно **Стиль**;
- выбрать в списке **Список** нужный тип стиля:
  - *Используемых стилей* — отображаются стили, которые задействованы в активном документе;
  - *Всех стилей* — отображаются все стили, доступные для документа;
  - *Специальных стилей* — отображаются только стили, созданные пользователем.
- выбрать в списке Стили имя того стиля, который необходимо применить.
- нажать кнопку команды Применить.

Рис. 5.8. **Диалоговое окно Стиль**

☑ Задание.

Для всех абзацев набранного текста:

- установите выравнивание текста абзацев «По ширине»;
- установите стиль заголовка к тексту «Заголовок 1».

Помимо ***стилевого*** форматирования в текстовом процессоре Word можно использовать ***непосредственное*** форматирование, меняющее вид отдельных символов, слов, предложений. При этом два типа форматирования не влияют друг на друга.

Дополнительные возможности форматирования и редактирования текста. Некоторые параметры форматирования абзацев текста, которые не учитывает шаблон документа **Нормальный**, нужно вносить вручную перед вводом текста. К ним относятся, например, создание красной строки, выравнивание текста по ширине строки, автоматический перенос слов по слогам и т.п. Все требуемые параметры можно задать командами **Формат/Абзац**, **Сервис/Параметры** и **Сервис/Расстановка переносов**. Все сделанные установки сохраняются в дальнейшем при записи файла документа.

Следует отметить, что одновременная запись в файл текста документа и таблицы стилей приводит к значительному увеличению размера файла документа по сравнению с файлами документов, выполненных в простых редакторах текстов.

Текстовый процессор Word может также автоматически отформатировать документ с использованием команды главного меню **Формат/Автоформат**. Текстовый процессор анализирует содержимое документа, а затем автоматически форматирует текст, назначая соответствующие стили. После форматирования пользователю в диалоговом окне ***Автоформат*** предлагается просмотреть изменения и либо принять их, либо отменить, либо использовать другие стили из имеющихся шаблонов.

Следовательно, при работе с документом можно сначала ввести текст, а затем применить к нему команду **Автоформат**, которая изменит внешний вид текста в соответствии с заданным стандартом. Таким образом, время, затрачиваемое на форматирование, можно существенно сэкономить.

Во время установки режима автоматического переноса слов можно указать, в каком месте желательно выполнить разрыв конкретного слова, если во время редактирования оно окажется в конце строки. Для вставки символа ***мягкого переноса*** требуется установить курсор в нужной позиции и нажать комбинацию клавиш **CTRL+дефис**. Для указания того, что в определенном месте слово разрывать нельзя (например, в месте дефиса двойной фамилии), существует комбинация клавиш **SHIFT+CTRL+дефис**.

Можно также в диалоговом окне команды **Сервис/Расстановка переносов** указать максимальное количество расположенных рядом строк текста, заканчивающихся символом переноса. Это делается с целью улучшить внешний вид документа. В этом же диалоговом окне можно перейти с автоматического на ручной режим переноса

слов. В этом режиме Word при каждой попытке разбиения слова выводит на экран диалоговое окно, в котором предлагаемое разбиение помечено маркером. Пользователь при желании может перенести маркер на нужное место и нажать на кнопку **ОК**.

Для проверки правописания и осуществления переноса слов, написанных на разных языках, используется команда главного меню **Сервис/Язык**. При этом к текстовому процессору подключается встроенный словарь соответствующего языка.

Если при вводе текста включен режим **Автозамена**, то происходит автоматический контроль и исправление ошибок в процессе набора слов текста. Чтобы пополнить список слов режима **Автозамена**, в которых часто допускаются опечатки или типичные ошибки, нужно командой **Сервис/Автозамена** вызвать диалоговое окно **Автозамена** и в нем в поле **Заменить** ввести слово с опечаткой, а в поле **На** его правильный вариант.

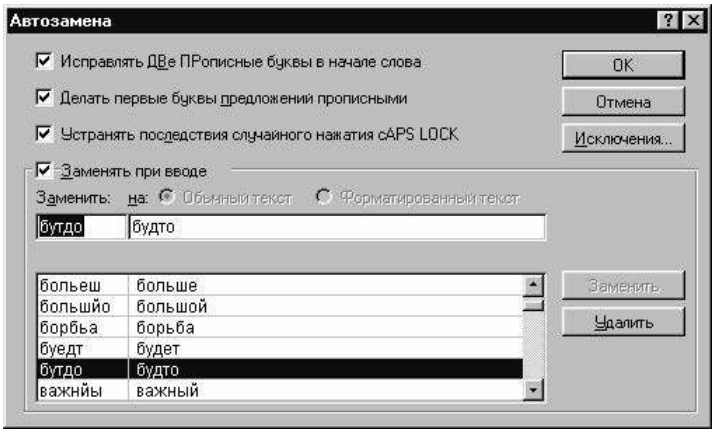


Рис. 5.9. **Диалоговое окно Автозамена**

Автозаменой можно воспользоваться и для быстрой вставки в текст часто повторяющегося оборота, текста, рисунка или графика. Например, пользователь хочет при наборе двух символов «юи» ввести название «Казанский юридический институт МВД РФ». Для этого в поле **Заменить** нужно вставить заменяемые символы, а соответствующее выражение для замены поместить в поле **На**.

Аналогичными возможностями обладает команда **Правка/Автотекст**. Для выделенного текста или иллюстрации в диалоговом окне **Автотекст** нужно ввести условное сокращение в поле **Имя** (длиной не более 31 символа), а в списке **Сделать элементы Автотекста доступными для** указать **Всех документов** (Обычный.dot). Если

теперь требуется вставить выделенный текст или оборот в нужное место, достаточно набрать имя, например, «юи», а затем нажать на кнопку **F3** — текст будет вставлен.

При вводе текста часто требуется заменить повторяющиеся слова в одном предложении или абзаце их **синонимами** или словами, близкими по смыслу. Для этого нужно *выделить слово* и вызвать диалоговое окно команды **Сервис/Тезаурус**. В списке **Значения** приведены варианты синонимов заменяемого слова. Пользователь выбирает нужное слово, активизирует его и нажимает на кнопку **Заменить**. Дополнительные синонимы можно попробовать получить, если в диалоговом окне нажать кнопку **Поиск**.

Вставка номеров страниц и колонтитулов. В процессоре Word наряду с автоматическим выравниванием строк существует и *автоматическая верстка страниц*. Если текст не будет умещаться на одной странице, то он автоматически переместится на следующую. На экране между страницами будет видна штриховая разделительная линия (для этого должен быть установлен флажок **Фоновая разбивка на страницы** на вкладке **Общие** диалогового окна команды **Сервис/Параметры**). *Жесткий разделитель страниц* с надписью **Разрыв страницы** задается или вручную (при одновременном нажатии клавиш **CTRL+ENTER**), или через диалоговое окно команды **Вставка/Разрыв** главного меню установкой переключателя **Начать новую страницу**.

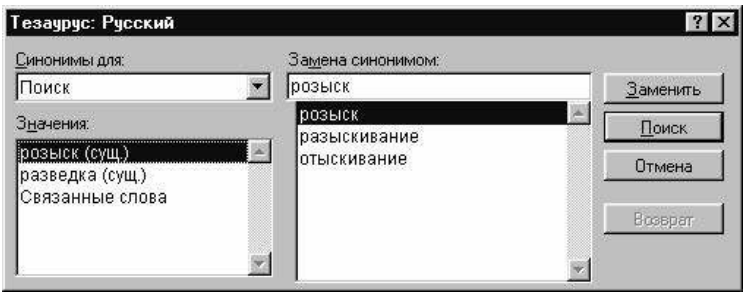


Рис. 5.10. **Диалоговое окно Тезаурус**

Если в процессе редактирования вставляется большой фрагмент текста, рисунок, таблица и т.п. в уже набранную страницу, то после вставки происходит автоматическое перераспределение текста между страницами.

Для того чтобы *пронумеровать страницы*, нужно использовать команду **Вставка/Номера страниц** главного меню. В диалоговом окне следует ввести информацию о местоположении номера на странице, решить, присоединять ли к нему номер главы и др. После

выполнения команды Word создает маленький *кадр* в указанном месте *колонтитула* (см. ниже) и вставляет в него номер страницы. При работе с номером страницы Word предоставляет все возможности, доступные при работе с кадрами, например возможность увеличить кадр, обрамить его рамкой, создать фон и т.п.

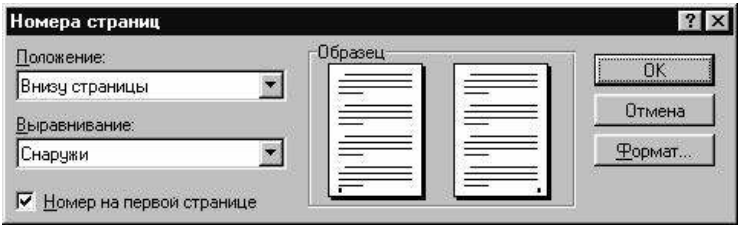


Рис. 5.11. **Диалоговое окно Номера страниц**

Если кроме номера на каждую страницу текста необходимо поместить другие сведения (например, название главы), то их вводят в верхний или нижний колонтитул, создание которых выполняется командой **Вид/Колонтитулы**. Текстовый процессор переходит в режим просмотра разметки страницы и выводит на экран панель инструментов **Колонтитулы**.

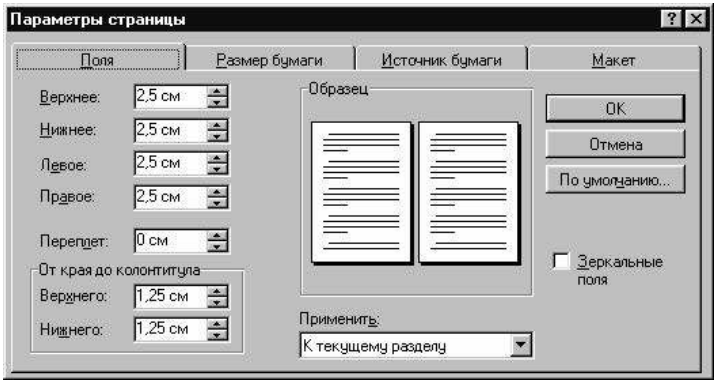


Рис. 5.12. **Диалоговое окно Параметры страницы**

Информация, введенная в колонтитуле всего одной страницы, появляется в колонтитулах всех страниц. Помимо номера страницы, в колонтитул (верхний, нижний, для четных, нечетных страниц) по желанию пользователя вставляются, например, названия глав, фамилия автора, дата создания документа, графические иллюстрации,

фирменный знак, обрамление или горизонтальная линия, отделяющая содержание колонтитула от текста документа. Расположение колонтитулов на странице (от верхнего и нижнего краев страницы) задается в диалоговом окне команды **Файл/Параметры страницы**.

☑ **Задание.**

- Пронумеруйте страницы (от центра, вверху).
- В нижнем колонтитуле введите текст:

> Компьютерные технологии в правоохранительных органах.

Выделение фрагментов и работа с ними. Как и при работе в любом текстовом процессоре, в Word важнейшей операцией является *выделение объекта* и его элементов. Можно выделить символ, слово, предложение, строки абзаца, рисунок, колонки текста, таблицу, весь документ и т.п.

Копировать, вырезать, перемещать, удалять выделенный фрагмент можно как с помощью манипулятора «мышь», так и с помощью **Главного меню** и комбинации «горячих» клавиш. Текстовый процессор имеет ***копилку***. В нее можно вырезать несколько отдельных фрагментов из текста. Для этого нужно выделить фрагмент, нажать **CTRL+F3**, затем выделить другой фрагмент, нажать **CTRL+F3** и т.д. Все они будут расположены в копилке в порядке очередности. Заканчивается операция тем, что курсор устанавливается на место, в которое нужно вставить фрагменты, и одновременно нажимается комбинация клавиш **CTRL+SHIFT+F3**. Копилка при этом освобождается. Если нужно вставить фрагменты, не освобождая копилку, то в диалоговом окне **Автотекст** надо выбрать слово **Копилка** и нажать кнопку **Вставить** — при этом Word вставит в нужное место содержимое копилки.

Помимо копилки, для работы с фрагментами в Word используется также ***буфер обмена*** (Clipboard), общий для всех документов и приложений Windows. Фрагменты текста можно копировать, вырезать в буфер обмена, а затем вставлять в другое место документа, другой документ, сделав его активным, например в редактор Write. Однако следует помнить, что емкость буфера ограничена. Он может вмещать не более 10 страниц текста или одно полноэкранное цветное изображение.

Работа со сносками и списками. При вводе текста иногда необходимо сделать сноску, указывающую на что-либо, например на название приказа. Сноски в текстовом процессоре Word могут быть размещены в различных местах: в конце страницы, в конце раздела или в конце текста документа.

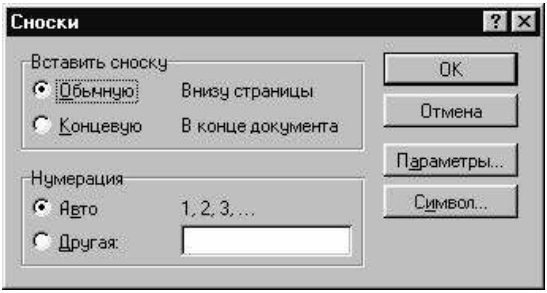


Рис. 5.13. **Диалоговое окно Сноски**

Вставка сноски происходит следующим образом. Если, работая в обычном режиме просмотра, пользователь закончил абзац и решил сделать сноску, то, введя команду **Вставка/Сноска,** он попадает в диалоговое окно **Сноски**. В этом окне нужно активизировать некоторые переключатели, например, **Обычную** и **Авто**, а затем нажать на кнопку **OK**. Word вставляет в конец последнего абзаца текста страницы номер сноски и открывает панель сноски, в которую можно вводить текст сноски. Для возврата в основной текст документа нужно нажать на кнопку **Закрыть**. Содержание сносок видно в режиме просмотра разметки страницы.

Word следит за нумерацией сносок, и если удалена какая-то из сносок, то будет выполнена их автоматическая перенумерация. Чтобы удалить сноску, надо выделить ее номер в тексте документа и нажать клавишу **DEL**. Чтобы перенести номер сноски в другое место, нужно выделить его и перетащить мышью в требуемую позицию.

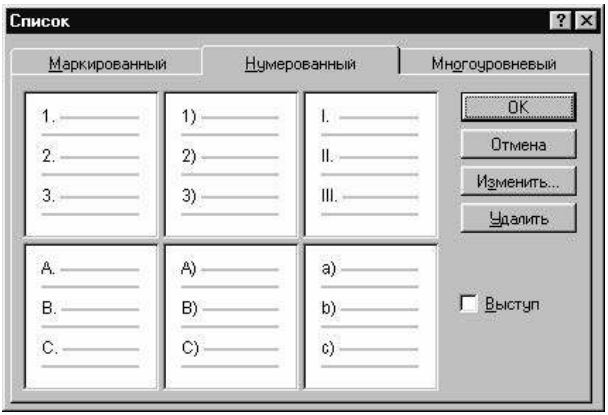


Рис. 5.14. **Диалоговое окно Список**

Часто в тексте встречаются *перечисления*, например перечисление функций работника того или иного подразделения, пунктов правил и инструкций. Их можно отметить в тексте какими-либо символами, перенумеровать или сделать иерархические отступы. Для этого необходимо выделить абзацы, которые надо свести в список, и выполнить команду **Формат/Список**. В диалоговом окне предстоит выбрать нужные позиции и нажать на кнопку **ОК**.

Если предлагаемые по умолчанию ***маркеры*** *списка* не подходят, их можно изменить, активизировав кнопкой **Изменить** диалоговое окно **Изменение нумерованного списка**: установить размер и цвет, задать вид выравнивания абзацев в списке, отступы, тип шрифта и т.д.

☑ **Задание.**

Поменяйте местами третий и четвертый абзацы.

В продолжение набранного выше текста введите следующий текст, содержащий список.

В ФБКИ подлежат учету:

1) особо опасные преступники;

2) особо опасные нераскрытые и раскрытые преступления с характерным способом совершения;

3) особо ценные предметы антиквариата, культуры и государственного значения.

Централизованные розыскные учеты на федеральном уровне ведутся совместно с централизованными криминалистическими учетами. В дальнейшем они будут информационно объединены в автоматизированном контуре на основе ФБКИ в интегрированную базу данных.

В ГИЦ подлежат централизованному розыскному учету:

- пропавшие без вести лица, неопознанные трупы, неизвестные больные и дети;
- лица, объявленные в розыск;
- похищенное нарезное огнестрельное оружие;
- похищенный и угнанный автотранспорт;
- похищенные предметы антиквариата и культурные ценности;
- похищенные документы общегосударственного обращения и номерные вещи;
- лица, представляющие оперативный интерес, по признакам внешности на базе видеозаписей (видеобанки и видеотеки лиц).

☑ **Задание.**

В текст вставьте сноску:

ФБКИ — Федеральный банк криминальной информации.

Оформление текста. В процессе ввода текста или после того как он набран, следует предусмотреть, в каких местах будут распола-

гаться рисунки, текстовые эффекты, формулы и др. Именно там нужно вставить пустые ***кадры.*** Без кадра иллюстрация при вставке в текст будет его разрывать, и текст может заканчиваться, например, над рисунком и продолжаться после него.

Для того чтобы текст «обтекал» иллюстрацию со всех сторон, ее необходимо поместить в кадр. Прямоугольная область для кадра создается командой **Вставка/Кадр**. В режиме просмотра разметки страницы на экране появляется крестик, который можно установить в нужном месте и растянуть с помощью мыши в прямоугольник кадра любого размера. Помимо иллюстраций в кадр можно вставлять и броский текст.

Чтобы привлечь внимание к тому или иному абзацу или отделить линией один фрагмент от другого, используются такие *графические элементы***,** как *линии обрамления* и *фон*. Активизировав команду **Формат/Обрамление и Заливка**, можно в диалоговом окне задать режимы работы с выделенным абзацем: вставить его в рамку желаемой толщины, заполнить ее фоном различного цвета и любой интенсивности. Чтобы отделить один раздел текста от другого, можно в соответствующем поле выбрать двойную, пунктирную или одинарную линию определенной толщины и цвета.

Характерной чертой Word является возможность автоматического разбиения текста на *колонки*. Если пользователь желает разбить какую-то часть документа на колонки, он отделяет этот текст *разрывами раздела* командой **Вставка/Разрыв** и в диалоговом окне устанавливает переключатель **На текущей странице**. После этого он вызывает диалоговое окно команды **Формат/Колонки,** в котором заполняются параметры: число колонок, их тип, ширина, интервал и т.д. Заполнение заканчивается нажатием на кнопку **ОК**.

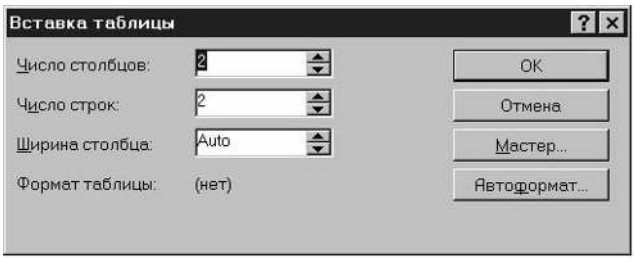


Рис. 5.15. **Диалоговое окно Вставка таблицы**

Используя диалоговое окно, можно создавать колонки одинаковой и разной ширины, добавлять вертикальную линию между ними, делать колонки разной длины, выравнивать их длину, вставлять

графические иллюстрации. До недавнего времени эти операции были возможны только в *настольных издательских системах.*

Создание и редактирование таблиц. Построение **таблиц** осуществляется автоматически командой **Таблица/Вставить** таблицу. В диалоговом окне нужно указать число столбцов и строк; после нажатия на кнопку **OK** таблица появится в месте расположения курсора.

Границы ячеек таблицы выделены пунктирной сеткой. В ячейки таблицы можно вводить не только числа, но и текстовые фрагменты, графические объекты. Высота ячейки автоматически изменяется, если размер вводимого объекта превышает ее размеры. Существуют клавиши перемещения внутри таблицы при вводе ее содержимого (**TAB, ALT+TAB**).

Когда таблица заполнена, ее можно отформатировать командой **Таблица/Автоформат** главного меню. В диалоговом окне команды предлагается большое количество шаблонов оформления таблицы, и пользователь может выбрать любой из них. Однако можно оформить внешний вид таблицы и вручную, выделив ее и применив команду **Формат/Обрамление и Заполнение**.

Таблицу можно *редактировать*: добавлять или удалять строки и столбцы; менять ширину столбцов и высоту строк; объединять ячейки по горизонтали и вертикали; если таблица занимает несколько страниц, автоматически повторять шапку таблицы — первую строку — на каждой странице; разбивать таблицу на две независимые части.

Рис. 5.16. **Диалоговое окно Автоформат таблицы**

Таблицу можно перемещать по тексту, если ее поместить в кадр. Другой возможный способ вставки таблицы в любом месте текста — *выделить* ее и внести под определенным именем в команду **Автотекст**.

Пользователю следует иметь в виду, что Word обладает рядом возможностей, которые в большей степени развиты у табличного процессора Excel, а именно: вводить ***формулы*** и ***функции*** в ячейки; проводить вычисления с данными в ячейках; строить диаграммы на основе данных, содержащихся в таблице.

Ввод формул в соответствующие ячейки осуществляется командой **Таблица/Формула** или командой **Вставка/Поле**, в диалоговом окне которой нужно выбрать поле **Формулы**. При написании формул обозначение колонок и строк таблицы, ссылок на ячейки такое же, как и у всех табличных процессоров.

☑ **Задание.**
Введите в набранный текст табл. 5.1.

☑ **Задание.**
Введите в ячейки табл. 5.1 формулы и функции.

Построение графиков и диаграмм. Для размещения в документе графиков и диаграмм при работе в Word можно использовать автономную программу Microsoft Graph. Она не является частью текстового процессора Word, а представляет собой одну из прикладных программ Windows.

Для построения ***диаграммы*** нужно *выделить* таблицу, установить курсор в месте вставки иллюстрации, вызвать программу MS Graph командой **Вставка/Объект** (или пиктокнопкой **Вставка диаграммы**) и среди объектов выбрать **Microsoft Graph**.

Таблица 5.1. ***Дорожно-транспортные происшествия, повлекшие гибель и ранение людей***

	1992 г.	1993 г.	1994 г.	1995 г.	1996 г.	В % к 1992 г.
Количество ДТП (тыс.)	36,5	37,1	35,6	32,8	29,5	
Число раненых (тыс.)	185	178,7	174,9	167,3	160,5	
Число погибших (тыс.)	200	192,8	189,9	183,9	178,4	
Всего пострадало (тыс.)						

В окне программы Graph расположены два взаимосвязанных окна: таблицы и диаграммы. В первом окне по умолчанию окажется выделенная таблица, а во втором окне — диаграмма. По своему желанию пользователь может изменить тип диаграммы, выбрав в меню **Graph** команду **Тип**. Средствами программы Graph можно редактировать диаграмму, изменять шрифт, размер, положение ее элементов. Для вставки полученной диаграммы в документ нужно поместить указатель мыши вне области диаграммы и щелкнуть левой клавишей мыши. Если возникла необходимость поменять тип диаграммы, нужно снова войти в программу **Graph**. Для этого достаточно дважды щелкнуть по рамке диаграммы.

Если в распоряжении пользователя имеется готовая таблица, созданная в Excel, то быстрее перенести ее в Word, чем создавать подобную в Microsoft Graph. Для этого надо щелкнуть по пиктокнопке **Excel**, открыть нужный табличный файл, выделить таблицу на рабочем листе и задать команду **Правка/Копировать**. Таблица будет помещена в буфер хранения. После этого нужно переключиться в документ Word и выполнить команду **Правка/Вставить** — таблица появится в тексте в том месте, где находится курсор. Аналогично можно переносить из Excel в Word и готовые диаграммы.

Поскольку импорт таблиц и графиков из Excel происходит без затруднений, *таблицы в Word следует использовать в основном для размещения текста и рисунков, а не для вычислений.*

Рис. 5.17. **Диалоговое окно Вставить рисунок**

Существует много способов практического применения таблиц. Пусть имеется файл с текстом визитной карточки. В новом документе построим таблицу с ячейками, приемлемыми для размера одной карточки. Поместим курсор в одну из ячеек. Далее выполним команду **Вставка-Файл** и в диалоговом окне выберем имя нужного файла. Word разместит в ячейке текст визитной карточки с сохранением ее формата. Через буфер обмена можно скопировать содержимое одной ячейки во все остальные. В результате при распечатке будет получена не одна, а сразу несколько визитных карточек.

Вставка рисунков. Чтобы вставить в документ ***рисунок***, нужно вызвать диалоговое окно команды **Вставка/Рисунок** и активизировать имя файла с нужным рисунком. Можно предварительно просмотреть иллюстрации в окошке **Просмотр**.

В диалоговом окне имеются два флажка: **Связать** и **Хранить рисунок в документе**. Если включить флажок **Связать**, то создается связь между документом и графическим файлом, и при распечатке документа будет печататься и рисунок. Если установить флажок **Хранить рисунок в документе**, Word сохраняет графику внутри документа, что приводит к заметному увеличению размера файла документа.

После заполнения диалогового окна и нажатия на кнопку **OK** рисунок окажется вставленным в то место документа, где находится курсор. Очевидно, что его можно поместить и в специально подготовленный пустой кадр. Если пользователь желает редактировать рисунок, нужно дважды щелкнуть по нему левой кнопкой мыши, чтобы запустить программу рисования Microsoft Draw.

Аналогичным образом в текст документа вставляется символы из набора специальных символов командой **Вставка/Символ**. В состав пакета Word входит графическая библиотека ClipArt Gallery, которая состоит из 90 файлов с небольшими рисунками.

☑ Задание.

На первой странице текста вставьте в верхний левый угол рисунок из файла disk.wmf, находящийся в подкаталоге Clipart каталога Winword.

В состав Word включены средства, позволяющие автоматизировать размещение названий к таблицам, рисункам, выделенному тексту, графику и др. Для этого нужно выделить объект, к которому планируется добавить название, и в диалоговом окне команды **Вставка/Название** выполнить все необходимые установки: определить метку названия (рисунок, таблица), указать положение названия по отношению к элементу документа (под\над выделенным объектом), в поле **Название** набрать текст названия объекта, например «Рисунок 1. Пустой кадр», и нажать на кнопку **OK**. Word авто-

матически подсоединит название к объекту и разместит его в соответствии с установками.

Проверка орфографии. Чтобы проверить **орфографию**, нужно установить курсор в начало текста (или *выделить* проверяемую часть текста) и выполнить команду **Сервис/Проверка орфографии** (клавиша **F7**).

Перед проверкой орфографии необходимо задать параметры проверки. Для этого следует:

- открыть меню **Сервис**;
- выбрать команду **Опции**;
- появится диалоговое окно **Опции**;
  выбрать кнопку **Орфография** в верхней части диалогового окна;
- установить флажок проверки **Всегда предлагать замену**;
- установить флажок проверки **Только из основного словаря**;
- установить в области **Пропустить** нужные флажки проверки (при необходимости);
- нажать на кнопку **ОК**.

Для проверки орфографии нужно:

- открыть меню **Сервис**;
- выбрать команду **Орфография**.

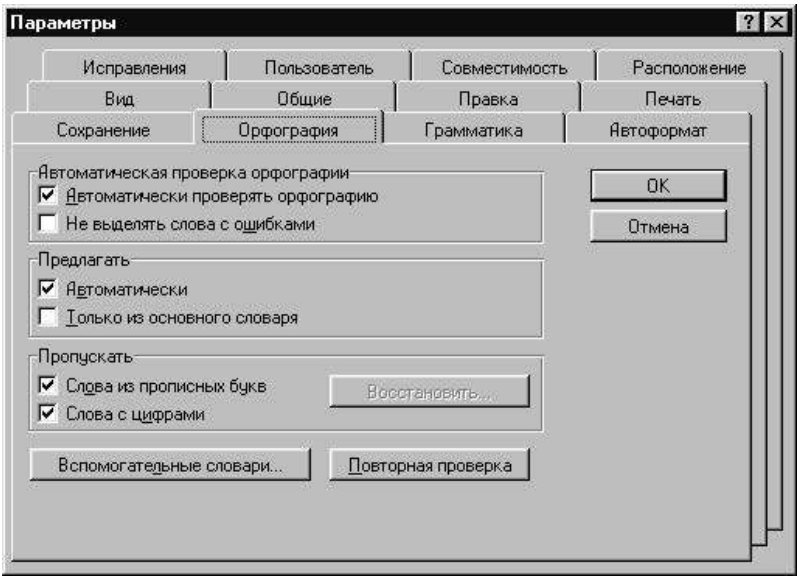


Рис. 5.18. **Диалоговое окно Параметры**

Если встречается неправильно написанное или незнакомое слово, оно выделяется и выводится в диалоговое окно, в котором предоставляется список слов, близких по написанию, в качестве предложений для исправления. Если этот список пуст, то в поле **Заменить на** нужно ввести правильное написание слова:

Если нажать на кнопку **Автокоррекция**, то эта пара слов внесется в список частых опечаток **Автокоррекции**. Для замены слова требуется нажать на кнопку **Заменить**. Если это слово и дальше может встречаться с ошибкой, то следует нажать на кнопку **Заменить Все**, тогда в процессе проверки правописания Word будет автоматически исправлять эту ошибку.

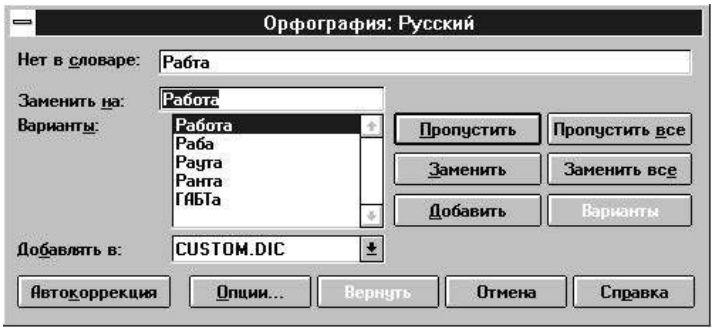


Рис. 5.19. **Диалоговое окно Орфография: Русский**

Если слово написано без ошибок, пользователь может записать его во вспомогательный словарь. Таких словарей можно создать несколько, например словарь для специальных терминов, словарь исключений. При проверке орфографии используется одновременно до 10 словарей. Средства Word позволяют проверять тексты на языках, словари которых включены в поставку. Язык для проверки можно выбрать в диалоговом окне команды **Сервис/Язык**.

☑ **Задание.**

Проверьте орфографию во всем набранном тексте.

Этап сохранения документа при работе с процессором Word

При завершении сеанса работы с Word необходимо записать документ на диск.

Сохранение документа в первый раз осуществляется командой **Файл/Сохранить как** (она также используется и для переименования файла). В диалоговом окне нужно указать, в каком каталоге и на какой диск должен быть помещен документ, а также в поле ввода **Имя файла** набрать имя файла и нажать на кнопку **ОК**.

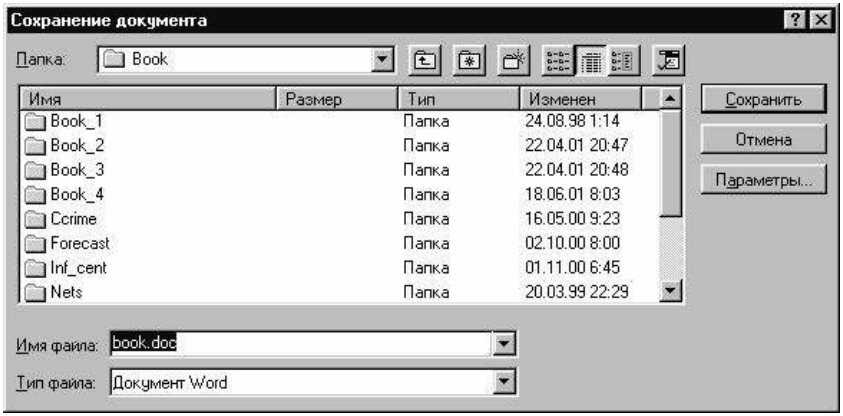


Рис. 5.20. **Диалоговое окно Сохранить как**

Если раньше использовалась команда **Сервис/Параметры** и во вкладке **Сохранение** диалогового окна был включен флажок **Запрашивать сводку**, то после нажатия на кнопку OK на экране появится диалоговое окно **Сводка**, в котором можно заполнить такие позиции, как заголовок, содержание, ключевые слова документа, имя автора, комментарии. Заполненная сводка облегчает впоследствии поиск документа.

Можно **защитить** документ от несанкционированного доступа, активизировав команду **Сервис/Установить Защиту** и в диалоговом окне задав пароль, состоящий максимум из 15 знаков (букв, цифр, символов и пробелов).

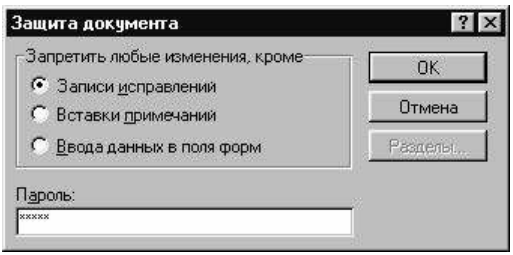


Рис. 5.21. **Диалоговое окно Защита документа**

При повторной записи документа используется более быстрая команда **Файл/Сохранить** — диалоговое окно при этом не появляется.

☑ **Задание.**

Сохраните документ в каталоге... с именем...

Загрузка документов осуществляется командой **Файл/Открыть**, и в диалоговом окне указываются данные о документе. Более быстрая загрузка происходит, когда пользователь открывает меню команды **Файл**. Имя открываемого файла находится внизу меню, среди имен сохраненных ранее файлов. Если файл защищен паролем, то при его открытии Word запросит пароль защиты.

Быстрый способ открытия файлов. Если во время предыдущего сеанса работы с Word for Windows редактировался какой-либо файл и пользователь хочет продолжить с ним работу, он может открыть его более быстрым способом. Для этого нужно:

- открыть меню **Файл**. В нижней части меню выводится список имен нескольких файлов, с которыми работали позже всего;
- щелкнуть левой кнопкой мыши на имени файла, который нужно открыть.

Дополнительные возможности текстового процессора WORD

После того как документ сохранен и вновь открыт, неплохо познакомиться со вспомогательными инструментами (программами), которыми можно воспользоваться, оформляя текст. Помимо упоминавшейся выше программы Microsoft Graph, ответственной за построение графиков, часто используются программы Equation Editor (редактор уравнений), Word Art (текстовые эффекты), MS Draw (рисование), MS Qrganization Chart (организация схем).

Все эти приложения вызываются командой **Вставка/Объект**. Во вкладке диалогового окна **Создать новый** находится нужная программа. Если вставленный объект из приложения в основной документ нуждается в дополнительном редактировании, надо «щелкнуть» по нему два раза мышью, и объект снова окажется в приложении, в котором он был создан, и может быть отредактирован средствами прикладной программы. Это достигается за счет OLE-технологии.

Кратко рассмотрим их возможности.

Редактор формул (уравнений) имеет нерусифицированное окно, и его команды приводятся в англоязычном варианте. Окно имеет панель математических символов и обеспечивает доступ к группе символов или шаблонов, с помощью которых изображаются математические операции. Для написания формулы требуется в выбранные шаблоны вставить соответствующие символы. Созданную формулу следует сопровождать комментарием, разъясняющим назначение отдельных переменных, и располагать его под формулой. Написание текста осуществляется командой **Style/Text**, а выбор русифицированного шрифта возможен в диалоговом окне команды **Style/Define**.

Формулу и пояснительный текст можно форматировать. Для включения созданной формулы в текущий документ следует установить курсор мыши вне кадра объекта, а в окне команды **Сервис/Параметры/Вид** выключить опцию **Пустые рамки рисунков**, иначе на месте формулы будет видна только рамка.

Текстовые эффекты — необычное расположение набранного текста в виде круга, синусоиды, треугольника и др. Такое написание используется для привлечения внимания в приглашениях, рекламных листках, построения фирменных знаков. После запуска Word Art выводит на экран надпись **Примерный текст**, вместо которого можно вводить свой набор. Имеется панель пиктокнопок для создания эффектов и 36 шаблонов изображения формы текста (наклоны, изгибы, вертикальное и горизонтальное смещение). С помощью этих шаблонов можно придать тексту практически любую форму.

Существуют также команды форматирования текста. Чтобы перенести построенный объект в документ в позицию курсора (а он уже установлен в пустом кадре), нужно щелкнуть мышью в любом месте вне текстового эффекта.

Рисование — создание рисунка средствами графического редактора MS Draw. Для того чтобы появилась панель рисования, нужно щелкнуть по пиктокнопке **Рисунок** стандартной панели инструментов или войти в программу командой **Вставка/Объект** и в диалоговом окне выбрать объект **Рисунок Microsoft Word**.

Для создания собственного рисунка существуют фактически те же возможности, что и у графического редактора Paintbrush, являющегося приложением Windows. Помимо этого, элементы, из которых состоит рисунок, можно разгруппировать, перемещать относительно друг друга, переворачивать, вращать, затем снова сгруппировать. Но все манипуляции выполняются только с *выделенными* элементами.

Если объект построен, его можно поместить впереди или позади текста документа (так называемые водяные знаки). В программе Рисование возможно создавать выноски (небольшие прямоугольники со стрелками), в которые внесены комментарии к рисунку. Чтобы рисунок перенести в документ, достаточно нажать на кнопку **Закрыть рисунок**.

Организация схем — программа, позволяющая быстро создать из предлагаемых блоков и линий сложную схему. В прямоугольники можно вводить текст, а над схемой ввести заголовок. Компоненты отдельных частей схем (шаблоны) изображены на пиктокнопках панели инструментов этого приложения. Вставка готовой схемы в Word документ происходит так же, как вставка диаграммы или рисунка.

Следует отметить, что вызов указанных программ, работа в них и возвращение в Word происходит замедленно.

Работа с большими документами. Если документ получился большим, то для нахождения нужных мест в документе, их помечают ***закладками***. Для создания закладки нужно поместить курсор на место ее вставки и в диалоговом окне команды **Правка/Закладка** присвоить закладке имя (первой в имени должна стоять буква). Количество закладок не ограничено, и они сохраняются от сеанса к сеансу.

Следует упомянуть о двух командах, которые также облегчают работу в Word: **Перейти** и **Сортировка**.

Для *быстрого перемещения курсора* по документу удобно пользоваться командой **Правка/Перейти**. В диалоговом окне имеется целый список элементов документа, куда необходимо поместить курсор. Это — страница, раздел, строка, закладка, сноска, примечание. Если требуется перейти, например, к месту, где находится закладка, в пустой строке окна надо ввести ее имя и нажать на кнопку **Перейти**.

Иногда нужно провести **сортировку** абзацев по первым буквам в алфавитном порядке, по датам и номерам, если они стоят в начале абзаца. Для сортировки абзацев нужно выделить их и в диалоговом окне команды **Таблица/Сортировка текста** указать параметры сортировки абзацев и нажать на кнопку **ОК**.

Аналогично можно сортировать строки в столбцах. Для этого нужно *выделить* таблицу и в диалоговом окне команды **Таблица/Сортировка** указать столбец, в котором будет проводиться сортировка, порядок сортировки (убывание/возрастание), в разделе **Затем** установить дополнительные критерии (вторые или третьи буквы или цифры), которые будут учитываться при сортировке с одинаковыми первыми буквами или цифрами.

Часто в документе требуется сделать ***ссылку*** на рисунок, таблицу или раздел, который встречался ранее в тексте, например: «см. рис. 2—1», «Подробнее см. раздел 2.3 на с. ». Word позволяет автоматически связать ссылку и объект, на который необходимо сослаться. Перед созданием перекрестной ссылки на некоторый объект необходимо предварительно пометить его, например, командой **Вставка/Название** (к таким помеченным элементам относятся названия рисунков, таблиц, заголовков, формул, сносок, закладок). При

редактировании документа объект может оказаться, например, на другой странице. Все изменения автоматически скажутся на ссылке.

Создание перекрестной ссылки должно начинаться с размещения в документе начального текста ссылки. Это могут быть, например, слова «см. рис. ». Далее в диалоговом окне команды **Вставка/Перекрестная ссылка** нужно выполнить все необходимые установки: указать тип ссылки (рисунок, таблица и др.); тип информации, которая должна быть размещена в ссылке (метку и номер рисунка, номер страницы и др.); в списке **Для какого объекта (рисунка)** выбрать конкретный элемент документа, на который требуется сослаться. При нажатии на кнопку **Вставить** в том месте документа, где находится курсор, будет размещена соответствующая ссылка. Можно расширить информацию, уже размещенную в ссылке, например, добавить номер страницы. Для закрытия диалогового окна следует нажать кнопку **Закрыть**.

Для обновления всех перекрестных ссылок необходимо выделить весь документ **CTRL+A** и нажать **F9**. Для обновления отдельной ссылки достаточно установить курсор в обновляемой ссылке и нажать **F9**.

Этап печати документа: операции подготовки к печати и печать

При совместной работе с документом его исполнителя и начальника (или рецензентов) автор может вставлять в документ разъяснения смысла слова тех или иных фрагментов текста. В документе они не видимы, но пронумерованы особой меткой и называются в меню Word ***примечаниями***. Чтобы текст примечания можно было прочитать, нужно щелкнуть по его маркеру два раза.

При печати документа примечания и их маркеры не печатаются. Создание примечания аналогично вводу сноски. Следует поместить курсор в конец абзаца, к которому требуется сделать пояснения. После выполнения команды **Вставка/Примечание** внизу окна документа откроется панель примечаний, а на месте курсора появится маркер с инициалами автора и номером примечания. После ввода комментария нужно нажать на кнопку **Закрыть**.

Получив файл документа, можно внести в его текст изменения, не уничтожая первоначального текста, а делая ***пометки исправлений.*** Внесение пометок осуществляется командой **Сервис/Исправления**. В диалоговом окне нужно включить флажок **Показывать исправления на экране**, нажать на кнопку **Параметры**, в результате появится вкладка **Исправления** с параметрами пометок.

Можно, например, для привлечения внимания исполнителя документа на строки с исправленным текстом проводить различные вертикальные линии на полях, зачеркивать удаленный текст с измене-

ниями цвета символов и подчеркивать новый текст с отображением символов другим цветом.

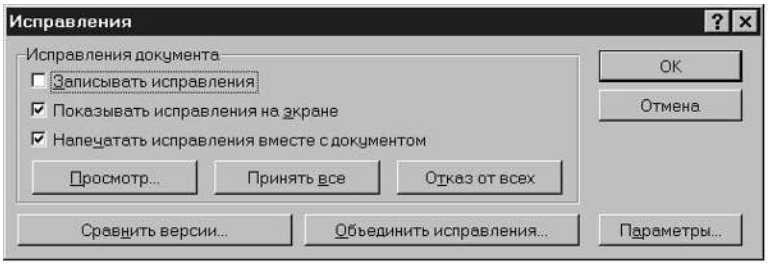


Рис. 5.22. **Диалоговое окно Исправления**

Если автор согласен со всеми исправлениями, он должен нажать на кнопку **Принять все** в диалоговом окне команды **Сервис/Исправления**. Тогда Word обновляет документ с учетом всех исправлений и убирает пометки.

Если же он не согласен с изменениями в тексте, он может нажать кнопку **Отказ от всех**, чтобы отменить все исправления. Однако более верный способ учета исправлений заключается во включении режима **Просмотр**. В этом случае автор, просматривая замечания, может либо соглашаться с ними либо отвергать каждое из исправлений в отдельности. Чтобы выйти из режима исправлений, нужно в диалоговом окне отключить флажок **Показывать исправления на экране**.

Одним из несомненных достоинств Word является возможность формирования ***предметного указателя***, который представляет собой перечень расположенных в алфавитном порядке терминов с указанием страниц, на которых они упомянуты. Он размещается, как правило, в конце документа.

Для создания предметного указателя нужно *выделить* слово, которое должно быть в него помещено, и нажать комбинацию клавиш **ALT+SHIFT+X**. В появляющемся диалоговом окне выделенный термин заносится в строку **Главный документ**. Его можно отредактировать, поставив, например, в именительном падеже, а затем нужно нажать кнопку **Пометить**, и выбранный термин заносится в предметный указатель.

После вставки всех терминов в указатель нужно установить курсор в конце документа, выполнить команду **Вставка/Оглавление и Указатели**. В диалоговом окне выбрать раздел **Указатель**, в поле **Тип** установить опцию **С отступом**, задать режим **Номера страниц вправо** и способ заполнения пространства между терминами и номерами страниц, определить количество колонок и нажать на кнопку **ОК**.

После того как документ полностью отредактирован, Word может автоматически создать ***оглавление*** документа. Однако оглавление сформируется, если заголовки документа предварительно структурированы и имеют стандартные стили. Иначе они воспринимаются как текст, и оглавление создать невозможно.

Для создания структурированного оглавления нужно установить курсор в начало документа и воспользоваться командой **Вставка/Оглавление и Указатели**. В диалоговом окне во вкладке **Оглавление** надо установить один из семи предлагаемых стилей формата оглавления, включить флажок **Номера страниц по правому краю**, указать количество уровней заголовков, выбрать заполнитель между заголовками и номерами страниц, после этого нажать на кнопку **ОК**.

Если заголовки не структурированы, нужно установить курсор в начало документа и войти в ***режим эскиза*** командой **Вид/Структура документа**. Чтобы различать стили абзацев, следует выделить на экране слева место для колонки стиля командой **Сервис/Параметры**. Во вкладке диалогового окна **Вид** надо установить ширину колонки стиля, равной 1,5—1,8 см. В этом случае напротив каждого абзаца будет стоять или имя стиля, если это текст, или **Заголовок**, если это заголовок.

Затем, прокручивая текст, следует останавливать курсор у нестандартных заголовков, и в панели инструментов **Структура** использовать кнопки повышения или понижения уровня заголовка, превращая тем самым нестандартные заголовки в стандартные. В результате такой манипуляции в колонке стиля появятся слова: **Заголовок 1**, **Заголовок 2** и т.д. Таким образом создается ***иерархическая структура заголовков***. Если заголовки сформированы, можно кнопкой на панели со знаком минус (−) сделать тексты под заголовками невидимыми. В этом случае останутся только заголовки, и будет видна структура документа. В указанном режиме можно менять местами и соответствующие заголовкам тексты.

Если заголовки не имеют нумерации, их можно пронумеровать как списки командой **Формат/Списки**. После этого можно создать оглавление.

Когда создается документ с большим количеством глав, разделов и параграфов, то *имеет смысл сначала создать его макет в виде структурной иерархии заголовков* в режиме эскиза, а затем уже вводить текст под структурированными заголовками в нормальном режиме просмотра документа.

Если пользователю необходимо узнать, сколько в тексте страниц, слов, символов, абзацев, строк, то информацию можно получить, выполнив команду **Сервис/Статистика**. Однако более полную статистику дает команда **Файл/Свойства**. В диалоговом окне нужно выбрать вкладку **Статистика**, и Word даст полную информацию о

размере файла, общем времени редактирования текста, числе его сохранений, времени создания, сохранения, распечатки текста и др.

Перед печатью желательно просмотреть документ. Командой **Файл/Просмотр** Word создает в центре окна уменьшенное изображение страницы.

Щелкнув мышью по странице, можно либо увеличить, либо уменьшить изображение. То же самое можно сделать, если воспользоваться кнопкой **Масштаб**.

Чтобы напечатать документ, надо установить параметры печати в диалоговом окне команды **Файл/Печать**: печатать ли весь текст, или текущую страницу, или диапазон страниц, сколько копий, печатать только текст или с изображением рисунков и других элементов, после чего нажать на кнопку **OK**. Можно печатать текст документа в альбомном и книжном режиме.

Если установлена фоновая печать, то **Диспетчер Печати** самостоятельно управляет печатью документа, предоставляя возможность пользователю работать в это время с каким-либо приложением Windows. Если в **Диспетчере Печати** имеется несколько документов, то он их выстраивает в очередь с приоритетами.

Помимо стандартного шаблона, например, Normal.dot в Word существуют несколько десятков *специальных шаблонов*. Их можно открыть в диалоговом окне командой **Файл/Создать**. Многие шаблоны из этого списка имеют дополнительное имя **Мастер**. В мастерах содержатся отработанные формы, заполнение которых пользователем производится в полуавтоматическом режиме.

Каждый мастер представляет собой стандартный документ с различными трафаретами и имеет свое имя, например **мастер расписаний**, **мастер служебных записок**, **мастер календаря** и др.

Если у сотрудника намечается юбилей или он награжден, то можно подготовить ему красиво оформленную грамоту, используя **мастер наградных листов**. Вызвав нужный мастер, пользователь должен вводить соответствующие данные в режиме диалога и нажимать на кнопку **Дальше** для перехода в следующее окно диалога. После завершения ввода всей информации нужно нажать кнопку **Изготовить** и мастер оформит документ в соответствии с введенным заданием.

Несомненным достоинством Word является возможность пользователей работать над составлением **Главного документа**, состоящего из множества поддокументов. Главный документ рассматривается как схема, каждый заголовок в которой представляет отдельный документ.

Средства работы с главным документом удобно использовать при работе в сети, когда он и его поддокументы хранятся на файл-сервере сети. Пользователи сети могут работать с любым поддокументом, от-

крывая при работе только главный документ. Когда пользователь вызывает заголовок в главном документе, он тем самым открывает соответствующий поддокумент. При этом нельзя менять имя файла поддокумента, иначе разрывается связь с главным документом.

Word отслеживает автора каждого поддокумента. Только автор имеет право редактировать поддокумент. Другой автор может открыть поддокумент только для чтения. Вход в главный документ осуществляется командой **Вид/Главный** документ. Совместная работа исполнителей над созданием главного документа в сети существенно ускоряет его подготовку.

Для более быстрой работы с *выделенным* объектом можно развернуть ***динамическое меню*** с командами, позволяющими манипулировать этим объектом. Для отображения меню на экране нужно установить указатель мыши на выделенный фрагмент и нажать правую кнопку мыши.

Контрольные вопросы и задания

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?
5. Назовите основные атрибуты шрифта. Оформите предложенный текст, используя различное шрифтовое оформление.
6. Назовите основные параметры оформления текстового документа и перенастройте их в соответствии с предложенным стандартом, пользуясь указанным текстовым редактором.
7. Назовите основные параметры абзаца, входящие в понятие «стиль оформления абзаца». Оформите предложенный текст, используя различные абзацные стили.
8. Представьте указанные данные в виде таблицы, используя различные средства оформления текста (рамка, фон ячеек, цвет шрифта и т.д.).
9. Какие типовые операции можно выполнить с выделенным текстовым фрагментом?
10. Какие функции выполняет буфер обмена?
11. В чем заключается сущность операции автозамены?
12. С какой целью производится форматирование документа?
13. В каких целях используются колонтитулы документа?
14. В чем заключаются основные преимущества использования шаблонов документов?
15. Как в текстовых процессорах производится проверка правописания слов?

Глава 6

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

6.1. Понятие информационно-вычислительной сети

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 обработки данных 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 млн 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 последние десятилетия к формированию основ концепции *сетевого компьютера.* Суть ее заключается в том, что ПК, работающий в сети, получает определенные преимущества перед автономным ПК:

- программы загружаются непосредственно из сети;
- нет необходимости иметь на ПК жесткий диск;
- экономятся время и средства на покупку и обновление ПО, так как 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.

6.2. Классификация ИВС

Вычислительные сети классифицируют по различным признакам:

➢ ***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.

➢ ***По способу управления.***

Сети с централизованным управлением, в которых выделяется 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 — сети Windows for Workgroups и Windows 95. Нажатием на кнопку мыши вы можете предоставить свой диск или принтер в коллективное пользование.

➢ ***По характеру выполняемых функций:***
- вычислительные;
- информационные.

➢ ***По составу вычислительных средств:***
- *однородные* — объединяют однородные вычислительные средства;
- *неоднородные* — объединяют различные вычислительные средства.

➢ ***По типу организации передачи данных:***
- коммутация каналов;
- коммутация сообщений;
- коммутация пакетов.

6.3. Базовая модель взаимодействия открытых систем

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 MKKTT (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 физиче-

ским 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 вычислительной 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 непрерывную 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.

6.4. Некоторые вопросы организации 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 (*American Standard Code for Information Interchange*) — передача символьной информации с помощью 7-битового кодирования, позволяющего закодировать заглавные и строчные буквы английского алфавита, а также некоторые спецсимволы;

8-битовые коды (например, КОИ-8 и др.) — для представления символов национальных алфавитов и специальных знаков (например, 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 аналогию 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, т.е. преобразовать в колебания звуковой частоты.

Еще один метод доступа к ЛВС 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.

При установке специального программного обеспечения любой персональный компьютер может обмениваться сообщениями с любым компьютером другой ЛВС посредством *электронной почты*.

6.5. Локальные вычислительные сети

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 сотрудников 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 1 Гбод;
- телефонная линия — от 2400 бод до 56 Кбод;
- спутник (10 000 компьютеров одновременно) — около 1 Мбод.

К о м п о н е н т ы ЛВС: сетевые устройства и средства коммуникаций.

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

- *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;
- *серверы* — отдельные компьютеры с программным обеспечением, выполняющие функции управления сетевыми ресурсами общего доступа;
- *сетевое программное обеспечение.*

Рассмотрим некоторые из перечисленных к о м п о н е н т о в с е т и 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 трудноразрешимой 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.

Рассмотрим подробнее свойства некоторых передающих сред.

➢ ***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 слабовосприимчив 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), при этом расстояние устойчивой передачи увеличивается до 10 км. Для ЛВС с топологией «шина» или «дерево» кабель должен иметь на конце *терминатор* (*согласующий резистор*).

➢ ***Ethernet-кабель.***

Толстый Ethernet — коаксиальный кабель с волновым сопротивлением 50 Ом (thick Ethernet, или желтый кабель — *yellow cable*). Использует 15-контактное стандартное включение. Максимально допустимое расстояние передачи без репитера не превышает 500 м, а общая длина сети Ethernet — 3000 м. Толстый Ethernet, вследствие магистральной топологии использует на конце лишь один терминатор. По параметрам помехозащищенности является дорогой альтернативой обычному коаксиальному кабелю.

Тонкий Ethernet — коаксиальный кабель с волновым сопротивлением 50 ом (thin Ethernet) и скоростью передачи информации 10^7 бит/с, более дешевый, чем толстый Ethernet.

ЛВС с кабелем thin Ethernet характеризуются низкой стоимостью, минимальными затратами при наращивании и не требуют дополнительного экранирования. Кабель присоединяется к сетевым платам рабочих станций с помощью тройниковых соединителей (T-connectors) с малогабаритными байонетными разъемами (CP-50). При соединении сегментов thin 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. Характеристики типовых передающих сред приведены в табл. 6.1.

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*.

Таблица 6.1. ***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

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». Преимущество конфигураций этого класса — простота организации сети.

➢ *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 соединения.

Для предотвращения коллизий в передаче информации чаще всего применяется *временной метод разделения*, согласно которому каждой подключенной рабочей станции в определенные моменты времени предоставляется исключительное право на использование канала передачи информации. Поэтому требования к пропускной способности сети при повышенной нагрузке, т.е. при вводе новых рабочих станций, снижаются.

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

В ЛВС с широкополосной передачей информации рабочие станции получают частоту, на которой они могут отправлять и получать информацию. Пересылаемые данные модулируются на соответствующих несущих частотах. Техника широкополосных сообщений

позволяет одновременно транспортировать в коммуникационной среде довольно большой объем информации.

Звездообразная топология. Топология сети в виде *звезды с активным центром* (рис. 6.1) 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.

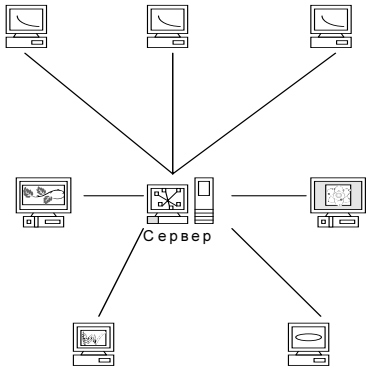


Рис 6.1. **Топология сети в виде звезды**

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 невозможно использовать ранее выполненные кабельные связи: к новой рабочей станции необходимо прокладывать отдельный кабель от центрального узла сети.

Звездообразная топология при хорошей производительности центрального узла *является одной из наиболее быстродействующих топологий* ЛВС, поскольку передача информации между рабочими станциями происходит по выделенным линиям, используемым только этими рабочими станциями. Частота запросов на передачу информации от одной станции к другой — невысокая по сравнению с другими топологиями.

Производительность ЛВС звездообразной топологии в первую очередь определяется параметрами центрального узла, который вы-

ступает в качестве сервера сети. Он может оказаться узким местом сети. В случае выхода из строя центрального узла нарушается работа сети в целом.

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. 6.2).

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 эффективной, 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.

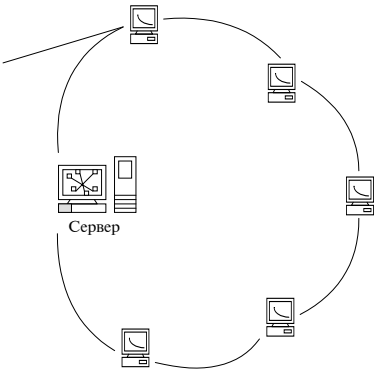


Рис. 6.2. **Кольцевая топология**

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 такая топология 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 до 16 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. Каждой рабочей станции присваивается соответствующий ей адрес, по которому передается управление (от старшего — к младшему и от самого младшего — к самому старшему). Разрыв соединения происходит только для нижерасположенного (ближайшего) узла вычислительной сети, так что лишь в редких случаях может нарушаться работа всей сети.

Шинная топология. В ЛВС с шинной топологией основная передающая среда (*шина*) — общая для всех рабочих станций (рис. 6.3). 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.

Однако в простейшей сети Ethernet с шинной топологией в качестве передающей среды используется тонкий Ethernet-кабель с тройниковым соединителем (Т-коннектором), поэтому расширение такой сети требует разрыва шины, что приводит к нарушению функционирования сети. Более дорогостоящие решения предполагают установку вместо Т-коннекторов пассивных штепсельных коробок.

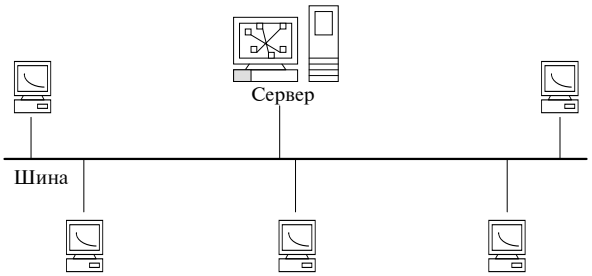


Рис. 6.3. **Шинная топология**

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 табл. 6.2.

Таблица 6.2. ***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

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.

Типы построения ЛВС по методам передачи информации

Сеть Token Ring. Этот стандарт разработан фирмой «IBM». В качестве передающей среды применяются неэкранированная или

экранированная витая пара или оптоволокно. Скорость передачи данных от 4 до 16 Мбит/с. В качестве метода управления доступом рабочих станций к передающей среде используется *маркерное кольцо* (Token Ring). Основные положения метода:

- кольцевая топология ЛВС;
- рабочая станция может передавать данные, только получив маркер, т.е. разрешение на передачу информации;
- в любой момент времени только одна станция в сети обладает таким правом.

В ЛВС Token Ring используются *три основных типа пакетов*:

- пакет Управление/Данные (Data/Command Frame);
- маркер (Token);
- пакет сброса (Abort).

➢ ***Пакет Управление/Данные.*** С помощью такого пакета выполняется передача данных или команд управления работой сети.

➢ ***Маркер***. Станция может начать передачу данных только после получения такого пакета. В кольце может быть только один маркер и, соответственно, только одна станция с правом передачи данных.

➢ ***Пакет Сброса.*** Посылка такого пакета вызывает прекращение передачи информации.

Сеть Token Ring допускает подключение компьютеров по звездообразной топологии.

Локальная сеть Arcnet. Arcnet (*Attached Resource Computer NETWork*) — простая, недорогая, надежная и гибкая архитектура ЛВС. Разработана корпорацией *Datapoint* в 1977 г. Впоследствии лицензию на Arcnet приобрела корпорация SMC (*Standard Microsistem Corporation*), которая стала основным разработчиком и производителем оборудования для сетей Arcnet. В качестве передающей среды используются витая пара, коаксиальный кабель с волновым сопротивлением 93 Ом и оптоволоконный кабель. Скорость передачи данных составляет 2,5 Мбит/с. При подключении устройств применяют топологии *шина* и *звезда*.

Метод управления доступом станций к передающей среде — *маркерная шина* (Token Bus). Метод предусматривает следующие правила:

- устройства, подключенные к сети, могут передавать данные, только получив разрешение на передачу (маркер);
- в любой момент времени только одна станция в сети обладает таким правом;
- данные, передаваемые одной станцией, доступны всем станциям сети.

Принципы работы. Передача каждого байта в Arcnet выполняется посылкой ISU (*Information Symbol Unit* — единица пе-

редачи информации), состоящей из трех служебных старт/стоповых битов и восьми битов данных. В начале каждого пакета передается начальный разделитель AB (*Alert Burst*), который состоит из шести служебных битов. Начальный разделитель выполняет функции преамбулы пакета.

В Arcnet определены пять типов пакетов:

1. *Пакет ITT* (Information To Transmit) — приглашение к передаче. Эта посылка передает управление от одного узла сети другому. Станция, принявшая пакет ITT, получает право на передачу данных.

2. *Пакет FBE* (Free Buffer Enquiries) — запрос о готовности к приему данных. Этим пакетом проверяется готовность узла к приему данных.

3. *Пакет данных.* С помощью этой посылки производится передача данных.

4. *Пакет ACK (*ACKnowledgments) — подтверждение приема. Подтверждение готовности к приему данных или подтверждение приема пакета данных без ошибок, т.е. ответ на FBE и пакет данных.

5. *Пакет NAK* (Negative AcKnowledgments) — неготовность к приему. Неготовность узла к приему данных в ответ на FBE или принятие пакета с ошибкой.

Локальная сеть Ethernet. Спецификацию Ethernet в конце 1970-х гг. предложила компания *Xerox.* Позднее к этому проекту присоединились компании *Digital Equipment Corporation* (DEC) и Intel. В 1982 г. была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet разработан стандарт IEEE 802.3.

Основные принципы работы:

- шинная топология на логическом уровне;
- все устройства, подключенные к сети, равноправны, т.е. любая станция может начать передачу в любой момент времени (если передающая среда свободна);
- данные, передаваемые одной станцией, доступны всем станциям сети.

6.6. 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: OS/2, Windows NT, Windows 95. 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: 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). Используются в операционных системах Novell NetWare v3.1x. 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). Используется в LANServer и LANManager. 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). В данном подходе все ресурсы сети: серверы, пользователи, сетевая печать, хране-

ние данных и т.п. рассматриваются 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. Пользователю, зарегистрированному на одном сервере, 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.

Рассмотрим более подробно характеристики некоторых сетевых операционных систем и требования, которые они предъявляют к программному и аппаратному обеспечению ЛВС.

Novell NetWare 3.11

Отличительные черты:
- эффективная файловая система;
- самый широкий выбор аппаратного обеспечения.

Основные характеристики и требования к аппаратному обеспечению:
- центральный процессор: 386 и выше;
- минимальный объем жесткого диска: 9 Мбайт;
- объем ОП (Оперативной Памяти) на сервере: 4 МБайт — 4 Гбайт;
- минимальный объем ОП РС (Рабочей Станции) клиента: 640 Кбайт;
- операционная система: собственная разработка Novell;
- протоколы: IPX/SPX;
- мультипроцессорность: нет;
- количество пользователей: 250;
- максимальный размер файла: 4 Гбайт;
- шифрование данных: нет;
- управление распределенными ресурсами сети: таблицы bindery на сервере;
- система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, поддержка накопителя на магнитной ленте, резервное копирование таблиц bindery и данных;
- сжатие данных: нет;
- файловая система клиентов: DOS, Windows, Mac (доп.), OS/2 (доп.), UNIX (доп.), Windows NT.

Windows NT Advanced Server 3.1, Microsoft Corp.

Отличительные черты:
- простота интерфейса пользователя;

- доступность средств разработки прикладных программ и поддержка прогрессивных объектно-ориентированных технологий.

Все это привело к тому, что эта операционная система может стать одной из самых популярных сетевых операционных систем.

Интерфейс напоминает оконный интерфейс Windows 3.1, время инсталляции — около 20 мин. Модульное построение системы упрощает внесение изменений и перенос на другие платформы. Обеспечивается защищенность подсистем от несанкционированного доступа и от их взаимного влияния (если зависает один процесс, это не влияет на работу остальных). Есть поддержка удаленных станций — Remote Access Service (RAS), но не поддерживается удаленная обработка заданий.

Windows NT предъявляет более высокие требования к производительности компьютера по сравнению с NetWare.

Основные характеристики и требования к аппаратному обеспечению:

- центральный процессор: 386 и выше, MIPS, R4000, DEC Alpha AXP;
- минимальный объем жесткого диска: 90 Мбайт;
- минимальный объем ОП на сервере: 16 Мбайт;
- минимальный объем ОП PC клиента: 12 Мбайт для NT, 512 Кбайт для DOS;
- операционная система: Windows NT;
- протоколы: NetBEUI, TCP/IP, IPX/SPX, AppleTalk, AsyncBEUI;
- мультипроцессорность: поддерживается;
- количество пользователей: не ограничено;
- максимальный размер файла: не ограничен;
- шифрование данных: уровень С-2;
- управление распределенными ресурсами сети: домены;
- система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, RAID 5, поддержка накопителя на магнитной ленте, резервное копирование таблиц домена и данных;
- сжатие данных: нет;
- фрагментация блоков (Block Suballocation): нет;
- файловая система клиентов: DOS, Windows, Mac, OS/2, UNIX, Windows NT.

NetWare 4, Nowell Inc.

Отличительная черта: применение специализированной системы управления ресурсами сети (*NetWare Directory Services*, NDS) позволяет строить эффективные информационные системы с количеством пользователей до 1000. В NDS определены все ресурсы, услуги и пользователи сети. Эта информация распределена по всем серверам сети.

Для управления памятью используется только одна область (pool), поэтому оперативная память, освободившаяся после выполнения каких-либо процессов, становится сразу доступной операционной системе (в отличие от NetWare 3).

Новая система управления хранением данных (*Data Storage Managment*) состоит из трех компонентов, позволяющих повысить эффективность файловой системы:

1. *Фрагментация Блоков или Разбиение Блоков Данных на Подблоки* (*Block Suballocation*). Если размер блока данных на томе 64 Кбайта, а требуется записать файл размером 65 Кбайт, то ранее потребовалось бы выделить 2 блока по 64 Кбайта. При этом 63 Кбайта во втором блоке не могут использоваться для хранения других данных. В NetWare 4 система выделит в такой ситуации один блок размером 64 Кбайта и два блока по 512 Байт. Каждый частично используемый блок делится на подблоки по 512 Байт, свободные подблоки доступны системе при записи других файлов.

2. *Упаковка Файлов* (*File Compression*). Долго не используемые данные система автоматически компрессирует, упаковывает, экономя таким образом место на жестких дисках. При обращении к этим данным автоматически выполняется декомпрессия данных.

3. *Перемещение Данных* (*Data Migration*). Долго не используемые данные система автоматически копирует на магнитную ленту либо другие носители, экономя таким образом место на жестких дисках.

Встроенная поддержка Протокола Передачи Серии Пакетов (*Packet-Burst Migration*). Этот протокол позволяет передавать несколько пакетов без ожидания подтверждения о получении каждого пакета. Подтверждение передается после получения последнего пакета из серии.

При передаче через шлюзы и маршрутизаторы обычно выполняется разбиение передаваемых данных на сегменты по 512 байт, что уменьшает скорость передачи данных примерно на 20%. Применение в NetWare 4 протокола LIP (*Large Internet Packet*) позволяет повысить эффективность обмена данными между сетями, так как в этом случае разбиение на сегменты по 512 байт не требуется.

Все системные сообщения и интерфейс используют специальный модуль. Для перехода к другому языку достаточно поменять этот модуль или добавить новый. Возможно одновременное использование нескольких языков: один пользователь при работе с утилитами использует английский язык, а другой в это же время русский.

Утилиты управления поддерживают DOS, Windows и OS/2-интерфейс.

Основные характеристики и требования к аппаратному обеспечению:

- центральный процессор: 386 и выше;
- минимальный объем жесткого диска: от 12 Мбайт до 60 Мбайт;

- объем ОП на сервере: 8 Мбайт — 4 Гбайт;
- минимальный объем ОП PC клиента: 640 Кбайт;
- операционная система: собственная разработка Novell;
- протоколы: IPX/SPX;
- мультипроцессорность: нет;
- количество пользователей: 1000;
- максимальный размер файла: 4 Гбайт;
- шифрование данных: С-2;
- управление распределенными ресурсами сети: NDS;
- система отказоустойчивости: дублирование дисков, зеркальное отражение дисков, SFT II, SFT III, поддержка накопителя на магнитной ленте, резервное копирование таблиц NDS;
- сжатие данных: есть;
- фрагментация блоков (*Block Suballocation*): есть;
- файловая система клиентов: DOS, Windows, Mac (5), OS/2, UNIX(доп.), Windows NT.

6.7. Глобальная компьютерная сеть Internet

История создания Internet

Около 20 лет назад Министерство обороны США создало сеть, которая явилась прародительницей Internet — она называлась ARPAnet и 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 (ЛВС), такие как Ethernet и др. На большинстве рабочих станций ЛВС была установлена операционная система UNIX, которая имела возможность работы в сети с протоколом Internet. 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. В конце 1980-х гг. NSF создал пять суперкомпьютерных центров, сделав их доступными для использования в любых научных учреждениях. Однако попытка ис-

пользовать для организации связи коммуникации ARPAnet потерпела крах, столкнувшись с бюрократией оборонной отрасли и проблемой обеспечения персоналом. В результате NSF построил собственную сеть, основанную на IP-технологии. Центры были соединены специальными телефонными линиями с пропускной способностью 56 Kbps (т.е. 56 Кбайт/с). Совместное использование суперкомпьютеров позволяло использовать множество других вещей, не относящихся к суперкомпьютерам. Поток сообщений в сети нарастал и в конечном итоге перегрузил управляющие сетью компьютеры и связывающие их телефонные линии.

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.

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

Основы устройства и функционирования Internet

Internet — это глобальная сеть, с развитием которой связывают новый этап в развитии информационной революции конца XX столетия. Сеть позволяет решить следующие проблемы:

- практически неограниченные возможности передачи и распространения информации;
- удаленный доступ к огромным массивам накопленных информационных ресурсов;
- общение между пользователями компьютерных сетей в различных странах мира.

Число пользователей Internet в мире строго подсчитать невозможно, но по приблизительным оценкам оно составляет несколько десятков миллионов человек. По одной из методик подсчета количество хост-компьютеров, подключенных к Internet, в январе 1996 г. превысило 9,5 млн, и этот показатель в последнее время ежегодно удваивался. Число пользователей в России, работающих в режиме on-line, превысило стотысячный рубеж, число хост-компьютеров составляет несколько десятков тысяч.

Internet представляет собой *всемирное объединение взаимосвязанных компьютерных сетей.* Использование общих протоколов семей-

ства TCP/IP и единого адресного пространства позволяет говорить об Internet как о единой глобальной «метасети», или «сети сетей». При работе на компьютере, имеющем подключение к Internet, можно установить связь с любым другим подключенным к Сети компьютером и реализовать обмен информацией с помощью того или иного прикладного сервиса Internet (WWW, FTP, E-mail и др.).

Домашний компьютер или рабочая станция локальной сети получает доступ к глобальной сети Internet благодаря установлению соединения (постоянного или сеансового) с компьютером *сервис-провайдера* — организации, сеть которой имеет постоянное подключение к Internet и предоставляет 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 Internet благодаря подключению к международным сервис-провайдерам — сетям, входящим в мировую магистральную инфраструктуру Internet. 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 Internet 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 Internet и оказывают существенное влияние на качество предоставляемых услуг.

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

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

Совет старейшин представляет собой группу приглашенных добровольцев, называемую IAB (Совет по архитектуре Internet). IAB ре-

гулярно собирается, чтобы утвердить стандарты и распределить ресурсы, такие, например, как сетевые адреса.

Пользователи Internet высказывают свои замечания и предложения на встречах IETF (Оперативного инженерного отряда Internet). IETF — это добровольная организация; которая регулярно собирается, чтобы обсудить текущие эксплуатационные и технические проблемы. Для решения важных проблем IETF создаются рабочие группы. По результатам исследования рабочая группа обычно выпускает доклад.

За Internet никто централизованно не платит: каждая сеть или пользователь платит за свою часть. Так, например, NSF платит за содержание NSFNET, а NASA — за Научную сеть NASA (NASA Science Internet). 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 построен Internet, 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 разных типов. Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу связи.

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

Персональный доступ в Internet, особенно в России, пока «дорогое удовольствие», однако многие организации, особенно институты, уже имеют доступ в Internet. В этом случае пользователь не платит «из своего кармана», не имеет дела с поставщиками услуг и т.д.

Имеются возможности получить доступ в Internet не через прямых распространителей, т.е. без лишних затрат. Одна из таких возможностей — служба, называемая Freenet, т.е. бесплатная сеть. Это информационная система, основанная соответствующим сообществом и обычно имеющая модемный доступ к Internet по телефону.

Уровни сети Internet

Пересылка битов в Internet происходит на *физическом уровне* схемы ISO OSI. Попытка дать краткое и доступное описание затруд-

нительна. Потребуется введение большого количества специальных терминов, понятий, описаний процессов на физическом уровне и т.д. Для понимания работы сети это необязательно. Можно считать, что существует канал, по которому перекачиваются биты.

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

Сеть Internet 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 не доступна. Это приводит к нерациональному использованию линий сети. Internet является *сетью с коммутацией пакетов*, чем принципиально отличается от сети с коммутацией каналов.

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

Протокол Internet (IP)

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

Различные части Internet 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 Internet узлы выясняют, куда следует пакет данных, решают, куда его дальше отправить и отправляют. Такой процесс называется *маршрутизацией*.

Для осуществления маршрутизации составляются таблицы маршрутизации. В Internet составление и модификация таблиц мар-

шрутизации определяются соответствующими протоколами: ICMP (*Internet Control Message Protocol*), RIP (*Routing Internet Protocol*) и OSPF (*Open Shortest Path First*). Узлы, занимающиеся маршрутизацией, называются *маршрутизаторами.*

В Internet имеется набор правил по обращению с пакетами. Протокол Internet (IP) берет на себя заботы по адресации и подтверждению того, что узлы понимают, что следует делать с данными по пути их следования. Суть работы протокола IP аналогична правилам обработки почтового конверта. В начало каждого пакета помещается заголовок, несущий информацию об адресате сети. Этой информации достаточно, чтобы определить, куда и как доставить пакет данных.

Адрес в Internet 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 Internet имеет в этой схеме уникальный адрес, аналогично обычному почтовому индексу. Существует несколько типов адресов Internet, 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.

Пересылаемая по сетям IP информация делится на части, раскладываемые в отдельные пакеты. Длина информации внутри одного пакета 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 Internet. Данные, помещенные в оболочку IP, содержат всю необходимую информацию для передачи их с компьютера пользователя получателю. Однако при пересылке информации с использованием протокола IP возникает ряд проблем, которые необходимо решать:

- большинство сообщений содержит более 1500 символов, т.е. превышает допустимый размер одного пакета;
- пакеты в сообщении могут следовать в последовательности, отличной от их исходного порядка;
- возможны ошибки в передаче пакетов.

Следующие уровни сети Internet 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*.

Приложения Internet — 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* Internet: 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.

Службы Internet

Рассмотрим самые популярные службы Internet. Эти приложения поддерживаются стандартом. Статистические данные показывают частоту использования того или иного протокола Internet, т.е. в некотором смысле, его популярность.

Удаленный доступ (telnet). *Удаленный доступ* — 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.

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 Internet класса не ниже dial-up.

Электронная почта (E-mail). Электронная почта — одна из самых популярных на сегодняшний день Internet-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 Internet.

E-mail (*Electronic mail*) — электронный аналог обычной почты. С ее помощью можно посылать сообщения, получать их в свой элек-

тронный 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. Можете посылать почту через шлюзы в сопредельные сети.

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.

Поиск данных и программ (Archie). Эта служба регулярно собирает с анонимных ftp-серверов информацию о содержащихся там файлах. Она позволяет производить поиск по названиям файлов и директорий и по описательным файлам, а именно по словам, там содержащимся. Искать можно по имени, по шаблону, по смысловым словам, которые могут содержаться в описании файла или программы.

Доступ к Archie осуществляется через особые Archie-серверы. Использование службы Archie требует наличие Internet-доступа класса dial-up. Help также доступен по электронной почте.

Служба Gopher. Служба Gopher интегрирует практически все возможности Internet. Она позволяет в удобной форме пользоваться всеми услугами, предоставляемыми сетью. Организована оболочка в виде множества вложенных на разную глубину меню, так что остается только выбрать нужный пункт и нажать ввод. В такой форме имеется доступ к сеансам telnet, ftp, E-mail и т.д.

Gopher-серверы получили широкое распространение. Их трафик составляет около 2% от общего трафика в сети. С одного сервера можно войти в другие.

Gopher должен быть установлен непосредственно на рабочем компьютере пользователя и он сугубо интерактивен, при этом доступ в Internet должен быть не хуже доступа по вызову.

Всемирная паутина World Wide Web (WWW). Гипертекст представляет собой текст со вставленными в него командами разметки, организующими ссылки на связанные места данного текста, других документов, рисунки, файлы и т.д. При просмотре гипертекста в *программе-броузере*, 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 по ссылкам можно попасть в текст другого документа, выполнить какое-нибудь действие или программу и т.д. Ссылаться можно на данные на других машинах в любом месте сети, тогда при активации этой ссылки эти данные автоматически передадутся на исходную машину и вы увидите на экране текст, данные, картинку, а если провести в жизнь идею мультимедиа, то услышите и звук, музыку, речь. В рамках службы WWW можно получать доступ ко всем другим службам: telnet, E-mail, ftp, Gopher, Archie, Usenet и т.п.

По возможностям WWW напоминает Gopher, однако это принципиально другая служба. В Gopher имеется жесткая структура меню. В WWW документ может иметь гипертекстовую структуру любой степени сложности. Пользователь может сам организовать структуры типа меню в гипертексте.

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.

Работать с WWW имеет смысл лишь на быстрых линиях. Использование WWW на медленных линиях — слишком дорогое удовольствие. К тому же WWW требует доступа в сеть в режиме on-line.

Поисковые системы. Для облегчения поиска необходимой информации в сети Internet созданы специальные средства поиска. Их

можно разделить на две основные группы: *каталоги* и *полнотекстовые системы*. Каталоги устроены по принципу библиографических справочных систем. В них каждая книга или статья находится на определенном месте в предметном или авторском указателе. В сетевом каталоге ссылки рассортированы по тематическим рубрикам и сопровождаются аннотациями. Сетевой каталог, в отличие от библиотечного, позволяет значительно ускорить работу: на его главной странице есть окно для поиска. После введения ключевого слова вы сразу получаете список рубрик и ссылок, в которых они встретились.

Самый популярный и старейший из каталогов Internet, содержащий ссылки более чем на полмиллиона web-страниц, «Yahoo!» Наиболее полные и популярные российские каталоги — www.list.ru, www.au.ru, www.ru, www.stars.ru. Они содержат ссылки на 20—30 тысяч сайтов и ежедневно пополняются на несколько десятков — сотен ссылок. На сервере поисковой системы «Rambler» размещен каталог (или рейтинг-классификатор) «Rambler's "Top 100"» (http://counter.rambler.ru/top100). Участвующие в нем сайты разбиты на 56 рубрик от «Авто и Мото» до «Юмор». В число этих рубрик входят такие популярные, как «Банки», «Искусство», «История», «Кино», «Компьютеры», «Медицина», «Музыка», «Образование», «Отдых», «Политика», «Природа», «Путешествия», «Работа», «Радио», «Развлечения», «Реклама», «Спорт», «Театр», «Телевидение», «Техника», «Транспорт», «Электроника».

В отличие от каталогов, хранящих только аннотации, поисковые системы Internet хранят весь текст web-страниц. Такой объем информации обрабатывается автоматически. Для этого поисковые машины ежедневно посещают web-страницы Сети и заносят их в свои базы. Человек может только инициировать процесс: как и в случае с каталогами, автор страницы должен послать поисковой системе заявку на свой новый материал. Если заявку не подать, поисковая система сама доберется до новой страницы, используя ведущую к ней ссылку. Но это произойдет нескоро. Поэтому после создания в Сети своей страницы рекомендуется «прописаться» в основных поисковых системах.

Старейшая из российских полнотекстовых поисковых систем — это «Rambler» (http://www.rambler.ru). Она начала работу в 1996 г. и располагает наиболее полным индексом. В первую тройку российских поисковых систем входят также «Яndex» (http://yandex.ru) и «Апорт» (http://www.aport.ru). В 2004 г. наиболее совершенной системой стала Google.ru, в которой собрано более 6 млрд документов с высокой степенью релевантности.

Релевантность при поиске в Internet — это соответствие ответа вопросу, имеющее две составляющих — *полноту* (при которой ничего не потеряно) и *точность* (при которой не найдено ничего лишнего).

В поисковую систему «Яndex» входят такие рубрики: «Культура и искусство», «Общество и политика», «Развлечения и отдых», «СМИ», «Дом и семья», «Наука и образование», «Экономика и финансы», «Компьютеры и Интернет», «Промышленность», «Работа и офис», «Товары и услуги», «Справочники», «Регионы».

Из поисковых систем глобального масштаба можно рекомендовать AltaVista (http://www.altavista.com), которая способна искать и русскоязычные документы, а также Lycos (http://www.lycos.com), Excite (http://www.excite.com), HotBot (http://www.hotbot.com).

Прежде чем поисковая система приступит к работе, надо ввести искомое слово или понятие в окошке поиска, а затем нажать мышью иконку «Найти».

Для того чтобы найти толкование какого-либо конкретного слова или понятия, используются онлайновые энциклопедии. Одной из крупнейших онлайновых энциклопедий является ресурс «Яндекс. Энциклопедии» (http://encycl.yandex.ru/) — этот проект содержит более 200 тыс. статей из 14 энциклопедий, в том числе из БСЭ и Энциклопедии Брокгауза и Ефрона. К крупным относится и Энциклопедия Кирилла и Мефодия, которую можно найти по адресу http://www.km.ru/.

Число пользователей сети Internet стремительно возрастает с каждым годом. Предполагается, что в 2005 г. оно возрастет до 1 млрд человек (15% населения Земли).

6.8. Информационно-вычислительная сеть ОВД

Защита прав и свобод граждан России, включая право на личную неприкосновенность и безопасность, право собственности, эффективное реагирование на изменения в криминогенной обстановке, борьбу с наиболее опасными видами преступлений и улучшение правопорядка в стране, невозможна без создания стройной системы информационного обеспечения органов внутренних дел от уровня горрайлиноргана до федерального уровня.

В решении этой глобальной задачи можно выделить ряд ключевых п р о б л е м:

1. *Обеспечение информационного обслуживания* (по запросам и в инициативном порядке) *органов внутренних дел России*, оперативных служб других заинтересованных ведомств в вопросах оперативно-справочной, розыскной и криминалистической информации.

2. *Обеспечение полноты и достоверности статистической информации* на основе укрепления учетно-регистрационной дисциплины.

По оценкам специалистов, на уровне горрайлинорганов в дежурных частях, у оперработников, следователей, сотрудников других под-

разделений, на документах первичного учета, в учетных журналах и других носителях накапливается до 70% всей информации, циркулирующей в органах внутренних дел, которая формирует банк оперативно-справочной и оперативно-розыскной информации. Структура и порядок формирования оперативно-справочных, розыскных и криминалистических учетов органов внутренних дел России определены Приказом МВД России от 31.08.1994 г. № 400 «О формировании и ведении централизованных оперативно-справочных, розыскных, криминалистических учетов, экспертно-криминалистических коллекций и картотек органов внутренних дел Российской Федерации», положениями которого должны руководствоваться сотрудники информационной службы в своей работе.

В соответствии с нормативными документами МВД России, на информационных работников штабов горрайлинорганов возлагается организация учетно-регистрационной и статистической работы и контроля за своевременностью регистрации заявлений, сообщений и иной информации о преступлениях.

Качественное и эффективное решение двух первых задач на современном этапе невозможно без применения новейших информационных технологий, без создания *интегрированных банков данных* разного уровня (*локального* — горрайлинорганы, *регионального* — МВД, ГУВД, УВД, УВДТ, *федерального* — МВД России) для оперативно-розыскных и криминалистических учетов, объединения их в *единое информационное пространство*, что предоставит быстрый и удобный доступ к информации с рабочих мест сотрудников ОВД в любое время суток в режиме реального времени.

Диапазон применения компьютерных технологий в области информационного обеспечения ОВД достаточно широк — от обработки статистики правонарушений до межмашинного обмена информацией оперативно-розыскного, справочного и криминалистического назначения в рамках территориальной информационно-вычислительной сети *локального* (горрайлинорганы), *регионального* (зонального) и *федерального* уровней.

Таким образом, формирование единой информационно-вычислительной сети органов внутренних дел с обеспечением прямого доступа пользователей (в первую очередь уровня горрайлинорганов) к информационным массивам интегрированных банков данных в режиме реального времени является третьим приоритетным направлением деятельности информационных подразделений в системе МВД.

Планируется объединение на логическом уровне региональных банков данных нескольких МВД, УВД близлежащих областей, находящихся в зоне экономического района. Такие зональные центры

(в пределах 10 на территории Российской Федерации) будут обеспечивать требуемый уровень интеграции информационных ресурсов и способствовать реальному формированию единого информационного пространства подразделений ОВД.

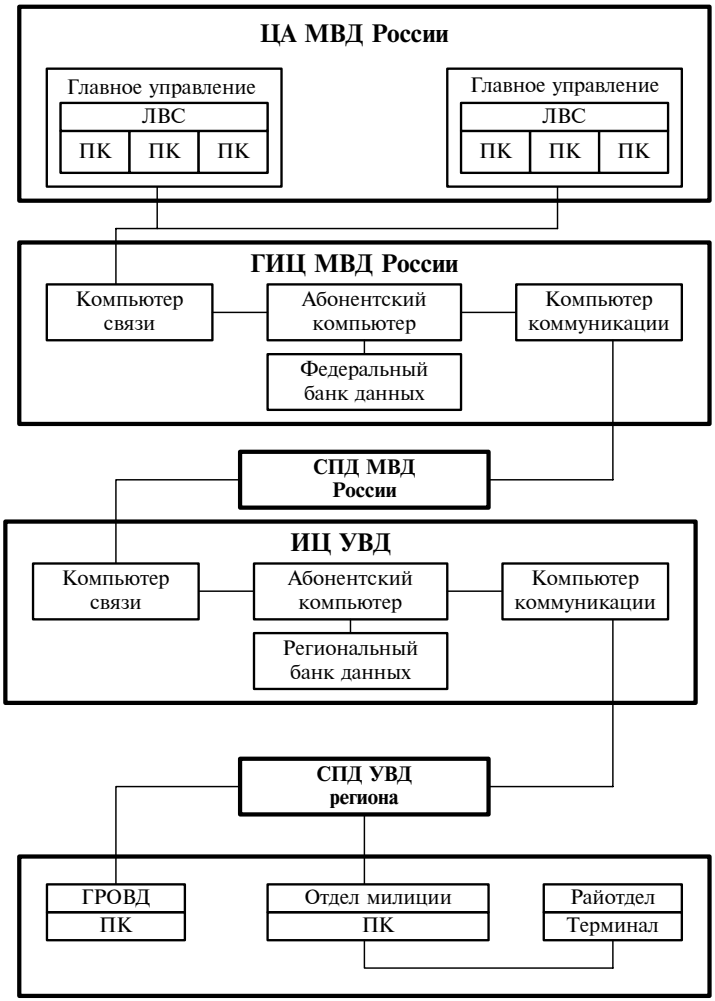


Рис. 6.4. **Структура информационного обеспечения МВД России**

Нормативной базой для проведения крупномасштабных работ по компьютеризации ОВД является «Концепция развития системы

информационного обеспечения ОВД в борьбе с преступностью», утвержденная Приказом МВД России от 12 мая 1993 г., на основе которой разработаны основные принципы создания ИВС, предложены типовые архитектурные и программно-технические решения, разрабатываются комплексы прикладных программных средств.

В целом концепция и техническое задание на создание ИВС ориентированы на несколько уровней сбора, обработки и накопления информации. На уровне горрайлинорганов рабочими местами являются персональные компьютеры IBM PC/386, объединенные, если это необходимо, в локальную вычислительную сеть.

На более высоком уровне основой системы являются такие компьютеры, как IBM 486 и MX-300, MX-500 фирмы «Сименс-Никсдорф» с большими объемами жестких дисков и оперативной памяти и высокой скоростью обработки данных. Эти компьютеры работают под управлением многопользовательской операционной системы UNIX и используют систему управления базами данных Oracle.

Основным достоинством ОС UNIX является возможность системными средствами решать проблему одновременной работы многих пользователей с разграничением их доступа к системным ресурсам и данным, независимо от способа подключения этих пользователей.

Все это послужит основой формирования региональных информационных сетей ОВД, объединяемых затем в единую информационно-вычислительную сеть МВД Российской Федерации, которая в техническом плане представляет собой совокупность связанных каналами и линиями связи информационно-вычислительных центров (районов, крупных городов, республик, краев и областей, экономических зон России в целом) с подключенными к ним терминалами в горрайлинорганах и службах МВД, УВД.

Сейчас в органах внутренних дел России накоплен значительный массив оперативно-розыскной и справочной информации, необходимой работникам правоохранительных органов для проведения оперативно-следственных и розыскных мероприятий, а также для решения других служебных задач. Только в автоматизированных базах данных, а также ручных картотеках ГИЦ и ИЦ МВД — УВД сосредоточено более 76 млн объектов. В целом, по экспертным оценкам, в ОВД ежегодно создается более 350 млн документов, из них примерно 10% — фактографические. В настоящее время постоянный информационный обмен ведется на трех уровнях:

- МВД России (ГИЦ) — информационный фонд — 45 млн документов;
- МВД, ГУВД, УВД — информационные центры — 77 млн документов;
- горрайлинорганы и учреждения — 250–300 млн документов.

Задачи информационных подразделений госавтоинспекции в этом направлении определены Приказами МВД России от 12 мая 1993 г. № 229 «Концепция развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью» и № 420-93 г.:

- внедрение перспективных информационных технологий, средств вычислительной техники и телекоммуникаций, локальных вычислительных сетей, типовых программных средств и автоматизированных рабочих мест для обобщения и анализа информации, информационной поддержки оперативно-служебной деятельности госавтоинспекции внутренних дел;
- обеспечение единообразия и совместимости средств вычислительной техники и телекоммуникаций, работоспособности общесистемных и прикладных программных средств, их адаптации с учетом специфики эксплуатируемых автоматизируемых систем обработки информации;
- изучение передового опыта в области компьютеризации, а также совершенствование технологии обработки информации.

Создание интегрированной вычислительной сети органов внутренних дел позволит обеспечить информационное взаимодействие различных подразделений оперативных служб, дежурных частей УВД, дежурных частей служб следствия и дознания, паспортной службы, ГАИ, разрешительной службы, городских и линейных органов внутренних дел с центральным банком данных (в масштабах города, области, региона, страны), содержащим информацию всех служб абонентов сети. Кроме того, абонентами сети могут выступать службы прокуратуры, суда, ФСК, налоговые и таможенные службы. Все абоненты сети являются одновременно и потребителями, и поставщиками информации в интегрированные банки данных.

Главное достижение — не в объеме информации, а в оперативности ее получения: там, где сейчас требуются часы, а нередко и дни, с созданием ИВС — потребуются минуты.

Кроме того, совместное функционирование в рамках ИВС интегрированных банков данных общего пользования даст возможность обеспечить единство информационной поддержки основных стадий уголовно-процессуальной деятельности.

Концентрация в рамках ИВС сигнальной, ориентирующей, розыскной и доказательственной информации, обеспечение логической взаимосвязи ее компонентов позволит, кроме того, повысить информированность каждого оперативного работника, создаст условия для более эффективного использования накопленной информации в процессе расследования, раскрытия и профилактики преступлений.

Создание интегрированной вычислительной сети также позволит информационной службе перейти от традиционных ныне видов

статистической и оперативно-справочной работы по поддержке в раскрытии и расследовании преступлений к ориентированию правоохранительных органов на розыск преступников; проведению сравнительной (предварительной) идентификации способов совершения преступлений, следов и вещественных доказательств, описаний лиц и примет похищенного имущества; выявлению в инициативном порядке криминогенных структур (связей, групп, соотношений событий и т.д.); оказанию действенной помощи в анализе и прогнозировании оперативной обстановки.

Контрольные вопросы и задания

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 Internet.
11. Как формируется универсальный адрес сетевого ресурса в Internet?
12. Назовите основные службы сети Internet.
13. Что представляет собой гипертекстовая структура?
14. Каковы основные достоинства и недостатки технологий доступа к информации в сети Internet.
15. Назовите основные цели и задачи создания информационно-вычислительной сети органов внутренних дел.

Часть III

ОСНОВЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ, ВЕРОЯТНОСТЬ, АНАЛИЗ ДАННЫХ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ПРАВОПРИМЕНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Глава 7

ОСНОВЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ. МНОЖЕСТВА И ПОДМНОЖЕСТВА

Математическая логика — современный вид формальной логики, изучающей правила выведения следствий из различных посылок, истинность которых очевидна. Математическая логика возникла в середине XIX в. для потребностей математики и стала применяться в самых различных областях знаний, в том числе и в правоприменительной деятельности.

Основным понятием математической логики является понятие *высказывания* (высказывания будем обозначать латинскими буквами: *a, b, c, ...*). Любое высказывание быть одновременно и истинным и ложным не может. Какой из этих случаев имеет место? При ответе на этот вопрос надо учитывать тот факт, что одно и то же высказывание может быть истинным в одних условиях и ложным в других. Например, *значение истинности* (т.е. истинность или ложность) высказывания «норма жилой площади устанавливается в размере 18 кв. м на одного человека» определяется принятым Жилищным кодексом.

7.1. Связки и таблицы истинности

Различают *простые* и *составные высказывания*. Высказывание «наследники умершей — ее муж и сын» — составное, в то время как высказывания «наследник умершей — ее муж» и «наследник умершей — ее сын» — простые. Связывание простых высказываний в составные осуществляется логическими операциями, называемыми *связками*.

Рассмотрим следующие с в я з к и: конъюнкцию, дизъюнкцию, отрицание, импликацию и двойную импликацию. Обозначим символами *a* и *b* два какие-либо высказывания.

➢ ***Конъюнкцией*** высказываний *a* и *b* называется высказывание $a \wedge b$ (*«a* и *b»*) истинное, если истинно каждое из высказываний *a* и *b*, в противном случае $a \wedge b$ ложно. Высказывание «юрист должен знать информатику и математику» является конъюнкцией высказываний: *a* = «юрист должен знать информатику» и *b* = «юрист должен знать математику».

Зависимость значения истинности составного высказывания от значений истинности его компонентов представляется *таблицей истинности.*

Таблица истинности высказывания $a \wedge b$ изображена на рис. 7.1.

a	b	$a \wedge b$
и	и	и
и	л	л
л	и	л
л	л	л

Рис. 7.1

➢ ***Дизъюнкцией*** высказываний a и b называется высказывание $a \vee b$ («a или b», иначе «a либо b») истинное, когда одно из высказываний истинно, а другое ложно, и ложное, когда оба высказывания ложны (рис. 7.2,*а*). Неоднозначность первой строки рис. 7.2,*а* объясняется тем, что обиходное употребление связки «или» двусмысленно: если «или» понимать в смысле «одно или другое, или оба», то при истинности обоих высказываний a и b будет истинно высказывание $a \vee b$; если же «или» понимать в смысле «одно или другое, но не оба», то одновременная истинность a и b невозможна, т.е. при истинности a и b высказывание $a \vee b$ будет ложно. Например, в высказывании «договор может быть заключен в устной или письменной форме» допускается возможность заключения договора не только в какой-то одной форме, но и в обоих. А в высказывании «5 марта я поеду на шахматный турнир в Москву или во Владивосток» исключено посещение обоих турниров одновременно. В математической логике для устранения двусмысленности связки «или» введены термины:

- *дизъюнкция в неисключающем смысле* — это дизъюнкция $a \vee b$, истинная при истинности не только одного из высказываний a или b, но и обоих (иначе, при истинности не менее одного из двух высказываний; иначе, при истинности по крайней мере одного из двух высказываний; иначе, при истинности хотя бы одного из двух высказываний); ее таблица истинности приведена на рис. 7.2,*б*;
- *дизъюнкция в исключающем смысле* (обозначим ее $a \underline{\vee} b$) — это дизъюнкция истинная при истинности только одного из высказываний a или b, но не обоих; ее таблица истинности изображена на рис. 7.2,*в*.

➢ ***Отрицанием*** высказывания a называют высказывание $\sim a$ («не a» или «неверно, что a»), отрицающее a.

a	b	$a \vee b$
и	и	и(л)?
и	л	и
л	и	и
л	л	л

а

a	b	$a \vee b$
и	и	и
и	л	и
л	и	и
л	л	л

б

a	b	$a \underline{\vee} b$
и	и	л
и	л	и
л	и	и
л	л	л

в

Рис. 7.2

Таблица истинности высказывания $\sim a$ изображена на рис. 7.3.

a	$\sim a$
и	л
л	и

Рис. 7.3

➢ ***Импликацией*** высказываний a и b называется высказывание $a \to b$ («если a, то b») ложное, когда a истинно, но b ложно, а в остальных случаях — истинное.

Таблица истинности высказывания $a \to b$ изображена на рис. 7.4. Ее первые две строки: «если как a, так и b истинны, то $a \to b$ истинно», «если a истинно, а b ложно, то $a \to b$ ложно» очевидны. При a ложном значение истинности высказывания $a \to b$, вообще говоря, неопределенно, но поскольку каждое высказывание должно быть либо истинным, либо ложным, считается, что при a ложном высказывание $a \to b$ истинно (см. рис. 7.4, 3-я и 4-я строки); основанием для принятия такого решения может служить как бы оправдание при a ложном импликации $a \to b$ «за недостаточностью улик»[1].

В юридических текстах в форме импликаций формулируют правовые предписания, разрешения и т.д.; например: «Если договор поднайма заключен без указания срока, наниматель обязан предупредить поднанимателя о прекращении договора поднайма за три месяца». Отметим, что импликация $a \to b$ при отсутствии смысловой связки между a и b звучит странно. Так, странно звучат импликации: «если $2 \times 2 = 4$, то $3 + 2 = 6$» и «если $3 + 2 = 6$, то $2 \times 2 = 4$», первая из которых ложна (см. рис. 7.4, 2-я строка), а вторая — истинна (см. рис. 7.4, 3-я строка). Но связка «если a, то b» не означает никакой причинно-следственной связи, не означает, что из a следует b (отношение следования рассматривается ниже): просто $a \to b$ —

[1] *Кемени Дж., Снелл Дж.* Введение в конечную математику. — М.: Мир, 1965.

это новое высказывание, образованное из *a* и *b*. Поэтому рассмотренные парадоксальные импликации имеют право на существование.

➢ ***Двойной импликацией*** высказываний *a* и *b* называется высказывание $a \leftrightarrow b$ (*«b*, если и только если *a*»); не путать с одинарной импликацией $a \rightarrow b$ («если *a,* то *b*»). Высказывание *«b,* если и только если *a»* означает истинность двух высказываний: «если *a* истинно, то и *b* истинно» и «если *a* ложно, то и *b* ложно». Поэтому двойная импликация $a \leftrightarrow b$ истинна только в этих случаях и ложна в остальных (см. рис. 7.5).

a	*b*	$a \rightarrow b$
и	и	и
и	л	л
л	и	и
л	л	и

Рис. 7.4

a	*b*	$a \leftrightarrow b$
и	и	и
и	л	л
л	и	л
л	л	и

Рис. 7.5

Форму двойной импликации имеет, например, высказывание «*совершивший уголовное преступление подлежит уголовному наказанию*» (=*b*), если и только если *возраст совершившего уголовное преступление не меньше 14 лет* (=*a*). Очевидно, что истинны высказывания: «если *возраст... не меньше 14 лет*, то... *подлежит... наказанию*» (рис. 7.5, 1-я строка) и «если *возраст... меньше 14 лет*, то *не подлежит... наказанию*» (рис. 7.5, 4-я строка), и ложны высказывания: «если *возраст... не меньше 14 лет*, то... *не подлежит... наказанию*» (рис. 7.5, 2-я строка) и «если *возраст... меньше 14 лет*, то... *подлежит... наказанию*» (рис. 7.5, 3-я строка).

Покажем, как строятся таблицы истинности составных высказываний. Последовательность построения таблицы для высказывания $(a \rightarrow b) \leftrightarrow (\neg a \vee b)$, компонентами которого являются простые высказывания *a* и *b,* приведена на рис. 7.6.

a	*b*	$a \rightarrow b$	$\neg a$	$\neg a \vee b$	$a \rightarrow b$	$\neg a \vee b$	$(a \rightarrow b) \leftrightarrow (\neg a \vee b)$
и	и	и	л	и	и	и	и
и	л	л	л	л	л	л	и
л	и	и	и	и	и	и	и
л	л	и	и	и	и	и	и

Рис. 7.6

Замечание.

Высказывания, в которых присутствуют скобки, следует читать подобно алгебраическим выражениям. В данном случае сначала выполня-

ется связка $a \to b$, стоящая в первой скобке, затем $\sim a$, затем связка $\sim a \vee b$ и наконец связка «$\leftrightarrow$».

Следовательно, при любой комбинации значений истинности высказываний a и b (см. рис. 7.6, первые два столбца) высказывание $(a \to b) \leftrightarrow (\sim a \vee b)$ всегда истинно.

Последовательность построения таблицы истинности высказывания $\sim((\sim a \wedge \sim b) \wedge (a \vee c))$, состоящего из трех простых высказываний a, b, c, приведена на рис. 7.7.

a	b	c	$\sim a$	$\sim b$	$\sim a \wedge \sim b$	$a \vee c$	$(\sim a \wedge \sim b) \wedge (a \vee c)$	$\sim((\sim a \wedge \sim b) \wedge (a \vee c))$
и	и	и	л	л	л	и	л	и
и	и	л	л	л	л	и	л	и
и	л	и	л	и	л	и	л	и
л	и	и	и	л	л	и	л	и
и	л	л	л	и	л	и	л	и
л	и	л	и	л	л	л	л	и
л	л	и	и	и	и	и	и	л
л	л	л	и	и	и	л	л	и

Рис. 7.7

Следовательно, высказывание $\sim((\sim a \wedge \sim b) \wedge (a \vee c))$ ложно, только когда a и b ложны, но c истинно; а в остальных случаях оно истинно.

Обратим внимание на то, что таблица истинности высказывания, состоящего из двух простых: a и b, содержала $2^2 = 4$ строки — столько различных комбинаций значений истинности двух простых высказываний; для высказывания, состоящего из трех простых: a, b, c, таблица содержала $2^3 = 8$ строк — столько различных комбинаций значений истинности трех высказываний. Для высказывания, состоящего из четырех простых, таблица истинности будет содержать $2^4 = 16$ строк и т.д.

Формально-логический анализ правовых норм позволяет в ряде случаев обнаружить неясности, двусмысленности в их применении. Например, по формулировке *«умышленное причинение телесного повреждения* ($=a$) или *нанесение побоев* ($=b$), повлекшее за собой *кратковременное расстройство здоровья* ($=c$) или *незначительную стойкую утрату трудоспособности* ($=d$), наказывается *лишением свободы на срок до одного года* ($=e$) или *исправительными работами на этот же срок* ($=f$)*»* возникают следующие вопросы:

- союзы *«или»* между a и b, между c и d, между e и f — это дизъюнкции в неисключающем смысле или в исключающем? Если, например, союз «*или*» между e и f — это дизъюнкция с

неисключением, т.е. $e \vee f$, то перечисленные в статье преступные действия могут быть наказаны и лишением свободы и исправительными работами; если же это дизъюнкция с исключением, т.е. $e \underline{\vee} f$, то используется только какой-то один вид наказания;

- слово *«повлекшее»* стоит после высказывания b и по правилам согласования должно относиться только к b; по содержанию же статьи это слово относится к обоим перечисленным преступным действиям и, следовательно, надо писать «повлекшие...»; но, с другой стороны, если часть статьи, расположенную перед словом *«повлекшее»*, заключить в скобки, т.е. рассматривать как одно высказывание $a \vee b$ (или $a \underline{\vee} b$), то неясности не было бы.

Условимся, что в рассматриваемой статье первые два «или» — это дизъюнкция с неисключением, а последнее «или» — с исключением и что часть статьи перед словом «повлекшее» заключена в скобки. Тогда логическая формула статьи будет такой: $((a \vee b) \wedge (c \vee d)) \rightarrow (e \underline{\vee} f)$; формула содержит 6 компонентов, ее таблица истинности будет содержать $2^6 = 64$ строки.

Анализ приведенной статьи убеждает в необходимости использования символического языка математической логики для уяснения смысла правовых контекстов, для построения норм права, не допускающих двусмысленных толкований.

7.2. Логические возможности. Логически истинные и логически ложные высказывания

Выше отмечалось, что число строк в таблице истинности высказывания, состоящего из n простых высказываний, равно 2^n — именно столько существует различных комбинаций значений истинности n простых высказываний. Однако в конкретных ситуациях появление некоторых из этих комбинаций невозможно в принципе, и поэтому число строк таблицы истинности «можно уменьшить».

Свяжем каждое высказывание с определенными *логическими возможностями* и условимся никакое предложение не рассматривать как высказывание до тех пор, пока не определено множество связанных с ним логических возможностей. Если же речь идет одновременно о нескольких высказываниях (а именно так обстоит дело при изучении составных высказываний), потребуем, чтобы каждое из них было связано с одним и тем же множеством логических воз-

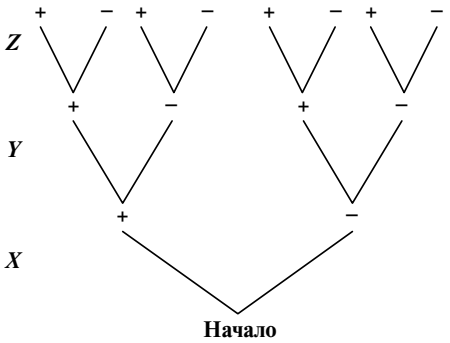
можностей. Понятие *множества логических возможностей* поясним на следующем примере.

Пример 7.1.

Жюри из трех человек *X, Y, Z* принимает решение большинством голосов, при этом есть только два варианта голосования для каждого члена жюри: «за» (+) и «против» (−). Возникающие при голосовании логические возможности представлены на рис. 7.8,*а*, а так называемое дерево логических возможностей — на рис. 7.8,*б*.

№ возможности	*X*	*Y*	*Z*
1	+	+	+
2	+	+	−
3	+	−	+
4	+	−	−
5	−	+	+
6	−	+	−
7	−	−	+
8	−	−	−

а



б

Рис. 7.8

Обратим внимание на то, что таблица истинности высказывания: «*X проголосует* “*за*” (=*a*) или *Y проголосует* “*за*” (=*b*), или *Z проголосует* “*за*” (=*c*)», т.е. высказывания $a \vee b \vee c$, (рис. 7.9) содержит столько же строк, сколько и таблица логических возможностей (рис. 7.8,*а*). Это объясняется тем, что все комбинации значений истинности высказываний *a, b, c* логически возможны.

К множеству логических возможностей предъявляются два требования:

- в любых условиях должна осуществляться одна и только одна из возможностей множества;
- в рамках этого множества должно определяться значение истинности любого высказывания по изучаемой проблеме.

Логические возможности в примере 7.1 (рис. 7.8) первому требованию удовлетворяют; они удовлетворяют и второму: ведь все логические возможности — это все мыслимые комбинации значений истинности высказываний *a, b, c*.

a	*b*	*c*	$a \vee b$	$a \vee b \vee c$	*№ возможности (см. рис. 7.8,а)*
и	и	и	и	и	1
и	и	л	и	и	2
и	л	и	и	и	3
л	и	и	и	и	5
и	л	л	и	и	4
л	и	л	и	и	6
л	л	и	л	и	7
л	л	л	л	л	8

Рис. 7.9

Логически истинным называют высказывание, истинное при каждой логической возможности. ***Логически ложным*** называют высказывание, ложное при каждой логической возможности.

В условиях примера 7.1 высказывания:

- «жюри примет какое-то решение» — логически истинное;
- «жюри не примет никакого решения» — логически ложное;
- «по крайней мере два члена жюри проголосуют “за” $(=(a \wedge b \wedge \sim c) \underline{\vee} \underline{\vee} (a \wedge \sim b \wedge c) \underline{\vee} (\sim a \wedge b \wedge c) \underline{\vee} (a \wedge b \wedge c))$» — истинно в возможностях № 2, 3, 5, 1 (рис. 7.8,*а*);
- «только два члена жюри проголосуют “за” $(=(a \wedge b \wedge \sim c) \underline{\vee} (a \wedge \sim b \wedge c) \underline{\vee} \underline{\vee} (\sim a \wedge b \wedge c))$» — истинно в возможностях № 2, 3, 5.

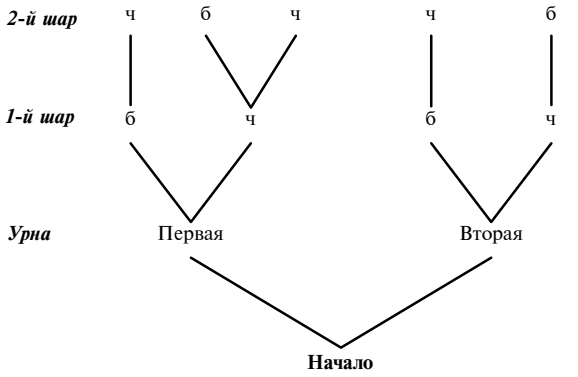
Для ряда проблем можно построить не одно, а несколько множеств логических возможностей. Поэтому ответ на вопрос «для скольких возможностей то или иное высказывание истинно?» зависит от рассматриваемого множества логических возможностей. Однако логически истинные (логически ложные) высказывания являются в этом отношении исключениями: они истинны (ложны) на любом множестве логических возможностей, относящемся к изучаемой проблеме.

Пример 7.2.

Имеются две урны, первая из которых содержит один белый и два черных шара с номерами 1 и 2, а вторая — белый и черный; из наудачу взятой урны вынимают последовательно два шара (к такой урновой модели сводится, например, следующая ситуация: известно, что в городе действуют две преступные группировки, в первой — одна женщина и двое мужчин, во второй — женщина и мужчина; двумя лицами, принадлежащими к какой-то одной группе, совершена кража). Множество логических возможностей и их дерево для случая, когда нас интересует только цвет вынутых шаров (пол преступников), изображены на рис. 7.10 (белый шар — «б», черный — «ч»), а для случая, когда нас интересует не только цвет (пол), но и номера вынутых шаров (фамилии мужчин из первой группировки), — изображены на рис. 7.11 (черный шар с номером 1 — «ч1»).

№ возможности	*Урна*	*1-й шар*	*2-й шар*
1	1	б	ч
2	1	ч	б
3	1	ч	ч
4	2	б	ч
5	2	ч	б

а



б

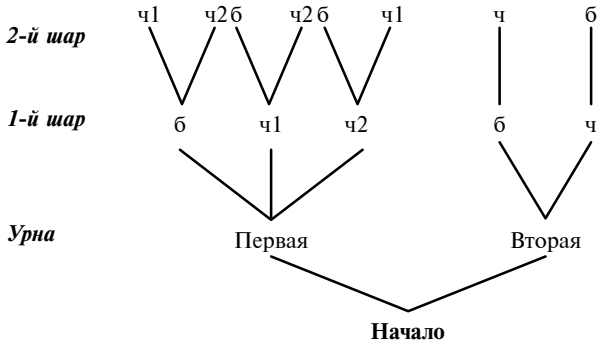
Рис. 7.10

Первое множество логических возможностей (см. рис. 7.10) «более грубое», чем второе (см. рис. 7.11): оно оказывается достаточным для определения значения истинности высказываний, в которых акцент сделан только на цвет, и недостаточным для высказываний, в которых фигурируют и цвет и номер шара; в рамках же второго,

более детального множества определяются значения истинности высказываний как первого, так и второго типа. Высказывание «выбрана 1-я урна и из нее вынуты белый и черный шары» истинно на первом множестве — в возможностях № 1, 2, а на втором — в возможностях № 1, 2, 3, 5. Высказывание «выбрана 1-я урна и из нее первым вынут белый шар, а вторым — черный» истинно на первом множестве только в возможности № 1, а на втором — в возможностях № 1, 2. Случаи же истинности высказывания «выбрана первая урна и из нее вынут белый шар и черный с номером 1» могут быть установлены только на втором множестве — это случаи № 1, 3.

№ возможности	*Урна*	*1-й шар*	*2-й шар*
1	1	б	ч1
2	1	б	ч2
3	1	ч1	б
4	1	ч1	ч2
5	1	ч2	б
6	1	ч2	ч1
7	2	б	ч
8	2	ч	б

а



б

Рис. 7.11

Обратим еще раз внимание на то, что число логических возможностей всегда не больше числа строк таблицы истинности любого высказывания по рассматриваемой проблеме. Так, если нас интересует только цвет вынутых шаров и простые высказывания таковы: a = «выбрана первая урна», b = «первым извлечен белый

шар», c = «вторым извлечен черный шар», то таблица истинности любого высказывания, состоящего из этих трех простых, будет иметь $2^3 = 8$ строк, тогда как логических возможностей — пять (см. рис. 7.10,*а*). Также обратим внимание на то, что высказывание, являющееся логически истинным, может иметь различные значения истинности в таблице истинности. В подтверждение составим таблицу истинности высказывания $a \rightarrow (\sim b \vee c)$, где a, b, c определены выше, и сопоставим ее с таблицей логических возможностей (см. рис. 7.10,*а*).

Таблица истинности приведена на рис. 7.12, в ней выделены строки, появление которых логически невозможно.

a	b	c	*№ возможности (см. рис. 7.10,а)*	$\sim b$	$\sim b \vee c$	$a \rightarrow (\sim b \vee c)$
и	и	и	1	л	и	и
и	и	л		л	л	л
и	л	и	3	и	и	и
л	и	и	4	л	и	и
и	л	л	2	и	и	и
л	и	л		л	л	и
л	л	и		и	и	и
л	л	л	5	и	и	и

Рис. 7.12

Следовательно, при любой логической возможности импликация $a \rightarrow (\sim b \vee c)$ истинна, т.е. это логически истинное высказывание. Словесная формулировка импликации такая: «если будет выбрана первая урна, то хотя бы один из двух вынутых шаров — черный»; в ее логической истинности нетрудно убедиться, взглянув на ответвления дерева логических возможностей, выходящие из корня «Первая» (см. рис. 7.10,*б*). Однако в рамках всей таблицы истинности высказывание $a \rightarrow (\sim b \vee c)$ не всегда истинно (см. первую выделенную строку на рис. 7.12).

7.3. Отношения следования, эквивалентности и несовместимости

Выше рассматривались отдельные высказывания (простые или составные). Но часто бывает нужно исходя из анализа множества логических возможностей, связанного с двумя высказываниями c и d, установить логические отношения между ними. Рассмотрим отношения следования, эквивалентности и несовместимости (совместимости).

Из высказывания *с логически следует* высказывание *d,* если при истинности *с* истинно всякий раз и *d.* Высказывания *с* и *d логически эквивалентны,* если из высказывания *с* логически следует высказывание *d*, и наоборот, из *d* логически следует *с.*

Высказывания *несовместимы,* если нет ни одной логической возможности для одновременной истинности этих высказываний, в противном случае высказывания *совместимы.*

Введенные отношения поясним на примере высказываний: $a \leftrightarrow b$, $a \rightarrow b$, $\sim b \rightarrow \sim a$. Составим их таблицы истинности (рис. 7.13).

a	b	$a \leftrightarrow b$	$a \rightarrow b$	$\sim b$	$\sim a$	$\sim b \rightarrow \sim a$	$(a \leftrightarrow b) \rightarrow (a \rightarrow b)$	$(a \rightarrow b) \leftrightarrow (\sim b \rightarrow \sim a)$
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
и	и	и	и	л	л	и	и	и
и	л	л	л	и	л	л	и	и
л	и	л	и	л	и	и	и	и
л	л	и	и	и	и	и	и	и

Рис. 7.13

Из высказывания $a \leftrightarrow b$ следует высказывание $a \rightarrow b$, так как при истинности $a \leftrightarrow b$ истинно всякий раз и $a \rightarrow b$; но из высказывания $a \rightarrow b$ не следует высказывание $a \leftrightarrow b$, так как при истинности $a \rightarrow b$ высказывание $a \leftrightarrow b$ может быть ложным (рис. 7.13, столбцы *3* и *4*). Эквивалентны высказывания: $a \rightarrow b$ и $\sim b \rightarrow \sim a$; обратим внимание на то, что значения истинности эквивалентных высказываний совпадают (рис. 7.13, столбцы 4 и 7). Высказывания a и $\sim a$ несовместимы, а, например, высказывания $a \rightarrow b$ и $\sim b \rightarrow \sim a$ совместимы.

Между отношением следования и импликацией, так же как между отношением эквивалентности и двойной импликацией, имеется тесная связь, но важно не путать эти понятия. Импликация и двойная импликация — это новые высказывания, составленные из двух данных, а следование и эквивалентность — это отношения между двумя высказываниями. Связь же между ними такова: *из высказывания с следует высказывание d, если и только если импликация* $c \rightarrow d$ *логически истинна; с и d эквивалентны, если и только если двойная импликация* $c \leftrightarrow d$ *логически истинна.* В подтверждение: из высказывания $a \leftrightarrow b$ следует $a \rightarrow b$ и импликация $(a \leftrightarrow b) \rightarrow (a \rightarrow b)$ логически истинна (рис. 7.13, столбец *8*); высказывания $a \rightarrow b$ и $\sim b \rightarrow \sim a$ эквивалентны и двойная импликация $(a \leftrightarrow b) \rightarrow (\sim b \rightarrow \sim a)$ логически истинна (рис. 7.13, столбец *9*).

Проанализируем некоторые часто используемые, в том числе и выше использованные, формы высказываний с позиций отношений следования и эквивалентности:

1. *Высказывание «а истинно, только если b истинно» и высказывание «если а истинно, то b истинно» эквивалентны.*

Действительно, высказывание «*a* истинно, только если *b* истинно» констатирует «если *b* ложно, то и *a* ложно», которое эквивалентно высказыванию «если *a* истинно, то *b* истинно», так как, допустив, что из истинности *a* следует ложность *b* и, имея в виду, что из ложности *b* следует ложность *a,* мы получим, что из истинности *a* следует ложность *a*, чего быть не может. Итак, высказывание «*a* истинно, только если *b* истинно» эквивалентно высказыванию «если *b* ложно, то *a* ложно», которое эквивалентно высказыванию «если *a* истинно, то *b* истинно». Поэтому высказывания *«a* истинно, только если *b* истинно» и «если *a* истинно, то *b* истинно» эквивалентны.

В подтверждение сказанного эквивалентны следующие три высказывания, составленные из высказываний *a* = «совершивший уголовное преступление подлежит уголовному наказанию» и *b* = «совершивший уголовное преступление не моложе 14 лет»:

- «совершивший уголовное преступление подлежит уголовному наказанию, только если совершивший не моложе 14 лет» («*a* истинно, только если *b* истинно»);
- «если совершивший уголовное преступление моложе 14 лет, то он не подлежит уголовному наказанию» («если *b* ложно, то *a* ложно»);
- «если совершивший уголовное преступление подлежит уголовному наказанию, то совершивший не моложе 14 лет» («если *a* истинно, то *b* истинно»).

Обратим внимание на то, что два последние высказывания символически записываются так: $\sim b \rightarrow \sim a$, $a \rightarrow b$; эквивалентность же этих связок была подтверждена выше (рис. 7.13, столбцы *7, 4, 9*). Оба высказывания, в рамках существующего УК, логически истинны.

Замечание.

Синонимами выражения *«a* истинно, только если *b* истинно» являются выражения: «*a* истинно только в том случае, если *b* истинно» и «*a* истинно только тогда, когда *b* истинно».

2. *Высказывание «a истинно, если и только если b истинно» и часто используемое в математике высказывание «истинность a является достаточным и необходимым условием истинности b» эквивалентны.*

Действительно, высказывание *«a* истинно, если и только если *b* истинно» констатирует следующее: «если *b* истинно, то *a* истинно» и «если *b* ложно, то и *a* ложно». А так как последнее высказывание эквивалентно высказыванию «если *a* истинно, то и *b* истинно» (см. пункт 1), то получим, что высказывания: «*a* истинно, если и только если *b* истинно» и «если *b* истинно, то *a* истинно, и, если *a* истинно, то *b* истинно» эквивалентны.

Далее, высказывание «истинность *a* является достаточным условием для истинности *b*» констатирует «если *a* истинно, то *b* истинно», а высказывание «истинность *a* является необходимым условием

истинности *b*» констатирует, что «*b* истинно, только если *a* истинно», или «если *b* истинно, то и *a* истинно». Поэтому высказывание «истинность *a* является достаточным и необходимым условием истинности *b*» эквивалентно высказыванию «если *a* истинно, то *b* истинно, и, если *b* истинно, то *a* истинно».

Следовательно, высказывания «*a* истинно, если и только если *b* истинно» и «истинность *a* является достаточным и необходимым условием истинности *b*» эквивалентны.

В подтверждение эквивалентны следующие два высказывания, составленные из высказываний *a* = «совершивший уголовное преступление подлежит уголовному наказанию» и *b* = «совершивший уголовное преступление не моложе 14 лет»:

- «совершивший уголовное преступление подлежит уголовному наказанию, если и только если совершивший не моложе 14 лет» («*a* истинно, если и только если *b* истинно»);
- «если совершивший уголовное преступление подлежит уголовному наказанию, то совершивший не моложе 14 лет, и, если совершивший уголовное преступление не моложе 14 лет, то совершивший подлежит уголовному наказанию» («истинность *a* является достаточным и необходимым условием истинности *b*»).

Обратим внимание на то, что последние два высказывания символически записываются так: $a \leftrightarrow b$, $(a \rightarrow b) \wedge (b \rightarrow a)$; нетрудно убедиться в эквивалентности этих связок. И далее поскольку, в рамках существующего УК, второе высказывание логически истинно, то и первое тоже логически истинно.

Высказывание же «произведение двух чисел — четное число, если и только если оба числа — четные» не является логически истинным, так как не является логически истинным высказывание «если произведение двух чисел — четное число, то оба числа — четные, и, если оба числа четные, то их произведение четно». Действительно, в последнем высказывании вторая часть логически истинна, но первая часть не является логически истинной: если произведение двух чисел — четное число, например 16, то из этого вовсе не следует, что эти два числа четные: такими числами могут быть 1 и 16. Логически истинно высказывание «произведение двух чисел — четное число тогда, когда оба числа — четные».

Замечание.

Синонимами выражения «*a* истинно, если и только если *b* истинно» являются «*a* истинно в том и только том случае, если *b* истинно» и «*a* истинно тогда и только тогда, когда *b* истинно».

7.4. Аргументы правильные и ложные

Под *аргументом* понимают утверждение того, что некоторое высказывание (заключение) логически следует из конъюнкции других

высказываний (посылок). Аргумент называют *правильным,* если действительно из конъюнкции посылок логически следует заключение, т.е. при истинности всех посылок всякий раз будет истинным и заключение. Аргумент, не являющийся правильным, называется *ложным.* Примем такую форму записи аргумента: выпишем все посылки, под ними проведем черту, под которой запишем заключение. Приведем примеры словесной и символьной записи аргументов:

Пример 7.3.

Правильный аргумент:

Посылки	Словесная форма	Символьная форма
1	Если *гражданин законопослушен* (=*a*), он *не совершит преступления* (=*b*).	$a \to b$
2	Иванов — законопослушный гражданин.	a
Заключение:	Иванов не совершит преступления.	b

Аргумент правильный, так как из конъюнкции двух посылок следует заключение. В подтверждение приведем таблицу истинности аргументации (рис. 7.14).

a	b	$a \to b$	$(a \to b) \wedge a$	b
и	и	и	и	и
и	л	л	л	л
л	и	и	л	и
л	л	и	л	л

Рис. 7.14

Сравнив два последних столбца рис. 7.14, видим, что при истинности конъюнкции $(a \to b) \wedge a$ посылок заключение b истинно, т.е. из конъюнкции двух посылок следует заключение.

Пример 7.4.

Ложный аргумент:

Посылки	*Словесная форма*	*Символьная форма*
1	Если *гражданин законопослушен* (=*a*), он *не совершит преступления* (=*b*).	$a \to b$
2	Иванов — не законопослушен.	$\sim a$
Заключение:	Иванов совершит преступление.	$\sim b$

Аргумент ложный: при истинности конъюнкции $(a\to b)\wedge\sim a$ посылок заключение $\sim b$ не всегда истинно, что видно из таблицы истинности этой аргументации, приведенной на рис. 7.15.

a	b	$a\to b$	$\sim a$	$(a\to b)\wedge\sim a$	$\sim b$
и	и	и	л	л	л
и	л	л	л	л	и
л	и	и	и	и	л
л	л	и	и	и	и

Рис. 7.15

Наиболее типичны следующие правильные аргументы:

$$\frac{a\to b \quad a}{b} \qquad \frac{a\to b \quad \sim b}{\sim a} \qquad \frac{a\to b \quad b\to c}{a\to c} \qquad \frac{a\leftrightarrow b \quad a}{b} \qquad \frac{a\vee b \quad \sim a}{b} \qquad \frac{a\to b \quad \sim c\to\sim b}{\sim c\to\sim a}$$

и следующие ложные аргументы:

$$\frac{a\to b \quad b}{a} \qquad \frac{a\to b \quad \sim a}{\sim b} \qquad \frac{a\wedge b \quad \sim a\to b}{\sim b} \qquad \frac{a\to b \quad \sim b\to\sim c}{c\to a} \qquad \frac{a\leftrightarrow b \quad b\vee c \quad \sim c}{\sim a}$$

В правильности (ложности) этих аргументов легко убедиться, составив их таблицы истинности.

Убедимся в правильности следующего аргумента, приведенного в работе Дж Кемени и Дж. Снелла «Введение в конечную математику»: «Если *Джонс — убийца* (=a), то *ему точно известны время смерти Смита* (=b) и *чем он был убит* (=c). Поэтому если *Джонс не знает, когда умер Смит* (=$\sim b$), или *не знает, чем он был убит* (=$\sim c$), то *Джонс не является убийцей* (=$\sim a$)». Символическая запись этого аргумента:

$$\frac{a\to(b\wedge c) \quad \sim b\vee\sim c}{\sim a}$$

Таблица истинности аргумента приведена на рис. 7.16:

a	b	c	$b\wedge c$	$a\to(b\wedge c)$	$\sim b$	$\sim c$	$\sim b\vee\sim c$	$(a\to(b\wedge c))\wedge(\sim b\vee\sim c)$	$\sim a$
и	и	и	и	и	л	л	л	л	л
и	и	л	л	л	л	и	и	л	л
и	л	и	л	л	и	л	и	л	л
л	и	и	и	и	л	л	л	л	и
и	л	л	л	л	и	и	и	л	л
л	и	л	л	и	л	и	и	и	и
л	л	л	л	и	и	и	и	и	и

Рис. 7.16

Из двух последних столбцов таблицы видно, что при истинности конъюнкции $(a \to (b \wedge c)) \wedge (\sim b \vee \sim c)$ посылок аргумента заключение $\sim a$ истинно, поэтому приведенный аргумент правильный.

7.5. Множества и операции над ними. Диаграмма Венна. Соотношения между множествами и высказываниями

Понятие множества не определяется, а лишь иллюстрируется примерами. Например, можно говорить о множестве статей ГК РФ, о множестве логических возможностей и т.д. Множества будем обозначать прописными латинскими буквами: **A**, **B**, ... Если элемент x принадлежит множеству **A**, пишут $x \in \mathbf{A}$ (читают: «x принадлежит множеству **A**»), в противном случае пишут $x \notin \mathbf{A}$ («x не принадлежит множеству **A**»). Множество, не содержащее ни одного элемента, называют *пустым;* его обозначают символом $\varnothing$.

Множество считается заданным, если о любом данном объекте можно однозначно сказать, принадлежит он этому множеству или нет. Существует *два способа* задания множества:

- дается полный перечень элементов множества; например, множество результатов голосования присяжного такого: {«за», «против», «воздержался»};
- указывается правило определения принадлежности любого объекта к рассматриваемому множеству; например, запись $\mathbf{A} = \{x: \mid x \mid < 10\}$ означает, что **A** состоит из таких чисел x, модуль которых меньше 10 (после двоеточия записано правило, которому должно удовлетворять число x, чтобы его можно было отнести к множеству **A**).

Два множества, состоящие из одних и тех же элементов, называются *равными*. Если множества **A** и **B** равны, то пишут $\mathbf{A} = \mathbf{B}$. Например, заданные перечнем элементов множества $\mathbf{A} = \{1, 2, 3\}$ и $\mathbf{B} = \{3, 2, 1\}$ равны, т.е. $\mathbf{A} = \mathbf{B}$, или $\{1, 2, 3\} = \{3, 2, 1\}$.

Если каждый элемент множества **B** является в то же время элементом множества **A**, то говорят, что **B** — часть, или, иначе, *подмножество* множества **A**. В этом случае пишут $\mathbf{B} \subset \mathbf{A}$ (читают «**B** — подмножество множества **A**»).

В последующем исходное множество будем называть *универсальным* и обозначать буквой $\mathbf{\Omega}$ (прописная греческая буква «омега»). *Собственные подмножества* множества $\mathbf{\Omega}$ — это те подмножества, которые содержат некоторые, но не все элементы $\mathbf{\Omega}$. Наряду с собственными подмножествами условимся само $\mathbf{\Omega}$ и пустое множество $\varnothing$ также считать подмножествами множества $\mathbf{\Omega}$.

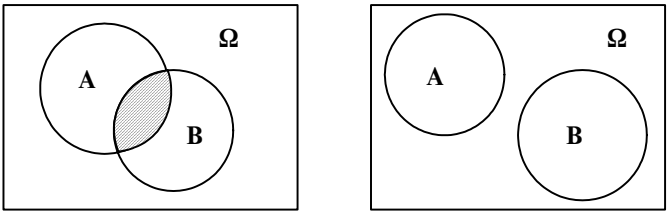
На базе множества $\mathbf{\Omega} = \{\omega_1, \omega_2\}$ можно образовать $2^2 = 4$ подмножества: $\{\omega_1\}$, $\{\omega_2\}$, $\mathbf{\Omega}$, $\varnothing$, из которых $2^2 - 2 = 2$ собственных —

это $\{\omega_1\}$ и $\{\omega_2\}$. На базе множества $\Omega = \{\omega_1, \omega_2, \omega_3\}$ можно образовать $2^3 = 8$ подмножеств: $\{\omega_1\}$, $\{\omega_2\}$, $\{\omega_3\}$, $\{\omega_1, \omega_2\}$, $\{\omega_1, \omega_3\}$, $\{\omega_2, \omega_3\}$, Ω, $\varnothing$, из которых $2^3 - 2 = 6$ собственных. На базе множества Ω, содержащего N элементов, можно образовать 2^N подмножеств, из которых $(2^N - 2)$ собственных.

Выше были рассмотрены способы, которыми из данных высказываний могут быть образованы новые высказывания. Рассмотрим аналогичный процесс образования новых множеств из данных множеств **A** и **B,** при этом будем предполагать, что и **A**, и **B**, и вновь образованное множество являются подмножествами некоторого универсального множества **Ω**.

Для наглядного представления операций над множествами используем *диаграмму Венна*[1], на которой универсальное множество **Ω** изображается прямоугольником, а его подмножества **A** и **B** — некоторыми фигурами, чаще кругами, внутри прямоугольника.

Пересечением множеств **A** и **B** называется множество **A∩B,** состоящее из тех и только тех элементов, которые принадлежат **A** и **B** одновременно (словосочетание «из тех и только тех» в данном контексте означает, что **A∩B** состоит из элементов, принадлежащих одновременно **A** и **B**, и никакие другие элементы в **A∩B** не входят). Пересечение **A∩B** множеств **A** и **B** на диаграмме Венна изображено на рис. 7.17,*а* заштрихованной областью. Если **A** и **B** не имеют общих элементов, то пересечение **A∩B** будет пустым множеством $\varnothing$, т.е. $\mathbf{A} \cap \mathbf{B} = \varnothing$ (рис. 7.17,*б*).



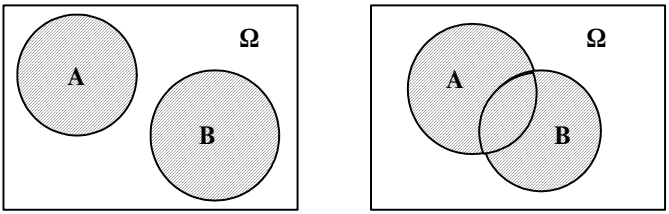
а *б*

Рис. 7.17

Объединением множеств **A** и **B** называется множество **A∪B,** состоящее из тех и только тех элементов, которые принадлежат **A** или **B** (или **A** и **B** одновременно, если таковые элементы есть) (рис. 7.18,*а* и 7.18,*б* — заштрихованные области).

---

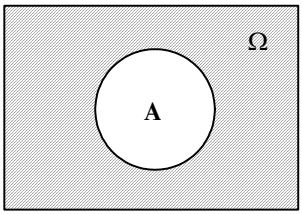
[1] *Венн Джон* (1834—1923) — английский логик.



а *б*

Рис. 7.18

Дополнением множества **A** называется множество $\overline{\mathbf{A}}$ (читают «не **A**»), состоящее из тех и только тех элементов множества **Ω**, которые не принадлежат **A** (рис. 7.19, заштрихованная область). Операция «дополнение» симметрична: если $\overline{\mathbf{A}}$ — дополнение **A**, то и **A** — дополнение $\overline{\mathbf{A}}$; поэтому **A** и $\overline{\mathbf{A}}$ называют *взаимодополняющими* множествами.



$\overline{\mathbf{A}}$

Рис. 7.19

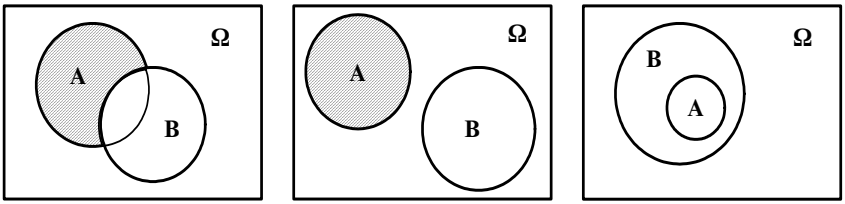
Разностью множеств **A** и **B** называется множество **A\B** (читают «**A** без **B**») всех тех элементов **A**, которые не принадлежат **B** (рис. 7.20,*а* — заштрихованная область).

Нетрудно убедиться в справедливости следующих утверждений:

- $\Omega\backslash\mathbf{A} = \overline{\mathbf{A}}$;
- если у **A** и **B** нет общих элементов, т.е. $\mathbf{A}\cap\mathbf{B} = \varnothing$, то $\mathbf{A}\backslash\mathbf{B} = \mathbf{A}$ (рис. 7.20,*б* — заштрихованная область) и $\mathbf{B}\backslash\mathbf{A} = \mathbf{B}$;
- если **A** — подмножество множества **B**, т.е. $\mathbf{A} \subset \mathbf{B}$, то $\mathbf{A}\backslash\mathbf{B} = \varnothing$ (рис. 7.20,*в*).

В качестве приложения введенных понятий рассмотрим задачу *«голосующие коалиции»*. Пусть имеется группа людей, голосующих «за» или «против» проведения какой-то меры (возможность «воздержания» исключим). Каждый член группы может иметь один или несколько голосов. Решение группы принимается согласно какому-либо правилу: или простым большинством, или 2/3 от общего чис-

ла голосов и т.д. Некоторые члены группы могут объединяться в коалицию с целью проведения названной меры. Коалицию называют *выигрывающей,* если ее голосов достаточно для проведения меры; *проигрывающей,* если члены, не вошедшие в коалицию, могут провести свое решение вопреки желанию коалиции. Коалицию называют *блокирующей,* если ее члены сами по себе, как и члены, не вошедшие в эту коалицию, не могут провести никакого решения.



A\B *а* **A\B = A** *б* **A\B = ∅** *в*

Рис. 7.20

Например, комитет состоит из трех членов: X (председатель), имеющий два голоса, и x_1 и x_2, имеющие по одному голосу каждый. Исход решается простым большинством голосов. Возможные варианты голосования трех членов указаны в таблице на рис. 7.21.

№ варианта	X		x_1	x_2
1	+	+	+	+
2	+	+	+	−
3	+	+	−	+
4	+	+	−	−
5	−	−	+	+
6	−	−	+	−
7	−	−	−	+
8	−	−	−	−

Рис. 7.21

За универсальное множество **Ω** примем множество $\{X, x_1, x_2\}$ всех членов комитета в предположении, что каждый из них высказался «за», $\mathbf{\Omega} = \{X, x_1, x_2\}$. Тогда, например, подмножество $\{X, x_1\}$ означает, что X и x_1 проголосовали «за», а x_2 — «против» (т.е. имеет место второй вариант голосования), а пустое множество ∅ означает, что все члены комитета проголосовали «против» (8-й вариант голосования). Количество подмножеств множества **Ω**, включая **Ω** и ∅, равно $2^3 = 8$, из которых 6 собственных (варианты 2−7). Так как

решение «за» принимается в 1, 2 и 3 вариантах голосования, а решение «против» в 8, 7 и 6 вариантах, то выигрывающими коалициями являются множества $\Omega = \{X, x_1, x_2\}, \{X, x_1\}, \{X, x_2\}$, а проигрывающими: $\varnothing$, $\{x_2\}$, $\{x_1\}$. Обратим внимание на следующее: если множество — коалиция **C** является выигрывающей (проигрывающей), то дополнение $\overline{\mathbf{C}}$ множества **C** — проигрывающая (выигрывающая) коалиция.

Для подтверждения приведем такую таблицу:

Выигрывающая коалиция (*множество* **C**)	*Проигрывающая коалиция* (*множество* $\overline{\mathbf{C}} = \Omega \backslash \mathbf{C}$)
$\mathbf{C} = \{X, x_1, x_2\}$	$\overline{\mathbf{C}} = \varnothing$
$\mathbf{C} = \{X, x_1\}$	$\overline{\mathbf{C}} = \{x_2\}$
$\mathbf{C} = \{X, x_2\}$	$\overline{\mathbf{C}} = \{x_1\}$

Среди выигрывающих коалиций выделяют минимальные выигрывающие (в задаче это коалиции $\{X, x_1\}$ и $\{X, x_2\}$). *Минимальная выигрывающая коалиция* — это такая выигрывающая коалиция, ни одно из собственных подмножеств которой не является выигрывающей коалицией. Выигрывающая коалиция $\{X, x_1\}$ — минимальная, так как ни одно из ее собственных подмножеств: $\{X\}$ и $\{x_1\}$, не является выигрывающей коалицией; то же относится и к коалиции $\{X, x_2\}$.

В 4-м и 5-м вариантах (рис. 7.21) решение принято не будет (нет большинства); поэтому коалиция $\{X\}$ и коалиция $\{x_1, x_2\}$ — блокирующие. Обратим внимание на то, что сумма чисел выигрывающих, проигрывающих и блокирующих коалиций равна числу подмножеств множества Ω.

Пример 7.5.

Интересным примером группы, принимающей решения, служит Совет безопасности ООН, состоящий при существовании СССР из одиннадцати членов: пяти представителей великих держав ($X_1, X_2, ..., X_5$), каждый из которых мог единолично блокировать любую меру, и шести представителей малых наций ($x_1, x_2, ..., x_6$). Каждый из 11 членов имел один голос (возможность «воздержания» исключим). Для принятия Советом какой-то меры необходимо, чтобы за нее проголосовало семь членов, включая «большую пятерку». За универсальное множество Ω примем множество $\{X_1, ..., X_5, x_1, ..., x_6\}$ всех членов Совета в предположении, что каждый из них высказался «за». Общее число вариантов голосования 11 членов равно $2^{11} = 2048$ — столько подмножеств имеет множество $\Omega = \{X_1, ..., X_5, x_1, ..., x_6\}$. Любое подмножество множества Ω, состоящее из «большой пятерки» и двух или более (не менее двух) представителей малых наций, будет выигрывающей коалицией; а лю-

бое подмножество, состоящее из четырех или менее (не более четырех) представителей малых наций будет проигрывающей коалицией. Примеры этих коалиций приведены в следующей таблице:

Выигрывающая коалиция (*множество* **C**)	*Проигрывающая коалиция* (*множество* $\overline{\mathbf{C}} = \Omega \backslash \mathbf{C}$)
$\mathbf{C} = \{X_1, ..., X_5, x_1, x_2\}$	$\overline{\mathbf{C}} = \{x_3, x_4, x_5, x_6\}$
$\mathbf{C} = \{X_1, ..., X_5, x_1, x_2, x_3\}$	$\overline{\mathbf{C}} = \{x_4, x_5, x_6\}$
$\mathbf{C} = \{X_1, ..., X_5, x_1, x_2, x_3, x_4\}$	$\overline{\mathbf{C}} = \{x_5, x_6\}$
$\mathbf{C} = \{X_1, ..., X_5, x_1, x_2, x_3, x_4, x_5\}$	$\overline{\mathbf{C}} = \{x_6\}$
$\mathbf{C} = \{X_1, ..., X_5, x_1, ..., x_6\}$	$\overline{\mathbf{C}} = \varnothing$
.....	.....

Общее число выигрывающих коалиций[1] равно 57 (столько же и проигрывающих коалиций), из которых 15 будут минимальными — это коалиции, состоящие из «большой пятерки» и двух представителей малых наций. Число блокирующих коалиций равно (2048 − 57 − 57) = 1934, среди них и единичные множества $\{X_1\}$, $\{X_2\}$, $\{X_3\}$, $\{X_4\}$, $\{X_5\}$.

Между множествами и высказываниями, а также между операциями над множествами и операциями, связывающими простые высказывания в составные, существует тесная связь.

Естественный *способ сопоставления высказываний с множествами* такой:

- для имеющихся высказываний *a*, *b*, *c*, ... находим множество **Ω** всех логических возможностей — универсальное множество;
- на множестве **Ω** выделяем подмножества **A**, **B**, **C**, ... логических возможностей, для которых истинны соответственно высказывания *a*, *b*, *c*, ...; **A**, **B**, **C**, ... называют *множествами истинности* соответствующих высказываний;
- каждому высказыванию поставим в соответствие его множество истинности.

Естественный *способ сопоставления операций связывания высказываний* и *операций над множествами* такой:

- множество истинности высказывания $a \wedge b$ — это множество $\mathbf{A} \cap \mathbf{B}$ (рис. 7.22, область двойной штриховки);
- множество истинности высказывания $a \vee b$ — это множество $\mathbf{A} \cup \mathbf{B}$ (рис. 7.22, вся заштрихованная область);

Замечание.

На рис. 7.22 множества **A** и **B** истинности высказываний *a* и *b* имеют общие элементы — это говорит о том, что допустима одновременная

[1] Способ подсчета чисел 57 и 15 изложен далее в задаче 7.7.

истинность a и b, т.е. a и b — совместимые высказывания. Множества **A** и **B** истинности несовместимых высказываний a и b не имеют общих точек (рис. 7.18,*а*), но и в этом случае множество истинности высказывания $a \vee b$ (точнее $a \underline{\vee} b$) — это множество $\mathbf{A} \cup \mathbf{B}$.

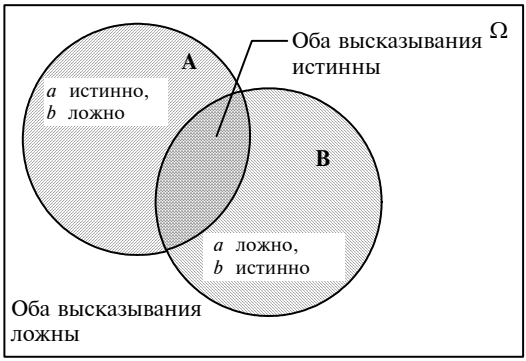
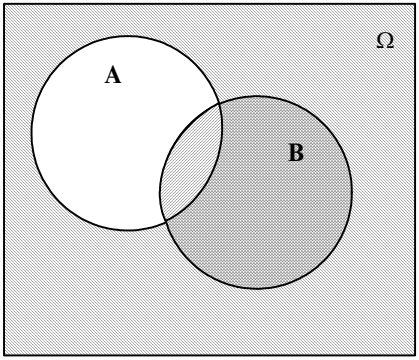


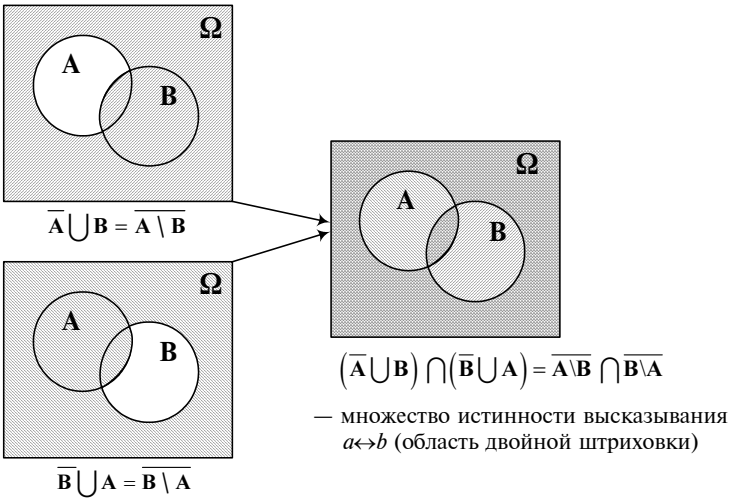
Рис. 7.22

- множество истинности высказывания $\sim a$ (иначе, множество «ложности» высказывания a) — это множество $\bar{\mathbf{A}}$ (рис. 7.19, заштрихованная область);
- множество истинности высказывания $a \to b$ — множество $\overline{\mathbf{A}} \cup \mathbf{B}$; это объясняется тем, что высказывание $a \to b$ эквивалентно высказыванию $\sim a \vee b$ (рис. 7.6, последние три столбца), множеством истинности которого является множество $\overline{\mathbf{A}} \cup \mathbf{B}$ (рис. 7.23, заштрихованная область); обратим внимание на то, что незаштрихованная на рис. 7.23 область — это множество $\mathbf{A} \setminus \mathbf{B}$, тогда заштрихованная область — это множество $\overline{\mathbf{A} \setminus \mathbf{B}}$, и следовательно, $\overline{\mathbf{A}} \cup \mathbf{B} = \overline{\mathbf{A} \setminus \mathbf{B}}$;
- множество истинности высказывания $a \leftrightarrow b$, эквивалентного высказыванию $(\sim a \vee b) \wedge (\sim b \vee a)$, — это множество $(\overline{\mathbf{A}} \cup \mathbf{B}) \cap (\overline{\mathbf{B}} \cup \mathbf{A})$, или равное ему множество $\overline{\mathbf{A} \setminus \mathbf{B}} \cap \overline{\mathbf{B} \setminus \mathbf{A}}$; последовательность построения множества истинности приведена на рис. 7.24;
- множество истинности логически истинного высказывания (напомним, это высказывание, истинное в каждом логически возможном случае) — это множество $\boldsymbol{\Omega}$ всех логических возможностей;
- множество истинности логически ложного высказывания — пустое множество $\varnothing$.



$\overline{\mathbf{A}} \cup \mathbf{B} = \overline{\mathbf{A} \setminus \mathbf{B}}$ — множество истинности высказывания $a \leftrightarrow b$ (вся заштрихованная область)

Рис. 7.23



— множество истинности высказывания $a \leftrightarrow b$ (область двойной штриховки)

Рис. 7.24

И наконец, *как на языке множеств выглядят отношения следования и эквивалентности?* Ответ:

- из высказывания a следует высказывание b, если и только если импликация $a \rightarrow b$ логически истинна; логическая же истинность высказывания $a \rightarrow b$ означает, что его множество истинности $\overline{\mathbf{A} \setminus \mathbf{B}} = \mathbf{\Omega}$, и тогда $\mathbf{A} \setminus \mathbf{B} = \varnothing$, но последнее равенство верно в том и только том случае, когда множество **A** является подмножеством множества **B**.

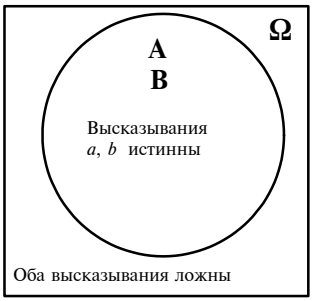
Итак, из высказывания a следует высказывание b, если и только если между множествами **A** и **B** истинности этих высказываний имеет место соотношение: $\mathbf{A} \subset \mathbf{B}$ (рис. 7.25);

- высказывания a и b эквивалентны, если и только если двойная импликация $a \leftrightarrow b$ логически истинна; логическая же истинность высказывания $a \leftrightarrow b$ означает, что его множество истинности $\overline{\mathbf{A} \setminus \mathbf{B}} \cap \overline{\mathbf{B} \setminus \mathbf{A}} = \Omega$, но последнее равенство верно в том и только том случае, когда $\mathbf{A} = \mathbf{B}$.

Итак, высказывание a эквивалентно высказыванию b, если и только если между множествами **A** и **B** истинности этих высказываний имеет место соотношение: $\mathbf{A} = \mathbf{B}$ (рис. 7.26).

$\mathbf{A} \subset \mathbf{B}$

Рис. 7.25



$\mathbf{A} = \mathbf{B}$

Рис. 7.26

Приведем итоговую таблицу соотношений между высказываниями и множествами:

Высказывание	*Множество истинности*
логически истинное	Ω
логически ложное	$\varnothing$
a	$\mathbf{A} \subset \Omega$
b	$\mathbf{B} \subset \Omega$
$a \wedge b$	$\mathbf{A} \cap \mathbf{B}$
$a \vee b$	$\mathbf{A} \cup \mathbf{B}$
$\sim a$	$\bar{\mathbf{A}}$
$a \rightarrow b$	$\bar{\mathbf{A}} \cup \mathbf{B} = \overline{\mathbf{A} \setminus \mathbf{B}}$
$a \leftrightarrow b$	$\left(\overline{\mathbf{A}} \cup \mathrm{B}\right) \cap \left(\overline{\mathbf{B}} \cup \mathrm{A}\right) = \overline{\mathbf{A} \setminus \mathbf{B}} \cap \overline{\mathbf{B} \setminus \mathbf{A}}$
Отношение между высказываниями	*Отношение между множествами истинности*
из a следует b	$\mathbf{A} \subset \mathbf{B}$
a эквивалентно b	$\mathbf{A} = \mathbf{B}$

Рис. 7.27

Выявленные соотношения позволяют перевести любую задачу, относящуюся к высказываниям, в задачу теории множеств, и наоборот, задачу, относящуюся к множествам, перевести на язык высказываний. Приведем пример, подтверждающий целесообразность такого перехода.

Пример 7.6.

Пусть требуется выяснить, совместимы или нет следующие высказывания:

1. Если *математика интересна* (=*a*), то *я буду над ней работать* (=*b*);

2. Если *математика не интересна* (=~*a*), то *я получу по этому предмету плохую оценку* (=*c*);

3. *Я не буду работать над математикой* (=~*b*), но *получу по этому предмету хорошую оценку* (=~*c*).

В принятых обозначениях символьные выражения высказываний таковы:

1) $a \to b$;

2) $\sim a \to c$;

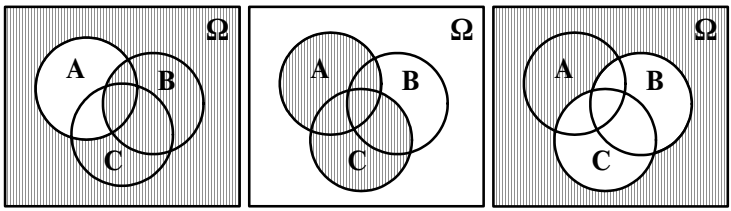
3) $\sim b \wedge \sim c$.

Ответим двумя способами: используя язык множеств и используя язык высказываний.

➢ ***Язык множеств***. Перейдем от высказываний к множествам истинности:

Высказывание	*Множество истинности*
1. $a \to b$	$\overline{\mathbf{A} \setminus \mathbf{B}}$
2. $\sim a \to c$	$\overline{\overline{\mathbf{A}} \setminus \mathbf{C}}$
3. $\sim b \wedge \sim c$	$\overline{\mathbf{B}} \cap \overline{\mathbf{C}}$

Множества истинности изобразим на диаграммах Венна (рис. 7.28, заштрихованные области).



$\overline{\mathbf{A} \setminus \mathbf{B}}$ $\quad$ $\overline{\overline{\mathbf{A}} \setminus \mathbf{C}}$ $\quad$ $\overline{\mathbf{B}} \cap \overline{\mathbf{C}}$

Рис. 7.28

Из диаграмм видно: нет элементов множества логических возможностей **Ω**, которые бы принадлежали одновременно всем трем множествам истинности, иначе нет ни одной логической возможности для одновременной истинности высказываний 1, 2, 3, поэтому эти высказывания несовместимы в совокупности; однако они попарно совместимы.

➢ ***Язык высказываний.*** Построим таблицы истинности высказываний 1, 2, 3 (рис. 7.29).

№	a	b	c	$a \to b$	$\sim a \to c$	$\sim b \wedge \sim c$
1	и	и	и	и	и	л
2	и	и	л	и	и	л
3	и	л	и	л	и	л
4	л	и	и	и	и	л
5	и	л	л	л	и	и
6	л	и	л	и	л	л
7	л	л	и	и	и	л
8	л	л	л	и	л	и

Рис. 7.29

В таблице нет ни одной строки, где бы все три высказывания: $a \to b$, $\sim a \to c$, $\sim b \wedge \sim c$ были бы одновременно истинны, поэтому высказывания несовместимы в совокупности; однако они совместимы попарно.

Результаты обоих подходов, естественно, совпали.

Контрольные вопросы и задания

1. Приведите примеры социально-правовых задач, решаемых математическими методами.

2. Дайте определение конъюнкции, дизъюнкции, отрицания, импликации, двойной импликации; таблицы истинности этих высказываний.

3. Приведите примеры логических формул правовых норм.

4. Дайте определение отношения следования, эквивалентности и несовместимости.

5. Приведите примеры необходимых и достаточных условий в формулировках правовых норм.

6. Дайте определение правильного и ложного аргумента. Приведите примеры аргументов, их словесной и символьной записи, примеры правильных и ложных аргументов.

7. Операции над множествами; изображение операций на диаграммах Венна. Сопоставление логических операций над высказываниями с операциями над множествами истинности этих высказываний.

Глава 8

ВЕРОЯТНОСТИ ВЫСКАЗЫВАНИЙ (СОБЫТИЙ). ВЫБОР РЕШЕНИЯ ПРИ НЕИЗВЕСТНЫХ ВЕРОЯТНОСТЯХ

В юридической практике часто можно услышать высказывания такого типа: «Я имею все шансы выиграть этот процесс», «Орудием убийства, скорее всего, был тяжелый предмет» и т.д. Эти высказывания относятся к определенным событиям. Так, первое высказывание относится к событию A — выигрывание процесса, а второе — к событию B — орудие убийства — тяжелый камень. Судя по высказываниям, в исходе этих событий мы не уверены: событие A, так же как и событие B, может произойти, а может и не произойти.

Событие, исход которого, судя по высказыванию, не однозначен, называется *случайным*, а само высказывание — *вероятностным*. События, о которых идет речь в высказываниях a, b, c, ... будем обозначать соответственно A, B, C, ... При этом договоримся, что высказывание $a \wedge b$ относится к событию $A \cap B$, $a \vee b$ к событию $A \cup B$, $\sim a$ к событию $\overline{A}$ и т.д. (знаки между событиями соответствуют знакам между множествами истинности высказываний — см. рис. 7.27).

Напомним, *маргинальными* высказываниями являются логически истинное (истинное в каждой логической возможности) и логически ложное. Логически истинное высказывание относится к *достоверному* событию (его будем обозначать буквой Ω) — оно происходит всегда, в каждой логической возможности; логически ложное высказывание относится к *невозможному* событию (его будем обозначать символом $\varnothing$) — оно не происходит никогда, ни в одной логической возможности. Например, достоверным является событие Ω — число выпавших очков при однократном подбрасывании игральной кости не больше шести, а невозможным — событие $\varnothing$ — число выпавших очков при однократном подбрасывании кости больше шести.

Можно ли изучать случайные события (а следовательно, и относящиеся к ним вероятностные высказывания), если заранее сказать, каков будет исход этих событий нельзя? Действительно, предвидеть результат единичного судебного процесса нельзя; однако опыт многократного проведения аналогичных процессов в типичных условиях

зачастую позволяет случайному событию A — выигрывание процесса (а следовательно, и высказыванию a = «я выиграю этот процесс») — приписать количественную меру $P(A)$ возможности появления события A (количественную меру $P(a)$ — истинности высказывания a), называемую *вероятностью* события A (высказывания a). Если такое «приписывание» возможно, то говорят, что изучаемое случайное событие статистически устойчиво.

Случайное явление обладает свойством *статистической устойчивости,* если некоторая функция результатов многократных наблюдений этого явления в типичных условиях предсказуема с большой степенью надежности, тогда как результат единичного наблюдения не предсказуем.

Дадим более подробные пояснения этого свойства. Например, исход единичного подбрасывания монеты предсказать нельзя; однако при многократном ее подбрасывании примерно в одинаковых условиях можно ожидать, с большой степенью уверенности, что герб появится примерно в 50% подбрасываний. Это подтверждают следующие эксперименты, проведенные в XVIII в.

Экспериментатор	*Количество подбрасываний* (n)	*Количество выпадений герба* (m)	*Относительная частота выпадения герба* ($\hat{p} = m/n$)
Бюффон	4040	2048	0,5069
К. Пирсон	12 000	6019	0,5016
К. Пирсон	24 000	12 012	0,5005

Относительная частота $\hat{p} = m/n$ выпадений герба при большом числе n наблюдений становится предсказуемой (в экспериментах $\hat{p} \approx 0{,}5$).

Я. Бернулли[1] доказал теорему, согласно которой относительная частота обладает свойством статистической устойчивости: *при увеличении числа n наблюдений, проводимых в типичных условиях, увеличивается* (*при выполнении достаточно общих ограничений*) *уверенность в незначительном отклонении относительной частоты* $\hat{p} = m/n$ *от некоторого постоянного числа p.* Устойчивость или практически отсутствующая колеблемость относительной частоты при больших числах наблюдений была подмечена во многих явлениях еще задолго до XVIII в. Так, еще в Древнем Китае было обнаружено, что для

[1] *Бернулли Якоб* (1654—1705) — профессор математики Базельского университета. Теорема Бернулли — важный частный случай закона больших чисел.

государств и больших городов отношение числа родившихся мальчиков к числу всех родившихся из года в год почти неизменно чуть больше 0,5.

Статистическая устойчивость свойственна, при выполнении определенных ограничений, не только относительной частоте, но и средней арифметической результатов наблюдений — это было доказано русским математиком П.Л. Чебышевым[1]: *при увеличении числа n наблюдений, проводимых в типичных условиях, увеличивается* (*при выполнении достаточно общих ограничений*) *уверенность в незначительном отклонении вычисленной по этим наблюдениям средней арифметической от некоторого постоянного числа.* Так, устойчивость свойственна среднему возрасту преступника, среднему числу ДТП, например, за месяц в крупном городе и т.д. Колеблемость этих средних при больших числах наблюдений (соответственно, обследованных преступников, месяцев) практически отсутствует.

Статистической устойчивостью, наряду с относительной частотой и средней арифметической, обладает и целый ряд других функций результатов наблюдений.

Математические методы изучения случайных явлений, обладающих свойством статистической устойчивости, предлагает *теория вероятностей и математическая статистика.*

8.1. Приписывание вероятностей случайным событиям (вероятностным высказываниям)

➢ ***Опытная вероятность.*** Выше было введено понятие относительной частоты $\hat{p}(A)$ появления случайного события A — это отношение числа m_A наблюдений, в которых появилось это событие A, к общему числу n проведенных наблюдений, $\hat{p}(A) = m_A/n$. Также было отмечено, что при выполнении достаточно общих ограничений, в силу теоремы Я. Бернулли, значение относительной частоты при проведении в типичных условиях большого числа n наблюдений становится предсказуемым (статистически устойчивым). Это служит основанием тому, чтобы относительную частоту появления события в большом числе n наблюдений принять за вероятность события; ее называют *опытной,* или *эмпирической,* или *статистической вероятностью.* Отметим, опытная вероятность не постоянна: при повторении n наблюдений число наблюдений m_A, в которых произойдет событие A, может отличаться от ранее полученного, в результате — новое значение относительной частоты, или опытной вероятности.

---

[1] *Чебышёв Пафнутий Львович* (1821—1894) — русский математик и механик, академик Петербургской АН.

Так как всегда $0 \le m_A \le n$, то $0 \le \hat{p}(A) \le 1$; для достоверного события Ω (оно появляется во всех испытаниях): $m_\Omega = n$ и опытная вероятность $\hat{p}(\Omega) = 1$; для невозможного события $\varnothing$ (оно не появляется ни в одном испытании): $m_\varnothing = 0$ и $\hat{p}(\varnothing) = 0$.

Замечание.

Из теоремы Я. Бернулли вовсе не вытекает, что устойчивость относительной частоты — неоспоримый факт. Например, как отмечается в работе В.Н. Тутубалина[1], бессмысленно с вероятностной точки зрения высказывание типа: «Медведь может выскочить из-за фиксированного куста с вероятностью 0,1, и тогда охотник убивает его с вероятностью 0,5», так как весьма сомнительно предположение статистической устойчивости относительной частоты появления медведя из-за данного куста, равно как и относительной частоты его «убивания» в этом случае (без чего приведенные в выражении вероятности не имеют смысла). Проверка статистической устойчивости трудна и не всегда выполнима; чаще всего вопрос ее выполнимости решается на интуитивном уровне с учетом накопленного опыта работы.

Нахождение опытной вероятности требует проведения большого числа наблюдений. Но как можно, например, провести многократно уникальный судебный процесс с тем, чтобы определить вероятность вынесения оправдания? Однако ряду статистически устойчивых явлений можно «приписать» вероятности (меры объективной возможности появления этих явлений), не проводя наблюдений; такие вероятности часто называют «доопытными».

➢ ***«Доопытная» вероятность.*** Пусть a — некоторое вероятностное высказывание, относящееся к случайному событию A. Естественен следующий алгоритм «приписывания» вероятности высказыванию a (событию A):

- высказывание a свяжем с множеством $\Omega = \{\omega_1, \omega_2, ...\}$ логических возможностей;
- каждому элементу ω_i множества Ω поставим в соответствие некоторое положительное число (вес $P(\omega_i)$ — вероятность логической возможности ω_i), такое, чтобы сумма этих чисел, весов равнялась единице:

$$\left.\begin{array}{l} P(\omega_i) > 0,\ i = 1, 2, ... \\ \sum\limits_{\omega_i \in \Omega} P(\omega_i) = 1 \end{array}\right\} \qquad \textbf{(8.1)}$$

(запись $\sum\limits_{\omega_i \in \Omega} P(\omega_i) = 1$ означает суммирование вероятностей всех тех элементов ω_i, которые образуют множество Ω);

[1] *Тутубалин В.Н.* Теория вероятностей. — М.: МГУ, 1972.

- на множестве Ω выделим подмножество **A** — множество истинности высказывания a (оно включает те и только те логические возможности, для которых высказывание a истинно);
- находим сумму вероятностей элементов, образующих множество **A**, которую и примем за вероятность $P(a)$ высказывания a (за вероятность $P(\mathrm{A})$ события A):

$$P(a) = P(\mathrm{A}) = \sum_{\omega_i \in \mathbf{A}} P(\omega_i). \qquad \textbf{(8.2)}$$

Заметим, если высказывание логически истинно, т.е. если высказывание относится к достоверному событию Ω, то множеством истинности этого высказывания будет все множество Ω, поэтому, учитывая (8.1), «доопытная» вероятность достоверного события $P(\Omega) = 1$. Множеством истинности логически ложного высказывания — высказывания, относящегося к невозможному событию $\varnothing$, будет пустое множество $\varnothing$, поэтому $P(\varnothing) = 0$. Окончательно, для любого высказывания a (события A)

$$0 \le P(a) = P(\mathrm{A}) \le 1.$$

В дальнейшем не будем делать различий между вероятностями высказывания a и относящегося к этому высказыванию события A.

Задача 1.

В городе работают три риелторских агентства X_1, X_2, X_3. Клиенту известно, что X_1 и X_2 имеют примерно одинаковые шансы решить его квартирный вопрос, а шансы X_3 в 1,5 раза меньше шансов X_1. Какова вероятность высказывания a = «клиент обратится в агентство X_1 или в агентство X_2»?

Решение.

Пусть множество логических возможностей $\Omega = \{\omega_1, \omega_2, \omega_3\}$, где ω_i — решение агентством X_i (i = 1, 2, 3) квартирного вопроса клиента. Множество истинности высказывания a — это множество $\mathbf{A} = \{\omega_1, \omega_2\}$, и согласно (8.2), $P(a) = P(\omega_1) + P(\omega_2)$. Элементу ω_3 присвоим вес $f > 0$, а элементам ω_1 и ω_2 веса 1,5f и 1,5f. Так как согласно (8.1) сумма этих весов должна равняться 1, то 1,5f + 1,5f + f = 1, f = 0,25, $P(\omega_3)$ = f = 0,25, $P(\omega_1) = P(\omega_2)$ = 0,375. Окончательно $P(a) = P(\omega_1) + P(\omega_2)$ = 0,75.

Нахождение вероятности высказывания a (события A) значительно упрощается, если число логических возможностей множества Ω конечно, например равно N, т.е. $\Omega = \{\omega_1, \omega_2, ..., \omega_N\}$, и есть основание считать эти возможности равновероятными, и потому приписать каждой из них один и тот же вес. Тогда, учитывая, что в соответствии с (8.1): $P(\omega_1) + ... + P(\omega_N) = 1$, получим $P(\omega_1) = ... = P(\omega_N) = 1/N$. И если множество **A** истинности высказывания a содержит M

логических возможностей, то $P(a) = P(\text{A}) = \sum_{\omega_i \in \mathbf{A}} P(\omega_i) = M/N$. *Классическая формула вероятности*:

$$P(a) = P(\text{A}) = M/N, \qquad \textbf{(8.3)}$$

где N — общее число равновероятных логических возможностей, связанных с высказыванием a (событием А);

M — число тех возможностей, при которых высказывание a истинно (событие А произойдет).

Задача 2.

В условиях примера 7.1 найти вероятности следующих высказываний: d = «только один член жюри проголосует «за», e = «по крайней мере один член жюри проголосует «за».

Решение.

При тайном голосовании трех членов жюри, поставленных в одинаковые условия, есть основание считать, что имеющиеся $N = 8$ логических возможностей (рис. 7.8,а) равновероятны. Высказывание d истинно при $M = 3$ — это возможности 4, 6, 7; поэтому $P(d) = 3/8$. Высказывание e истинно в $M = 7$ возможностях — это возможности 1÷7, поэтому $P(e) = 7/8$.

Замечание.

В условиях примера 7.2 логические возможности не равновероятны (это относится как к «грубому» множеству — см. рис. 7.10, так и к «более детальному» — см. рис. 7.11): ведь составы урн различны. Однако в рамках «каждой отдельно взятой урны» логические возможности равновероятны. Поэтому вероятность высказывания a = «из первой урны будет извлечен белый шар», в котором выбор первой урны зафиксирован как истина, можно рассчитать по классической формуле:

- при использовании «грубого» множества (см. рис. 7.10,а) общее число равновероятных возможностей $N = 3$ — это возможности 1, 2, 3, из которых $M = 2$ возможности ведут к появлению белого шара; $P(a) = 2/3$;
- при использовании «более детального» множества (см. рис. 7.11,а) $N = 6$ — это возможности 1÷6, из которых $M = 4$ возможности ведут к появлению белого шара; по-прежнему

$$P(a) = \frac{4}{6} = \frac{2}{3}.$$

При использовании классической формулы вероятности в решении конкретных задач числовые значения входящих в формулу величин N и M не всегда очевидны. Часто их определение требует применения правил и формул *комбинаторики* — специального раздела математики, изучающего задачи составления тех или иных комбинаций из заданного множества элементов. Отметим, что сами

по себе комбинаторные задачи часто возникают и в правоприменительной деятельности; например, классификация причин преступности по степени их сходства, составление вариантов расследования сложных многоэпизодных дел и т.д.

8.2. Правила и формулы комбинаторики при вычислении вероятностей

1. ***Правило суммы:*** если элемент x можно выбрать n_x способами и если после его выбора элемент y можно выбрать n_y способами, то выбор «либо x, либо y» можно осуществить $n_x + n_y$ способами.

2. ***Правило произведения:*** если элемент x можно выбрать n_x способами и если после его выбора элемент y можно выбрать n_y способами, то выбор упорядоченной пары (x, y) можно осуществить $n_x n_y$ способами.

Пример 8.1.

Различающиеся только цветом $n_x + n_y$ шаров распределены по двум урнам: в первой урне n_x шаров, во второй n_y. Выберем случайным образом урну (это можно сделать так: подбросим монету и при выпадении орла выберем первую урну; цифры — вторую), а затем из нее выберем случайным образом шар (так как шары различаются только цветом, то это можно сделать так: перемешать шары и, закрыв глаза, вытащить один). Так как заранее не известно, из какой урны будет вынут шар, то число вариантов цвета для шара, вынутого либо из первой, либо из второй урны, равно $n_x + n_y$.

Теперь случайным образом выберем шар из первой урны, а затем случайным образом выберем шар из второй урны. Так как шар, вынутый из первой урны, имеет n_x вариантов цвета и при каждом из этих вариантов шар, вынутый из второй урны, имеет n_y вариантов цвета, то различных упорядоченных пар цветов для двух вынутых шаров (упорядоченность пар цветов означает, что, например, пары «синий, белый» и «белый, синий» различны) будет $n_x n_y$.

3. ***Перестановки:***

Перестановками без повторений из n различных элементов называются все возможные последовательности этих n элементов.

Число перестановок без повторений из n элементов обозначают символом P_n и подсчитывают так:

$$P_n = n! = 1 \cdot 2 \cdot \ldots \cdot n \qquad \textbf{(8.4)}$$

(символ $n!$ читается «эн факториал»; $n!$ равен произведению натуральных чисел от 1 до n; по определению $0! = 1$).

Перестановками с повторением из n элементов k типов ($k \le n$):

число элементов 1-го типа n_1,
число элементов 2-го типа n_2,
...,
число элементов k-го типа n_k

$$\sum_{i=1}^{k} n_i = n,$$

называются все возможные последовательности исходных n элементов.

Число перестановок с повторениями обозначают символом

Пример 8.2.
Перестановки без повторений из $n = 3$ различных элементов: a, b, c таковы: a,b,c; b,a,c; b,c,a; a,c,b; c,b,a; c,a,b. Число перестановок равно 6. И согласно формуле (8.4) получим такой же результат:

$$P_3 = 3! = 1 \cdot 2 \cdot 3 = 6.$$

$\overline{P}_{n=n_1+n_2+\ldots+n_k}$ и подсчитывают так:

$$\overline{P}_{n=n_1+n_2+\ldots+n_k} = \frac{n!}{n_1!\, n_2!\, \ldots\, n_k!}. \quad \textbf{(8.5)}$$

Пример 8.3.
Перестановки элементов с повторениями из $n = 3$: a,a,b двух типов (тип «a» повторяется $n_1 = 2$ раза, тип «b» повторяется $n_2 = 1$ раз), таковы: a,a,b; a,b,a; b,a,a. Число перестановок равно 3. И согласно формуле (8.5) получим такой же результат:

$$\overline{P}_{3=2+1} = \frac{3!}{2!\ 1!} = 3.$$

Замечания.

- Если все n элементов разных типов, т.е. число типов $k = 1 + 1 + \ldots + 1 = n$, то число перестановок с повторениями равно числу перестановок без повторений. Действительно,

$$\overline{P}_{n=1+1+\ldots+1} = \frac{n!}{1!\ \ 1!\ldots 1!} = n! = P_n.$$

- Обратим внимание на то, что при любом виде перестановок (и без повторений, и с повторениями) каждая перестановка включает все n исходных элементов и одна перестановка отличается от другой только порядком следования этих элементов.

Задача 3.

По следствию должны пройти пять человек: A, B, C, D, E. Какова вероятность того, что в списке этих пяти человек, составленном случайным образом:

а) B будет следовать сразу после A;

б) B не будет перед A?

Решение.

Список из пяти человек можно составить $N = 5!$ способами — это общее число равновероятных возможностей.

а) «B *следует сразу после* A» в списках следующих видов:

- A, B, ?, ?, ? — таких списков $P_3 = 3!$, так как последовательность трех букв — трех человек C, D, E на последних трех местах — это некоторая перестановка букв C, D, E, а число таких перестановок равно $P_3 = 3!$,
- ?, A, B, ?, ? — таких списков тоже 3!,
- ?, ?, A, B, ? — таких списков тоже 3!,
- ?, ?, ?, A, B — таких списков тоже 3!.

Поэтому в соответствии с правилом суммы число списков, в которых В следует сразу после А, равно: $M = 3! + 3! + 3! + 3! = 4 \cdot 3!$ и искомая вероятность $P = M/N = (4 \cdot 3!)/5! = 1/5$.

б) «В *не будет перед* А» в списках следующих видов:

- А, $\underbrace{?, ?, ?, ?}_{\text{места для В}}$ — таких списков $P_4 = 4!$ (последовательность четырех различных букв B, C, D, E на последних четырех местах — это некоторая перестановка этих букв, а число таких перестановок равно $P_4 = 4!$),
- ?, А, $\underbrace{?, ?, ?}_{\text{места для В}}$ — таких списков $4! - 3!$ (если бы не было ограничений на расположение В, то число списков вида «?, А, ?, ?, ?» было бы равно 4!; из этого числа надо вычесть количество списков вида «В, А, ?, ?, ?», а их 3!),
- ?, ?, А, $\underbrace{?, ?}_{\text{места для В}}$ — таких списков $4! - 2 \cdot 3!$ (из 4! списков вида «?, ?, А, ?, ?» вычитаем 3! списков вида «В, ?, А, ?, ?» и 3! списков вида «?, В, А, ?, ?»),
- ?, ?, ?, А, В — таких списков 3!.

Поэтому число списков, в которых «В *не будет перед* А», $M = 4! + (4! - 3!) + (4! - 2 \cdot 3!) + 3! = 60$ и вероятность того, что в списке, составленном случайным образом, «В *не будет перед* А», $P = M/N = 60/5! = 0{,}5$.

Задача 4.

Какова вероятность получить слово «*юрист*», переставляя в случайном порядке буквы этого слова? Какова вероятность получить слово «*математика*», переставляя в случайном порядке буквы этого слова?

Решение.

В слове «*юрист*» все 5 букв разные: число перестановок этих букв равно $N = P_5 = 5!$ и лишь М = 1 вариант из 5! вариантов дает слово «*юрист*». Поэтому вероятность получить это слово $P = M/N = 1/5! = 1/120$.

В слове «*математика*» $n = 10$ букв, однако различных букв $k = 6$:
«*м*», которая повторяется $n_1 = 2$ раза,
«*а*», которая повторяется $n_2 = 3$ раза,
«*т*», которая повторяется $n_3 = 2$ раза,
«*е*», которая повторяется $n_4 = 1$ раз,
«*и*», которая повторяется $n_5 = 1$ раз,
«*к*», которая повторяется $n_6 = 1$ раз.

Поэтому перестановки букв слова «*математика*» — это перестановки с повторениями из $n = 10$ элементов $k = 6$ типов, и в соответствии с формулой (8.5) общее число таких перестановок $\bar{P}_{10=2+3+2+1+1+1} = \dfrac{10!}{2!\ 3!\ 2!\ 1!\ 1!\ 1!} = 151\,200$.

Из них только одна перестановка дает слово «*математика*»; вероятность получить это слово, случайно переставляя буквы, равна 1/151 200.

4. *Размещения:*

Размещениями без повторений из n различных элементов по m элементов ($m < n$) называются все такие последовательности m различных элементов, выбранных из исходных n, которые отличаются друг от друга или порядком следования элементов, или составом элементов.

Число размещений без повторений из n элементов по m обозначают символом A_n^m,

$$A_n^m = \frac{n!}{(n-m)!}, \qquad \textbf{(8.6)}$$

где $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$;
$(n - m)! = 1 \cdot 2 \cdot \ldots \cdot (n - m)$.

Пример 8.4.

Размещения без повторений из $n = 3$-х различных элементов: a,b,c по $m = 2$ элементов таковы: a, b; b, a; a, c; c, a; b, c; c, b. Число размещений равно 6; и согласно формуле (8.6) получим такой же результат:

$$A_3^2 = \frac{3!}{(3-2)!} = \frac{3!}{1!} = \frac{1 \cdot 2 \cdot 3}{1} = 6.$$

Размещениями с повторениями из элементов k типов по m элементов (k и m могут быть в любых соотношениях: $m<k$, $m \geq k$) называются все такие последовательности m элементов, принадлежащих исходным типам, которые отличаются друг от друга или порядком следования элементов, или составом элементов.

Число размещений с повторениями из k типов элементов по m элементов обозначают $\overline{A_k^m}$,

$$\overline{A_k^m} = k^m. \qquad \textbf{(8.7)}$$

Пример 8.5.

Размещения с повторениями из элементов двух типов ($k = 2$): тип «a» и тип «b», по $m = 3$ элементов таковы: a,a,a; b,a,a; a,b,a; a,a,b; b,b,a; b,a,b; a,b,b; b,b,b. Число размещений с повторениями равно 8; и согласно формуле (8.7) получим такой же результат:

$$\overline{A_3^2} = 2^3 = 8.$$

Замечание.

Формулой (8.7) мы пользовались и ранее, не приводя ее. Так подсчет числа строк в таблице истинности высказывания, состоящего из трех ($m = 3$) простых высказываний, каждое из которых может быть двух ($k = 2$) типов (или «и» — истинным, или «л» — ложным), или подсчет числа подмножеств множества Ω, состоящего из трех элементов $m = 3$, для каждого из которых может быть $k = 2$ варианта (или элемент войдет в подмножество, или не войдет), — это подсчет числа размещений с повторениями:

$$\overline{A_k^m} = \overline{A_2^3} = 2^3 = 8.$$

➢ ***Выборка без возвращения и выборка с возвращением***

Выборка без возвращения. Пусть имеется совокупность n элементов, пронумерованных числами 1, 2, ..., n; назовем эту совокупность *генеральной.* Случайным образом выберем элемент (этот выбор можно осуществить так: номера напишем на одинаковых карточках и, перемешав карточки, вслепую наугад вытащим одну; ее номер и будет номером отобранного элемента). Отобранный элемент отложим в сторону. Повторим выбор m раз ($m < n$), не возвращая отбираемые элементы в исходную генеральную совокупность (не возвращая отбираемые карточки обратно). В результате окажется выбранной некоторая группа из m элементов. Ее называют m — *выборкой без возвращения* из генеральной совокупности объема n. Вернем m отобранных элементов в генеральную совокупность и вновь «без возврата» отберем из n элементов m элементов и т.д. Сколько существует различных m выборок, если различными считать выборки, отличающиеся или составом номеров вошедших в них элементов, или порядком следования номеров? Число таких выборок равно числу размещений без повторений (ведь в выборке не может оказаться одинаковых номеров) из n по m:

$$A_n^m = \frac{n!}{(n-m)!}.$$

Выборка с возвращением. Из той же совокупности n элементов отберем m элементов, но перед выбором каждого следующего элемент, отобранный на предыдущем шаге, будем возвращать в исходную генеральную совокупность, предварительно запомнив его номер. Выбранную (запомненную) группу из m элементов называют m — *выборкой с возвращением* из генеральной совокупности объема n (при выборке с возвращением m и n могут находиться в любом соотношении: $m \le n$ и $m > n$). Поскольку каждый из отобранных m элементов может быть n типов: иметь номер 1, иметь номер 2, ..., иметь номер n, то число различных m выборок с возвращением равно числу размещений с повторениями (ведь в выборке могут оказаться два и более одинаковых номеров) из элементов n типов по m элементов:

$$\overline{A_n^m} = n^m .$$

Задача 5.

В фирме работают 8 человек одинаковой квалификации, среди них Иванов, Петров, Сидоров. Случайно выбранным трем из них (из восьми) поручают три различных вида работ (первому выбранному — работу перво-

го вида, второму выбранному — второго вида, третьему — третьего вида). Какова вероятность того, что работа первого вида будет поручена Иванову, второго — Петрову, третьего — Сидорову?

Решение.

Отбор трех человек из восьми в условиях задачи — это выборка без возврата, где важен не только состав отобранных людей, но и то, в каком порядке они отобраны, так как от порядка отбора зависит распределение работ. Поэтому число вариантов отбора $m = 3$ из $n = 8$ будет $N = A_8^3 = \frac{8!}{(8-3)!} = 336$, и только в одном варианте ($M = 1$) из этих 336 работа первого вида будет поручена Иванову, второго — Петрову, третьего — Сидорову. Поэтому искомая вероятность $P = M/N = 1/336$.

Задача 6.

Замок камеры хранения имеет четыре диска, каждый из которых разделен на 10 секторов; на секторах каждого из дисков написаны цифры 0, 1, 2, ..., 9. Какова вероятность открыть закрытую камеру для человека:

а) забывшего все, что он набрал на дисках, закрывая камеру;

б) помнящего только цифру, набранную на первом диске;

в) помнящего только, что ни на втором, ни на третьем, ни на четвертом диске он не набирал цифры 6?

Решение.

а) Пытаясь открыть камеру с четырьмя дисками, человек, по сути, выбирает количество цифр $m = 4$ из $n = 10$, при этом осуществляется выбор с возвратом. Общее число вариантов такого выбора $N = \overline{A_{10}^4} = 10^4$, из которых только в варианте M = 1 камера откроется. Поэтому искомая вероятность равна $1/10^4$.

б) При известной цифре на первом диске, общее число вариантов набора цифр на трех оставшихся дисках $N = \overline{A_{10}^3} = 10^3$. Искомая вероятность равна $1/10^3$.

в) На первом диске может быть набрана любая из десяти цифр. Число вариантов набора цифр (уже не из десяти, а из девяти) на трех оставшихся дисках равно $\overline{A_9^3} = 9^3$. Общее число вариантов набора цифр на четырех дисках, с учетом правила произведения, будет $N = 10 \cdot 9^3$. Искомая вероятность равна $1/(10 \quad 9^3)$.

5. *Сочетания:*

Сочетаниями без повторений из n различных элементов по m элементов ($m < n$) называются все такие последовательности m различных элементов, выбранных из исходных n, которые отличаются друг от друга составом элементов.

Сочетаниями с повторениями из элементов k типов по m элементов (k и m могут быть в любых соотношениях: $m \le k$, $m > k$) называются все такие последовательности m элементов, принадлежащих исходным типам, ко-

Число сочетаний без повторений из n элементов по m обозначают символом C_n^m.

$$C_n^m = \frac{n!}{m!(n-m)!}. \qquad \textbf{(8.8)}$$

Пример 8.6.

Сочетания без повторений из трех различных элементов, $n = 3$: a, b, c по $m = 2$ таковы: a, b; a, c; c, b (сочетания отличаются друг от друга только составом элементов, поэтому, например, последовательности «a, b» и «b, a» — это одно и то же сочетание). Число сочетаний без повторений — 3. И согласно формуле (8.8) получим такой же результат:

$$C_3^2 = \frac{3!}{2!(3-2)!} = 3.$$

торые отличаются друг от друга составом элементов.

Число сочетаний с повторениями из k типов элементов по m элементов обозначают символом $\overline{C_k^m}$.

$$\overline{C_k^m} = \frac{(k+m-1)!}{m!(k-1)!}. \qquad \textbf{(8.9)}$$

Пример 8.7.

Сочетания с повторениями из элементов двух типов, $k = 2$: тип «a» и тип «b» по $m = 3$ таковы: a, a, a; b, a, a; b, b, a; b, b, b (сочетания отличаются друг от друга только составом элементов, поэтому, например, последовательности: «b, a, a», «a, b, a» и «a, a, b» — это одно и то же сочетание). Число сочетаний с повторениями — 4. И согласно формуле (8.9) получим такой же результат

$$\overline{C_2^3} = \frac{(2+3-1)\ !}{3!\ (2-1)\ !} = \frac{4!}{3!1!} = 4.$$

Задача 7.

В примере 7.5 в качестве «голосующей коалиции» был рассмотрен Совет безопасности ООН. Каково число выигрывающих и минимальных выигрывающих коалиций в Совете безопасности?

Решение.

Напомним, выигрывающая коалиция включает «большую пятерку» и не менее двух из шести представителей малых наций. Поскольку «большая пятерка» в любой выигрывающей коалиции обязательно должна присутствовать, то вариативность выигрывающих коалиций определяется количеством (или 2, или 3, или 4, или 5, или 6) и составом вошедших в них представителей малых наций. Число вариантов выбора из 6 представителей малых наций двух представителей равно числу сочетаний (ведь порядок выбора не важен!) без повторений из $n = 6$ по $m = 2$, т.е.

$C_6^2 = \frac{6!}{2!\ (6-2)!} = 15$ — именно столько будет минимальных выигрывающих коалиций. Аналогично, число вариантов выбора из 6 представителей малых наций трех равно $C_6^3 = 20$, четырех — $C_6^4 = 15$, пяти — $C_6^5 = 6$,

шести — $C_6^6 = 1$. Окончательно, число выигрывающих коалиций в соответствии с правилом суммы равно $C_6^2 + C_6^3 + C_6^4 + C_6^5 + C_6^6 = 57$.

Задача 8.

Известно, что 5 из 40 пассажиров автобуса замешаны в похищении крупной суммы денег. На остановке к автобусу подошел инспектор уголовного розыска и заявил, что ему для обнаружения по крайней мере одного преступника достаточно произвести обыск у шести наугад выбранных пассажиров. Что руководило инспектором: риск или трезвый расчет?

Решение.

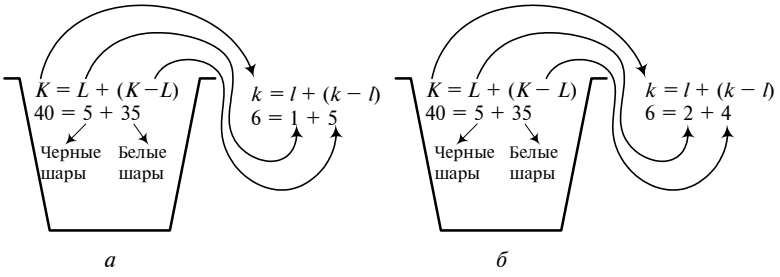
Дадим «урновую» интерпретацию условий задачи. Пусть $K = 40$ пассажиров — это 40 пронумерованных шаров в урне, из которых $L = 5$ — черные (это виновные пассажиры) и $K - L = 35$ — белые (это невиновные). Из урны наудачу берут $k = 6$ шаров (пассажиров). Число вариантов выбора $k = 6$ из $K = 40$ шаров $N = C_K^k = C_{40}^6$ (используем сочетания без повторений, так как шары пронумерованы разными числами и важны номера отобранных шаров, но не порядок). По условию в выборке должен оказаться по крайней мере один черный шар (виновный), т.е. в выборке должен оказаться:

- либо $l = 1$ черный шар и $k - l = 5$ белых,
- либо $l = 2$ черных шара и $k - l = 4$ белых,
- либо $l = 3$ черных шара и $k - l = 3$ белых,
- либо $l = 4$ черных шара и $k - l = 2$ белых,
- либо $l = 5$ черных шаров и $k - l = 1$ белый.

Число вариантов выбора $l = 1$ черного шара (виновного) из $L = 5$ черных равно $C_L^l = C_5^1$, а поскольку в каждом таком варианте должно быть выбрано $k - l = 6 - 1 = 5$ белых шаров (невиновных) из $K - L = 40 - 5 = 35$ белых, что можно сделать $C_{K-L}^{k-l} = C_{35}^5$ способами, то число вариантов выбора $l = 1$ черного шара и $k - l = 5$ белых, согласно правилу произведения, равно $C_L^l C_{K-L}^{k-l} = C_5^1 C_{35}^5$ (8.1,*а*). Аналогично число вариантов отбора:

- $l = 2$ черных и $k - l = 6 - 2 = 4$ белых шара равно $C_L^l C_{K-L}^{k-l} = C_5^2 C_{35}^4$ (рис. 8.1,*б*),
- $l = 3$ черных и $k - l = 3$ белых равно $C_5^3 C_{35}^3$,
- $l = 4$ черных и $k - l = 2$ белых равно $C_5^4 C_{35}^2$,
- $l = 5$ черных и $k - l = 1$ белых равно $C_5^5 C_{35}^1$.

Тогда число вариантов выбора 6 шаров (пассажиров) из 40, в которых окажется по крайней мере один черный шар (виновный), согласно правилу суммы, будет $M = C_5^1 C_{35}^5 + C_5^2 C_{35}^4 + C_5^3 C_{35}^3 + C_5^4 C_{35}^2 + C_5^5 C_{35}^1 = 2\,215\,220.$ И вероятность обнаружения в выборке из шести пассажиров по крайней мере одного преступника равна $P = \frac{M}{N} = \frac{2\,215\,220}{C_{40}^6} = 0{,}58,$ т.е. вероятность превысила значение 0,5, что, по-видимому, и дало основание инспектору назвать число 6.



а *б*

Рис. 8.1

Вероятность того, что при отборе «без возвращения» k шаров из K пронумерованных шаров, среди которых L черных и $K - L$ белых, в выборке окажется l черных и $k - l$ белых, рассчитывается по формуле *гипергеометрической* вероятности:

$$P = \frac{C_L^l C_{K-L}^{k-l}}{C_K^k}. \qquad \textbf{(8.10)}$$

Задача 9.

Инвестор формирует портфель ценных бумаг. Он может вложить свои деньги в акции 5 различных фирм. Сколькими способами инвестор может образовать набор из 7 акций и какова вероятность того, что в набор попадут 4 акции, принадлежащие различным фирмам?

Решение.

По условию из акций, количество типов которых $k = 5$, инвестор составляет набор из семи акций ($m = 7$), в число таких наборов может в том числе входить и набор, все 7 акций которого принадлежат какой-то одной фирме. Очевидно, что для инвестора важен только состав набора: акции каких фирм и в каких количествах они входят в набор, и совсем не важен порядок следования отобранных акций. Поэтому количество таких наборов равно числу сочетаний с повторениями из элементов $k = 5$ типов по $m = 7$ элементов: $N = \overline{C_5^7}$ или, учитывая формулу (8.9), $N = \overline{C_5^7} = \frac{(5+7-1)!}{7!(5-1)!} = 330.$

Среди этих наборов количество наборов, в каждом из которых 4 акции принадлежат различным фирмам, равно числу сочетаний без повторений из 5 элементов (5 различных фирм) по 4: $M = C_5^4 = \frac{5!}{4!\,1!} = 5.$

Искомая вероятность $P = \frac{M}{N} = \frac{C_5^4}{\overline{C_5^7}} = \frac{5}{330} = \frac{1}{66}.$

8.3. Вычисление вероятностей составных высказываний

Ранее было введено понятие несовместимых высказываний. Несовместимость высказываний, определенных на множестве логических возможностей (универсальном множестве) Ω, означает, что эти высказывания никогда не могут оказаться одновременно истинными.

Введем понятие независимости высказываний. Пусть a и b — два высказывания, определенные на универсальном множестве Ω. Предположим, что получена информация, согласно которой высказывание, скажем, a истинно. Вероятность высказывания b после получения такой информации о высказывании a называется *условной вероятностью* и обозначается символом $P_a(b)$, который следует читать «вероятность b при условии a». Высказывание b *не зависит* от a, если вероятность b при условии a равна вероятности b, т.е.

$$P_a(b) = P(b). \qquad \textbf{(8.11)}$$

Свойство независимости является *взаимным*: если b не зависит от a, то и a не зависит от b, т.е. $P_b(a) = P(a)$. При независимых a и b также независимы a и $\sim b$, $\sim a$ и b, $\sim a$ и $\sim b$.

Если $P_a(b) \neq P(b)$, то высказывания a и b *зависимы* (также зависимы a и $\sim b$, $\sim a$ и b, $\sim a$ и $\sim b$).

Пример 8.8.

Вернемся к примеру 7.2. Имеется две урны; в первой лежат один белый и два черных шара, во второй — один белый и один черный. Наугад выбирается одна из урн и из нее последовательно без возвращения вынимаются два шара.

Каждой из пяти логических возможностей (рис. 8.10,*а*) соответствует свой «путь». Отрезки, составляющие путь, назовем «ветвями». Присвоим им вероятности.

Введем высказывания: a = «выбрана первая урна», b = «первый выбранный шар белый», c = «второй выбранный шар белый» (рис. 8.2).

Рассуждаем так. Выбор наугад одной из двух урн означает, что $P(a) = P(\sim a) = \frac{1}{2}$, где $\sim a$ — это высказывание «выбрана не первая (а вторая) урна»; эти вероятности проставлены на соответствующих ветвях (рис. 8.2). Далее, если выбрана первая урна, т.е. истинно высказывание a, то $P_a(b) = \frac{1}{3}$, а $P_a(\sim b) = \frac{2}{3}$: ведь в первой урне три шара, из которых один белый и два черных. Далее, если истинно высказывание $a \wedge b$, т.е. выбрана 1-я урна и из нее взят белый шар, то в урне останется 2 шара и оба они черные, поэтому $P_{a \wedge b}(\sim c) = \frac{2}{2} = 1$.

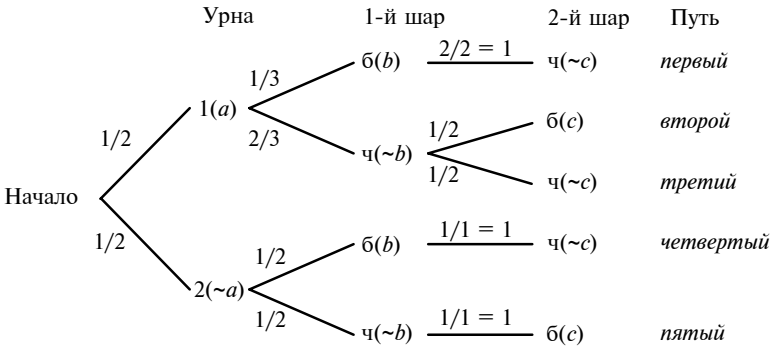


Рис. 8.2

Итак, вероятности ветвей первого пути таковы:

$$P(a) = \frac{1}{2},\ P_a(b) = \frac{1}{3},\ P_{a\wedge b}(\sim c) = 1.$$

Аналогично, вероятности ветвей:

- *второго пути* $P(a) = \frac{1}{2},\quad P_a(\sim b) = \frac{2}{3},\quad P_{a\wedge\sim b}(c) = \frac{1}{2};$
- *третьего пути* $P(a) = \frac{1}{2},\quad P_a(\sim b) = \frac{2}{3},\quad P_{a\wedge\sim b}(\sim c) = \frac{1}{2};$
- *четвертого пути* $P(\sim a) = \frac{1}{2},\quad P_{\sim a}(b) = \frac{1}{2},\quad P_{\sim a\wedge b}(\sim c) = \frac{1}{1} = 1;$
- *пятого пути* $P(\sim a) = \frac{1}{2},\quad P_{\sim a}(\sim b) = \frac{1}{2},\quad P_{\sim a\wedge\sim b}(c) = \frac{1}{1} = 1.$

Можно ли выразить условную вероятность $P_a(b)$ через «безусловные» вероятности? Да, если $P(a) \neq 0$, т.е. если высказывание a не является логически ложным. Соответствующая формула имеет вид:

$$P_a(b) = \frac{P(a \wedge b)}{P(a)},\ P(a) \neq 0. \qquad \textbf{(8.12)}$$

Обоснование формулы таково: информация о том, что высказывание a истинно, сокращает число логических возможностей универсального множества Ω, на котором определены высказывания a и b и их вероятности $P(a)$ и $P(b)$; оно будет сведено к числу возможностей множества $\mathbf{A}$ истинности высказывания a. Это, в свою очередь, приводит: во-первых, к уменьшению всех вероятностей, определенных на Ω, в $P(a)$ раз и, во-вторых, к тому, что множеством истинности высказывания b будет не $\mathbf{B}$, а $\mathbf{A} \cap \mathbf{B}$.

Поэтому $P_a(b) = \sum_{\omega_i \in A \cap B} \frac{P(\omega_i)}{P(a)} = \frac{1}{P(a)} \sum_{\omega_i \in A \cap B} P(\omega_i) = \frac{1}{P(a)} P(a \wedge b)$,

получили формулу (8.12).

Из формулы (8.12) вытекают следующие формулы:

➢ ***Формула вероятности конъюнкции двух зависимых высказываний***

$$P(a \wedge b) = P(a) P_a(b). \qquad \textbf{(8.13)}$$

➢ ***Формула вероятности конъюнкции двух независимых высказываний*** (напомним, что в этом случае $P_a(b)=P(b)$)

$$P(a \wedge b) = P(a) P(b). \qquad \textbf{(8.14)}$$

Обобщение формулы (8.13) на случай трех высказываний a, b, c имеет вид:

$$P(a \wedge b \wedge c) = P(a) P_a(b) P_{a \wedge b}(c). \qquad \textbf{(8.15)}$$

Замечание.

Для расчета $P(a \wedge b \wedge c)$ можно использовать 3! = 6 тождественных формул, в том числе, например, такую:

$$P(a \wedge b \wedge c) = P(c \wedge a \wedge b) = P(c) P_c(a) P_{c \wedge a}(b).$$

Обобщение формулы (8.14) на случай трех независимых в совокупности высказываний a, b, c (a, b, c — независимы в совокупности, если независимы a и b, a и c, b и c, $a \wedge b$ и c, $a \wedge c$ и b, $b \wedge c$ и a) имеет вид:

$$\mathrm{P}(a \wedge b \wedge c) = P(a) P(b) P(c). \qquad \textbf{(8.16)}$$

Пример 8.9.

В примере 8.8 были приписаны вероятности ветвям всех путей дерева логических возможностей (рис. 8.2). Используя введенные в примере высказывания a, b и c, найдем вероятность каждой логической возможности:

№ возможности	*Высказывание*	*Вероятность*
1	$a \wedge b \wedge \sim c$	$P(a) P_a(b) P_{a \wedge b}(\sim c) = \frac{1}{2} \cdot \frac{1}{3} \cdot 1 = \frac{1}{6}$
2	$a \wedge \sim b \wedge c$	$P(a) P_a(\sim b) P_{a \wedge \sim b}(c) = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{6}$
3	$a \wedge \sim b \wedge \sim c$	$\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{6}$
4	$\sim a \wedge b \wedge \sim c$	$\frac{1}{2} \cdot \frac{1}{2} \cdot 1 = \frac{1}{4}$
5	$\sim a \wedge \sim b \wedge c$	$\frac{1}{2} \cdot \frac{1}{2} \cdot 1 = \frac{1}{4}$

Заметим, логические возможности не равновероятны. Однако равновероятны возможности 1, 2, 3, соответствующие высказыванию a = «выбрана первая урна»; вероятность каждой из них равна 1/6. Аналогично, равнове-

роятны возможности 4 и 5, соответствующие высказыванию $\sim a$ = «выбрана вторая урна»; вероятность каждой из них равна 1/4.

Из рассмотренного выше алгоритма приписывания высказываниям вероятностей вытекают следующие формулы:

➢ ***Формула вероятности дизъюнкции двух несовместимых высказываний:***

$$P(a \vee b) = P(a) + P(b). \qquad \textbf{(8.17)}$$

Действительно, множеством истинности высказывания $a \vee b$ является множество $\mathbf{A} \cup \mathbf{B}$, где $\mathbf{A}$ и $\mathbf{B}$ — множества истинности соответственно высказываний a и b, и в соответствии с (8.2)

$$P(a \vee b) = \sum_{\omega_i \in \mathbf{A} \cup \mathbf{B}} P(\omega_i).$$

Из несовместимости же a и b следует, что $\mathbf{A}$ и $\mathbf{B}$ не имеют общих точек (рис. 7.18,*а*), поэтому

$$\sum_{\omega_i \in \mathbf{A} \cup \mathbf{B}} P(\omega_i) = \sum_{\omega_i \in \mathbf{A}} P(\omega_i) + \sum_{\omega_i \in \mathbf{B}} P(\omega_i) = P(a) + P(b).$$

Окончательно $P(a \vee b) = P(a) + P(b)$.

➢ ***Формула вероятности дизъюнкции двух совместимых высказываний:***

$$P(a \vee b) = P(a) + P(b) - P(a \wedge b). \qquad \textbf{(8.18)}$$

Действительно, множества истинности $\mathbf{A}$ и $\mathbf{B}$ совместимых высказываний имеют общие точки (рис. 7.18,*б*) и в этом случае

$$\sum_{\omega_i \in \mathbf{A} \cup \mathbf{B}} P(\omega_i) = \sum_{\omega_i \in \mathbf{A}} P(\omega_i) + \sum_{\omega_i \in \mathbf{B}} P(\omega_i) - \sum_{\omega_i \in \mathbf{A} \cap \mathbf{B}} P(\omega_i) \text{ или}$$

$$P(a \vee b) = P(a) + P(b) - P(a \wedge b).$$

➢ ***Формула вероятности отрицания высказывания:***

$$P(\sim a) = 1 - P(a). \qquad \textbf{(8.19)}$$

Действительно, с одной стороны противоположные высказывания a и $\sim a$ несовместимы и согласно (8.17): $P(a \vee \sim a) = P(a) + P(\sim a)$. С другой стороны, высказывание $a \vee \sim a$ — логически истинное, поэтому $P(a \vee \sim a) = 1$. Окончательно $P(a) + P(\sim a) = 1$ или $P(\sim a) = 1 - P(a)$.

Обобщение формулы (8.17) на случай трех попарно несовместимых высказываний a, b, c имеет вид

$$P(a \vee b \vee c) = P(a) + P(b) + P(c). \qquad \textbf{(8.20)}$$

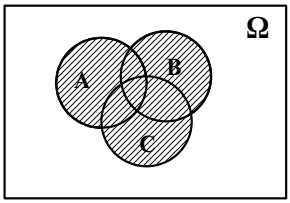
Замечание.

Из попарной несовместимости трех высказываний следует несовместимость всех трех; однако обратное утверждение неверно: при несовместимости a, b, c возможна их попарная совместимость (см. пример 6).

Обобщение формулы (8.18) на случай трех высказываний имеет вид:

$$P(a\vee b\vee c) = P(a) + P(b) + P(c) - P(a\wedge b) - P(a\wedge c) - P(b\wedge c) + P(a\wedge b\wedge c). \quad \textbf{(8.21)}$$

В справедливости этой формулы нетрудно убедиться, используя изображенные на рис. 8.3 множества **A**, **B**, **C** истинности высказываний a, b, и c и множество $\mathbf{A}\cup\mathbf{B}\cup\mathbf{C}$ (оно заштриховано) истинности высказывания $a\vee b\vee c$.



$\mathbf{A}\cup\mathbf{B}\cup\mathbf{C}$

Рис. 8.3

Задача 10.

В группе 9 человек, из которых положительные оценки имеют:

6 человек — по юриспруденции ($=a$),
5 — по математике ($=b$),
7 — по информатике ($=c$),
4 — по юриспруденции и математике ($=a\wedge b$),
2 — по юриспруденции и информатике ($=a\wedge c$),
3 — по математике и информатике ($=b\wedge c$),
1 — по всем трем предметам ($=a\wedge b\wedge c$).

Если ли в этих сведениях ошибка?

Решение.

По условию задачи высказывания a, b и c совместимы как попарно, так и все три. Поэтому общие точки (логические возможности) будут иметь как любая пара множеств **A**, **B**, **C** истинности этих высказываний, так и все три (рис. 8.3). В группе 9 человек, $P(a) = 6/9$, $P(b) = 5/9$, $P(c) = 7/9$, $P(a\wedge b) = 4/9$, $P(a\wedge c) = 2/9$, $P(b\wedge c) = 3/9$, $P(a\wedge b\wedge c) = 1/9$ и в соответствии с (8.21):

$$P(a\vee b\vee c) = \frac{6}{9}+\frac{5}{9}+\frac{7}{9}-\frac{4}{9}-\frac{2}{9}-\frac{3}{9}+\frac{1}{9} = \frac{10}{9} = 1\frac{1}{9}.$$

Получили: вероятность $P(a\vee b\vee c) > 1$, чего быть не может. Следовательно, в сведениях есть ошибка.

Задача 11.

Жюри состоит из трех человек X, Y, Z; X и Y, каждый с вероятностью $p = 0{,}8$, принимают правильное решение, а Z для вынесения решения подбрасывает монету. Члены жюри действуют независимо. Решение принимается большинством голосов. Какова вероятность правильного решения?

Решение.

Введем высказывания:

a = «X примет правильное решение», $P(a) = 0{,}8$, $P(\sim a) = 0{,}2$;

b = «Y примет правильное решение», $P(b) = 0{,}8$, $P(\sim b) = 0{,}2$;

c = «Z примет правильное решение», $P(c) = 0{,}5$, $P(\sim c) = 0{,}5$.

Правильное решение будет принято, если правильное решение будет принято какими-то двумя членами жюри или всеми тремя: правильное решение примут X, Y, но не Z; или X, Z, но не Y; или Y, Z, но не X; или X, Y и Z, т.е. будет истинно высказывание: $(a \wedge b \wedge \sim c) \vee (a \wedge \sim b \wedge c) \vee (\sim a \wedge b \wedge c) \vee (a \wedge b \wedge c)$. Поскольку компоненты этой дизъюнкции *попарно несовместимы,* а компоненты конъюнкций, расположенных в каждой скобке, *независимы* по условию задачи, то искомая вероятность

$$P((a \wedge b \wedge \sim c) \vee (a \wedge \sim b \wedge c) \vee (\sim a \wedge b \wedge c) \vee (a \wedge b \wedge c)) =$$

$$= P(a \wedge b \wedge \sim c) + P(a \wedge \sim b \wedge c) + P(\sim a \wedge b \wedge c) + P(a \wedge b \wedge c) =$$

$$= P(a)P(b)P(\sim c) + P(a)P(\sim b)P(c) + P(\sim a)P(b)P(c) + P(a)P(b)P(c) =$$

$$= 0{,}8 \cdot 0{,}8 \cdot 0{,}5 + 0{,}8 \cdot 0{,}2 \cdot 0{,}5 + 0{,}2 \cdot 0{,}8 \cdot 0{,}5 + 0{,}8 \cdot 0{,}8 \cdot 0{,}5 = 0{,}8.$$

Дерево логических возможностей с указанием вероятностей путей изображено на рис. 8.4; пути, ведущие к принятию положительного решения, и их вероятности выделены.

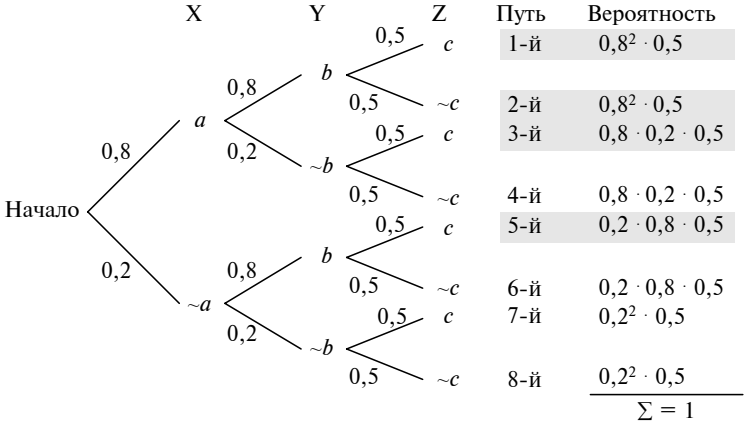


Рис. 8.4

Приведем (без вывода) еще ряд наиболее часто используемых формул вычисления вероятностей.

➢ ***Формула полной вероятности***

$$P(a) = P(h_1)P_{h_1}(a) + P(h_2)P_{h_2}(a) + \ldots + P(h_n)P_{h_n}(a) \qquad \textbf{(8.22)}$$

используется, если выполняются следующие условия

1) высказывание a истинно лишь при истинности одного из высказываний h_1, h_2, ..., h_n, называемых гипотезами;
2) гипотезы h_1, h_2, ..., h_n попарно несовместимы;
3) дизъюнкция $h_1 \vee h_2 \vee \ldots \vee h_n$ гипотез — логически истинное высказывание.

(8.23)

Замечание.

Выполнение второго и третьего условий тождественно требованию:

$$P(h_1) + P(h_2) + \ldots + P(h_n) = 1.$$

Множества истинности высказываний, удовлетворяющих условиям (8.23), для случая трех гипотез ($n = 3$) изображены на рис. (8.5). В силу попарной несовместимости гипотез никакая пара множеств $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ их истинности не имеет общих точек; а в силу логической истинности дизъюнкции гипотез множество истинности дизъюнкции $\mathbf{H}_1 \cup \mathbf{H}_2 \cup \mathbf{H}_3 = \mathbf{\Omega}$, где $\mathbf{\Omega}$ — универсальное множество логических возможностей, на котором определены все четыре высказывания: a, h_1, h_2, h_3.

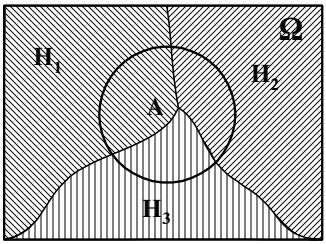


Рис. 8.5

➢ ***Формула Байеса***

$$P_a(h_i) = \frac{P(h_i)P_{h_i}(a)}{P(a)}, \qquad i = 1 \div n \qquad \textbf{(8.24)}$$

используется, если в дополнение к условиям (8.23) выполняется условие:

4) имеется информация о том, что высказывание a будет истинным. **(8.25)**

Задача 12.

В пирамиде 10 винтовок, из которых 4 с оптическим прицелом. Вероятность того, что стрелок поразит мишень при выстреле из винтовки с оптическим прицелом равна 0,95; для винтовки без оптического прицела эта вероятность равна 0,8. Стрелок поразит мишень из наудачу взятой винтовки. Что вероятнее: стрелок будет стрелять из винтовки с оптическим прицелом или без него?

Решение:

Пусть a = «стрелок поразит мишень из наудачу взятой винтовки», h_1 = = «наудачу взятая стрелком винтовка — с оптическим прицелом», h_2 = «наудачу взятая стрелком винтовка — без оптического прицела». По условию задачи:

$$P(h_1)=0,4;\ P(h_2)=0,6;\quad P_{h_1}(a)=0,95;\ P_{h_2}(a)=0,8.$$

Требования (8.23) и (8.25) выполняются: a может быть истинным лишь при истинности h_1 или h_2; $P(h_1) + P(h_2) = 1$; есть информация об истинности a.

Используем формулы (8.22) и (8.24):

$$P(a)=P(h_1)P_{h_1}(a)+P(h_2)P_{h_2}(a)=0,4\cdot 0,95+0,6\cdot 0,8=0,86;$$

$$P_a(h_1)=\frac{P(h_1)\cdot P_{h_1}(a)}{P(a)}=\frac{0,4\cdot 0,95}{0,86}=\frac{19}{43};$$

$$P_a(h_2)=\frac{P(h_2)\cdot P_{h_2}(a)}{P(a)}=\frac{0,6\cdot 0,8}{0,86}=\frac{24}{43}$$

(обратим внимание на то, что $P_a(h_2) + P_a(h_1) = 1$).

Так как $P_a(h_2) > P_a(h_1)$, то более вероятно, что стрелок будет стрелять из винтовки без оптического прицела.

➢ ***Формула Бернулли*** используется в следующих условиях:

1) проводится n *независимых* испытаний (независимость испытаний означает, что исходы любых из них не влияют на исходы других);
2) каждое испытание имеет два исхода: один исход называют «успехом», а другой — «неудачей»;
3) вероятность p «успеха» в отдельно взятом, или единичном, испытании постоянна и от испытания к испытанию не меняется (это условие обеспечивается проведением испытаний примерно в одинаковых, или иначе — в типичных, условиях).

(8.26)

Испытания, удовлетворяющие условиям (8.26), называются *испытаниями Бернулли*; формула Бернулли имеет следующий вид

$$P_n(m)=C_n^m p^m q^{n-m}, \qquad \textbf{(8.27)}$$

где $P_n(m)$ — вероятность появления m успехов в n испытаниях ($m = 0$, 1, ..., n), $C_n^m = \dfrac{n!}{m!(n-m)!}$ — число сочетаний из n по m, $q = 1 - p$ — вероятность «неудачи» в единичном испытании.

Используя (8.27), рассчитаем вероятности того, что число успехов $m = 0, 1, 2, ..., n$:

m	0	1	...	n	
$P_n(m) =$ $= C_n^m p^m q^{n-n}$	$C_n^0 p^0 q^{n-0} =$ $= q^n$	$C_n^1 p^1 q^{n-1} =$ $= npq^{n-1}$	...	$C_n^n p^n q^{n-n} =$ $= p^n$	$\sum = 1$

(8.28)

Замечание.

Сумма всех вероятностей — это вероятность логически истинного высказывания «при проведении n испытаний число успехов равно 0 или 1, или 2, ..., или n», поэтому она равна 1.

Ряд (8.28) называют *рядом распределения вероятностей Бернулли* по числу успехов или *биномиальным рядом распределения*.

Число успехов m^*, которому соответствует наибольшая вероятность, называют *наивероятнейшим числом*; m^* можно найти, не составляя ряда (8.28), следующим образом:

- если $np + p$ — дробное число, то m^* — целое число, лежащее в интервале $(np - q, np + p)$;
- если $np + p$ — целое число, то наивероятнейших чисел будет два: $m_1^* = np - q$ и $m_2^* = np + p$ (вероятности этих чисел будут одинаковыми, $P_n(m_1^*) = P_n(m_2^*)$, и наибольшими в сравнении с другими вероятностями ряда (8.28)).

Представим, что проведено достаточно много серий испытаний по n испытаний в каждой серии и в каждой серии зафиксировано число успехов:

	1-я серия	*2-я серия*	*3-я серия*	...
Число испытаний в серии	n	n	n	...
Число успехов в серии	m_1	m_2	m_3	...

Правомочен вопрос: каково среднее число успехов в одной серии. (Это число обозначим $\overline{m}$, в теории вероятностей его называют *математическим ожиданием числа успехов* и обозначают Mm). И далее, поскольку в n испытаниях успехов может быть 0, 1, 2, ..., n, то правомочен вопрос: каков в среднем разброс этих чисел (конечно, с

учетом вероятностей их появления) вокруг среднего числа $\overline{m}$. Характеристику этого разброса называют *средним квадратическим отклонением числа успехов* и обозначают греческой буквой σ_m — «сигма»; иногда в качестве характеристики разброса используют *дисперсию* числа успехов $Dm = \sigma_m^2$.

Для биномиального ряда распределения:

$$\overline{m}\ (\text{или } Mm) = np,\ Dm = npq,\ \sigma_m = \sqrt{npq}\ . \qquad \textbf{(8.29)}$$

Задача 13.

Примерно 20% судебных дел — это дела по обвинению в краже. В порядке прокурорского надзора проверено 4 наудачу отобранных дела. а) К а к о в а вероятность появления среди отобранных дел хотя бы одного дела о краже? б) К а к о в о наивероятнейшее число дел о краже среди отобранных и какова вероятность этого числа? в) К а к о в ы среднее число дел о краже и среднее квадратическое отклонение числа дел о краже среди четырех дел?

Решение.

В условиях задачи: число испытаний $n = 4$, «успех» — наугад взятое дело — это дело о краже, вероятность успеха $p = 0{,}2$, вероятность неудачи $q = 0{,}8$.

а) Судя по вопросу, число m успехов может равняться 1 или 2, или 3, или 4 и никак не может быть равно 0. Так как $P_4(0) + P_4(1) + P_4(2) + P_4(3) + P_4(4) = 1$, то искомая вероятность $P_4(1 \le m \le 4) = 1 - P_4(0) = 1 - C_4^0\, 0{,}2^0 0{,}8^{4-0} = 1 - 0{,}8^4 = 1 - 0{,}4096 = 0{,}5904$.

б) Так как $np + p = 4 \cdot 0{,}2 + 0{,}2 = 1$ — целое число, то наивероятнейших чисел будет два:

$m_1^* = np - q = 4 \cdot 0{,}2 - 0{,}8 = 0$ и $m_2^* = np + p = 1$. Вероятности этих чисел $P_4(0) = 0{,}4096$, $P_4(1) = C_4^1 0{,}2^1 0{,}8^3 = 0{,}4096$. Как и следовало ожидать, вероятности одинаковы, и они будут наибольшими, в чем нетрудно убедиться, составив ряд распределения (8.28):

m	0	1	2	3	4	
$P_4(m)$	0,4096	0,4096	0,1536	0,0256	0,0016	$\Sigma = 1$

в) Требуемые характеристики вычислим по формулам (8.29): $\overline{m} = np = 4 \cdot 0{,}2 = 0{,}8$ — таково среднее число дел о краже среди четырех наудачу выбранных (если наудачу взять 20 дел, то в среднем среди них будет 4 дела о кражах), $\sigma = \sqrt{npq} = \sqrt{4 \cdot 0{,}2 \cdot 0{,}8} = 0{,}8$ — таков в среднем разброс количеств дел о краже среди четырех наудачу отобранных дел около $\overline{m} = 0{,}8$ (для 20 случайно отобранных дел разброс количества дел о краже около среднего числа, равного 4, будет 1,79).

➢ ***Формула Пуассона***

$$P(m)=\frac{(a)^m}{m!}\mathrm{e}^{-a},\ m=0,1,...,\ n, \qquad \textbf{(8.30)}$$

где $P(m)$ — вероятность появления m успехов в n испытаниях, $a = np$, e = 2,71828... — основание натурального логарифма. Формула дает хорошее приближение к вероятностям, рассчитанным по формуле Бернулли (8.27), если число испытаний n *велико* (n — несколько сотен), а вероятность p успеха в единичном испытании *мала*, близка к нулю. Вследствие малости вероятности p формулу Пуассона называют также *формулой редких явлений*.

При бесконечно большом числе n испытаний *ряд распределения вероятностей Пуассона* по числу успехов или *пуассоновский ряд распределения* таков:

m	0	1	2	...	
$P(m)$	$\frac{a^0}{0!}\mathrm{e}^{-a}=\mathrm{e}^{-a}$	$\frac{a^1}{1!}\mathrm{e}^{-a}=a\mathrm{e}^{-a}$	$\frac{a^2}{2!}\mathrm{e}^{-a}$	...	$\Sigma=1$

(8.31)

Обратим внимание на то, что этот ряд, в отличие от биномиального ряда (8.28), — бесконечный, но сумма его вероятностей, как и для конечного ряда (8.28), равна единице.

При пуассоновском распределении*:*

- среднее число успехов ($\overline{m}$ или Mm) и дисперсия числа успехов (Dm или σ_m^2) равны числу a:

$$\overline{m}\ \ (\text{или } Mm) = Dm = a;\ \sigma_m = \sqrt{a}\,; \qquad \textbf{(8.32)}$$

- наивероятнейшее число успехов m^* находят так: если a — дробь, то m^* целое число из интервала $(a-1,\ a)$; если a — целое, то наивероятнейших чисел два: $m_1^* = a-1$ и $m_2^* = a$.

Задача 14.

Примерно 0,1% судебных дел — это дела по обвинению в убийстве. Проверено 200 наудачу взятых судебных дел. Какова вероятность того, что среди них дел об убийстве будет: а) 0; 1; 2; 3; б) хотя бы одно в) более трех?

Решение.

По условию $n = 200$, $p = 0{,}001$ — есть основания использовать формулу Пуассона; $a = np = 0{,}2$.

а) Требуемые вероятности вычислим по формуле Пуассона (8.30), и для сопоставления те же вероятности вычислим по формуле Бернулли (8.27) (с точностью до четырех десятичных разрядов):

m	0	1	2	3	
$P(m)=\frac{0{,}2^m}{m!}\mathrm{e}^{-0{,}2}$	0,8187	0,1638	0,0164	0,0010	Σ = 0,9999
$P_{200}(m)=C_{200}^m(0{,}001)^m(0{,}999)^{200-m}$	0,8186	0,1639	0,0163	0,0011	Σ = 0,9999

Различий между вероятностями Пуассона и Бернулли практически нет (они будут тем меньше, чем больше n и меньше p). Итоговые суммы вероятностей не равны 1, поскольку по условию задачи число m дел об убийстве может быть равным не только 0, 1, 2, 3, но и 4, 5, ..., 200.

б) Судя по вопросу, m может быть равным или 1, или 2, ..., или 200, иначе $1 \le m \le 200$, но не 0. Поэтому искомая вероятность P_{200} $(1 \le m \le 200) = 1 - P_{200}$ $(m = 0) = 1 - 0{,}8187 = 0{,}1813$.

в) P_{200} $(3 < m \le 200) = 1 - P_{200}$ $(0 \le m \le 3) = 1 - 0{,}9999 = 0{,}0001$.

Формулу Пуассона в несколько ином виде, а именно:

$$P_t(m)=\frac{(\lambda t)^m}{m!}\mathrm{e}^{-\lambda t},\ \text{где } m = 0,\ 1,\ ..., \qquad \textbf{(8.33)}$$

используют для подсчета $P_t(m)$ — вероятности того, что за промежуток времени длиной t наступит m событий *простейшего потока* — это поток однородных событий, происходящих в случайные моменты времени, обладающий тремя довольно типичными для многих ситуаций с в о й с т в а м и:

- одновременное наступление двух или более событий практически невозможно;
- поток установившийся, стационарный с *интенсивностью,* равной λ (интенсивность — это среднее число событий потока, происходящих в единицу времени);
- поток без последействия, т.е. на вероятность появления любого числа событий в любой промежуток времени не влияет ни число событий, ни моменты их появления вне этого промежутка.

Задача 15.

При установившейся на протяжении суток криминогенной обстановке в городе в среднем за сутки происходят 15 правонарушений. К а к о в о наивероятнейшее число правонарушений за сутки, за 1 час и к а к о в ы вероятности этих чисел? Предполагается, что поток правонарушений простейший.

Решение.

По условию количество правонарушений в сутки = 15. При t = 1 сут. наивероятнейшее число правонарушений $m_1^* = \lambda t - 1 = 14$ и $m_2^* = \lambda t = 15$. Вероятности этих чисел максимальны в сравнении с вероятностями любого другого количества преступлений и равны:

$$P_{1\text{сут}}(14)=\frac{15^{14}}{14!}\mathrm{e}^{-15}=\frac{15^{14}\cdot 15}{14!\cdot 15}\mathrm{e}^{-15}=\frac{15^{15}}{15!}\mathrm{e}^{-15}=P_{1\text{сут}}(15),$$

$$P_{1\text{сут}}(14)=P_{1\text{сут}}(15)=0{,}102\,436.$$

При $t = 1$ ч $= 1/24$ сут. наивероятнейшее число правонарушений — целое число из интервала $\left(15\cdot\frac{1}{24}-1,\ 15\cdot\frac{1}{24}\right)$; это число $m^* = 0$. Его вероятность

$$P_{1/24}(0)=\frac{\left(15\cdot\frac{1}{24}\right)^0}{0!}\mathrm{e}^{-15\cdot\frac{1}{24}}=\mathrm{e}^{-0{,}625}=0{,}535\,261.$$

Биномиальное (8.28) и пуассоновское (8.31) распределения довольно часто используются в решении задач правоприменительной деятельности, но, конечно, ими не ограничиваются все возможные распределения вероятностей.

➢ ***Понятие случайной величины.***

Случайной величиной (СВ) назовем переменную X, множество значений которой известно, но не известно, какое именно (одно из них) обязательно появится при проведении опыта, иначе — при наблюдении переменной X. Например, СВ является число m успехов в n испытаниях (множество значений этого числа известно — это $\{0, 1, 2, ..., n\}$, но каким именно будет число успехов при проведении опыта, состоящего в n испытаниях, сказать до проведения опыта нельзя). СВ является и число происшедших событий простейшего потока, с той лишь разницей, что множество значений этого числа будет не конечным, а бесконечным — $\{0, 1, 2, ...\}$. Однако в обоих случаях значения величины «изолированы» друг от друга; такую величину называют *дискретной*. Если величина может принять любое значение из одного или нескольких отрезков, то ее называют *непрерывной*. Так, возраст правонарушителя в принципе может быть любой точкой, например, на отрезке [14, 80], поэтому возраст — непрерывная величина. Однако если возраст измерять полным числом лет, то возраст — дискретная величина.

Говорят, что дискретная СВ X задана, если известно не только множество ее значений, но и вероятности этих значений; иначе, если известно распределение вероятностей по значениям величины X. Ряд

x	x_1	x_2	...	x_v	
p	p_1	p_2	...	p_v	$\Sigma = 1$

, **(8.34)**

где x_1, x_2, ..., x_ν, — расположенные в порядке возрастания «все» значения СВ X (здесь предполагается, что число этих значений конечно), а p_1, p_2, ..., p_ν, — вероятности этих значений, называют *рядом распределения вероятностей* СВ X.

Среднее значение, иначе математическое ожидание *СВ X* находят по формуле:

$$MX = x_1p_1 + ... + x_\nu p_\nu, \qquad \textbf{(8.35)}$$

дисперсию СВ X — по одной из двух тождественных формул:

$$\left.\begin{aligned} DX &= (x_1 - MX)^2 p_1 + (x_2 - MX)^2 p_2 + ... + (x_\nu - MX)^2 p_\nu; \\ DX &= x_1^2 p_1 + x_2^2 p_2 + ... + x_\nu^2 p_\nu - (MX)^2, \end{aligned}\right\} \qquad \textbf{(8.36)}$$

среднее квадратическое отклонение СВ X — характеристику среднего разброса значений СВ X вокруг MX — по формуле:

$$\sigma_X = \sqrt{DX}\ . \qquad \textbf{(8.37)}$$

Подставив в (8.35) — (8.37) составляющие биномиального ряда распределения (8.28) или пуассоновского (8.31) — в последнем случае число слагаемых бесконечно, можно получить выражения (8.29) или (8.32) соответствующих характеристик: математического ожидания Mm, дисперсии Dm и среднего квадратического отклонения σ_m числа успехов.

Типичным примером непрерывной СВ является *нормально распределенная* СВ X, вероятность попадания которой в малый интервал длиной h с центром в точке x

$$P\,(X \in h) = hf\,(x),$$

где $f(x) = \dfrac{1}{\sigma_X\sqrt{2\pi}}\,\mathrm{e}^{-\dfrac{(x-MX)^2}{2\sigma_X^2}}$

— функция плотности распределения «нормальных» вероятностей (ее график изображен на рис. 8.6); MX, σ_X — математическое ожидание и среднее квадратическое отклонение нормально распределенной СВ X.

Для нормально распределенной СВ X

$$P(|X - MX| < \varepsilon) = \Phi(\varepsilon/\sigma_X), \qquad \textbf{(8.38)}$$

где $\Phi(\varepsilon/\sigma_X)$ — значение функции $\Phi\,(z) = \dfrac{2}{\sqrt{2\pi}}\int\limits_0^z \mathrm{e}^{\frac{-x^2}{2}}\,dx$

при $z = \varepsilon/\sigma_X$.

Таблицы значений этой функции при различных $z \geq 0$ имеются, например, в работе В.Н. Калининой и В.Ф. Панкина[1]. Приведем значения $\Phi(z)$ лишь при некоторых z:

z	1	1,65	1,96	2	2,58	3
$\Phi(z)$	0,6827	0,9011	0,9500	0,9544	0,9901	0,9973

(8.39)

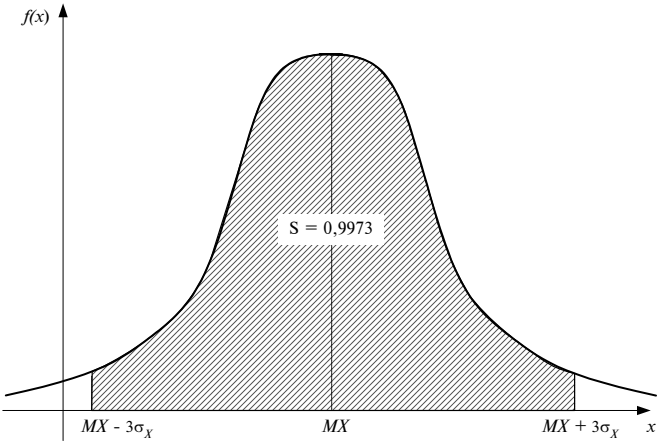


Рис. 8.6

В частности, при $\varepsilon = 3\sigma_X$ из (8.38) получим

$$P\left(\left|X - MX\right| < 3\sigma_X\right) = \Phi\left(3\sigma_X / \sigma_X\right) = \Phi(3) = 0{,}9973; \qquad \textbf{(8.40)}$$

геометрически эта вероятность интерпретируется как заштрихованная на рис. 8.6 площадь. Соотношение (8.40) носит название *«правила трех сигм»* для нормально распределенной СВ X.

Более подробно с дискретными и непрерывными СВ можно ознакомиться в работе В.Н. Калининой и В.Ф. Панкина, а также в работе В.А. Колемаева и В.Н. Калининой[2].

➢ ***Формула Лапласа.*** При большом числе n испытаний вероятность того или иного числа m ($m = 0, 1, ..., n$) успехов будет малым числом. Так, при стократном подбрасывании монеты ($n = 100$) наивероятнейшее число выпадений герба $m^* = np = 100 \cdot 0{,}5 = 50$, а рассчитанная по формуле Бернулли (8.27) вероятность этого числа

[1] *Калинина В.Н.*, *Панкин В.Ф.* Математическая статистика. — М.: Дрофа, 2002.
[2] *Колемаев В.А.*, *Калинина В.Н.* Теория вероятностей и математическая статистика. — М.: ЮНИТИ, 2003.

$P_{100}(50) \approx 0{,}08$, и это наибольшая вероятность; вероятности других чисел будут меньше: например, вероятность $P_{100}(40) \approx 0{,}00002$. В этом случае более ценную информацию дает знание вероятности того, что абсолютная величина отклонения числа успехов m в n испытаниях от среднего числа успехов $\overline{m} = np$ не превзойдет некоторого заранее заданного числа. Нижнюю границу для этой вероятности можно получить по формуле:

$$P\left(|m - np| < z\sqrt{npq}\right) \geq 1 - \frac{1}{z^2},$$

где z — любое положительное число.

Более точное значение вероятности $P\left(|m - np| < z\sqrt{npq}\right)$ при большом числе n испытаний дает *формула Лапласа*:

$$P\left(|m - np| < z\sqrt{npq}\right) \approx \Phi(z). \qquad \textbf{(8.41)}$$

При $z = 3$, учитывая, что $\sigma_m = \sqrt{npq}$, получим $P\left(|m - np| < 3\sigma_m\right) \approx$ $\approx \Phi(3) = 0{,}9973$, т.е. получение в n испытаниях числа успехов m, абсолютная величина отклонения которого от среднего числа $\overline{m} = np$ будет меньше трех средних квадратических отклонений $3\sigma_m$, является практически достоверным событием. Это утверждение — *«правило трех сигм»* для числа успехов m в большом числе испытаний n.

С неравенством, стоящим в скобках формулы (8.41), проведем такие тождественные преобразования:

$$|m - np| < z\sqrt{npq} \rightarrow \left|p - \frac{m}{n}\right| < z\sqrt{\frac{pq}{n}} \rightarrow -z\sqrt{\frac{pq}{n}} < p - \frac{m}{n} < z\sqrt{\frac{pq}{n}} \rightarrow$$

$$\rightarrow \frac{m}{n} - z\sqrt{\frac{pq}{n}} < p < \frac{m}{n} + z\sqrt{\frac{pq}{n}}.$$

Окончательно,

$$P\left(\frac{m}{n} - z\sqrt{\frac{pq}{n}} < p < \frac{m}{n} + z\sqrt{\frac{pq}{n}}\right) \approx \Phi(z). \qquad \textbf{(8.42)}$$

Относительную долю $\hat{p} = m/n$ успешных испытаний называют *точечной оценкой вероятности* p успеха в единичном испытании, интервал

$$\left(\frac{m}{n} - z\sqrt{\frac{pq}{n}};\ \ \frac{m}{n} + z\sqrt{\frac{pq}{n}}\right) \qquad \textbf{(8.43)}$$

называют $\Phi(z)\cdot 100\%$ – ной *интервальной оценкой вероятности* p (например, при $z = 1{,}96$ получим 95%-ную интервальную оценку), а величину

$$\varepsilon = z\sqrt{\frac{pq}{n}} \qquad \textbf{(8.44)}$$

— *ошибкой выборочной вероятности* $\hat{p} = m/n$.

Замечание.

Напомним, в формулах (8.42) — (8.44) n должно быть достаточно большим числом. При неизвестной вероятности p полагают $pq \approx \hat{p}\hat{q} = \frac{m}{n}\left(1 - \frac{m}{n}\right)$.

В заключение, формулы Пуассона (8.30) и Лапласа (8.41) вытекают соответственно из теоремы Пуассона и теоремы Лапласа, с точными формулировками которых можно познакомиться в работе В.А. Колемаева и В.Н. Калининой[1], а также в работе В.Н. Тутубалина[2]. Эти теоремы наряду с ранее упоминавшимися теоремами Бернулли и Чебышева, а также ряд других теорем, касающихся изучения вероятностного поведения результатов большого числа n испытаний составляют *закон больших чисел.*

8.4. Выбор решения при неизвестных вероятностях

Выбрать решение в условиях известных вероятностей высказываний довольно просто. При неизвестных вероятностях, что типично для многих практических задач, выбрать решение можно лишь на основании экспериментальных данных. Проиллюстрируем процедуру такого рода.

Следователь X полагает, что он, побеседовав с подследственным, с 90%-ной гарантией может отличить виновного от невиновного. Его начальник Y считает, что X такой способностью не обладает. Кто из них прав? Такой вопрос не возник бы, если была бы известна истинная вероятность p отличить следователем виновного от невиновного. Однако относительно значения этой вероятности выдвинуто д в е г и п о т е з ы:

- *нулевая гипотеза* H_0: $p = 0{,}9$ (так думает X),
- *альтернативная гипотеза* H_1: $p = 0{,}5$ (так думает Y).

Предлагается провести такой эксперимент. Следователь X беседует с подследственными, число которых $n = 10$, причем начальнику Y известно, кто из них виновен, а кто — не виновен. И если число m правильных ответов будет не меньше 8, $8 \le m \le 10$, то принимается

---

[1] *Колемаев В.А., Калинина В.Н.* Теория вероятностей и математическая статистика. — М.: ЮНИТИ, 2003.

[2] *Тутубалин В.Н.* Теория вероятностей. — М.: МГУ, 1972.

гипотеза H_0, т.е. правым считается следователь; если $0 \le m < 8$, то принимается гипотеза H_1, т.е. прав начальник.

Поступив таким образом, можно совершить о ш и б к у двух родов:

- будет принята гипотеза H_1, тогда как на самом деле верной является H_0 — это ошибка первого рода, ее вероятность обозначают $\alpha: \alpha = P_{H_0}(H_1)$, где $P_{H_0}(H_1)$, — вероятность принять H_1, если на самом деле верна H_0; α называют *уровнем значимости*;
- будет принята гипотеза H_0, тогда как на самом деле верна H_1 — это *ошибка второго рода*, ее вероятность обозначают β: $\beta = P_{H_1}(H_0)$.

П р а в и л ь н о е р е ш е н и е также может быть двух родов:

- будет принята гипотеза H_0, тогда как на самом деле она верна; вероятность такого решения
$$P_{H_0}(H_0) = 1 - P_{H_0}(H_1) = 1 - \alpha;$$
- будет принята гипотеза H_1, тогда как на самом деле она верна; вероятность такого решения
$$P_{H_1}(H_1) = 1 - P_{H_1}(H_0) = 1 - \beta.$$

Верная гипотеза	*Принятая гипотеза*	
	H_0	H_1
H_0	$P_{H_0}(H_0) = 1 - \alpha$ (правильное решение)	$P_{H_0}(H_1) = \alpha$ (ошибка первого рода)
H_1	$P_{H_1}(H_0) = \beta$ (ошибка второго рода)	$P_{H_1}(H_1) = 1 - \beta$ (правильное решение)

Насколько приемлем описанный выше эксперимент для каждой из конфликтующих сторон?

Следователь X считает, что верна гипотеза H_0: $p = 0{,}9$, и он заинтересован в том, чтобы по результатам эксперимента H_0 была принята, т.е. чтобы при испытаниях $n = 10$ число успешных было не меньше 8, $8 \le m \le 10$. Поэтому вероятность «удовлетворения его интереса» равна:

$$P_{H_0}(H_0) = P_{10}(8 \le m \le 10) = C_{10}^{8} \cdot 0{,}9^8 \cdot 0{,}1^2 + C_{10}^{9} \cdot 0{,}9^9 \times$$
$$\times 0{,}1^1 + C_{10}^{10} \cdot 0{,}9^{10} \cdot 0{,}1^0 = 0{,}93.$$

Начальник Y считает, что верна гипотеза H_1: $p = 0{,}5$, и он заинтересован в том, чтобы эта гипотеза была принята, т.е. чтобы при 10 испытаниях число успешных было меньше 8, $0 \le m < 8$. Поэтому вероятность «удовлетворения его интереса» равна:

$$P_{H_1}(H_1) = P_{10}(0 \le m < 8) = 1 - P(8 \le m \le 10) =$$
$$= 1 - \left(C_{10}^{8} \cdot 0,5^{8} \cdot 0,5^{2} + C_{10}^{9} \cdot 0,5^{9} \cdot 0,5^{1} + C_{10}^{10} \cdot 0,5^{10} \cdot 0,5^{0}\right) = 0,945.$$

Вероятности для X и для Y примерно одинаково высоки, поэтому они оба согласятся разрешить существующие между ними разногласия с помощью описанного выше эксперимента. При таких высоких вероятностях правильных решений вероятности ошибочных решений невысоки: вероятность ошибки первого рода равна

$$\alpha = P_{H_0}(H_1) = 1 - P_{H_0}(H_0) = 1 - 0,93 = 0,07,$$

а вероятность ошибки второго рода

$$\beta = P_{H_1}(H_0) = 1 - P_{H_1}(H_1) = 1 - 0,945 = 0,055.$$

Рассмотрим еще одну процедуру выбора решений при неизвестных вероятностях на основе результатов достаточно большого числа испытаний.

Истинная вероятность p успешности испытания неизвестна. Однако интуиция подсказывает, что, скорее всего, p равно числу p_0. Следует ли принять гипотезу H_0: $p = p_0$ или нет?

Для получения ответа на этот вопрос в «стандартных» схемах проверки гипотез такого типа требуется:

- *во-первых*, провести n испытаний Бернулли, зафиксировать число m успешных и найти их относительную долю $\hat{p} = \dfrac{m}{n}$;
- *во-вторых,* сформулировать исходя из содержания задачи альтернативную гипотезу H_1 (H_1: $p \ne p_0$ или H_1: $p < p_0$, или H_1: $p > p_0$);
- *в-третьих*, задать числовое значение вероятности α ошибки первого рода; обычно для α используются значения: 0,1; 0,05; 0,01; 0,005; 0,001.

Принцип проверки гипотезы H_0 такой: если происходит то, что при справедливости H_0 происходить не должно, то H_0 отклоняют (принимают H_1); в противном случае — H_0 принимают. Рассмотрим алгоритмы проверки гипотезы H_0: $p = p_0$ для *трех видов* альтернативной гипотезы. При этом будем считать, что n достаточно велико.

1) H_0: $p = p_0$, H_1: $p \ne p_0$.

Если предполагаемое значение p_0 вероятности p не попадает внутрь интервальной оценки (8.43) вероятности, чего не должно происходить при справедливости H_0, т.е.

если $p_0 \notin \left(\frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}};\ \frac{m}{n} + z\sqrt{\frac{p_0 q_0}{n}} \right)$,

то H_0 отклоняют (принимают H_1);

если $p_0 \in \left(\frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}};\ \frac{m}{n} + z\sqrt{\frac{p_0 q_0}{n}} \right)$, **(8.45)**

то H_0 принимают.

Здесь $q_0 = 1 - p_0$, z — число, при котором функция $\Phi(z) = 1 - \alpha$.

2) H_0: $p = p_0$, H_1: $p > p_0$.

Если $p_0 < \frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}}$, то H_0 отклоняют (принимают H_1); **(8.46)**

если $p_0 > \frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}}$, то H_0 принимают.

Здесь z — число, при котором $\Phi(z) = 1 - 2\alpha$.

3) H_0: $p = p_0$, H_1: $p < p_0$.

Если $p_0 > \frac{m}{n} + z\sqrt{\frac{p_0 q_0}{n}}$, то H_0 отклоняют (принимают H_1); **(8.47)**

если $p_0 < \frac{m}{n} + z\sqrt{\frac{p_0 q_0}{n}}$, то H_0 принимают.

Здесь z — число, при котором $\Phi(z) = 1 - 2\alpha$.

Рассмотренные алгоритмы позволяют, при заданной вероятности α ошибки первого рода, получить наименьшую вероятность β ошибки второго рода. Принимая гипотезу H_0, следует понимать, что это вовсе не означает, что H_0 является единственно подходящей гипотезой: просто гипотеза H_0 не противоречит результатам испытаний; однако таким же свойством наряду с H_0 могут обладать и другие гипотезы.

Задача 16.

Городская статистика раскрываемости преступлений утверждает, что раскрывается примерно 4 на каждые 10 преступлений. УВД одного из районов утверждает, что за последний месяц раскрыло 49 преступлений из 100. Случайны ли результаты УВД или они свидетельствуют о высоком профессионализме его работников?

Принять $\alpha = 0{,}05$.

Решение.

Пусть p — вероятность раскрытия преступления районным УВД; ее истинное значение неизвестно. Известно лишь, что из $n = 100$ преступлений УВД раскрыло $m = 49$, т.е. $\hat{p} = \frac{m}{n} = 0{,}49$. Судя по городской статистике, вероятность p оценивается числом $p_0 = 0{,}4$, а судя по результатам работы УВД $p > 0{,}4$. Поэтому примем H_0: $p = 0{,}4$, а H_1: $p > 0{,}4$ — это случай 2. По условию $\alpha = 0{,}05$. Найдем z, при котором $\Phi(z) = 1 - 2\alpha = 1 - 2 \cdot 0{,}05 = 0{,}90$; из (8.39) $z = 1{,}65$. Далее,

$$\frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}} = 0{,}49 - 1{,}65\sqrt{\frac{0{,}4 \cdot (1-0{,}4)}{100}} = 0{,}409.$$

Так как $p_0 = 0{,}4 < 0{,}409$, то в соответствии с (8.46) принимаем гипотезу H_1, согласно которой вероятность раскрытия преступления районным УВД больше, чем вероятность в целом по городу, — это говорит о высоком профессионализме его работников.

Допустим, что вопрос задачи звучит так: случайно или нет отличие результатов УВД от городских? По-прежнему примем H_0: $p = 0{,}4$, но H_1: $p \neq 0{,}4$ — это случай 1. При $\alpha = 0{,}05$ $\Phi(z) = 1 - \alpha = 0{,}95$ и $z = 1{,}96$, интервал $\left(\frac{m}{n} - z\sqrt{\frac{p_0 q_0}{n}};\ \frac{m}{n} + z\sqrt{\frac{p_0 q_0}{n}}\right)$ будет таким (0,394; 0,586). Так как $p_0 = 0{,}4 \in (0{,}394;$ 0,586), то согласно (8.45) гипотезу H_0: $p = 0{,}4$ принимаем; считаем, что вероятность раскрытия преступления районным УВД такая же, как и в целом по городу. Кажущаяся про-тиворечивость этого и ранее полученного выводов объясняется различием альтернативных гипотез: здесь H_1: $p \neq 0{,}4$, а ранее H_1: $p > 0{,}4$.

Контрольные вопросы и задания

1. Приведите примеры вероятностных высказываний и случайных событий в правоприменительной деятельности.
2. Свойство статистической устойчивости и смысл теорем Я. Бернулли и П.Л. Чебышева.
3. Классическая формула вероятности; опытная вероятность.
4. Понятия перестановок, размещений и сочетаний с повторениями и без повторений; соответствующие комбинаторные формулы.
5. Понятие условной вероятности; какие высказывания называются независимыми и зависимыми?
6. Вероятность конъюнкции и дизъюнкции высказываний.
7. Формула полной вероятности и формула Байеса.
8. Формулы Бернулли и Пуассона, условия их использования.
9. Приведите примеры дискретных и непрерывных случайных величин в социально-правовых задачах. Назовите основные характеристики случайной величины.
10. Нормальный закон распределения.
11. Основные понятия проверки статистических гипотез: нулевая и альтернативная гипотезы, ошибки первого и второго рода, правильные решения первого и второго рода, уровень значимости. Примеры статистических гипотез в социально-правовых задачах.

Глава 9

АНАЛИЗ ДАННЫХ В MICROSOFT EXCEL

Пакет «Анализ данных» в Microsoft Excel включает следующие программы[1]:

1. Однофакторный дисперсионный анализ.
2. Двухфакторный дисперсионный анализ с повторениями.
3. Двухфакторный дисперсионный анализ без повторений.
4. Корреляция.
5. Ковариация.
6. Описательная статистика.
7. Экспоненциальное сглаживание.
8. Двухвыборочный *F*-тест для дисперсии.
9. Анализ Фурье.
10. Гистограмма.
11. Скользящее среднее.
12. Генерация случайных чисел.
13. Ранг и персентиль.
14. Регрессия.
15. Выборка.
16. Парный двухвыборочный *t*-тест для средних.
17. Двухвыборочный *t*-тест с одинаковыми дисперсиями.
18. Двухвыборочный *t*-тест с различными дисперсиями.
19. Двухвыборочный *z*-тест для средних.

Дадим краткое изложение методов, положенных в основу наиболее часто используемых программ, приведем соответствующие примеры и интерпретации результатов.

9.1. Генеральная совокупность и выборка. Статистический ряд распределения и выборочные характеристики (Excel — программы №№ 6, 10, 15)

Понятия генеральной совокупности и выборки были введены при изучении комбинаторной формулы размещений. Расширим эти

[1] *Персон Р.* Microsoft Excel 97 в подлиннике. Т. 1, 2. Пер. с англ. — BHV — Санкт-Петербург, 1997.

понятия. *Выборкой* назовем реально наблюдаемые значения (в том числе и повторяющиеся) случайной величины X, а все теоретически домысливаемые значения этой величины назовем *генеральной совокупностью*. Выборку или наблюдаемые значения СВ X обозначим $x_1, x_2, \ldots, x_n$; n — *объем выборки*.

Замечание.

Если СВ X — *булева*[1], т.е. СВ X принимает только *два* значения: 1 — при успешном испытании, 0 — при неудачном испытании, то выборка $x_1, x_2, \ldots, x_n$ представляет собой последовательность единиц и нулей, n — число испытаний (наблюдений СВ X).

➢ ***Программа № 15 «Выборка»*** из чисел рабочего листа — генеральной совокупности отбирает числа:

- *либо в соответствии с введенным периодом l* отбора: 1-е, $(1 + l)$-е, $(1 + 2l)$-е число и т.д. (периодическая выборка);
- *либо случайным образом*, при этом любое из чисел может быть отобрано неоднократно (случайная повторная выборка); при таком отборе нужно ввести «число выборок» — это объем выборки n.

Задание генеральной совокупности множеством чисел, среди которых, конечно, могут быть и повторяющиеся, — исключительный случай. Более употребительным способом задания генеральной совокупности является указание закона распределения вероятностей случайной величины X, в частности для дискретной величины — указание ряда распределения вероятностей.

Основными числовыми характеристиками выборки $x_1, x_2, \ldots x_n$, или *выборочными характеристиками*, являются:

- выборочное среднее

$$\overline{x} = \frac{x_1 + \ldots + x_n}{n}; \qquad \textbf{(9.1)}$$

- *выборочная дисперсия* $\hat{D}X$, которую вычисляют по одной из двух тождественных формул:

$$\left.\begin{aligned} \hat{D}X &= \frac{(x_1 - \overline{x})^2 + \ldots + (x_n - \overline{x})^2}{n}, \\ \hat{D}X &= \frac{x_1^2 + \ldots + x_n^2}{n} - (\overline{x})^2, \end{aligned}\right\} \qquad \textbf{(9.2)}$$

- *выборочное среднее квадратическое отклонение* $\hat{\sigma}_X = \sqrt{\hat{D}X}$ — это характеристика среднего разброса попавших в выборку чисел около выборочной средней.

---

[1] *Буль Джордж* (1815—1864) — английский математик и логик.

Аналогичные характеристики генеральной совокупности называют генеральными характеристиками. Если генеральная совокупность задана рядом распределения вероятностей случайной величины X, то:

- *генеральное среднее* MX, называемое иначе математическим ожиданием случайной величины X, вычисляется по формуле (8.35);
- *генеральная дисперсия* DX вычисляется по одной из двух тождественных формул (8.36);
- *генеральное среднее квадратическое отклонение* $\sigma_X = \sqrt{DX}$.

Замечание.

При изучении по выборке булевой СВ X:

- выборочное среднее $\overline{x} = m/n = \hat{p}$, где n — общее число испытаний (наблюдений СВ X), m — число успехов в этих испытаниях, а генеральное среднее $MX = p$, где p — вероятность успеха в единичном испытании;
- выборочная дисперсия $\hat{D}X = \hat{p}(1-\hat{p}) = \hat{p}\hat{q}$, а генеральная дисперсия $DX = p(1 - p) = pq$.

В реальных задачах исследователь располагает, как правило, результатами выборочных наблюдений (статистическими данными) и не знает «всей» генеральной совокупности. Вычисленные по этим данным выборочные характеристики являются оценками соответствующих генеральных характеристик. Будем предполагать, что наблюдения независимы и проведены примерно в одинаковых, иначе в типичных, условиях. При выполнении этих предположений выборочное среднее $\overline{x}$ является «хорошей оценкой» генерального среднего MX. Более же «хорошей оценкой» генеральной дисперсии DX, особенно при малом объеме выборки, является не выборочная дисперсия $\hat{D}X$, а так называемая «несмещенная оценка» генеральной дисперсии, вычисляемая по формуле

$$s_X^2 = \frac{(x_1 - \overline{x})^2 + \ldots + (x_n - \overline{x})^2}{n-1} \qquad \textbf{(9.3)}$$

и называемая *дисперсией выборки*.

Величину

$$s_X = \sqrt{s_X^2} \qquad \textbf{(9.4)}$$

называют *выборочным стандартным отклонением*.

Говоря о выборке, следует иметь в виду, что это:

- либо конкретные числа x_1, x_2, ..., x_n, и тогда все выборочные характеристики — это тоже числа;
- либо обозначения X_1, X_2, ..., X_n тех чисел, которые могли бы попасть в выборку; а поскольку нельзя заранее предвидеть,

какие числа попадут в выборку, то значения выборочных характеристик не предсказуемы; в этом случае выборочные характеристики — это случайные величины и они, как и любая случайная величина, имеют математическое ожидание и дисперсию. В частности, дисперсия выборочного среднего, если его интерпретировать как случайную величину, $D\overline{X} = \frac{DX}{n}$, а выборочная оценка этой дисперсии $s^2_{\overline{X}} = \frac{s^2_X}{n}$; величину $s_{\overline{X}} = \frac{s_X}{\sqrt{n}}$ называют *стандартной ошибкой выборочного среднего.*

В ряде задач не ограничиваются использованием выборочного среднего $\overline{x}$ в качестве оценки генерального среднего MX, а строят *интервальную оценку генерального среднего* — это интервал

$$\left(\overline{x} - t_{n-1,1-\gamma} \cdot s_{\overline{X}};\ \ \overline{x} + t_{n-1,1-\gamma} \cdot s_{\overline{X}}\right), \qquad \textbf{(9.5)}$$

который с достаточно высокой вероятностью, равной числу γ, накроет генеральное среднее (число $t_{n-1,\,1-\gamma}$ определяется по специальным таблицам критических точек распределения Стьюдента[1] в зависимости от $k = n-1$ и $p = 1-\gamma$), т.е.

$$P(\overline{X} - t_{n-1,1-\gamma} \cdot s_{\overline{X}} < MX < \overline{X} + t_{n-1,1-\gamma} \cdot s_{\overline{X}}) = \gamma, \qquad \textbf{(9.6)}$$

или $P\left(\left|\overline{X} - MX\right| < t_{n-1,1-\gamma} \cdot s_{\overline{X}}\right) = \gamma.$

Величину

$$\varepsilon = t_{n-1,1-\gamma} \cdot s_{\overline{X}} \qquad \textbf{(9.7)}$$

называют *ошибкой выборочного среднего*, гарантируемой с надежностью γ.

Замечание.

Строго говоря, формулы (9.5)—(9.7) предполагают, что X — нормально распределенная СВ.

При неизвестном числовом значении генерального среднего MX гипотезу H_0: $MX = a_0$ (генеральное среднее равно числу a_0), при альтернативной гипотезе H_1: $MX \neq a_0$, проверяют так: строят интервальную оценку (9.5) генерального среднего, отвечающую вероятности $\gamma = 1-\alpha$, где α — заданное числовое значение уровня значимости; если интервал (9.5) не накрывает число a_0, гипотезу H_0 не принимают, в противном случае — принимают.

---

[1] *Колемаев В.А.*, *Калинина В.Н.* Теория вероятностей и математическая статистика. — М.: ЮНИТИ, 2003.

Замечание.

При изучении булевой СВ X по выборке достаточно большого объема n формула (9.5) даст интервальную оценку вероятности p успеха в единичном испытании, а (9.7) даст ошибку выборочной вероятности $\hat{p} = m/n$.

➢ ***Программа № 6 «Описательная статистика»*** вычисляет характеристики выборки — совокупности чисел, введенных в рабочий лист. По умолчанию уровень надежности $\gamma = 0{,}95$.

Пример 9.1.

В ходе исследования рецидивной преступности из документов были собраны данные о числе повторных судимостей 100 случайно отобранных человек, имевших в прошлом одну или более судимостей. Среди отобранных не имели повторных судимостей 50 человек, а по остальным — числа повторных судимостей оказались такими: 1, 1, 1, 2, 3, 1, 1, 1, 1, 2, 2, 1, 2, 1, 1, 1, 1, 1, 2, 3, 1, 1, 1, 1, 1, 2, 2, 1, 1, 1, 1, 1, 2, 2, 1, 2, 1, 3, 4, 1, 1, 1, 1, 1, 1, 1, 1, 3, 1, 1.

Распечатка результатов работы «Описательной статистики» приведена на рис. 9.1. В распечатке наряду с ранее рассмотренными характеристиками приведены:

медиана — число, находящееся в центре ряда данных, расположенных в неубывающем порядке; если в центре этого ряда будет два числа, то медиана равна среднему арифметическому этих чисел;

мода — число, наиболее часто встречающееся в ряду данных;

эксцесс и асимметричность — смысл этих понятий разъясняется ниже.

Последнее число в распечатке: 0,175 — это ошибка (9.7) ε выборочного среднего, гарантируемая с 95%-ной надежностью; в соответствии с (9.5), с вероятностью 95% можно утверждать, что интервал (0,535; 0,885) накроет генеральное среднее число повторных судимостей (узнать это число, вообще говоря, нельзя: ведь для этого потребовалось бы собрать данные о числе повторных судимостей не 100 человек, а всех судимых в прошлом). Поскольку найденный интервал не накрывает, например, число 1, то гипотезу H_0: $MX = 1$ о том, что генеральное среднее число повторных судимостей равно 1 (при альтернативе H_1: $MX \neq 1$), принять, на уровне значимости $\alpha = 1 - \gamma = 1 - 0{,}95 = 0{,}05$, нельзя.

Чтобы составить представление о закономерности варьирования чисел в «неизвестной» генеральной совокупности, результаты выборочных наблюдений группируют.

Продолжим пример 9.1. Сгруппируем 100 данных о числе повторных судимостей так: различающиеся наблюдения (их называют *вариантами*, x_i) расположим в порядке возрастания и для каждого варианта x_i укажем число m_i — частоту (кратность) варианта и число $\hat{p}_i = \dfrac{m_i}{n}$ — частость (относительную частоту, статистическую или опытную вероятность) варианта:

Число повторных судимостей x_i	0	1	2	3	4	Итого
Количество человек m_i	50	35	10	4	1	$n = 100$
Опытная вероятность $\hat{p}_i = \frac{m_i}{n}$ (число людей в %)	0,5 (50%)	0,35 (35%)	0,1 (10%)	0,04 (4%)	0,01 (1%)	1 (100%)
Вероятность Пуассона* $p_i = \frac{(0,71)^{x_i}}{(x_i)!} e^{-0,71}$	0,49	0,35	0,12	0,03	0,01	

(9.8)

* Содержание этой строки разъясняется далее.

Судя по ряду: рецидивистов с двумя судимостями в 3,5 раза больше числа рецидивистов с тремя судимостями; в свою очередь число рецидивистов с тремя судимостями в 2,5 раза больше, чем рецидивистов с четырьмя судимостями.

Распределение опытных (статистических) вероятностей по вариантам:

Вариант, x_i	$x_1\ x_2 \ldots\ x_\ell$	
Опытная вероятность $\hat{p}_i$	$\hat{p}_1\ \hat{p}_2 \ldots\ \hat{p}_\ell$	$\Sigma = 1$

(9.9)

называют *статистическим рядом распределения*. Чем этот ряд отличается от ряда распределения вероятностей (8.34)? В ряду распределения вероятностей указываются все возможные значения случайной величины и «истинные» вероятности этих значений; в статистическом ряду указываются значения — варианты, зафиксированные в проведенных наблюдениях, и опытные вероятности вариантов, которые могут и не совпадать с истинными вероятностями.

➢ ***Программа № 10 «Гистограмма»*:**

- группирует числа, введенные в рабочий лист, при этом граничные значения — «карманы» либо вводятся в рабочий лист в возрастающем порядке, либо рассчитываются автоматически (как точки, равномерно распределенные между минимальным и максимальным наблюдениями), а частота текущего «кармана» — это число наблюдений, *не больших* этого «кармана» и *больших* предыдущего «кармана»;

- подсчитывает по требованию «интегральный %» — это ряд накопленных частостей (опытных вероятностей) в процентах;
- строит по требованию *гистограмму* — столбиковую диаграмму частот и график «интегральных %».

Распечатка результатов «Гистограммы» для 100 данных о числе повторных судимостей (см. пример 9.1) при введенных граничных значениях 0, 1, 2, 3, 4 приведена на рис. 9.2.

Столбец 1	
Среднее	0,710
Стандартная ошибка	0,088
Медиана	0,500
Мода	0,000
Стандартное отклонение	0,880
Дисперсия выборки	0,774
Эксцесс	1,709
Асимметричность	1,334
Интервал	4,000
Минимум	0,000
Максимум	4,000
Сумма	71,000
Счет	100,000
Уровень надежности (95,0%)	0,175

Рис. 9.1

Замечание.

Приводимая в распечатке программы «Описательная статистика» (см. рис. 9.1) асимметричность (A) является характеристикой асимметричности гистограммы (если правая ветвь длиннее левой, $A > 0$; в противном — $A < 0$), а эксцесс (E) является характеристикой «островершинности» гистограммы по сравнению с нормальной кривой (см. рис. 8.6) (чем больше E, тем «островершиннее» гистограмма). Для нормальной кривой $A = E = 0$.

Продолжим пример 9.1. Обратим внимание на то, что выборочное среднее число судимостей ($\overline{x} = 0{,}71$) примерно равно дисперсии числа судимостей ($s_X^2 = 0{,}77$). Это служит основанием выдвижения гипотезы H_0: СВ X (число повторных судимостей случайно выбранного человека, имеющего в прошлом судимость) имеет пуассоновское распределение. Напомним, что математическое ожидание Mm (в условиях примера Mm — это генеральное среднее число повторных судимостей) и дисперсия Dm (генеральная дисперсия числа повторных судимостей) этого распределения совпадают, см. (8.32). Пуассоновские вероятности, рассчитанные по формуле (8.30), в которой $a = Mm$ заменено на выборочное среднее число повторных судимостей, $a \approx \overline{x} = 0{,}71$, приведены в последней

строке (9.8). Пуассоновские вероятности практически не отличаются от опытных, гипотеза H_0 согласуется с результатами наблюдений.

Карман	*Частота*	*Интегральный %*
0	50	50,00%
1	35	85,00%
2	10	95,00%
3	4	99,00%
4	1	100,00%
Еще	0	100,00%

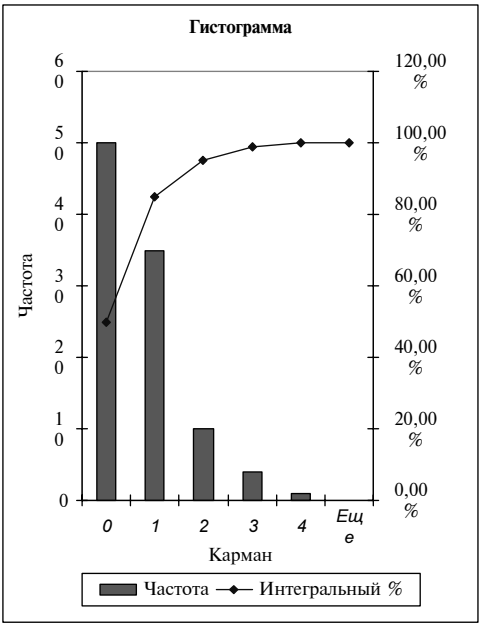


Рис. 9.2

Для выявления закономерности варьирования наблюдений в случае большого числа вариантов, что обычно бывает при изучении непрерывной величины (например, времени, прошедшего между освобождением рецидивиста из мест лишения свободы и совершением нового преступления) строят *интервальный статистический ряд.*

Пример 9.2.

По документам $n = 100$ рецидивистов собраны сведения о времени X между окончанием меры наказания за первое преступление и привлечением к наказанию за второе преступление. Не приводя этих данных, отметим,

что число различающихся данных оказалось достаточно большим, при этом $x_{\min} = 0$ (рецидивист совершил второе преступление до окончания меры наказания за первое), а $x_{\max} = 7{,}5$ (лет). Длину h интервала группирования сведений определим по формуле Стэрджеса (которая для многих задач дает оптимальную длину интервала, позволяющую выявить характерные черты варьирования наблюдений):

$$h = \frac{x_{\max} - x_{\min}}{1 + 3{,}322 \cdot \log n} = \frac{7{,}5}{1 + 3{,}322 \cdot \log 100} \approx 1 \ (\text{год}).$$

Сами интервалы будут такими: ($x_{\min}$; $x_{\min} + h$), ($x_{\min} + h$; $x_{\min} + 2\,h$), ...; построение интервалов заканчивают как только конец очередного интервала не станет равным или большим $x_{\max}$. В условиях задачи интервалы будут такими: (0; 1), (1; 2), (7; 8). Распечатка результатов программы «Гистограмма» при введении в качестве карманов чисел 1, 2, 3, ..., 8 приведена на рис. 9.3.

Карман	*Частота*	*Интегральный %*
1	40	40,00
2	26	66,00
3	15	81,00
4	9	90,00
5	5	95,00
6	3	98,00
7	1	99,00
8	1	100,00
Еще	0	100,00

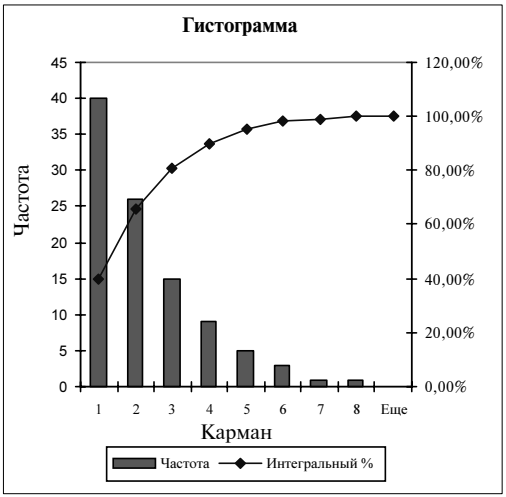


Рис. 9.3

Судя по распечатке у 40 рецидивистов промежуток времени X между преступлениями не превысил 1 года ($X \le 1$), у 26 рецидивистов: $1 < X \le 2$, у 15 рецидивистов: $2 < X \le 3$ и т.д.

В ряде задач статистические данные задаются в сгруппированном виде. Формулы расчета выборочных характеристик: $\overline{x}$, $\hat{D}X$, $\hat{\sigma}_X$ по данным, сгруппированным в статистический ряд, таковы:

$$\overline{x} = \frac{\sum_{i=1}^{l} x_i m_i}{n};\ \hat{D}X = \frac{\sum_{i=1}^{l} \left(x_i - \overline{x}\right)^2 m_i}{n} = \frac{\sum_{i=1}^{l} x_i^2 m_i}{n} - \left(\overline{x}\right)^2;\ \hat{\sigma}_X = \sqrt{\hat{D}X}\ , \quad \textbf{(9.10)}$$

где l — число групп ряда,

x_i — вариант (центр интервала для интервального ряда),

m_i — частота варианта (интервальная частота).

Продолжим пример 9.2. Вычислим среднюю продолжительность $\overline{x}$ времени пребывания на свободе и среднее квадратическое отклонение $\hat{\sigma}_X$ времени.

Результаты группировки, приведенные на рис. 9.3, запишем в следующую таблицу:

Интервал	0–1	1–2	2–3	3–4	4–5	5–6	6–7	7–8	
Центр интервала x_i	0,5	1,5	2,5	3,5	4,5	5,5	6,5	7,5	
Частота m_i	40	26	15	9	5	3	1	1	$n = 100$
Опытная вероятность $\hat{p}_i = \frac{m_i}{n}$	0,4	0,26	0,15	0,09	0,05	0,03	0,01	0,01	$\Sigma = 1$
Экспоненциальная вероятность p_i	0,419	0,241	0,139	0,080	0,046	0,026	0,015	0,009	

(9.11)

В соответствии с формулами (9.10)

$\overline{x} = (0{,}5 \cdot 40 + ... + 7{,}5 \cdot 1)/100 = 1{,}81$ (года),

$$\hat{\sigma}_X = \sqrt{\left(0{,}5^2 \cdot 40 + ... + 7{,}5^2 \cdot 1\right)/100 - 1{,}81^2} = 1{,}53 \text{ (года)}.$$

Обратим внимание на то, что $\overline{x} \approx \hat{\sigma}_X$ — это свойственно распределениям, построенным по наблюдениям «экспоненциальной» СВ — это непрерывная СВ X, вероятность попадания которой в малый интервал длиной h с центром в точке x рассчитывается так: $P\left(X \in h\right) = h\lambda e^{-\lambda x}$, где $\lambda = \frac{1}{MX}$.

Заменив генеральное среднее MX на выборочное среднее $\overline{x} = 1{,}81$, рассчитаем «экспоненциальные» вероятности попадания времени пребывания рецидивиста на свободе в соответствующие интервалы; они практически не отличаются от опытных вероятностей.

9.2. Сравнение характеристик двух генеральных совокупностей (Excel — программы № 8, №№ 16—19)

Допустим, что требуется на основании выборочных обследований сравнить два города по среднему возрасту и «вариабельности» (дисперсии) возраста гражданина, впервые нарушившего уголовное законодательство (или сравнить названные характеристики в одном городе до и после проведения соответствующих профилактических мероприятий). Переведем задачу на язык математики.

Введем о б о з н а ч е н и я:

X, MX, DX — возраст случайно выбранного нарушителя, средний возраст и дисперсия возраста нарушителя в первом городе соответственно;

Y, MY, DY — аналогичные характеристики для второго города.

Не имея возможности собрать сведения о возрасте всех нарушителей городов, а располагая лишь выборочными обследованиями: в первом городе собраны данные о возрасте n_X нарушителей, а во втором — n_Y, требуется проверить гипотезы H_0: $MX = MY$ и H_0: $DX = DY$ о том, что средний возраст нарушителя в городах одинаков и вариабельность (дисперсия) возраста одинакова.

Алгоритмы проверки гипотез H_0: $MX = MY$ и H_0: $DX = DY$ реализованы в программах № 8, №№ 16—19. Строго говоря, эти алгоритмы предполагают, что:

а) n_X наблюдений СВ X (n_Y наблюдений СВ Y) проведены в типичных условиях;

б) все $n_X + n_Y$ наблюдений независимы;

в) СВ X (СВ Y) — нормально распределенная СВ.

Замечание.

Названные программы могут использоваться и для решения задач такого типа. Допустим, требуется сравнить две вероятности: p_X — вероятность того, что случайно выбранный юноша — наркоман и p_Y — вероятность того, что случайно выбранная девушка — наркоманка. Не имея возможности обследовать всех юношей и девушек на предмет употребления наркотиков, собирают сведения о *достаточно большом* числе n_X юношей — это первая выборка, и *достаточно большом* числе n_Y девушек — это вторая выборка. Каждая из выборок — некоторая последовательность единиц и нулей: 1 — обследуемый употребляет наркотики, 0 — не употребляет. По сути в этой задаче речь идет об изучении двух булевых СВ: X и Y. А поскольку для булевой СВ X математическое ожидание $MX = p_X$, а дисперсия $DX = p_X(1 - p_X) = p_X q_X$, то гипотеза H_0: $MX = MY$ равносильна гипотезе H_0: $p_X = p_Y$, а гипотеза H_0: $DX = DY$ равносильна гипотезе H_0: $p_X q_X = p_Y q_Y$.

Еще раз обратим внимание на то, что наблюдения булевой СВ — это некоторая последовательность единиц и нулей.

➢ ***Программа № 8 «Двухвыборочный F-тест для дисперсий»*** используется для проверки гипотезы H_0: $DX = DY$ (генеральные дисперсии одинаковы). Исходные данные — введенные в рабочий лист наблюдения переменной 1 (СВ *X)* и наблюдения переменной 2 (СВ *Y*), а также уровень значимости α — вероятность отвергнуть верную гипотезу H_0. По этим данным программа рассчитывает: средние $\bar{x}$ и $\bar{y}$, дисперсии s_X^2 и s_Y^2 и ряд других величин, необходимых для проверки гипотезы H_0: $DX = DY$. Среди этих величин: *df* — число степеней свободы, которое равно: $n_x - 1$ для переменной 1 и $n_Y - 1$ для переменной 2; $F = s_X^2 / s_Y^2$; вероятность «*P* одностороннее», называемая «рассчитанным уровнем значимости»: если «*P* одностороннее» $> \alpha$, гипотезу H_0: $DX = DY$ принимают; если «*P* одностороннее» $< \alpha$, то H_0 не принимают; принимают альтернативную гипотезу H_1, которая может быть двух видов:

H_1: $DX > DY$, если $s_X^2 > s_Y^2$, и H_1: $DX < DY$, если $s_X^2 < s_Y^2$.

При альтернативе $H_1 : DX \neq DY$ в диалоговое окно следует вместо α ввести $\alpha/2$; если «*p* одностороннее» $> \frac{\alpha}{2}$, принимают H_0, в противном — H_1.

Пример 9.3.

Выборочные данные о возрасте (полное число лет) граждан, впервые совершивших уголовные преступления, таковы: 15, 17, 15, 21, 21, 18, 20 — в первом микрорайоне; 25, 16, 19, 24, 19, 20, 21, 23, 23 — во втором. Распечатка результатов программы № 8 при $\alpha = 0{,}05$ приведена на рис. 9.4. Вероятность «*P* одностороннее» = 0,413 > α, поэтому гипотезу H_o: $DX = DY$ (при альтернативе H_1: $DX < DY$, ведь дисперсия s_X^2 первой выборки меньше дисперсии s_Y^2 второй выборки) принимаем: генеральная «вариабельность» возраста нарушителя в обоих микрорайонах одинакова, или различие выборочных дисперсий $s_X^2 = 6{,}81$ и $s_Y^2 = 8{,}361$ незначимо, несущественно, связано со случайными ошибками выборки.

Программы №№ 16—19 используются для проверки гипотезы H_0: $MX - MY = a$ (разность генеральных средних равна числу *a*). В программах число *a* названо *гипотетической разностью средних;* по умолчанию $a = 0$ и тогда проверяемая гипотеза H_0: $MX = MY$. При описании программ примем, не оговаривая особо, что $a = 0$.

➢ ***Программа № 17 «Двухвыборочный t-тест с одинаковыми дисперсиями»*** используется для проверки гипотезы только в том случае, когда есть основание считать равными генеральные дисперсии,

$DX = DY$, хотя числовые значения этих дисперсий и неизвестны. В качестве альтернативы к гипотезе H_0: $MX - MY = a$ при $a = 0$ может быть:

$$H_1: MX > MY;\ H_1: MX < MY;\ H_1: MX \neq MY.$$

Двухвыборочный F-тест для дисперсии

	Переменная 1	*Переменная 2*
Среднее	18,143	21,111
Дисперсия	6,810	8,361
*Н*аблюдения	7,000	9,000
df	6,000	8,000
F	0,814	
$P(F \leq t)$ одностороннее	0,413	
F критическое одностороннее	0,241	

Рис. 9.4

Исходные данные программы — наблюдения величин X и Y и вероятность α.

Продолжим пример 9.3. По данным примера была принята гипотеза H_0: $DX = DY$ (принятие H_0 служит основанием считать дисперсии равными, но не означает, что равенство дисперсий — абсолютная истина). Распечатка результатов программы № 17 при $\alpha = 0{,}05$ и «гипотетической разности средних» = 0 приведена на рис. 9.5.

Двухвыборочный t-тест с одинаковыми дисперсиями

	Переменная 1	*Переменная 2*
Среднее	18,143	21,111
Дисперсия	6,810	8,361
Наблюдения	7,000	9,000
Объединенная дисперсия	7,696	
Гипотетическая разность средних	0,000	
df	14,000	
t-статистика	-2,123	
$P(T <= t)$ одностороннее	0,026	
t критическое одностороннее	1,761	
$P(T <= t)$ двухстороннее	0,052	
t критическое двухстороннее	2,145	

Рис. 9.5

В распечатке «Объединенная дисперсия» — это оценка генеральной дисперсии обеих совокупностей, равная

$s^2 = \dfrac{s_X^2\,(n_X - 1) + s_Y^2\,(n_Y - 1)}{(n_X - 1) + (n_Y - 1)} = \dfrac{6{,}81 \cdot 6 + 8{,}36 \cdot 8}{6 + 8} = 7{,}696$; число степеней свободы $df = n_X + n_Y - 2 = 14$, статистика $t = \dfrac{(\overline{x} - \overline{y}) - a}{s\sqrt{1/n_X + 1/n_Y}} = -2{,}123$.

Альтернативой гипотезе H_0: $MX = MY$ (средний возраст преступника для микрорайонов одинаков) может быть:

- гипотеза H_1: $MX < MY$ (ведь $\overline{x} = 18{,}143 < \overline{y} = 21{,}111$); в этом случае H_0 принимают, если рассчитанный «Односторонний уровень значимости», или вероятность «P одностороннее» > α, в противном — принимают H_1 («P одностороннее» = 0,026 < α = 0,05, поэтому принимаем H_1);
- гипотеза H_1: $MX \neq MY$; в этом случае H_0 принимают, если «P двухстороннее» > α, в противном случае принимают H_1 («P двухстороннее» = 0,052 > α = 0,05, принимаем гипотезу H_0).

Пример показывает, что при неизменной вероятности α отвергнуть верную гипотезу H_0 ответ на вопрос о том, принять или не принять гипотезу H_0, зависит и от вида альтернативы H_1.

Приведем описание назначения программ №№ 18, 19, 16; останавливаться на интерпретации их результатов не будем, поскольку вопрос о том, принять или не принять гипотезу H_0: $MX - MY = a$ здесь решается так же, как и в программе № 17.

➢ ***Программа № 18 «Двухвыборочный t-тест с различными дисперсиями»*** используется для проверки гипотезы H_0: $MX - MY = a$, когда есть основание считать генеральные дисперсии неравными: $DX \neq DY$, хотя числовые значения этих дисперсий и неизвестны.

➢ ***Программа № 19 «Двухвыборочный z-тест для средних»*** используется для проверки гипотезы H_0: $MX - MY = a$, когда числовые значения генеральных дисперсий DX и DY известны.

➢ ***Программа № 16 «Парный двухвыборочный t-тест для средних»*** используется для проверки гипотезы H_0: $MX - MY = a$, когда СВ X и СВ Y одноименные и наблюдаются «в паре»; в этом случае число n_X наблюдений СВ X равно числу n_Y наблюдений СВ Y, $n_X = n_Y$.

9.3. Дисперсионный анализ (Excel — программы №№ 1–3)

Дисперсионный анализ используется для выявления влияния на изучаемую СВ Y некоторых факторов, обычно не поддающихся количественному измерению. Суть метода состоит в разложении об-

щей вариации СВ Y на части, соответствующие раздельному и совместному влиянию факторов, и изучении этих частей. Модели дисперсионного анализа в зависимости от числа факторов классифицируются на однофакторные, двухфакторные и т.д.

Однофакторный дисперсионный анализ выясняет, существует или нет влияние зафиксированных уровней $A^{(1)}$, $A^{(2)}$, ..., $A^{(v)}$ фактора A на СВ Y. Исходными данными являются результаты наблюдений СВ Y при зафиксированных уровнях фактора A, записываемые в виде таблицы, столбцы которой назовем группами (числа наблюдений в группах могут быть разными):

Уровни фактора A			
$A^{(1)}$	$A^{(2)}$	...	$A^{(v)}$
* Результаты наблюдений СВ Y	Результаты наблюдений СВ Y		Результаты наблюдений СВ Y *

(9.12)

Строго говоря, д и с п е р с и о н н ы й а н а л и з предполагает, что:

а) все наблюдения независимы;

б) при каждом уровне фактора наблюдения проводятся в типичных условиях, а их результаты — нормально распределенные СВ с дисперсиями (генеральными), не изменяющимися при переходе от одного уровня фактора к другому;

в) модель формирования результата наблюдений в i-й группе (i = = 1, 2, ..., v) такая: результат наблюдения = некоторой постоянной величине (не зависящей от номера группы) + эффект $\theta^{(i)}$ (неслучайный) влияния уровня $A^{(i)}$ фактора A + случайный эффект влияния прочих неконтролируемых факторов, в среднем равный нулю.

Дисперсионный анализ проверяет гипотезу $H_0: \theta^{(1)} = \theta^{(2)} = = ... = \theta^{(v)} = 0$ (эффекты влияния зафиксированных уровней фактора A — нулевые, иначе «фактор A не влияет на изучаемую СВ Y»).

➢ ***Программа № 1 «Однофакторный дисперсионный анализ»*** в качестве исходных данных использует результаты наблюдений по группам, введенные в рабочий лист, и уровень значимости α — вероятность отклонения верной гипотезы $H_0: \theta^{(1)} = \theta^{(2)} = ... = \theta^{(v)} = 0$. «Входной интервал» — это данные «от * до *» (9.12). Вычисляет: групповые средние $\overline{y}^{(1)}, \overline{y}^{(2)}, ..., \overline{y}^{(v)}$, несмещенные оценки s_1^2, s_2^2, ..., s_v^2 неизменяю-

щихся групповых генеральных дисперсий и ряд других характеристик, необходимых для проверки гипотезы H_0.

Пример 9.4.

Владелец трех типовых юридических контор пытается выяснить, отличаются ли они по объему выполняемой работы, измеренному в д.е. Для этого в каждой из контор были собраны следующие сведения о еженедельном объеме выполненных работ:

Контора		
1-я	*2-я*	*3-я*
* 280	300	350
250	250	240
200	210	170
290	310	200
	270	150
	300	*

Распечатка результатов работы программы № 1 при $\alpha = 0{,}05$ приведена на рис. 9.6. В распечатке, например, среднее 255 — это среднее наблюдений первого столбца: $\bar{y}^{(1)} = (280 + 250 + 200 + 290)/4$, а дисперсия 1633,3(3) — это дисперсия $s_1^2 = [(280 - 255)^2 + (250 - 255)^2 + (200 - 255)^2 + (290 - 255)^2] / (4 - 1)$ наблюдений первого столбца.

Однофакторный дисперсионный анализ

ИТОГИ				
Группы	Счет	Сумма	Среднее	Дисперсия
Столбец 1	4,000	1020,000	255,000	1633,333
Столбец 2	6,000	1640,000	273,333	1466,667
Столбец 3	5,000	910,000	182,000	1470,000

Дисперсионный анализ

Источник вариации	*SS*	*df*	*MS*	*F*	*P*-Значение	*F* критическое
Между группами	24326,667	2,000	12163,333	8,058	0,006	3,885
Внутри групп	18113,333	12,000	1509,444			
Итого	42440,000	14,000				

Рис. 9.6

Не приводя формул подсчета и не объясняя смысла всех чисел таблицы «Дисперсионный анализ» на рис. 9.6 (эти вопросы подробно изложены в работе В.А. Колемаева и В.Н. Калининой[1], обратим внимание лишь на «*P*-Значение», называемое «рассчитанным уровнем значимости»: если «*P*-Значение» > заданного уровня значимости α, гипотезу H_0 о равенстве нулю эффектов влияния зафиксированных уровней фактора принимают; при «*P*-Значение» < α гипотезу H_0 не принимают.

В случае «непринятия» гипотезы H_0 об отсутствии влияния фактора *A* вычисляют *коэффициент детерминации*:

$$\eta^2_{Y/A} = \frac{SS,\ \text{Между группами}}{SS,\ \text{Итого}} \cdot 100\%,$$

показывающий, какой процент вариации или изменчивости наблюдений СВ *Y* (принимаемой за 100%) объясняется изменчивостью уровней фактора *A*, или просто влиянием фактора *A*.

В распечатке «*P*-Значение» = 0,006, что меньше α = 0,05, поэтому гипотезу $H_0: \theta^{(1)} = \theta^{(2)} = \theta^{(3)} = 0$ о равенстве нулю «эффектов влияния контор» на еженедельный объем выполняемых работ не принимаем: конторы различаются по объему выполняемых работ; коэффициент $\eta^2_{Y/A} = \frac{24326,67}{42440} \cdot 100\% = 57,3\%$ — такова, судя по выборке, доля вариации еженедельного объема выполняемых работ, объясняемая влиянием фактора-контора.

В *двухфакторном дисперсионном анализе* рассматривается два фактора: *A,* принимающий v_A уровней $A^{(1)}, A^{(2)}, ..., A^{(v_A)}$, и *B,* принимающий v_B уровней $B^{(1)}, B^{(2)}, ..., B^{(v_B)}$. Исходная база анализа — наблюдения изучаемой СВ *Y*, проведенные при различных комбинациях уровней факторов, обычно записываемые в виде таблицы (9.13).

➢ ***Программа № 3 «Двухфакторный дисперсионный анализ без повторений»*** предполагает, что при каждой комбинации уровней факторов *A* и *B* проведено только одно наблюдение СВ *Y*. Эти наблюдения вводятся в рабочий лист в виде таблицы, у которой число строк равно v_A, а число столбцов равно v_B. По полученной на выходе таблице дисперсионного анализа можно проверить д в е г и п о т е з ы:

- *гипотезу* $H_A: \theta_A^{(1)} = \theta_A^{(2)} = ... = \theta_A^{(v_A)} = 0$ (эффекты влияния зафиксированных уровней фактора *A* — нулевые); если «*P*-Зна-

[1] *Колемаев В.А., Калинина В.Н.* Теория вероятностей и математическая статистика. — М.: ЮНИТИ, 2003.

чение, Строки» > α, где α — заданная вероятность отвергнуть верную гипотезу H_A, H_A принимают: считают, что фактор A не влияет на изучаемую СВ Y; если «P-Значение, Строки» < α, гипотезу H_A не принимают и в этом случае вычисляют коэффициент детерминации $\eta^2_{Y/A} = \dfrac{SS,\ \text{Строки}}{SS,\ \text{Итого}} \cdot 100\%$, показывающий, какой процент вариации наблюдений связан с влиянием фактора A;

- *гипотезу* H_B: $\theta_B{}^{(1)} = \theta_B{}^{(2)} = ... = \theta_B{}^{(\nu_B)} = 0$; ее проверка проводится аналогично, с той лишь разницей, что используется «P-Значение, Столбцы» и

$$\eta^2_{Y/B} = \frac{SS,\ \text{Столбцы}}{SS,\ \text{Итого}} \cdot 100\%.$$

*	$B^{(1)}$	$B^{(2)}$	...	$B^{(\nu_B)}$
$A^{(1)}$	Результаты наблюдений СВ Y	Результаты наблюдений СВ Y	...	Результаты наблюдений СВ Y
$A^{(2)}$	Результаты наблюдений СВ Y	Результаты наблюдений СВ Y	...	Результаты наблюдений СВ Y
⋮	...	...	...	...
$A^{(\nu_A)}$	Результаты наблюдений СВ Y	Результаты наблюдений СВ Y	...	Результаты наблюдений СВ Y *

(9.13)

➢ ***Программа № 2 «Двухфакторный дисперсионный анализ с повторениями»*** предполагает, что при каждой комбинации уровней факторов A и B проведено одинаковое число k наблюдений СВ Y, при этом $k > 1$. Все наблюдения вводятся в рабочий лист в виде (9.13) «от * до *», при этом «внутриклеточные» наблюдения вводятся как столбцы, а имена $A^{(1)}$, $A^{(2)}$... строк и $B^{(1)}$, $B^{(2)}$... столбцов можно не указывать. Поскольку в каждой клетке k наблюдений, записанных в столбик, то число занятых строк рабочего листа равно $(\nu_A \cdot k + 1)$, а число столбцов $(\nu_B + 1)$. «Входной интервал» — это данные «от * до *». Дополнительно вводятся: «Число строк на вы-

борку» — это число k (количество наблюдений в каждой клетке таблицы (9.13)) и α.

По полученной на выходе таблице дисперсионного анализа можно проверить три гипотезы:

- *гипотезу* H_A: $\theta_A^{(1)} = ... = \theta_A^{(\nu_A)} = 0$ (эффекты влияния уровней фактора A — нулевые); если «*P*-Значение, Выборка» $> \alpha$, гипотезу H_A принимают; при «*P*-Значение, Выборка» $< \alpha$ H_A не принимают и вычисляют коэффициент детерминации $\eta^2_{Y/A} = \frac{SS, \text{Выборка}}{SS, \text{Итого}} \cdot 100\%$, показывающий процент общей вариации наблюдений СВ Y, объясняемый влиянием фактора A;
- *гипотезу* H_B: $\theta_B^{(1)} = ... = \theta_B^{(\nu_B)} = 0$ (эффекты влияния уровней фактора B — нулевые); здесь с α сравнивают «*P*-Значение, Столбцы»; в случае непринятия H_B вычисляют $\eta^2_{Y/B} = \frac{SS,\ \text{Столбцы}}{SS,\ \text{Итого}} \cdot 100\%$;
- *гипотезу* H_{AB}: «эффекты влияния взаимодействия уровней факторов A и B — нулевые»; здесь с α сравнивают «*P*-Значение, Взаимодействие»; в случае непринятия гипотезы H_{AB} вычисляют коэффициент детерминации $\eta^2_{Y/AB} = \frac{SS,\ \text{Взаимодействие}}{SS,\ \text{Итого}} \cdot 100\%$, показывающий процент общей вариации наблюдений СВ Y, объясняемый влиянием взаимодействия факторов A и B.

9.4. Корреляция и регрессия (Excel — программы № 4, № 14)

При исследовании процессов государственно-правового регулирования общественных отношений большую роль играет изучение взаимосвязей этих процессов, построение математических моделей, позволяющих провести количественный анализ состояния и динамики процессов.

Наиболее употребительной характеристикой степени взаимосвязи двух случайных величин X и Y является *коэффициент корреляции*. По парным наблюдениям этих величин, представленным в форме следующей таблицы:

Номер наблюдения	*X*	*Y*
1	x_1	y_1
2	x_2	y_2
.	.	.
.	.	.
n	x_n	y_n

выборочный коэффициент корреляции вычисляется по формуле:

$$r_{X,Y} = \frac{\overline{xy} - \overline{xy}}{\hat{\sigma}_X \hat{\sigma}_Y}, \qquad \textbf{(9.14)}$$

где $\overline{xy} = (x_1y_1 + x_2y_2 + ... + x_ny_n) / n$;

$$\overline{x} = (x_1 + x_2 + ... + x_n) / n;$$

$$\hat{\sigma}_X^2 = \left(x_1^2 + x_2^2 + ... + x_n^2\right) / n - (\overline{x})^2.$$

Из формулы (9.14) вытекает:

$$r_{X,Y} = r_{Y,X}; \quad r_{X,X} = \frac{\overline{xx} - \overline{x}\ \overline{x}}{\hat{\sigma}_X \hat{\sigma}_X} = \frac{\hat{\sigma}_X^2}{\hat{\sigma}_X^2} = 1.$$

Сформулируем и дадим графическую иллюстрацию свойств коэффициента корреляции:

1) $-1 \le r_{X,Y} \le 1$, причем:

- $-1 < r_{X,Y} < 0$, если и только если при увеличении значений любой одной из величин значения другой имеют тенденцию к уменьшению (рис. 9.7,*а*), и $0 < r_{X,Y} < 1$, если и только если при увеличении значений любой одной из величин значения другой имеют тенденцию к увеличению (рис. 9.7,*б*);
- $\left|r_{X,Y}\right| = 1$, если и только если парные наблюдения, т.е. точки с координатами (x_i, y_i), лежат на одной прямой (рис. 9.7,*в*,*г*);

2) чем меньше точки (x_i, y_i) рассеяны около некоторой прямой, тем ближе $\left|r_{X,Y}\right|$ к единице, и наоборот, чем ближе $\left|r_{X,Y}\right|$ к единице, тем меньше точки (x_i, y_i) рассеяны около прямой (рис. 9.7, *а* и *д*, *б* и *е*). Если точки рассеяны около линии, отличной от прямой, например, около параболы, то $\left|r_{X,Y}\right|$ близок к нулю (рис. 9.7, *ж*).

Из свойств коэффициента корреляции $r_{X,Y}$ вытекает, что $r_{X,Y}$ — это характеристика степени линейной взаимосвязи наблюдений СВ *X* и *Y*; величину $r_{X,Y}^2 \cdot 100\%$ называют *коэффициентом линейной детерминации*; его интерпретируют так: судя по наблюдениям, процент

вариации одной величины, объясняемый линейным влиянием другой, равен $r^2_{X,Y} \cdot 100\%$.

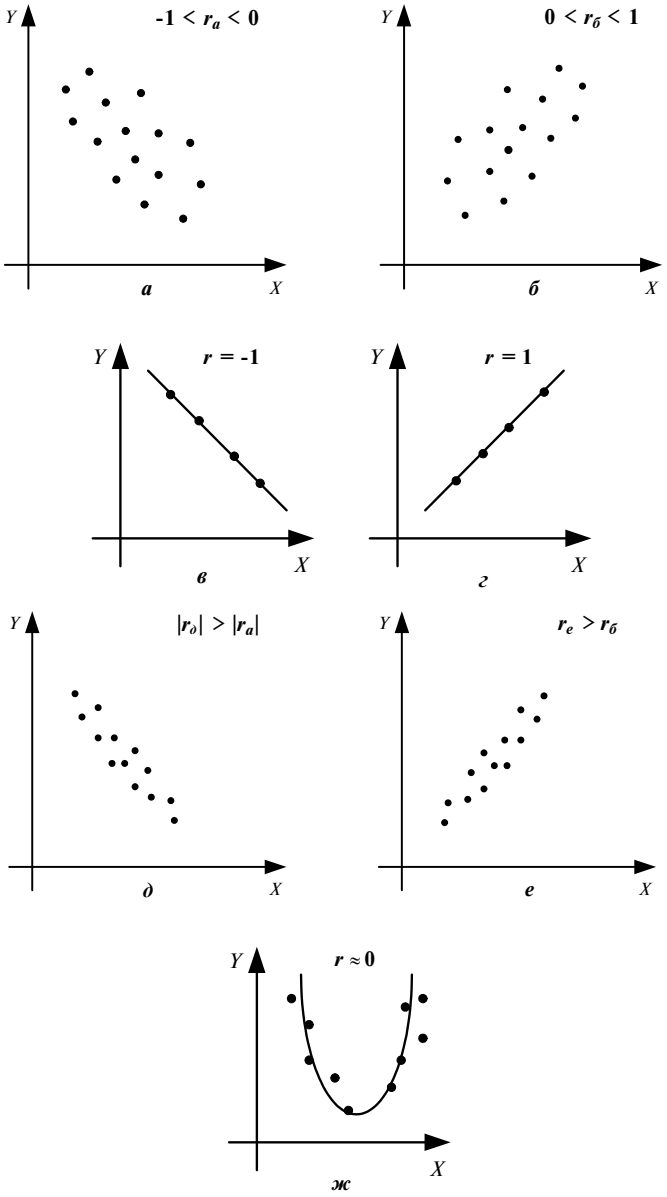


Рис. 9.7

➢ ***Программа № 4 «Корреляция»*** в качестве входных данных использует введенные в рабочий лист столбцы (или строки) наблюдений двух и более величин; на выходе — коэффициенты корреляции между каждой парой величин.

Пример 9.5.

В восьми районах собраны сведения о числе (Y) правонарушений за год, численности $X1$ населения (тыс. чел.) и размере $X2$ ежемесячного среднедушевого дохода (у.е.):

Y	367	133	100	200	120	270	120	260
$X1$	750	367	267	500	233	700	317	600
$X2$	18	20	33	18	31	18	31	20

Распечатка результатов программы № 4 (наблюдения величины Y введены в первый столбец, $X1$ — во второй, $X2$ — в третий) приведена на рис. 9.8. Расположенные на диагонали единицы — это коэффициенты корреляции: $r_{Y,Y}, r_{X1,X1}, r_{X2,X2}$; коэффициенты корреляции $r_{X1,Y} = 0{,}966$, $r_{X2,Y} = -0{,}762$, $r_{X2,X1} = -0{,}838$. Поясним, например, смысл $r_{X2,Y} = -0{,}762$; «−» означает, что, судя по наблюдениям, с увеличением ежемесячного среднедушевого дохода ($X2$) число (Y) правонарушений уменьшается; $r^2_{X2,Y} \times 100\% = 58\%$ — таков, судя по наблюдениям, процент вариации количества правонарушений (размера дохода), объясняемый линейным влиянием размера дохода (количества правонарушений).

	Столбец 1	*Столбец 2*	*Столбец 3*
Столбец 1	1,000		
Столбец 2	0,966	1,000	
Столбец 3	−0,762	−0,838	1,000

Рис. 9.8

Наиболее используемым методом построения математических моделей зависимостей по выборочным наблюдениям является *метод наименьших квадратов.* Поясним его на данных примера 9.5.

Предположим, что число Y правонарушений в районе связано с численностью $X1$ населения и среднедушевым доходом $X2$, называемых факторами, зависимостью

$$Y = \alpha_0 + \alpha_1 X1 + \alpha_2 X2 + \varepsilon \qquad \textbf{(9.15)}$$

(ε — случайный эффект влияния на Y прочих неконтролируемых факторов), называемой *двухфакторной линейной регрессией*; («линейность» означает, что и параметры α_0, α_1, α_2 регрессии, и факторы

$X1$ и $X2$ входят в регрессию в первой степени). Метод наименьших квадратов рекомендует находить оценки $\hat{\alpha}_0$, $\hat{\alpha}_1$, $\hat{\alpha}_2$ неизвестных параметров α_0, α_1, α_2, исходя из следующего требования:

$$\sum_{i=1}^{n} \underbrace{(\hat{\alpha}_0 + \hat{\alpha}_1 X1_i + \hat{\alpha}_2 X2_i}_{\hat{Y}_i} - Y_i)^2 \to \min ,$$

читаемого так: сумма квадратов отклонений значений $\hat{Y}_i$, рассчитанных по уравнению

$$\hat{Y}_i = \hat{\alpha}_0 + \hat{\alpha}_1 X1_i + \hat{\alpha}_2 X2_i , \qquad \textbf{(9.16)}$$

от наблюдений Y_i СВ Y, зафиксированных при значениях $X1_i$ и $X2_i$ факторов $X1$ и $X2$, должна быть минимальной.

Метод наименьших квадратов гарантирует получение «наилучших» оценок параметров регрессии («наилучших» — в смысле возможности, зная эти оценки, вынести достаточно надежные суждения о числовых значениях неизвестных параметров), строго говоря, при выполнении следующих требований:

а) все наблюдения СВ Y должны быть независимыми;

б) при каждом фиксированном наборе значений факторов наблюдения СВ Y проводятся в типичных условиях, а их результаты — нормально распределенные СВ с дисперсией, не изменяющейся при переходе от одного набора значений факторов к другому;

в) случайный эффект ε влияния прочих неконтролируемых факторов в регрессии (9.15) в среднем должен быть равным нулю.

В дополнение заметим, что «качество» оценок, полученных методом наименьших квадратов, тем выше, чем больше число наблюдений n по сравнению с числом m включенных в регрессию факторов.

➢ ***Программа № 14 «Регрессия»*** в качестве исходных данных использует:

- введенный в рабочий лист столбец наблюдений СВ *Y;*
- введенные в рабочий лист столбцы наблюдений по факторам $X1$, $X2$ ... (максимальное число факторов равно 16); «входной интервал X» определяется первым и последним наблюдениями соответственно первого и последнего факторов;
- уровень надежности (по умолчанию 95%) — это вероятность γ, используемая при построении интервальных оценок (уровень значимости $\alpha = 1 - \gamma$);
- если регрессия имеет вид $Y = \alpha_1 X1 + \alpha_2 X2 + \varepsilon$, т.е. в (9.15) константа α_0 отсутствует, то «в константу — ноль» следует поместить флажок.

Используя метод наименьших квадратов, программа вычисляет оценки параметров регрессии и проводит статистический анализ этих оценок.

Распечатка результатов работы программы № 14 для данных примера 9.5 (в рабочий лист введены три столбца) при $\gamma = 0{,}95$, регрессии вида (9.15) и выводе «остатков» приведена на рис. 9.9.

Вывод итогов

Регрессионная статистика	
Множественный *R*	0,970
R-квадрат	0,941
Нормированный *R*-квадрат	0,917
Стандартная ошибка	27,444
Наблюдения	8,000

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	2,000	59 799,742	29 899,871	39,700	0,001
Остаток	5,000	3765,758	753,152		
Итого	7,000	63 565,500			

	Коэффициенты	*Стандартная ошибка*	*t-статистика*	*P-значение*	*Нижние 95%*	*Верхние 95%*
Y-пересечение	−102,080	107,119	−0,953	0,384	−377,438	173,278
Переменная *X*1	0,524	0,095	5,513	0,003	0,280	0,768
Переменная *X*2	2,274	2,823	0,805	0,457	−4,984	9,531

Вывод остатка

Наблюдение	*Предсказанное Y*	*Остатки*
1	331,907	35,093
2	135,731	−2,731
3	112,880	−12,880
4	200,887	−0,887
5	90,514	29,486
6	305,703	−35,703
7	134,537	−14,537
8	257,842	2,158

Рис. 9.9

Поясним смысл наиболее важных результатов.

Регрессионная статистика:

Множественный $R = 0{,}970$ — такова, судя по наблюдениям, степень линейной зависимости числа Y правонарушений от двух факторов: численности $X1$ населения и среднедушевого дохода $X2$ (R — это множественный коэффициент корреляции, всегда: $0 \le R \le 1$; при одном факторе X: $R = \left| r_{X,Y} \right|$).

R-квадрат = 0,941 — судя по наблюдениям, 94,1% вариации числа правонарушений связано с линейным влиянием численности населения и среднедушевого дохода.

Стандартная ошибка = 27,444 — ошибка s, возникающая при замене фактических наблюдений Y_i рассчитываемыми $\hat{Y}_i$ по формуле (9.16);

$$s = \sqrt{\sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2/(n-m-1)} = \sqrt{\sum_{i=1}^{n} \text{«остатки»}^2/(n-m-1)},$$

где n — число наблюдений, m — число факторов (в примере $n = 8$, $m = 2$).

Дисперсионный анализ:

В первой таблице приведены результаты, необходимые для проверки гипотезы H_0: $\alpha_2 = \alpha_1 = 0$ (неизвестные параметры регрессии (9.15) одновременно равны нулю). Если «Значимость F» > α, гипотезу H_0 принимают: регрессионная модель (9.15) лишена смысла и отвергается; если «Значимость F» < α, гипотезу H_0 отвергают: регрессионная модель (9.15) адекватна. В примере «Значимость F» = 0,001 < α (напомним, $\alpha = 1 - \gamma = 1 - 0{,}95 = 0{,}05$): модель (9.15) адекватна.

Во второй таблице:

«Y-пересечение» — 102,08 — это оценка $\hat{\alpha}_0$,

«Переменная $X1$» 0,524 — это оценка $\hat{\alpha}_1$,

«Переменная $X2$» 2,274 — это оценка $\hat{\alpha}_2$,

Окончательно уравнение (9.16) имеет вид:

$$\hat{Y} = -102{,}08 + 0{,}524X1 + 2{,}274X2. \qquad \textbf{(9.17)}$$

Во второй и третьей строках этой таблицы приведены 95%-ные интервальные оценки генеральных параметров α_1 и α_2:

$$0{,}280 < \alpha_1 < 0{,}768; \qquad \textbf{(9.18)}$$

$$-4{,}984 < \alpha_2 < 9{,}531. \qquad \textbf{(9.19)}$$

Зная эти оценки, проверим на уровне значимости $\alpha = 1 - 0{,}95 = = 0{,}05$ гипотезы:

- H_0: $\alpha_1 = 0$ при альтернативе H_1: $\alpha_1 \neq 0$. Интервал (9.18) не накрывает число 0, поэтому гипотезу H_0 отвергаем; в этом случае говорят, что оценка $\hat{\alpha}_1$ статистически значима;

- H_0: $\alpha_2 = 0$ при альтернативе H_1: $\alpha_2 \neq 0$. Интервал (9.19) накрывает число 0, поэтому гипотезу H_0 принимаем: оценка $\hat{\alpha}_2$ статистически незначима.

Вывод остатка:

Здесь приведено «Предсказанное Y» — это $\hat{Y}_i$, рассчитанные по уравнению (9.17), и «Остатки» — это разности (Y_i — $\hat{Y}_i$). Зная эти остатки, можно рассчитать среднюю относительную ошибку (в %) предсказаний:

$\Delta = \frac{1}{n}\sum_{i=1}^{n}\frac{\left|Y_i - \hat{Y}_i\right|}{Y_i}\cdot 100\%$. В условиях примера $\Delta = 9{,}4\%$.

Подведем итог:

- модель (9.15) формирования годового числа Y правонарушений правомерна, так как гипотеза H_0: $\alpha_1 = \alpha_2 = 0$ отвергается при 5%-ном уровне значимости;
- уравнение (9.17) имеет достаточно хорошие характеристики: $R = 0{,}970$ близок к своему максимальному значению, равному 1; ошибка Δ невысока: $\Delta = 9{,}4\% < 10\%$. Поэтому уравнение можно использовать для прогноза годового числа правонарушений в районе при известной численности населения и размере ежемесячного среднедушевого дохода;
- использовать оценку $\hat{\alpha}_2 = 2{,}274$ для выяснения влияния фактора $X2$ (среднедушевого дохода) на Y (количество правонарушений) нельзя, так как была принята гипотеза H_0: $\alpha_2 = 0$; поэтому удалим фактор $X2$ из модели (9.15) и проведем расчеты для модели: $Y = \alpha_0 + \alpha_1 X1 + \varepsilon$.

Распечатка результатов работы программы № 14 (в рабочий лист введены два столбца — наблюдения величины Y и величины $X1$ из примера 9.15) приведена на рис. 9.10.

Итог в этом случае такой:

- модель $Y = \alpha_0 + \alpha_1 X1 + \varepsilon$ адекватна, так как «Значимость F» = $0{,}00 < \alpha$ (в примере $\alpha = 0{,}05$), и следовательно, гипотеза H_0: $\alpha_1 = 0$ отвергается; оценка $\hat{\alpha}_1$ — статистически значима;
- рассчитанное уравнение $\hat{Y} = -18{,}412 + 0{,}460X1$ имеет достаточно хорошие характеристики: $R = 0{,}966 \approx 1$ (обратим внимание на то, что при уменьшении числа факторов значение множественного коэффициента R всегда уменьшается); ошибка $\Delta\alpha = 9{,}97\% > 9{,}4\%$. Однако новое уравнение со «статистической точки зрения» лучше уравнения (9.17): «Стандартная ошибка нового уравнения» = 26,628, тогда как «Стандартная ошибка уравнения (9.17)» = 27,444;
- 95%-ная интервальная оценка параметра α_1: $0{,}337 < \alpha_1 < 0{,}583$. Смысл оценки $\hat{\alpha}_1 = 0{,}460$ таков: при росте численности района на одну ты-

сячу можно ожидать увеличения количества преступлений в среднем на 0,46 единицы; верхний 95%-ный предел этого увеличения составит 0,583; отсюда при росте численности на две тысячи можно ожидать увеличения количества преступлений в среднем на 0,92, а 95%-ный верхний предел этого увеличения составит 1,16 единицы.

Вывод итогов

Регрессионная статистика	
Множественный *R*	0,966
R-квадрат	0,933
Нормированный *R*-квадрат	0,922
Стандартная ошибка	26,628
Наблюдения	8,000

Дисперсионный анализ

	df	*SS*	*MS*	*F*	*Значимость F*
Регрессия	1,000	59 311,349	59 311,349	83,652	0,000
Остаток	6,000	4254,151	709,025		
Итого	7,000	63 565,500			

	Коэффициенты	*Стандартная ошибка*	*t-статистика*	*P-Значение*	*Нижние 95%*	*Верхние 95%*
Y-пересечение	−18,412	25,288	−0,728	0,494	−80,289	43,465
Переменная *X*1	0,460	0,050	9,146	0,000	0,337	0,583

Вывод остатка

Наблюдение	*Предсказанное Y*	*Остатки*
1	326,519	40,481
2	150,374	−17,374
3	104,383	−4,383
4	211,542	−11,542
5	88,746	31,254
6	303,524	−33,524
7	127,379	−7,379
8	257,533	2,467

Рис. 9.10

Конечно, эти выводы имеют место лишь при сохранении в целом той криминологической ситуации, которая имела место во время сбора статистических данных.

Контрольные вопросы и задания

1. Вычисление средней, дисперсии, моды и медианы по ряду наблюдений. Построение статистического и интервального рядов распределения. Гистограмма и кумулятивная кривая.
2. Точечные и интервальные оценки генерального среднего и вероятности. Погрешность выборочного среднего и вероятности.
3. Парный коэффициент корреляции, его смысл и свойства.
4. Метод наименьших квадратов. Пример использования регрессивного анализа при моделировании социально-правовых процессов.
5. Содержание пакета «Анализ данных» в Microsoft Excel и примеры задач правоприменительной деятельности, решаемых с использованием пакета.

Глава 10

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ СТАТИСТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

Информационной базой изучения преступности является государственная уголовная статистика, основу которой составляет первичный статистический учет (зарегистрированных преступлений и лиц, их совершивших; движения уголовных дел), осуществляемый органами внутренних дел. С помощью уголовной статистики определяется состояние преступности, ее уровень, структура и динамика; выявляются причины и условия, способствующие совершению преступлений, исследуются личности преступников, изучается система борьбы с преступностью.

Первостепенное значение для анализа оперативной обстановки и разработки адекватных мер реагирования на ее изменения имеет четко налаженная система сбора, обработки и выдачи информации о состоянии преступности и результатах борьбы с ней.

Учетно-регистрационная и статистическая работа в органах внутренних дел всегда была одним из наиболее трудоемких процессов. В ней принимают участие практически все службы и подразделения МВД — следователи, дознаватели, оперативные работники, руководители подразделений и другие сотрудники.

Государственная статистическая отчетность утверждается постановлением Госкомитета России по статистике и согласовывается с Генеральной прокуратурой России. В настоящее время под эгидой Госкомитета России прорабатывается вопрос о создании единой для всех правоохранительных органов (органы прокуратуры, военной прокуратуры, внутренних дел, Федеральной службы контрразведки, Федеральной пограничной службы, Государственного таможенного комитета, Департамента налоговой полиции) государственной отчетности о состоянии преступности.

Ведомственная статистическая отчетность утверждается приказом министра внутренних дел России. Головной организацией в органах внутренних дел в вопросах разработки и совершенствования ведомственной статистической отчетности является ГИЦ МВД Рос-

сии. Статистическая информация из подчиненных органов внутренних дел может быть истребована через ГИЦ в регламентном (на основании утвержденных форм статистической отчетности) или запросном (по поручению руководства Министерства) режимах.

Статистическая отчетность формируется на основе документов первичного учета, журнальных учетов, протоколов, рапортов, статистических отчетов подчиненных подразделений, а также иных документированных источников.

Единый учет преступлений заключается в первичном учете и регистрации выявленных преступлений и лиц, их совершивших. Он осуществляется в соответствии с Инструкцией о едином учете преступлений, 3-е издание которой утверждено Генеральной прокуратурой и МВД России 14 декабря 1994 г. № 20-1-85/94. Учет преступлений органами внутренних дел охватывает 95% криминальных проявлений и дает довольно полную картину оперативной обстановки в стране и ее регионах.

Инструкция разрешает *безбумажную технологию обработки статистической информации*, т.е. устраняет правовые препятствия на пути широкомасштабной информатизации в сфере учетно-регистрационной и статистической деятельности органов внутренних дел.

Первичный учет осуществляется путем заполнения документов первичного учета (статистических карточек):

- на выявленное преступление (форма № 1);
- о результатах расследования (раскрытия) преступления (форма № 1.1);
- на преступление, по которому лицо, его совершившее, установлено (форма № 1.2);
- на лицо, совершившее преступление (форма № 2);
- на лицо, подозреваемое в совершении преступления (форма № 2.1);
- о движении уголовного дела (форма № 3);
- о результатах возмещения материального ущерба и изъятия предметов преступной деятельности (форма № 4);
- о результатах рассмотрения дела в суде (форма № 6).

Документы первичного учета, зарегистрированные в районных, городских и транспортных органах внутренних дел в журналах учета, немедленно пересылаются в информационные центры МВД–УВД–УВДТ.

В информационных центрах на основе карточек ведутся по каждому району, городу контрольные журналы учета преступлений, уголовных дел и лиц, их совершивших. На основе обработанных карточек первичного учета в информационных центрах производится первичное формирование статистической отчетности о преступности.

Органы внутренних дел на базе документов первичного учета осуществляют выдачу *четырех форм государственной отчетности*:

- отчет о зарегистрированных, раскрытых и нераскрытых преступлениях (ф. 1);
- отчет о лицах, совершивших преступления (ф. 2);
- единый отчет о преступности (1-Г),
- отчет о следственной работе (1-Е), а также 16 форм ведомственной отчетности, дающих весьма детальную картину как состояния преступности, так и результатов деятельности различных служб органов внутренних дел по обеспечению правопорядка в стране, раскрытию преступлений, розыску преступников.

Помимо форм отчетности, базирующихся на документах первичного учета, в ГИЦ обрабатываются еще 47 форм, освещающих различные стороны оперативно-служебной деятельности.

О с н о в н ы м и з а д а ч а м и в области учетно-регистрационной и статистической работы остаются:

- регистрация и учет преступлений и административных правонарушений; лиц, их совершивших; уголовных дел; материалов; протоколов;
- проведение сверок учетных данных со статистическими данными информационных центров соответствующих МВД, ГУВД, УВД, УВДТ;
- осуществление контроля за полнотой и своевременностью регистрации в подразделениях горрайлиноргана заявлений, сообщений, иной информации о преступлениях и правонарушениях;
- осуществление контроля за своевременностью представления и качеством оформления подразделениями ГОРОВД документов первичного учета, в том числе формирующих оперативно-справочные, розыскные и криминалистические учеты регионального и федерального уровня;
- осуществление контроля за полнотой и объективностью сведений, отражаемых в документах первичного учета (об участии сил и средств в раскрытии преступления, о нахождении лица в момент совершения преступления в состоянии алкогольного опьянения и других);
- формирование совместно с подразделениями горрайлиноргана статистических отчетов по установленным МВД России формам;
- подготовка для руководства и подразделений горрайлиноргана справочной информации по данным, содержащимся в учетно-регистрационных и статистических документах.

Совершенствованию уголовной статистики в органах внутренних дел уделяется постоянное внимание. В этой связи можно выделить три направления:

- *улучшение системы статистических показателей* с целью более полного и точного отражения состояния и тенденций развития преступности, а также деятельности органов внутренних дел;
- *использование математических методов* с целью углубления аналитических исследований в процессе обработки статистической информации;
- автоматизация сбора и обработки статистической информации.

Автоматизированные аналитико-статистические ИС предназначены для сбора и обработки статистической информации. Поскольку статистика имеет дело с массовыми общественными явлениями, *первой особенностью* таких систем является сбор и обработка больших массивов первичной информации, полученной в результате статистического наблюдения; *вторая особенность* — оформление результатов обработки в виде разнообразных таблиц и графиков (большой объем выходной информации).

Накапливаемый массив статистических данных используется не только для составления в установленные сроки утвержденной статистической отчетности, но и в целях выдачи информации по разовым запросам. Следовательно, автоматизированные информационные системы, помимо аналитических задач, обеспечивают выполнение и справочных функций. В этом особенно наглядно проявляются достоинства вычислительной техники.

Далее будут рассмотрены примеры использования автоматизированных аналитико-статистических ИС в правоохранительной деятельности.

10.1. Справочная информационно-аналитическая система ГИБДД

Цель — обеспечить информационно-аналитическую службу ГИБДД на уровне МВД, УВД компьютерным инструментарием сбора, накопления, анализа информации и подготовки отчетов по основным показателям аварийности на транспорте.

Основные задачи:

- ведение и корректировка основных статистических показателей ДТП в регионах по годам;
- получение абсолютных и относительных показателей аварийности на основе имеющихся статистических показателей ДТП;
- прогнозирование статистических показателей ДТП в регионах;
- анализ состояния аварийности по группам регионов с оценкой резервов снижения уровня аварийности по разным категориям;

- ранжирование регионов по основным показателям аварийности с учетом структуры ДТП и их динамики за последние годы.

Система ориентирована на пользователя, не знакомого с правилами анализа крупномасштабных электронных таблиц. Сотрудник информационно-аналитической службы имеет возможность:

- вводить новые статистические показатели аварийности, корректировать старые и быстро определять степень наполненности базы данных по разным информационным срезам, регионам и годам;
- получать выборки абсолютных и относительных показателей, беря исходные данные аварийности за разные годы, по любым регионам, и представлять их в табличной форме;
- при создании таблицы манипулировать столбцами, придавая ей лучшую форму и сортируя строки-регионы по столбцам. Промежуточные аналитические таблицы могут включаться в конечный отчет.

Прогнозирование статистического показателя аварийности строится на основе автоматического выбора лучшего типа экстраполяционной модели (из девяти имеющихся). Пользователю предоставляется возможность вывести результаты прогнозных расчетов как в табличном виде, так и в виде столбиковой диаграммы.

Анализ резервов снижения аварийности позволяет выделить среди однотипных в социально-экономическом плане регионов такие, у которых состояние аварийности значительно ниже или выше по интересующим видам ДТП.

10.2. Автоматизированная информационная система «ГРОВД»

Автоматизированная информационная система (АИС) «ГРОВД» создана с целью совершенствования информационного обеспечения оперативно-розыскной и управленческой деятельности городских и районных органов внутренних дел.

Техническим обеспечением системы является сеть персональных компьютеров, работающих под управлением программно-инструментального средства FLINT (Академия МВД РФ). На базе АИС «ГРОВД» разработано и успешно используется кафедральное учение «Поиск 1».

АИС «ГРОВД» включает в себя следующие *учетно-информационные задачи*:

1) ПОДУЧЕТНИК (ЛИЦО);
2) ПОДУЧЕТНИК (ПРЕСТУПЛЕНИЕ);
3) АДМИНИСТРАТИВНАЯ КАРТОТЕКА;

4) ПОХИЩЕННЫЕ ВЕЩИ;
5) УЧЕТ ОРУЖИЯ;
6) НЕРАСКРЫТЫЕ ПРЕСТУПЛЕНИЯ;
7) УЧЕТ ЗАЯВЛЕНИЙ И СООБЩЕНИЙ;
8) СТАТИСТИКА;
9) УЧЕТ ЛИЧНОГО АВТОМОТОТРАНСПОРТА (АМТ).

Информационной основой указанных задач являются формализованные первичные документы (карточки), реквизиты которых достаточно полно и однозначно характеризуют соответствующие объекты учета.

Функциональные возможности АИС «ГРОВД»:

- накопление сведений об интересующих органы внутренних дел объектах учета согласно перечисленным задачам;
- оперативная коррекция накопленной информации;
- поиск интересующих сведений как по полным и (или) контекстным значениям реквизитов, а также по числовым интервалам;
- вывод найденных в системе сведений в максимальном объеме, в объеме, ограниченном требованиями пользователя, а также в специальных формах вывода, в том числе табличных;
- сортировка найденных записей по алфавиту, по датам, по убывающим значениям числовых реквизитов;
- многократное последовательное уточнение запроса в одном сеансе поиска;
- возможность проверки других массивов на наличие записей, относящихся к интересующему объекту, например проверка лиц, найденных в базе данных ПОДУЧЕТНИК (ЛИЦО) на их принадлежность к массивам ПОДУЧЕТНИК (ПРЕСТУПЛЕНИЕ), УЧЕТ ОРУЖИЯ, АДМИНИСТРАТИВНАЯ КАРТОТЕКА, УЧЕТ ЛИЧНОГО АМТ;
- защита информации от несанкционированного доступа посредством введения специальных паролей;
- изменение, в случае необходимости, первичных учетных документов (добавление/исключение реквизитов или изменение их параметров) без потери накопленной информации.

АИС «ГРОВД» в различных вариантах, адаптированных к местным условиям, и дополненная конкретными пожеланиями пользователей, эксплуатируется во многих регионах России и республиках СНГ на уровне не только горрайорганов, но и областных управлений. В сравнении с аналогичными системами, созданными на базе иных программных продуктов, АИС «ГРОВД» отличается своей надежностью, возможностью работы с неограниченным количеством объектов учета, удобством использования и доступностью освоения, а также соответствием принятой концепции информатизации органов внутренних дел.

Развитие АИС «ГРОВД» заключается в возможности включения в систему новых задач, а также в разработке специальной многофункциональной системы для проведения статистического анализа криминогенной обстановки в регионе на основании информации о зарегистрированных органами внутренних дел объектах учета.

10.3. Автоматизированная информационная система «КАДРЫ»

Адаптированная к рабочему месту сотрудника кадрового аппарата автоматизированная информационная система (АИС) «Кадры» предназначается для автоматизации процесса управления кадровым составом.

Применение АИС «Кадры» позволяет в диалоге с компьютером:

- накапливать и анализировать информацию по кадровому составу;
- производить расчеты по выслуге лет, связанные с присвоением очередных званий и уходом на пенсию;
- использовать информацию, хранящуюся в памяти ЭВМ, для автоматизации процесса подготовки кадровых документов;
- хранить и использовать справочную информацию как по личным делам, так и регламентирующую работу с кадрами;
- осуществлять эффективный контроль со стороны руководителей кадровых подразделений за состоянием кадровой работы.

АИС реализует следующие функции:

- ввод документов с возможностью символьного и цифрового представления информации, синтаксического и логического контроля; использование различных форм ввода документа;
- поиск документов по совокупности значений одного и (или) нескольких реквизитов; последовательный или прямой доступ к данным в зависимости от заданного поискового предписания;
- использование итерационного подхода при выборе данных;
- вывод полученной при поиске информации на экран видеотерминала, печать в виде отдельных первичных документов по произвольной форме (анкетный вид), списка первичных документов по произвольной совокупности реквизитов (табличный вид), статистических данных.

Система предусматривает адаптацию к конкретному пользователю, содержит удобные средства задания конфигурации, имеет возможность графического представления исходных данных.

Дальнейшее развитие АИС «Кадры» заключается в создании на ее основе системы поддержки кадровых решений, содержащей интеллектуальную составляющую, предоставляющую возможность ра-

боты с качественной, субъективной информацией и ориентированную на неподготовленного пользователя.

10.4. Автоматизированная система сбора и обработки отчетных данных управления государственной службы охраны «ОХРАНА»

«ОХРАНА» — это автоматизированная система сбора и обработки отчетных данных Управления Государственной службы охраны (УГСО) МВД. Система п о з в о л я е т:

1. Вводить, хранить и корректировать ежеквартальные отчетно-статистические данные подразделений УГСО МВД:

- итоговые сведения об объектах охраны и обособленных помещениях, их централизация и техническая оснащенность;
- сведения о находящихся в эксплуатации: ПЦН, концентраторах, средствах радиосвязи, зарядных устройствах, а также сигналах тревоги, поступивших на ПЦН;
- сведения о численности охраны, технической службы, а также о допущенных и предотвращенных кражах;
- сведения об охраняемых промпредприятиях, а также лицах, участвовавших в хищениях;
- показатели работы и дисциплины различных категорий работников сторожевой службы;
- сведения о находящихся в эксплуатации: системах централизованной охраны, устройствах уплотнения, концентраторах малой емкости, приемно-контрольных приборах, приборах для охраны квартир, приборах-датчиках, датчиках-извещателях, технических средствах для оснащения промпредприятий, шлейфах сигнализации, а также о вспомогательном оборудовании.

2. Вводить, хранить и корректировать отчетно-статистические данные подразделений УГСО МВД, представляемые ежемесячно в телеграммах:

- итоговые сведения о допущенных кражах, мелких хищениях, объектах и помещениях, принятых вновь под охрану, подключенных к ПЦН и другая информация;
- итоговые сведения о ложных сигналах тревоги, поступивших на ПЦН, а также информация о причинах их поступления.

3. Подготавливать отчеты на основании введенных отчетно-статистических данных по каждому подразделению УГСО МВД, представляемых ежеквартально и ежемесячно:

- суммарные данные по управлению, а также по каждому подразделению за конкретные год и квартал:
- общий отчет по управлению;

- сведения по технике;
- сведения о наличии СЦИ в подразделениях;
- сведения по средствам радиосвязи;
- численность охраны, охраняемых объектов;
- сведения о допущенных кражах;
- сведения о предотвращенных кражах;
- сведения о задержанных лицах;
- мелкие хищения;
- сведения о работниках охраны;
- данные по выбранному подразделению за год и месяц;
- допущенные кражи;
- ложные сигналы тревоги;
- суммарные данные по управлению на конец выбранного полугодия, а также абсолютный и относительный приросты по каждому показателю.

10.5. Справочная информационно-аналитическая система ГУ ОХРАНЫ РФ

Цель — обеспечить информационно-аналитическую службу охраны верхнего уровня (МВД/УВД) компьютерным инструментарием сбора, накопления, анализа и подготовки отчетов по основным показателям деятельности службы.

Основные задачи:

- ведение и корректировка основных статистических показателей деятельности службы в регионах по годам;
- получение любых абсолютных и относительных показателей деятельности службы на основе имеющихся исходных статистических показателей;
- прогнозирование статистических показателей деятельности службы в регионах.

Система ориентирована на пользователя, не знакомого с системами ведения и анализа крупномасштабных электронных таблиц общего назначения. Сотрудник информационно-аналитической службы имеет возможность:

- в диалоговом режиме вводить новые статистические показатели деятельности службы, корректировать старые и быстро определять степень наполненности базы данных по разным информационным срезам, регионам и годам;
- получать любые выборки абсолютных и относительных показателей, беря исходные данные о деятельности службы за разные годы, по любым регионам, и представлять их в табличной форме, готовой к включению в текстовые файлы;

- в процессе формирования таблицы манипулировать столбцами, придавая таблице лучшую форму, и сортируя строки-регионы по любому столбцу. Любые промежуточные формы аналитических таблиц могут накапливаться в выходном файле-отчете.

Прогнозирование любого статистического показателя деятельности службы строится на основе автоматического выбора лучшего типа экстраполяционной модели. Пользователь имеет возможность вывести результаты прогнозных расчетов как в табличном виде, так и в виде столбиковой диаграммы.

10.6. АСУ «РОВД»

АСУ «РОВД» — это комплекс информационных, программных, технических и организационных средств, обеспечивающих работу информационно-аналитического подразделения РОВД.

ИПС «Слежение» — это подсистема АСУ «РОВД», обеспечивающая ввод, хранение, корректировку и выдачу информации в соответствии с требованиями, предъявляемыми условиями работы информационно-аналитического подразделения РОВД. Структура ИПС «Слежение» предусматривает интеграцию всех имеющихся видов учета РОВД со всеми их взаимосвязями.

Виды учета:

1. КУП — информация о заявлениях и сообщениях о преступлениях и происшествиях, их разрешении и дальнейшем расследовании возбужденных уголовных дел. Цель — оперативно-поисковые возможности в отыскании похищенного и оперативная отработка лиц, задержанных за совершение конкретных преступлений. Данная форма осуществляет и аналитические возможности в пределах всей введенной информации, является основой при структурном построении статистических форм и базой для картотеки угнанного транспорта.

2. ФОРМА 1 — аналог единой статистической карточки на выявленное преступление, созданная на базе КУП, имеющая все поисковые режимы; является базой для статистики о заволокиченных преступлениях.

3. ФОРМА 1.1 — аналог единой статистической карточки о раскрытии преступлений или других результатах расследования, анализа деятельности каждого конкретного следователя, движения уголовного дела.

4. ФОРМА 2 — аналог единой статистической карточки на лицо, совершившее преступление, имеющая все атрибуты поисковых режимов с учетом характеристики данного лица.

5. ФОРМА 3 — аналог единого статистического талона о принятом решении по уголовному делу, его движению по подследственности.

6. ФОРМА 6 — информация о результатах судебного расследования.

Система пользователя АСУ «РОВД» состоит из программных модулей, реализующих взаимодействие пользователя с базами данных. Она обеспечивает проведение следующих видов работ:

- ввод информации о событиях, лицах и объектах, представляющей оперативный интерес (преступления, вещи и пр.); в предусмотренных случаях применяется автоматическое кодирование используемых реквизитов;
- хранение, корректировка и управление данными;
- автоматизированная поддержка (по команде пользователя) связей между информацией, имеющейся по одному и тому же событию, лицу или объекту;
- ввод, хранение и корректировка кодов предметов, преступников, происшествия, места происшествия и способа совершения преступления;
- выполнение интерактивных запросов;
- получение необходимых форм отчетности.

10.7. Автоматизированная система паспортного отделения

Автоматизированная система паспортного отделения (АСПО) служит для автоматизации работы сотрудников паспортного отделения районного отдела милиции (полиции). Система построена на принципах интеграции информации и обеспечивает автоматическое поддержание связей между следующими основными массивами информации:

- установочные данные на лицо и информация о его родственниках — информация о паспортах и вклеивании фотографий;
- информация о прописке и выписке лиц — дела по розыску утраченных и похищенных паспортов;
- судимости лиц, прописывающихся на обслуживаемой территории — розыскные дела на госдолжников и неплательщиков алиментов;
- административные правонарушения в сфере паспортной системы — информация об административном надзоре за лицом;
- информация о выезде лиц за рубеж.

В системе информация связана по ключевым реквизитам таким образом, что при обращении за получением информации о любом объекте (о лице, паспорте) пользователю предоставляется экран (досье), содержащий информацию, которая имеет отношение к запрашиваемому объекту, независимо от того, когда и от кого эта информация была получена (если она имеется). Появление новой или уточнение старой информации о любом объекте учета автоматически приводит к изменению информационной емкости досье независимо от того, по какому поводу это досье было сформировано.

После ввода информации любой категории, например о лице, пользователю предоставляется досье для ввода остальной связанной информации. При этом вся информация концентрируется в одном досье.

Система располагает набором регламентных запросов, позволяющим осуществлять поиск информации по заранее сформированным поисковым реквизитам баз данных.

Генератор запросов позволяет сформировать поисковый запрос по любой совокупности всех связанных баз данных и перевести его в регламентные.

Система включает в себя *перечень регламентных статистических отчетов*. Для пополнения перечня пользователем в системе предусмотрены точки входа, а также исходные тексты программ, формирующих регламентные отчеты.

Тексты форматов ввода, классификаторов и сообщений системы выведены в отдельный текстовый файл, в котором возможна их корректировка, а также перевод текстов на другой язык.

Сервис администратора базы данных предоставляет возможность ограничения по паролю и коду круга лиц, имеющих возможность ввода, просмотра или внесения изменений в имеющуюся информацию. Имеется возможность формировать страховые копии баз данных, изменять содержимое классификаторов информации, вести протокол работы системы.

АСПО является составной частью локальной вычислительной сети районного отдела милиции (полиции) и непосредственно ориентирована на автоматизацию адресного бюро республики, области, района.

Контрольные вопросы и задания

1. Что является информационной базой изучения преступности?
2. Каким документом регламентируется ведение статистической отчетности в органах внутренних дел?
3. В каких формах осуществляется первичный учет в органах внутренних дел?
4. Назовите формы государственной статистической отчетности органов внутренних дел.
5. Назовите основные задачи в области учетно-регистрационной и статистической работы.
6. Охарактеризуйте направления совершенствования уголовной статистики в органах внутренних дел.
7. Охарактеризуйте основные возможности статистического анализа данных в АСУ «РОВД».

Часть IV

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Глава 11

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В дежурных частях, у оперработников, участковых инспекторов милиции, следователей, сотрудников экспертно-криминалистических подразделений, паспортно-визовых аппаратов, других подразделений на документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения, в которых содержатся сведения:

- о правонарушителях и преступниках;
- о владельцах автомототранспортных средств;
- о владельцах огнестрельного оружия;
- о событиях и фактах криминального характера, правонарушениях;
- о похищенных и изъятых вещах, предметах антиквариата; а также другая, подлежащая хранению, информация.

Службы и подразделения органов внутренних дел характеризуются данными:

- о силах и средствах, которыми располагает орган;
- о результатах их деятельности.

Перечисленные выше сведения используются при организации работы подразделений и принятии практических мер по борьбе с преступностью и правонарушениями[1].

Кроме указанных сведений широко используется научная и техническая информация, необходимая для совершенствования деятельности органов внутренних дел.

В информационном обеспечении органов внутренних дел центральное место занимают учеты, которые используются для реги-

[1] Организация деятельности информационных работников горрайлинорганов внутренних дел: Сб. материалов для занятий в системе служебной подготовки / Под ред. *Ю.А. Буничева.* — М.: ГИЦ МВД РФ, 1995.

страции первичной информации о преступлениях и лицах, их совершивших.

Учет — это система регистрации и хранения информации о лицах, совершивших преступления, о самих преступлениях и связанных с ними фактах и предметах.

Учет подведомственных МВД преступлений охватывает 95% криминальных проявлений и дает достаточно полную картину оперативной обстановки в стране и ее регионах.

В целом по России в последние годы с помощью информации, содержащейся в учетах, раскрывается от 19 до 23% совершаемых преступлений, или почти каждое четвертое от общего числа по линии уголовного розыска[1].

11.1. Оперативно-справочные, оперативно-розыскные и дактилоскопические учеты

Первоначально учеты назывались *уголовной регистрацией*, что отражало суть деятельности по регистрации преступников.

Информацию о лицах упорядочивали по определенным группам признаков, что способствовало своевременному поиску необходимых сведений. В последующем учитывать стали не только самих преступников, но и предметы, следы, имевшие отношение к совершенному преступлению.

Впервые учеты были применены во Франции А. Бертильоном в начале XIX века. В предложенном им криминалистическом учете фотоснимки преступников группировались по определенным признакам. Впоследствии Р.А. Рейсом была разработана система ведения картотеки с антропологическим описанием личности, в которую заносились такие характеристики, как рост, цвет глаз, параметры головы и др. Наиболее эффективной оказалась немецкая система учета, состоявшая из трех взаимосвязанных частей для регистрации признаков внешности преступников — альбома фотографий, картотеки особых примет и фототеки[2].

В СССР в 1961 г. была введена Инструкция по учетам в органах внутренних дел. При МВД СССР в 1971 г. был создан Главный научный информационный центр управления информацией (ГНИЦУИ), впоследствии переименованный в Главный информационный центр (ГИЦ), а в МВД, УВД были созданы информационные центры (ИЦ).

---

[1] Федеральные учеты ГИЦ в борьбе с преступностью. — М., 1994.

[2] Программа компьютеризации органов внутренних дел РФ на 1991 г. и ближайшую перспективу: Утверждена Приказом МВД РФ № 104 от 05.07.91 г.

Главный информационный центр — самый крупный банк оперативно-справочной и розыскной информации в системе МВД России. На него возложена задача обеспечения органов и учреждений внутренних дел различной информацией — статистической, розыскной, оперативно-справочной, криминалистической, производственно-экономической, научно-технической, архивной. Это уникальные, многопрофильные централизованные массивы информации, в целом насчитывающие около 50 млн учетных документов.

В пофамильной оперативно-справочной картотеке на судимых лиц сосредоточено свыше 25 млн учетных документов, дактилоскопической — 17 млн. ГИЦ располагает уникальной базой данных на машинных носителях, содержащей статистические отчеты МВД, ГУВД, УВД, УВДТ по 50 формам за период с 1981 по 1992 г. и в ретроспективе до 1974 г.

Информационные центры МВД, УВД являются важнейшим звеном в системе информационного обеспечения органов внутренних дел Российской Федерации. На них ложится основная нагрузка в обеспечении информационной поддержки органов внутренних дел в раскрытии и расследовании преступлений, розыске преступников.

Информационные центры являются головными подразделениями в системе МВД, УВД, УВДТ в области информатизации: обеспечения статистической, оперативно-справочной, оперативно-розыскной, криминалистической, архивной и иной информацией, а также компьютеризации и построения региональных информационно-вычислительных сетей и интегрированных банков данных. Информационные центры выполняют возложенные на них обязанности в тесном взаимодействии с подразделениями аппарата МВД, УВД, УВДТ и горрайлинорганами, а также ГИЦ МВД России.

С помощью учетов получается информация, которая помогает в раскрытии, расследовании и предупреждении преступлений, розыске преступников, установлении личности неизвестных граждан и принадлежности изъятого имущества. Они формируются в горрайлинорганах, ИЦ МВД, ГУВД, УВД по территориальному (региональному) принципу и образуют федеральные учеты ГИЦ МВД России. Кроме того, учеты имеются в паспортных аппаратах.

Наряду с учетами в органах внутренних дел ведутся *экспертно-криминалистические централизованные коллекции и картотеки*, которые создаются и хранятся в ЭКЦ МВД России (федеральные) и ЭКУ МВД, ГУВД, УВД (региональные). Коллекции и картотеки ЭКУ и ЭКЦ ориентированы прежде всего на обеспечение раскрытия и расследования преступлений.

Накапливаемая в учетах, коллекциях и картотеках оперативно-справочная, розыскная и криминалистическая информация именуется *криминальной*.

Учеты классифицируются по функциональному и объектовому признакам.

- *Функционально* учеты разделяются на три группы:
  - оперативно-справочные;
  - розыскные;
  - криминалистические.
- *По объектовому признаку* учеты разделяют на три группы:
  - лиц;
  - преступлений (правонарушений);
  - предметов.

Основная оперативно-справочная и розыскная информация формируется в горрайлинорганах. Часть ее оседает на месте, а другая — направляется в ИЦ и ГИЦ для формирования единого банка данных.

Информационная база системы МВД построена *на принципе централизации учетов*. Ее составляют оперативно-справочные, розыскные и криминалистические учеты и картотеки, сосредоточенные в ГИЦ МВД России и ИЦ МВД, УВД, УВДТ, и локальные учеты горрайлинорганов. В целом их массивы оцениваются примерно в 250—300 млн учетных документов.

Централизованные оперативно-справочные, криминалистические и розыскные учеты располагают следующими сведениями о гражданах России, иностранцах и лицах без гражданства:

- судимость, место и время отбывания наказания, дата и основание освобождения;
- перемещение осужденных;
- смерть в местах лишения свободы, изменение приговора, амнистия, номер уголовного дела;
- место жительства и работы до осуждения;
- задержание за бродяжничество;
- группа крови и дактилоформула осужденных.

Дактилоскопический учет позволяет устанавливать личность преступников, арестованных, задержанных, а также неизвестных больных и неопознанных трупов. Дактилоскопические картотеки насчитывают 18 млн дактилокарт. В них поступает свыше 600 тыс. запросов, по которым выдается около 100 тыс. рекомендаций. Информация картотек способствовала раскрытию преступлений или установлению лица в 10 тыс. случаев. В настоящее время это преимущественно ручные картотеки.

Порядок формирования и ведения централизованных оперативно-справочных, розыскных, криминалистических учетов, экспертно-криминалистических коллекций и картотек органов внутренних дел Российской Федерации регламентируется Приказом МВД России № 400 от 31.08.93 г.

Учеты органов внутренних дел в зависимости от способа обработки информации подразделяются на три вида: ручные, механизированные, автоматизированные.

Автоматизированные учеты состоят из ряда автоматизированных информационно-поисковых систем (АИПС). Накопление и обработка криминальной информации с помощью АИПС осуществляется в региональных банках криминальной информации (РБКИ)[1].

Автоматизированные информационно-поисковые системы используются для выполнения основных функций органов внутренних дел. Их особенность заключается в накоплении и постоянном корректировании больших массивов информации о лицах, фактах и предметах, представляющих оперативный интерес.

АИПС работают преимущественно по принципу «запрос — ответ», поэтому обработка информации в них связана в основном не с преобразованием первичных данных, а с их поиском.

Принципиальную особенность АИПС составляет понятие «информационный поиск». *Информационный поиск* — это процесс отыскания в каком-то множестве документов тех, которые посвящены указанной в информационном запросе теме (предмету) или содержат необходимые потребителю факты, сведения[2].

Автоматизированные информационно-поисковые системы принято подразделять на *документальные* и *фактографические*. Такое деление основано на различии объектов поиска. В документальных — объектами поиска являются документы, их копии или библиографическое описание. В фактографических — искомыми объектами могут быть записи, характеризующие конкретные факты или явления.

В системе органов внутренних дел АИПС решают задачи сбора, хранения, поиска и выдачи оперативно-розыскной и справочной информации.

Приведем основные АИПС и кратко охарактеризуем их назначение и возможности.

➢ АИПС «КАРТОТЕКА» — автоматизированный пофамильный и дактилоскопический учет, служит для получения сведений о гражданах РФ, иностранцах и ЛБГ: о судимости, месте и времени отбывания наказания, дате и основании освобождения, о смерти в местах лишения свободы, об изменении приговора, амнистии, о месте жительства и работе до осуждения; о розыске лиц, задержанных за бро-

---

[1] Федеральные учеты ГИЦ в борьбе с преступностью. — М., 1994.

[2] Информатика и вычислительная техника в деятельности органов внутренних дел. Ч. 4. Автоматизация решения практических задач в органах внутренних дел: Учеб. пособ. / Под ред. *В.А. Минаева*. — М.: ГУК МВД РФ, 1996.

дяжничество, перемещении осужденных; группе крови, дактилоскопической формуле.

➢ АИПС «ОПОЗНАНИЕ» выдает информацию о лицах, пропавших без вести, неопознанных трупах, неизвестных больных и детях — гражданах Российской Федерации, СНГ и лицах без гражданства.

➢ АИПС «ФР-ОПОВЕЩЕНИЕ» обеспечивает учет преступников, разыскиваемых по искам предприятий и организаций (госдолжников) или граждан (неплательщиков алиментов), пропавших без вести, отрабатывает запросы на лиц, находящихся в федеральном розыске, а также готовит циркуляры на объявление или прекращение розыска.

➢ АИПС «ОРУЖИЕ» позволяет вести учет утраченного (похищенного, утерянного) и выявленного (изъятого, найденного, добровольно сданного) вооружения (стрелковое оружие, гранатометы, артиллерийские системы и другое вооружение).

➢ АИПС «АВТОПОИСК» содержит информацию о легковых и грузовых автомобилях, автобусах, полуприцепах отечественного и иностранного производства со следующими установочными данными — госномер, номера двигателя, кузова и шасси. В информационных центрах МВД, УВД дополнительно осуществляется регистрация мотоциклов, мотороллеров и мотоколясок.

➢ АИПС «АНТИКВАРИАТ» выдает сведения об утраченных и выявленных предметах, представляющих историческую, художественную или научную ценность. К ним относят археологические находки, предметы древности, антропологические и этнографические предметы, исторические реликвии, художественные произведения и предметы искусства.

➢ АИПС «ВЕЩЬ» информирует пользователя о похищенных и изъятых номерных вещах, а также документах, ценных бумагах общего государственного обращения в связи с совершенными преступлениями.

➢ АИПС «СЕЙФ» позволяет осуществлять сбор, обработку и выдачу информации о преступлениях, при совершении которых взламывались металлические хранилища.

В настоящее время начато внедрение автоматизированных информационно-поисковых систем «ДОСЬЕ» и «НАСИЛИЕ».

➢ АИПС «ДОСЬЕ» позволяет получить сведения об особо опасных рецидивистах, «ворах в законе», «авторитетах» преступного мира и др.: установочные данные, приметы, место работы, жительства, связи, привычки и т.д.

➢ АИПС «НАСИЛИЕ» обеспечивает такими сведениями о тяжких нераскрытых и раскрытых преступлениях, связанных с насилием против личности, как предмет посягательства, место, время и способ совершения, описание изъятых следов и др.

Для учета правонарушений, совершенных иностранцами и лицами без гражданства, разработана и функционирует АИПС «КРИМИНАЛ-И», включающая *пять подсистем*:

- АИПС «Криминал-И Адмпрактика» содержит сведения об иностранцах и ЛБГ, совершивших административные правонарушения;
- АИПС «Криминал-И Преступление» выдает сведения о происшествиях и преступлениях с участием иностранцев и ЛБГ;
- АИПС «Криминал-И ДТП» обеспечивает сведениями об иностранцах и ЛБГ, участниках ДТП на территории России;
- АИПС «Криминал-И Розыск» содержит данные о находящихся в розыске или разысканных иностранцах;
- АИПС «Криминал-И Наказание» содержит сведения об иностранцах и гражданах России, постоянно проживающих за границей, находящихся под следствием, арестованных или отбывающих наказание на территории РФ.

В АИПС вся поступающая информация учитывается и систематизируется таким образом, что позволяет, во-первых, организовать неоднократное обращение к ней различных аппаратов и служб органов внутренних дел и, во-вторых, постоянно пополнять ее новой и удалять устаревшую информацию. При этом необходимо подчеркнуть важнейшую характеристику автоматизированных информационных систем: однократный ввод информации и последующее многократное ее использование. Информация концентрируется, обрабатывается, хранится и выдается пользователям в строгом соответствии с нормативными актами, регламентирующими ведение оперативно-розыскных и профилактических учетов органов внутренних дел.

Первые автоматизированные информационные системы появились в полиции США в начале 1950-х гг. и предназначались для обеспечения розыска угнанных автомашин. В Европе АИПС стали эксплуатироваться с середины 1950-х гг. в полиции ФРГ. В настоящее время во всех развитых странах компьютерные системы применяются для решения широкого круга полицейских задач.

В РФ в системе ОВД функционирует система информационного обеспечения органов внутренних дел — *сеть автоматизированных банков данных* (АБД), которая поддерживает в настоящее время значительный объем информации. В состав системы входят около 3 тысяч горайорганов, 89 информационных центров министерств и управлений, 20 информационных подразделений управлений внутренних дел на транспорте, а также большое число предприятий и учреждений ОВД.

К настоящему времени в 16 регионах, на которые приходится 51% общей регистрации преступлений, закончен монтаж и ведется отладка программно-технических комплексов, приобретенных по

контракту с фирмой «Сименс-Никсдорф». В целом по МВД внедрено и находится в круглосуточной эксплуатации свыше 250 локальных вычислительных сетей, более 40 территориально распределенных информационных систем с удаленным доступом к банкам данных непосредственно из ГОРОВД, а также порядка 3000 автоматизированных рабочих мест на базе ПЭВМ.

11.2. Современные информационные технологии в правоохранительной деятельности

Современные информационные технологии можно определить как систему операций по сбору, хранению, обработке и передаче информации, осуществляемых по каналам связи с использованием компьютерной техники[1].

Основными принципами современной информационной технологии являются:

- интерактивный, «дружественный» интерфейс работы;
- интегрированность с другими программными продуктами;
- гибкость процесса изменения данных и постановки задач.

Выделяют несколько *видов* информационных технологий:

- ИТ обработки данных;
- ИТ управления;
- ИТ автоматизации офиса;
- ИТ поддержки принятия решений;
- ИТ экспертных систем

и т.д.

Примерами современных информационных технологий автоматизации офиса являются электронная почта, аудиопочта, текстовый процессор, электронные таблицы, телеконференции, видеотекст и т.д.

Одной из самых популярных общеупотребительных информационных технологий является *мультимедиа.* Понятие «мультимедиа» обобщает различные технологии, объединенные с помощью соответствующих аппаратно-программных средств. К мультимедиа можно отнести:

- неподвижное изображение на экране дисплея, сопровождаемое звуковыми эффектами;
- графическое изображение со звуком;
- движущееся изображение;
- анимация, т.е. последовательность изображений, создающая эффект движущегося изображения (аналог мультипликации).

---

[1] Основы автоматизации управления в органах внутренних дел: Учебник / Под ред. *В.А. Минаева, А.П. Полежаева.* — М.: Академия МВД РФ, 1993.

В органах внутренних дел внедрение новых информационных технологий идет через построение на основе современных компьютеров локальных, региональных и общегосударственной отраслевых информационно-вычислительных сетей, которые будут способствовать дальнейшему совершенствованию информационного обеспечения ОВД[1].

Одними из основных компонентов информационно-вычислительной сети общего пользования органов внутренних дел (ИВС ОВД) являются Федеральный банк криминальной информации (ФБКИ) вместе с РБКИ, которые представляют собой единую информационную структуру ОВД.

Работы по автоматизации информационного обеспечения органов внутренних дел ведутся с начала 1970-х гг. Вначале информационные центры оснащались ЭВМ типа Минск-22, Минск-32, затем ЭВМ типа ЕС и СМ, которые использовались главным образом для обработки статистических данных. Слабость технической базы и отсутствие развитых программных средств (в том числе СУБД) не позволяли реализовать концепцию единой базы данных как на региональном, так и на федеральном уровнях.

Сейчас большинство регионов России приступило к созданию региональных информационных систем, но эти процессы пока еще носят стихийный характер. Разрабатываемые системы зачастую реализуют собственный язык манипулирования данными, свои потоки и форматы данных, свои решения в части архитектуры и выбора технических средств. Такой подход может сделать невозможным в дальнейшем реализацию единого информационного пространства. Очевидна необходимость единой, от уровня горрайлинорганов, отделений милиции до федеральных учетов ГИЦ, стройной системы информационного обслуживания массового пользователя.

До сих пор компьютеризация правоохранительных органов сводилась к поставке только персональных компьютеров и создания на их базе простейших автономных систем, дорогостоящих автоматизированных «пишущих машинок» и «записных книжек». С помощью одних только персональных ЭВМ невозможно решить проблемы информатизации, так как прежде всего необходимы крупные хранилища колоссальных картотек — интегрированные банки данных. Вся информация по всем категориям учета систематизируется, хранится и поддерживается в актуальном состоянии в одном месте, с обеспечением межрегионального обмена, а также прямого доступа к ней практических работников с мест в пределах своей компетенции. Эти функции обеспечивают мощные базовые ЭВМ и специализированные сетевые компьютерные средства.

---

[1] Техническое задание на создание информационной вычислительной сети органов внутренних дел РФ: Утверждено Министром ВД 22.02.92 г.

ГИЦ подготовил план технического переоснащения информационных центров, рассчитывая на развитие контракта с фирмой «Сименс-Никсдорф» и получение суперсовременных ЭВМ типа RM−600 в качестве центральных машин для ИВС зонального и регионального уровня.

Высокая производительность и надежность этих вычислительных комплексов позволяет включить их в качестве опорных в единую сеть МВД России с выходом на компьютерные сети смежных ведомств в системе правоохранительных органов Российской Федерации, а также в страны СНГ.

Одновременно разрабатывается программное обеспечение для информационных систем разного уровня: ГОРОВД — МВД, УВД — МВД России. Для автоматизированных рабочих мест используются известные пакеты — FLINT, PARADOX, Clipper, текстовые редакторы LEXICON, WinWord, сетевые СУБД, БИНАР-3, а в последнее время начинается внедрение мощного средства — ORACLE, которое обеспечивает многопользовательский многозадачный режим работы территориально распределенной компьютерной сети.

В 1994 г. велись работы по созданию и внедрению более 150 новых систем и задач, внедрению интегрированных банков данных в 6 региональных центрах.

В целом в органах внутренних дел России в автоматизированном режиме с помощью ЭВМ обрабатываются задачи оперативно-розыскного и справочного назначения с количеством обрабатываемых запросов примерно 10 млн в год, а также задачи учетно-статистического, управленческого и производственно-экономического назначения. Всего же в машинном контуре ежегодно обрабатывается свыше 150 млн документов.

Планируется объединение на логическом уровне региональных банков данных нескольких МВД, УВД близлежащих областей, находящихся в зоне экономического района. Такие зональные центры (в пределах 10 на территории Российской Федерации) будут обеспечивать требуемый уровень интеграции информационных ресурсов и способствовать реальному формированию единого информационного пространства подразделений ОВД.

Нормативной базой для проведения крупномасштабных работ по компьютеризации ОВД является «*Концепция развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью*», утвержденная Приказом МВД РФ № 229 от 12 мая 1993 г., на основе которой разработаны основные принципы создания ИВС, предложены типовые архитектурные и программно-технические решения, разрабатываются комплексы прикладных программмных средств.

В целом концепция и техническое задание на создание ИВС ориентированы на несколько уровней сбора, обработки и накопле-

ния информации. На уровне горрайлинорганов рабочими местами являются персональные компьютеры IBM PC, объединенные, если это необходимо, в локальную вычислительную сеть.

На более высоком уровне основой системы являются такие компьютеры, как MX-300, MX-500 фирмы «Сименс-Никсдорф» с большими объемами жестких дисков и оперативной памяти и высокой скоростью обработки данных. Эти компьютеры работают под управлением многопользовательской операционной системы (ОС) UNIX и используют систему управления базами данных Oracle.

Основным достоинством ОС UNIX является возможность системными средствами решать проблему одновременной работы многих пользователей с разграничением их доступа к системным ресурсам и данным, независимо от способа подключения этих пользователей.

Все это послужит основой формирования региональных информационных сетей ОВД, объединяемых затем в единую информационно-вычислительную сеть (ИВС) МВД Российской Федерации, которая в техническом плане представляет собой совокупность связанных каналами и линиями связи информационно-вычислительных центров (районов, крупных городов, республик, краев и областей, экономических зон России в целом) с подключенными к ним терминалами в горрайлинорганах и службах МВД, УВД.

Кроме информационных центров МВД, УВД, традиционно оснащавшихся ЭВМ большой и средней мощности для обработки статистики и ведения централизованных автоматизированных учетов, в настоящее время идет активное внедрение вычислительной техники в городские и районные подразделения ОВД.

Многие регионы используют возможности модемной связи по телефонным каналам для передачи в ГИЦ данных форм статистической отчетности и получения сборников, подготовленных в ГИЦ, а также для обмена между собой различной информацией.

Использование модемной связи позволило уменьшить трудоемкость обработки статистической отчетности в ГИЦ и повысить ее оперативность, сократить количество ошибок, минимизировать затраты ручного труда. В ГИЦ по модемной связи с соблюдением определенных требований могут быть переданы сведения по любой несекретной форме статистической отчетности, которые будут своевременно обработаны автоматизированным программным комплексом.

Создание и внедрение в практическую деятельность органов внутренних дел современных информационных технологий, *реализованных в виде различных информационных систем*, происходит столь быстрыми темпами, что не только у непосвященных, но и у специалистов подчас не хватает времени, чтобы оценить всю глубину и масштабность происходящих процессов. Конечная эффективность значительных затрат, вкладываемых в информатизацию деятельно-

сти правоохранительных органов, в определяющей мере зависит от настоящего профессионализма и умения работать с информацией.

11.3. Автоматизированные информационные системы

Информационная технология (ИТ) тесно связана с информационными системами (ИС), которые являются для нее *основной средой функционирования*[1].

Информационная технология является процессом, состоящим из четко регламентированных правил, действий, этапов обработки данных. Основная цель ИТ — в результате переработки первичной информации получить необходимую для пользователя информацию.

Информационная система является средой, составляющими элементами которой являются компьютеры, компьютерные сети, программные продукты, базы данных, люди и т.д. Основное назначение ИС — организация хранения и передачи информации. ИС — человеко-компьютерная система для организации хранения, обработки и выдачи информации в интересах достижения поставленной цели, использующая компьютерную информационную технологию.

Обычно в термин ИС обязательно вкладывается понятие автоматизируемой системы, при этом предполагается, что в процессе обработки информации главная роль отводится компьютеру. Можно дать следующее определение автоматизированной информационной системы (АИС):

АИС (Банк данных) — это совокупность тем или иным образом структурированных данных (базы данных) и комплекса аппаратно-программных средств для хранения данных и манипулирования ими (рис. 11.1).

Под *структурированием* понимают процесс приспособления данных к нуждам автомата, например ограничение длины и значений данных, т.е. введение соглашений о способах представления данных.

Базой данных (БД) в строгом смысле слова называют файл взаимосвязанных структурированных данных, определенных посредством схемы, не зависящей от программ, и расположенных на запоминающих устройствах с прямым доступом. В качестве последних чаще всего выступают магнитные диски.

В последнее время наибольшее распространение получили *реляционные БД* (РБД). В них информация хранится в одной или нескольких таблицах. Связь между таблицами осуществляется посред-

---

[1] Информатика и вычислительная техника в деятельности органов внутренних дел. Ч. 5. Аналитическая деятельность и компьютерные технологии: Учеб. пособ. / Под ред. *В.А. Минаева*. — М.: ГУК МВД РФ, 1996.

ством значений одного или нескольких совпадающих полей. Каждая строка таблицы в РБД уникальна. Для обеспечения уникальности строк используются *ключи*, которые включают одно или несколько полей. Ключи хранятся в упорядоченном виде, что обеспечивает прямой доступ к записям таблицы во время поиска.

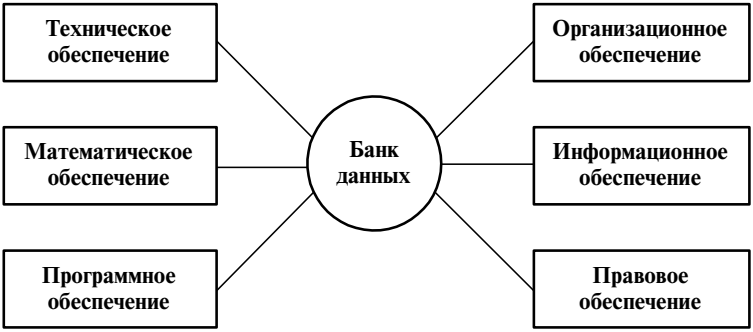


Рис. 11.1. **Состав Банка данных**

Для взаимодействия пользователя с БД используются ***системы управления баз данных*** (СУБД) — комплекс программ и языковых средств, предназначенных для создания, ведения и использования баз данных.

Современные СУБД обеспечивают:

- набор средств для поддержки таблиц и соотношений между связанными таблицами;
- развитый пользовательский интерфейс, позволяющий вводить и модифицировать информацию, выполнять поиск и представлять информацию в текстовом или графическом виде;
- средства программирования высокого уровня, с помощью которых можно создавать собственные приложения.

Подходить к рассмотрению многообразия АИС можно по-разному (рис. 11.2). Так, можно исходить из функционального назначения АИС (табл. 11.1). Можно классифицировать АИС по назначению:

- АИС для сбора и обработки учетно-регистрационной и статистической информации;
- АИС оперативного назначения;
- АИС для использования в следственной практике;
- АИС криминалистического назначения;
- АИС для использования в экспертной практике;
- АИС управленческого назначения

и т.д.

Использование АИС в следственной, оперативно-розыскной и экспертной деятельности рассмотрена далее.

Однако при такой классификации не учитываются многие важнейшие характеристики АИС, такие как характер выдаваемой информации, способ организации поискового массива, тип критерия смыслового соответствия и т.д. Одна из наиболее полных классификаций по *признакам, отражающим возможность унификации* при создании и использовании АИС, предложена, например, в работе, изданной под редакцией А.П. Полежаева и А.И. Смирнова[1].

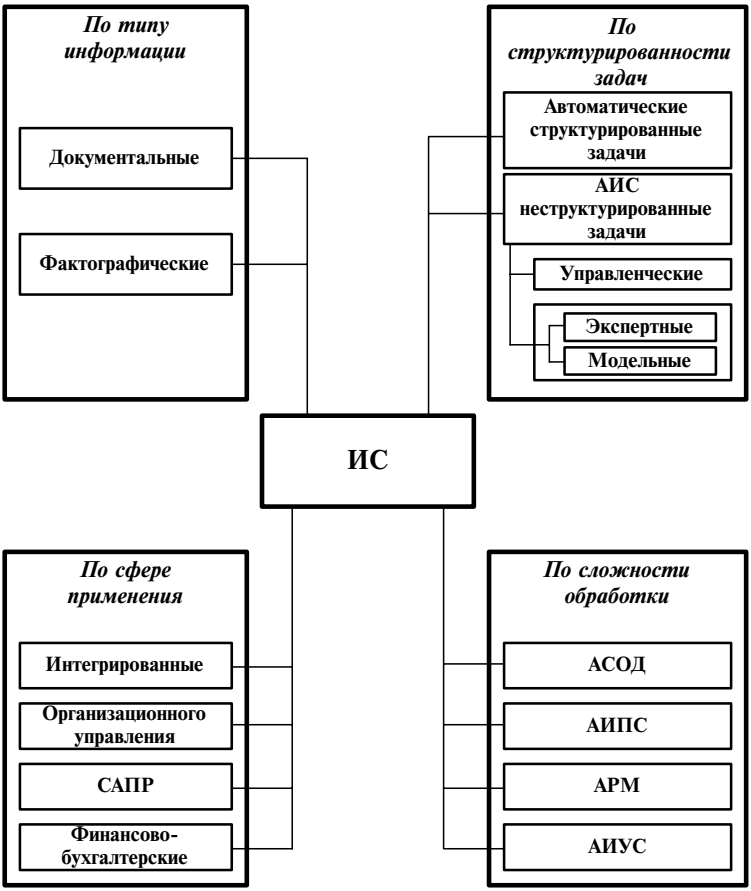


Рис. 11.2. **Классификация информационных систем**

[1] Основы применения вычислительной техники в органах внутренних дел / Под ред. *А.П. Полежаева*, *А.И. Смирнова*. — М.: Академия МВД, 1988.

Таблица 11.1. ***Функции автоматизированных информационных систем***

Управленческие системы	*Финансовые системы*	*Кадровые системы*	*Производственные системы*
Контроль за деятельностью организации	Бухгалтерский учет и расчет зарплаты	Учет персонала организации	Исследование спроса и прогноз продаж
Анализ стратегических и тактических ситуаций	Финансовый прогноз и анализ	Контроль сроков, поощрений, взысканий, выслуги	Анализ и прогноз производственных затрат
Выявление тактических проблем	Составление финансового плана	Планирование отпусков	Рекомендации по снижению себестоимости
Обеспечение выработки решений	Контроль расходов и доходов	Анализ и планирование переподготовки	Учет заказов
	Корректировка бюджета	Анализ и прогноз потребности в трудовых ресурсах	

Опыт практического применения АИС показал, что наиболее точной, соответствующей самому назначению АИС следует считать классификацию по степени сложности технической, вычислительной, аналитической и логической обработки используемой информации. При таком подходе к классификации можно наиболее тесно связать АИС и соответствующие информационные технологии, основные виды которых были приведены выше (см. раздел 11.2).

Соответственно, на наш взгляд, можно выделить следующие в и д ы А И С, используемые в деятельности органов внутренних дел:

- автоматизированные системы обработки данных (АСОД);
- автоматизированные информационно-поисковые системы (АИПС);
- автоматизированные информационно-справочные системы (АИСС);
- автоматизированные рабочие места (АРМ);
- автоматизированные системы управления (АСУ);
- экспертные системы (ЭС) и системы поддержки принятия решений.

Классификация АИС определяет место каждой системы, ее связь с другими системами и пути возможного построения новых информационных систем. Так, например, сочетание АИСС и АСОД получило название автоматизированной информационно-расчетной системы, а в состав АСУ может входить одновременно несколько АРМ и ЭС.

Рассмотрим каждый из перечисленных в классификации типов АИС подробнее и приведем конкретные примеры использования соответствующих систем.

➢ ***Автоматизированные системы обработки данных*** (АСОД) предназначены для решения хорошо структурированных задач, по которым имеются входные данные, известны алгоритмы и стандартные процедуры обработки. АСОД применяются в целях автоматизации повторяющихся рутинных операций управленческого труда персонала невысокой квалификации. Как самостоятельные ИС АСОД в настоящее время практически не используются, но вместе с тем они являются обязательными элементами большинства сложных ИС, таких как АИСС, АРМ, АСУ. В частности, в ОВД АСОД используются для статистической обработки информации по заданным формам отчетности.

➢ ***Автоматизированные информационно-поисковые системы*** (АИПС) — системы, обеспечивающие отбор и вывод информации по заданному в запросе условию. АИПС и рассматриваемые далее АИСС являются основными составляющими элементами информационной технологии управления. Важность АИПС в управлении состоит в том, что необходимость работы с ними и, соответственно, результаты используются на всех уровнях управления — начиная от операционного и кончая стратегическим. Примеры АИПС, которые в практической работе правоохранительных органов реализованы как автоматизированные учеты, были рассмотрены выше.

➢ ***Автоматизированные информационно-справочные системы*** (АИСС) — системы, работающие в интерактивном режиме и обеспечивающие пользователей сведениями справочного характера. Они производят ввод, систематизацию, хранение, выдачу информации по запросу пользователя без сложных преобразований данных.

АИСС «СВОДКА» позволяет работать с базой данных, создаваемой по поступающей в органы внутренних дел оперативной информации о происшествиях и преступлениях, осуществлять поиск в БД по реквизитам, а также вести статистическую обработку данных, составлять отчеты при поступлении запросов и после исполнения документов.

АИСС «ГАСТРОЛЕРЫ» предназначена для автоматизированной обработки оперативными подразделениями УВДТ и ОВДТ информации о лицах, представляющих оперативный интерес для органов внутренних дел на транспорте, и их связях; похищенных на транспорте, неразысканных или добровольно сданных вещах, имеющих индивидуальные номера или характерные особенности.

Система позволяет решить три основные задачи: «ЛИЦО», «НЕРАСКРЫТЫЕ ПРЕСТУПЛЕНИЯ», «ВЕЩИ». Для работы требуется

IBM PC-совместимый компьютер и пакет прикладных программ FLINT 3.03 или 4.0.

АИСС «Грузы—ЖД» разработана для автоматизированного сбора, хранения и выдачи информации о фактах хищения груза и багажа на железнодорожном транспорте, по которым возбуждены уголовные дела, а также о раскрытых хищениях грузов. Система может работать в составе автоматизированного рабочего места (АРМ) и в локальной вычислительной сети (ЛВС). Требования к техническому обеспечению АИСС такие же, как и для АИСС «Гастролеры».

АИСС «НАРКОБИЗНЕС» предназначена для сотрудников отдела по незаконному обороту наркотиков. Использование системы межзадачных связей позволяет выявлять лица, их связи с событиями, друг с другом, оружием и адресами, проходящими по разным видам учетов. АИСС применяется для проведения оперативной и учетно-аналитической работы в горрайорганах и МВД республик.

Широко используемой в ОВД системой является АИСС «Картотека-Регион», предназначенная для работы с пофамильными учетами осужденных, разыскиваемых и задержанных за бродяжничество лиц. Использование АИСС для получения справочной информации из оперативно-справочных картотек позволяет не только снизить затраты ручного труда на 40% и повысить эффективность решения оперативно-служебных задач, но и получать необходимые аналитико-статистические данные и решать производственно-хозяйственные задачи, в частности, по распределению осужденных лиц в соответствии с профессиональными навыками, мерой наказания, режимом содержания и потребностью производства. Входящий в состав АИСС программно-технический комплекс обеспечивает постановку на автоматизированный учет немашинно-ориентированных документов анкетного типа. В качестве СУБД АИСС «Картотека—Регион» взята «Adabas», а программирование прикладных задач может осуществляться на алгоритмическом языке PL/1. Среднее время поиска в БД по установочным данным на массиве 1,7 млн документов составляет 2—3 секунды.

АИСС «СПЕЦАППАРАТ» предназначена для работы со спецаппаратом и позволяет планировать оперативно-розыскные мероприятия на основе быстрого и качественного обеспечения их необходимой информацией. Можно, например, быстро найти круг лиц, проходящих по однотипным фактам из массива спецсообщений, по способам совершения преступлений, адресам и т.п.

➢ ***Автоматизированные рабочие места*** (АРМ) — индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста. В состав АРМ входят, как правило, ПК, принтер, графопостроитель, сканер и другие устройства, а также такие прикладные программы,

как, например, текстовые редакторы, электронные таблицы, средства деловой графики и т.п., т.е. офисные приложения. АРМ являются основной средой ИТ автоматизации профессиональной деятельности[1].

Понятие АРМ не является до конца устоявшимся. Так, иногда под АРМ понимают рабочее место, оборудованное всеми аппаратными средствами, необходимыми для выполнения определенных функций. Также можно встретить понятие АРМ как условного названия программного пакета, предназначенного для автоматизации рабочего процесса. По-видимому, *АРМ следует рассматривать как системы, структура которых, т.е. совокупность всех подсистем и элементов, определяется функциональным назначением.* Поскольку АРМ отличаются от АСОД, АИСС и АИПС развитыми функциональными возможностями, последние могут входить в состав АРМ в качестве подсистем.

Обычно различают т р и с п о с о б а построения АРМ в зависимости от структуры исполнения — *индивидуального* пользования, *группового* пользования и *сетевой*. Преимущества и недостатки каждого способа очевидны; следует лишь заметить, что сетевой способ построения кажется наиболее перспективным, поскольку позволяет получать информацию из удаленных банков данных, вплоть до федерального и международного уровня, а также обмениваться интересующей информацией между структурными подразделениями, не прибегая к другим средствам связи.

При работе с АРМ от специалиста не требуется детального знания системного и прикладного программного обеспечения. Гораздо важнее, чтобы он умел ориентироваться в предметной области изучаемого явления.

Примером АРМ оперативного назначения может служить АРМ «ГРОВД», которое создано с целью совершенствования информационного обеспечения оперативно-розыскной и управленческой деятельности городских и районных органов внутренних дел. АРМ спроектировано как совокупность взаимосвязанных подсистем, каждая из которых может функционировать автономно. Система позволяет выполнять статистическую обработку информации.

➢ ***Автоматизированные системы управления*** (АСУ) представляют собой комплекс программных и технических средств, предназначенных для автоматизации управления различными объектами. Основная функция АСУ — обеспечение руководства информацией. На практике АСУ реализуются в виде совокупности связанных между собой АРМ.

---

[1] Информатика и вычислительная техника в деятельности органов внутренних дел. Ч. 4. Автоматизация решения практических задач в органах внутренних дел: Учеб. пособ. / Под ред. *В.А. Минаева.* — М.: ГУК МВД РФ, 1996.

Примером современной АСУ ОВД является АСУ «Дежурная часть» (АСУ ДЧ), которая предназначена для автоматизации управления силами и средствами подразделений и служб ОВД в процессе оперативного реагирования на преступления и правонарушения. АСУ выполняет следующие основные функции:

- автоматизированный сбор и анализ информации об оперативной обстановке в городе, выдача решений и целеуказаний подразделениям ОВД, экипажам патрульных автомобилей, контроль за их исполнением в реальном масштабе времени;
- автоматизированный сбор, обработка, хранение, документирование и отображение на средствах индивидуального и коллективного пользования в ДЧ и подразделениях ОВД информации о расстановке сил и средств, о положении и числе патрульных автомобилей, фактах преступлений и правонарушений на фоне электронных карт;
- автоматизированный сбор по каналам связи из подразделений и служб ОВД информации о лицах, совершивших правонарушения, похищенных вещах, угнанных транспортных средствах, другой оперативно-розыскной и справочной информации, а также выдача информации по запросам подразделений ОВД из региональных и общегородских банков данных;
- автоматическая регистрация деятельности подразделений ОВД, подготовка аналитических и статистических отчетов, ретроспективный анализ процессов и событий.

Сравнительно новым и перспективным направлением использования компьютерных технологий в органах внутренних дел являются экспертные системы[1].

➢ ***Экспертные системы*** (ЭС) — это системы искусственного интеллекта, включающие базу знаний, набор правил и механизм вывода, позволяющие на основании правил и предоставляемых пользователем фактов распознать ситуацию, поставить диагноз, сформулировать решение или дать рекомендацию для выбора действия.

Автоматизированные экспертные системы представляют собой комплексы программного обеспечения ЭВМ, основанные на алгоритмах искусственного интеллекта, в особенности на методах решения проблем, и предполагающие использование информации, полученной от специалистов.

Экспертная система основана на знаниях. Знания возникают как результат переработки информации, накопленной в определенной предметной области. Образно говоря,

Знания = Факты + Убеждения + Правила.

---

[1] *Баранов А.К., Карпычев В.Ю., Минаев В.А.* Компьютерные экспертные технологии в органах внутренних дел: Учеб. пособ. — М.: Академия МВД РФ, 1992.

Следует различать знания и данные. Основное свойство знаний — их активность, первичность по отношению к процедурам, в отличие от данных, играющих по отношению к процедурам пассивную роль[1].

На практике экспертные системы обычно представляют собой программы для ЭВМ, моделирующие действия эксперта-человека при решении задач в узкой предметной области на основе накопленных знаний, составляющих базу знаний. Они предназначены для решения строго очерченного класса профессиональных задач, входящих в компетенцию данного эксперта.

Экспертные системы включают в себя три основных элемента: базу знаний, машину вывода и интерфейс пользователя.

База знаний содержит информацию о том, что известно об исследуемом предмете в настоящий момент. Она создается на основе исследований в данной области и опыта практических работников. На практике база знаний представляет собой набор правил, относящихся к конкретной предметной области.

База знаний содержит известные факты, выраженные в виде объектов, атрибутов и условий. Помимо описательных представлений, она включает выражения неопределенности, т.е. ограничения на достоверность факта. База знаний отличается от базы данных вследствие своего символьного, а не числового или буквенного содержания. Она представляет более высокий уровень абстракции и имеет дело с классами объектов, а не с самими объектами. Сбором знаний и формированием баз знаний занимается специалист, так называемый инженер-когнитолог.

Машина вывода предназначена для построения заключений. Ее действия аналогичны рассуждениям эксперта, который оценивает проблему и предлагает решения. В поиске решения на основе известных правил машина вывода обращается к базе знаний, пока не найдет вероятный путь к получению приемлемого результата.

Интерфейс пользователя способствует взаимодействию между системой и пользователем и диалогу между ними. С использованием естественного языка он создает видимость произвольной беседы, применяя повседневные выражения в правильно построенных предложениях.

Когда началась массовая разработка экспертных систем, естественно, возникла идея пустых экспертных систем, в которых зафиксированы средства представления знаний и способ работы решателя, а база знаний пуста. При переходе к конкретной проблемной области база заполняется инженером-когнитологом в процессе работы с экспертом.

---

[1] Экспертные системы. Принцип работы и примеры. — М.: Радио и связь, 1987. — С. 3.

Для облегчения процесса создания подобных систем были разработаны так называемые экспертные оболочки — Интерэксперт, Insiqht GURU. Закладывая имеющиеся данные в пустую оболочку экспертной системы, можно создать экспертные системы по различным направлениям деятельности. Основное применение в правоохранительной деятельности ЭС находят в настоящее время в следственной практике.

Экспертные системы используются и в других видах деятельности. ЭС «БЛОК» предназначена для сотрудников подразделений по борьбе с экономической преступностью и помогает установить возможные способы совершения краж при проведении строительных работ. Система позволяет:

- на этапе ввода исходных данных сформулировать проблему;
- определить возможные способы совершения краж;
- составить список признаков, соответствующих тому или иному способу совершения кражи, который используется для планирования мероприятий по раскрытию преступления.

Для выработки решения о способе совершения преступлений используются следующие группы признаков: экономические, технологические, товароведческие, бухгалтерские, оперативные, а также причастные лица и документы — носители информации.

Система отличается простотой ввода новых данных, что дает возможность быстро адаптировать ее в процессе эксплуатации. В ЭС имеются подсистема помощи и подсистема обучения пользователя.

ЭС «БЛОК» реализована на базе естественной языковой оболочки ДИЕС для экспертных и информационных систем. Для разработки системы привлекались наиболее опытные сотрудники подразделений по борьбе с экономической преступностью. В развитие ЭС «БЛОК» предусматривается возможность обращения к автоматизированным учетам органов внутренних дел.

С 1964 г. во ВНИИСЭ успешно действует ЭС «АВТОЭКС» (последний вариант 1988 г. «Мод-ЭксАРМ»). Система в режиме диалога решает восемь вопросов, связанных с наездом на пешехода. ЭС обеспечивает высокий уровень автоматизации экспертного исследования. В ней автоматизировано большинство операций: экспертный анализ исходных данных, выбор хода исследования, выполнение расчетов, составление заключения, формулирование вывода с последующей распечаткой.

С помощью системы можно получить ответы на вопросы, касающиеся определения численных значений различных параметров дорожно-транспортного происшествия: скорость автомобиля, его остановочный путь, удаление автомобиля от места наезда в конкретный момент времени и т.п. Решаются также и расчетно-логические вопросы, например наличие или отсутствие у водителя транспортного

средства технической возможности предотвратить наезд на пешехода. На производство одной экспертизы затрачивается в среднем пять минут: три минуты на ввод данных и две — на исследование и печать. Система также позволяет исследовать наезды транспортных средств на препятствие и столкновения транспортных средств.

➢ ***Системы поддержки принятия решений*** — новый класс АИС, представляющий собой симбиоз АИС.

Все большее применение в правоохранительной деятельности находят также *компьютерные системы обработки изображений*, ***автоматизированные информационно-распознающие системы*** (АИРС). Обычно они представляют собой достаточно сложные системы, требующие специального аппаратного обеспечения.

Контрольные вопросы и задания

1. Для какого класса прикладных задач ОВД целесообразно использовать СУБД?
2. Назовите основные функции СУБД.
3. Что такое *реляционная база данных*? Приведите примеры.
4. Назовите основные элементы базы данных.
5. Что такое *запись в базе данных*?
6. Данные какого типа могут размещаться в полях базы данных? В чем их отличие?
7. Какие операции можно выполнить с данными разных типов?
8. Как формируется запрос в базу данных?
9. Поясните смысл логического объединения по ИЛИ при формировании запроса в базу данных. Приведите примеры.
10. Поясните смысл логического объединения по И при формировании запроса в базу данных. Приведите примеры.
11. Для чего нужны словари в базе данных? Приведите примеры словарных реквизитов.
12. Как формируется отчет в базе данных?
13. Что называется ключевым полем (ключом) базы данных? Приведите пример простого и сложного ключа.
14. Что такое *индексное поле* и как его используют в базах данных?
15. Назовите действующие информационно-поисковые системы ОВД. Каким образом осуществляется обмен данными с этими системами?

Глава 12

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В СЛЕДСТВЕННОЙ, ОПЕРАТИВНО-РОЗЫСКНОЙ И ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

12.1. Информационные технологии следственной деятельности

Работа следователя — творческий процесс расследования преступного деяния, формы деятельности следователя по существу не изменились с прошлого века. В следственной практике по-прежнему преобладают рукописное оформление процессуальных документов и машинописные работы без применения современных технических средств. Характерным примером является задача по контролю за расследованием уголовных дел.

Компьютеризация работы следствия сдерживается не в последнюю очередь потому, что компьютер используется в основном как пишущая машинка. Однако даже применение текстовых процессоров снижает технические трудозатраты на составление основных процессуальных документов и обвинительных заключений примерно в 3—6 раз.

Для перестройки работы следователя следует использовать новые информационные технологии.

Цели информатизации следственной деятельности следующие:

- автоматизация процесса следственного производства — создания процессуальных и иных документов;
- автоматизация составления календарных планов и сетевых графиков расследования;
- накопление и анализ информации по уголовным делам, особенно объемным и многоэпизодным, для автоматизированного составления следственных документов, постановлений о привлечении в качестве обвиняемого, обвинительного заключения;
- получение справочной информации по уголовным делам из оперативно-справочных и оперативно-розыскных учетов;

- разработка автоматизированных методик расследования уголовных дел по различным видам преступлений;
- сбор данных о расследуемых уголовных делах, статистический анализ по установленным формам;
- автоматизация контроля за соблюдением процессуальных сроков, выполнением планов;
- создание и использование баз данных в составе АИПС для получения необходимой в ходе следствий информации;
- анализ информации о преступлениях лет.

Концептуальная модель автоматизированного рабочего места следователя (АРМС) — это многофункциональный аппаратно-программный комплекс, создаваемый на базе персонального компьютера и других средств, включенных в вычислительную сеть МВД (территориальную, локальную, региональную), обеспечивающий реализацию компьютерной технологии в деятельности следователя. В состав АРМС могут входить все виды АИС — начиная от АСОД и кончая ЭС.

Важнейшими компонентами программного обеспечения (ПО), входящими в состав АРМС, следует считать ПО расследования уголовного дела и ПО обработки сопутствующей информации, непосредственно связанной с уголовно-процессуальной деятельностью.

Программное обеспечение расследования уголовного дела решает следующие задачи:

- создание процессуальных документов (протоколы, постановления и т.д.);
- получение информации по запросам (справки, характеризующие материалы и т.д.);
- анализ процессуальных документов (формула обвинения, обвинительное заключение, постановление о прекращении уголовного дела и т.д.).

Отсюда следует и *перечень автоматизируемых функций*:

- заполнение процессуальных документов;
- поиск необходимых сведений в имеющихся материалах уголовного дела (фамилии, имена, клички, даты, суммы, эпизоды, протоколы, постановления и т.д.);
- оформление характеризующего материала;
- составление материалов профилактических мероприятий;
- систематизация материалов уголовного дела;
- составление формулы обвинения;
- составление обвинительного заключения и других необходимых документов;
- подготовка справочных материалов для направления в суд.

В следственно-процессуальной деятельности именно возможность быстрой текстовой компоновки и подготовки документов по стандартным бланкам имеет решающее значение.

Программное обеспечение обработки сопутствующей информации и дополнительного анализа материалов уголовного дела нацелено на р е ш е н и е следующих з а д а ч:

- получение сведений о лицах, проходящих по делу;
- поиск и анализ связей лиц, проходящих по делу;
- получение сведений о вещественных доказательствах (описание, денежная оценка, место хранения, как появились в деле и т.д.);
- поиск и анализ данных об эпизодах преступлений (место, время, участники, способ совершения, вещественные доказательства и т.д.).

Соответственно, а в т о м а т и з а ц и и п о д л е ж а т функции поиска, анализа и выдачи информации:

- о лицах, сведения о которых имеются в деле;
- о связях лиц, проходящих по данному делу;
- о вещественных доказательствах;
- об эпизодах преступлений.

Удельный вес перечисленных факторов сильно меняется в зависимости от количественных и качественных характеристик уголовных дел:

- количества эпизодов, участников следственного процесса;
- вида и состава преступлений.

В результате проведенного рассмотрения можно сформулировать *основные общие требования к программному обеспечению АРМС*:

1. Возможность эффективной работы с текстовой, документальной информацией.

2. Лексическая проверка подготавливаемых документов.

3. Печать выходных документов в машинописном виде.

4. Поддержка архива стандартных документов, форм отчетности.

5. Интерактивный поиск и компоновка текстовых фрагментов.

6. Автоматизированная подборка данных в табличном виде, простейшие статистические расчеты.

7. Поиск и анализ информации в структурированном, формализованном виде.

8. Возможность работы в диалоговом режиме, обеспечивающем поддержку принятия решений, анализ процессуальных документов на предмет наличия связей и т.д.

Очевидно, что указанному набору требований не может полностью удовлетворить ни одно из существующих программных средств, будь то текстовый редактор, электронная таблица, СУБД, любой из видов АИС. Так, например, текстовый редактор отвечает лишь требованию *1* («Лексикон»), а иногда и требованию *2* (WORD), но никак не более того. Программное средство «БИНАР-3» вполне отве-

чает требованиям *4*, *5* и *6*, а с подключением текстового редактора и требованию *1*, но не удовлетворяет требованиям *2* и *3*. Как следствие, АРМС должно являться согласованным набором офисных программных средств и различных видов АИС, и только в этом случае можно рассчитывать на комплексную автоматизацию следственной деятельности на основе современных информационных технологий.

Нет необходимости рассматривать возможности текстовых процессоров, электронных таблиц, СУБД, поскольку они достаточно полно освещены в литературе. Далее будут рассмотрены примеры различных видов АИС, применяемых в следственной деятельности[1].

➢ ***Диалоговый Конструктор (ДК) БИНАР-3*** предназначен для решения задач информационной *поддержки принятия решений, информационно-логических задач,* построения цепочек связей и идентификации объектов учета на совокупности взаимосвязанных объектов учета. Позволяет хранить и обрабатывать структурированные символьные, числовые данные, а также, с подключением текстового редактора, и текстовые фрагменты, имеет развитые средства настройки базы данных и получения отчетов по запросам.

База данных ДК БИНАР формируется в виде совокупности информационных массивов, называемых *объектами учета* (ОУ):

1. Информация по уголовному делу:
- учетная карточка на расследуемое уголовное дело, а также на нераскрытые преступления (объект учета — КАРТОЧКА);
- содержимое эпизодов уголовного дела (ОУ ЭПИЗОД);
- сведения о причастных лицах (ОУ ЛИЦО);
- сведения об организациях (ОУ ОРГАНИЗАЦИЯ).

2. Источники получения доказательств:
- показания лиц (обвиняемых, подозреваемых, свидетелей и др.) (ОУ ПОКАЗАНИЯ);
- описание вещественных доказательств (ОУ ВЕЩЕСТВЕННЫЕ ДОКАЗАТЕЛЬСТВА);
- сведения о документах, фигурирующих в деле, в том числе и процессуальных, и финансовых (ОУ ФИНАНСОВЫЕ ДОКУМЕНТЫ, ИНЫЕ ДОКУМЕНТЫ).

В процессе ввода информации пользователь устанавливает необходимые связи между объектами учета. Структура и характер связей задаются при настройке базы данных.

Состав и структура базы данных могут и расширяться до 32 различных объектов учета. Объем записей по каждому объекту учета практически составляет до 1 000 000 ед.

---

[1] См.: Каталог программных средств, рекомендуемых к внедрению в практику СЭУ МЮ СССР, 1989.

Встроенные средства формирования отчетов ДК БИНАР обеспечивают вывод на экран или принтер следующей информации:

- реквизитов отдельных экземпляров объектов учета, а также связанных с ними объектов;
- перечня как прямых, так и косвенных связей выбранного экземпляра объекта с другими объектами учета, причем глубину связей, т.е. число звеньев в цепочке, можно варьировать;
- статистических данных, например распределения числа причастных лиц, сумм хищений и т.д.;
- сведений по допрашиваемому лицу из базы данных в бланк допроса, сформированный пользователем;
- фрагментов обвинительного заключения, в пакетном режиме, по взаимосвязанным объектам, например содержимого эпизодов в сопровождении документов и показаний лиц.

К системе подключается календарь с возможностью записи плановых мероприятий по дням и часам.

ДК БИНАР устанавливается на ПК типа IBM PC с объемом оперативной памяти не менее 640 Кбайт. Для работы системы на базе ДК необходимо не менее 518 Кбайт свободной памяти. Базовой СУБД является CLIPPER (NANTUCKET, версия SUMMER-87). Ряд модулей написан на Ассемблере и Си.

Наиболее эффективна работа ДК БИНАР в локальной сети с распределенными базами данных, обеспечивающими работу следственной бригады, каждый сотрудник которой вводит информацию и необходимые связи в базу данных независимо. Средствами ДК БИНАР может быть получена обобщенная информация об объектах преступления и связях, выявленных в ходе анализа информации из базы данных.

При подготовке и оформлении текстовых документов возможности ДК БИНАР ограничены и требуют подключения дополнительного внешнего офисного ПО.

➢ Система анализа и учета уголовного дела (САУД-М), созданная на основе интегрированного пакета МАСТЕР, включает в себя:

- текстовый процессор;
- электронную таблицу;
- простую СУБД;
- пакет графического отображения данных;
- коммуникационный пакет.

САУД-М позволяет систематизировать материалы уголовного дела и производить их анализ. В основе работы системы находится семичленная формула расследования, включающая *классические элементы состава преступления*, подлежащие доказыванию:

- субъекты — лица, проходящие по делу;

- объекты преступного посягательства;
- иные материальные предметы;
- время совершения преступления;
- место совершения преступления;
- способ совершения преступления;
- мотив совершения преступления.

Порядок работы в САУД выглядит следующим образом. По каждому из эпизодов уголовного дела проходит ряд лиц: обвиняемые, свидетели и др., а также процессуальные доказательства — документы и выписки из них. *Объекты* — лица и доказательства — связаны с различными эпизодами. Задача пользователя системы состоит в подготовке выписок из процессуальных документов и установлении их связи с объектами. В результате, например, находясь в конкретном эпизоде, можно узнать, кто из обвиняемых и свидетелей проходит по нему, какие доказательства к нему относятся, какие мероприятия намечены. Характер связей не детализируется. Набор однотипных объектов характеризуется описателем, который представляется пользователю в виде меню.

В целом структура пакета представляется как система взаимосвязанных меню, обеспечивающих доступ к нужной информации. В САУД-М установлена жесткая система автоматической установки связей между объектами:

1. Эпизод — выписка — мероприятие — *7*.
2. Эпизод — выписка — *7*.
3. Эпизод — *7* — мероприятие.
4. Документ — выписка — эпизод.
5. Документ — эпизод — выписка.

Здесь «*7*» — экземпляр из семичленной формулы расследования (субъект, объект, место, время, мероприятие, способ, действие, мотив). Систему связей можно дополнить, пользуясь встроенным языком программирования интегрированного пакета МАСТЕР.

В САУД-М включен *аппарат индексации по системе ключевых слов*, определяемых с помощью тезауруса, для проведения выборки нужных документов. Имеется также *набор бланков процессуальных документов*, которые пользователь может загрузить и заполнить в текстовом редакторе, и *подсистема ведения календаря* и регистрации плановых мероприятий.

К основным недостаткам системы следует отнести отсутствие поддержки работы в локальной сети и невозможность работы с формализованной информацией.

➢ ***Гипертекстовая система ИНТЕЛТЕКСТ*** предназначена для создания текстовых документов — отчетов, обзоров, рекомендаций, обосновывающих и аналитических материалов. ИНТЕЛТЕКСТ обеспечивает ведение *базы текстовых документов*, установление семан-

тических связей между ее элементами и построение из них новых текстов. Основной информационной единицей является фрагмент текста. Имеются средства и для создания текстовых фрагментов, и для их компоновки из первичных документов.

На экране дисплея фрагмент представляется в текстовом окне.

Каждый фрагмент характеризуется набором необязательных атрибутов:

- *ключевых слов*, которые используются системой для автоматической или интерактивной простановки связей. В каждой информационной базе ведется собственный список ключевых слов;
- *рубрик* — типов фрагментов, например «допросы», «показания», «протоколы осмотра», «лица» и т.д.;
- *ссылок* — библиографических ссылок на источник, из которого взят текст документа либо комментарии.

Источники имеют свой каталог.

Для каждого фрагмента текста создается меню атрибутов, предназначенное для быстрого просмотра атрибутов фрагмента — рубрик, ключевых слов, ссылок, а также смежных фрагментов текстов. По любой комбинации из атрибутов возможен поиск фрагментов, результаты которого после анализа пользователь может поместить в папку. Папке можно присвоить имя и сохранить ее *в каталоге папок*. Папки можно просматривать и корректировать — добавлять текстовые фрагменты, удалять старые и т.п. Каждый фрагмент может иметь *смысловые связи* с другими фрагментами. Все связи — двунаправленные. Именно за счет связей фрагменты объединяются в *смысловую сеть* — гипертекст. В результате каждый фрагмент имеет смежные фрагменты, список которых всегда можно просмотреть.

Связи могут проставляться пользователем как в интерактивном режиме, так и в автоматическом режиме с помощью системы. В последнем случае производится подбор вариантов на связь с данным фрагментом по заданным ключевым словам, и результат представляется пользователю для анализа. Можно задать некоторое пороговое значение количества общих ключевых слов, при котором связи будут проставлены системой автоматически.

По смысловой сети связей пользователь может осуществлять навигацию как автоматически, так и вручную: он выбирает начальный фрагмент, смотрит список смежных с ним фрагментов, выделяет интересующий его текст, затем смотрит смежные с ним фрагменты и т.д. Созданная пользователем тематическая подборка преобразуется в единый текстовый документ, который может быть отредактирован с помощью встроенного редактора, выведен в файл, на принтер и т.д.

В интерфейсе системы ИНТЕЛТЕКСТ поддерживается концепция «поверхности рабочего стола». Текстовое окно может иметь от одного до трех полей — текст, аннотация, заголовок. Поддерживается свободное расположение и перемещение окон по экрану, изменение формата окна или его полей, изменений набора полей, прокрутка, масштабирование и т.д.

ИНТЕЛТЕКСТ поддерживает также альтернативные методы поиска информации в базе текстовых документов — по строке текста, по тексту заголовка, по подстроке аннотации и т.д.

➢ ***АРМС для расследования конкретных видов преступлений*** в настоящее время широко внедряются в следственную практику. Отделом информатизации и технического обеспечения Следственного комитета МВД РФ совместно с ВНИИ МВД разработаны следующие автоматизированные методики расследования преступлений:

1. Грабежи и разбойные нападения.

2. Кража из жилища.

3. Незаконный оборот наркотических средств.

Банк данных АРМС *по расследованию грабежей и разбойных нападений* основан на материалах эмпирических исследований, а также результатах изучения ведомственных нормативных актов и специальной литературы. В архивном виде базовый комплект АРМС размещается на одной дискете.

АРМ состоит из трех блоков:

1. Уголовно-правовая квалификация грабежей и разбойных нападений;

2. Методика расследования грабежей и разбойных нападений с целью завладения имуществом;

3. Справочный архив.

Первый блок АРМ предназначен для квалификации грабежей и разбойных нападений. В нем сосредоточены сведения о каждом элементе состава данных преступлений.

Во втором блоке в диалоговом режиме реализована автоматизированная методика следственных действий, позволяющая учесть конкретные ситуации, которые складываются из исходных данных о происшествии:

1) *подозреваемый*: задержан; известен, но не задержан; не известен и не задержан;
2) *свидетели и очевидцы*: есть; нет;
3) *потерпевший*: известен; неизвестен;
4) *вид и способ совершения преступления*:
   - *грабежи*: путем рывка; с применением психического насилия; с применением физического насилия;

- *разбой*: с применением огнестрельного оружия; с применением холодного оружия; с применением психического и физического насилия; с введением в организм сильнодействующих веществ.

В разделе рекомендаций по тактике следственных действий особое внимание уделяется проведению осмотра места происшествия, порядку осмотра и описания огнестрельного оружия, методике выявления разбоя, основным вопросам, подлежащим выяснению при допросах потерпевшего, свидетеля или очевидца, подозреваемого.

В отдельном разделе дается также перечень возможных экспертиз по данной категории преступлений и вопросы, решаемые при их производстве.

Третий блок АРМ содержит словарь наиболее часто встречающихся жаргонных слов.

АРМС *по обеспечению расследования краж из жилья* состоит из трех блоков:

1. Уголовно-правовая квалификация краж.

2. Методика расследования краж из жилищ граждан.

3. Типовые версии.

Первый блок АРМ предназначен для оказания помощи в квалификации краж и содержит сведения обо всех элементах состава данного вида преступлений.

Во втором блоке содержится диалоговая автоматизированная методика следственных действий. Учитываются следующие исходные данные о происшествии:

1) *подозреваемый*: задержан на месте преступления или недалеко от него; задержан вне места происшествия с вещами, похожими на похищенное; известен, но не задержан; не известен и не задержан; явился с повинной;
2) *потерпевший*: известен; неизвестен;
3) *свидетели и очевидцы*: есть; нет;
4) *способ совершения преступления*:
   - проникновение в помещение с преодолением препятствий;
   - проникновение в помещение под благовидным предлогом либо через незапертую дверь;
   - проникновение в помещение по приглашению потерпевшего, его родственников, знакомых.

Особое внимание уделяется проведению осмотра места происшествия, порядку предъявления для опознания, основным вопросам, подлежащим выяснению при допросах потерпевшего, свидетеля-очевидца, подозреваемого. В особом разделе дается также перечень возможных экспертиз по данной категории преступлений.

Третий блок АРМС содержит типовые версии о личности предполагаемого преступника.

АРМС *по расследованию преступлений, связанных с незаконным оборотом наркотических средств* состоит из следующих шести блоков:

1. Выдвижение версии.

2. Методика расследования.

3. Обстоятельства, подлежащие выяснению.

4. Словари жаргонных терминов и синонимов.

5. Пояснения.

6. Синонимы.

Первый блок АРМ предназначен для выдвижения версий в зависимости от набора исходных данных.

Второй блок представляет собой автоматизированную методику проведения следственных действий, учитывающую следующие исходные данные о происшествии:

1) *подозреваемый*: задержан; известен, но не задержан; не известен и не задержан;
2) *способ выявления преступления*: задержан с поличным; оперативные данные;
3) *свидетели и очевидцы*: есть; нет;
4) *цель незаконных действий*: сбыт; без сбыта.

Третий блок АРМ содержит список обстоятельств, подлежащих выяснению при расследовании преступлений.

Четвертый блок содержит словари названий наркотических средств с указанием их описания, жаргонных названий, возможных способов употребления и вопросов, решаемых криминалистическими подразделениями.

В пятом блоке АРМ находятся пояснения по классификации изъятых наркотических средств по объему, совместно с краткими сведениями о наиболее распространенных наркотических средствах.

Шестой блок включает формы документов, необходимых для проведения следственных действий по данному виду преступлений.

Работа пользователя с системой осуществляется в диалоговом интерактивном режиме, что существенно облегчает проведение анализа и не требует специальной подготовки.

➢ ***Специальная информационная система*** (SIS) представляет собой комплекс программ учета следственных действий, предназначенный для автоматизации следственных действий следственных подразделений, анализа деятельности следователей и подразделений, выявления тенденций и выработки управленческих решений. Система SIS содержит следующие связанные между собой общей логической схемой м о д у л и:

- *Модуль учета уголовных дел* — учет обвиняемых, подозреваемых, потерпевших, свидетелей и собственно уголовных дел. Является основой комплекса, поскольку позволяет вводить и корректировать данные.

- *Модуль работы с документами* — формирование следственных документов по уголовным делам, начиная от простых бланков и кончая генерацией запросов и обвинительных заключений.
- *Модуль контроля дел и сроков* — контроль уголовных дел по срокам как в подразделениях, так и закрепленных за конкретными следователями.
- *Архив уголовных дел* выполняет две функции:
  1) хранение информации о делах, направленных в суд;
  2) хранение исполненных документов с целью разгрузить рабочие базы системы для ускорения обработки информации.
- *Модуль дела отчетного периода* — статистический учет и формирование документов статистики по уголовным делам.
- *Сервисные функции* — необходимые для работы с системой справочники и ряд других подсистем.
- *Модуль настройки и утилит* — настройка на аппаратные средства, поддержка обслуживания баз данных системы и резервного копирования информации.

В системе SIS все учетные операции выполняются в течение определенного периода, называемого расчетным. В пределах этого периода все документы сохраняются в оперативном ведении. Продолжительность периода устанавливается пользователями системы. По истечении срока, когда информация в базе данных системы полностью введена и проверена, расчетный период закрывается. При этом данные о делах, направленных в суд, переносятся в архивную базу данных и становятся доступными только для печати и просмотра. Возврат к закрытым периодам в системе SIS программно не поддерживается.

Закрытие периода может выполняться в произвольный момент времени. Так, закрытие января может быть произведено в феврале, марте, декабре и т.д.

Выполнена система SIS в виде одного исполняемого модуля с общей базой данных. Система поставляется в локальном и сетевом вариантах. В локальном варианте система может применяться в следственных подразделениях с малой нагрузкой. При значительном объеме следственных действий рекомендуется применение сетевой версии программы с ведением учетных операций на 3—5 компьютерах.

В качестве сетевой ОС могут использоваться Novell — совместимые сети с выделенным или невыделенным сервером. Соответственно возможны и разные конфигурации системы. Для сетей Novell Netware 3.11 и выше база данных содержится на файл-сервере, а рабочие станции могут не иметь жесткого диска. Для одноранговых сетей Netware Lite и тому подобных временные файлы системы размещаются на рабочих станциях, которые должны иметь жесткие диски достаточного объема, а также высокую производительность.

➢ ***Экспертные системы, применяющиеся в следственной практике*** занимают особое место среди программного обеспечения. Существует несколько видов экспертных систем (ЭС) раскрытия и расследования преступлений.

1. *ЭС прогнозирования преступлений*: системы позволяют установить зависимость между личностными качествами преступников и выбором места совершения преступления.

2. *ЭС выявления скрытых преступлений*, например выявления признаков скрытых хищений на производстве. Анализ показателей деятельности предприятия позволяет сделать вывод о предполагаемом хищении, который потом проверяется оперативным путем или с помощью ревизии.

3. *ЭС поиска и установления личности преступника*, например ЭС «ПОИСК». Система после анализа первичной информации, полученной на месте происшествия, выдает типовые версии о личности подозреваемого, сужает круг подозреваемых лиц и по мере поступления новых данных уточняет типологические свойства личности неизвестного преступника.

Приведем в качестве примера *ЭС для расследования убийств.* Основа системы — база знаний, состоит из трех модулей:

- базы знаний о преступлении как системы уголовно-релевантного события;
- базы знаний о криминалистической характеристике убийств;
- базы знаний о системе способов собирания, фиксирования и использования информации об элементах преступления, их уголовно-процессуальной регламентации.

Для взаимодействия этих модулей используются программы ввода информации о текущей следственной ситуации и выдвижения следственных версий и рекомендаций по их проверке. При этом фиксируются:

- данные об элементах расследуемого события (преступник, потерпевший, способ совершения и сокрытия преступления, орудие убийства, мотив, место и время убийства);
- сведения об источниках доказательственной информации об элементах преступления;
- способы и средства собирания, фиксирования и использования этой информации;
- уголовно-процессуальная регламентация расследования убийств.

В начале своей работы экспертная система в диалоге со следователем получает информацию о расследуемом событии. На мониторе появляется строка: «Выберите направление расследования: если обнаружен труп — введите *1*, если части расчлененного трупа — *2*». И далее в подобном диалоговом режиме следователь работает с системой. Версий может быть несколько, каждая со своим фактором уверенно-

сти, который подсчитывается специалистами из субъективных оценок и статистики.

К настоящему времени разработаны и используются программы для расследования убийств с расчленением трупа, преступлений на сексуальной почве («Маньяк»), расследования грабежей и разбоев («Грабитель») и многие другие.

12.2. Информационные технологии оперативно-розыскной деятельности

Информационная технология оперативно-розыскной деятельности во многом схожа с информационной технологией деятельности следователя. Оперативные работники как орган дознания выполняют многие следственные действия, пользуются законодательными актами и методиками расследования преступлений. АРМ оперативного работника может отличаться от АРМ следователя наличием специальных программ ведения оперативной работы, исключающих доступ посторонних лиц к конфиденциальной информации, а также автоматизированных банков данных оперативно-розыскной информации.

Очевидно, что центральную роль в раскрытии и расследовании преступлений играют централизованные и региональные *оперативно-справочные, оперативно-розыскные* и *криминалистические учеты.*

Наиболее сложными и дорогостоящими являются ***дактилоскопические автоматизированные учеты*** (***АДИС***). С 1994 г. успешно эксплуатируются две АДИС: «Сонда-Фрес» и «Папилон». Поскольку данные системы используются преимущественно сотрудниками экспертно-криминалистических подразделений, они далее будут рассмотрены более подробно.

В целях полного и быстрого раскрытия преступлений необходимо повысить эффективность использования сведений, поступающих от свидетелей и потерпевших — очевидцев совершения преступлений. Существенную помощь в оперативно-розыскной деятельности должны сыграть интенсивно внедряемые ***автоматизированные системы учета лиц по элементам внешности*** (***АИРС***), которые можно отнести к *двум основным типам*:

- созданные по типу «субъективный портрет»;
- использующие видео- и фотоизображения.

Субъективный портрет используется при отождествлении личности по признакам внешности. Использование субъективных портретов существенно расширяет возможности установления личности преступников, скрывшихся с мест происшествия, и иных лиц, имеющих отношение к расследуемому событию.

Внедрение в практику ОВД компьютерных систем составления субъективных портретов позволяет получить следующие п р е -

и м у щ е с т в а по сравнению с традиционными системами (рисованный портрет, идентификационные комплекты и т.д.):

1. Возможность использования пространственных перемещений и плоскостных трансформаций элементов внешнего облика, сопутствующих признаков (одежда, украшения), изменения размеров и взаиморасположения отдельных элементов лица, цвета и тона изображений, а также дорисовки, ретуширования и т.д.

2. Сокращение временных затрат на изготовление субъективного портрета за счет устранения трудоемких операций по подбору элементов внешности, монтажу портрета и его доработке, фотографической фиксации и тиражирования субъективного портрета.

3. Возможность распечатки и тиражирования портрета совместно с изготовлением текста розыскной ориентировки.

4. Сохранение субъективного портрета в электронной форме, пригодной для последующей проверки по картотеке субъективных портретов.

Обычно при изготовлении компьютерных субъективных портретов применяются одномасштабные типизированные рисунки элементов внешности человека, а создание портретной композиции осуществляется по традиционной методике изготовления субъективных портретов, отработанной на базе систем «ИКР-2» и «Портрет».

Первой компьютерной системой построения композиционных портретов стала система «ЭЛЛИ» (элементы лица). В дальнейшем появились «ФОТОРОБОТ» (МГТУ им. Н.Э. Баумана, Москва) и «КРИС» (УВД Юго-Западного административного округа Москвы и УВД Рязанской области). Для указанных компьютерных систем характерна по существу *полная реализация традиционной методики* изготовления портрета, заключающейся в следующем:

- возможность произвольной последовательности монтажа составляющих элементов субъективного портрета;
- наличие режима просмотра элементов внешности;
- наличие средств ретуширования композиционных портретов;
- возможность создания временного массива элементов, который заполняется из основного массива элементами, наиболее подходящими, в соответствии с показаниями очевидцев, для последующего монтажа окончательного варианта.

➢ ***Система «ФОТОРОБОТ»*** предназначена для создания субъективных портретов лиц, подозреваемых в совершении преступлений. Процесс создания композиционного портрета становится оперативным, повышается эффективность решения задач, связанных с розыском или опознанием лиц, представляющих оперативный интерес. Автоматически решается задача накопления субъективных портретов в базе данных системы, получения печатных копий необходимых изображений в требуемой форме и передача их по линиям связи.

Компоновка портрета осуществляется из отдельных элементов: прически, глаза, носы — мужские и женские, изображения усов, очков, головных уборов, частей одежды, кулонов, серег и др. Дополнительно имеются группы с элементами профильного портрета. Количество элементов в некоторых группах достигает 250 и выше. Портреты можно дополнять «вручную» различными элементами: родимыми пятнами, шрамами и др. Имеется возможность менять взаиморасположение элементов портрета, осуществлять их сдвиг, поворот, сжатие и растяжение. Возможен также автоматический перебор элементов выбранной группы. В будущем предусматривается ввод и накопление в системе фотографий с возможностью вычленения из них отдельных элементов (например, носы, брови) и пополнение ими соответствующих наборов.

В США широко применяется система «Айденти-кит», включающая в себя до 525 штриховых рисунков элементов внешности.

Опыт эксплуатации систем показал, что необходимым является расширение массивов элементов внешности, которое может осуществляться разными способами.

Один из способов заключается в проведении деформирующих операций с изображениями элементов внешности в процессе монтажа композиционного портрета:

- пропорциональное и независимое по осям масштабирование элементов;
- расширение (сжатие) элементов относительно осей симметрии;
- вращение элементов;
- зеркальное отображение элементов;

Другой способ заключается во включении в массив новых элементов. Для этого могут использоваться, например, фрагменты изображений реальных лиц. Практика свидетельствует о том, что для успешной работы по изготовлению субъективных портретов необходимо иметь компьютерную систему, которая объединяла бы возможности формирования полутоновых и рисованных изображений. Данное положение обусловлено особенностями восприятия изображений различными людьми с разным типом мышления[1].

В 1995 г. в МГТУ им. Н.Э. Баумана была разработана компьютерная система «Фоторобот-С» (ФРС-2). Результаты тестирования показали, что система «ФРС-2» успешно объединяет в себе различные массивы элементов: базу полутоновых изображений и базу рисованных элементов внешности.

Компьютерная система «ФРС-2» позволяет составлять субъективные портреты, максимально приближенные по своим изобрази-

---

[1] *Кочетыгов А.В.* Влияние графической доработки компьютерного субъективного портрета на восприятие очевидца // Экспертная практика, 1995, № 39.

тельным свойствам к фотографии. *Графический редактор системы «ФРС-2»* включает в себя:

- рисование «пером»;
- рисование «кистью»;
- различные «распылители»;
- выполнение операций микширования;
- выполнение операций осветления (затемнения);
- выполнение операций контрастирования (деконтрастирования);
- выполнение операций фокусировки (расфокусировки);
- выполнение операций бленд-эффекта;
- выполнение операций удаления (восстановления).

База данных системы «ФРС-2» позволяет вести картотеку субъективных портретов, которая сопровождается информацией, необходимой для поиска по различным описаниям внешности человека[1].

Опыт использования субъективных портретов показывает, что в первые десять дней после событий, послуживших поводом для составления портрета, наиболее успешная работа по актуализации мысленного образа возможна с компьютерными системами, имеющими полутоновые базы данных. В дальнейшем, по прошествии 10-дневного срока, портрет может изготавливаться с использованием как полутоновых изображений, так и рисованных изображений.

Потребность оперативных и следственных подразделений органов внутренних дел в составлении компьютерных субъективных портретов постоянно возрастает. Оперативные и следственные подразделения ставят задачу разработки систем, которые позволили бы изготавливать субъективные изображения фигуры и элементов одежды разыскиваемого лица. Это обусловлено тем обстоятельством, что во многих случаях очевидцы не видели лица преступника, но хорошо запомнили его фигуру и одежду.

Среди систем второго типа в настоящее время в России эксплуатируются две системы — «ПОРТРЕТ» и «FACE MANAGER». Данные системы могут производить выборку по типу «словесный портрет», но в то же время позволяют хранить и обрабатывать видеоинформацию.

➢ ***АИРС «ПОРТРЕТ»*** разработана для решения оперативно-розыскных задач, требующих накопления, хранения и быстрого поиска карточек с фотографиями лиц, склонных к совершению преступления.

Система «ПОРТРЕТ» позволяет создать базу данных, содержащую графическую информацию. Это могут быть фотографии, снятые сканером, сделанные непосредственно цифровой фотокамерой, или изображения, полученные с видеокамеры или видеомагнитофона.

---

[1] *Зудин С.И.* О тестировании компьютерных программ для составления субъективных портретов // Экспертная практика, 1996, № 40.

Поиск осуществляется по любым параметрам, как то: фамилия, дата рождения, место жительства, состав и способ совершения преступления, а также по словесному описанию примерного вида: форма лица, глаз, носа, бровей и т.п. без жестких требований к данным.

➢ ***Система «FACE MANAGER»*** позволяет хранить и обрабатывать текстовую и графическую информацию и может использоваться для поиска подозреваемых лиц по совокупности признаков, для опознания или как картотека с фотоснимками. Информация, накопленная в базе данных системы, может пересылаться по телефонным каналам с возможностью занесения ее в аналогичные базы других районов и городов.

«FACE MANAGER» позволяет создать и заполнить базу данных, просматривать в удобной форме информацию, осуществлять поиск необходимых записей и их распечатку. Основным преимуществом данной системы перед обычными системами управления базами данных является возможность хранения информации в виде изображений. Информация подвергается эффективному сжатию, что существенно экономит дисковую память компьютера. Система также обеспечивает надежную защиту от несанкционированного доступа.

Система «FACE MANAGER» предназначена, главным образом, для хранения видеоизображений лиц, но может быть использована и для хранения другой информации (например, следов подошв обуви).

Система «FACE MANAGER» имеет следующие р е ж и м ы:

- *видеокаталог* — в этом режиме на экране монитора появляется одновременно двадцать уменьшенных изображений;
- *детальный просмотр* — используются увеличенные цветные изображения, предусмотрены просмотр по одному изображению и по паре изображений);
- *поиск карточек* — возможность поиска записей по определенной совокупности признаков;
- *фильтр* — в текстовом каталоге содержатся только записи из текущей выборки);
- *распечатка текстового каталога;*
- *экспорт данных;*
- *импорт данных;*
- *режим редактирования изображения.*

Преимущества системы «FACE MANAGER» заключаются в том, что в каждую карточку можно «врезать» три изображения. Система позволяет делать в записях карточек свободные комментарии. Данная АИРС интересна также тем, что позволяет производить распечатывание отдельных кадров с видеокассет, отснятых в процессе проведения следственных и оперативно-розыскных действий. Это способствует более качественному документированию. На базе дан-

ной системы разработан также комплекс по созданию субъективных портретов.

Решающую роль в продвижении информационных технологий в правоохранительной деятельности и, прежде всего, в обеспечении оперативно-розыскной деятельности должно сыграть создание единой информационно-вычислительной сети ОВД.

Создание ***интегрированной вычислительной сети*** (ИВС) органов внутренних дел позволит обеспечить информационное взаимодействие различных подразделений оперативных служб, дежурных частей УВД, дежурных частей служб следствия и дознания, паспортной службы, ГИБДД, разрешительной службы, городских и линейных органов внутренних дел с центральным банком данных в масштабах города, области, региона, страны, содержащим информацию всех служб абонентов сети. Абонентами сети могут выступать также службы прокуратуры, суда, ФСК, налоговые и таможенные службы. Все абоненты сети являются одновременно и потребителями, и поставщиками информации в интегрированные банки данных.

Главная цель внедрения ИВС — оперативность получения информации. Там, где сейчас требуются часы, а нередко и дни, с созданием ИВС потребуются минуты.

Концентрация в рамках ИВС сигнальной, ориентирующей, розыскной и доказательственной информации, обеспечение логической взаимосвязи ее компонентов позволит, кроме того, повысить информированность каждого оперативного работника, создаст условия для более эффективного использования накопленной информации в процессе расследования, раскрытия и профилактики преступлений.

Создание интегрированной вычислительной сети позволит информационной службе перейти от традиционных ныне видов оперативно-справочной работы по поддержке раскрытия и расследования преступлений к ориентированию правоохранительных органов на розыск преступников; к проведению сравнительной предварительной идентификации способов совершения преступлений, следов и вещественных доказательств, описаний лиц и примет похищенного имущества; к выявлению в инициативном порядке криминогенных структур (связей, групп, соотношений событий и т.д.), к оказанию действенной помощи в анализе и прогнозировании оперативной обстановки.

12.3. Информационные технологии экспертной деятельности

Возрастающий поток информации об объектах судебной экспертизы, необходимость ее оперативной обработки, решение все более

сложных экспертных задач при постоянном росте количества экспертиз приводит к необходимости внедрения в экспертную практику компьютерных технологий[1].

Внедрение компьютеров в экспертных подразделениях дает следующие преимущества:

- сокращаются затраты рабочего времени на производство одной экспертизы;
- автоматизируются рутинные операции в работе;
- уменьшается вероятность экспертной ошибки и обеспечивается методическое единообразие в решении экспертных задач и их процессуальном оформлении.

Работа в рассматриваемой области идет по пути создания АРМ экспертов различных специальностей. Можно выделить следующие направления:

- создание автоматизированных банков данных экспертной информации, т.е. различных типов АИС;
- создание автоматизированных программных комплексов решения экспертных задач.

Поскольку в процессе производства экспертиз и исследований приходится оперировать огромным количеством разнообразной как чисто криминалистической, так и справочно-вспомогательной информации, в экспертных учреждениях создаются ***экспертные АИС и банки данных*** (АБД). Сейчас практически нет ни одного вида экспертиз, в котором не использовались бы АИС или банки данных. Можно выделить несколько видов АИС и АБД, создаваемых для использования в экспертной деятельности.

➢ ***Пулегильзотеки*** позволяют идентифицировать оружие по стреляным пулям и гильзам. Так, например, АИС «Модель оружия» позволяет установить модель оружия по следам, оставленным механизмом оружия на гильзе, а система «Патрон» определяет вид патрона по его характеристикам.

➢ ***Дактилоследотеки*** (АДИС) применяются при ведении дактилоскопических автоматизированных учетов в целях осуществления оперативной проверки следов пальцев рук, изымаемых с места происшествия, по массивам дактилокарт ранее осужденных или определенного круга подозреваемых лиц.

Входными данными для автоматизированной дактилоскопической информационной системы (АДИС) являются дактилокарты с отпечатками пальцев рук и карточки с изображениями следов с мест нераскрытых преступлений на фотоснимках, прозрачных пленках

---

[1] Использование математических методов и ЭВМ в экспертной практике: Сборник научных трудов. — М., 1989.

или непосредственно на объектах. Решение вопроса о принадлежности отпечатков или следов конкретному лицу производится экспертом-криминалистом на основе совокупности общих и частных признаков папиллярных узоров.

С конца 1980-х гг. начались попытки внедрения в деятельность ОВД автоматизированных информационных дактилоскопических систем на основе персональных компьютеров, с помощью которых можно автоматически кодировать отпечатки и следы пальцев рук, сохранять их изображение в памяти и производить сравнительный анализ.

Следы и отпечатки пальцев рук очень трудны для машинной обработки: в них нет устойчивости признаков ни по наименованию, ни по размерам, ни по топографическим и геометрическим параметрам. Первые отечественные АДИС оказались малопригодными на практике. Зарубежные же дактилоскопические системы оказались слишком дороги, при этом большинство из них (например, «Дермалог») очень требовательны к качеству следов и отпечатков пальцев рук.

В 1992–1993 гг. по инициативе ЭКЦ МВД России было впервые проведено конкурсное тестирование более десятка АДИС. Тестирование в полном объеме прошли четыре отечественные системы, которые Приказом МВД России от 3 августа 1993 г. № 365 были представлены к проведению опытных испытаний в ряде УВД. В мае 1994 г. на научно-методическом совете в ЭКЦ МВД России были особо выделены две системы:

- «*Папилон*», разработчик — ТОО «Системы Папилон» (г. Миасс Челябинской области);
- «*Сонда-Фрес*», разработчик — СП «Совиндейта» (г. Миасс Челябинской области).

В настоящее время проходит активное внедрение этих систем в деятельность ОВД Российской Федерации. Автоматизированная дактилоскопическая информационная система (АДИС) «Папилон» предназначена для ввода отпечатков с дактилоскопических карт и следов пальцев, изъятых с мест нераскрытых преступлений, автоматического их индексирования, осуществления поиска по базам данных (до 0,5 млн дактилоскопических карт) и следов пальцев рук (до 50 тыс.) в органах внутренних дел любого уровня (от МВД, УВД до горрайлинорганов). Система спроектирована как совокупность автоматизированных рабочих мест «Дактилоследотека»[1].

С 1995 г. осуществляется внедрение АДИС «Папилон», объединенной с автоматизированной пофамильной картотекой, в ВЦ ин-

[1] Системы «Папилон»: Руководство пользователя. — Миасс, 1998.

формационных центров, с подсоединением к ней с помощью ИВС выносных АРМ «Дактилоследотека» в дактилоскопической картотеке ИЦ, в экспертно-криминалистических подразделениях, дежурных частях. Такая организация системы позволит всем заинтересованным службам пользоваться базами данных как дактилоскопической, так и пофамильной картотек.

Достоинство системы состоит в том, что она автоматически определяет тип папиллярного узора и индексирует отпечатки, правильно распознает их общую структуру и до 95% частных признаков. На качество обработки следов не влияет масштаб, повороты и другие виды искажений. В 40 подразделениях органов внутренних дел, где эксплуатируется эта система, с ее помощью раскрыто более 250 тяжких преступлений.

В некоторых регионах России успешно внедряется автоматизированная дактилоскопическая система «Сонда-Фрес», обладающая близкими к АДИС «Папилон» характеристиками при эксплуатации на базах данных до 10–15 тысяч дактилокарт. Однако обмен информацией между двумя системами возможен только на уровне исходных изображений, с последующим повторным индексированием в другой АДИС и, соответственно, дублированием информации.

Полученный к настоящему времени опыт внедрения АДИС позволил выявить основные проблемы, которые приходится решать, и возникающие при этом сложности.

Одна из основных проблем, возникающих в ходе внедрения АДИС — недостаток дактилокарт для введения в систему. На местах не ведется дактилоскопический учет на тех лиц, которые формально подлежат постановке на учет. Не практикуется негласное дактилоскопирование криминогенных категорий при отсутствии к тому формальных оснований. Поэтому основная часть базы данных в АДИС — дактилокарты, поступившие из следственных изоляторов, на лиц, находящихся под следствием или ранее судимых.

Другая проблема — низкое качество дактилоскопирования. Отпечатки пальцев рук на дактилокартах «забиты» типографской краской или, наоборот, не пропечатаны, накладываются один на другой, выполнены со сдвигом в процессе прокатки пальца, бумага, на которой производится дактилоскопирование, рыхлая, волокнистая и т.п. В результате только 10–30% дактилокарт удовлетворяют требованиям, предъявляемым к качеству дактилоскопирования подучетных лиц для занесения в АДИС.

Не проводится проверка по дактилоучетам на предмет установления причастности к ранее совершенным преступлениям лиц, привлекаемых за совершение корыстных преступлений: лиц, находившихся в розыске; трупов, в том числе некриминального характера;

лиц, проходящих по делам оперативного учета и административного надзора при их заведении и прекращении и т.д.

Дополнительные сложности возникают из-за неопределенности в решении вопроса о месте дактилоучетов. Дактилоскопический учет преступного элемента в низовых подразделениях всегда был привилегией оперативных аппаратов, поскольку только они могут определить контингент лиц, подлежащих постановке на данный вид оперативного учета, обеспечить своевременную постановку и снятие с него. Поэтому многие проблемы могут быть сняты принятием единого нормативного документа, регламентирующего порядок формирования и использования дактилоскопических учетов в оперативно-розыскной, следственной и архивной работе.

Необходимость же автоматизации процесса поиска следов с мест преступлений по значительным массивам дактилокарт совершенно очевидна. Без использования АДИС возможности дактилоскопии в работе по раскрытию и расследованию преступлений сводятся в основном лишь к подтверждению, т.е. установлению идентичности изъятых с места преступления следов с отпечатками рук конкретного человека или выборки его из ограниченного количества подозреваемых лиц. В результате многотысячные массивы дактилокарт подучетных лиц и следов рук с мест преступлений остаются лежать «мертвым» грузом. Внедрение АДИС позволит раскрывать именно те преступления, перспективы раскрытия которых оперативным путем были минимальными.

Оптимальная схема организации единой АДИС регионального масштаба — двухуровневая. Первый уровень составляют центральный сервер и связанные с ним рабочие станции, часть из которых установлена в ГОРОВД. Базы данных (БД) дактилокарт и БД следов с мест преступлений хранятся и обрабатываются на центральной станции, программно-технические возможности которой позволяют работать с большими объемами информации. Пополнение БД и запросы на проведение поисков по всей региональной БД или по какой-либо ее части могут производиться непосредственно из ГОРОВД. В связи с большим объемом графической информации передача по модемным линиям связи может оказаться затруднительной, поэтому информацию с мест целесообразно передавать на центральный сервер записанной на стримерные кассеты или магнитные диски. Результаты поиска можно передавать в ГОРОВД по модемной связи для окончательного этапа сравнивания. В крупных географически удаленных от областного, краевого центра городских отделах внутренних дел могут быть оборудованы кустовые АДИС с обеспечением возможности работы с единой краевой (областной) АДИС по обмену базами данных и по проведению запросных поисков.

Двухуровневая организация автоматизированной дактилоскопической системы с единой общекраевой (общеобластной) базой данных позволяет получить следующие п р е и м у щ е с т в а перед автономными АДИС:

- обеспечивается большая эффективность использования дактилоскопических учетов в раскрытии преступлений, особенно межрегиональных;
- уменьшается объем технических средств, необходимых для обеспечения работы АДИС. В ГОРОВД сосредотачивается минимальный объем технических средств: сканер для считывания отпечатков на дактилокартах и следов рук с мест преступлений; «живой сканер» для бескраскового дактилоскопирования подучетных лиц; ПК для обеспечения обмена информацией с центральной АДИС и просмотра рекомендательных списков; модем, стример и часть других периферийных устройств (соответственно снижается стоимость программно-технических комплексов АДИС);
- упрощается задача по их техническому обслуживанию и обеспечению нормального, бесперебойного функционирования АДИС;
- появляется возможность полного и равномерного использования средств вычислительной техники, вплоть до организации работы круглосуточно и без выходных, например работы центральной станции в дежурном режиме, что позволит оперативно отрабатывать любые срочные запросы по всей региональной базе данных.

➢ ***Следотеки*** созданы для трасологических исследований подошв обуви. Исследование следов подошв обуви — один из наиболее часто встречающихся видов трасологических экспертиз. В настоящее время состояние проблемы производства трасологических экспертиз по следам подошв обуви, особенно по источникам производственного происхождения, и вопросы установления вида обуви не отвечают современным требованиям следствия и судопроизводства.

Примером АДИС для трасологических экспертиз может служить система «Обувь», созданная в НИИСЭ, и система «Сапог» МЮИ МВД РФ. Данные системы опираются на кодировку элементов подошв обуви и рельефного рисунка. Вводится также изображение данной обуви и описание ее верха.

В 1989 г. в НИИСЭ была разработана АИС для определения марки машинописного шрифта, которая содержит сведения о более чем 70 марках шрифтов отечественного и зарубежного производства. Был также создан банк данных о 98 марках пишущих машин.

В настоящее время ведутся работы по созданию ряда других автоматизированных банков данных и АИС экспертно-криминалистического профиля: *взрывчатых веществ* отечественного производства (АБД «ВВ»), *текстильных волокон* (АИС «Волокно» и АРПК «Контакт»), *рентгенограмм* (АИС «Фазан»), характеристик *автоэмалей*

(АИС «Марка»), *красителей шариковых авторучек* (АИС «Спектр»), *стекол фарных рассеивателей* автомашин (АИС «Стекло»), характеристик *металлов и сплавов*, *бумаги* (АИС «Бумага» по определению предприятий — изготовителей бумаги), *библиотек ИК-спектров* (АИС «БИРСИ», Германия) и т.д.

Вторым направлением использования современных ИТ в экспертной деятельности является разработка ***автоматизированных программных комплексов решения экспертных задач*** (АПК). Примером действующего комплекса является АПК «Контакт», осуществляющий автоматизированную оценку достоверности факта контактного взаимодействия объектов волокнистой природы. При определении частоты встречаемости только одного волокна с заданными свойствами приходится осуществлять поиск в базе данных, содержащей сведения о более чем 12 000 волокон.

АПК «Контакт» действует в НИИСЭ с 1986 г. и позволяет использовать его и при проведении экспертиз в регионах. Эксперт-волокновед передает имеющуюся у него информацию о предметах одежды и находящихся на них волокнах в вычислительный центр НИИСЭ, где специалист вводит ее в систему, получает результаты в виде вероятностно-статистических оценок контактного взаимодействия и передает их в установленной форме в подразделение, где проводится экспертиза.

В 1987 г. во ВНИИСЭ был создан АПК «Внешняя баллистика». Данная система позволяет автоматизировать исследования, сопряженные с определением возможности поражения пулей или дробью, выстреленной из огнестрельного оружия.

С 1986 г. во ВНИИСЭ действует АПК «ГАЗХРОМ», используемый в процессе производства криминалистической экспертизы материалов, веществ и изделий. Программа позволяет считывать в автоматическом режиме хроматограммы, осуществлять расчеты и другие операции. Данный комплекс включает в себя в качестве подсистемы АИС «Газовая хроматография».

Созданы также АПК для решения задач судебно-почерковедческой экспертизы: исполнителя кратких почерковых объектов (АПК «ДИА»), идентификации исполнителя текста, выполненного измененным почерком (АПК «ИРИС»), установления факта намеренного искажения почерка (АПК «РОЗА»), дифференциации подлинных кратких и простых подписей, выполненных в обычных условиях, и не подлинных, выполненных с подражанием после предварительной тренировки (АПК «МАК»).

Большое значение имеет ***автоматизация физико-химических исследований***. ПК применяется для контроля и управления работой спектрометров, накопления сигналов, хранения и анализа полученных спектров. В качестве примера можно привести использование средств вычислительной техники в спектрофотометрии в ультрафиолетовом, видимом и инфракрасном диапазонах, спектроскопии электронного

парамагнитного резонанса (ЭПР) и методов масс-спектрометрии. Созданы и действуют АПК исследования спектров веществ. Так, в НИИСЭ действует АПК исследования ИК-спектров, основанный на комплексе программ «БИРСИ» (Германия) и использующий различные библиотеки ИК-спектров, в том числе библиотеки ИК-спектров фармпрепаратов криминалистической лаборатории штата Джорджия (США).

Трудно переоценить эффективность использования компьютерных технологий при ***автоматизации судебно-фоноскопических экспертиз***. Уровень использования современных информационных технологий в экспертной деятельности демонстрирует АПК криминалистического исследования фонограмм «Signal Viewer»[1]. Система позволяет решить следующие основные задачи: идентификация личности по речевому сигналу; исследование признаков монтажа магнитной фонограммы; диагностика и идентификация объектов, воспроизводящих звук; установление содержания речи, неразборчивой из-за импульсных помех и шумов; выявление оригинала и копии фонограммы и др.

Эксперт-фоноскопист получает возможность криминалистического исследования фонограммы по форме, близкой к техническому исследованию документов. Исследуя фонограмму, эксперт постоянно видит на экране три основные формы исследуемого фонообъекта: *общий обзор* в виде динамики уровня мощности; *микросегмент* в виде осциллограммы в текущей точке анализа фонообъекта; *семь основных форм анализа фонообъекта* (осциллограмму, амплитудно-фазовый спектр, функции гармоничности и индикатора основного тона голоса, сонограмму, гармонограмму и интонограмму).

Анализ динамических амплитудных образов (сонограмм) позволяет обнаруживать гармонические компоненты сигналов, что делает систему незаменимой при исследовании признаков монтажа фонограмм и дает значительно больше информации для идентификации личности по речевому сигналу.

В перспективе предусматривается разработка специализированных систем автоматического анализа и построения признаков исследуемых фонообъектов, требуемых для криминалистики.

Контрольные вопросы и задания

1. Дайте определение автоматизированного рабочего места (АРМ).
2. Приведите примеры АРМ сотрудников ОВД.
3. Назовите известные вам компьютерные программы для автоматизации деятельности сотрудников ОВД различных подразделений.
4. Укажите необходимый состав программно-аппаратных средств для АРМ сотрудника конкретной специализации.

---

[1] *Женило В.Р., Минаев В.А.* Компьютерные технологии в криминалистических фоноскопических исследованиях и экспертизах: Учеб. пособ. — М.: Академия МВД РФ, 1994.

Глава 13

СПРАВОЧНЫЕ ПРАВОВЫЕ СИСТЕМЫ

Обеспечение работников правоохранительных органов 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 поставленную задачу. 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).

Вначале считалось, что СПС создают лишь дополнительное удобство 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:

1. 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.

2. Использование в СПС специальных поисковых программных средств, что позволяет осуществлять поиск в режиме реального времени по всей информационной базе.

3. Возможность работы СПС с использованием телекоммуникационных средств, т.е. с применением электронной почты или сети Internet. 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.

В настоящий момент в России работают более десяти фирм, разрабатывающих программное обеспечение СПС, ведущих компьютерные нормативно-правовые информационные базы и оказывающих услуги по информационному обеспечению с использованием современных компьютерных технологий.

Ряд СПС был создан в сотрудничестве с государственными учреждениями для обеспечения их нужд и с использованием государственных вложений. К ним относятся: СПС Научного центра правовой информации при Минюсте РФ «Эталон», СПС республиканских и региональных органов законодательной и исполнительной власти, например СПС Госсовета Республики Татарстан, СПС Центра компьютерных разработок при мэрии Санкт-Петербурга и т.п. Информационные базы таких систем достаточно объемны, часто содержат уникальные документы. Так, база СПС «Эталон» имеет размер 1 Гбайт и содержит документы узкоюридической направленности. Однако работа массового пользователя с такими системами затруднена ввиду отсутствия эффективных каналов поддержки обновления базы, сервисного обслуживания систем, а также из-за ограниченных возможностей программной оболочки, в частности, в аспекте внесения изменений и создания собственных тематических баз.

Поэтому широкое признание пользователей получили коммерческие справочные правовые системы, такие как «КонсультантПлюс» (АО «КонсультантПлюс»), «Гарант» (НПП «Гарант-сервис»), «Кодекс» (ГП «Центр компьютерных разработок», Санкт-Петербург), «Юсис» (Юридическое агентство «Intralex»). 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 гг. в России было установлено около 4000 СПС, то в 1995—1996 гг. уже более 100 000 таких систем. Работа со справочными правовыми системами становится нормой для специалистов различных уровней.

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;
- формирование пользовательской базы;
- скорость поиска документов по базе;
- актуальность информации и оперативность поступления документов;
- степень аутентичности документов оригиналу;
- юридическая обработка документов;
- 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 пакеты «Гарант», «КонсультантПлюс», «Дело и право».

При поиске по слову в названии документа в большинстве пакетов пользователю самому необходимо ограничить длину слова. Однако, например, программа «Юрисконсульт» найдет нужные слова, даже если они стоят 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», «Гарант» 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.

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 пяти лет назад и в настоящее время их пользователями являются более 120 000 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 40 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 два взаимосвязанных компонента: *информационно-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, со-

ставляющие Информационный банк СПС «КонсультантПлюс», представляют собой преимущественно текстовые поля.

Все программные модули СПС «КонсультантПлюс» реализованы на языке C++ 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 следующим аспектам:

- виду документа;
- регистрационному номеру документа;
- названию органа, принявшего документ;
- названию документа;
- ключевым словам;
- 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 «КонсультантПлюс»: *АО «КонсультантПлюс» — 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 Internet.

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.

1. *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.

2. *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 — документы, на которые действует просматриваемый. *Обратные ссылки* — документы, которые действуют на просматриваемый. Ссылки четко классифицированы по 17 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.

3. *Режим «папок» документов*, т.е. возможность сохранять сформированные подборки документов по некоторым тематикам, про-

изводить их объединение или пересечение. Становится возможной коллективная работа нескольких пользователей над одной проблемой.

Встроенный редактор в DOS-версии 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.

➢ ***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.

➢ ***КонсультантАрбитраж*** — 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 более 50 регионов: Москва, Санкт-Петербург, Астрахань, Екатеринбург, Омск, Тюмень, Нижний Новгород и т.д.

➢ ***КонсультантПлюс: Региональное законодательство.*** Первая в России свободная база нормативных актов органов местной власти и органов управления более 58 регионов России.

➢ ***КонсультантПлюс: Россия-СНГ***. Содержит многосторонние документы СНГ, двусторонние договоры России.

➢ ***КонсультантПлюс: ДеловыеБумаги*** — еще одна СПС семейства. Эта система представляет собой универсальную «мини-канцелярию», содержащую формы большинства стандартных деловых документов.

Системы семейства «КонсультантПлюс» работают на любых IBM-совместимых компьютерах, в средах DOS и Windows 95, в локальных сетях, доступны в сети Internet в режиме on-line.

Обновление баз СПС производится курьером, по почте, по электронным сетям Internet, РЕЛКОМ, РОСНЕТ. По модему возможно ежедневное обновление.

Системы также могут распространяться и обновляться на лазерных компакт-дисках. Имеется возможность ведения собственной базы данных.

В июне 1997 г. осуществлен *переход на 32-разрядную Windows версию.* Теперь пользователь может обращаться к одной и той же базе посредством трех программных оболочек: DOS, 16- и 32-разрядных версий Windows.

В сентябре 1997 г. версия СПС «КонсультантПлюс 6.0» прошла тестирование в США и признана полностью совместимой с операционными системами Windows NT и Windows 95. «КонсультантПлюс 6.0» стала единственной справочной правовой системой, получившей от компании «Microsoft» лого «Designed for Microsoft Windows NT and Windows 95». 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. По определению компании Microsoft, лого свидетельствует, что продукт прошел соответствующие испытания и является полностью функциональным в системах Windows NT и Windows 95; обеспечивает стабильную работу в различных режимах работы компьютера, в том числе и в критических ситуациях; позволяет полноценно применять 32-разрядные технологии.

В версии 6.0 достигнут крупнейший в России объем Информационного банка, включающего на середину 1997 г. свыше 200 000 документов. 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 г. 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 207 представительств в 120 регионах России и СНГ. Среди крупнейших клиентов компании — Центральный банк Российской Федерации, Внешторгбанк России, Сбербанк России и другие, а также ведущие аудиторские и консалтинговые фирмы.

Постоянными партнерами компании являются органы власти и управления федерального и регионального уровней: Государственная Дума РФ, Администрация Президента РФ, Министерство фи-

нансов, 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 Internet. СПС работает под управление ОС MS DOS, Windows 95, Windows NT, OS/2.

В июне 1997 г. вышла СПС нового поколения 4.0. Новая версия СПС разработана 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 хорошие показатели по аутентичности электронных копий документов официальным.

Информационные ресурсы в СПС «ГАРАНТ» на середину 1997 г. включают в себя 17 универсальных и специализированных БД, содержащих не утратившие актуальности документы, выпущенные с 1924 г. различными эмитентами, относящимися к высшим органам государственной власти и управления, а также БД «Российское законодательство на английском языке», шестиязычный Толковый словарь «Бизнес и право», *информационный банк* «Законодательство субъектов Российской Федерации», содержащий региональные базы данных, в том числе законодательства Москвы и Санкт-Петербурга. В информационных ресурсах компании «Гарант-Сервис» содержится более 150 000 документов и несколько гигабайт дополнительной экономической информации.

Информационные ресурсы СПС «Гарант» разделены на следующие четыре группы:

- ***Правовые Базы*** — программные продукты, поступающие в продажу и устанавливаемые на компьютер пользователя. Каждая из баз содержит полный комплект документов и сопроводительную аналитическую информацию по своей тематике.
- ***Базы-Справочники и Программы, связанные с правовой тематикой.***
- ***Электронный Архив*** — общий банк документов, хранящихся в компании «Гарант-Сервис» преимущественно в электронном виде. Информация из банка может *дополнить* Правовые Базы и может быть предоставлена по телекоммуникационным каналам в течение одного дня.
- ***Библиотека Гаранта*** — документы на бумажных носителях, к которым компания «Гарант-Сервис» имеет доступ и которые может передать пользователям в печатном виде.

Правовые Базы Гаранта включают общезначимые документы. По состоянию на середину 1997 г. универсальные и специализированные базы Гаранта содержат более 30 000 нормативных документов.

Правовые Базы СПС содержат следующие б а з ы д а н н ы х:

- «Законодательство России» (универсальная база, около 9250 документов);
- «Законодательство России на английском языке» (около 6300 документов);
- «Таможенное законодательство»;
- «Банковское законодательство»;
- «Землепользование. Недропользование. Природоохрана»;
- «Жилищное законодательство»;
- «Международное право»;
- «Налоговое и бухучет»;
- «Суд и арбитраж»;
- «Идеальная бухгалтерия»;
- «Формы правовых документов»;

а также региональные базы нормативных документов 41 региона России (около 60 000 документов).

Кодекс. В системе «Кодекс» имеется 33 базы данных.

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.

Кодекс позволяет просмотреть перечень документов, связанных с данным, а также создать *собственную базу данных.* «Кодекс» имеет полный набор средств для создания и ведения произвольного числа пользовательских баз данных.

О полноте и достоверности правовых баз данных. Подборкой документов, составляющих информационные базы коммерческих СПС, занимаются сами разработчики, заключая с органами власти дого-

воры 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. Вопрос возмещения материальных убытков из-за неточных или неполных сведений каждый разработчик решает 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 и задания

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. Определение гипертекста. Характеристика и использование гипертекста в СПС.
11. Документ как единица информационного банка СПС.
12. Методика поиска документов в СПС при известных реквизитах.
13. Методика поиска документов в СПС в случае, когда реквизиты неизвестны.
14. Сравнительная характеристика справочных правовых систем (Гарант, КонсультантПлюс, ЮСИС и т.д.).

Часть V

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глава 14

ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

14.1. Основы законодательства РФ в области информационной безопасности и защиты информации

Информация как объект правового регулирования

Развитие компьютерной техники и ее широкое внедрение в различные сферы человеческой деятельности вызвало рост числа противозаконных действий, объектом или орудием совершения которых являются электронно-вычислительные машины. 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 суммы денег, уклоняться от налогообложения, заниматься промышленным шпионажем, уничтожать программы конкурентов и т.д.

Информационная сфера или ***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:

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;

- защите информации, прав субъектов, участвующих в информационных процессах и информатизации (Федеральный закон «Об информации, информатизации и 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, 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» называется ***антропоцентрическим подходом***.

Федеральный закон «Об информации, информатизации и защите информации» определяет информацию как «*сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления*». Учитывая социальный аспект рассматриваемого объекта, добавим: включаемой в оборот в виде, понятном для восприятия человеком.

Закон вводит также термин ***документированная информация*** (документ) и определяет ее как «зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать».

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, называется ***техноцентрическим подходом***.

Согласно приведенному определению, *документированная информация* (документ) *есть*, *по сути дела*, *объект материальный*, что дает основание относить ее также и к категории вещей. На нее распространяется право вещной собственности. Следует отметить, что документированная информация относится к вещам особого рода. Главное отличие заключается в единстве информации и материаль-

ного 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 *меры защиты информации* можно разделить на следующие виды:

- правовые;
- организационные;
- технические.

Какое место занимают правовые меры в системе комплексной защиты информации? Во-первых, правовое обеспечение защиты информации относится к неформальным способам защиты. Во-вторых, в большинстве отечественных работ[1] правовые меры защиты информации принято рассматривать в рамках организационно-правового обеспечения защиты информации.

Объединение организационных и правовых мер вызвано отчасти объективно сложившимися обстоятельствами, а именно:

- проблемы законодательного регулирования защиты информации регламентировались ограниченным и явно недостаточным количеством нормативно-правовых актов;
- в отсутствие законодательства по вопросам защиты информации разрабатывалось большое количество ведомственных нормативных документов, основное назначение которых заклю-

[1] Основы информационной безопасности: Учебник / *В.А. Минаев*, *С.В. Скрыль*, *А.П. Фисун* и др. — Воронеж: Воронежский институт МВД России, 2000.

чалось в определении организационных требований по обеспечению защиты информации;
- внедрение автоматизированных информационных систем требует соответствующего правового обеспечения их защиты, однако на практике в развитии правовой базы не произошло существенных изменений и приоритет остается за организационными мерами.

Организационно-правовое обеспечение защиты информации представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию и функционирование защиты конкретных объектов и систем. 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, вопреки сложившимися традициям, не следует ограничиваться рассмотрением вопросов правовой защиты информации в рамках правовых аспектов комплексной защиты информации.

К правовым мерам следует отнести нормы законодательства, касающиеся вопросов обеспечения безопасности информации. 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;

---

[1] Основы информационной безопасности: Учебник / *В.А. Минаев*, *С.В. Скрыль*, *А.П. Фисун* и др. — Воронеж: Воронежский институт МВД России, 2000.

- 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 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 и в российских законах начала 1990-х гг.

Законодательство России в области информационных правоотношений начало формироваться начиная с 1991 г. и к настоящему времени включает *пятнадцать основных законов*:

- Закон «О банках и банковской деятельности» от 2.12.90 г. № 395-1 (в ред. ФЗ РФ от 30.02.96 г. № 17);
- Закон «О средствах массовой информации» от 27.12.91 г. № 124-1 (в ред. ФЗ РФ от 3.01.95 г. № 6, от 06.06.95 г. № 87, от 19.07.95 г. № 114, от 27.12.95 г. № 211);
- Патентный закон РФ от 23.09.92 г. № 3517-1;
- Закон «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 г. № 3523-1;
- Закон «О правовой охране топологий интегральных микросхем» от 23.09.92 г. № 3526-1;
- Основы законодательства об Архивном фонде РФ и архивах от 7.07.93 г. № 5341-1;
- Закон «Об авторском праве и смежных правах» от 9.07.93 г. № 5351-1 (с изменениями от 19.07.95 г.);

- Закон «О государственной тайне» от 21.07.93 г. № 5485-1;
- Закон «Об обязательном экземпляре документов» от 29.12.94 г. № 77-ФЗ;
- Закон «О связи» от 16.02.95 г. № 15-ФЗ;
- Закон «Об информации, информатизации и защите информации» от 20.02.95 г. № 24-ФЗ;
- Закон «Об оперативно-розыскной деятельности» от 12.08.95 г. № 144;
- Закон «О внешней разведке» от 10.01.96 г. № 5;
- Закон «Об участии в международном информационном обмене» от 5.06.96 г. № 85-ФЗ;
- Закон «Об электронной цифровой подписи» от 10.01.2002 г. № 1-ФЗ.

В базовых законах определены понятия, объекты, цели и правовые основы защиты информации и информационных ресурсов. Принимая в расчет то обстоятельство, что знание нормативной базы является необходимым условием обеспечения информационной безопасности, представляется целесообразным кратко рассмотреть содержание основных законодательных актов в порядке их принятия.

➢ ***Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»*** от 23.09.92 г. № 3523-1 и ***Закон РФ «О правовой охране топологий интегральных микросхем»*** от 23.09.92 г. № 3526-1 позволили законодательно защитить программное обеспечение компьютеров и права авторов и разработчиков программного обеспечения. До принятия этих законов, по сути, не существовало правовой защиты программного обеспечения и баз данных от незаконного копирования и тиражирования.

Закон РФ «О правовой охране программ *для вычислительных машин и баз данных*» впервые в российской практике отразил понятия, термины и правовые конструкции, касающиеся основных объектов и субъектов охраняемой сферы. Так, например, в главе 1 Закона дано определение следующих понятий: «программа для ЭВМ», «модификация программы», «база данных» и ряда других. Программы для ЭВМ и базы данных были отнесены к объектам авторского права. В главе 2 Закона сформулированы понятия исключительных авторских прав разработчиков программ — авторство, личные права, имущественные права и т.д. В главе 3 регламентируется порядок использования программ для ЭВМ и баз данных. Глава 4 посвящена собственно правовым аспектам защиты: наложению ареста на экземпляры программ и баз данных, изготовленные, воспроизведенные, распространенные, проданные, ввезенные или использованные другим образом либо предназначенные для использования в нарушение прав авторов и иных правообладателей. В главе предусмотрена уголовная ответственность за выпуск под своим именем чужой

программы или базы данных либо их незаконное воспроизведение или распространение.

➢ ***Закон РФ «Об авторском праве и смежных правах»*** урегулировал отношения, которые возникают в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач эфирного или кабельного вещания (смежные права). Закон «Об авторском праве и смежных правах» является одним из базовых в системе информационного законодательства России, поэтому он уточняет и повторяет ряд формулировок, касающихся авторских и смежных прав на программы и базы данных для компьютеров.

➢ ***Закон РФ «О государственной тайне»*** сформировал отношения в области защиты информации в случае ее отнесения к государственной тайне. Поскольку основная цель принятия Закона — обеспечение безопасности Российской Федерации в информационной сфере, в нем раскрываются основные понятия, касающиеся специальных информационных отношений. В Законе закреплено определение *носителей сведений*, составляющих государственную тайну. К ним отнесены *материальные объекты*, *в том числе и физические поля*, *в которых сведения*, с*оставляющие государственную тайну*, *находят свое отражение в виде символов*, *образов*, *сигналов*, *технических решений и процессов*. Важным моментом следует признать приведенную в Законе *классификацию средств защиты информации*: технические, криптографические, программные и другие средства, а также средства контроля эффективности защиты информации. Определен в Законе и порядок доступа к сведениям, составляющим государственную тайну.

➢ ***Закон РФ «Об обязательном экземпляре документов»*** вводит понятие документа. Согласно определению, документ — это материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и практического использования. В Законе, впервые в России, приведена также классификация документов. В соответствии с классификацией алгоритмы и программы для компьютеров отнесены к электронным изданиям и неопубликованным документам. Для правового регулирования электронного документооборота важным является данное в ст. 5 Федерального закона определение *официального документа*, под которым понимается произведение печати, публикуемое от имени органов законодательной, исполнительной и судебной власти, носящее законодательный, нормативный, директивный или информационный характер.

➢ ***Федеральный закон «О связи»*** установил правовые основы деятельности в области связи, полномочия органов государственной

власти по регулированию услуг в области связи, определил права и обязанности юридических и физических лиц, предоставляющих услуги связи или пользующихся ими.

В Законе отмечено, что связь функционирует на территории Российской Федерации как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти, обороны, безопасности, правоохранительных органов, а также юридических и физических лиц в услугах электрической и почтовой связи. В соответствии с Законом, связь является неотъемлемой частью производственной и социальной инфраструктуры Российской Федерации и включает в себя все сети и сооружения электрической и почтовой связи, за исключением внутрипроизводственных и технологических сетей связи. Средства связи совместно со средствами вычислительной техники составляют техническую основу процессов сбора, обработки, накопления и распространения информации.

С точки зрения вопросов защиты информации важными являются приведенные в тексте закона о п р е д е л е н и я ряда понятий:

электрическая связь (электросвязь) — всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам;

сети электросвязи — технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания;

взаимоувязанная сеть связи Российской Федерации — комплекс технологически сопряженных сетей электросвязи на территории Российской Федерации, обеспеченный общим централизованным управлением;

сеть связи общего пользования — составная часть взаимоувязанной сети связи Российской Федерации, открытая для пользования всем физическим и юридическим лицам, в услугах которой этим лицам не может быть отказано;

ведомственные сети связи — сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетворения производственных и специальных нужд, имеющие выход на сеть связи общего пользования;

внутрипроизводственные и технологические сети связи — сети электросвязи федеральных органов исполнительной власти, а также предприятий, учреждений и организаций, создаваемые для управления внутрипроизводственной деятельностью и технологическими процессами, не имеющие выхода на сеть связи общего пользования;

выделенные сети связи — сети электросвязи физических и юридических лиц, не имеющие выхода на сеть связи общего пользования;

предприятия, учреждения и организации связи — юридические лица независимо от форм собственности, предоставляющие услуги электрической или почтовой связи физическим и юридическим лицам в качестве основного вида деятельности;

оператор связи — физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи;

услуги связи — продукт деятельности по приему, обработке, передаче и доставке почтовых отправлений или сообщений электросвязи;

пользователи связи — физические и юридические лица, являющиеся потребителями услуг связи;

лицензия — документ, устанавливающий полномочия физических и юридических лиц в соответствии с настоящим Федеральным законом и иными правовыми актами для осуществления деятельности в области связи;

сертификат — документ, подтверждающий, что надлежащим образом идентифицированные оборудование или услуга связи соответствуют требованиям нормативных документов;

оконечное оборудование — подключаемые к абонентским линиям и находящиеся в пользовании абонентов технические средства формирования сигналов электросвязи для передачи или приема заданной абонентами информации по каналам связи;

средства связи — технические средства, используемые для формирования, обработки, передачи или приема сообщений электросвязи либо почтовых отправлений.

В Законе прописаны и некоторые вопросы, касающиеся обеспечения информационной безопасности в области связи. В соответствии со ст. 31 защита прав пользователей связи на предоставление услуг электрической и почтовой связи надлежащего качества, получение информации о таких услугах и об их исполнителях, а также механизм реализации этих прав регулируются законодательством Российской Федерации. Нормативные правовые акты субъектов Российской Федерации, регулирующие отношения в области связи в соответствии с полномочиями субъектов Российской Федерации, не могут ограничивать права пользователей связи, установленные соответствующими федеральными законами.

В ст. 32 говорится, что тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией Российской Федерации. Все операторы связи обязаны обеспечить соблюдение тайны связи. Информация о почтовых отправлениях и передаваемых по сетям электрической связи сообщениях, а также сами эти отправления и сообщения

могут выдаваться только отправителям и адресатам или их законным представителям.

Прослушивание телефонных переговоров, ознакомление с сообщениями электросвязи, задержка, осмотр и выемка почтовых отправлений и документальной корреспонденции, получение сведений о них, а также иные ограничения тайны связи допускаются только на основании судебного решения.

Должностные и иные лица, работники связи, допустившие нарушение указанных положений, привлекаются к ответственности в порядке, установленном законодательством Российской Федерации.

Согласно ст. 33 Закона, операторы связи несут ответственность за сохранность принятых почтовых и иных отправлений, доставку их по назначению в установленные сроки.

➢ ***Федеральный закон «Об информации, информатизации и защите информации»*** был принят Государственной Думой Федерального Собрания Российской Федерации 25 января 1995 г. Закон подписан Президентом Российской Федерации 20 февраля 1995 г. № 24-ФЗ и вступил в силу со дня его официального опубликования в «Российской газете» 22 февраля 1995 г. № 39.

1. Федеральный закон «Об информации, информатизации и защите информации» регулирует отношения, возникающие при:

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
- создании и использовании информационных технологий и средств их обеспечения;
- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах» (п. 2 ст. 1).

2. В соответствии со ст. 4 Закона информационные ресурсы, являясь объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами. *Правовой режим информационных ресурсов* определяется нормами, устанавливающими:

- порядок документирования информации;
- право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;
- категорию информации по уровню доступа к ней;
- порядок правовой защиты информации.

3. В ст. 5 Закона определено, что документ, полученный из автоматизированной информационной системы, приобретает юриди-

ческую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации. В этом случае юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Следует иметь в виду, что при соблюдении указанных условий, в том числе при подтверждении юридической силы документа электронной цифровой подписью, этот документ может признаваться в качестве доказательства по делу, рассматриваемому арбитражным судом.

4. В ст. 6 Закона установлено, что информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находиться в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.

5. В соответствии со ст. 23 Закона защита прав субъектов в сфере информационных процессов и информатизации осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба. При решении вопроса о возможности рассмотрения арбитражным судом дел данной категории следует исходить из подведомственности споров, установленной Арбитражным процессуальным кодексом Российской Федерации.

6. Ст. 24 Закона устанавливает защиту прав на доступ к информации, в частности, отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке. Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба (ст. 24, п. 1, абзац 3). При определении подведомственности указанных споров необходимо руководствоваться ст. 20 и 22 Арбитражного процессуального кодекса Российской Федерации (после 1 июля 1995 г. — новым Арбитражным процессуальным кодексом Российской Федерации), а также учитывать требования Постановления Пленума Верховного суда Российской Федерации и Пленума Высшего Арбитражного суда Российской Федерации от 18 августа 1992 г. № 12/12 относительно субъектного состава участников спора и характера правоотношений. Неисполнение или не-

надлежащее исполнение обязательств по договору поставки, купли-продажи и по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом (ст. 24, п. 1, абзац 2).

В Законе «Об информации, информатизации и защите информации» определен ряд важнейших понятий:

информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

документированная информация (*документ*) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

информационная система — организационно упорядоченная совокупность документов (массивов документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

информация о гражданах (*персональные данные*) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

государственная тайна — документированная информация, правовой режим которой установлен Законом Российской Федерации «О государственной тайне»;

конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

средства обеспечения автоматизированных информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), исполь-

зуемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

защита информации — организационные, правовые, технические и технологические меры по защите информации, предотвращающие угрозы безопасности и (или) устраняющие их последствия;

собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

пользователь (*потребитель*) *информации* — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

➢ ***Федеральный закон РФ «Об участии в международном информационном обмене»*** № 85-ФЗ принят Государственной Думой 5 июня 1996 г. и вступил в силу 4 июля 1997 г. Закон преследует следующие цели:

- создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства;
- защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене;
- защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

В соответствии с п. 2 ст. 1 Федерального закона он, наряду с другими федеральными законами и иными нормативными правовыми актами, устанавливает порядок международного обмена конфиденциальной и массовой информацией.

Вместе с тем Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации «Об авторском праве и смежных правах».

В Законе введен ряд новых терминов — «информационные продукты», «информационные услуги», «информационная безопасность», «информационная сфера», даны их определения, а также уточнены некоторые ранее введенные определения.

Массовая информация — предназначенные для неограниченного круга лиц печатные, аудиосообщения, аудиовизуальные и иные сообщения и материалы.

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информа-

ционных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

Информационные продукты (*продукция*) — документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Информационные услуги — действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Собственник документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена — субъект, реализующий полномочия владения, пользования, распоряжения указанными объектами в объеме, устанавливаемом законом.

Владелец документированной информации, информационных ресурсов, информационных продуктов и (или) средств международного информационного обмена — субъект, реализующий полномочия владения, пользования и распоряжения указанными объектами в объеме, устанавливаемом собственником.

Пользователь (*потребитель*) информации, средств международного информационного обмена — субъект, обращающийся к собственнику или владельцу за получением необходимых ему информационных продуктов или возможности использования средств международного информационного обмена и пользующийся ими.

Информационные процессы — процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Международный информационный обмен — передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу Российской Федерации.

Средства международного информационного обмена — информационные системы, сети и сети связи, используемые при международном информационном обмене.

Информационная сфера (*среда*) — сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

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 документирован-

ная 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.

➢ ***Федеральный закон «Об электронной цифровой подписи»*** (от 10.01.2002 г.) имеет целью 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. Действие Закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

В законе определен ряд терминов, важных с точки зрения обеспечения безопасности информации:

электронный документ — документ, в котором информация представлена в электронно-цифровой форме;

электронная цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

владелец сертификата ключа подписи — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

закрытый ключ электронной цифровой подписи — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

подтверждение подлинности электронной цифровой подписи в электронном документе — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;

пользователь сертификата ключа подписи — физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

информационная система общего пользования — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

корпоративная информационная система — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

В соответствии со ст. 4 Закона электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент

проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Согласно ст. 5 создание ключей электронных цифровых подписей осуществляется для использования:
- в информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;
- в корпоративной информационной системе в порядке, установленном в этой системе.

Кроме законов, на первом этапе деятельности по созданию и развитию законодательства в области информационной безопасности были изданы

➢ ***Указы Президента Российской Федерации***:
- «О создании Государственной технической комиссии при Президенте Российской Федерации» от 5.01.92 г. № 9;
- «Концепция правовой информатизации России» от 28.06.93 г. № 966;
- «О дополнительных гарантиях прав граждан на информацию» от 31.12.93 г. № 2334 (с изменениями от 17 января 1997 г.);
- «Об основах государственной политики в сфере информатизации» от 20.01.94 г. № 170 (с изменениями от 26 июля 1995 г., 17 января, 9 июля 1997 г.);
- «Вопросы деятельности Комитета при Президенте Российской Федерации по политике информатизации» от 17.02.94 г. № 328 (с изменениями от 9 июля 1997 г.);
- «О президентских программах по правовой информатизации» от 4.08.95 г. № 808;
- «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» от 3.04.95 г. № 334;
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.95 г. № 1203 (с изменениями от 24 января 1998 г.)
- «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» от 9.01.96 г. № 21;

- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20.01.96 г. № 71 (с изменениями от 21 апреля, 6 июня 1996 г., 14 июня 1997 г.);
- «Об утверждении перечня сведений конфиденциального характера» от 6.03.97 г. № 188.

Президентом Российской Федерации утверждена ***Доктрина информационной безопасности Российской Федерации*** (9.09.2000 г. № Пр-1895), которая опубликована в «Российской газете» от 28.09.2000 г. № 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 (п. 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 (п. 1 раздела I).

---

[1] О Доктрине информационной безопасности Российской Федерации. Письмо ВАС РФ № С1-7/УЗ-1121 от 31.10.2000 г.

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 социально значимой информации;
- манипулирование информацией (дезинформация, сокрытие или искажение информации) и др. (п. 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 (п. 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 (п. 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 (п. 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 ха-

рактера, а также повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

6. В Доктрине сформулированы основные положения государственной политики обеспечения информационной безопасности Российской Федерации (п. 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 (п. 11 раздела III).

➢ ***Уголовный кодекс РФ***, вступивший в действие в 1997 г., 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.

К уголовно наказуемым отнесены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В тех случаях, когда общественно опасные действия в области информационных отношений совершаются без применения компьютерных средств, законодатель нередко относит их к другим, соответствующим родовым объектам.

Так, клевета или оскорбление (ст. ст. 129, 130), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), нарушение авторских, смежных изобретательских и патентных прав (ст. ст. 146, 147) находятся в разделе «Преступления против личности». Кража, мошенничество, хищение предметов, имеющих особую ценность, умышленное уничтожение или повреждение имущества, заведомо ложная реклама, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. ст. 158, 159, 164, 167, 182, 187, 189) — в разделе «Преступления в сфере экономики» и т.д.

Таким образом, информационные отношения получили и уголовно-правовую защиту. Из этого следует, что *конфиденциальная документированная информация* 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 в настоящее время законодательная база обеспечения защиты информации в стране находится в состоянии становления. Продолжается процесс ее создания и совершенствования.

14.2. Понятие и виды защищаемой по законодательству РФ информации

Ст. 10 Федерального закона «Об информации, информатизации 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 документированная информация, отнесенная законом к категории ограниченного доступа.

Документированная информация (документ) — зафиксированная на материальном носителе информации с реквизитами, позволяющими ее идентифицировать.

В соответствии с ФЗ «Об информации, информатизации и защите 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.

Таким образом, согласно ФЗ «Об информации, информатизации и защите информации», для того, чтобы информация могла быть отнесена к категории с ограниченным доступом, необходимо соблюдение, по крайней мере, двух условий:

1) она должна быть документированной, т.е. зафиксированной на материальном носителе;

2) должен существовать нормативный акт (закон), в соответствии с которым ограничивается доступ к ней.

Информация с ограниченным доступом, в свою очередь, подразделяется на сведения, составляющие государственную тайну и конфиденциальную информацию (ст. 10 ч. 2 ФЗ «Об информации, информатизации и защите информации»). Классификация информации по категориям доступа приведена на рис. 14.1.

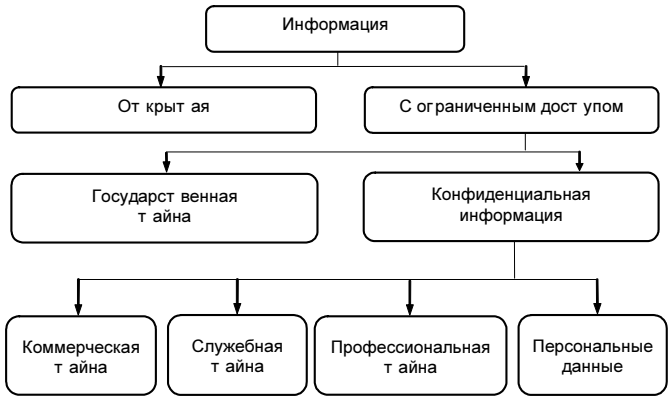


Рис. 14.1. **Классификация информации по категориям доступа**

Существует мнение, что 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].

Перечень видов информации с ограниченным доступом и соответствующая нормативная база представлены в табл. 14.1.

Следует отметить, что из всех многочисленных видов конфиденциальной информации в Законе «Об информации, информатизации и защите информации» упомянуты лишь личная и семейная тайны, персональные данные, тайна переписки, телефонных, почтовых, телеграфных и иных сообщений.

Однако рассмотрение действующего законодательства позволяет сделать следующий вывод: конфиденциальность или тайна есть обязательное свойство только документированной информации, которая подлежит дальнейшей защите ее собственником в зависимости от

[1] *Карпычев В.Ю.* Основы информационной безопасности: Учеб. пособ. — М.: ГУ НПО «Специальная техника и связь» МВД России, 2001.

Таблица 14.1. ***Классификация информации ограниченного доступа***

Информация с ограниченным доступом	*Нормативные и законодательные акты*
Государственная тайна	ФЗ «О государственной тайне», ст. ст. 275, 276, 283, 284 УК РФ
Конфиденциальная информация	ФЗ «Об информации, информатизации и защите информации», ст. 10
Персональные данные	ФЗ «Об информации, информатизации и защите информации», ст. 11
Личная и семейная тайна	Конституция РФ, ст. 23; ФЗ «Об информации, информатизации и защите информации», ст. 11; ГК РФ, ст. 150
Служебная тайна	ГК РФ, ст. 139
Служебная информация	ФЗ «О рынке ценных бумаг», ст. 31
Коммерческая тайна	ГК РФ, ст. 139
Сведения о сущности изобретения... («ноу-хау»)	Указ Президента РФ № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна следствия и судопроизводства	Указ Президента РФ № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна связи	ФЗ «О связи», ст. 32; ФЗ «Об информации, информатизации и защите информации», ст. 11
Тайна страхования	ГК РФ, ст. 946
Тайна усыновления	Семейный кодекс РФ, ст. 139; УК РФ, ст. 155
Тайна исповеди	ФЗ «О свободе совести и религиозных объединениях», ст. 3
Банковская тайна	ГК РФ, ст. 857; ФЗ «О внесении изменений и дополнений в Закон РСФСР “О банках и банковской деятельности в РСФСР”», ст. 26; УК РФ, ст. 183
Нотариальная тайна	Основы законодательства РФ о нотариате ст. 16, 29
Адвокатская тайна	Закон РСФСР «Об утверждении Положения об адвокатуре РСФСР», ст. 16
Врачебная тайна	Основы законодательства Российской Федерации «Об охране здоровья граждан», ст. 161; Закон РФ «О трансплантации органов и (или) тканей человека», ст. 14

степени секретности. Так, ст. 2 ФЗ «Об информации, информатизации и защите информации» устанавливает, что конфиденциальной информацией является документированная информация, доступ к

которой ограничивается в соответствии с законодательством Российской Федерации, а ст. 21 того же Закона устанавливает положение, согласно которому защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу.

Главной чертой настоящего этапа развития информационных отношений в области обеспечения информационной безопасности является переход от ведомственных, преимущественно технократических подходов к защите информационных ресурсов, к комплексному государственному регулированию вопросов защиты информации.

Однако уже в ФЗ «Об участии в международном информационном обмене» государственная тайна определяется как один из видов конфиденциальной информации (ст. 8). Такая путаница сохраняется в ряде других законов, где ссылки на «иные охраняемые секреты, иные охраняемые законом тайны» предполагают продолжение списка видов информации с ограниченным доступом.

В Указе Президента РФ от 6.03.97 г. № 188 «Об утверждении перечня сведений конфиденциального характера» 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.

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, касающегося профессиональной тайны, слов «и так далее» предполагает его продолжение.

ФЗ «Об информации, информатизации и защите информации» в ч. 3, ст. 10 закрепляет *перечень сведений, которые не разрешается относить к информации с ограниченным доступом*, а именно:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Таким образом, анализ действующего законодательства показывает, что:

1. Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (ФЗ «Об информации, информатизации и защите информации»).

2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать (ФЗ «Об информации, информатизации и защите информации»).

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, и массовой, предназначенной для неограниченного круга лиц (ФЗ «Об информации, информатизации и защите 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 (Закон РФ «Об авторском праве и смежных правах», ст. 146 УК РФ);
- информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (ФЗ «Об информации, информатизации и защите информации», ст. 140 УК РФ) и др.

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является нарушением его прав, т.е. неправомерной.

7. Неправомерное использование документированной информации наказуемо.

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

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 как условие, способствующее или препятствующее 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 являющиеся 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, по-

среднической, 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.

Собственно коммерческая тайна специальной уголовно-правовой и режимной защитой не обладает.

Определение и вопросы гражданско-правовой охраны служебной и коммерческой тайны рассмотрены в ст. 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 неизвестности 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 практически к 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?

Ответ на первый вопрос содержится в Постановлении Правительства РСФСР от 5.12.91 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну». Согласно Постановлению к таковым относятся:

- учредительные документы (решение о создании предприятия или договор учредителей) и Устав;
- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежах;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;
- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Этим же нормативным актом запрещено государственным и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

- о размерах имущества предприятия и его денежных средствах;
- о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;
- о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;
- о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

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. 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.

Проблема состоит в том, кто и как должен обеспечить защиту коммерческой тайны. Действующее законодательство напрямую не ставит ее под свою защиту. Если допустить, что соответствующая норма имелась бы, например, в Уголовном кодексе, то и это еще не говорило бы о том, что коммерческая тайна надежно защищена. Наличие нормы предполагает лишь, что в случае нарушения содержащегося в ней запрета виновный понесет соответствующее наказание. Однако сам факт наличия соответствующей нормы следовало бы считать положительным.

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 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 быть 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

[1] *Фатьянов А.А.* Тайна и право. — М.: МИФИ, 1999.

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 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 со 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. В соответствии со ст. 16 Закона РСФСР «Об утверждении Положения об адвокатуре РСФСР», адвокат не вправе разглашать сведения, сообщенные ему доверителем в связи с оказанием юридической помощи.

Адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя (ст. 15 Закона).

➢ ***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 ст. 139 или ст. 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 связи.*** Федеральный закон «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами — физическими или юридическими лицами — по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией Российской Федерации.

Обязанность обеспечения соблюдения тайны связи возлагается на оператора связи, под которым понимается физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи.

➢ ***Тайна усыновления.*** Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения).

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

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам (ст. 310 УК «Разглашение данных предварительного расследования»).

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.*** 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. 124 Арбитражного процессуального кодекса Российской Федерации.

Персональные данные

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.

Основные положения работы с информацией о частной жизни получили закрепление в Федеральном законе «Об информации, информатизации и защите информации» от 20 февраля 1995 г. Согласно этому закону информация о гражданах (персональные данные), т.е. сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, относится к категории конфиденциальной (ст. 2, ч. 5 ст. 10, ч. 1 ст. 11). Ключевым в определении персональных данных следует считать понятие «идентификация».

Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона (ч. 1 ст. 11).

В настоящее время закон о персональных данных еще не принят. Поэтому достаточно трудно определить 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.

14.3. 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

В соответствии с Федеральным законом «Об информации, информатизации и защите информации» документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Таким образом, 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 ст. 5 Федерального закона «Об информации, информатизации и защите информации» говорится следующее: документирование информации является обязательным условием включения информации в информационные ресурсы. 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, информатизации и защите 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 гг. американскими математиками У. Диффи и М. Хеллмэном.

Возможность использования ЭЦП прописана в Законе «Об информации, информатизации и защите информации»: юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. 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 — набор знаков и символов для подтверждения подлинности электронных документов. В основе создания и использования ЭЦП лежат математические принципы. В России в 1994 г. 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 определенной длины);
2) выработки ЭЦП под документом;
3) проверки подписи.

Цифровую подпись практически невозможно подделать. Проверить подлинность подписи может любой участник электронного документооборота (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 цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе».

Следует заметить, что попытки разработать ***правовой режим электронного документа*** предпринимались в нашей стране с середины 1970-х гг. Приказом № 158 от 29 декабря 1980 г. Государственный комитет СССР по делам изобретений и открытий утвердил Положение о Всесоюзной магнитно-ленточной службе патентной информации. Государственный комитет по науке и технике СССР Постановлением № 100 от 20 апреля 1981 г. 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 машинном 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;
- вводились понятия 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 поздние 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, информатизации и защите информации» (п. 3 ст. 5) гласит: «Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуни-

кационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования».

Принципиально новая ситуация сложилась после принятия Закона «Об информации, информатизации и защите информации» и нового Гражданского кодекса РФ. Ряд основных положений закона, касающихся ЭЦП и электронного документа, рассматривался выше. Поэтому обратимся к статьям ГК РФ, касающимся использования электронных документов и электронно-цифровой подписи.

1. Согласно ст. 160, использование электронно-цифровой подписи либо иного аналога собственно ручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

2. В соответствии со ст. 434 договор в письменной форме может быть заключен путем обмена посредством электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

3. Согласно ст. 847, договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом.

Таким образом, новый ГК РФ 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 РФ 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.

«Положение о государственном лицензировании в области защиты информации» утверждено решением Гостехкомиссии РФ и ФАПСИ 27 апреля 1994 г., а «Типовые требования к заявителям» утверждены ФАПСИ 15 июня 1995 г. Указом Президента РФ от 3 апреля 1995 г. № 334 «О мерах в области шифровальных средств» запрещена деятельность юридических и физических лиц в области

шифровании информации без лицензии. Государственным организациям запрещено использовать не имеющие сертификата средства криптографической защиты информации.

Электронный документ как доказательство

С точки зрения правового режима важным является вопрос о возможности использования электронного документа в качестве доказательства. В 1979 г. Государственный арбитраж СССР принял Инструктивные указания № И-1-4. В соответствии с этим документом, данные на машинном носителе информации могут быть использованы в качестве доказательств по арбитражному делу. Для этого они должны быть преобразованы в форму, пригодную для обычного восприятия и хранения в деле.

Очевидно, что не существует препятствий для использования электронных документов в качестве доказательств, если соблюден ряд условий.

Во-первых, представляемые документы, подготовленные с помощью электронно-вычислительной техники, должны быть надлежащим образом оформлены. Документ должен обладать юридической силой, которую придает присутствие необходимых реквизитов.

Во-вторых, документы, подготовленные с помощью электронно-вычислительной техники и представляемые в арбитраж в качестве доказательств по делу, должны быть представлены в таком виде, который позволял бы уяснить их содержание. Данные, содержащиеся на техническом носителе (перфоленте, перфокарте, магнитной ленте, магнитном диске и т.п.), могут быть использованы в качестве доказательств по делу только в случаях, когда они преобразованы в форму, пригодную для обычного восприятия и хранения в деле.

Отдельного рассмотрения требует вопрос об использовании в качестве доказательств документов, в которых использована система электронно-цифровой подписи. Такая подпись как набор знаков и символов в силу технических свойств не может существовать в форме, пригодной для обычного восприятия. Поэтому в суд должны быть предъявлены традиционные копии документа.

С учетом того, что бумажная копия и подлинник электронного документа имеют одинаковую юридическую силу, остается открытым только вопрос о процедуре создания традиционной копии документа.

Проблема частично решена в Письме Высшего арбитражного суда РФ от 19 августа 1994 г. Согласно этому, письменные доказательства представляются в подлиннике или в заверенной надлежащим образом копии.

При возникновении вопроса об авторстве и подлинности подписи назначается судебная экспертиза. Основное отличие заключа-

ется в виде экспертизы, которую необходимо провести для установлении авторства или подлинности подписи — графологической или технической.

В Письме Высшего Арбитражного суда РФ от 7 июня 1995 г. говорится, что юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронно-цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии программно-технических средств, обеспечивающих идентификацию подписи и при соблюдении установленного режима их использования.

Если учесть, что в ГК РФ и Законе «Об информации, информатизации и защите информации» признается возможность использования электронно-цифровой подписи для удостоверения электронных документов и существует процедура создания бумажных копий, которые имеют одинаковую юридическую силу с подлинником, то электронные документы подпадают под традиционное понятие «письменные доказательства».

Процедура разрешения конфликтов

Для нормального функционирования систем электронного документооборота (ЭДО) необходимо разработать процедуры разрешения возможных конфликтов. Стороной таких конфликтов, кроме участников ЭДО и фирмы-провайдера, может быть и фирма — разработчик программного обеспечения.

Предполагается, что договор с фирмой-разработчиком учитывает наличие эталонного образца программного обеспечения, который может храниться только у фирмы-провайдера или у всех участников ЭДО. Для этого требуется выполнение двух основных условий:

- должно быть документально подтверждено, что каждому участнику системы ЭДО (включая фирму-провайдера) установлено программное обеспечение, соответствующее эталонному образцу;
- хранение эталонных образцов организуется таким образом, чтобы исключить возможность изменения эталонного образца программного обеспечения без ведома сторон.

Такой режим может быть обеспечен системой из нескольких открытых ключей.

Лицензирование и сертификация в области систем обеспечения безопасности информации

Сегодня, когда современные информационные технологии интенсивно внедряются во все сферы жизни и деятельности общества,

национальная и (как ее часть) экономическая безопасность государства начинает напрямую зависеть от обеспечения информационной безопасности. Именно поэтому с целью создания гарантий по обеспечению необходимой стойкости средств защиты информации государство берет на себя ответственность за лицензирование деятельности организаций, занимающихся защитой информации, и сертификацию соответствующих технических средств.

Государственные интересы в области защиты информационных ресурсов страны в настоящее время обеспечивают Гостехкомиссия РФ и ФАПСИ. ГТК РФ строит свою работу на оказании практической помощи в решении вопросов обеспечения защиты информации в глобальных сетях.

Задачей ФАПСИ является обеспечение безопасного обмена информацией органов государственной власти, одним из аспектов решения которой стало создание в ближайшее время специального защищенного домена сети Internet, обеспечивающего эффективную информационную поддержку оперативного государственного управления и организацию доступа к необходимым зарубежным информационным ресурсам.

Сегодняшний уровень защиты от внешних информационных угроз в глобальных открытых сетях не может быть сочтен удовлетворительным: до сих пор в России отсутствует всеобъемлющая и технически выверенная стратегия в этой области. С целью изменения ситуации должен быть безотлагательно разработан и осуществлен комплекс мер в области законодательства и стандартизации средств, обеспечивающих информационную безопасность России. К первоочередным задачам в этом направлении относятся:

- принятие специального закона, аналогичного «Computer Security Act» в США, возлагающего на конкретные госструктуры ответственность за методологическую поддержку работ в области информационной безопасности;
- выработку унифицированных подходов к обеспечению безопасности для организаций различного профиля, размера и форм собственности;
- обеспечение появления на рынке достаточного числа разнообразных сертифицированных средств для решения задач информационной безопасности.

Одной из проблем в области защиты информации в России является отсутствие официальных документов с подробными рекомендациями по построению безопасных информационных систем, аналогичных разработанным, например, Американским институтом стандартных технологий (США) и британскому стандарту. Хотя в Великобритании не существует нормативных актов, требующих вы-

полнения государственных стандартов, около 60% британских фирм и организаций добровольно используют разработанный стандарт, а остальные намерены внедрять его рекомендации в ближайшее время.

Лицензирование и сертификация в области систем обеспечения безопасности информации могут снизить остроту этой проблемы. Необходимо создание пользователю гарантий того, что используемые им средства защиты информации способны обеспечивать необходимый уровень защиты. Именно лицензирование может способствовать тому, что проблемой защиты информации будут заниматься только высококвалифицированные специалисты в этой области, а создаваемые ими продукты будут находиться на соответствующем уровне и смогут пройти сертификацию.

Без проведения сертификации невозможно оценить, содержит ли то или иное средство потенциально вредные недокументированные возможности, наличие которых особенно характерно для большинства зарубежных продуктов, способные в определенный момент привести к сбоям в работе системы и даже к необратимым для нее последствиям. Характерным примером таких недокументированных возможностей является заложенная фирмой «Ericsson» при разработке телефонных станций, на базе которых МПС РФ строит свою телефонную сеть, возможность блокировать их работу при получении вызова определенного телефонного номера, который фирма отказывается назвать. И этот пример не является единственным.

Процесс сертификации программного продукта занимает примерно столько же времени, сколько и его разработка, и практически невозможен без исходных текстов программ с комментариями. В то же время многие зарубежные фирмы не желают представлять исходные тексты своих программных продуктов в российские сертификационные центры. Например, несмотря на принципиальное согласие фирмы «Microsoft» на сертификацию в России ОС Windows NT, в которой уже выявлено более 50 ошибок, связанных с обеспечением безопасности, этот вопрос уже в течение многих месяцев не может сдвинуться с мертвой точки из-за отсутствия ее исходных текстов.

Трудности с сертификацией приводят к тому, что раньше других среди продуктов одного класса сертификат быстрее получают самые простые, в силу чего они кажутся пользователю более надежными. Длительные же сроки сертификации приводят к тому, что фирма-разработчик успевает вывести на рынок новую версию своего продукта, и процесс становится бесконечным.

Сертификацию технических средств защиты информации затруднительно проводить без соответствующих стандартов, создание которых в России не в последнюю очередь сдерживается из-за отсутствия финансовых средств. Эта проблема решается, если появля-

ются несколько фирм, заинтересованных в сбыте, и несколько организаций, заинтересованных в использовании соответствующих технических средств. Например, плодом совместных усилий подобных организаций, фирм и ГТК РФ стала разработка Руководящего технического материала ГТК РФ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Он позволил классифицировать средства, которые способны в какой-то степени обеспечить защиту корпоративных сетей от внешних вторжений.

Документ предполагает существование нескольких классов межсетевых экранов: от простейших, позволяющих только осуществлять контроль потоков информации, до самых сложных, выполняющих полное перекодирование входящей информации, полностью защищающее корпоративную сеть от воздействий извне. Уже сегодня сертификацию на соответствие техническим условиям, разработанным в соответствии с Руководящим техническим материалом, что допускается действующим законодательством, прошли такие межсетевые экраны, как Sun Screen, SKIPbridge и Pandora. Однако и при их сертификации без борьбы не обошлось.

Internet заостряет любую проблему обеспечения безопасности в сетевой среде до предела, и если раньше можно было игнорировать развитие информационных технологий, мировой опыт и международное законодательство в области защиты информации и коммуникаций, то сейчас этого себе позволить уже нельзя. Internet ведет жесткий отбор, у него своя система лицензирования и сертификации, где неудачник отсекается без объяснений, независимо от того, есть у него какой-либо документ либо нет.

С учетом требований информационной безопасности и мировой практики деятельности в сфере защиты информации представляется целесообразным присоединение России к сложившимся системам международной стандартизации и сертификации информационных технологий, что на практике означает:

- приведение национальных и отраслевых стандартов в соответствие с международными;
- участие представителей России в международных системах сертификации (в том числе в сертификационных испытаниях);
- возможность признания в России международных сертификатов.

Что касается восприятия сертификатов пользователями, то сегодня на российского пользователя завораживающе действует само слово «сертификат», причем часто даже не обращается внимание, на соответствие чему он выдан. Например, межсетевые экраны зачас-

тую сертифицируются не на обеспечение защиты корпоративной сети при передаче информации по открытым каналам связи, а в качестве, например, однопользовательской системы для доступа ко всем ресурсам сети, после чего пользователю не без успеха внушается мысль, что ему предлагается сертифицированное средство.

Можно ли в настоящее время использовать несертифицированные средства защиты? Запрета на это нет, но только тогда, когда, как это прямо оговорено в законе, они используются для обработки информации ограниченного доступа или для подключения к сетям внутрикорпоративного информационного обмена. Однако использование несертифицированных средств, в соответствии с законодательством, не позволяет решать спорные вопросы в судебном порядке и грозит убытками. Ситуацию не спасает даже запись в договоре с фирмой, поставившей несертифицированное оборудование, о ее материальной ответственности в случае конфликта при проведении платежных операций, поскольку при использовании такого оборудования юридически невозможно доказать наличие факта выполнения операции, явившейся предметом конфликта.

Кроме того, в соответствии с действующим законодательством, любая организация, занимающаяся сбором и обработкой персональных данных (например, операций с пластиковыми карточками), должна иметь лицензию на право заниматься подобной деятельностью и использовать для этого сертифицированные средства.

В ближайшее время должен выйти документ о порядке сертификации Автоматизированных банковских систем (АБС), подготовленный по инициативе Госстандарта с привлечением ЦБ РФ, ФАПСИ, ГТК и Министерства связи. В нем описан порядок сертификации устройств и систем, входящих в АБС, и оговорено, что сертификации подлежат все системы, подключаемые к системе ЦБ РФ. Надзор и контроль за сертификацией возлагается на ЦБ РФ.

Существуют серьезные проблемы обеспечения информационной безопасности банков, которые до сих пор не нашли своего решения. Например, как обеспечить защищенный обмен информацией с представительством банка за рубежом? Здесь имеет место юридическая коллизия, в соответствии с которой, с одной стороны, вывозить отечественные средства защиты за рубеж можно только по специальному разрешению, а с другой, — можно использовать средства защиты зарубежного производства, только прошедшие российскую сертификацию, а таковые отсутствуют.

Другой вопрос: нужно ли банку самому разрабатывать защищенную автоматизированную систему. Для того чтобы банк мог разрабатывать защищенную АБС, он должен получить лицензию от ГТК, если система не будет содержать средств шифрования информации,

и дополнительно в ФАПСИ, если будут использоваться криптографические средства. При этом банк не получит лицензию, если в его уставе прямо не записано, что он может заниматься разработкой защищенных систем, поскольку подобная деятельность относится к сфере оказания услуг.

ЦБ РФ располагает достаточно объемным методическим документом по организации информационной защиты кредитно-финансовых учреждений, разработанным первоначально в виде концепции фирмой «Ланит» и согласованным с ГТК. Он описывает все необходимые шаги защиты банковской информации от угроз и пути их реализации.

Защищенная автоматизированная система с элементами криптозащиты, основанными на продукте «Верба», была реализована и прошла аттестацию. В соответствии с законодательством, системы подлежат аттестации, а их элементы — сертификации в Клиринговом центре МФД. Разработкой концепции системы занималась фирма «Амулет», не имеющая лицензии и не являющаяся специалистом в подобных вопросах. После экспертизы концепции системы в ГТК находившийся на стадии реализации проект пришлось коренным образом перерабатывать при помощи специализированных фирм, и МФД понес крупные дополнительные расходы.

Даже специализированные организации практически никогда в одиночку не работают над созданием защищенных информационных систем, поэтому банку заниматься разработкой защищенной АБС нет смысла, так как сложность подобных работ очень высока. Во Франции несколько банков на паях создали фирму, которая взяла на себя решение задачи создания защищенной АБС и разработала такую систему.

Если возникает потребность в подобной системе, можно пойти либо по такому же пути, либо, что более эффективно, создать организацию, которая смогла бы четко сформулировать требования по модификации существующих АБС для их реализации одной из фирм, имеющих лицензию на разработку систем информационной безопасности.

Для решения проблем информационной безопасности необходима тесная координация деятельности всех субъектов, которых касаются вопросы безопасности: пользователей, производителей средств безопасности и государственных органов, создающих нормативные документы и осуществляющих надзорные функции.

В соответствии с установленным законодательством, функции контроля и регулирования разработки, эксплуатации, сертификации программных и технических средств защиты информации от несанкционированного доступа, а также лицензирования предприятий на

право деятельности в области защиты информации возложены на Государственную техническую комиссию при Президенте Российской Федерации (далее — Гостехкомиссия).

Гостехкомиссией России разработана необходимая нормативная база в области защиты информации от несанкционированного доступа. Рассмотрим структуру основных руководящих документов.

1. «*Защита от несанкционированного доступа к информации. Термины и определения*» — устанавливает единый терминологический стандарт в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, являющийся обязательным для применения во всех видах документации.

2. «*Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации*» — описывает основные принципы, на которых базируется проблема защиты информации от несанкционированного доступа и ее отношение к общей проблеме безопасности информации. В концепции отражены следующие вопросы: определение несанкционированного доступа, основные принципы защиты, модель нарушителя в автоматизированных системах, основные способы несанкционированного доступа, основные направления обеспечения защиты, основные характеристики технических средств защиты, классификация автоматизированных систем, организация работ по защите. Указанная концепция предназначена для заказчиков, разработчиков и пользователей средств вычислительной техники и автоматизированных систем, основное назначение которых: обработка, хранение и передача защищаемой информации.

3. «*Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации*» — устанавливает классификацию контрольно-кассовых машин, автоматизированных кассовых систем, информационных технологий и требования по защите информации, связанной с налогообложением. В соответствии с этим документом устанавливается два класса контрольно-кассовых машин, автоматизированных кассовых систем и информационной техники. К первому классу относятся системы, обрабатывающие информацию о денежных оборотах на сумму до 350 минимальных размеров оплаты труда в сутки, а ко второму — на сумму свыше 350 минимальных размеров оплаты труда.

4. «*Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации*» — регламентирует требования

защищенности средств вычислительной техники от несанкционированного доступа, применяемые к общесистемным программным средствам и операционным системам. Здесь выделяются семь классов защищенности, которые подразделяются на четыре группы. Каждый класс содержит перечень необходимых для реализации механизмов защиты информации от несанкционированного доступа.

5. «*Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации*» — классифицирует автоматизированные системы в зависимости от наличия в них информации различного уровня конфиденциальности, уровней полномочий субъектов доступа, режимов обработки данных по девяти классам и оговаривает совокупность требований к каждому из них. В зависимости от особенностей обработки информации в автоматизированных системах классы делятся на три группы.

6. «*Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации*» — декларирует требования к различным классам межсетевых экранов. Всего выделяется пять классов защищенности межсетевых экранов. Классификация производится в зависимости от класса защищенности автоматизированных систем, для защиты которых используется межсетевой экран.

На основе руководящих документов и нормативной базы Гостехкомиссии России производится разработка, сертификация и использование средств защиты информации от несанкционированного доступа, а также лицензирование предприятий на право деятельности в области защиты информации на территории Российской Федерации.

14.4. Правовые аспекты защиты информации в сети Internet

О глобальной компьютерной сети, известной под английским названием Internet, часто говорят, что ее возникновение и непредсказуемо бурное развитие может стать крупнейшим событием в истории мировой цивилизации конца XX — начала XXI века. Не имеет смысла спорить, насколько соответствует оценка действительному положению вещей, но вряд ли еще к какому-либо аспекту развития информационных технологий было привлечено столь пристальное внимание не только специалистов, но и всевозрастающего числа людей самых разных профессий. К началу 2004 г. число пользователей Internet во всем мире исчислялось уже сотнями миллионов,

при этом ежедневно к сети подключаются десятки тысяч новых клиентов. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям во всем мире, друг с другом.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи удаленного интерактивного доступа к данным. Несколько лет назад были созданы оболочки, поддерживающие функции сетевого поиска и доступа к распределенным информационным ресурсам и электронным архивам.

Internet, служивший когда-то исключительно исследовательским и учебным группам, становится все более популярной средой и в деловом мире. Компании привлекает быстрота обмена информацией, низкая стоимость услуг глобальной связи, удобство проведения совместных работ, доступность программного обеспечения, уникальные по сути возможности работы с базами данных различного профиля, размещенными в Сети. Поэтому они рассматривают глобальную сеть как необходимое дополнение к своим собственным локальной сетям.

Фактически Internet состоит из множества локальных и глобальных сетей, принадлежащих различным компаниям и предприятиям, связанным между собой разнородными линиями связи. Internet можно представить себе в виде мозаики, сложенной из небольших сетей разной величины, которые активно взаимодействуют одна с другой, пересылая файлы, сообщения и т.п. При низкой стоимости услуг (часто это только фиксированная ежемесячная плата за используемые выделенные или телефонные линии) пользователи могут получить доступ к коммерческим и некоммерческим информационным службам США, Канады, Австралии и многих европейских стран. В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с материалов о новых научных открытиях и заканчивая прогнозом погоды на завтра.

Кроме того, Internet предоставляет уникальные возможности дешевой, надежной и конфиденциальной глобальной связи. Это оказывается очень удобным для фирм, имеющих свои филиалы по всему миру, транснациональных корпораций и структур управления. Обычно использование инфраструктуры Internet для международной связи обходится значительно дешевле прямой связи через спутниковый канал или через телефонные линии.

В настоящее время Internet испытывает период подъема во многом благодаря активной поддержке со стороны правительств США и европейских стран. Ежегодно в США выделяется около 1—2 млн

долларов на создание новых элементов сетевой инфраструктуры. Исследования в области сетевых коммуникаций финансируются также правительствами Великобритании, Швеции, Финляндии, Германии.

Однако всемирная электронная нервная система таит в себе скрытую угрозу собственникам, владельцам и пользователям. Так, в начале 1999 г. представители ФБР выступили с довольно неожиданным заявлением. По их утверждению, правительства по крайней мере 23 стран наращивают усилия в сфере промышленного шпионажа, направленные против американских компаний.

Необходимость принятия мер в сфере борьбы с компьютерной преступностью (КП) привела к созданию в 1997 г. специального подразделения — Управления по борьбе с преступлениями в сфере высоких технологий — в составе МВД России. Следует особо отметить, что Управление было создано на базе подразделения «Р», занимающегося поиском оперативной информации в радиоэлектронных и компьютерных информационных сетях.

Характерно, что тенденции, наблюдаемые в настоящий момент в России, начали прослеживаться в США и развитых странах Европы уже около десяти лет назад. Так, еще в 1993 г. *каждое четвертое из пяти расследованных ФБР компьютерных преступлений* было связано с несанкционированным доступом к компьютерам через сеть Internet. Анализ имеющихся данных показывает, что существует прямая зависимость между числом пользователей сети Internet и количеством инцидентов в области компьютерной безопасности, зарегистрированных CERT — Координационным центром быстрого реагирования на экстренные ситуации, связанные с компьютерами (рис. 14.2).

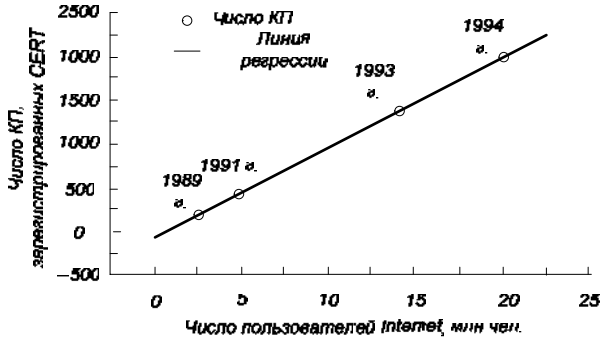


Рис. 14.2. **Зависимость количества компьютерных преступлений от числа пользователей Internet**

Движение компьютерной преступности в сеть приводит не только к количественным, но и к качественным изменениям в структуре преступности. Так, все более очевидны угрозы сетевой безопасности не от внешних нападений, а от внутренних. Именно собственные сотрудники организаций чаще всего используют незаконный выход в Internet в рабочее время, подключаются к модему в обход сетевого экрана, пользуются электронной почтой для рассылки личных сообщений. По данным независимых исследований сотрудниками совершается более 50% правонарушений в сфере информации. Западные фирмы всерьез озабочены вопросами ограничения доступа своих сотрудников в сеть Internet с рабочих мест, если это напрямую не связано с их служебными обязанностями.

Другой характерный пример — распространение компьютерных вирусов. Основную угрозу сегодня представляют *макровирусы*, на долю которых приходится *80% вирусных заражений*. Эпидемии, вызываемые этими вирусами, связаны с их распространением через *электронную почту* с вложенными файлами текстового процессора Word и электронной таблицы Excel. По вине электронной почты произошло в 1996 г. 23%, а в 1997 г. более 50% вирусных атак на корпоративные системы[1]. Алгоритмы вирусов становятся все более «зверскими» и могут приводить к потере всей информации и порче аппаратного обеспечения компьютера. Каждое нападение вируса на корпоративный сетевой узел обходится в среднем в 8366$. При этом на восстановление работоспособности узла тратится в среднем 44 часа и 21,7 человекодня работы. Исследователи отмечают, что с перемещением в сеть компьютерная преступность становится также все более организованной.

Чтобы проверить, насколько просто «воровать» с помощью глобальной сети Internet информацию, редакция журнала «Der Spiegel» пригласила в свой компьютерный центр специалистов небольшой фирмы «Information Management Gesellschaft» (IMG). IMG разрабатывает программы на базе ПО Notes американского концерна «Lotus». Он считается создателем одного из самых защищенных программных пакетов. И все же «Der Spiegel» назвал эту систему «стальным сейфом с задней стенкой из картона». Для компьютерного воровства программисту IMG оказалось достаточно одной дискеты, на которой была записана так называемая маска для рассылки электронной почты. Посмотрим, как он действовал. Программист посылал на чей-нибудь электронный Notes-адрес сообщение и через несколько минут получал ответ, в котором содержались электронные координаты адресата, в том числе его скрытый пароль.

---

[1] КомпьютерПресс, 1998, № 6 (102). — С. 124.

Послание программиста, кроме текста, содержало специально созданную спрятанную программу. Когда адресат начинал читать полученный (вполне банальный) текст, программа-шпион внедрялась в компьютер (этот принцип применяется вирусами в документах программ Word и Excel компании «Microcoft»). Затем ей оставалось дождаться момента, когда пользователь снова наберет пароль. Этот шифр фиксировался и отсылался программисту-испытателю. Он содержал не только индивидуальный пароль, но и идентификатор пакета Notes. После этого программа-шпион уничтожала саму себя. Когда программист познакомил представителей «Lotus» со своими несложными манипуляциями и предложил улучшить информационную защиту, шеф отдела «Lotus» по новым продуктам Алекс Морроу сказал, что «теперешняя архитектура персональных компьютеров вообще ненадежна. Это проблема всей отрасли, а не только "Lotus"»[1].

Согласно данным Агентства национальной безопасности, США сильнее других стран зависят от сетевой инфраструктуры — здесь сосредоточено более 40% вычислительных ресурсов мира (для сравнения, в России — менее 1%) и около 60% информационных ресурсов Internet.

Очевидно, что потери несут и другие страны, однако они, в отличие от США, пока не афишируют свои проблемы. В результате напрашивается логичный вопрос — возможна ли правовая защита в информационных сетях, в частности в Internet?

Internet мало исследован с точки зрения юридической специфики отношений, возникающих в связи с его существованием и практическим применением. Прежде всего предстоит решить *два вопроса принципиального характера.*

➢ *Вопрос первый* — о юридической природе самого Internet. Что это — субъект права, вступающий в различные отношения со своими клиентами, или объект правоотношений, природу которых еще только предстоит уточнить?

➢ *Вопрос второй* — о праве, применимом к этим правоотношениям. Если оно существует, то какая нормативная база его составляет, к какой системе и отрасли эти правовые нормы можно отнести? Если их до сих пор нет, то на чем основывалось развитие Internet до настоящего времени и что стоило бы предпринять в этом отношении в будущем?

Кроме того, можно выделить и множество частных проблем. Они либо уже возникали в процессе использования Internet, либо в ближайшее время неизбежно заявят о себе. В конечном итоге вопросы,

---

[1] *Чуищев И.М.* Может ли хакер защитить от компьютерных преступлений? // Юрист, 1999, № 2.

связанные с функционированием Internet, затрагивают огромные материальные, информационные, людские ресурсы и соответствующие объемы денежных средств. Все это не может остаться без внимания публичной власти, а значит, и без принятия нормативного регулирования в этой сфере.

Как уже отмечалось выше, Internet не является чем-то единым. Ни в одной стране мира не существует организационной структуры, выступающей в качестве его единоличного собственника или владельца.

Не является владельцем Internet и федеральное правительство США, практически прекратившее субсидирование даже отдельных отраслей сетей на территории государства. Не имеет прямого отношения к Internet и Министерство обороны США, владеющее собственной засекреченной компьютерной сетью.

Для обычного клиента представителем того, что называется Internet, выступает поставщик, предоставляющий ему канал связи с соответствующим программным обеспечением. В тех случаях, когда клиент совершает возмездную сделку во время сеанса связи в Internet (например, подписывается на заинтересовавший его журнал в электронной версии), он знает, что его контрагентом выступает не поставщик, а организация, предоставляющая указанную услугу (издательская фирма или редакция). По сути, такая сделка соответствует процессу обычной, некомпьютерной подписки на печатные издания.

Для фирмы-поставщика сетевых услуг представителем Internet являются специализированные компании, способные разместить информацию на своих компьютерах (называемых серверами) и сделать ее доступной для других пользователей сети (на условиях фирмы-производителя). Такая специализированная компания (владелец сервера) часто одновременно является и поставщиком сетевых услуг, но так бывает не всегда, и в этом случае владелец сервера входит в Internet на общих основаниях.

Для поставщика представителем Internet выступают более крупные сети, предоставляющие ему возможность соединения с ними. У каждой из таких сетей есть собственный владелец, но, конечно, по отдельности ни один из них все сети, объединяемые Internet, ни технически, ни юридически контролировать не может.

Представители наиболее крупных сетей Internet объединены в несколько организаций, называемых «сообществом Internet». Однако эти организации не являются органами управления Сетью. Они занимаются в первую очередь согласованием технических стандартов (обмена данными, соединений сетей и т.д.), а также регистрацией так называемых узловых компьютеров (соединенных между собой точками встречи) и доменных адресов или имен (идентификационных названий таких компьютеров). Само по себе это очень важно

для технического функционирования сети, но недостаточно для организации управления сетью в целом.

Все вышесказанное подтверждает, что у Internet невозможно выделить признаки, обычно характеризующие юридическое лицо. Internet не обладает организационным единством, не инкорпорирован ни в одной из стран мира и не создан как международная организация. Internet не имеет собственного обособленного имущества, так как используемые в нем материальные и информационные ресурсы принадлежат на праве собственности самым разным субъектам. Каналы связи принадлежат телекоммуникационным компаниям; компьютеры, производящие подключение к сети, — поставщикам; компьютеры клиентов — самим клиентам; техническое и программное обеспечение работы магистральных сетей — владельцам таких сетей; распространяемая на коммерческих условиях информация — ее производителям и прочим владельцам.

Не способен Internet иметь также какие-либо самостоятельные права и нести обязанности, так как за каждым возникающим при работе в Internet правоотношением стоит конкретный правоспособный субъект. Скажем, при подключении клиента к Сети его контрагентом выступает поставщик, при покупке через Сеть какого-либо товара (например, информации о рынке недвижимости либо самой недвижимости) — соответствующая организация-продавец, а при производстве по сделке через сеть — специализированная финансовая фирма (например, так называемый виртуальный банк).

Легко заметить, что во всех возникающих правоотношениях и взаимодействующие субъекты, и характер их ответственности совершенно различны. Иначе говоря, Internet однозначно не является ни зарегистрированной организацией, ни юридическим лицом вообще.

В настоящий момент мнение о «новизне» Internet как субъекта права представляется безосновательным. Поскольку Internet не является юридическим лицом, а организации, вступающие в вышеуказанные правоотношения, способны самостоятельно осуществлять свои права и нести обязанности, нет никакой необходимости искусственно соединять их в некий «множественный субъект».

Итак, Internet не является субъектом права, т.е. участником правоотношений. Но может быть, Internet — *объект права*, т.е. по его поводу возникают правоотношения?

Попытаемся рассмотреть приведенные выше примеры правоотношений по поводу работы в Internet с целью выявления их предметного основания. Подключение компьютера клиента к локальной сети поставщика осуществляется путем совершения нескольких юридически значимых действий, природа которых хорошо известна и не является чем-то исключительным. Это продажа программного (программы входа в Internet) и аппаратного обеспечения (модем);

аренда канала связи (можно провести аналогию с продажей машинного времени на ЭВМ или с использованием телефонной линии при междугороднем разговоре). Иначе говоря, используются договор купли-продажи, договор аренды, а также, в определенной степени, нормы об охране исключительных прав на предоставленное программное обеспечение (его нельзя переустановить еще на один компьютер без регистрации нового пользователя). В случае покупки какого-либо товара через Сеть также применяются достаточно проработанные понятия — договор купли-продажи, право собственности на продаваемый товар и т.д.

Другими словами, правовые отношения порождает не Internet как компьютерная сеть, а сами объекты, которые тем или иным образом связаны с такой сетью. Эти объекты либо уже хорошо известны (товары, выставленные на продажу по каталогу), либо менее исследованы с точки зрения юридической науки, но не представляют собой чего-то необычного (например, информация в том или ином виде или услуги по размещению рекламных страниц на серверах). Таким образом, Internet как компьютерная сеть не создает каких-либо новых объектов и товаров, а лишь предоставляет возможности для их создания, размещения и реализации между пользователями сети.

Что же касается отношений, которые возникают в связи с функционированием Internet как компьютерной сети, то, во-первых, они по сути не носят правового характера, а относятся к сфере технических стандартов и спецификаций. Во-вторых, если правовое регулирование все же применяется, его предметом становятся услуги, субъективные права и материальные объекты, принципиально не отличающиеся от существовавших до появления сети Internet.

В результате напрашивается единственно возможный вывод — сам по себе Internet как компьютерная сеть не является каким-либо объектом права. Вопросы правового регулирования Internet нельзя поставить в один ряд, например, с регулированием исключительных прав, права собственности или деликтной ответственности. Не может быть Internet в строгом смысле и объектом гражданского права, подобно имуществу, информации или правам на результаты интеллектуальной деятельности.

Может быть, раз Internet не является ни объектом, ни субъектом права, разговор о какой-либо юридической специфике его функционирования является вообще беспредметным?

К сожалению, все далеко не так просто. Специфика отношений, связанных с работой в сети Internet, безусловно, имеется. Его появление и развитие вносит много принципиально нового в характер взаимоотношений между людьми и организациями, связывающимися между собой через Сеть, также влечет возникновение новых субъектов деятельности — производителей сетевых услуг.

Сфера правоотношений, связанных с Internet, во многом пересекается со сферой регулирования авторского права. Размещение объектов, охраняемых авторским правом, в компьютерной сети не меняет принципиальных положений об их охране. Однако Internet предоставляет самые широкие возможности для фактически бесконтрольного воспроизведения и распространения таких объектов. Предполагается, что все пользователи сети, размещающие в ней информацию, содержащую перепечатки, изображения и другие зарегистрированные объекты исключительного права, обязаны предварительно получать согласие официальных владельцев на воспроизведение информации. Это, к сожалению, происходит далеко не всегда. Споры по поводу нарушений исключительных прав рассматриваются судами в общем порядке. Можно предположить, что число конфликтных ситуаций будет быстро увеличиваться[1].

Технические возможности Internet вызвали появление новых проблем и в области охраны авторских прав. Так, самым удобным и оперативным способом поиска нужной подписчику информации в «начальных страницах» являются специальные поисковые программы, автоматически просматривающие множество хранящихся на серверах документов и отображающие их на компьютер подписчика. Поскольку процесс поиска занимает доли секунды, получение согласия на копирование даже одной «начальной страницы» нереально.

Для теоретического решения проблемы копирования «начальных страниц» некоторые американские юристы предполагают использовать концепцию «подразумеваемой лицензии», которой владельцы «сетевых участков» располагают вследствие размещения в Сети их информации. Если доступ к такой информации или услуге обеспечивается за плату, то потребителю подробно сообщаются условия, на которых он может воспользоваться предлагаемой услугой (или информацией). Если же информация имеет общедоступный (бесплатный) характер, то потребитель вправе использовать ее, но не с целью извлечения прибыли. Критерии «некоммерческого» использования соответствуют общим началам охраны авторских прав и уточняются судебной практикой.

При анализе правоотношений в сети Internet нельзя не затронуть вопрос о правовой защите *безопасности передачи данных*, содержащих *конфиденциальную информацию*. Обеспечивает ли Internet сохранение тайны передачи информации через электронную почту; можно ли скопировать информацию, не предназначенную для передачи третьим лицам; защищена ли информация, передаваемая по сети, от компьютерных вирусов? Пока большинство экспертов дает

---

[1] *Богатырев Р.* Совершенно секретно, или Всемирная электронная нервная система // Мир ПК, 1998, № 4.

неутешительный ответ: Internet не обеспечивает желательного уровня безопасности.

Проблема кроется не столько в отсутствии необходимых технических возможностей, сколько в политике компаний, предоставляющих сетевые услуги. Можно установить соответствующие уровни защиты, для взлома которых потребуются такие затраты средств и рабочего времени, что они станут просто невыгодными для недобросовестного пользователя сети. Но при этом неизбежно возникнут неудобства у других пользователей (потребуется запоминать много дополнительной информации, например паролей; возможно, потребуется приобретать дополнительное оборудование), что снизит для многих из них привлекательность оказываемых услуг и побудит обратиться к конкурентам.

Основным методом обеспечения конфиденциальности является применение средств шифрования. Однако его применение непосредственно затрагивает интересы государственной безопасности государств. США, например, ограничивают пределы применения средств шифрования при передаче информации через сеть. Особо жестко регулируется (по существу, запрещается) передача и экспорт собственно шифровальных средств — компьютерных программ и аппаратного обеспечения. Возникает коллизия между интересами государства и частного пользователя.

С правовых позиций проблема имеет определенное теоретическое значение: соответствуют ли вводимые ограничения конституционным правам на свободу слова (в более узком значении — на передачу информации). Практическое значение решения проблемы заключается в обеспечении возможности охраны имущественных и иных законных интересов пользователей сети при совершении возмездных сделок[1].

Заслуживает упоминания еще один немаловажный аспект специфики правоотношений, возникающих по поводу Internet — вопрос доказывания фактов, имеющих юридическое значение.

Производимые пользователями сети операции с информацией (ввод данных, их перезапись, копирование и обработка) подобны составлению письменных документов и их рассылке. Однако, в отличие от письменных документов на бумажном носителе, информация, циркулирующая по сети, не может быть так же легко предъявлена для считывания и изучения. По крайней мере, требуется специальное оборудование (компьютер), чтобы указанную информацию можно было извлечь из сети для непосредственного восприятия и осмысления.

---

[1] *Богатырев Р.* Совершенно секретно, или Всемирная электронная нервная система // Мир ПК, 1998, № 4.

Вопрос о признании документов на электронных носителях в качестве аналога письменных доказательств неоднозначно решается в разных правовых системах. Развитие Internet хотя и усложняет решение вопроса об использовании циркулирующей в сети информации в качестве доказательств, однако, одновременно делает этот вопрос чрезвычайно актуальным.

Тема защиты авторских прав неизменно встает при всяком серьезном разговоре про Internet. По статистике, ежегодный прирост сетевого пиратства в Internet составляет 700%. Очевидно, что проблемы авторского права в Internet реально существуют и поэтому подлежат обсуждению.

Размещение объектов, охраняемых авторским правом, в компьютерной сети не меняет принципиальных положений об их охране, но сеть Internet предоставляет самые широкие возможности для фактически бесконтрольного воспроизведения и распространения таких объектов. Предполагается, что все пользователи сети, размещающие в ней информацию, содержащую перепечатки, изображения и другие зарегистрированные объекты исключительного права, обязаны предварительно получать согласие официальных владельцев на воспроизведение информации. Однако это делается далеко не всегда.

Какие законы защищают права интеллектуальной собственности в сети Internet? Имеющиеся нормативные правовые акты, затрагивающие отношения по поводу Internet, можно охарактеризовать следующим образом. Во-первых, кодифицированного законодательства по сети Internet нет по существу ни в одной стране мира. Во-вторых, практически отсутствует регулирование отношений по поводу Internet на межгосударственном уровне.

Закон РФ «Об авторском праве и смежных правах» гласит: «Если международным договором, в котором участвует Российская Федерация, установлены иные правила, чем те, которые содержатся в настоящем законе, то применяются правила международного договора». Поэтому ничто не обязывает Россию «бежать впереди всех» в этом вопросе.

Однако программное пиратство является далеко не единственным аспектом проблемы авторских прав в Internet. Не менее важен вопрос об использовании в Сети других объектов авторского права — литературных и музыкальных произведений, рисунков и фотографий. Если следовать букве закона, то большая часть всех авторских произведений, доступных в российском сегменте сети Internet, оказалась там на незаконных основаниях. То есть без письменного (или как-либо иначе зафиксированного) согласия авторов. И это относится не только к электронным библиотекам, создаваемым в

большинстве своем энтузиастами на общественных основаниях, но и вполне солидным, корпоративным контент-провайдерам, вроде «Россия онлайн» или «Гарант-Парк». Все они торгуют электронными версиями российских бумажных изданий, т.е. собраниями авторских текстов, не только не заручившись согласием авторов, но даже не ставя тех в известность о факте публикации. Очевидно, они полагают, что этого и не нужно делать, если имеется подписанный договор с тем изданием, веб-версией которого они торгуют. Однако в соответствии со ст. 30 или 31 действующего российского закона *авторское право делегированию не подлежит.*

Преследовать сетевых пиратов по закону ничуть не сложнее, чем обычных пиратов, торгующих контрафактной продукцией — не нужно ни слежки, ни рейдов ОМОНа: вещественные доказательства выставлены в Internet на всеобщее обозрение. Проблема состоит в том, что преследование пиратов противоречит интересам самих авторов, чьи номинальные права ущемлены. Российская практика, например, не знает ни одного случая возбуждения дела по факту незаконной публикации в Internet. В Америке число таких исков исчисляется по меньшей мере сотнями.

Контрольные вопросы и задания

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. Охарактеризуйте сущность понятий и терминов, используемых в законодательстве: «неправомерный доступ», «вредоносные программы», «уничтожение», «модификация», «блокирование информации».
12. Дайте определение *несанкционированного доступа* (НСД) к компьютерным ресурсам.
13. Какие меры необходимо применять для защиты компьютерной информации?

14. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
15. Назовите основные цели государства в области обеспечения информационной безопасности.
16. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
17. В тексте какого закона приведена классификация средств защиты информации?
18. Какой закон определяет понятие «официального документа»?
19. В тексте какого закона определены нормы, устанавливающие правовой режим информационных ресурсов?
20. Что в соответствии с законодательством понимается под защитой информации?
21. Поясните содержание термина «информационная безопасность».
22. Какой закон определяет понятие «электронный документ»?
23. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
24. Назовите основные положения Доктрины информационной безопасности Российской Федерации.
25. Что входит в понятие «профессиональная тайна»?
26. Что представляют собой технико-математические аспекты организационно-правового обеспечения информации?
27. Дайте определение электронного документа.
28. Как можно придать юридическую силу электронному документу?
29. Что представляет собой электронно-цифровая подпись?
30. Какие алгоритмы содержит система электронно-цифровой подписи?
31. Назовите основные условия, необходимые для введения ЭЦП в гражданский документооборот.
32. Каковы основные особенности правового режима электронного документа?
33. Назовите основные ограничения на использование электронных документов.
34. Какие условия необходимо выполнить с целью использования электронного документа в качестве доказательства?
35. Какие задачи в области законодательства следует отнести к первоочередным в области лицензирования и сертификации?
36. Можно ли использовать несертифицированные средства защиты информации?
37. Рассмотрите структуру основных руководящих документов Гостехкомиссии РФ в области защиты информации от несанкционированного доступа.
38. Какие основные особенности глобальной сети Internet с позиций субъекта и объекта права?
39. Как обеспечить безопасность и конфиденциальность информации в сети Internet?

Глава 15

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Защита информации требует 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.

15.1. 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 осуще-

ствляется 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, т.е. 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.

15.2. Защита информации от потери и разрушения

Рассмотрим моменты, связанные с защитой информации на персональном компьютере, не интегрированном в сеть.

Потеря информации при работе на ПК может произойти, 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 при-

чины 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: off-line, line-interactive и on-line. Устройства off-line — 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 on-line 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.

15.3. 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 Internet. 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 (НСД) 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, так как 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;
- комбинированные 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. Главный 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 обладают 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-аппарат-ные 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.

15.4. Защита информации от компьютерных вирусов

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 нежелатель-

ные 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 так же, как обычно. Внешне работа зараженной программы выглядит так же, как и незараженной.

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 ни 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: детекторы, 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.

Поэтому очевидно, 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 опе-

ративной 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 обра-

зом 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, они 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-ревизоры 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 ее 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 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 непонятно;
- 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.

15.5. 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 (MS DOS, Windows, Novell), а также разные сетевые протоколы (TCP/IP, VMS, MVS). 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].

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.

---

[1] Локальные вычислительные сети: Справочник: В 3-х кн. — Кн. 1. Принципы построения, архитектура, коммуникационные средства / Под ред. *С.В. Назарова*. — М.: Финансы и статистика, 1994.

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 подразделять на непреднамеренные, или случайные, и 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;
- компрометация информации;
- несанкционированный обмен информацией;
- отказ от информации;
- отказ в обслуживании;
- несанкционированное использование ресурсов сети;
- ошибочное использование ресурсов сети.

У*грозы 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 *виртуальных* сетях 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, предусмотренными МОС, 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, 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 сто-

роной. 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 аппаратные 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 пароли 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 то же 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:

1) времени и точки доступа;
2) наличия в БД определенных сведений;
3) текучести состояния СУБД;
4) полномочий пользователя;
5) предыстории обращения к данным.

В первом случае доступ к БД с каждого 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 права 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.

15.6. 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 которой 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.

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 Internet. 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 структуре 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 Internet, когда уже установлены брандмауэры, предназначенные для контроля за потоками информации между информационной системой и сетью Internet.

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 в рабочих станциях, подавляющее большинство которых (более 90%) работает под управлением MS DOS или Windows'9X 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 мень-

ше 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 обесеспечения 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 и задания

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. Дайте определение несанкционированного доступа (НСД) к компьютерным ресурсам.
5. Перечислите наиболее типичные способы несанкционированного доступа к информации.
6. Какие технические средства используются для защиты компьютерной информации?
7. Что такое *идентификация* и *аутентификация пользователя*?
8. Назовите основные субъекты идентификации и аутентификации.
9. С помощью каких программных средств обеспечивается защита информации от НСД на рабочей станции?
10. С помощью каких программных средств обеспечивается защита информации от НСД в информационной сети?
11. Дайте определение криптографических методов защиты информации.
12. Перечислите основные методы шифрования информации.
13. Поясните основные принципы работы криптографических программ.
14. Назовите программные средства восстановления удаленной либо испорченной компьютерной информации.
15. В каких случаях удаленный файл может быть полностью и успешно восстановлен?
16. Как обнаружить появление вируса на компьютере до периода его активизации?
17. Какие профилактические меры необходимо применять для защиты от вирусной атаки?
18. Каковы преимущества антивирусных программ-ревизоров перед антивирусными программами-детекторами?
19. Перечислите основные службы безопасности сети.
20. Какие механизмы безопасности сети считаются основными?
21. Назовите основные вопросы политики безопасности при построении защиты информации в корпоративной системе.
22. Назовите возможные способы защиты информации в корпоративной сети от шпионажа и диверсий.

Часть VI

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Глава 16

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

16.1. Понятие компьютерных преступлений и их классификация

Одним из негативных последствий информатизации общества является и появление так называемой компьютерной преступности. В литературе до настоящего времени ведется полемика о том, какие действия следует относить к разряду компьютерных преступлений. Сложность решения вопроса заключается также и в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк — от преступлений традиционного типа до требующих высокой математической и технической подготовки.

Появление на рынке в 1974 г. компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, ее сохранности и целостности. Организационные меры, а также программные и технические средства защиты информации оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства в работу компьютерных систем дала о себе знать в странах с развитой информационной инфраструктурой. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе и уголовно-правовые средства защиты. Так, например, в Уголовном кодексе Франции в 1992 г. система преступлений против собственности пополнилась специальной главой «О посягательствах на системы автоматизированной обработки данных». В ней предусмотрена ответственность за незаконный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы системы, или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Изучить и разработать

проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации, счел необходимым и Совет Европы.

Развивалась компьютерная преступность и в СССР. Так, одно из первых в нашей стране компьютерных преступлений, совершенное в 1979 г. в Вильнюсе, — хищение 78 584 рублей — удостоилось занесения в международный реестр подобных правонарушений. Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматизированной обработки информации. Определенным этапом стало принятие в 1992 г. Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных». Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таковых влечет уголовную ответственность. Однако соответствующих изменений в УК РФ внесено не было. В 1994 г. был принят Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, а в 1995 г. — Федеральный закон об информации, информатизации и защите информации. Логическим развитием правовой системы, создающей условия безопасности автоматизированной обработки информации, стало включение в УК РФ 1996 г. группы статей, предусматривающих основания уголовной ответственности за нарушения в сфере компьютерной информации.

Хотя действующее в большинстве стран уголовное законодательство является достаточно гибким, чтобы квалифицировать правонарушения этого типа, социальные и технические изменения создают все новые и новые проблемы. Поэтому некоторые из известных мировой практике компьютерных посягательств не подпадают под действие уголовного законодательства и в юридическом смысле не могут считаться преступными. Так, есть точка зрения, что компьютерных преступлений как преступлений специфических в юридическом смысле не существует и следует говорить лишь о компьютерных аспектах преступлений[1].

Вместе с тем специалисты в данной области исследований пришли к выводу, что к разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах[2], а орудием посягательства служит компьютер. По этому пути пошло и российское законодательство.

---

[1] *Батурин Ю.М.* Право и политика в компьютерном круге. — М.: Наука, 1987.

[2] *Россинская Е.Р.*, *Усов А.И.* Судебная компьютерно-техническая экспертиза. — М.: Право и закон, 2001.

Следует заметить, что с точки зрения уголовного законодательства охраняется *компьютерная информация*, которая определяется как информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Вместо термина компьютерная информация можно использовать и термин *машинная информация*, под которой подразумевается информация, запечатленная на машинном носителе, в памяти ЭВМ, системе ЭВМ или их сети. В качестве предмета или *орудия* преступления, согласно законодательству, может выступать компьютерная информация, компьютер, компьютерная система или компьютерная сеть.

При рассмотрении вопросов ***классификации компьютерных преступлений*** и их криминалистической характеристики целесообразно исходить из определения компьютерного преступления в широком смысле слова. В этом случае под *компьютерным преступлением* следует понимать предусмотренные законом общественно опасные деяния, совершаемые с использованием средств компьютерной техники. Правомерно также использовать термин «компьютерное преступление» в широком значении как социологическую категорию, а не как понятие уголовного права.

Классификация компьютерных преступлений может быть проведена по различным основаниям. Так, например, можно условно подразделить все компьютерные преступления на две большие категории: преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. При этом не принимаются во внимание так называемые «околокомпьютерные» преступления, связанные с нарушением авторских прав программистов, незаконным бизнесом на вычислительной технике, а также физическим уничтожением компьютеров и т.п.

Одна из наиболее общих классификаций была предложена в 1983 г. группой экспертов Организации экономического сотрудничества и развития. В соответствии с ней выделяются следующие криминологические группы компьютерных преступлений:

- экономические преступления;
- преступления против личных прав и частной сферы;
- преступления против государственных и общественных интересов.

Экономические компьютерные преступления являются наиболее распространенными. Они совершаются по корыстным мотивам и включают в себя компьютерное мошенничество, кражу программ («компьютерное пиратство»), кражу услуг и машинного времени, экономический шпионаж.

Компьютерными преступлениями против личных прав и частной сферы являются незаконный сбор данных о лице, разглашение частной информации (например, банковской или врачебной тайны), незаконное получение информации о расходах и т.д.

Компьютерные преступления против государственных и общественных интересов включают преступления, направленные против государственной и общественной безопасности, угрожающие обороноспособности государства, а также злоупотребления с автоматизированными системами голосования и т.п.

Подходить к классификации компьютерных преступлений наиболее оправдано с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены. Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

➢ *Несанкционированный доступ в корыстных целях к информации, хранящейся в компьютере или информационно-вычислительной сети.* Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются беззащитны против этого приема. Самый простой путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей.

Несанкционированный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы одного пользователя остаются открытыми, то другие пользователи могут получить доступ к не принадлежащим им частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

➢ *Разработка и распространение компьютерных вирусов.* Программы-вирусы обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

➢ *Ввод в программное обеспечение «логических бомб».* Это такие программы, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

➢ *Халатная небрежность при разработке, создании и эксплуатации программно-вычислительных комплексов компьютерных сетей, приведшая к тяжким последствиям.* Проблема небрежности в области компьютерной техники сродни вине по неосторожности при использовании любого другого вида техники.

Особенностью компьютерных систем является то, что абсолютно безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

➢ *Подделка и фальсификация компьютерной информации.* По-видимому, этот вид компьютерной преступности является одним из наиболее распространенных. Он является разновидностью несанкционированного доступа с той лишь разницей, что пользоваться им может сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К фальсификации информации можно отнести также подтасовку результатов выборов, референдумов и т.п. Если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели, в том числе корыстные.

➢ *Хищение программного обеспечения.* Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения программного обеспечения значительно более сложна. Значительная часть программного обеспечения в России распространяется путем кражи и обмена краденым.

➢ *Несанкционированное копирование, изменение или уничтожение информации.* При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

➢ *Несанкционированный просмотр или хищение информации из банков данных, баз данных и баз знаний.* В данном случае под базой данных

следует понимать форму представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Приходится констатировать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений, возрастанию их удельного веса в общей доле материальных потерь от различных видов преступлений. Потери же отдельно взятого государства в таких случаях могут достигать колоссальных размеров.

По данным МВД России, с 1992 по 1994 г. из банковских структур преступниками по фальшивым кредитным авизо и поддельным ордерам было похищено более 7 трлн руб. В связи с ростом подобных хищений еще в конце 1993 г. в ЦБ России и региональных РКЦ были установлены компьютерные системы защиты от фальшивых платежных документов. По данным ЦБ России за 2003 г., ежеквартально выявляется фиктивных платежей на десятки миллиардов рублей, которые преступники внедряют в сети подразделений банка.

16.2. Криминалистическая характеристика компьютерных преступлений

Компьютерные преступления имеют общую родовую криминалистическую характеристику, включающую сведения о способах совершения преступлений, лицах, их совершивших, данные о потерпевшей стороне, обстоятельствах преступлений и типичных следственных версиях.

На основе анализа конкретных уголовных дел по преступлениям, совершенным с использованием средств компьютерной техники, а также всестороннего изучения специальной литературы *выделяется свыше 20 основных способов совершения преступлений в сфере компьютерной информации и около 40 разновидностей*. Число их постоянно увеличивается по причине использования преступниками различных комбинаций и логической модификации алгоритмов. Такое поведение обусловлено как сложностью самих средств компьютерной техники, так и разнообразием и постоянным усложнением выполняемых информационных операций, многие из которых отражают движение материальных ценностей, финансовых и денежных средств, научно-технических разработок и т.д.

В то же время следует подчеркнуть, что практически все способы совершения преступлений в сфере компьютерной информации имеют свои индивидуальные, присущие только им признаки, по которым их можно распознать и классифицировать в отдельные

общие группы. Исследование показало, что в большинстве случаев преступниками используются различные количественные и качественные комбинации нескольких основных способов, имеющих достаточно простой алгоритм исполнения и хорошо известных отечественной юридической практике по традиционным видам преступлений. По мере их модификации и постоянного усложнения логических связей появляются все новые и новые способы, отличительной особенностью которых является уже наличие сложных алгоритмов действий преступника, которые от преступления к преступлению все более совершенствуются и модернизируются. Происходит как бы «естественный отбор».

Все способы совершения компьютерных преступлений классифицируются по *группам*:

1) перехват информации;
2) несанкционированный доступ к средствам компьютерной техники (СКТ);
3) манипуляция данными и управляющими командами;
4) комплексные методы.

Рассмотрим каждую из этих групп подробнее.

➢ ***Перехват информации***. *К первой группе* относятся способы совершения преступлений в сфере компьютерной информации, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата.

1. *Непосредственный* (*активный*) *перехват*. Осуществляется с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В связи с этим различают:

а) *форсированный перехват*, представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

б) *перехват символов* — выделение из текста, набираемого пользователем на клавиатуре терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;

в) *перехват сообщений* — несанкционированное подключение специального терминала к линии связи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

После подключения к каналу связи, вся информация записывается на физический носитель или переводится в человекочитаемую

форму посредством бытовой или специальной радиоэлектронной аппаратуры.

При этом программные средства позволяют в реальном времени просматривать передаваемую информацию, выбирая интересующие фрагменты практически незаметно для отправителя и получателя.

В качестве примера активного перехвата, но уже радиорелейной связи, можно привести действия преступной группы в Воронеже, собравшей из легально приобретенной аппаратуры сканеры, позволяющие считывать номера и персональные идентификационные коды абонентов сотовой сети в момент автоматического обмена этой информацией между зарегистрированной абонентской станцией и центральным процессором сотовой компании.

2. *Электромагнитный* (*пассивный*) *перехват.* Не все перехватывающие устройства требуют непосредственного подключения к системе, данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них. Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излучение, возникающее при функционировании многих средств компьютерной техники, включая и средства коммуникации.

Дело в том, что электронно-лучевая трубка, являющаяся центральным элементом компьютерного устройства для видеоотображения информации на экране (дисплее), излучает в окружающее пространство электромагнитные волны, несущие в себе определенную информацию, данные («электронный смог»). Волны, излучаемые этим прибором, примерно так же, как при телевизионном вещании, проникают сквозь различные физические преграды с некоторым коэффициентом ослабления, например через стекло оконных проемов и стены строений, а принимать их можно, как показывают данные многочисленных экспериментов, на расстоянии до 1000 м. Как только эти сигналы приняты соответствующей аппаратурой и переданы на другой компьютер (преступника), можно получить изображение, идентичное изображению, возникающему на мониторе «передающего» компьютера, для чего достаточно настроиться на его конкретную индивидуальную частоту.

Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 г. в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании PTT Вим-Ван-Эк шокировал специалистов тем, что с помощью разработанного им устройства из своего автомобиля, находящегося на улице, «снял» данные с экрана дисплея персонального компьютера, установленного на восьмом этаже здания, расположенного на расстоянии 100 м от автомобиля.

3. *Аудиоперехват* или *снятие информации по виброакустическому каналу.* Данный способ совершения преступления является наиболее опасным и достаточно распространенным.

Этот способ съема информации имеет две разновидности: *заходовую* (заносную) и *беззаходовую.* Первая заключается в установке инфитивного телефона (прослушивающего устройства) в аппаратуру средств обработки информации, в различные технические устройства, на проводные коммуникационные линии, а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте, с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств. Вторая — беззаходовая разновидность — наиболее опасная. Акустические и вибрационные датчики съема информации устанавливают на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать сигналы.

4. «*Уборка мусора*». Этот способ совершения преступления заключается в неправомочном использовании преступником отходов информационного процесса, оставленных пользователем после работы. Этот вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования СКТ. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы или же преступник записывает только небольшую часть своей информации при законном доступе, а затем считывает предыдущие записи, выбирая нужные ему сведения.

> Примечателен здесь случай из зарубежной практики, когда сотрудник службы безопасности коммерческого вычислительного центра, обслуживающего несколько крупных нефтяных компаний, находясь на своем посту в зале работы клиентов, обратил внимание на то, что у одного из клиентов, работавших на компьютере, перед тем как загорится световой индикатор записи его информации на магнитный диск, всегда сравнительно продолжительное время горит индикатор считывания информации. Проведенной по данному факту доследственной проверкой было установлено, что клиент занимался промышленным шпионажем.

В некоторых случаях преступником могут осуществляться действия, направленные на восстановление и последующий анализ данных, содержащихся в стертых файлах.

➢ ***Несанкционированный доступ к средствам компьютерной техники.*** *Ко второй группе* способов совершения преступлений в сфере компьютерной информации относятся действия преступников, на-

правленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся следующие:

1. «*За дураком*». Этот способ часто используется преступниками для проникновения в запретные зоны — электронные системы. Он заключается в использовании преступником из числа внутренних пользователей путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент, когда сотрудник, отвечающий за работу средства компьютерной техники, выбранной в качестве предмета посягательства, кратковременно покидает свое рабочее место, оставляя терминал или персональный компьютер в активном режиме.

2. «*За хвост*». Этот способ съема информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе.

3. «*Компьютерный абордаж*». Данный способ совершения преступления в сфере компьютерной информации осуществляется преступником путем случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата. После успешного соединения с вызываемым абонентом и появления в головном телефоне преступника специфического позывного сигнала, свидетельствующего о наличии модемного входа/выхода на вызываемом абонентном номере, преступником осуществляется механическое подключение собственного модема и персонального компьютера к каналу телефонной связи. После чего преступником производится подбор кода доступа к компьютерной системе жертвы (если таковой вообще имеется) или используется заранее добытый код.

Стоит обратить внимание на то, что существует множество программ-«взломщиков». Эти программы работают по принципу простого перебора символов, которые возможно ввести через клавиатуру персонального компьютера.

По существу, «компьютерный абордаж» является подготовительной стадией преступления в сфере компьютерной информации.

4. *Неспешный выбор.* Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может не спеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства. Обычно такой способ используется преступником в отношении тех,

кто не уделяют должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы.

5. «*Брешь*». В отличие от «неспешного выбора», когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется их конкретизация: определяются участки, имеющие ошибки или неудачную логику программного построения; выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены. Последнее возможно лишь высококвалифицированным программистом или лицом, непосредственно разработавшим данную программу.

«*Люк*». Данный способ является логическим продолжением предыдущего. В этом случае в найденной «бреши» программа «разрывается» и туда дополнительно преступник вводит одну или несколько команд. Такой «люк» «открывается» по мере необходимости, а включенные команды автоматически выполняются. При совершении компьютерного преступления данным способом следует обратить внимание на то, что при этом всегда преступником осуществляется предметная модификация (изменение) определенных средств компьютерной техники.

6. «*Маскарад*». Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Самый простейший путь к проникновению в такие системы — получить коды и другие идентифицирующие шифры законных пользователей.

7. «*Мистификация*». Иногда по аналогии с ошибочными телефонными звонками случается так, что пользователь с терминала или персонального компьютера подключается к чьей-либо системе, будучи абсолютно уверенным в том, что он работает с нужным ему абонентом. Этим фактом и пользуется преступник, формируя правдоподобные ответы на запросы владельца информационной системы, к которой произошло фактическое подключение, и поддерживая это заблуждение в течение некоторого периода времени, получая при этом требуемую информацию, например коды доступа или отклик на пароль.

8. «*Аварийный*». В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы данной программы заключается в том, что она позволяет достаточно быстро обойти все имеющиеся средства защиты информации и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным.

Такие программы являются универсальным «ключом» в руках преступника.

9. «*Склад без стен*». Несанкционированный доступ к компьютерной системе в этом случае осуществляется преступником путем использования системной поломки, в результате которой возникает частичное или полное нарушение нормального режима функционирования систем защиты данных. Например, если нарушается система иерархичного либо категорийного доступа к информации, у преступника появляется возможность получить доступ к той категории информации, в получении которой ему ранее было отказано.

➢ ***Манипуляция данными и управляющими командами.*** *К третьей группе* способов совершения преступлений в сфере компьютерной информации относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники.

Рассмотрим наиболее широко используемые преступниками способы совершения преступлений из третьей группы:

1. *Подмена данных* — наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в данном случае направлены на изменение или введение новых данных, которое осуществляется, как правило, при вводе-выводе информации. В частности, данный способ совершения преступления применяется для приписывания счету «чужой» истории, т.е. модификации данных в автоматизированной системе банковских операций, приводящей к появлению в системе сумм, которые реально на данный счет не зачислялись.

Например, таким способом экономистом Брестского областного производственного объединения К. были совершены хищения денежных средств. Как свидетельствуют материалы уголовного дела, будучи экономистом по учету заработной платы и отвечая за достоверность документов и сдачу их в ОАСУ, К. на протяжении ряда лет вносила в документы начисления заработной платы подложные документы, в результате чего заработная плата начислялась на счета вымышленных лиц и переводилась в сберкассы г. Бреста на специально открытые ею счета: на имя матери К., сестры, знакомого.

Частным вариантом способа подмены данных является способ *подмены кода*. Он заключается в изменении кода данных, например, бухгалтерского учета.

2. «*Троянский конь*». Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем принимающей «троянского коня» программы, с одновременным

сохранением прежней работоспособности. По существу, «троянский конь» — это модернизация уже рассмотренного нами способа «люк» с той лишь разницей, что он «открывается» не при помощи непосредственных действий самого преступника («вручную»), а автоматически — с использованием специально подготовленной для этих целей программы без дальнейшего непосредственного участия самого преступника.

Из зарубежной практики известен факт использования «троянского коня» одним американским программистом. Он вставил в программное обеспечение персонального компьютера по месту своей работы команды, которые не выводили на печать для отчета определенные поступления денежных средств. Эти суммы особым образом шифровались и циркулировали только в информационной среде компьютера. Похитив бланки выдачи денег, преступник заполнял их с указанием своего шифра, а затем проставлял в них определенные суммы денег, соответствующие операции по их выдаче также не выводились на печать и, следовательно, не могли подвергнуться документальной ревизии.

Справедливости ради следует отметить, что «троянский конь» иногда бывает и полезным. Вот пример того, как «троянский конь» помог обнаружить нарушение авторских прав.

Две американские фирмы разрабатывали программное обеспечение для тестирования компьютеров в условиях сильной нагрузки на них. Первая фирма предложила второй заключить соглашение. Вторая фирма отказалась. Вскоре после этого маленькая независимая компания купила лицензию на программу первой, более удачливой фирмы. И вдруг эта фирма получает электронное письмо из Internet о том, что ее программа запущена в сети второй фирмы-конкурента — и ее исследуют. Естественно, первая фирма возбудила уголовное дело против конкурента.

История эта показательна потому, что письмо было послано самой программой тестирования загрузки компьютеров в ответ на некоторые действия с ней. По-видимому, в условиях Internet это более действенный способ защиты авторских прав, чем электронные ключи и ключевые дискеты[1].

2.1. «*Троянская матрешка*». Является разновидностью «троянского коня». Особенность этого способа заключается в том, что во фрагмент программы потерпевшей стороны вставляются не команды, собственно выполняющие незаконные операции, а команды, формирующие эти команды, и после выполнения своей функции, т.е. когда уже будет автоматически на программном уровне создан «троянский конь», самоуничтожающиеся. Иначе говоря, это про-

[1] *Чупщев И.М.* Может ли хакер защитить от компьютерных преступлений? // Юрист, 1999, № 2.

граммные модули-фрагменты, которые создают «троянского коня» и самоликвидируются на программном уровне по окончании исполнения своей задачи.

2.2. «*Троянский червь*». Еще одна разновидность способа «троянский конь». Данный способ совершения преступления характеризуется тем, что в алгоритм работы программы, используемой в качестве орудия совершения преступления, наряду с ее основными функциями, уже рассмотренными нами выше, закладывается алгоритм действий, осуществляющих саморазмножение, программное автоматическое воспроизводство «троянского коня». «Программы-черви» автоматически копируют себя в памяти одного или нескольких компьютеров (при наличии компьютерной сети) независимо от других программ. При этом используется тактика компьютерных вирусов, которые будут рассмотрены нами далее.

3. «*Салями*». Такой способ совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях. Данный способ основан на методике проведения операций перебрасывания на подставной счет мелочи — результата округления, которая на профессиональном бухгалтерском языке называется «салями». Мелочный преступный расчет в этом случае построен на том, что ЭВМ в секунду совершает миллионы операций. В то время как высококвалифицированный бухгалтер за целый день может выполнить лишь до двух тысяч таких операций. На этом строится и тактика использования «троянского коня», основанная на том, что отчисляемые суммы столь малы, что их потери практически незаметны, а незаконное накопление суммы осуществляется за счет совершения большого количества операций.

4. «*Логическая бомба*». Иногда из тактических соображений хищения удобнее всего совершать при стечении каких-либо обстоятельств, которые обязательно должны наступить. В этих случаях преступниками используется рассматриваемый способ совершения преступления, основанный на тайном внесении изменений в программу потерпевшей стороны набора команд, которые должны сработать (или срабатывать каждый раз) при наступлении определенных обстоятельств через какое-либо время. Далее включается алгоритм программ «троянского коня».

«*Временная бомба*». Является разновидностью «логической бомбы», которая срабатывает по достижении определенного момента времени. Например, в США получили широкое распространение преступления, в которых преступником используется способ «временной бомбы» для хищения денежных средств. Механизм применения этого способа заключается в следующем. Преступником, находящимся в стране «А», посредством заранее введенной в банк данных автоматизированной системы межбанковских электронных

операций программы — «временной бомбы» — в стране «Б», похищаются деньги в определенный заданный момент времени при стечении благоприятных обстоятельств. Все манипуляции с ценными данными, а также начало осуществления бухгалтерских операций с ними производятся и контролируются программой. Преступнику лишь остается в определенный момент времени снять деньги, поступившие на заранее открытый счет. Аналогично происходят и преступления, направленные на разрушение определенных данных и информации в компьютерной системе для различных преступных целей.

5. *Компьютерные вирусы.* Наиболее распространенный способ совершения компьютерных преступлений, с которым сталкиваются пользователи персональных компьютеров, — это компьютерные вирусы. Последние являются особого типа вредоносными программами, доставляющими пользователям и обслуживающему ПК персоналу немало неприятностей[1]. В самом общем виде этот способ совершения преступлений в сфере компьютерной информации является ничем иным, как логической модернизацией способа «троянский конь», выполняющего алгоритм, например, типа «сотри все данные этой программы, перейди в следующую и сделай то же самое».

Компьютерным вирусом называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы.

С программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), искажение и стирание (уничтожение) данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

Очевидна аналогия понятий компьютерного и биологического вирусов. Однако не всякая могущая саморазмножаться программа является компьютерным вирусом. *Вирусы всегда наносят ущерб* — препятствуют нормальной работе ПК, разрушают файловую структуру и т.д., поэтому их относят к разряду так называемых вредоносных программ.

Исторически появление компьютерных вирусов связано с идеей создания самовоспроизводящихся механизмов, в частности программ, которая возникла в 1950-х гг. Дж. фон Нейман еще в 1951 г. предложил метод создания таких механизмов, и его соображения получили дальнейшее развитие в работах других исследователей. Пер-

---

[1] *Безруков Н.Н.* Компьютерные вирусы. — М.: Наука, 1991.

выми 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.

Создатели вирусов сосредоточили свои усилия в области ПК вследствие их массовости и практически полного отсутствия эффективных средств защиты как на аппаратном уровне, так и на уровне ОС. Среди побудительных мотивов, движущих авторами вирусов, можно назвать следующие:

- стремление «насолить» кому-либо;
- неестественная потребность в совершении преступлений;
- желание самоутвердиться, озорство и одновременно недопонимание всех последствий распространения вируса;
- невозможность использовать свои знания в конструктивном русле (это в большей степени экономическая проблема);
- уверенность в полной безнаказанности (в ряде стран отсутствуют нормы правовой ответственности за создание и распространение вирусов).

Основными каналами проникновения вирусов в персональный компьютер являются накопители на сменных носителях информации и средства сетевой коммуникации, в частности сеть Internet.

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 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 центра университета и личных дискет студентов. К февралю 1989 г. в США этим вирусом было поражено около 4 тыс. ПК.

В дальнейшем количество вирусов и число зараженных ими компьютеров стало лавинообразно увеличиваться, что потребовало принятия срочных мер как технического, так и организационного и юридического характера. Появились различные антивирусные средства, вследствие чего ситуация стала напоминать гонку вооружений и средств защиты от них. Определенный эффект был достигнут в результате принятия рядом развитых стран законодательных актов о компьютерных преступлениях, среди которых были и статьи, касающиеся создания и распространения компьютерных вирусов.

В настоящее время в мире насчитывается более 50 тыс. вирусов, включая *штаммы*, т.е. разновидности вирусов одного типа. Вирусы не признают границ, поэтому большинство из них курсирует и по России. Более того, проявилась тенденция увеличения числа вирусов, разработанных отечественными программистами. Если ситуация не изменится, то в будущем Россия сможет претендовать на роль лидера в области создания вирусов.

Классификация вирусов. *Жизненный цикл компьютерных вирусов*, как правило, включает следующие фазы:

1) латентный период, в течение которого вирусом никаких действий не предпринимается;
2) инкубационный период, в пределах которого вирус только размножается;
3) активный период, в течение которого наряду с размножением выполняются несанкционированные действия, заложенные в алгоритме вируса.

Первые две фазы служат для того, чтобы скрыть источник вируса, канал его проникновения и инфицировать как можно больше файлов до выявления вируса. Длительность этих фаз может определяться предусмотренным в алгоритме временным интервалом, наступлением какого-либо события в системе, наличием определенной конфигурации аппаратных средств ПК (в частности, наличием НЖМД) и т.д.

Компьютерные *вирусы классифицируются в соответствии со следующими признаками*:

- среда обитания;
- способ заражения среды обитания;
- способ активизации;
- способ проявления (деструктивные действия или вызываемые эффекты);
- способ маскировки.

Вирусы могут внедряться только в те программы, которые, в свою очередь, могут содержаться или в файлах, или в некоторых компонентах системной области диска, участвующих в процессе загрузки операционной системы.

В соответствии со средой обитания различают:

- файловые вирусы, инфицирующие исполняемые файлы;
- загрузочные вирусы, заражающие компоненты системной области, используемые при загрузке ОС;
- файлово-загрузочные вирусы, интегрирующие черты первых двух групп.

Файловые вирусы могут инфицировать:

- позиционно-независимые перемещаемые машинные программы, находящиеся в COM-файлах;

- позиционно-зависимые перемещаемые машинные программы, размещаемые в EXE-файлах;
- драйверы устройств (SYS- и BIN-файлы);
- файлы с компонентами DOS;
- объектные модули (OBJ-файлы);
- файлы с программами на языках программирования (в расчете на компиляцию этих программ);
- командные файлы (BAT-файлы);
- объектные и символические библиотеки (LIB- и др. файлы);
- оверлейные файлы (OVL-, PIF- и др. файлы).

Наиболее часто файловые вирусы способны внедряться в COM- и (или) EXE-файлы.

Загрузочные вирусы могут заражать:

- загрузочный сектор на дискетах;
- загрузочный сектор системного логического диска, созданного на винчестере;
- внесистемный загрузчик на жестком диске.

Загрузочные вирусы распространяются на дискетах в расчете на то, что с них будет осуществлена попытка загрузиться, что происходит не так часто. У файловых вирусов инфицирующая способность выше.

Файлово-загрузочные вирусы обладают еще большей инфицирующей способностью, так как могут распространяться как в программных файлах, так и на дискетах с данными.

Способы заражения среды обитания зависят от типа последней. Зараженная вирусом среда называется вирусоносителем. При имплантации тело файлового вируса может размещаться:

- в конце файла;
- в начале файла;
- в середине файла;
- в хвостовой (свободной) части последнего кластера, занимаемого файлом.

Наиболее легко реализуется внедрение вируса в конец COM-файла. При получении управления вирус выбирает файл-жертву и модифицирует его следующим образом:

1) дописывает к файлу собственную копию (тело вируса);
2) сохраняет в этой копии оригинальное начало файла;
3) заменяет оригинальное начало файла на команду передачи управления на тело вируса.

При запуске инфицированной описанным способом программы первоначально инициируется выполнение тела вируса, в результате чего:

1) восстанавливается оригинальное начало программы (но не в файле, а в памяти!);
2) возможно, отыскивается и заражается очередная жертва;

3) возможно, осуществляются несанкционированные пользователем действия;
4) производится передача управления на начало программы-вирусоносителя, в результате чего она выполняется обычным образом.

Имплантация вируса в начало COM-файла производится иначе: создается новый файл, являющийся объединением тела вируса и содержимого оригинального файла. *Два описанных способа внедрения вируса ведут к увеличению длины оригинального файла.*

Имплантация вируса в середину файла наиболее сложна и специализирована. Сложность состоит в том, что в этом случае вирус должен «знать» структуру файла-жертвы (например, COMMAND.COM), чтобы можно было внедриться, в частности, в область стека. Описанный *способ имплантации не ведет к увеличению длины файла.*

Проявлением (деструктивными действиями) вирусов могут быть:

- влияние на работу ПК;
- искажение программных файлов;
- искажение файлов с данными;
- форматирование диска или его части;
- замена информации на диске или его части;
- искажение системного или несистемного загрузчика диска;
- разрушение связности файлов путем искажения таблицы FAT;
- искажение данных в CMOS-памяти.

Большую часть вирусов первой группы, вызывающих визуальные или звуковые эффекты, неформально называют «иллюзионистами». Другие вирусы этой же группы могут замедлять работу ПК или препятствовать нормальной работе пользователя, модифицируя и блокируя функции выполняемых программ, а также операционной системы. Вирусы всех остальных групп часто называют «вандалами» из-за наносимого ими, как правило, непоправимого ущерба.

В соответствии со *способами маскировки* различают:

- немаскирующиеся вирусы;
- самошифрующиеся вирусы;
- стелс-вирусы.

Авторы первых вирусов уделяли особое внимание механизмам размножения (репликации) с внедрением тел в другие программы. Маскировка же от антивирусных средств не осуществлялась. Такие вирусы называются немаскирующимися.

В связи с появлением антивирусных средств разработчики вирусов сосредоточили усилия на обеспечении маскировки своих изделий. Сначала была реализована идея самошифрования вируса. При этом лишь небольшая его часть является доступной для осмыслен-

ного чтения, а остальная расшифровывается непосредственно перед началом работы вируса. Такой подход затрудняет как обнаружение вируса, так и анализ его тела специалистами.

Появились также стелс-вирусы, названные по аналогии с широкомасштабным проектом по созданию самолетов-невидимок.

Методы маскировки, используемые стелс-вирусами, носят комплексный характер и могут быть условно разделены на две категории:

1) маскировка наличия вируса в программе-вирусоносителе;
2) маскировка присутствия резидентного вируса в ОЗУ.

К первой категории относятся:

1) автомодификация тела вируса;
2) реализация эффекта удаления тела вируса из вирусоносителя при чтении последнего с диска, в частности, отладчиком (это осуществляется путем перехвата прерывания, конечно, в случае наличия резидентного вируса в ОЗУ);
3) имплантация тела вируса в файл без увеличения его размера;
4) эффект неизменности длины инфицированного файла (осуществляется аналогично п. 2);
5) сохранение неизменным оригинального начала программных файлов.

Например, при чтении каталога средствами DOS резидентный вирус может перехватить соответствующее прерывание и искусственно уменьшить длину файла. Конечно реальная длина файла не меняется, но пользователю выдаются сведения, маскирующие ее увеличение. Работая же с каталогами непосредственно (в обход средств DOS), можно получить истинную информацию о характеристиках файла. Такие возможности предоставляет, в частности, оболочка Norton Commander.

Ко второй категории методов маскировки можно отнести:

1) занесение тела вируса в специальную зону резидентных модулей DOS, в хвостовые части кластеров, в CMOS-память, видеопамять и т.п.;
2) модификацию списка несистемного загрузчика, о чем уже говорилось;
3) манипулирование обработчиками прерываний, в частности специальные методы их подмены, с целью обойти резидентные антивирусные средства;
4) корректировку общего объема ОЗУ.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается резидентно (т.е. до перезагрузки DOS) в памяти компьютера и время от времени заражает программы и выполняет вредные действия на компьютере.

При повседневной работе *пользователь в состоянии обнаружить вирус по его симптомам*. Естественно, что симптомы вируса непосредственно определяются реализованными в нем способами проявления, а также другими характеристиками вируса. В качестве симптомов вирусов выделяют следующие:

- увеличение числа файлов на диске;
- уменьшение объема свободной оперативной памяти;
- изменения времени и даты создания файла;
- увеличение размера программного файла;
- появление на диске зарегистрированных дефектных кластеров;
- ненормальная работа программы;
- замедление работы программы;
- загорание лампочки дисковода в то время, когда к диску не должны происходить обращения;
- заметное возрастание времени доступа к жесткому диску;
- сбои в работе операционной системы, в частности ее зависание;
- невозможность загрузки операционной системы;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов).

Наряду с компьютерными вирусами существуют и другие опасные программы, например так называемые «черви», формально именуемые *репликаторами*. Их основная особенность состоит в способности к размножению без внедрения в другие программы. Репликаторы создаются с целью распространения по узлам вычислительной сети и могут иметь начинку, состоящую, в частности, из вирусов. В этом отношении можно провести аналогию между червем и шариковой бомбой.

Примером репликатора является программа Christmas Tree, рисующая на экране дисплея рождественскую елку, а затем рассылающая свои копии по всем адресам, зарегистрированным средствами электронной почты.

Характерным примером преступления с использованием компьютерного вируса является уголовное дело, возбужденное ГУВД Свердловской области по факту распространения гр. Флягиным программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию информации и нарушению работы ЭВМ. Флягин, используя свой домашний персональный компьютер «Packard Bell 486-CX-33», модем «US-Robotics» и телефон, зарегистрированный на Екатеринбургской ПС, а также установленную им специализированную компьютерную программу «Maxi'mus 3.00» (BBS — Bulletin Board Sistem — электронную доску объявлений), обеспечивающую работу компьютера с удаленными пользователями через телефонную сеть, распространял программы для ЭВМ, заведомо приводящие к несанкционированному унич-

тожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Сами же «вирусы» он переписывал с помощью сети Internet с одного из серверов в Бразилии.

6. «*Асинхронная атака*». Такой способ совершения преступления очень сложен и требует хорошего знания операционной системы. Операционная система — это комплекс программных средств, обеспечивающих управление информационными процессами при функционировании компьютерной системы. Столь сложный программный продукт практически ни при каких условиях невозможно проверить на предмет достоверности работы и логической завершенности. Иначе говоря, особенности функционирования операционной системы при всех условиях остаются неизвестными. Этим и пользуются преступники при организации «асинхронных атак».

Используя асинхронную природу функционирования операционной системы, преступник заставляет последнюю работать при ложных условиях, вследствие чего управление обработкой информации частично или полностью нарушается. Если преступник, совершающий «асинхронную атаку», достаточно искусен, то он может использовать данную ситуацию, чтобы внести изменения в операционную систему или направить ее функционирование на выполнение своих корыстных целей, причем вне операционной системы эти изменения будут не заметны.

7. *Моделирование.* Для совершения преступлений в сфере компьютерной информации все более характерным становится использование преступником способа компьютерного моделирования: моделирования поведения устройства или системы с помощью программного обеспечения. Моделируются процессы, в которые преступники хотят вмешаться, и планируемые способы совершения преступления. Например, в последнее время преступниками с целью ухода от налогообложения все чаще используется так называемая «черная» или «двойная» бухгалтерия, основанная на существовании двух одновременно работающих программ автоматизированного бухгалтерского учета с взаимопересекающимися контрольными данными. В данном случае одна из них функционирует в легальном режиме, а другая — в нелегальном для проведения незаконных теневых бухгалтерских операций. Иногда одновременно с этими программами существует и третья, используемая только одним лицом, входящим в состав преступных групп и сообществ, выполняющим роль бухгалтера по ведению общественной кассы преступной группировки.

7.1. *Реверсивная модель* — разновидность способа моделирования, заключается в следующем: создается модель конкретной системы, на которую планируется совершить нападение. В нее вводятся ре-

альные исходные данные и учитываются планируемые действия. Затем исходя из полученных данных подбираются максимально приближенные к действительности желаемые результаты. После чего модель совершения преступных действий «прогоняется» назад, к исходной точке, и преступнику становится ясно, какие манипуляции с входными-выходными данными нужно совершить, чтобы достичь желаемого корыстного результата. Обычно «прокручивание» модели вперед-назад осуществляется преступником многократно, чтобы выявить возникающие ошибки и просчеты в механизме планируемых преступных действий. Таким образом, осуществляется оптимизации действий при проведении криминальных «операций» и минимизируется возможный при этом риск их «провала».

7.2. «*Воздушный змей*». Механизм совершения хищения денежных средств заключается в следующем. В двух или нескольких банках открываются счета на некоторые несуществующие суммы. Далее деньги переводятся из одного банка в другой и обратно с постепенным увеличением сумм. До того как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходит извещение в данный банк о том, что общая сумма покрывает требование о первом переводе. Этот цикл многократно повторяется («воздушный змей» поднимается все выше и выше) до тех пор, пока на нужном счете не оказывается достаточная сумма денег (фактически она постоянно «перескакивает» с одного счета на другой, как бы «парит в воздухе», постоянно увеличиваясь в размерах). Когда сумма достигает требуемого значения, деньги оперативно снимаются с закрытием счетов и впоследствии отмываются (легализуются). Обычно, как показывает практика, в подобные преступные операции преступниками включается большое число банков.

7.3 «*Ловушка на живца*» («*подсадная утка*») — еще одна разновидность способа моделирования. Преступником создается специальная программа, которая затем записывается на физический носитель и под любым предлогом вручается или подкидывается потерпевшей стороне с расчетом на то, что ее по каким-либо причинам заинтересует данная программа и она постарается ознакомиться с ней. Алгоритм программы построен таким образом, что при ее работе в определенный момент времени автоматически моделируется системная поломка компьютерной системы, на которой был запущен данный программный продукт с целью проверки его качества и работоспособности. Затем указанная программа записывает данные и информацию, которые могут заинтересовать преступника. После того как программа выполнила заданные ей функции, она изымается у потерпевшей стороны с использованием различных способов.

8. *Копирование* (*тиражирование*). Этот способ совершения преступления заключается в действиях преступника, направленных на

незаконное копирование (тиражирование) программных средств компьютерной техники, а также типологий интегральных микросхем. Копирование осуществляется преступником посредством воспроизведения данных с сохранением исходной информации на любом материальном носителе.

Существуют две разновидности применения преступником указанного способа. В первом случае копирование осуществляется посредством законного (санкционированного) доступа к средствам компьютерной техники, во втором — посредством несанкционированного доступа с использованием способов, рассмотренных нами выше. В последнем случае будет иметь место применение комплексного метода совершения преступления (совокупность двух и более способов совершения преступления), которые будут рассмотрены нами в следующей, четвертой группе.

9. *Преодоление программных средств защиты.* Этот способ является вспомогательным и предназначен для подготовки совершения компьютерного преступления способами, рассмотренными выше. Он заключается в действиях преступника, направленных на умышленное преодоление программных средств защиты компьютерной техники и имеет несколько разновидностей.

9.1. *Незаконное создание копии ключевой дискеты* осуществляется преступником путем электромагнитного переноса всей структуры и информации, расположенных на ключевой дискете-оригинале, защищенной от копирования программными средствами, на дискету-копию, в результате чего аутентификационная часть системы защиты воспринимает копию ключевой дискеты как оригинал.

9.2. *Модификация кода системы защиты* заключается в модификации (изменении) кода модуля системы защиты, выполняющего следующие функции: 1) проверку ключевой дискеты; 2) корректировку счетчика установок на жесткий магнитный диск (винчестер), защищенного от копирования программного средства с ключевой дискеты; 3) проверку санкционированности запуска защищенного информационного ресурса.

Обычно модификация сводится к простому обходу кода модуля, выполняющего перечисленные выше функции. В некоторых случаях модуль подвергается существенным изменениям, позволяющим обойти проверки систем защиты. Основная задача заключается в определении логики работы модуля. Последующее же внесение изменений в него остается «делом техники» и не представляет особого труда для преступника, разгадавшего логику построения защиты.

9.3. *Моделирование обращений к ключевой дискете.* Многие программные средства защиты информации логически используют не прямую, как это принято, работу с контроллером, а средства системы BIOS — прерывание 13h. Этим и пользуются преступники, про-

граммно моделируя результат обращения ЭВМ к ключевой дискете путем перехвата прерывания 13h.

9.4. *Использование механизма установки/снятия программных средств защиты информации.* Некоторые программные средства защиты используют при их установке на винчестер привязку к физическому расположению файла на диске. Одновременно с этим в алгоритм работы этих средств включаются функции, обеспечивающие их снятие с винчестера с одновременным восстановлением исходного состояния счетчика установок, так как защищенные программные средства нельзя перемещать путем использования стандартных средств сохранения/восстановления файлов. Использовав же функцию снятия защищенной программы с винчестера, можно тем самым получить возможность незаконного тиражирования защищенных программных продуктов в корыстных целях. Для этого преступником осуществляется следующий алгоритм действий: 1) получается санкционированный или несанкционированный доступ к защищенному программному средству, расположенному на винчестере; 2) анализируется структура размещения и содержание всех файлов, созданных на винчестере программой установки; 3) выполняется копирование защищенной программы с винчестера (при этом восстанавливается исходный счетчик установок); 4) восстанавливаются сохраненное состояние системы и ее содержимое. В результате всех этих действий получается ключевая дискета с исходным счетчиком установок и нелегальная копия программного продукта на винчестере.

9.5. *Снятие системы защиты из памяти ЭВМ.* Данный способ заключается в следующем. Система защиты через определенное время автоматически загружает в память ЭВМ защищаемое программное средство, расшифровывает его и передает управление расшифрованному коду. В этот момент в оперативной памяти компьютерной системы находится полностью расшифрованная программа и для получения несанкционированной копии остается только сохранить ее в каком-либо файле. Этим и пользуются преступники.

Рассмотренные выше способы совершения преступлений в сфере компьютерной информации, относящиеся к подгруппе преодоления программных средств защиты, и представляют собой переходную категорию между первыми тремя группами способов и четвертой.

➢ ***Комплексные методы.*** *К четвертой группе* способов совершения преступлений в сфере компьютерной информации относятся комплексные методы, под которыми понимается использование преступником двух и более способов, а также их различных комбинаций при совершении преступления. Эти способы были подробно рассмотрены в первых трех группах. Некоторые из них оказываются вспомогательными, работающими на основной способ, выбранный

преступником в качестве центрального, исходя из конкретной преступной цели и ситуации.

Помимо способов в криминалистическую характеристику компьютерных преступлений входят также цели совершения преступлений. Можно выделить следующие типичные преступные *цели совершения компьютерных преступлений*:

- хищение денег (подделка счетов и платежных ведомостей;
- фальсификация платежных документов, вторичное получение уже произведенных выплат, перечисление денег на подставные счета и т.д.);
- приписка сверхурочных часов работы;
- хищение вещей (совершение покупок с фиктивной оплатой, добывание запасных частей и редких материалов);
- хищение машинной информации;
- внесение изменений в машинную информацию;
- кража машинного времени;
- подделка документов (получение фальшивых дипломов, фиктивное продвижение по службе);
- несанкционированная эксплуатация системы;
- саботаж;
- шпионаж (политический и промышленный).

Мотивами совершения компьютерных преступлений, как показали исследования зарубежных и российских исследователей, являются следующие[1]:

1) корыстные соображения — 66%;
2) политические цели — 17%;
3) исследовательский интерес — 7%;
4) хулиганство — 5%;
5) месть — 5%.

Для подавляющего большинства преступлений характерны корыстные мотивы — 52% всех компьютерных преступлений; с разрушением и уничтожением средств компьютерной техники сопряжено 16% преступлений, с подменой исходных данных — 12%, с хищением данных и программ — 10%, с хищением услуг — 10%[2]. В этой связи интересными представляются результаты опроса, проведенного в 1988 г. среди 1600 специалистов по информационной безопасности в 50 странах мира[3].

Результаты опроса свидетельствуют, что самой распространенной угрозой безопасности были компьютерные вирусы — важнейшим

---

[1] *Вехов В.Б.* Компьютерные преступления. — М.: Право и Закон, 1996.
[2] Там же. — С. 42.
[3] PC WEEK/RE. № 1, 19 января, 1999.

этот тип угрозы назвали 60% опрошенных. В 1991 и 1992 гг. эти цифры составляли 22 и 44% соответственно.

В полном отсутствии финансовых потерь из-за нарушений в области защиты информации уверены 28% опрошенных. Среди тех, кто признает наличие таких потерь, их доли распределились так, как показано на диаграмме (рис. 16.1).

Опрос показал также, что основная часть угроз по-прежнему исходит от персонала компаний. На то, что хотя бы один из авторизованных пользователей был уличен в компьютерном злоупотреблении, указало 58% респондентов (в 1991 г. — 75%). Опасность от внешних злоумышленников не так велика, как это представляется средствами массовой информации. Неавторизованные пользователи проникали в корпоративные сети только в 24% случаев. Поставщики и покупатели являлись источниками атак лишь в 12% случаев.

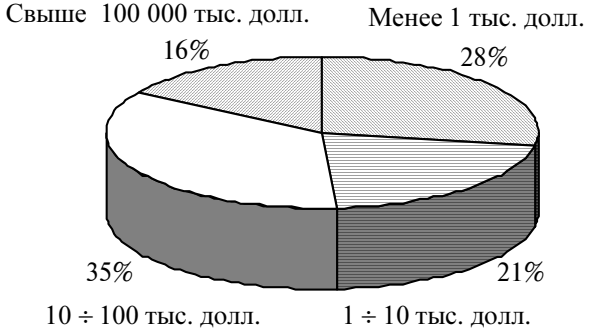


Рис. 16.1. **Финансовые потери в результате нарушений безопасности**

В этой связи особый интерес приобретает характеристика личности преступника. С криминалистической точки зрения можно выделить *несколько самостоятельных обособленных групп компьютерных преступников.*

К первой группе можно отнести лиц, сочетающих определенные черты профессионализма с элементами изобретательности и развлечения. Такие люди, работающие с компьютерной техникой, весьма любознательны, обладают острым умом, а также склонностью к озорству. Они воспринимают меры по обеспечению безопасности компьютерных систем как вызов своему профессионализму и стараются найти технические пути, которые доказали бы их собственное превосходство. При этом они не прочь поднять свой престиж, похвастаться перед коллегами умением найти

слабости в компьютерной системе защиты, а иногда и продемонстрировать, как эти слабости можно использовать. Постепенно они набирают опыт, приобретают вкус к такого рода деятельности и пытаются совмещать свои занятия с получением некоторой материальной выгоды. Такой путь проходит большинство хакеров.

Вторую группу составляют лица, страдающие особого рода информационными болезнями, развившимися на почве взаимодействия со средствами компьютерной техники.

Компьютерные системы действует на основе строго определенных правил и алгоритмов, ограниченных рамками задачи. Человек часто руководствуется чувствами, старается пояснить свою цель, аргументировать постановку задачи, ввести при необходимости новые данные и т.п. Некоторые люди попадают в такие ситуации, когда не могут адаптироваться к требованиям современной компьютерной технологии. У них развивается болезненная реакция, приводящая к неадекватному поведению. Чаще всего она трансформируется в особый вид компьютерного преступления — *компьютерный вандализм*.

Обычно он принимает форму физического разрушения компьютерных систем, их компонентов или программного обеспечения. Часто этим занимаются из чувства мести уволенные сотрудники, а также люди, страдающие компьютерными неврозами.

К третьей группе, представляющей наибольший интерес, относятся специалисты или профессиональные компьютерные преступники. Эти лица обладают устойчивыми навыками, действуют расчетливо, маскируют свои действия, всячески стараются не оставлять следов. Цели их преимущественно корыстные. Особенно опасно, если лица такой направленности оказываются среди сотрудников организации или среди авторизованных пользователей информационной системы.

В 1998 г. в Экспертно-криминалистическом центре МВД РФ был проведен классификационный анализ лиц, замешанных в применении компьютеров для совершения противоправных деяний. Обобщенный портрет отечественного хакера, созданный на основе уголовного преследования такого рода лиц, выглядит примерно так: это мужчина в возрасте от 15 до 45 лет, либо имеющий многолетний опыт работы на компьютере, либо, напротив, почти не обладающий таким опытом; в прошлом к уголовной ответственности не привлекался; является яркой, мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник, по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках группы окружающих его людей; любит уединенную работу; приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы.

Существенную роль в структуре криминалистической характеристики компьютерных преступлений играют также *сведения о потерпевшей стороне.* Изучение жертв компьютерных преступлений часто дает больше информации для решения вопросов компьютерной безопасности, чем изучение лиц, совершающих компьютерные преступления. По опубликованным данным, относящимся к группе развитых стран, среди жертв собственники системы составляли 79%; клиенты — 13%; третьи лица — 8%[1].

Особенность криминалистической характеристики компьютерных преступлений заключается и в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним. Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты своей репутации) существенно превосходят уже причиненный ущерб. И, во-вторых, преступник приобретает широкую известность в деловых и криминальных кругах, что в дальнейшем позволяет ему с выгодой использовать приобретенный опыт.

Организации, жертвы компьютерных преступлений, с неохотой сообщают об этом в правоохранительные органы. *Латентность компьютерных преступлений чрезвычайно высока.* Часто виновные лица просто увольняются или переводятся в другие структурные подразделения. Иногда с виновного взыскивается ущерб в гражданском порядке. Принимая решение, жертва компьютерного преступления руководствуется одним или несколькими из указанных ниже факторов:

- компьютерный преступник, как правило, не рассматривается как типичный уголовный преступник;
- расследование компьютерных преступлений может нарушить нормальное функционирование организации, привести к приостановке ее деятельности;
- расследование компьютерных преступлений, в том числе и силами самой фирмы, является делом весьма дорогостоящим;
- будучи разоблаченными, компьютерные преступники в большинстве случаев отделываются легкими наказаниями, зачастую условными — для пострадавших это является одним из аргументов за то, чтобы не заявлять о преступлении;

---

[1] PC WEEK/RE. № 1, 19 января, 1999.

- законодательство не всегда применимо к компьютерным преступлениям, что приводит к серьезным затруднениям при правильной их квалификации;
- правоохранительные органы не склонны относить многие из компьютерных правонарушений к категории преступлений и, соответственно, отказывают в возбуждении уголовного дела;
- компьютерный преступник воспринимается как незаурядная личность;
- жертва боится серьезного, компетентного расследования, так как оно может вскрыть неблаговидную, если не незаконную, механику ведения дел в организации;
- расследование компьютерных преступлений может выявить несостоятельность мер безопасности, принимаемых ответственным за них персоналом организации, привести к нежелательным осложнениям, постановке вопросов о профессиональной пригодности и т.д.;
- опасение увеличения размеров страховых взносов, если компьютерные преступления становятся для организации регулярными;
- боязнь потери клиентов вследствие утраты репутации;
- раскрытие компьютерных преступлений сопряжено, как правило, с открытием финансовых, коммерческих и других служебных тайн, которые могут стать достоянием гласности во время судебного рассмотрения дел.

Вопросы предотвращения и раскрытия компьютерных преступлений сегодня касаются каждой организации. Важно, чтобы администрация хорошо понимала, какие условия делают возможными такие посягательства. Руководителям не обязательно быть экспертами в области информационной безопасности, но они должны четко представлять себе возможные проблемы и последствия, связанные с потерей критичной информации.

Существует много косвенных признаков того, что в организации, учреждении готовится или осуществляется компьютерное преступление. Выявление этих признаков не требует специальных знаний и, учитывая это обстоятельство, можно предусмотреть дополнительные меры по совершенствованию компьютерной безопасности и предотвращению преступлений. Наиболее общие индикаторы таковы:

- сотрудники дают подозрительные объяснения по поводу распределения денежных и материальных средств;
- производится перезапись данных без серьезных на то причин;
- данные заменяются, изменяются или стираются;
- данные не обновляются;
- на ключевых документах появляются подделанные подписи;

- появляются фальшивые записи;
- персонал системы без видимых на то оснований начинает работать сверхурочно;
- персонал возражает против осуществления контроля за записью данных;
- у работников, непосредственно работающих с компьютерами, появляется ненормальная реакция на рутинные вопросы;
- некоторые сотрудники отказываются уходить в отпуск;
- отдельные работники начинают слоняться без дела в других подразделениях;
- жалобы клиентов становятся хроническими и др.

Рис. 16.2. **Выявление преступлений в сфере компьютерной информации**

По оценкам ведущих зарубежных и отечественных специалистов (рис. 16.2), 90% преступлений в сфере компьютерной информации остаются не обнаруженными или о них не сообщается в правоохранительные органы по различным причинам, а из оставшихся 10% обнаруженных и зарегистрированных преступлений раскрывается только каждое десятое. При этом зарегистрированные преступления в информационной сфере обнаруживаются следующим образом:

1) выявляются в результате регулярных проверок доступа к данным службами коммерческой безопасности — 31%;
2) устанавливают с помощью агентурной работы, а также при проведении оперативных мероприятий по проверкам заявлений граждан (жалобам клиентов) — 28%;
3) случайно — 19%;
4) в ходе проведения бухгалтерских ревизий — 13%;
5) в ходе расследования других видов преступлений — 10%.

Наряду с общими обстоятельствами, подлежащими установлению при расследовании компьютерных преступлений, *необходимо* в обязательном порядке *выяснить*:

1) *характеристику объекта, где совершено преступление*:

- технические и конструктивные особенности помещений, связанные с установкой и эксплуатацией вычислительной техники (специальное оборудование полов, потолков и окон, каналы кабельных и вентиляционных шахт, установка и фактическое состояние устройств кондиционирования воздуха, система электропитания и иные особенности);
- особенности установки средств комплекса вычислительной техники (сосредоточены в одном месте или расположены в различных помещениях);
- связь компьютеров между собой посредством локально-вычислительной сети (ЛВС), устройств телекоммуникации и состояние линий связи;
- структура, конфигурация сети ЭВМ и внешних информационных связей;
- режим работы;

2) *состав вычислительного комплекса*:

- тип, модель, тип и размер энергонезависимых носителей информации и другие характеристики компьютеров;
- наличие и типы периферийных устройств;
- состав и аппаратура организации локальной вычислительной сети;
- наличие, модель и характеристики устройств телекоммуникации;
- используемое программное обеспечение;
- использование программно-аппаратных средств защиты;

3) *организацию работы со средствами вычислительной техники*;

4) *способы преодоления программной и аппаратной защиты*:

- подбор ключей и паролей;
- предварительное хищение ключей и паролей;
- отключение средств защиты;
- использование несовершенства средств защиты;
- разрушение средств защиты;
- использование специальных программных средств;

5) *содержание и назначение информации, подвергшейся воздействию*;

6) *количественные и качественные характеристики информации* (объем, включая примерный объем архивной информации, возможность использования без инсталляции (установки) ключевых дискет и аппаратных ключей-паролей, способ шифрования).

Кроме того, подлежат выяснению обстоятельства, характерные для того или иного вида преступлений данной категории. К таким обстоятельствам относятся:

- режим и фактическое состояние охраны;
- наличие и техническая характеристика охранной сигнализации, вид охранной техники;
- технические средства, использованные при совершении преступления;
- режим доступа к средствам вычислительной техники;
- разграничение доступа к средствам вычислительной техники и машинным носителям;
- организация доступа к ресурсам ЭВМ, сети ЭВМ (в том числе по устройствам телекоммуникации), к кодам, паролям и другой идентифицирующей информации;
- организация противовирусной защиты — наличие разработанных правил эксплуатации ЭВМ и документации об ознакомлении с ними.

Уровень компьютерной преступности определяется во многом объективными причинами и напрямую зависит от общего уровня информатизации общества. Большинством зарубежных и отечественных исследователей отмечается отставание России в вопросах компьютеризации от развитых стран в среднем на 20 лет. Если в США первое компьютерное преступление было зафиксировано в 1966 г., то в бывшем СССР — в 1979 г. Поэтому тенденции развития компьютерной преступности в России могут заметно отличаться от таковых в развитых странах. По мнению экспертов в данной области, следует прежде всего ожидать значительного количественного роста компьютерных преступлений. Этому способствует ряд причин, среди которых основными можно считать: *во-первых*, резкий рост безработицы и падение уровня жизни среди так называемой «беловоротничковой» прослойки населения на фоне общего экономического кризиса и кризиса неплатежей; *во-вторых*, массовая неконтролируемая компьютеризация и использование новейших электронных средств во всех сферах деятельности, прежде всего финансовых, банковских и кредитных учреждениях всех форм собственности; *в-третьих*, отсутствие соответствующей правовой базы, препятствующей в сколько-нибудь заметной мере распространению и пресечению компьютерных преступлений. Если в США на сегодня действует более 2000 законов и подзаконных актов, в той или иной мере касающихся компьютерных преступлений и связанных с ними явлений, а аналогичные нормы действуют также в ФРГ, Великобритании и Франции, то в России их число не превышает и 10, включая статьи нового Уголовного кодекса РФ.

На наш взгляд, преимущественное внимание на фоне ожидаемого количественного роста компьютерных преступлений следует обратить на выявление качественных изменений и основных тенденций развития компьютерной преступности в России с целью их возможной профилактики и пресечения. К таким тенденциям можно отнести следующие:

- перенос центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей, что вызвано широким применением межбанковской системы электронных платежей и компьютерных систем связи, в рамках которой, по различным оценкам, совершается около 40% всех банковских операций в России;
- преимущественный рост компьютерных преступлений, совершаемых в сфере экономики и денежного обращения, к которым относятся финансовые хищения, мошенничества, подлоги и т.д. Это вызвано, прежде всего, большим количеством финансовых средств, находящихся в этой сфере при отсутствии надежных средств защиты информации и устойчивой дезорганизации платежной системы России;
- перерастание компьютерной преступности в разряд транснациональных преступлений, чему способствует относительная легкость преодоления систем защиты в компьютерных сетях и доступа к коммерческим секретам крупнейших мировых корпораций и банков, включая Всемирную компьютерную сеть Internet. Компьютерные преступления позволяют наиболее простым способом отмывать «грязные» капиталы (наркобизнес, незаконный оборот оружия и др.) и переводить крупные суммы денег на офшорные счета за рубежом;
- существенное омоложение в ближайшие годы компьютерной преступности за счет притока молодого поколения профессионалов-компьютерщиков, чему способствует раннее знакомство учащейся молодежи с компьютерами и отсутствие при этом устойчивых моральных принципов;
- одна из самых опасных тенденций — сращивание компьютерной преступности с организованной преступностью. Современные компьютерные преступления носят в своей массе организованный характер, требуют специальной подготовки и больших материальных и финансовых затрат на их проведение. Интеграция в международные преступные сообщества и коррупция в среде должностных лиц также способствуют этому положению;
- распространение таких компьютерных преступлений, как компьютерный экономический и политический шпионаж, шантаж и преступления против личности.

На современном этапе развития ИТ в России назрела необходимость детального изучения проблемы основ криминалистического исследования компьютерной преступности. Следует отметить, что при совершении компьютерных преступлений, также как и при совершении любых других общеизвестных видов преступлений, остаются «следы», обнаружение, фиксация и исследование которых является непременным условием при расследовании и раскрытии как данного вида преступлений, так и в борьбе с «техногенной» преступностью в целом.

Решение задачи борьбы с преступлениями в сфере компьютерной информации видится также в более объективном и тщательном подходе в законотворчестве к регламентированию общественных отношений, связанных с рассматриваемой темой. Необходимо привлекать к этой работе профессионалов из подразделений правоохранительных органов, людей, занятых в сферах бизнеса технологий и телекоммуникаций.

В Уголовный кодекс РФ требуется внести новые составы преступлений, которые позволили бы более точно определить круг преступных деяний в сфере высоких технологий и телекоммуникаций. Необходимо уйти от общих составов главы 28 УК в сторону конкретизации.

Особенно следует понимать, что в будущем не отдельные лица и даже не группы злоумышленников смогут использовать достижения в сфере высоких технологий и телекоммуникаций для своих преступных целей, но и целые государства, стоящие на позиции открытой и скрытой конфронтации, будут вести враждебные действия в информационной сфере.

В заключение рассмотрения вопроса о криминалистической характеристике компьютерных преступлений хотелось бы особо подчеркнуть, что, по данным многочисленных опросов, лишь небольшое число респондентов осведомлено о существовании тех или иных видов и способов совершения преступлений в сфере компьютерной информации, что еще раз подчеркивает актуальность проведенного выше рассмотрения.

Объясняется же столь опрометчивая неосведомленность очень просто — количество зарегистрированных компьютерных преступлений в России пока еще не очень велико. Не получившие до сих пор, в основном по экономическим причинам, необходимого развития крупные государственные и корпоративные информационные системы именно в силу своей содержательной и технической отсталости не стали объектом вторжений со стороны как отечественных, так и зарубежных информационных преступников, хотя и подвергаются массовому «пиратскому» копированию.

Банковские информационные системы стали создаваться и продолжают развитие уже с учетом имевшихся на Западе проблем с конфиденциальностью, многие из них и сейчас закрыты от внешнего доступа. Эти и другие подобные обстоятельства дают основание полагать, что угрозы информационной преступности именно в области компьютерной информации для российских субъектов реальны, однако пока не имеют той остроты, как для стран, развитых в области информационных технологий. Практика последних лет показывает, что пока еще отечественные «преступные таланты» ищут жертвы для нападения преимущественно в зарубежных информационных системах.

Кроме того, многие организации даже при установлении факта подобного преступления предпочитают ограничиваться разрешением конфликта своими силами, поскольку убытки от расследования могут оказаться выше суммы причиненного ущерба. (Изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что неприемлемо ни для одной организации.) Их руководители опасаются подрыва своего авторитета в деловых кругах и, как следствие, потери большого числа клиентов, неминуемого раскрытия в ходе судебного разбирательства системы безопасности организации либо выявления собственной незаконной деятельности.

Но даже при отсутствии перечисленных обстоятельств руководители организаций, работающих в информационной сфере, сомневаются в возможности положительного решения их проблем правоохранительными органами. Тем не менее органами внутренних дел уже проведены как организационные, так и практические мероприятия, направленные на совершенствование борьбы с компьютерными преступлениями.

В Следственном комитете при МВД России создан Отдел по организации расследования преступлений в сфере компьютерной информации, а в следственных управлениях крупных регионов — специализированные подразделения по расследованию данного вида преступлений. Оперативно-розыскная деятельность по выявлению, пресечению и раскрытию правонарушений в сфере телекоммуникаций и компьютерной информации осуществляется имеющимся в министерстве Управлением по борьбе с преступлениями в сфере высоких технологий и его подразделениями на местах.

В настоящее время активно ведется работа по подготовке и обучению сотрудников как следственных, так и оперативных подразделений. Для этих целей, помимо ведущих российских специалистов, приглашаются и специалисты правоохранительных органов зарубежных стран, уже давно столкнувшихся с проблемой компьютерной преступности.

Таким образом, созданы все необходимые условия для успешной борьбы с этим видом общественно опасных деяний.

Контрольные вопросы и задания

1. Какие существуют противоправные действия в отношении компьютерной информации?
2. В чем заключается проблема информационных нападений? Приведите примеры информационных нападений.
3. Назовите основные особенности информационной компьютерной преступности в России.
4. Какие виды компьютерных преступлений вы знаете? Как их предупреждать?
5. Охарактеризуйте способы совершения информационных компьютерных преступлений.
6. Что представляет собой компьютерный вирус? Назовите основные типы вирусов.
7. В чем заключаются отрицательные проявления компьютерных вирусов?
8. Что такое *инкубационный период развития вируса*?
9. Что такое *резидентный вирус* и как он действует?
10. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
11. Является ли вредоносной программа, обеспечивающая снятие защиты от копирования компьютерных игр?

Глава 17

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

17.1. Общие положения методики расследования компьютерных преступлений

Особенностями расследования преступлений в области компьютерной информации являются:

а) широкое использование при проведении следственных и оперативно-розыскных действий лиц, сведущих в области применения информационных технологий;

б) специфические приемы работы (осмотры, изъятие, хранение и т.п.) с машинными носителями в ходе производства следственных действий;

в) особенности выдвижения и проверки следственных версий.

На данном этапе развития средств компьютерных и информационных технологий вопрос о поиске и привлечении специалистов для оказания помощи следователю является крайне актуальным. Понятно, что при таком интенсивном развитии указанных технологий юрист-следователь не в состоянии отслеживать все технологические изменения в данной области. Специалисты крайне необходимы для участия в большинстве важнейших следственных действий — при обысках, осмотрах и выемках, а также при допросах.

Следует отметить, что информационные технологии достаточно разнообразны и выбор специалиста для решения конкретных задач весьма сложен. При решении в ходе следственных действий задач изъятия технических средств может быть полезен специалист, знающий элементы и устройства вычислительной техники и систем управления, знакомый с вопросами функционирования автоматизированных систем управления. Для установления фактов проникновения извне в информационные системы специалист должен обладать дополнительно знаниями в области математического обеспечения вычислительных систем и организации вычислительных процессов, а также знать основы методов защиты информации и

информационной безопасности. При исследовании систем ЭВМ и их сетей специалист должен иметь специализацию в области математического и программного обеспечения вычислительных комплексов, систем и сетей, а также желательны познания в области сетей, узлов связи и распределения информации.

Поиск таких специалистов следует проводить заблаговременно на предприятиях и в учреждениях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, в учебных и научно-исследовательских организациях. В крайнем случае могут быть привлечены сотрудники организации, компьютеры которой подверглись вторжению.

Общие правила обращения с вычислительной техникой и носителями информации:

- все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством;
- применение средств криминалистической техники — магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ЭВМ, должно быть согласовано со специалистом;
- необходимо исключить попадание мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.);
- при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок);
- диапазон допустимых температур при хранении и транспортировании должен варьироваться в температурных пределах от 0° до + 50° С;
- со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

Для следственных действий, сопряженных с изъятием ЭВМ, машинных носителей и информации, характерен ряд общих проблем, связанных со спецификой изымаемых технических средств.

Так, необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств. Ими может, например, использоваться специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи.

Известна легенда о хакере, который создал в дверном проеме магнитное поле такой силы, что оно уничтожало магнитные носи-

тели информации при выносе их из его комнаты. Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер требовать пароль периодически и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожатся. Изобретательные владельцы компьютеров устанавливают иногда скрытые команды DOS, удаляющие или архивирующие с паролями важные данные, если некоторые процедуры запуска машины не сопровождаются специальными действиями, известными только им.

Следует иметь в виду возможность возрастания в ходе обыска напряжения статического электричества, которое может повредить данные и магнитные носители. Желательно иметь с собой и использовать устройство для определения и измерения магнитных полей (например, компас). Вещественные доказательства в виде ЭВМ, машинных носителей требуют особой аккуратности при транспортировании и хранении. Им противопоказаны резкие броски, удары, повышенные температуры, влажность, задымленность (в том числе табачный дым) и запыленность. Все эти внешние факторы могут повлечь потерю данных, информации и свойств аппаратуры.

В протоколах следственных действий следует детально фиксировать не только факт обнаружения и (или) изъятия того или иного объекта, но и описывать местонахождение этого объекта во взаимосвязи с другими найденными на месте объектами.

При невозможности изъятия носителей информации, требуется принять меры к исключению доступа к ним заинтересованных лиц. Идеальным средством обеспечения сохранности вычислительной техники является исключение доступа в помещение, в котором она установлена, с одновременным отключением источников электропитания. Если последнее не представляется возможным (компьютер является сервером или рабочей станцией в сети), с помощью специалиста создаются условия только для приема информации. В этом случае опечатываются все необходимые узлы, детали, части и механизмы компьютерной системы. Компьютеры и их комплектующие опечатываются путем наклеивания на разъемы листа бумаги и закрепления его краев на боковых стенках компьютера клеем или клейкой лентой, чтобы исключить возможность работы с ними в отсутствие владельца или эксперта. Магнитные носители упаковываются, хранятся и перевозятся в специальных экранированных контейнерах или стандартных дискетных или иных алюминиевых футлярах, исключающих разрушающее воздействие ударов, различных электромагнитных и магнитных полей и наводок, направленных излучений. Пояснительные надписи могут наноситься только на специальные самоклеящиеся этикетки для дискет, причем сна-

чала делается соответствующая надпись, а потом этикетка наклеивается на предназначенный для этого участок на дискете. Если на дискете уже имеется этикетка с какой-либо надписью, проставляется только порядковый номер, а пояснительные надписи под этим номером делаются на отдельном листе, который вкладывается в коробку.

Недопустимо *приклеивать что-либо непосредственно к магнитным носителям*, *пропускать через них бечеву*, *пробивать отверстия*, *наносить подписи*, *пометки*, *печати*, *прикасаться пальцами или любым предметом к рабочей поверхности носителей*, *разбирать корпуса лент*, *винчестеров*, *дискет*, *сгибать носители*, *изменять состояние переключателей*, *подносить близко к источникам электромагнитного излучения*, *сильным осветительным и нагревательным приборам*, *подвергать воздействию воды и влаги.*

Если на объекте было отключено электроснабжение, например, в связи с пожаром или взрывом, то до его включения следует проверить, находятся ли все компьютеры и периферийные устройства в отключенном состоянии. Участие специалиста при производстве следственных действий в данном случае необходимо и потому, что для сокрытия информации на компьютерах могут быть установлены специальные защитные программы, которые при определенных условиях автоматически производят полное или частичное стирание информации.

Транспортирование и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия металлодетекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры.

Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковывания, транспортирования и хранения изъятых объектов решается следователем в каждом конкретном случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса Российской Федерации. В качестве понятых при производстве следственных действий рекомендуется привлекать лиц, обладающих специальными познаниями в области компьютерной техники и информатики.

Как уже отмечалось, при расследовании компьютерных преступлений важную роль играют особенности выдвижения и проверки следственных версий. Анализ отечественного и зарубежного опыта показывает, что можно выделить *три типичные следственные ситуации*:

1. Собственник информационной системы собственными силами выявил нарушения целостности конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник самостоятельно выявил указанные нарушения в системе, однако не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности конфиденциальности информации в информационной системе и виновном лице стали общеизвестны или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности конфиденциальности информации;

в) причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности конфиденциальности информации в системе и характера совершенных виновным действий;

г) отношения виновного лица к совершенным действиям и наступившим последствиям.

При отсутствии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации указанных выше доказательств, за исключением указанных в п.г.

Следует принять меры к розыску виновного и поиску его рабочего места, откуда осуществлялось вторжение в информационную систему.

Осуществляется поиск:

- места входа в данную информационную систему и способа входа в систему — вместе и с помощью должностных лиц (собственника информационной системы);
- путей следования, через которые вошел в «атакованную» систему злоумышленник и (или) проникли его программы, до рабочего места злоумышленника — вместе и с помощью должностных лиц (собственника информационной системы), а также иных информационных и коммуникационных систем.

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника-одиночки. В таком случае он сам или, если действует группа, один из ее членов либо является сотрудником данного учреждения, либо имеет свободный доступ к компьютерам (представитель службы технической или программной поддержки, программист, работающий по контракту и т.д.), умеет работать с вычислительной техникой, хорошо представляет, какая информация и где расположена в компьютере. Интерес обычно представляет информация, содержащая государственную или коммерческую тайну (например, информация базы данных о передвижении оружия, наркотиков и т.д.).

В основном, как правило, информация преступниками копируется на магнитный носитель, хотя не исключена возможность передачи ее по сетям телекоммуникации, распечатки на бумаге, кино-, фото-, видеосъемки изображения экрана и действий оператора или перехват с помощью специальных технических средств. Копирование может осуществляться как на портативный компьютер (Notebook) с подключением его к локальной вычислительной сети, так и непосредственно к последовательному или параллельному порту конкретной ЭВМ с помощью специального кабеля.

Преступление обычно происходит в рабочее время и внешне не отличается от обычной работы в учреждении. Похищенная информация используется в дальнейшем самими преступниками для подготовки хищений или может быть продана заинтересованным лицам.

Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие *общие версии*:

- преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике;
- преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений;
- преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней;
- преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценности компьютерной информации.

Приведенный перечень следственных версий является общим и в зависимости от конкретной ситуации может быть расширен.

17.2. Особенности тактики осмотра места происшествия

При осмотре места происшествия следователь обязательно должен использовать помощь незаинтересованных специалистов в области установки и функционирования средств электронно-вычислительной техники, программирования, а также специалиста-криминалиста.

Прежде чем приступить к осмотру места происшествия, следователь и участники следственно-оперативной группы должны *знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации.* Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством.

Осмотр места происшествия следует начать с запрещения доступа к средствам вычислительной техники всем лицам, работающим на объекте.

Следует принять меры к выявлению и изъятию следов рук, оставшихся на защелках дисководов, кнопках включения питания, участках корпуса около винтов крепления крышки корпуса, клавишах клавиатуры и мыши, разъемах портов и сетевых плат, а также на кнопках печатных устройств. В этих местах обычно остаются следы рук преступников. Кроме того, нельзя исключать возможности доступа в помещение, где находится компьютерная техника и информация, посторонних лиц посредством взлома, подбора ключей, в том числе паролей к электронным замкам, на которых также могут остаться следы. При осмотре кабельных соединений ЛВС требуется убедиться в их целостности, отсутствии следов подключения нештатной аппаратуры.

В связи с возможностью совершения преступлений по сетям телекоммуникации и ЛВС необходимо установить и зафиксировать в протоколе осмотра расположение всех компьютеров в сети, конкретное назначение каждого компьютера, наличие сервера, места прокладки кабелей, устройств телекоммуникации (модемов, факс-модемов), их расположение и подключение к каналам телефонной связи. Требуется также выяснить наличие специальных средств защиты от несанкционированного доступа к информации, принять меры к установлению ключей (паролей).

При непосредственном осмотре средств вычислительной техники необходимо отразить их размещение в помещении, предназначение, название (обычно указывается на лицевой стороне), серийный номер, комплектацию (наличие и тип дисководов, сетевых карт, разъ-

емов и др.), наличие и тип подключенных периферийных устройств (принтеров, сканеров, модемов и т.д.), наличие соединения с ЛВС и (или) сетями телекоммуникации, состояние устройств (целое или со следами вскрытия).

Описывая внешнее состояние вычислительной техники, нужно обращать внимание на места подключения (например, соединительный кабель между коммуникационными портами принтера и системным блоком компьютера) периферийных устройств, винты крепления крышек корпуса, поверхности под системным блоком, монитором и другими устройствами. Обычно в этих местах происходит скопление пыли, а значит, могут остаться следы, характер или отсутствие которых должно быть отражено в протоколе. Также должны быть отмечены наличие и состояние всех пометок, пломб, специальных знаков и наклеек (инвентарных номеров, записей на память, контрольных маркеров фирм-продавцов и др.), нанесенных на корпуса и устройства компьютеров, наличие загрязнений, механических повреждений и их локализация.

При осмотре средств электронно-вычислительной техники рекомендуется независимо от того, включен компьютер или нет, описать в протоколе положение всех переключателей на всех блоках и устройствах. При наличии включенной техники зафиксировать в протоколе осмотра состояние индикаторных ламп (включены или нет, каким цветом горят, мигают и с какой частотой), а также информацию, высвечиваемую на всевозможных индикаторах и табло. Описать информацию, высвечиваемую на мониторе, при этом необходимо учитывать, что для предотвращения выгорания экрана в большинстве компьютеров используют специальные заставки — хранители экрана, которые могут быть защищены паролем. В протоколе также должен быть зафиксирован вид этого хранителя. В дополнение к протоколу, кроме составления схемы расположения компьютеров и периферийных устройств в помещении и соединения компьютеров в сети, с помощью видео- или фотосъемки рекомендуется зафиксировать информацию на экране монитора, индикаторных панелях, положение переключателей и состояние индикаторных ламп всех устройств компьютерной системы, о чем сделать соответствующие записи в протоколе.

Перед выключением питания требуется корректно завершить все исполняемые в данный момент программы, по возможности сохранить всю промежуточную информацию (тексты, информацию состояния, содержание буферов обмена и др.) в специальных файлах, если возможно — на отдельных дискетах, в противном случае — на жестком диске компьютера. В протоколе указать имена этих файлов, вид информации, сохраняемой в каждом, расположение файлов (наименование дискет и их маркировку или логический диск и

каталог на винчестере компьютера); выключить компьютер, который подвергся воздействию, а при наличии сети требуется выключить все компьютеры в сети. Если из-за особенностей функционирования системы это сделать невозможно, то следует принять все меры для исключения доступа к информации данного компьютера, по возможности снять с нее копию и принять меры для фиксации всех изменений информации, которые будут происходить впоследствии.

В ходе осмотра внутреннего устройства компьютера необходимо с помощью специалиста установить наличие внутри компьютера нештатной аппаратуры, следов противодействия аппаратной системы защиты — разрушение или временное изъятие микросхем, отключение внутреннего источника питания (аккумулятора).

При осмотре места происшествия также следует обращать особое внимание на записи, относящиеся к работе компьютерной техники. В них могут оказаться сведения о процедурах входа-выхода с компьютерной системой, пароли доступа и т.п.

17.3. Особенности тактики обыска

Приемы, обеспечивающие поиск и изъятие компьютерной информации при проведении обыска, могут быть сгруппированы в рекомендации по различным этапам.

Перед обыском объекта, где по имеющейся информации находятся средства компьютерной техники (СКТ), желательно *получить оперативную ориентировку по следующим вопросам*:

1. Количество СКТ на месте, где предполагается произвести обыск, наличие устройств бесперебойного питания. Сведения об используемых телекоммуникационных средствах: есть ли модем для связи компьютеров через телефонную сеть, объединены ли несколько компьютеров в локальную сеть внутри организации, имеется ли сервер — компьютер, который обслуживает остальные персональные компьютеры; есть ли подключение к региональной или глобальной сети. Часть этих сведений можно получить на основе предварительного анонимного посещения объекта, часть может сообщить провайдер — фирма — поставщик сетевых услуг. Наличие электронной связи в организации могут прояснить «шапки» бланков писем, реклама, прайс-листы и приглашения «посетить нашу web-страницу в сети Internet».

2. Профессиональный уровень обслуживания компьютера в организации или уровень владельца — пользователя компьютера, в том числе его профессиональные навыки в области вычислительной техники. Предусмотреть возможность или даже необходимость привлечь при обыске к сотрудничеству лицо, ответственное за эксплуатацию СКТ, а при наличии сети — сетевого администратора.

3. Есть ли на СКТ программные или программно-аппаратные средства защиты от несанкционированного доступа. Если на СКТ имеются средства защиты, попытаться установить код доступа. Можно рассчитывать на последующие специальные приемы «взлома», поскольку некоторые популярные системы, в частности Windows 95/98, имеют слабые программные средства защиты и поддаются проникновению с использованием настроек или специальных программ. Выяснить, не защищает ли информацию электронный ключ — компактная электронная приставка размером со спичечный коробок, устанавливаемая на параллельный или последовательный порт (разъем) компьютера. Электронный ключ разрешает пользоваться защищенной программой и ее данными только при своем наличии. Возможно, компьютер защищен от доступа устройством чтения смарт-карт. Если на компьютере эти устройства предусмотрены, но в данный момент не подключены, можно предложить владельцу предъявить их добровольно или найти путем обычного обыска.

Целесообразно *обеспечить участие* в обыске специалиста в компьютерной технике и информатике: программиста, системного аналитика, инженера по средствам связи или сетевому обслуживанию.

По возможности, в качестве понятых следует пригласить лиц, разбирающихся в компьютерной технике. В последние годы специалистов можно подобрать в солидных компьютерных фирмах с опытом услуг и преподавания на курсах по соответствующему профилю.

Необходимо *подготовить переносную аппаратуру* для считывания и хранения изымаемой информации. С собой можно взять переносной компьютер и программное обеспечение, набор которого должен быть сформирован по совету с экспертами, а также переносные накопители информации со сменными носителями, способные вместить большой объем информации. Например: стример (ленточные кассеты), сменный жесткий диск, дисководы и диски сверхплотной записи (устройства Zip, a: Drive, DVD) и т.п.

Прийти на объект обыска лучше в момент максимального рабочего режима и срочно принимать меры по обеспечению сохранности СКТ и имеющихся на них данных. Необходимо распорядиться, чтобы персонал покинул рабочие места без прекращения работы техники и без завершения программ. Лучший вариант здесь — «оставить все как есть». На обзорной стадии обыска лицам, находящимся в помещении, запрещается прикасаться к включенным СКТ. Можно установить охрану, наблюдение, отделить находящихся на месте обыска сотрудников организации в определенной части помещения и т.д. Не разрешать выключать электроснабжение объекта. Если же электроснабжение на данный момент отключено, то перед

его восстановлением желательно отключить от электросети всю компьютерную технику.

Учитывается изображение, существующее на экране дисплея компьютера, если он включен. Если изображение на экране монитора выдает сообщение о текущем процессе удаления (уничтожения) информации, необходимо пойти на крайнюю меру — экстренно отключить компьютер от сети, а последующее включение провести с помощью специалиста. Необходимо занести в протокол названия программ, работавших в момент обыска, название и характер документов, с которыми шла работа.

Следует определить, соединены ли СКТ, находящиеся на объекте обыска, в локальную вычислительную сеть и есть ли управляющий компьютер — сервер. Серверу нужно уделить особое внимание, так как там находится большой объем информации. Хотя и на рядовом компьютере сети (на рабочей станции) тоже может находиться собственная информация. В случае сетевого соединения с другим компьютером по внутренней сети или по глобальной — установить его сетевой адрес.

Изымаются (при наличии) документы регистрации включения информационной системы и подключения к ней, журнал оператора ЭВМ, иные записи, относящиеся к работе на СКТ. В некоторых ситуациях, особенно перед изъятием, желательно составить для протокола план-эскиз помещения, указав на нем расположение СКТ. Возможно изъятие официальных планов или схем, составленных и утвержденных в самой организации. Подробно описывается порядок соединения между собой всех устройств, фиксируется наличие либо отсутствие используемого канала связи (модемы, сеть). Устанавливается тип связи, используемая в этих целях аппаратура, абонентский номер. Отмечается серийный номер (если он доступен) компьютера и его индивидуальные признаки. Рекомендуется исследовать, а при необходимости приобщать к делу магнитные носители информации: дискеты и жесткие диски, кассеты ленточных стримеров. В последнее время избранная информация может записываться по инициативе владельца на лазерный диск, поэтому при наличии таких дисков их тоже можно исследовать.

В отдельных случаях при обыске нужно искать тайники, где могут храниться сменные компьютерные носители информации; с помощью специалиста вскрывать корпуса аппаратных средств компьютерной техники, чтобы обнаружить специально отключенные внутренние носители информации, например дополнительный жесткий диск.

Если обыск проходит по делу о разработке программ в преступных целях, необходимо найти и изъять текст программы с компьютера или его распечатку. По делу о незаконном производстве пиратских программ для нелицензионного распространения без разрешения

разработчика необходимо описать найденную «готовую продукцию», перечень программ, размещенных на лазерных дисках, попросить предъявить разрешение фирмы или автора на выпуск именно этой программной продукции. С другой стороны, в организациях при обыске можно определить по компьютеру перечень установленных программ и потребовать лицензию или другие документы, подтверждающие законность их использования. *Установленной* считается программа, которая извлечена из сжатого (архивного) состояния и (после прохождения этапа предупреждения о необходимости лицензионного использования) установлена (инсталлирована) в рабочий каталог.

После выполнения указанных мероприятий можно приступить к поиску информации на компьютере. Машинные носители информации не читаемы визуально. В связи с этим следователь стоит перед дилеммой: изымать все СКТ «вслепую» и разбираться, есть ли на них значимая для дела информация после завершения обыска, или изучить с помощью специалиста на месте обыска содержащуюся на СКТ информацию, чтобы определить, что следует изъять.

В литературе встречаются рекомендации изымать все СКТ, обнаруженные на месте обыска. Полностью согласиться с подобным предложением нельзя. Изымать все средства компьютерной техники не всегда возможно и целесообразно[1].

Значительную, зачастую преимущественную долю данных на компьютере занимают программы, а документы составляют только часть. Кроме технических сложностей существуют и экономические: в случае выхода из строя ЭВМ банк, как правило, может «продержаться» не более двух дней, оптовая фирма — 3—5, компания обрабатывающей промышленности — 4—8, страховая компания — 5—6 дней. В связи с этим радикальное изъятие компьютерной техники грозит последующими претензиями пострадавших организаций. Поэтому желателен экспресс-анализ информации, содержащейся на СКТ, который, кстати, целесообразен и для оптимизации дальнейших поисковых действий следователя.

В ситуации, когда изъять СКТ и приобщить к делу в качестве вещественного доказательства невозможно либо нецелесообразно, следует распечатать интересующую информацию на принтере либо скопировать интересующие следствие сведения на дискеты, а большой объем информации — на стример, на переносной диск сверхбольшой емкости типа Zip или даже на дополнительный жесткий диск. Не изымая весь компьютер, можно изъять из системного блока жесткий диск, провести контрольную распечатку идентификации

---

[1] *Комиссаров В., Гаврилов М., Иванов А.* Обыск с извлечением компьютерной информации // Законность, 1999, № 3.

принтера на нескольких видах бумаги. В организациях с большим объемом информации может применяться резервное копирование на выделенный компьютер, который надо отсоединить от сети и временно расположить в отдельной комнате для исследования в ближайшие дни. Понятым даются необходимые пояснения.

Что и как искать на компьютере? Надо сказать, что в современных СКТ объем хранимой информации огромен и разнообразен, поэтому выбор интересующих сведений становится трудоемкой задачей. Однако современные программные средства предоставляют высокий сервис не только пользователю, но, как это ни неожиданно, и преступнику, и следователю. Не вдаваясь в технические подробности, изложим возможности оперативного поиска, осведомленность о которых поможет в работе.

Многие текстовые и финансовые программы сохраняют список документов последних сеансов работы и могут их мгновенно вызвать, если, конечно, они не удалены или не перемещены в другое место. На диске компьютера пользователи обычно сохраняют документы в каталогах (в папках) со стандартными наименованиями: МОИ ДОКУМЕНТЫ, ДОКУМЕНТЫ, DOCS, АРХИВ, ПЕТРОВ, USER (пользователь). Файлы документов имеют в названии характерное уточнение («расширение»), т.е. часть имени, которая стоит после точки в названии файла — письмо.txt, сведения, doc, платеж.xls, архив 98.zip, входящие.arj, счета.rar и т.п. Значительный интерес при наличии могут составить базы данных или данные из программы-«ежедневника», которые являются компьютерным аналогом записной книжки с адресами. Все компьютерные файлы хранят дату последнего изменения, а после некоторых программ — и дату первоначальной записи файла под этим именем.

Мощные программы при сохранении файла приписывают к полезной информации дополнительную (служебные данные, которые удается выявить при необходимости специальными программами просмотра): сведения о зарегистрированном владельце или организации (если владелец ввел такие данные при установке программы), об установленном принтере. Иногда внутрь файла попадает «соседняя» информация из документа, который обрабатывался в памяти параллельно.

Автоматический поиск среди огромного объема информации на диске помогают вести программы поиска документов по имени файла или по дате, размеру и даже по словам в тексте документа. Часть информации хранится в сжатом виде, и ее прямой просмотр невозможен. Однако существуют программы поиска и в таких сжатых файлах. Ко многим шифровальным защитам документов и сжатым архивам известны программы подбора «забытых» паролей.

«Средний» пользователь обычно не догадывается, что фрагменты или целые файлы, которые программы создают как временную

подсобную базу для работы, нередко остаются на диске и после окончания работы. Во всяком случае такие хранилища обрывков временных файлов целесообразно проверять при обыске. Популярный программный пакет Microsoft Office после установки на компьютере ведет негласный файл-протокол, куда заносит дату и время всех включений компьютера. Программы связи и работы с сетью запоминают адреса многих интернет-контактов пользователя, документы электронной почты с адресами отправителя.

Если пользователь не попросит иначе, то современные операционные системы удаляют файлы не «начисто», а сначала «в корзину» — некий «чулан для хлама», просмотрев который, информацию можно восстановить. Но даже в случае удаления файла, минуя корзину, остается вероятность восстановления, поскольку место его на диске не очищается, а только помечается как неиспользованное.

Остающиеся на месте обыска СКТ можно опечатать путем наклеивания листа бумаги с подписями следователя и понятых на разъемы электропитания, на крепеж и корпус. Не допускается пробивать отверстия в магнитных носителях, ставить на них печати. Пояснительные надписи на этикетку для дискет наносятся фломастером, но не авторучкой или жестким карандашом.

Если есть необходимость изъять СКТ после обыска, следует выйти из программы, исполняемой компьютером для операционной системы Windows 95/98, правильно завершить работу самой системы, а затем отключить электропитание всех средств компьютерной техники, подлежащих изъятию. Как уже отмечалось, желательно описать в протоколе рабочие кабельные соединения между отдельными блоками аппаратуры. Аппаратные части СКТ разъединяются с соблюдением необходимых мер предосторожности, одновременно пломбируются их технические входы и выходы. При описании изымаемых магнитных носителей машинной информации в протоколе отражается заводской номер, тип, название, а при их отсутствии подробно описываются тип, размер, цвет, надписи. Фиксацию указанных сведений в протоколе обыска желательно дополнить видеосъемкой либо фотосъемкой. Магнитные носители информации при транспортировании и хранении не должны оказаться вблизи мощных магнитных полей.

17.4. Особенности тактики назначения и проведения экспертиз при расследовании преступлений в сфере компьютерной информации

В зависимости от стоящих перед следствием задач и спецификой объектов исследования для установления конструктивных особенностей и состояния компьютеров, периферийных устройств,

магнитных носителей и пр., компьютерных сетей, причин возникновения сбоев в работе указанного оборудования, а также изучения информации, хранящейся в компьютере и на магнитных носителях, назначается компьютерно-техническая экспертиза.

Объектами компьютерно-технической экспертизы являются:

- компьютеры в сборке, их системные блоки;
- периферийные устройства (дисплеи, принтеры, дисководы, модемы, клавиатура, сканеры, манипуляторы типа «мышь», джойстики и пр.), коммуникационные устройства компьютеров и вычислительных сетей;
- магнитные носители информации (жесткие и флоппи-диски, оптические диски, ленты);
- словари поисковых признаков систем (тезаурусы), классификаторы и иная техническая документация, например технические задания и отчеты;
- электронные записные книжки, пейджеры, телефонные аппараты с памятью номеров, иные электронные носители текстовой или цифровой информации, техническая документация к ним.

Компьютерно-техническая экспертиза может быть поручена специалистам в области носителей машинной информации, программного обеспечения, баз данных и аппаратного обеспечения ЭВМ как экспертных, так и других учреждений. В частности, соответствующие специалисты могут быть в информационных центрах, учебных и научно-исследовательских заведениях. Кроме того, для производства данного вида экспертиз можно привлекать квалифицированных специалистов фирм и организаций, занимающихся разработкой программного и аппаратного обеспечения для компьютеров, их эксплуатацией и ремонтом. Данный вид экспертиз может быть поручен специалистам в области эксплуатации ЭВМ (системным программистам, инженерам по обслуживанию, непосредственно работающим с данного вида носителями и др.) и программистам, которые обладают соответствующей квалификацией.

При вынесении постановления о назначении компьютерно-технической экспертизы следователем, в постановлении о ее назначении обязательно указываются серийный номер компьютера и его индивидуальные признаки (конфигурация, цвет, надписи на корпусе и т.д.).

В рамках этого рода экспертиз выделяются два вида:

- *техническая экспертиза компьютеров и их комплектующих*, которая проводится в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей и пр., компьютерных сетей, а также причин возникновения сбоев в работе вышеуказанного оборудования;

- *экспертиза данных и программного обеспечения*, осуществляемая в целях изучения информации, хранящейся в компьютере и на магнитных носителях.

Вопросы, выносимые на разрешение компьютерно-технической экспертизы, в зависимости от вида экспертизы, также подразделяются на две группы.

А. *Вопросы, разрешаемые технической экспертизой компьютеров и их комплектующих* (*диагностические*).

1. Компьютер какой модели представлен на исследование? Каковы технические характеристики его системного блока и периферийных устройств? Каковы технические характеристики данной вычислительной сети?

2. Где и когда изготовлен и собран данный компьютер и его комплектующие? Осуществлялась ли сборка компьютера в заводских условиях или кустарно?

3. Соответствует ли внутреннее устройство компьютера и периферии прилагаемой технической документации? Не внесены ли в конструкцию компьютера изменения (например, установка дополнительных встроенных устройств: жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и пр., иные изменения конфигурации)?

4. Исправен ли компьютер и его комплектующие? Каков их износ? Каковы причины неисправности компьютера и периферийных устройств? Не содержат ли физических дефектов магнитные носители информации?

5. Не производилась ли адаптация компьютера для работы с ним специфических пользователей (левша, слабовидящий и пр.)?

6. Каковы технические характеристики иных электронных средств приема, накопления и выдачи информации (пейджер, электронная записная книжка, телефонный сервер)? Исправны ли эти средства? Каковы причины неисправностей?[1]

В. *Диагностические вопросы, разрешаемые экспертизой данных и программного обеспечения.*

1. Какая операционная система использована в компьютере?

2. Каково содержание информации, хранящейся на внутренних и внешних магнитных носителях, в том числе какие программные продукты там находятся? Каково назначение программных продуктов? Каков алгоритм их функционирования, способа ввода и вывода информации? Какое время проходит с момента введения данных до вывода результатов при работе данной компьютерной программы, базы данных?

---

[1] Расследование преступлений в сфере компьютерной информации / Под ред. *А.Н. Родионова*. — М., 1998.

3. Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем или оригинальными разработками?

4. Не вносились ли в программы данного системного продукта какие-либо коррективы (какие), изменяющие выполнение некоторых операций (каких)?

5. Соответствует ли данный оригинальный компьютерный продукт техническому заданию? Обеспечивается ли при его работе выполнение всех предусмотренных функций?

6. Использовались ли для ограничения доступа к информации пароли, скрытые файлы, программы защиты и пр.? Каково содержание скрытой информации? Не предпринимались ли попытки подбора паролей, взлома защитных средств и иные попытки несанкционированного доступа?

7. Возможно ли восстановление стертых файлов? Возможно ли восстановление дефектных магнитных носителей информации? Каково содержание восстановленных файлов?

8. Каков механизм утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных?

9. Имеются ли сбои в функционировании компьютера, работе отдельных программ? Каковы причины этих сбоев? Не вызваны ли сбои в работе компьютера влиянием вируса (какого)? Распространяется ли негативное влияние вируса на большинство программ или он действует только на определенные программы? Возможно ли восстановить в полном объеме функционирование данной программы (текстового файла), поврежденного вирусом?

10. Каково содержание информации, хранящейся на пейджере, в электронной записной книжке и пр.? Имеется ли в книжке скрытая информация и каково ее содержание?

11. Когда производилась последняя корректировка данного файла или инсталляция данного программного продукта?

12. Каков был уровень профессиональной подготовки в области программирования и работы с компьютерной техникой лица, произведшего данные действия с компьютером и программным обеспечением?

С. *Вопросы идентификационного характера, разрешаемые компьютерно-технической экспертизой.*

1. Имеют ли комплектующие компьютера (печатные платы, магнитные носители, дисководы и пр.) единый источник происхождения?

2. Не написана ли данная компьютерная программа определенным лицом (решается комплексно при производстве компьютерно-технической и автороведческой экспертиз)?

Кроме приведенного выше перечня вопросов, разрешаемых компьютерно-технической экспертизой, для использования на практике, в зависимости от объекта исследования и конкретной обстановки, можно привести дополнительные примеры, расширяющие перечень вопросов, подлежащих выяснению при исследовании таких объектов, как носители информации, программное обеспечение, базы данных и аппаратное обеспечение ЭВМ.

Перечень вопросов, разрешаемых при исследовании носителей машинной информации.

1. Каков тип носителя, его технические характеристики (на каких типах ЭВМ может быть использован, максимально-допустимая емкость записи и пр.)?

2. Имеет ли носитель механические повреждения?

3. Как размечен носитель, в каком формате информация записана на него?

4. Какая информация записана на данный носитель?

5. Как информация физически размещена на носителе (для лент — последовательность записи, для дисков — сектора, дорожки, цилиндры и пр.)?

6. Как информация размещена логически на носителе (файлы, каталоги, логические диски)?

7. Имеются ли повреждения информации (плохие сектора, потерянные блоки и пр.)?

8. Возможна ли коррекция информации на носителе?

9. Имеется ли на носителе компьютерный вирус, если да, то какой, какие изменения вносит и возможна ли его нейтрализация без ущерба для информации?

10. Являются ли изменения на носителе результатом действия вируса?

11. Возможно ли копирование информации с данного носителя и возможно ли физическое копирование носителя в целом?

12. При повреждении носителя, возможно ли восстановление информации?

13. Какая информация ранее была записана на данный носитель (отмечена как стертые файлы) и возможно ли ее восстановление?

14. Какой объем занимает вся информация на носителе, ее отдельные части и сколько имеется свободного места?

15. Какое время занимает копирование данной информации с учетом типа ЭВМ?

16. Требуются ли для работы с информацией на носителе специальные аппаратные или программные средства дешифрации и перекодировки?

17. Нет ли на носителе специальных программ, уничтожающих информацию в случае несанкционированного доступа, отсутствия

ключей и паролей или использования на другом компьютере, стоит ли счетчик возможных инсталляций и другие средства защиты, возможен ли их обход и каким образом?[1]

Под программным обеспечением (программами для ЭВМ) понимается совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

Программное обеспечение обычно хранится на магнитных, оптических или электронных (непосредственно установлено в микросхемах памяти компьютера) носителях машинной информации и управляет работой вычислительной системы. Кроме того, коды программ, входные, выходные и промежуточные данные могут находиться на бумажном носителе (перфолента, перфокарта). Вся информация, относящаяся к программному обеспечению, независимо от формы носителя, является объектом экспертизы и должна быть представлена эксперту.

Перечень вопросов, разрешаемых при исследовании программного обеспечения.

1. Каково назначение данного программного обеспечения?

2. Кто разработчик данного обеспечения?

3. Каким образом данное программное обеспечение распространяется, кто является владельцем данной копии, имеется ли лицензия или разрешение на использование данного продукта. Каков серийный номер данной копии программного обеспечения?

4. С какими входными и выходными данными оно работает, каким образом и в какой форме эти данные вводятся в ЭВМ, создаются ли (а если создаются, то где) временные файлы и файлы статистики и их содержание, в какой форме выдается, где хранится или куда передается выходная информация?

5. Требует ли данная программа при своей работе ввода паролей и наличия ключей (дискет, заглушек и пр.). Если требует, то, каким образом они хранятся и кодируются, имеется ли возможность прочитать файл с паролем с помощью простейших редакторов?

6. Возможен ли обход паролей при запуске программы через отладчик?

7. Имеются ли на машинном носителе исходные коды программ на языке программирования?

8. Когда последний раз вносились изменения в программу (например, по дате и времени создания или внесения изменений в файлы)?

---

[1] Расследование преступлений в сфере компьютерной информации / Под ред. *А.Н. Родионова*. — М., 1998.

9. Имеются ли в программе изменения по сравнению с исходной версией, что было изменено, к каким последствиям данные изменения приводят?

10. Имеются ли в программе враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Каким образом эти функции осуществляются и к каким последствиям приводят?

11. Возможно ли самопроизвольное распространение данной программы, т.е. является ли данная программа компьютерным вирусом?

12. Возможно ли осуществление копирования информации или требуется инсталляция?

13. Были ли внесены в программу изменения, направленные на преодоление защиты?

14. Количественные (занимаемый объем, требуемое количество дискет, количество файлов и пр.) и качественные (назначение конкретных файлов, требование к оборудованию и пр.) характеристики программы?

15. Соответствие алгоритма работы конкретной программы требованиям, указанным в техническом задании или заявленным в инструкции по эксплуатации?

16. Имеются ли ошибки при проведении расчетов с помощью данной программы (правильно ли происходит округление чисел, правильный ли алгоритм расчета конкретных данных и пр.?

17. Определить тип ЭВМ, систему ЭВМ, совместимую с программным и аппаратным обеспечением данного компьютера, если ее нет, то каким образом это влияет на нормальную работу программы?

18. Имеется ли полная совместимость конкретного программного обеспечения с другими программами, выполняемыми на данном компьютере, если нет, то каким образом это влияет на нормальное функционирование системы?

Под базами данных понимается форма представления и организации совокупности данных (статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ. С точки зрения организации базы данных могут представлять собой информацию в текстовых файлах и информацию в файлах со специальной структурой, которые обрабатываются специальными программами (системами управления базами данных, сокращенно СУБД), именно их в компьютерной терминологии называют базами данных.

Базы данных обычно хранятся на магнитных, оптических или электронных носителях машинной информации или непосредственно установлены в микросхемах памяти компьютера. Кроме того, коды

баз данных, входные, выходные и промежуточные данные могут находиться на бумажном носителе (распечатки исходных текстов программ баз данных, перфолента, перфокарта). Вся информация, относящаяся к базам данных, независимо от формы носителя, является объектом экспертизы и должна быть представлена эксперту.

Перечень вопросов, разрешаемых при исследовании баз данных.

1. Каким образом организована база данных?

2. В каком формате записана информация и какие СУБД могут ее обрабатывать?

3. Какая информация записана в данной базе?

4. Информация в базе записана обычным образом или закодирована?

5. Когда последний раз обновлялась информация?

6. Имеются ли в данной базе скрытые (помеченные для удаления) поля, каково их содержание?

7. Имеются ли повреждения или изменения в записях базы по сравнению с эталоном или резервной копией, если да, то какие?

8. Сколько записей в базе?

9. Имеется ли в данной базе запись конкретного содержания?

10. Возможно ли внести изменение в данную базу с помощью простейших программных средств (например, текстовых редакторов и пр.)?

Под аппаратным обеспечением ЭВМ понимается комплекс технических средств, предназначенных для автоматизированной обработки информации, обеспечения хранения и передачи ее по каналам связи, ведения диалога с пользователем и выполнения других функций в составе компьютерной системы. Аппаратное обеспечение в свою очередь *подразделяется на*:

I. Центральные устройства ЭВМ (центральный процессор; оперативное и постоянное запоминающие устройства; системную шину; другие устройства для обеспечения работы вычислительной системы — контроллеры, таймер, тактовый генератор, различные буферы и пр.).

II. Периферийные устройства (видеоподсистема; накопители различных типов; устройства вывода информации; устройства ввода информации; устройства организации ЛВС и телекоммуникации; другие устройства, сопряженные с компьютером и которые функционируют под его управлением).

III. Вспомогательные устройства (устройства электропитания; различные фильтры — сетевые, экранные и пр.; аппаратура защиты, работающая автономно от центрального процессора, — генераторы помех и пр.).

Перечень вопросов, разрешаемых при исследовании аппаратного обеспечения ЭВМ.

1. Каковы тип устройства и его технические характеристики?

2. Исправно ли данное устройство или нет, тип неисправности (отказ или сбой), как она влияет на работу системы в целом?

3. Полностью ли совместимы между собой компоненты данного устройства, если нет, то как это сказывается на его работе?

4. Полностью ли совместимо данное устройство с каким-либо конкретным устройством, если нет, то как сказывается это на их работе?

5. Имеются ли на устройстве следы ремонта, повреждений, демонтажа микросхем, замены блоков?

6. Соответствует ли комплектация устройства технической документации, если нет, то какие компоненты были изменены, демонтированы?

7. Нет ли в данном устройстве дополнительных блоков (жучков) с враждебными функциями, если есть, то их предназначение?

8. Возможно ли на данном оборудовании решать какие-либо конкретные задачи?

9. Какой уровень излучений у данного устройства, возможен ли его прием специальными техническими средствами для последующей расшифровки информации, если возможен, то на каком расстоянии?

10. Возможно ли отключение аппаратных средств защиты и как это влияет на работу системы?

11. Соблюдались ли правила эксплуатации?

12. Могла ли данная проблема возникнуть в результате несоблюдения правил технической эксплуатации?

В качестве примера успешного расследования уголовного дела о «компьютерном» преступлении, когда была назначена и проведена компьютерно-техническая экспертиза, можно привести случай, имевший место в г. Москве. Так, житель г. Москвы К. открыл в одном из столичных банков счета на вымышленных лиц, подделав их паспорта, и внес на эти счета суммы от 50 до 100 долларов США. Затем он вступил в преступный сговор с начальником отдела автоматизации этого банка Р., который внес изменения в программное обеспечение, использовавшееся при осуществлении банковских операций, в результате чего на открытые расчетные счета было переведено в совокупности более 250 тыс. долл. США. По поддельным паспортам К. получил со счетов эту сумму и присвоил ее. Компьютерно-техническая экспертиза программного обеспечения позволила установить, как модифицирована исходная программа и на каком уровне доступа к ней (т.е. кем) могла быть произведена эта модификация. В итоге преступники были установлены и привлечены к ответственности.

При расследовании компьютерных преступлений могут быть назначены и другие судебные экспертизы.

По делу о хищении валютных средств во Внешэкономбанке, совершенных путем использования компьютерных расчетов, комплексной судебно-бухгалтерской и информационно-технической экспертизой были установлены следующие нарушения порядка эксплуатации:

- отсутствие организации по обеспечению информационной безопасности;
- нарушение технологического цикла проектирования, разработки, испытаний и сдачи в эксплуатацию программного обеспечения системы автоматизации банковских операций;
- совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения, что позволяло разработчикам после сдачи компьютерной системы в промышленную эксплуатацию иметь доступ к закрытой информации в нарушение установленных правил (под предлогом доводки программного обеспечения);
- использование незарегистрированных в установленном порядке программ;
- неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций по обработке компьютерной информации и лиц, эксплуатирующих ЭВМ[1].

Контрольные вопросы и задания

1. Какие виды мероприятий необходимо проводить для защиты компьютерной информации?
2. Какие данные об обстановке совершения компьютерного преступления следует считать основными?
3. Назовите типичные следственные ситуации и следственные действия первоначального этапа расследования компьютерного преступления.
4. В чем заключаются особенности производства осмотров и обысков при расследовании информационных преступлений.
5. Опишите порядок осмотра и изъятия компьютера и устройств ввода-вывода информации.
6. Перечислите наиболее типичные способы неправомерного доступа в компьютер и информационную сеть.

---

[1] Руководство для следователей / Под ред. *Н.А. Селиванова* и *В.А. Снеткова*. — М., 1997.

7. Как следует проводить диагностику компьютера на наличие вирусов?
8. Может ли вирус с дискеты попасть на винчестер, если дискета заражена вирусом и работа ведется только с дискетой?
9. Как проверить дискету на присутствие вируса?
10. Как защитить дискету от вирусов?
11. Любой ли файл может быть заражен компьютерным вирусом?
12. Каким образом компьютерный вирус распространяется через дискету, на которой находятся только текстовые файлы?
13. Могут ли вирусы остаться на дискете после того, как проведено ее лечение антивирусной программой?
14. Может ли быть заражен вирусом архивный файл?
15. Можно ли проводить лечение зараженного вирусом компьютера, запуская антивирусные программы с винчестера?
16. Происходит ли полное уничтожение вирусов на дисках компьютера при форматировании?
17. Могут ли быть заражены вирусом файлы самих антивирусных программ?
18. Как можно закрыть архивный файл от несанкционированного доступа?
19. Как квалифицировать действия лица, укравшего системный блок с целью неправомерного доступа к информации, находящейся на машинном носителе?
20. Как оценить действия лица, неправомерно скопировавшего компьютерную базу данных организации, содержащую сведения о частных лицах — сотрудниках и поставщиках организации, и изготовившего компакт-диски для ЭВМ с этой информацией для их последующей розничной продажи?

ЗАКЛЮЧЕНИЕ

В современных условиях персональный компьютер стал для сотрудников правоохранительных органов «орудием производства», сейчас без знания персонального компьютера и соответствующего программного обеспечения уже невозможно представить работу сотрудника следствия, криминалиста, а тем более сотрудника штаба или информационного подразделения. Поэтому эти категории сотрудников должны иметь навыки работы на персональном компьютере, знать и применять в повседневной практике методы обработки деловой и аналитической информации с использованием ПК.

Что должен знать и что освоить сотрудник правоохранительных органов для успешной организации управленческой, следственной и оперативной деятельности с использованием компьютерной технологии работы с информацией?

Во-первых, основные понятия информатики и используемые термины, 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;
- 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);
- использование специализированных прикладных статистических программных пакетов;
- работу со справочными правовыми системами.

Очевидно, что в рамках одной книги детально осветить все вышеперечисленные вопросы не представляется возможным. Так, не были описаны подробно методы работы с пакетами прикладных программ общего назначения, такими как текстовые редакторы, 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:

- 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 вводный курс, рассчитанный на пользователей начального и среднего уровня квалификации.

За время написания и подготовки книги к изданию произошли серьезные изменения в области компьютерных информационных технологий — сменилось не одно поколение микропроцессоров (Pentium MMX, Celeron, Pentium II, Pentium III, Pentium IV); значительно, почти до 4 ГГц, возросла тактовая частота микропроцессоров; появились новые типы микросхем оперативной и кэш-памяти и существенно, на порядок, возрос их объем; возросли быстродействие и емкость накопителей на жестких магнитных дисках; на смену

накопителям CD ROM пришли накопители DVD ROM, способные хранить до 20 Гбайт информации; появились новые типы видеоадаптеров и мониторов; сменились два поколения операционных систем (Windows 95, Windows 98), появилось большое количество мультимедийных программных продуктов и офисных приложений (MSOffice 2000, MSOffice XP). Громадный шаг вперед был сделан в развитии глобальных компьютерных сетей, прежде всего сети Internet, 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, поможет в освоении не только описанных в книге технических и программных средств, но и новых, более удобных и совершенных, предназначенных не только для грамотной работы на компьютере но и, что имеет первостепенное значение, для компетентного выполнения профессиональных функций. Мы надеемся, что материал книги послужит для читателей стартовой базой для движения вперед, ибо нет предела совершенству.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Андреев В.Б.* Правовая информатика: Учеб. пособ. — М.: ИМП, 1998.
2. *Баранов А.К.*, *Карпычев В.Ю.*, *Минаев В.А.* Компьютерные экспертные технологии в органах внутренних дел: Учеб. пособ. — М.: Академия МВД РФ, 1992.
3. *Батурин Ю.М.* Право и политика в компьютерном круге. — М.: Наука, 1987.
4. *Батурин Ю.М.* Проблемы компьютерного права. — М.: Юрид. лит., 1991.
5. *Батурин Ю.М.*, *Жодзишский А.М.* Компьютерные преступления и компьютерная безопасность. — М.: Юрид. лит., 1991.
6. *Бауэр Ф.Л.*, *Гооз Г.* Информатика: Вводный курс: В двух частях. — Ч. 1. — М.: Мир, 1990.
7. *Безруков Н.Н.* Компьютерные вирусы. — М.: Наука, 1991.
8. *Богатов Д.И.*, *Богатов И.Г.*, *Минаев В.А.* Информатика и математика для юристов. Краткий курс в таблицах и схемах: Учеб. пособ. / Под ред. В.А. Минаева. — М.: Приор, 1998.
9. *Боровков В.П.* Популярное введение в программу «Statistica». — М.: Компьютер пресс, 1998.
10. *Вехов Б.В.* Компьютерные преступления: способы совершения, методика расследования. — М.: Право и Закон, 1996.
11. *Воскресенский Г.М.*, *Дударев Г.И.*, *Масленников Э.П.* Статистические методы обработки и анализа социальной информации в управленческой деятельности органов внутренних дел. — М.: Академия МВД СССР, 1986.
12. *Гаврилов О.А.*, *Колемаев В.А.* Математические модели в криминологии. — В кн.: Правовая кибернетика. — М.: Наука, 1970.

13. *Гудков П.Б.* Компьютерные преступления в сфере экономики. — М.: МИ МВД России, 1995.

14. *Гульбин Ю.* Преступления в сфере компьютерной информации // Российская юстиция, 1997, № 10. — С. 24—25.

15. *Демидов В.Н.* Криминологическая характеристика преступности в России и Татарстане: Учеб. пособ. — М.: ВНИИ МВД России, 1998.

16. *Дьяконов В.П.* Справочник по расчетам на микрокалькуляторах. — 3-е изд., доп. и перераб. — М.: Наука, 1989.

17. *Дьяконов В.П.* Справочник по алгоритмам и программам на языке БЕЙСИК для персональных ЭВМ. — М.: Наука, 1989.

18. *Женило В.Р.* Информатика и вычислительная техника в деятельности органов внутренних дел. — Ч. 3. Программное обеспечение компьютерной технологии: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1996.

19. *Женило В.Р.*, *Минаев В.А.* Компьютерные технологии в криминалистических фоноскопических исследованиях и экспертизах: Учеб. пособ. — М.: Академия МВД РФ, 1994.

20. *Ивахненко А.Г.*, *Юрачковский Ю.П.* Моделирование сложных систем по экспериментальным данным. — М.: Радио и связь, 1987.

21. *Информатика.* Базовый курс: Учебник для вузов / Под ред. С.В. Симоновича. — СПб.: Питер, 1999.

22. *Згадзай О.Э.*, *Казанцев С.Я.*, *Филиппов А.В.* Информатика и математика для юристов: Учебник. — Казань: Изд-во Казан. ун-та, 2000.

23. *Информатика* и вычислительная техника в деятельности органов внутренних дел. — Ч. 2. Аппаратные средства компьютерной техники: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1995.

24. *Информатика* и вычислительная техника в деятельности органов внутренних дел. — Ч. 4. Автоматизация решения практических задач в органах внутренних дел: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1996.

25. *Информатика* и вычислительная техника в деятельности органов внутренних дел. — Ч. 5. Аналитическая деятельность и компьютерные технологии: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1996.

26. *Информатика* и вычислительная техника в деятельности органов внутренних дел. — Ч. 6. Информационно-вычислительные сети в органах внутренних дел: Учеб. пособ. / Под ред. В.А. Минаева. — М.: ГУК МВД РФ, 1997.

27. *Информационные* технологии управления в органах внутренних дел / Под ред. проф. В.А. Минаева. — М.: Академия управления МВД РФ, 1997.

28. *Исаков С.А.* Информационно-техническое обеспечение органов внутренних дел: Учеб. пособ. — М.: Юридический институт МВД РФ, 1994.

29. *Использование* математических методов и ЭВМ в экспертной практике: Сборник научных трудов. — М., 1989.

30. *Казанцев С.Я.*, *Мазуренко П.И.* Использование ЭВМ в деятельности правоохранительных органов. — Казань: Казанский филиал Юридического института МВД РФ, 1997.

31. *Калинина В.Н.*, *Панкин В.Ф.* Математическая статистика. — М.: ЮНИТИ, 2002.

32. *Каталог* программных средств, рекомендуемых к внедрению в практику СЭУ МЮ СССР. — М., 1989.

33. *Кемени Дж.*, *Снелл Дж.* Введение в конечную математику. — М.: Мир, 1965.

34. *Кидмайер М.* Мультимедиа. — СПб.: BHV-Санкт-Петербург, 1994.

35. *Колемаев В.А.*, *Калинина В.Н.* Теория вероятностей и математическая статистика. — М.: ЮНИТИ, 2003.

36. *Комментарий* к Уголовному кодексу Российской Федерации / Под ред. А.В. Наумова. — М.: Юристъ, 1996.

37. *Компьютерные* технологии обработки информации: Учеб. пособ. / Под ред. С.В. Назарова. — М.: Финансы и статистика, 1995.

38. *Компьютерные* технологии в юридической деятельности: Учеб. и практ. пособ. / Под ред. проф. Н. Полевого, канд. юрид. наук. В. Крылова. — М.: БЕК, 1994.

39. *Концепция* развития системы информационного обеспечения органов внутренних дел в борьбе с преступностью: Утверждена Приказом МВД РФ № 229 от 12.05.93 г.

40. *Коршунов Ю.М.* Математические основы кибернетики. — М.: Энергоатомиздат, 1987.

41. *Криминалистика* и компьютерная преступность. Материалы научно-практического семинара: Сб. статей. — М.: ЭКЦ МВД России, 1993.

42. *Крылов В.В.* Расследование преступлений в сфере информации. — М.: Городец, 1998.

43. *Левин А.* Самоучитель работы на компьютере. — 5-е изд. — М.: Нолидж, 1999.

44. *Локальные* вычислительные сети: Справочник: В 3-х кн. — Кн. 1. Принципы построения, архитектура, коммуникационные средства / Под ред. С.В. Назарова. — М.: Финансы и статистика, 1994.

45. *Ляпунов Ю.*, *Максимов В.* Ответственность за компьютерные преступления // Законность, 1997, № 1. — С. 8—15.

46. *Мак-Кланг Кр.Дж.*, *Герриери Дж.А.*, *Мак-Кланг К.А.* Микрокомпьютеры для юристов: Пер. с англ. А.П. Полежаева. — М.: Юрид. лит., 1988.

47. *Маркарян А.А.* Интеграция достижений естественных и технических наук в криминалистику. — Ижевск: УдГУ, 1996.

48. *Мельников В.В.* Защита информации в компьютерных системах. — М.: Финансы и статистика, 1997.

49. *Методология* и методика прогнозирования в сфере борьбы с преступностью: Труды Академии МВД СССР. — М.: Академия МВД СССР, 1989.

50. *Минаев В.А.* Кадровые ресурсы органов внутренних дел: Современные подходы к управлению. — М.: Академия МВД СССР, 1991.

51. *Минин А.Я.* Основы управления и информатики: Курс лекций. — Екатеринбург: Екатеринбургская высшая школа МВД России, 1993.

52. *Минин А.Я.* Информатизация криминологических исследований: теория и методология. — Екатеринбург: Изд-во Урал. ун-та, 1992.

53. *Наука* и техника на службе следствия: Информационный бюллетень Следственного управления МВД РТ. Вып. 5. — Казань, 1996.

54. *Об информации*, информатизации и защите информации: Федеральный закон от 22 февраля 1995 г. // Российская газета, 1995.

55. *Организация* деятельности информационных работников горрайлинорганов внутренних дел: Сб. материалов для занятий в системе служебной подготовки / Под ред. Ю.А. Буничева. — М.: ГИЦ МВД РФ, 1995.

56. *Основы* автоматизации управления в органах внутренних дел: Учебник / Под ред. В.А. Минаева, А.П. Полежаева. — М.: Академия МВД РФ, 1993.

57. *Основы* математического моделирования в деятельности органов внутренних дел: Учеб. пособ. / Под ред. В.А. Минаева. — М.: Академия МВД РФ, 1993.

58. *Персон Р.* Microsoft Excel 97 в подлиннике. Т. 1, 2: Пер. с англ. — BHV-Санкт-Петербург, 1997.

59. *Першиков В.И.*, *Савинков В.М.* Толковый словарь по информатике. — 2-е изд., доп. — М.: Финансы и статистика, 1995.

60. *Петровский А.*, *Леонтьев Б.* Эффективный хакинг для начинающих и не только. — М.: Познавательная книга плюс, 1999.

61. *Полевой Н.С.* Криминалистическая кибернетика: Учеб. пособ. — 2-е изд. — М.: МГУ, 1989.

62. *Правовая* информатика и кибернетика: Учебник / Под ред. Н.С. Полевого. — М.: Юрид. лит., 1993.

63. *Проблемы* программирования, организации и информационного обеспечения предварительного следствия: Межвуз. межвед. сб. науч. трудов. — Уфа, 1989.

64. *Программа* компьютеризации органов внутренних дел РФ на 1991 год и ближайшую перспективу: Утверждена Приказом МВД РФ № 104 от 05.07.91 г.

65. *Расследование* неправомерного доступа к компьютерной информации / Под ред. И.Г. Шурухнова. — М.: Щит, 1999.

66. *Симонович С.В.* и др. Информатика для юристов и экономистов. — СПб.: Питер, 2001.

67. *Симонович С.В.*, *Евсеев Г.А.* Практическая информатика: Учеб. пособ. Универсальный курс. — М.: АСТ-Пресс, 1998.

68. *Симонович С.В.*, *Евсеев Г.А.*, *Алексеев А.Г.* Специальная информатика: Учеб. пособ. — М.: АСТ-Пресс, 1998.

69. *Сойер Б.*, *Фостер Д.Л.* Программирование экспертных систем на Паскале: Пер. с англ. — М.: Финансы и статистика, 1990.

70. *Соковых Ю.Ю.* Квалификация преступлений и информатика // Информационный бюллетень следственного комитета МВД РФ. — 1993. № 4(46).

71. *Статистическое* моделирование и прогнозирование: Учеб. пособ. / Под ред. А.Г. Гранберга. — М.: Финансы и статистика, 1990.

72. *Техническое* задание на создание информационной вычислительной сети органов внутренних дел РФ: Утверждено Министром ВД 22.02.92 г.

73. *Тутубалин В.Н.* Теория вероятностей. — М.: МГУ, 1972.

74. *Федеральные* учеты ГИЦ в борьбе с преступностью. В помощь работникам органов внутренних дел / Под ред. Г.Л. Лежикова. — М.: ГИЦ МВД РФ, 1994.

75. *Фигурнов В.Э.* IBM PC для пользователя. — Изд. 6-е, перераб. и доп. — М.: Инфра-М, 1995.

76. *Щербинин А.И.*, *Игнатов Л.Н.*, *Пучков С.И.*, *Котов И.А.* Сравнительный анализ программных средств автоматизации уголовно-процессуальной деятельности // Информационный бюллетень Следственного комитета МВД РФ. — 1993, № 3(46). — С. 73—82.

77. *Щербинин А.И.*, *Ильин С.Н.*, *Игнатов Л.Н.* Использование персональных ЭВМ в расследовании сложных многоэпизодных дел о хищениях в банковской сфере // Информационный бюллетень Следственного комитета МВД РФ. — 1993, № 4(46).

78. *Экспертные* системы. Принцип работы и примеры. — М.: Радио и связь, 1987.

79. *Яромич С.А.* Информатика вокруг нас: Словарь-справочник. — Одесса: Маяк, 1991.

80. *Крылов В.* Информационные преступления — новый криминалистический объект // Российская юстиция, 1997, № 4.

ОГЛАВЛЕНИЕ