ФГБОУ ВПО «Воронежский государственный
технический университет»

А.В. Мандрыкин Д.М. Шотыло

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕНЕДЖМЕНТЕ

Утверждено Редакционно-издательским советом
университета в качестве учебного пособия

Воронеж 2014

УДК 004

Мандрыкин А.В. Информационные технологии в менеджменте: учеб. пособие [Электронный ресурс]. – Электрон. текстовые, граф. данные (17,5 Мб) / А.В. Мандрыкин, Д.М. Шотыло. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2014. – 1 электрон. опт. диск (DVD-R). – Систем. требования: ПК 500 и выше; 256 Мб ОЗУ; Windows XP; MS Word 2007 или более поздняя версия; 1024x768; DVD-ROM; мышь. – Загл. с экрана.

Информационные технологии являются одним из основополагающих теоретических, методических и практических элементов формирования у студента современного мышления, основанного на понимании роли электронной (цифровой) информации в различных сферах деятельности и самом процессе обучения, преимуществ создания, получения, обработки и использования информации с помощью компьютерной техники и информационных коммуникаций.

Издание соответствует требованиям Федерального государственного образовательного стандарта высшего профессионального образования по направлению 38.03.02 “Менеджмент”, всем профилям, дисциплинам “Информационные технологии в менеджменте” и “Информационные технологии в логистике”.

Табл. 6. Ил. 41. Библиогр.: 7 назв.

Рецензенты: отдел проектирования и разработки прикладного программного обеспечения ВГАСУ (ведущий инженер В.В. Тарасов);
канд. экон. наук, доц. Е.В. Шкарупета

ВВЕДЕНИЕ

В процессе управления экономическими системами менеджерам высшего звена сложно организовать свою деятельность с учётом автоматизации многих бизнес-процессов. Эффективность автоматизации в данном случае напрямую зависит от рационального управления информационными технологиями.

Цель дисциплины заключается в освоении студентами современных информационных технологий в экономике и управлении, обеспечивающих управление информацией и управление с помощью информации деятельностью предприятия или организации и повышающих надёжность и оперативность трудоёмких процессов использования информационных ресурсов.

Задачи дисциплины заключаются в приобретении знаний в освоении навыкам работы с: компьютером как средством управления информацией; информационными технологиями в деятельности предприятия или организации, системами электронного документооборота, корпоративными информационными системами и базами данных для решения информационных, экономических и управленческих задач; Интернет-технологиями в глобальных компьютерных сетях; антивирусными программами и межсетевыми экранами для обеспечения информационной безопасности и защиты информации в информационно-экономических системах; пакетами прикладных программ в бухгалтерском учёте, финансовой, маркетинговой и логистической деятельности предприятия или организации.

Требования к результатам освоения дисциплины:

- понимание роли и значения информации и информационных технологий в развитии современного общества и экономических знаний;

- владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией;

- способность работать с информацией в глобальных компьютерных сетях и корпоративных информационных системах.

В результате изучения дисциплины студент должен:

знать:

- основные понятия, современные принципы работы с информационными технологиями, методы и средства управления

информацией и управление с помощью информации деятельностью предприятия или организации;

- основные понятия и современные принципы работы с деловой информацией, а также иметь представление о корпоративных информационных системах и базах данных для решения информационных, экономических и управленческих задач;

- способы обеспечения информационной безопасности и защиты информации в информационно-экономических системах;

- основные понятия и современные принципы работы с Интернет-технологиями в глобальных компьютерных сетях;

уметь:

- определять целесообразность и внедрять информационные технологии и автоматизированные информационные системы для решения экономических и управленческих задач;

- применять информационные технологии для решения управленческих и экономических задач;

- применять информационные технологии для обеспечения информационной безопасности и защиты информации в информационно-экономических системах;

- использовать Интернет-технологии в глобальных компьютерных сетях для решения информационных, экономических и управленческих задач;

владеть:

- методами управления информацией и методами управления с помощью информации деятельностью предприятия или организации для решения информационных, экономических и управленческих задач на основе информационных технологий и комплексной автоматизации экономических систем;

- навыками работы с программным обеспечением для работы с деловой информацией и основными информационными технологиями и автоматизированными информационными системами, используемыми для решения экономических и управленческих задач;

- навыками обеспечения информационной безопасности и защиты информации в информационно-экономических системах на основе антивирусных программ и межсетевых экранов;

- навыками работы с основами Интернет-технологий в глобальных компьютерных сетях.

1. ПОНЯТИЕ, СВОЙСТВА, КЛАССИФИКАЦИЯ, ЭТАПЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Введение в информационные технологии

Результаты научных исследований показывают, что информация и научные знания в последние годы играют все большую роль в жизни общества. Об информации сегодня говорят как о *стратегическом ресурсе общества*, определяющем уровень развития государства, его экономический потенциал и положение в мировом сообществе.

Во многих развитых странах мира сегодня активно идет процесс перехода от индустриального к информационному обществу. В этих условиях средства создания и использования информационных ресурсов в любой развитой стране должны быть на уровне современных требований. Такими средствами являются:

- научная методология, используемая в информационной сфере общества;
- программно-аппаратные средства информатизации;
- современные информационные технологии.

Указанные средства в последние годы все более широко используются практически во всех сферах социальной практики. Что же касается информационных технологий, то, повышая эффективность использования информационных ресурсов, они выступают не только как важнейший инструмент деятельности в информационной сфере общества, но также и как мощный *катализатор развития научно-технического прогресса*. Именно поэтому проблема развития и совершенствования информационных технологий сегодня занимает одно из приоритетных мест в стратегии научно-технического и социально-экономического развития передовых стран мира, является важным аспектом их национальной политики.

1.2. Определение “Информационная технология” и “Информационная система”

Информация – это сведения об окружающем мире (объектах, явлениях, событиях, процессах и т.д.), которые уменьшают имеющуюся степень неопределенности, неполноты знаний,

отчужденные от их создателя и ставшие сообщениями (выраженными на определенном языке в виде знаков, в том числе и записанными на материальном носителе), которые можно воспроизводить путем передачи людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств, вычислительных средств и т.д.).

Информационная технология (ИТ) – процесс, использующий совокупность средств и методов сбора, получения, накопления, хранения, обработки, анализа и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

В толковом словаре по информатике дается следующее определение: «***ИТ*** – совокупность методов, производственных процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации для снижения трудоемкости процессов использования информационных ресурсов, повышения их надежности и оперативности».

Информационные ресурсы – совокупность данных, представляющих ценность для организации (предприятия) и выступающих в качестве материальных ресурсов. К ним относятся файлы данных, документы, тексты, графики, знания, аудио- и видеоинформация.

Таким образом, ***цель применения ИТ*** – производство информации для ее анализа человеком и принятия на его основе решения по выполнению какого-либо действия, а также снижение трудоемкости использования информационных ресурсов.

Информационная система (ИС) – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Информационная технология является процессом, а информационная система – средой. Таким образом, информационная технология является более емким понятием, чем информационная система, т.е. может существовать и вне сферы информационной системы.

1.3. Составляющие и свойства информационных технологий

Информационные технологии практически могут реализовываться как в неавтоматизированном (традиционном или, по-другому, «бумажном»), так и в автоматизированном виде. Во втором случае Информационная технология базируется и зависит от технического, программного, информационного, методического и организационного обеспечения.

Техническое обеспечение – это персональный компьютер, оргтехника, линии связи, оборудование сетей.

Программное обеспечение, находящееся в прямой зависимости от технического и информационного обеспечения, реализует функции накопления, обработки, анализа, интерфейса с компьютером.

Информационное обеспечение – совокупность данных, представленных в определенной форме для компьютерной обработки.

Организационное и методическое обеспечение представляют собой комплекс мероприятий, направленных на функционирование компьютера и программного обеспечения для получения результата. Включает в себя:

- нормативно-методические материалы по подготовке и оформлению управленческих и иных документов в рамках конкретной функции обеспечения управленческой деятельности;
- инструктивные и нормативные материалы по эксплуатации технических средств, в том числе по технике безопасности работы и по условиям поддержания нормальной работоспособности оборудования;
- инструктивные и нормативно-методические материалы по организации работы управленческого и технического персонала в рамках конкретной информационной технологии обеспечения управленческой деятельности.

Основными ***свойствами*** информационной технологии являются:

- целесообразность;
- наличие компонентов и структуры;
- взаимодействие с внешней средой;
- целостность;
- развитие во времени.

1. *Целесообразность* – главная цель реализации информационной технологии состоит в повышении эффективности производства на базе использования современных ЭВМ, распределенной переработке информации, распределенных баз данных, различных информационных вычислительных сетей путем обеспечения циркуляции и переработки информации.

2. *Компоненты и структура:*

• функциональные компоненты – это конкретное содержание процессов циркуляции и переработки информации;

• структура информационной технологии – это внутренняя организация, представляющая собой взаимосвязи образующих ее компонентов, объединенных в две большие группы: опорную технологию и базу знаний:

Опорная технология – совокупность аппаратных средств автоматизации, системного (ОС, СУБД) и инструментального программного обеспечения (алгоритмические языки, системы программирования, языки спецификаций, технология программирования), на основе которых реализуются подсистемы хранения и переработки информации.

База знаний представляет собой совокупность знаний, хранящихся в памяти ЭВМ. База знаний представляет отображение предметной области. Она включает в себя базу данных (плановые задания, научно-техническая информация и т.п.).

3. *Взаимодействие с внешней средой* – взаимодействие информационной технологии с объектами управления, взаимодействующими предприятиями и системами, наукой, промышленностью программных и технических средств автоматизации.

4. *Целостность* – информационная технология является целостной системой, способной решать задачи, не свойственные ни одному из ее компонентов.

5. *Реализация во времени* – обеспечение динамичности развития информационной технологии, ее модификация, изменение структуры, включение новых компонентов.

ИТ играют важную стратегическую роль, которая быстро возрастает. Это объясняется преимуществами их использования:

• ИТ позволяют активизировать и эффективно использовать информационные ресурсы общества, что экономит другие виды

ресурсов – сырье, энергию, полезные ископаемые, материалы, оборудование, людские ресурсы, социальное время.

• ИТ реализуют наиболее важные, интеллектуальные функции социальных процессов.

• ИТ позволяют оптимизировать и во многих случаях автоматизировать информационные процессы в период становления информационного общества.

• ИТ обеспечивают информационное взаимодействие людей, что способствует распространению массовой информации.

• ИТ занимают центральное место в процессе интеллектуализации общества, в развитии системы образования, культуры, новых (экранных) форм искусства, в популяризации шедевров мировой культуры, истории развития человечества.

• ИТ играют ключевую роль в процессах получения, накопления, распространения новых знаний. Первое направление – ***информационное моделирование*** – позволяет проводить «вычислительный эксперимент» даже в тех условиях, которые невозможны в натуральном эксперименте из-за опасности, сложности, дороговизны. Второе направление, основанное на методах ***искусственного интеллекта***, позволяет находить решения плохо формализуемых задач, задач с неполной информацией, с нечеткими исходными данными. Третье направление – основано на методах ***когнитивной графики*** – совокупности приемов и методов образного представления условий задачи, которые позволяют сразу увидеть решение либо получить подсказку для его нахождения.

• ИТ позволяет реализовать методы информационного моделирования глобальных процессов, что обеспечивает возможность прогнозирования многих природных ситуаций, повышенной социальной и политической напряженности, экологических катастроф, крупных технологических аварий.

1.4. Классификация информационных технологий

Для того, чтобы правильно понять и оценить, грамотно разработать и использовать информационные технологии в различных сферах жизни общества необходима их предварительная классификация.

Классификация информационных технологий осуществляется, в основном, по тем или иным признакам, связанным с областью их

практического использования, т.е. из чисто прагматических соображений.

1. Классификация по назначению и характеру использования

- базовые (обеспечивающие) информационные технологии;
- прикладные (функциональные) информационные технологии.

Базовые информационные технологии представляют собой наиболее эффективные способы организации *отдельных фрагментов* тех или иных информационных процессов, связанных с преобразованием, хранением или же передачей определенных видов информации.

Информационные технологии базового типа могут быть классифицированы относительно классов задач, на которые они ориентированы. Базовые технологии базируются на совершенно разных платформах, что обусловлено различием видов компьютеров и программных сред, поэтому при их объединении на основе предметной технологии возникает проблема системной интеграции. Она заключается в необходимости приведения различных ИТ к единому стандартному интерфейсу.

Примерами таких технологий могут быть технологии *сжатия информации, ее кодирования и декодирования, распознавания образов* и т.п.

Характерным признаком базовых информационных технологий является то, что они не предназначены для непосредственной реализации конкретных информационных процессов, а являются лишь теми базовыми их компонентами, на основе которых и проектируются затем прикладные информационные технологии.

Основная задача ***прикладных информационных технологий*** – рациональная организация того или иного вполне конкретного информационного процесса. Осуществляется это путем адаптации к данному конкретному применению одной или нескольких базовых информационных технологий, позволяющих наилучшим образом реализовать отдельные фрагменты этого процесса.

Примером прикладной информационной технологии может служить технология ввода в ЭВМ речевой информации. С технологической точки зрения весь информационный процесс здесь разделяется на несколько последовательных этапов, на каждом из

которых используется своя базовая технология. Такими этапами в данном случае являются:

1. Аналого-цифровое преобразование речевого сигнала и ввод полученной цифровой информации в память ЭВМ. Базовой технологией здесь является *аналого-цифровое преобразование*, а реализуется эта технология, как правило, аппаратным способом при помощи специальных электронных устройств, характеристики которых заранее оптимизированы и хорошо известны проектировщикам.

2. Выделение в составе цифровой речевой информации отдельных фонем того языка, на котором произносилась речь, и отождествление их с типовыми "образами" этих фонем, хранящимися в памяти вычислительной системы. Базовой технологией здесь является *технология распознавания образов*.

3. Преобразование речевой информации в текстовую форму и осуществление процедур ее морфологического и синтаксического контроля. Базовыми технологиями здесь являются *процедуры морфологического и синтаксического контроля текста*, сформированного на основе анализа речевой информации, и внесение в него необходимых корректур, связанных с исправлением ошибок.

2. Классификация по предметной области

Предметная ИТ – набор программных средств для реализации типовых задач или процессов в определенной области. Например, пакет 1С-Бухгалтерия.

Информационные технологии могут обслуживать различные предметные области: бухгалтерский учет, управление персоналом, производственный менеджмент и пр.

3. Классификация по пользовательскому интерфейсу

Набор приемов взаимодействия пользователя с приложением называют ***пользовательским интерфейсом***. Пользовательский интерфейс включает три понятия: общение приложения с пользователем, общение пользователя с приложением и язык общения, который определяется разработчиком программного приложения. Пользовательский интерфейс зависит от интерфейса, обеспечиваемого операционной системой.

Классификация ИТ по типу пользовательского интерфейса позволяет говорить о системном и прикладном интерфейсе. И если последний связан с реализацией некоторых функциональных ИТ, то

системный интерфейс – это набор приемов взаимодействия с компьютером, который реализуется операционной системой или ее надстройкой. Современные операционные системы поддерживают командный, WIMP- и SILK.- интерфейсы. В настоящее время поставлена проблема создания общественного интерфейса (social interface).

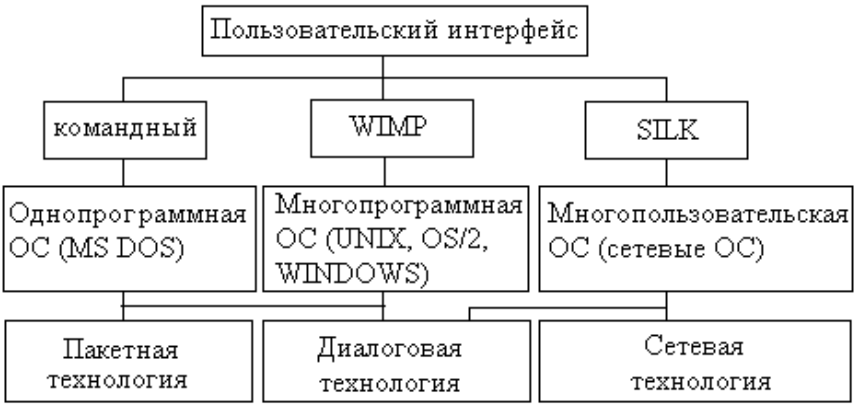


Рис. 1.1. Классификация ИТ по типу пользовательского интерфейса

Командный интерфейс – самый простой. Он обеспечивает выдачу на экран системного приглашения для ввода команды. Например, в операционной системе MS-DOS приглашение выглядит как C:\>, а в операционной системе UNIX – это обычно знак доллара.

WIMP-интерфейс расшифровывается как Windows (окно) Image (образ) Menu (меню) Pointer (указатель). На экране высвечивается окно, содержащее образы программ и меню действий. Для выбора одного из них используется указатель.

SILK-интерфейс расшифровывается – Speech (речь) Image (образ) Language (язык) Knowledge (знание). При использовании SILK-интерфейса на экране по речевой команде происходит перемещение от одних поисковых образов к другим по смысловым семантическим связям.

Общественный интерфейс будет включать в себя лучшие решения WIMP- и SILK-интерфейсов. Предполагается, что при использовании общественного интерфейса не нужно будет

разбираться в меню. Экранные образы однозначно укажут дальнейший путь. Перемещение от одних поисковых образов к другим будет проходить по смысловым семантическим связям.

4. Классификация по степени взаимодействия между собой

Информационные технологии различаются по степени их взаимодействия между собой. Они могут быть реализованы различными техническими средствами: дискетное и сетевое взаимодействие, а также с использованием различных концепций обработки и хранения данных: распределенная информационная база и распределенная обработка данных:

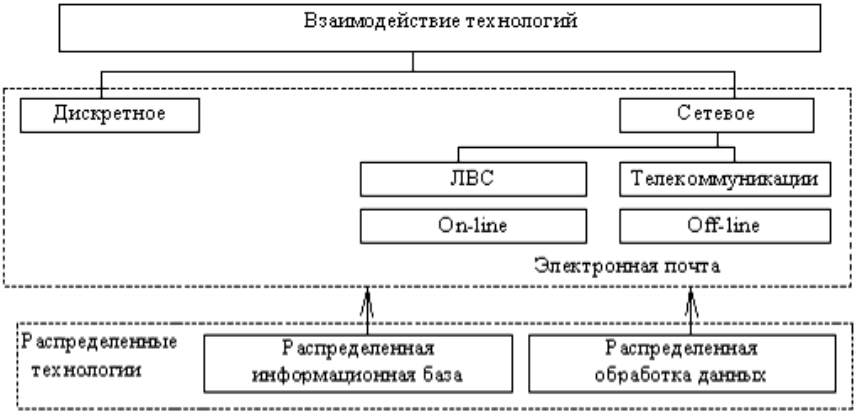


Рис. 1.2. Взаимодействие технологий

5. Классификация ИТ по типу обрабатываемой информации

Данная классификация (рис. 1.3) в известной мере условна, поскольку большинство этих ИТ позволяет поддерживать и другие виды информации. Так, в текстовых процессорах предусмотрена возможность выполнения примитивных расчетов, табличные процессоры могут обрабатывать не только цифровую, но и текстовую информацию, а также обладают встроенным аппаратом генерации графики. Однако каждая из этих технологий все-таки в большей мере акцентирована на обработке информации определенного вида.

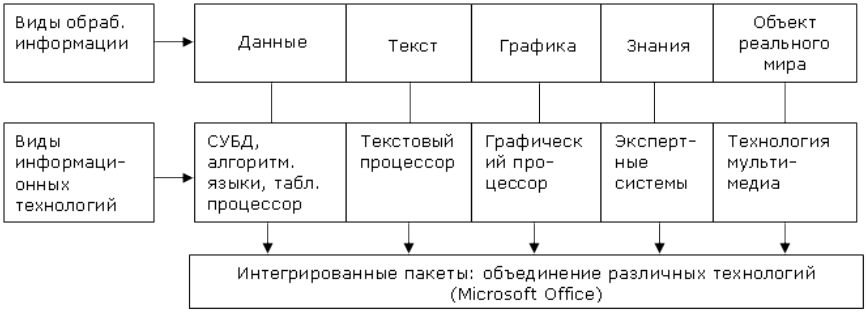


Рис. 1.3. Классификация ИТ по типу обрабатываемой информации

6. Классификация ИТ по платформе

Разнообразие технических средств и операционных систем вынудили разработчиков систем ввести понятие платформы. Платформа определяет тип оборудования и программного обеспечения, на которых можно установить покупаемую информационную технологию. Она имеет сложную структуру.

Главным компонентом платформы является тип ЭВМ, определяемый типом процессора: Macintosh, Atary, Sincler, Intel и т.д.

Следующим компонентом является операционная система, работающая на том или ином процессоре. Например, Windows NT работает на многих типах процессоров: Intel, MIPS, ALPHA, Power PC.

Многие ИТ не зависят от добавочного оборудования и наличия других программных средств. Их называют компьютерными ИТ. Например, к ним относятся текстовые, графические, табличные процессоры.

Часть ИТ зависит от добавочного оборудования. Например, сетевые ИТ зависят от сетевого оборудования: модемов, адаптеров, каналов связи и т.д. и программных средств, их обслуживающих.

Часть ИТ требует дополнительного оборудования и специальных программных средств его обслуживания. Например, в технологии мультимедиа используются приводы CD-ROM, видеокарты, звуковые карты и т.д. А так как технология мультимедиа может быть использована в сетях ЭВМ, она также зависит и от сетевого оборудования.

Новейшие ИТ представляют собой продукт интеграции различных ИТ. Поэтому их платформа зависит от всех структурных частей: типа процессора, работающей на нем ОС, типа дополнительного оборудования, поддерживающих это оборудование программных средств.

7. Классификация ИТ по типу носителя информации

Классифицируя информационную технологию по типу носителя информации, можно говорить о бумажной (входные и выходные документы) и безбумажной (сетевая технология, современная оргтехника, электронные деньги, документы) технологиях.

8. Классификация ИТ по степени типизации операций

Информационные технологии классифицируются *по степени типизации операций*: пооперационные и попредметные технологии. Пооперационная, когда за каждой операцией закрепляется рабочее место с техническим средством. Это присуще пакетной технологии. Попредметная технология подразумевает выполнение всех операций на одном рабочем месте, например, при работе на персональном компьютере, в частности, АРМ.

Существуют классификации ИТ и по другим признакам, например, по степени автоматизации задач управления, по способу построения сети ЭВМ и т.д.

1.5. Критерии эффективности ИТ

Функциональные критерии, значения которых характеризуют степень достижения при данной технологии тех желаемых характеристик информационного процесса, которые необходимы пользователю. Такими характеристиками могут быть, например:

- объемно-временные характеристики реализуемого информационного процесса (скорость передачи данных, объем памяти для хранения информации и т. п.);

- надежностные характеристики реализации информационного процесса (вероятность правильной передачи или преобразования информации, уровень ее помехозащищенности и др.):

- параметры, характеризующие степень достижения основного конечного результата информационного процесса, реализуемого при помощи данной технологии (правильность распознавания речи или

изображения, качество формируемой графической информации и др.).

Ресурсные критерии, значения которых характеризуют количество и качество различного вида ресурсов, необходимых для реализации данной информационной технологии. Такими ресурсами могут быть:

- материальные ресурсы (инструментально-технологическое оборудование, необходимое для успешной реализации данной технологии);
- энергетические ресурсы (затраты энергии на реализацию информационного процесса при данной технологии);
- людские ресурсы (количество и уровень подготовки персонала, необходимого для реализации данной технологии);
- временные ресурсы (количество времени, необходимого для реализации информационного процесса при данной технологии его организации);
- информационные ресурсы (состав данных и знаний, необходимых для успешной реализации информационного процесса).

1.6. Этапы развития информационных технологий

История информационных технологий берёт свое начало задолго до возникновения современной дисциплины информатика, появившейся в 20-м веке. Информационные технологии связаны с изучением методов и средств сбора, обработки и передачи данных с целью получения информации нового качества о состоянии объекта, процесса или явления.

Ввиду возрастания потребностей человечества в обработке всё большего объёма данных, средства получения информации совершенствовались от самых ранних механических изобретений до современных компьютеров. Также в рамках информационных технологий идёт развитие сопутствующих математических теорий, которые сейчас формируют современные концепции.

Информационные технологии активизируют и эффективно используют информационные ресурсы общества (научные знания, открытия, изобретения, технологии, передовой опыт), что позволяет получить существенную экономию других видов ресурсов – сырья, энергии, полезных ископаемых, материалов и оборудования,

людских ресурсов, социального времени. К настоящему времени ИТ прошли несколько эволюционных этапов, смена которых определяется главным образом развитием научно-технического прогресса, появлением новых технических средств переработки информации. Основным техническим средством технологии переработки информации является персональный компьютер, который существенно повлиял как на концепцию построения и использования технологических процессов, так и на качество информации, получаемой после обработки.

Существует несколько точек зрения на развитие информационных технологий, которые определяются различными признаками деления.

Признак деления – вид задач и процессов обработки информации.

1 этап. (60-70 гг.) – обработка данных в вычислительных центрах в режиме коллективного пользования. Основным направлением развития информационной технологии являлась автоматизация рутинных действий человека.

2 этап (с 80-х гг.) – создание информационных технологий, направленных на решение стратегических задач (перспективных, долгосрочных).

Признак деления – проблемы, стоящие на пути информатизации общества.

1 этап (до конца 60-х гг.) характеризуется проблемой обработки больших объемов данных в условиях ограниченных возможностей аппаратных средств.

2 этап (до конца 70-х гг.) связывается с распространением ЭВМ серии IBM/360/ Проблема этого этапа – отставание программного обеспечения от уровня развития аппаратных средств.

3 этап (с начала 80-х гг.) – компьютер становится инструментом непрофессионального пользователя, а информационные технологии - средством поддержки принятия его решений.

4 этап (с начала 90-х гг.) – создание современной технологии межорганизационных связей и информационных систем.

Признак деления – преимущество, которое приносит компьютерная технология.

1 этап (с начала 60-х гг.) характеризуется довольно эффективной обработкой информации при выполнении рутинных

операций с ориентацией на централизованное коллективное использование ресурсов вычислительных центров.

2 этап (с середины 70-х гг.) связан с появлением персональных компьютеров. Изменился подход к созданию информационных систем – ориентация смещается в сторону индивидуального пользователя для поддержки принимаемых им решений. На этом этапе используется как централизованная обработка данных, характерная для первого этапа, так и децентрализованная, базирующаяся на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.

3 этап (с начала 90-х гг.) связан с понятием анализа стратегических преимуществ в бизнесе и основан на достижениях телекоммуникационной технологии распределенной обработки информации. Информационные системы имеют своей целью не просто увеличение эффективности обработки данных и помощь управленцу. Соответствующие информационные технологии должны помочь достичь намеченных целей.

Признак деление – виды инструментария технологии.

1 этап (до второй половины XIX в) – “ручная” информационная технология, инструментарий которой составляли: перо, чернильница, книга. Коммуникация осуществлялась ручным способом путем отправки по почте писем, пакетов, депеш. Основная цель технологии – представление информации в нужной форме.

2 этап (с конца XIX в) – “механическая” технология, инструментарий которой составляли: пишущая машинка, телефон, оснащенная более совершенными средствами доставки почта. Основная цель технологии - представление информации в нужной форме более удобными средствами.

3 этап (40-60 гг. XX в) – “электрическая” технология, инструментарий которой составляли: большие ЭВМ и соответствующее программное обеспечение, электрические пишущие машинки, ксероксы, портативные диктофоны.

Изменяется цель технологии. Акцент в информационной технологии начинает перемещаться с формы представления информации на формирование ее содержания.

4 этап (с начала 70-х гг.) – “электронная” технология, основным инструментарием которой становятся большие ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ) и информационно-поисковые системы (ИПС), оснащенные

широким спектром базовых и специализированных программных комплексов. Центр тяжести технологии еще более смещается на формирование содержательной стороны информации для управленческой среды различных сфер общественной жизни, особенно на организацию аналитической работы. Был приобретен опыт формирования содержательной стороны управленческой информации и подготовлена профессиональная, психологическая и социальная база для перехода на новый этап развития технологии.

5 этап (с середины 80-х гг.) – “компьютерная” (“новая”) технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов разного назначения. На этом этапе происходит процесс персонализации АСУ, который проявляется в создании систем поддержки принятия решений определенными специалистами. Подобные системы имеют встроенные элементы анализа и интеллекта для разных уровней управления, реализуются на персональном компьютере и используют телекоммуникации. Начинают широко использоваться в различных областях глобальные и локальные компьютерные сети.

1.7. Контрольные вопросы

1. Основные понятия информационных технологий
2. Составляющие ИТ и их характеристики
3. Основные свойства ИТ
4. Направления классификации ИТ
5. Классификация ИТ по пользовательскому интерфейсу
6. Основные критерии эффективности ИТ
7. Этапы развития ИТ

2. ИНФОРМАЦИОННАЯ МОДЕЛЬ ПРЕДПРИЯТИЯ. АВТОМАТИЗАЦИЯ ДЕЛОПРОИЗВОДСТВА И ДОКУМЕНТООБОРОТА

2.1. Информационные потоки на предприятии

Любая организация существует в некоторой внешней среде. Эта же организация порождает свою внутреннюю среду. В соответствии с источником возникновения информации по отношению к организации имеется внутренняя и внешняя информация, составляющая в целом информационные ресурсы этой организации.

Рассмотрим более подробно, что может представлять собой внешняя информация по целевому назначению.

1. Рыночная информация. Обширнейшая составляющая внешней информации, объединяющая очень разнообразные сведения, от очень «узкоспециализированных» до весьма общих, касающихся, например, мнений аналитиков о мировых рыночных тенденциях какого-либо товара. Рыночная информация влияет на маркетинговую деятельность фирм и разработку новых товаров и услуг.

2. Информация о конкурентах. Представляет собой одну из составляющих рыночной информации, но настолько важную, что обычно рассматривается особо. Эта информация может касаться используемых конкурентами производственных технологий, маркетинговой политики, специалистов, поставщиков сырья и т.п.

3. Макроэкономическая и геополитическая информация (эта информация может требоваться фирмам для долгосрочного стратегического планирования).

4. Информация о поставщиках: издержки, надежность, качество и время доставки.

5. Внешняя финансовая информация: валютные курсы, динамика курсов акций, движение на рынке капитала и т.д.

6. Информация из государственных органов и органов управления: законы, постановления, сообщения налоговых органов и пр.

Внутренняя деловая среда формируется совокупностью структурных подразделений предприятия с работающими там людьми, а также технологическими, социальными, экономическими

и другими отношениями между ними. Они порождают плановую, контрольную, учетную, научно-техническую, аналитическую и другую информацию.

В отличие от внешней информации информация внутренней среды, как правило, точная и достаточно полно отражает финансово-хозяйственное состояние предприятия. Обработка внутренней информации обычно осуществляется с помощью стандартных формализованных процедур.

По целевому назначению внутренняя информация может быть разделена на следующие категории.

1. Информация о производстве и сбыте: издержки, производительность труда, качество продукции, отходы производства, поставки, методы и каналы сбыта и т.д.

2. Информация о трудовых ресурсах: уровень квалификации и обучение персонала, расходы на кадровое обеспечение, моральное состояние сотрудников.

3. Внутренняя финансовая информация: финансовые показатели работы фирмы по данным бухгалтерских балансов и другой отчетности.

Бизнес-информация может быть получена через официальные и неофициальные информационные каналы; характер способа получения бизнес-информации может быть как активным (в этом случае речь идет о поиске источников информации), так и пассивным (здесь подразумевается анализ информации из уже известных источников). Для практических целей обычно используют различные комбинации источников и способов получения информации (таблица).

Источники и способы получения информации

		Информационные каналы (источники)	
		Официальные (формальные)	Неофициальные (неформальные)
Характер способа получения информации	Активный	Поставщики коммерческой информации; торговые ассоциации; правительственные учреждения; библиотеки; коммерческие учреждения и др.	Торговые ярмарки, конференции, поставщики, заказчики и т.п.
	Пассивный	Система правового обеспечения; банки, бухгалтеры, инструкции, информационные бюллетени (от торговых организаций и пр.)	Знакомства, реклама и т.д.

В процессе информационного поиска все больше фирм ориентируются на использование средств поиска в режиме он-лайн, таких, как поисковые системы в Интернете.

2.2. Моделирование бизнес-процессов предприятия

В настоящее время в России резко возрос интерес к общепринятым на Западе стандартам менеджмента, однако, для их комплексной реализации на предприятии необходимо предварительно провести исследование бизнес-процессов (как правило, путем моделирования бизнес-процессов), построить информационную модель предприятия, реализовать перепроектирование (реинжиниринг бизнес-процессов).

Для решения задач моделирования сложных систем существуют хорошо отработанные методики:

- объектно-ориентированное моделирование;
- ***CASE***- технологии;
- имитационное моделирование и другие.

Большая часть программных средств, реализующих ту или иную методику моделирования бизнес-процессов, базируются на стандарте, реализованном в методологии ***IDEF***. Часто также используются:

- методика структурного анализа и структурного проектирования ***SA/SD*** – реализует так называемый подход функциональной декомпозиции (при моделировании сложные системы разбиваются на составные части, каждая из которых рассматривается отдельно от других – ***декомпозиция***);
- методика ***SADT*** – использует систему, похожую на IDEF, и также используется для описания функций и структур данных на основе декомпозиции.

Для реализации вышеприведенных методик используются в основном следующие средства:

- DFD (data flow diagrams) – диаграммы потоков данных;
- ERD (entity relationship diagrams) – диаграммы «сущность-связь»;
- STD (state transition diagrams) - диаграммы переходов состояний;
- Сети Петри их расширения (стохастические сети Петри, раскрашенные сети Петри и т.д.).

Стандарты IDEF

В настоящий момент к семейству IDEF можно отнести следующие стандарты:

- IDEF0 – методология функционального моделирования. С помощью наглядного графического языка IDEF0, изучаемая система предстает перед разработчиками и аналитиками в виде набора взаимосвязанных функций. Как правило, моделирование средствами IDEF0 является первым этапом изучения любой системы;

- IDEF1 – методология моделирования информационных потоков внутри системы, позволяющая отображать и анализировать их структуру и взаимосвязи (является дальнейшим развитием графического языка описания функциональных систем SADT (Structured Analysis and Design Teqnique);

- IDEF1X (IDEF1 Extended) – методология построения реляционных структур. IDEF1X относится к типу методологий “Сущность-взаимосвязь” (ER – Entity-Relationship) и, как правило, используется для моделирования реляционных баз данных, имеющих отношение к рассматриваемой системе;

- IDEF2 – методология динамического моделирования развития систем. В связи с весьма серьезными сложностями анализа динамических систем от этого стандарта практически отказались, и его развитие приостановилось на самом начальном этапе. Однако в настоящее время присутствуют алгоритмы и их компьютерные реализации, позволяющие превращать набор статических диаграмм IDEF0 в динамические модели, построенные на базе “раскрашенных сетей Петри” (CPN – Color Petri Nets);

- IDEF3 – методология документирования процессов, происходящих в системе, которая используется, например, при исследовании технологических процессов на предприятиях. С помощью IDEF3 описываются сценарий и последовательность операций для каждого процесса. IDEF3 имеет прямую взаимосвязь с методологией IDEF0 – каждая функция (функциональный блок) может быть представлена в виде отдельного процесса средствами IDEF3;

- IDEF4 – методология построения объектно-ориентированных систем. Средства IDEF4 позволяют наглядно отображать структуру объектов и заложенные принципы их взаимодействия, тем самым

позволяя анализировать и оптимизировать сложные объектно-ориентированные системы;

- IDEF5 – методология онтологического исследования сложных систем. С помощью методологии IDEF5 онтология системы может быть описана при помощи определенного словаря терминов и правил, на основании которых могут быть сформированы достоверные утверждения о состоянии рассматриваемой системы в некоторый момент времени. На основе этих утверждений формируются выводы о дальнейшем развитии системы и производится её оптимизация.

CASE-технологии

CASE-средства (Computer-Aided Software/System Engineering) появились в первую очередь для проектирования информационных систем (ИС). Но, так как накопленный опыт оказался удачным, они начали применяться также для реинжиниринга бизнес-процессов.

Интегрированное CASE-средство содержит следующие компоненты:

- репозиторий, являющийся основой CASE-средства. Он должен обеспечивать хранение версий проекта и его отдельных компонентов синхронизацию поступления информации от различных разработчиков при групповой разработке, контроль метаданных на полноту и не противоречивость;
- графические средства анализа и проектирования, обеспечивающие создание и редактирование иерархически связанных диаграмм, образующих модели;
- средства разработки приложений;
- средства конфигурационного управления;
- средства документирования;
- средства тестирования;
- средства управления проектом;
- средства реинжиниринга.

На сегодняшний день российский рынок программного обеспечения располагает широким спектром CASE-средств: Erwin+Bpwin, "CASE.Аналитик", Designer/2000 и т.д.

2.3. Автоматизация документооборота

Любой электронный документ должен быть создан посредством или приложения (текстовый редактор, электронные таблицы и т.п.), или специальным инструментом, входящим в СЭД (система электронного документооборота), для приведения документа, находящегося в неприемлемом для системы виде, в стандартизированный вид. Отсюда вырисовываются две основные задачи при организации работы с документами:

- обеспечение взаимодействия средств создания электронных документов и средств администрирования документов, т.е. какими бы приложениями ни создавался документ, в СЭД должны быть средства вовлечения его в электронный документооборот;
- обеспечение перевода внешних документов в стандарт системы.

Под понятием внешних документов подразумеваются бумажные и электронные документы, созданные вне рамок СЭД. В случае бумажных документов, а также фото-, звуковых и прочих "аналоговых" документов необходима их оцифровка, т. е. перевод в адекватную электронную форму.

Система электронного документооборота должна поддерживать все типы документов, обращающихся на предприятии, при этом обеспечить безболезненный переход с имеющихся систем, решающих локальные задачи, на единую систему электронного документооборота предприятия.

При выборе системы нужно придерживаться принципа поддержки максимально возможного количества платформ (операционных систем). Необходима поддержка многоплатформенных серверов баз данных, таких как Sybase, Oracle, Informix. Выбираемая система должна быть открыта для эксплуатируемых и новых приложений.

Обычно внедрение новых систем выполняется поэтапно. Поэтому выбираемая система должна быть модульной. Каждый из модулей обеспечивает решение определенных задач. При этом не должно составлять труда их включение в работающую систему. Модули по возможности должны быть независимы друг от друга.

Потребительские свойства системы электронного документооборота могут быть расширены за счет ряда дополнительных функций, многие из которых являются

обязательными при организации тендеров (конкурсов) на приобретение системы:

- интеграция со средствами пакета MS Office;
- автоматизированная регистрация документа, поступившего по электронной почте;
- поддержка средств электронной цифровой подписи;
- возможность задания логических связей между документами;
- полнотекстовый поиск по электронным копиям документов;
- разделение прав доступа пользователей различным категориям документов;
- Web-доступ к документационной базе данных (доступ через Интернет);
- ведение реестров рассылки;
- возможность проектирования произвольных отчетных форм без привлечения фирмы-разработчика;
- ведение электронных архивов документов;
- поддержка средств криптографической защиты информации.

В ряде зарубежных систем обеспечивается поддержка специальных функций, прежде всего связанных с лингвистическим анализом текстов документов:

- автоаннотирование – автоматическое составление аннотации документа по его полному тексту;
- авторубрицирование – автоматическое отнесение документа к той или иной тематической рубрике;
- автосвязывание – автоматическая установка гиперссылок между документами;
- семантический анализ, результатом которого может быть указание пользователю о недостаточности информации для успешного поиска документа в дальнейшем;
- формирование связных отчетов по заданной тематике на базе архива хранимых документов (так называемое “копание данных”).

Система электронного документооборота, отвечающая перечисленным принципам, состоит из трех частей: системы управления документами, системы массового ввода бумажных документов, системы автоматизации деловых процессов.

Система управления документами должна обеспечить интеграцию с приложениями. Это сложная работа, но ее достоинство в том, что сохраняются принятые на предприятии виды документов.

Следующей задачей является обеспечение хранения документов на разных носителях (дисках, стримерах и т.д.). К тому же надо обеспечить быстрый поиск и доступ к различным устройствам хранения информации.

Вторую часть электронного документооборота составляет ***система массового ввода*** бумажных документов. Эта система предназначена для массового ввода документов архива и перевода их в электронный вид, например, путем использования сканера и распознающих программ (класса OCR – Optical Character Recognition) типа FineReader.

После того как документ распознан, он поступает в систему управления документами, где проводится его индексация.

Третья часть электронного документооборота – ***система автоматизации деловых процессов*** (АДП). Она предназначена для моделирования деятельности каждого сотрудника, работающего с электронным документооборотом.

По оценкам аналитиков при использовании электронного документооборота рост производительности сотрудника увеличивается на 25-50 %, сокращается время обработки одного документа более чем на 75 % и уменьшаются расходы на оплату площади для хранения документов на 80 %.

Классификация систем электронного документооборота

Классификация СЭД возможна в зависимости от специфических задач, определенной «ниши», занимаемой в рамках общей системы документооборота. Особенности таких продуктов обусловлены специфическими концепциями и моделями бизнес-процессов предприятия, что является основой для автоматизации различных областей делопроизводства. В этом случае эксперты выделяют такие группы решений, как системы WorkFlow (технология автоматизации деловых процессов), системы делопроизводства, электронные архивы документов, системы коллективной обработки документов и комплексные системы управления документами.

Термин ***WorkFlow*** характеризует системы, направленные на автоматизацию большого числа бизнес-процессов компании, при этом удельный вес каждого из них невелик. WorkFlow позволяет работать с такими бизнес-процессами, контент которых

подвергается постоянным изменениям и дополнениям. Важной особенностью является возможность работы с неструктурированными данными.

Данные системы позволяют строго регламентировать направления документопотока в зависимости от типа документа и значений его реквизитов, автоматически направляя документ определенному исполнителю при возникновении заранее сформулированных условий.

Системы делопроизводства – это автоматизированные системы построения и контроля за выполнением потоков документов в соответствии с представлением заданной логики делопроизводства в программном обеспечении. То есть речь идет о создании документов в потоковом режиме с возможностью слабой или жесткой маршрутизации и отслеживанием жизненного цикла каждого документа. Системы делопроизводства, как правило, ориентированы на отдельные сферы применения: финансы, производство, управление продажами, хотя отчетность, генерируемая ими, пронизывает всю организационную структуру предприятия.

Электронные архивы представляют собой интегрированные в информационную систему предприятия систематизированные каталоги корпоративных документов.

Системы коллективной обработки документов предполагают поддержку совместной работы с документом, включая разработку маршрутов движения документа и описание сценария движения, определения круга лиц, причастных к работе с документом, установку уровня их прав и полномочий.

Комплексные системы синтезируют функции отдельных приложений и подсистем и подразумевают комплексную автоматизацию бизнес-процессов предприятия.

Существует также расширенная классификация СЭД:

СЭД, ориентированные на автоматизацию бизнес-процессов (business process EDM), используются для специфических вертикальных и горизонтальных приложений. EDMS-системы обеспечивают полный жизненный цикл работы с документами, включая работу с образами, управление записями и потоками работ, управление содержимым.

Корпоративные СЭД (enterprise-centric EDM) обеспечивают корпоративную инфраструктуру (доступную всем корпоративным

пользователям) для создания документов, коллективной работы над ними и их публикации. Базовые функции корпоративных СЭД аналогичны функциям СЭД, ориентированным на бизнес-процессы.

Системы управления контентом (Content Management Systems) обеспечивают создание, доступ и управление контентом, доставку содержимого.

Системы управления информацией (Information Management Systems) или порталы обеспечивают агрегирование информации, управление информацией и ее доставку через Internet/intranet/extranet.

Системы управления изображениями/образами (Imaging Systems) осуществляют конвертацию отсканированной с бумажных носителей информации и микрофильмов в электронную форму. В число базовых функций стандартной системы обработки изображений входят: сканирование, хранение, ряд возможностей по поиску изображений и др.

Системы управления потоками работ (WorkFlow Management Systems). Системы данного типа предназначены для обеспечения маршрутизации потоков работ любого типа (определения путей маршрутизации файлов) в рамках корпоративных структурированных и неструктурированных бизнес-процессов. Они используются для повышения эффективности и степени контролируемости корпоративных бизнес-процессов.

Классификацию СЭД можно дополнить также ***системами управления корпоративными электронными записями***.

Российский рынок систем автоматизации делопроизводства

В зависимости от применяемых технологий, аналитики РБК предлагают следующее деление представленных на российском рынке СЭД на группы:

1. Системы западного производства, среды разработок.
2. Российские системы, в основе которых лежит Lotus Domino/Notes.
3. Полностью российские разработки.

В первой группе на российском рынке представлено только три западные системы: Documentum, DOCS Open/DOCSFusion и Lotus Domino.Doc.

Ко второй группе относятся такие решения, как CompanyMedia и OfficeMedia («ИнтерТраст»), БОСС-Референт («АйТи»), «ЗОЛУШКА» (НТЦ ИРМ), «Эскадо Интерпроком» (ЛАН). Аналитики отмечают популярность на российском рынке продуктов на основе Lotus Domino/Notes.

Все остальные системы, представленные в России, можно отнести к третьей группе, в том числе:

- DocsVision – Digital Design
- LanDocs – Ланит
- Optima-WorkFlow – Optima и т.п.

Следует отметить, что пока именно российские системы, к которым можно отнести и системы, основанные на Lotus Domino/Notes, контролируют большую часть рынка. Именно эти программные продукты отвечают особенностям российского документооборота и делопроизводства. Западные системы пока занимают менее 10% российского рынка.

Электронная цифровая подпись

До сих пор достаточно актуальна проблема правового режима электронной копии документа. Техническое решение этой проблемы существует – любые данные, представленные в электронной форме, могут быть зашифрованы и снабжены *электронной цифровой подписью*.

Электронная цифровая подпись (ЭЦП) – это последовательность символов (кодов), которая позволяет однозначно связать автора документа, содержание документа и владельца ЭЦП. Использование электронной подписи имеет характерные недостатки – необходимо специальное техническое (средства криптографии, передачи данных и т.п.), организационное и правовое обеспечение.

Чтобы последовательность символов, представляющих сообщение, могла однозначно идентифицировать ее автора, необходимо, чтобы она обладала уникальными признаками, известными только отправителю и получателю сообщения. Это достигается применением средств шифрования (более общий термин – *криптография*). Если обе стороны используют один и тот же метод шифрования сообщений, известный только им, то мы можем говорить о том, что они общаются в *защищенном канале*.

Под *шифром* понимается совокупность процедур и правил криптографических преобразований, используемых для зашифрования и расшифрования информации по ключу шифрования.

Метод шифрования – это формальный алгоритм, описывающий порядок преобразования исходного сообщения в результирующее.

Ключ шифрования – это набор параметров (данных), необходимых для применения метода. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

В состав ЭЦП можно включить специальные данные, характеризующие само сообщение, чтобы исключить возможность внесения в него изменений в канале связи (любой вид транспортировки). Для этого используется понятие *дайджеста сообщения*.

Дайджест сообщения – это уникальная последовательность символов, однозначно соответствующая содержанию сообщения. Обычно дайджест имеет фиксированный размер, например 128 или 168 бит, который не зависит от длины самого сообщения. Дайджест сообщение вставляется в состав ЭЦП вместе со сведениями об авторе и шифруется вместе с ними.

Однако такой механизм нельзя считать удовлетворительным, поскольку в нем нет однозначного соответствия между текстом сообщения и величиной контрольной суммы. Можно предложить алгоритм, который позволит по известной контрольной сумме создать новое сообщение, отличное от исходного, но имеющее ту же контрольную сумму.

Современной математике известны специальные функции, не обладающие свойством обратимости. Они позволяют из одной последовательности чисел (из одного сообщения) получить другую последовательность (другое сообщение) таким образом, что обратное преобразование невозможно. Такие функции, используемые в криптографии, называют *хэш-функциями*.

Преобразование шифрования может быть симметричным или ассиметричным относительно преобразования расшифрования. Соответственно различают:

- симметричные криптосистемы шифрования (с единым ключом);

- ассиметричные криптосистемы шифрования (с двумя ключами);

- комбинированные криптосистемы шифрования.

В *симметричной криптосистеме шифрования* используется один и тот же ключ для зашифрования и расшифрования информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение.

Соответственно с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете.

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечиваются как конфиденциальность и подлинность, так и целостность передачи информации.

Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например, дискете или смарт-карте; обязательно принятие мер, обеспечивающих недоступность персонального ключевого носителя кому-либо, кроме его владельца.

Ассиметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие ассиметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и её последующего расшифрования используются различные ключи:

- *открытый ключ* используется для шифрования информации;

- *закрытый ключ* (секретный ключ) используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа.

Так, закрытый ключ мы и получатель храним у себя, а открытый мы и получатель можем спокойно передавать кому угодно. Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ из открытого ключа. Поэтому открытый ключ может свободно передаваться по каналам связи. Итого, мы используем открытый ключ получателя для шифрования, а получатель, в свою очередь, использует свой закрытый ключ для расшифровывания.

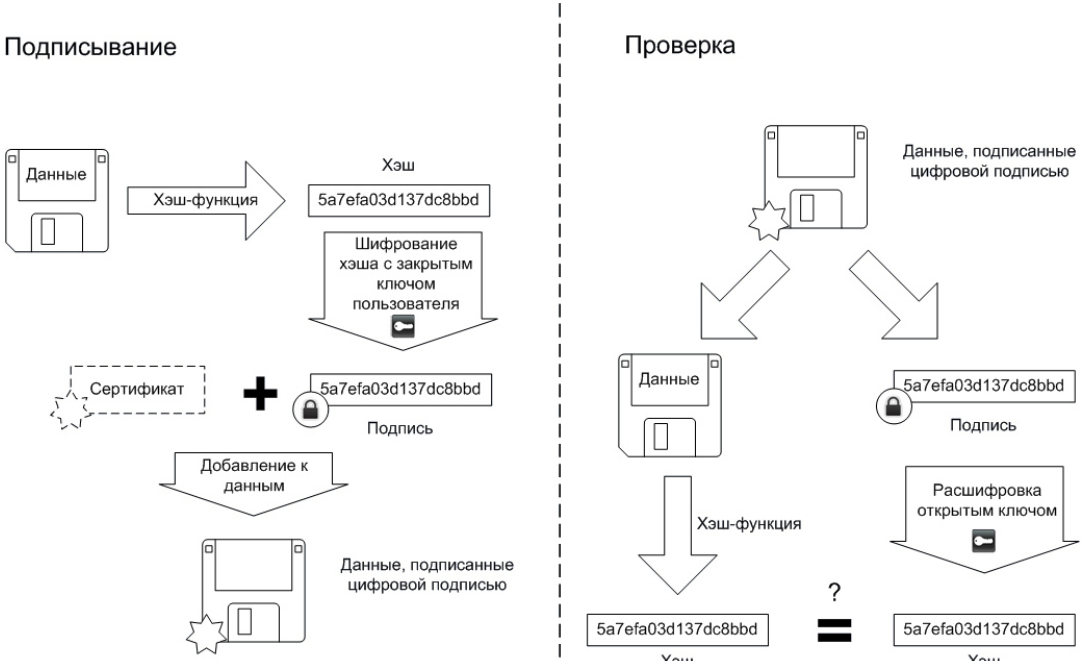
Преимуществом ассиметричных криптографических систем перед симметричными криптосистемами является то, что в данном случае решена сложная проблема распределения ключей между пользователями.

Однако ассиметричное шифрование существенно медленнее симметричного, поскольку при шифровании и расшифровке используются весьма ресурсоёмкие операции. Кроме этого, сами ключи для данных операций существенно длиннее аналогичных для операций симметричного шифрования, так как требуется максимально обезопасить закрытый ключ от подбора по открытому (нет математического доказательства необратимости используемых в ассиметричных алгоритмах функций). А значит, большие объемы информации данным способом шифровать просто невыгодно.

Анализ рассмотренных выше особенностей симметричных и ассиметричных криптографических систем показывает, что при совместном использовании (*комбинированной криптосистеме шифрования*) они эффективно дополняют друг друга, компенсируя недостатки.

Так, например, достаточно большой объем данных мы зашифруем по первому способу, а чтобы донести ключ, с помощью которого мы их зашифровали, до получателя, мы сам ключ зашифруем по второму способу. Тогда и получим, что хоть асимметричное шифрование и медленное, но объем зашифрованных данных (то есть ключа, на котором зашифрованы большие данные) будет маленьким, а значит, расшифровывание пройдет достаточно быстро, и дальше уже в дело вступит более быстрое симметричное шифрование.

Или, к примеру, исходное сообщение обрабатывается *хэш-функцией*, после чего образуется некий *хэш-код*. Он так же уникален для данного сообщения, как отпечатки пальцев уникальны для человека (хэш-функция обладает свойством необратимости). Это и есть *дайджест сообщения*. Его нередко называют *отпечатком*, или *оттиском*, по аналогии с отпечатками пальцев. Его также иногда называют *электронной печатью*, или *штампом*. Дайджест сообщения присоединяется к электронной подписи и далее является ее составной частью.



Алгоритм подписи и проверки данных

Принимающая сторона расшифровывает сообщение, проверяет электронную подпись с помощью своей половины ключа, затем обрабатывает сообщение той же хэш-функцией, что и отправитель, после чего сличает полученный дайджест с тем, который содержался в подписи. Если дайджесты совпали, значит, сообщение не подвергалось изменениям в канале связи.

2.4. Контрольные вопросы

1. Классификация информационных потоков на предприятии
2. Характеристика источников бизнес-информации
3. Структура стандартов семейства IDEF
4. Применение CASE-технологий для моделирования бизнес-процессов
5. Основные задачи при организации работы с документами
6. Принципы выбора системы электронного документооборота
7. Структура систем электронного документооборота
8. Классификация систем электронного документооборота
9. Характеристика систем класса WorkFlow
10. Российский рынок систем электронного документооборота
11. Структура и методы применения электронной цифровой подписи
12. Структура и механизм использования дайджеста сообщения

3. НАПРАВЛЕНИЯ АВТОМАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

3.1. «Лоскутная» автоматизация на основе автоматизированных рабочих мест

В последние годы возникла концепция распределенных систем управления, где предусматривается локальная обработка информации. Для реализации идеи распределенного управления необходимо создание для каждого уровня управления и каждой предметной области автоматизированных рабочих мест (АРМ) на базе профессиональных персональных ЭВМ.

Автоматизированное рабочее место (АРМ), или в зарубежной терминологии, “рабочая станция”, представляет собой место пользователя специалиста – той или иной профессии, оборудованное средствами, необходимыми для автоматизации выполнения им определенных функций. Такими средствами, как правило, является ПК, дополняемый по мере необходимости другими вспомогательными электронными устройствами, а именно: печатающими устройствами, оптическими сканирующими устройствами или считывателями штрихового кода, устройствами графики, средствами сопряжения с другим АРМ и с ЛВС и т.д.

При этом основным назначением АРМ можно считать децентрализованную автоматизированную обработку информации на рабочих местах, использование соответствующих “своих” баз данных при одновременной возможности вхождения в локальные сети АРМ и ПК, а иногда и в глобальные вычислительные сети, включающие мощные ЭВМ.

Классификация АРМ

Первым этапом проектирования АРМ должно быть определение конкретного типа разрабатываемого продукта.

С учетом областей применения возможна классификация АРМ по функциональному признаку:

1. АРМ административно-управленческого персонала.
2. АРМ проектировщика аппаратуры, автоматизированных систем управления и т.д.

3. АРМ специалиста в области экономики, математики, физики, и т. д.

4. АРМ производственно-технологического назначения.

Важным классификационным признаком АРМ является режим его эксплуатации, по которому выделяются ***одиночный***, ***групповой*** и ***сетевой*** режимы эксплуатации.

В первом случае АРМ реализуется на обособленной ПЭВМ, все ресурсы которой находятся в монопольном распоряжении пользователя. Такое рабочее место ориентировано на решение нестандартных, специфических задач.

При групповом режиме эксплуатации на базе одной ЭВМ реализуется несколько рабочих мест, объединенных по принципу административной или функциональной общности. Групповой режим эксплуатации обычно используется для организации распределенной обработки данных в пределах отдельного подразделения или организации для обслуживания стабильных групп специалистов и руководителей.

Сетевой режим эксплуатации АРМ объединяет достоинства первого и второго. Здесь каждое АРМ строится на базе одной ЭВМ, но в то же время имеется возможность использовать общие ресурсы вычислительной сети.

Другим подходом к классификации АРМ является их систематизация по видам решаемых задач. Возможны следующие группы АРМ:

1. Для решения информационно-вычислительных задач.
2. Задач подготовки и ввода данных.
3. Информационно-справочных задач.
4. Задач бухгалтерского учета.
5. Задач статистической обработки данных.
6. Задач аналитических расчетов.

Принципы конструирования АРМ

При конструировании АРМ необходимо учитывать следующие принципы:

1. Максимальная ориентация на конечного пользователя, достигаемая созданием инструментальных средств адаптации АРМ к уровню подготовки пользователя, возможностей его обучения и самообучения.

2. Формализация профессиональных знаний, т.е. возможность предоставления с помощью АРМ самостоятельно автоматизировать новые функции и решать новые задачи в процессе накопления опыта работы с системой.

3. Проблемная ориентация АРМ на решение определенного класса задач, объединенных общей технологией обработки информации, единством режимов работы и эксплуатации.

4. Модульность построения, обеспечивающая сопряжение АРМ с другими элементами системы обработки информации, а также модификацию и наращивание возможностей АРМ без прерывания его функционирования.

5. Эргономичность, т.е. создание для пользователя комфортных условий труда и дружественного интерфейса общения с системой.

Типовая структура АРМ

Структурно АРМ включает функциональную и обеспечивающую части:

Рис. 3.1. Типовая структура АРМ

Функциональная часть определяет содержание конкретного АРМ и включает описание совокупности взаимосвязанных задач, отражающих особенности автоматизируемых функций деятельности пользователя.

В основе разработки функционального обеспечения лежат требования пользователя к АРМ и его функциональная спецификация, включающая описание входной и выходной информации, средств и методов достижения достоверности и качества информации, применяемых носителей, интерфейсов связи. Обычно сюда же относятся описания средств защиты от несанкционированного доступа, восстановления системы в сбойных ситуациях, управление в нестандартных случаях.

Обеспечивающая часть включает традиционные виды обеспечения: информационное, программное, техническое, технологическое и др.

Информационное обеспечение включает описание организации информационной базы, регламентирует информационные связи, предопределяет состав и содержание всей системы информационного отображения. К ней также относятся массивы информации, хранящиеся в локальных базах данных. Сюда же относятся и сами СУБД.

Программное обеспечение (ПО) АРМ подразделяется на общее и функциональное. Общее программное обеспечение включает операционные системы, прикладные программы, расширяющие возможности операционных систем, программные средства диалога и др. Функциональное программное обеспечение предназначено для автоматизации решения функциональных задач, включает универсальные программы и функциональные пакеты.

Техническое обеспечение АРМ представляет собой комплекс технических средств обработки информации на базе ПЭВМ, предназначенный для автоматизации функций специалиста в предметной и проблемной областях его профессиональных интересов. К техническим средствам, непосредственно образующим АРМ, надо еще присовокупить средства связи (телефон, факс).

Технологическое обеспечение АРМ предназначено для организации технологического процесса использования АРМ применительно к комплексу решаемых задач по функциям специалиста.

Организационное обеспечение АРМ имеет своей целью организацию их функционирования, развития, подготовки кадров, а также администрирования. Сюда относятся: планирование работы, учет, контроль, анализ, регулирование, документальное оформление прав и обязанностей пользователей АРМ.

АРМ на предприятии

Основными функциями АРМ на предприятии является сбор, хранение и обработка информации на рабочих местах специалистов, информационное обслуживание аппарата управления для подготовки и обеспечения управленческих решений.

При определении состава АРМ на промышленных предприятиях необходимо учитывать состав решаемых задач и функции управления.

На предприятии имеются следующие группы АРМ:

• АРМ управленческого персонала;

• АРМ специалистов функциональных отделов (экономист, бухгалтер и т.п.);

• АРМ оператора управления (контролер, диспетчер);

• АРМ технических работников (секретарь).

3.2. Комплексная автоматизация деятельности предприятий на основе корпоративных информационных систем

3.2.1. Средства автоматизации на этапах ЖЦИ

На каждом этапе жизненного цикла изделия используются свои средства автоматизации (рис. 3.2).

На этапе проектирования – это системы САПР, в состав которых входят следующие подсистемы:

- **CAE** (*Computer Aided Engineering*) – система расчетов и инженерного анализа;

- **CAD** (*Computer Aided Design*) – система конструкторского проектирования;

- **CAM** (*Computer Aided Manufacturing*) – система проектирования технологических процессов;

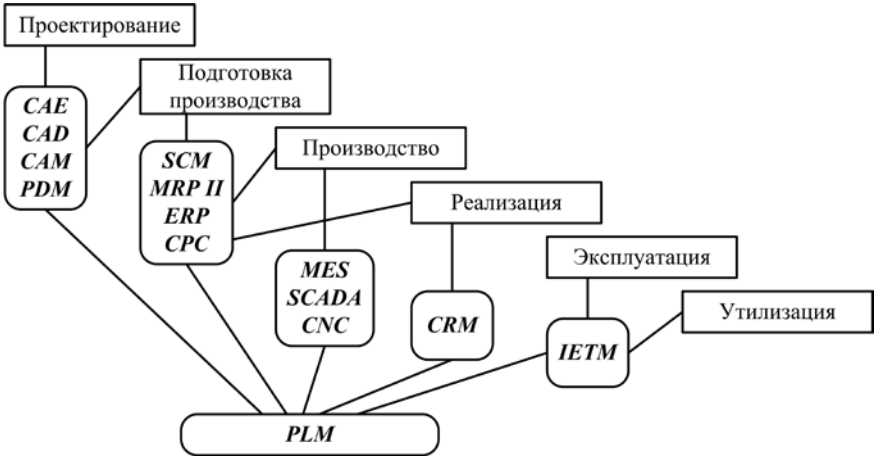


Рис. 3.2. Средства автоматизации на этапах ЖЦИ

- **PDM** (*Product Data Management*) – система управления проектными данными. Также обеспечивает координацию работы систем CAE/CAD/CAM.

На этапах эксплуатации и утилизации средства автоматизации представлены интерактивными электронными техническими руководствами (**ИЭТР**, **IETM** – *Interactive Electronic Technical Manuals*).

На всех остальных этапах, как правило, используются различные корпоративные информационные системы.

Интеграцию всех средств автоматизации на предприятии с целью создания единого информационного пространства предприятия обеспечивают системы **PLM** (*Product Lifecycle Management – Управление жизненным циклом*) – системы управления данными об изделии в едином информационном пространстве на протяжении всех этапов жизненного цикла изделия. Часто в этих целях используют системы **CALS** (*Continuous Acquisition and Life-cycle Support – Непрерывная информационная поддержка поставок и жизненного цикла*).

3.2.2. Корпоративные информационные системы

Понятие и классификация КИС

В настоящее время перед стоит проблема создания современной информационной системы управления предприятием. Существующие сейчас на большинстве российских предприятий системы управления в основном устарели и морально, и физически, наблюдается непрозрачность, дублирование информации, низкая оперативность ее получения, недостаточная достоверность и детализация Решение данной проблемы возможно путем внедрения современных корпоративных информационных систем.

Под корпоративной информационной системой (КИС) понимается система, реализующая информационные технологии для применения эффективных методов управления предприятием масштаба корпорации.

Главная задача КИС – эффективное управление всеми ресурсами предприятия (материально-техническими, финансовыми, технологическими и интеллектуальными) для получения максимальной прибыли и удовлетворения материальных и профессиональных потребностей всех сотрудников предприятия.

КИС по своему составу – совокупность различных программно-аппаратных платформ, универсальных и специализированных приложений различных разработчиков, интегрированных в единую информационно-однородную систему, которая наилучшим образом решает в некотором роде уникальную задачу каждого конкретного предприятия.

Различают *заказные* (уникальные) и *тиражируемые* КИС.

Под *заказными КИС* обычно понимают системы, создаваемые для конкретного предприятия, не имеющие аналогов и не подлежащие в дальнейшем тиражированию. *Тиражируемые КИС* имеют типовую структуру, а при внедрении должны адаптироваться к конкретному предприятию.

Часто используется также следующая классификация КИС:

1. Простые (“коробочные”) КИС реализуют небольшое число бизнес-процессов организации. Типичным примером являются бухгалтерские, складские и небольшие торговые системы наиболее широко представленные на российском рынке. Например, системы таких фирм как 1С, Инфин и т.д.

2. Системы среднего класса отличаются большей глубиной и широтой охвата функций. Данные системы предлагают российские и зарубежные компании. Как правило, это системы, которые позволяют вести учет деятельности предприятия по многим или нескольким направлениям: финансы, логистика, персонал, сбыт.

К высшему классу относятся системы, которые отличаются высоким уровнем детализации хозяйственной деятельности предприятия. Современные версии таких систем обеспечивают планирование и управление всеми ресурсами организации.

Международные стандарты управления предприятием

Современные КИС базируются на международных стандартах построения управленческих информационных систем. Рассмотрим некоторые из них.

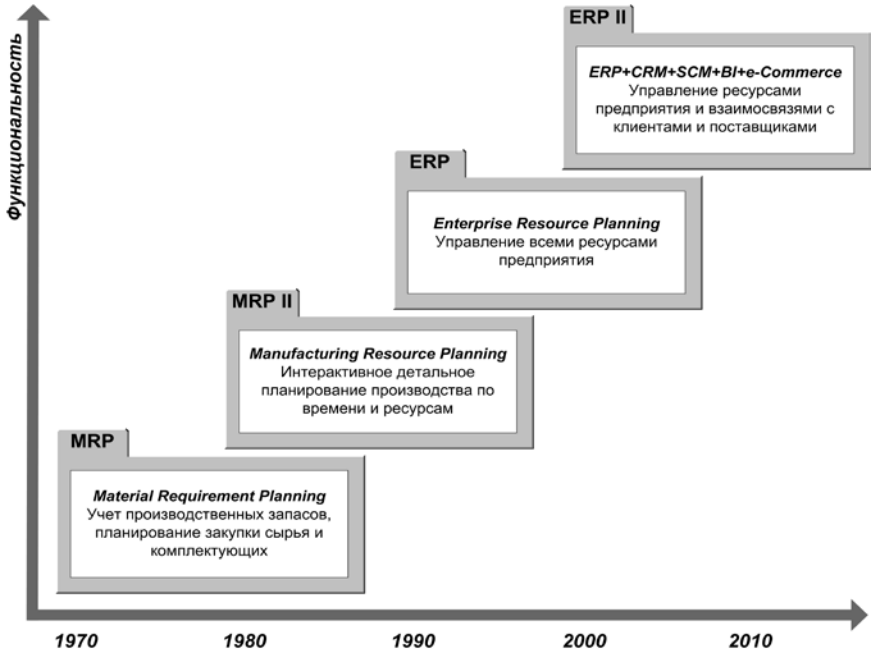


Рис. 3.3. Основные исторически сложившиеся классы систем управления предприятиями

Одной из первых, получивших официальный статус стандарта, была методика ***MPS*** (*Master Production Schedule*). В её основу входило формирование объёма продаж по определённым периодам, так называемое объёмно-календарное планирование, по которому производился план пополнения запасов.

В конце 1960-х возникла методология ***MRP*** (*Materials Requirement Planning – планирование материальных потребностей*). Именно этот стандарт считается первым в целой линейке систем автоматизации управления предприятиями класса КИС. Главной задачей MRP является то, чтобы каждый элемент производства, каждая комплектующая деталь были в нужное время в нужном количестве.

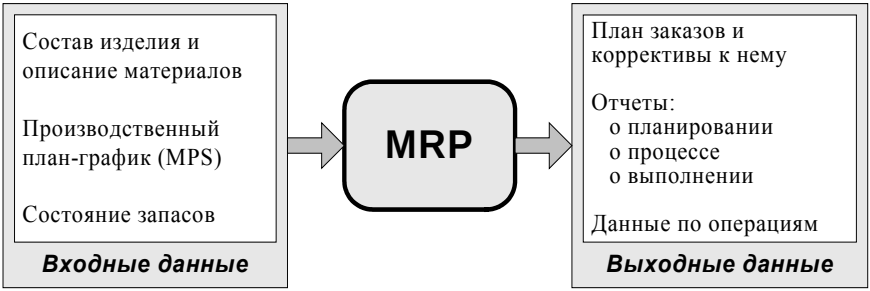


Рис. 3.4. Структура MRP системы

Система MRP имеет следующие преимущества:

- возможность оптимизации (синхронизации) времени поступления материалов и выпуска (сбыта) продукции;
- снижение уровня складских запасов;
- более точная информация для производственного учета.

Недостатком методологии MRP является учет ограниченного перечня производственных факторов (в расчетных моделях и алгоритмах не учитываются реальные производственные мощности, состояние трудовых и финансовых ресурсов предприятия).

Системы класса MRP по соотношению цена/качество подходят для небольших предприятий, где функции управления ограничиваются учётом (бухгалтерским, складским, оперативным), управлением запасами на складах и управлением кадрами, т.е. цепочкой “склад – цех”. Как правило, стоимость установки таких систем и владения ими невысока. Они поставляются обычно в виде

типового готового решения, подстраиваемого при внедрении под специфику конкретного предприятия.

Аналогичная методология была разработана и для планирования производственных мощностей. Она получила название ***CRP*** (*Capacity Resource Planning – планирование производственных мощностей*).

Объединенная система планирования MRP-CRP получила название ***MRP II*** (*Manufacturing Resource Planning - планирование производственных ресурсов*).

Стандарт ***APICS*** на системы класса MRP II содержит описание 16 групп функций (функциональных блоков) системы:

- Sales and Operation Planning (Планирование продаж и производства).
- Demand Management (Управление спросом).
- Master Production Scheduling (Составление плана производства).
- Material Requirements Planning (Планирование материальных потребностей).
- Bill of Materials (Спецификации продуктов).
- Inventory Transaction Subsystem (Управление складом).
- Scheduled Receipts Subsystem (Плановые поставки).
- Shop Plow Control (Управление на уровне производственного цеха).
- Capacity Requirements Planning (Планирование потребностей в мощностях).
- Input/output control (Контроль входа/выхода).
- Purchasing (Материально-техническое снабжение).
- Distribution Resource Planning (Планирование ресурсов распределения).
- Tooling Planning and Control (Планирование и управление инструментарием).
- Financial Planning (Управление финансами).
- Simulation (Моделирование).
- Performance Measurement (Оценка результатов деятельности).

Таким образом, в отличие от MRP применение MRP II позволяет осуществлять оперативное планирование и управление цепочкой “сбыт – производство – склад – снабжение”, т. е. всем производственным процессом, а не отдельными его фрагментами. Большая часть российских КИС относится именно к этому классу.

Рис. 3.5. Структура MRP II-системы

Характерная черта систем MRPII – специализация на конкретном типе производства. Предназначены они для средних предприятий, а стоимость колеблется в довольно широком диапазоне: примерно 30-300 тыс. долларов, иногда больше. С небольшими доработками типового функционала системы MRPII могут внедриться около 2-4 мес., а при построении системы на основе индивидуального проекта первые очереди могут быть введены в строй через 4-8 мес. и более.

Следующий этап развития КИС представлен системами ***ERP*** (*Enterprise Resource Planning – планирование ресурсов предприятия*). Если системы MRP II используются для планирования исключительно ресурсов производства, то системы ERP занимаются планированием всех ресурсов предприятия.

Основным назначением ERP-систем является автоматизация взаимоувязанных процессов планирования, учёта и управления по главным направлениям деятельности компании.

Рис. 3.6. Структура ERP-системы

Часто вся присущая концепции ERP совокупность задач реализуется не одной интегрированной системой, а некоторым комплексом ПО, в основе которого, как правило, лежит базовый ERP-пакет, а к нему через соответствующие интерфейсы подключены специализированные продукты.

ERP-системы предназначены в значительной степени для крупных предприятий. Их внедрение, как правило, связано с кардинальной перестройкой структуры и системы управления предприятием и может проводиться в течение нескольких лет. Стоимость внедрения подобных систем нередко даже превышает стоимость лицензии и может достигать нескольких миллионов долларов.

Дальнейшее развитие ERP системы получили за счет реализации новых функций, что было отражено в появлении целой линейки новых стандартов.

Одной из современных концепций управления ресурсами предприятия является концепция ***CSRP*** (*Customer Synchronized Resource planning – планирование ресурсов, синхронизированное с потребителем*), предложенная фирмой SYMIX (USA). Эта концепция охватывает почти полностью весь жизненный цикл товара (производственный, логистический, предпродажный, послепродажный) и позволяет координировать в реальном времени традиционное планирование производства в соответствии с

требованиями покупателя, т.е. сочетает в себе механизмы ERP и CRM.

Модуль ***CRM*** (*Customer Relationships Management – Управление взаимоотношениями с клиентами*) позволяет эффективно управлять контактами с клиентами, рекламными кампаниями, сбытом, проводить маркетинговые исследования.

Как правило, в состав любой CRM системы входят следующие подсистемы:

- EMA (*Enterprise Marketing Automation*) – Автоматизация маркетинговых акций;
- SFA (*Sales Force Automation*) – Система автоматизации работы торговых агентов;
- CSS (*Customer Service & Support*) – Система управления сервисным обслуживанием клиентов.

CRM системы в настоящее время представлены на рынке корпоративных систем и как модули в составе ERP систем, и как отдельные решения.

Сравнительно недавно появился новый стандарт – ***MES*** (*Manufacturing Execution System*) – это система управления производством, которая связывает воедино все бизнес-процессы предприятия с производственными процессами, оперативно поставляет объективную и подробную информацию руководству. Кроме того, система MES проводит анализ и определяет наиболее эффективное решение проблемы.

Технология MES позволяет ***в режиме реального времени*** оперативно контролировать, оптимизировать, документировать и планировать производственные процессы от начала формирования заказа до выпуска готовой продукции.

По мере активного развития Интернет-технологий в 90-х появляется новое направление деятельности – электронный бизнес (*e-business*) – термин, которым обозначают методики и организационные принципы, позволяющие предприятию взаимодействовать со своими контрагентами через Интернет.

Эти и другие новые функции, появившиеся в интегрированных системах управления, выходят за традиционные рамки ERP. По предложению Gartner Group в 2000 году, концепция ERP-систем нового поколения на фоне широкого применения Интернет-технологий в практике корпоративного управления, получила название ***ERP II*** (*Enterprise Resource and Relationship*

Processing – Управление ресурсами и внешними отношениями предприятия).

Системы ERP II вобрали в себя и объединили все основные выделенные к этому моменту типы корпоративных приложений:

- систему планирования ресурсов предприятия ***ERP*** в прежнем понимании этого термина;

- систему управления взаимоотношениями с клиентами ***CRM*** (*Customer Relation Management*);

- систему управления цепочками поставок ***SCM*** (*Supply Chain Management*) – предназначены для автоматизации и управления всеми этапами снабжения предприятия и для контроля всего товародвижения на предприятии;

- средства аналитики и поддержки принятия решений ***BI*** (*Business Intelligence*);

- систему управления данными ***IMS*** (*Information Management System*) для интеграции всех компонентов;

- средства электронной коммерции и взаимодействия через Интернет ***e-commerce***.

Потребности бизнеса постоянно растут и все реже одной информационной системе удается удовлетворить их хотя бы наполовину. Во многом именно по этой причине наиболее оправданным методом сегодня признается создание сетей, в которых обеспечивается взаимодействие разнородных систем, причем, как правило, разных производителей.

Некоторые разработчики ERP-систем, сейчас меняют стратегию и открыто заявляют о движении в сторону открытости своих систем для максимальной интеграции с продуктами конкурентов. Новое явление получило название ***Collaborative ERP*** (слово Collaborative означает "сотрудничество с соперниками") и позиционируется как следующая ступень после ERP-II. Таким образом, «коллаборация» позволяет легко встраивать систему в уже имеющиеся корпоративные среды".

Помимо вышеперечисленных нельзя не упомянуть и о некоторых других сложившихся и применяемых стандартах управления, например, JIT.

JIT (*Just-In-Time – точно в срок*). Метод, ориентированный на организацию бездефектного производства при минимуме издержек. Для того чтобы она работала, требуются высочайшая организация и точнейшая синхронизация всех производственных процессов.

Методы JIT (под названием «Канбан») появились впервые в Японии в фирме Toyota. Сейчас они получают распространение, и их можно встретить уже в некоторых западных ERP-системах.

Мировой и российский рынок КИС

На сегодняшний день на российском рынке представлены все значимые в мире разработчики ERP, основные из которых представлены в таблице.

Мировой и российский рынок КИС

	2010, %%	2009, %%	Изменение, п.п.
SAP	50,5	50,1	0,4
1С	26	22,3	3,7
Oracle	8,2	9,6	-1,4
Microsoft Dynamics	7,4	7,1	0,3
«Галактика»	2,4	3,9	-1,5
Прочие	5,5	7	-1,5

Источник: IDC

В отраслевом разрезе российский рынок ERP-систем представляет собой довольно неоднозначную картину. Более 40 % всех внедрений приходится сегодня на промышленность. Рост ERP-потребления определяют увеличение прибыльности и повышение качества управления компаний. Многие промышленные предприятия выходят на международные бизнес-площадки, что повышает требования к качеству информации для управленческого персонала.

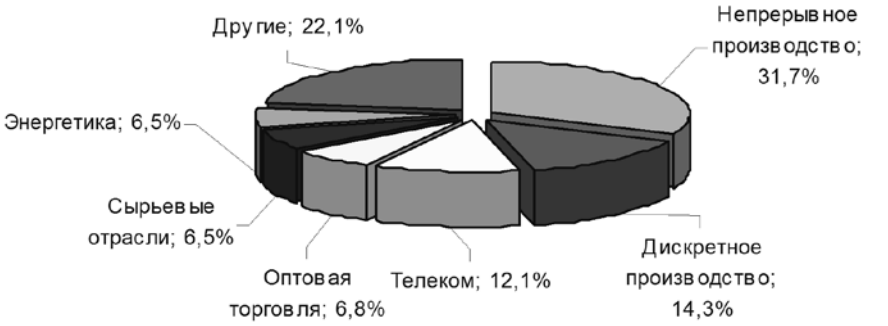


Рис. 3.7. Объемы внедрений ERP-систем по отраслям

Около 88% малых предприятий имеют только одну ERP-систему, и только 6% имеют две и 4% имеют 3 системы. Среди компаний среднего размера лишь 58% компаний имеют одну ERP-систему, 22% имеют две системы, 10% имеют три системы, 4% имеют четыре системы. В крупных предприятиях только 20% имеют одну ERP-систему, 18% имеют две системы, 22% имеют три системы, по 9% имеют три и четыре системы, и целых 31% компаний имеют более четырех установленных систем. Отметим, что по классификации Aberdeen, к малым компаниям относятся имеющие менее 50 млн. долларов годового оборота, а к крупным – имеющие более 1 млрд. долларов.

Принципы выбора КИС

В процессе выбора КИС следует руководствоваться следующими критериями:

- репутация фирмы и системы, стаж пребывания фирмы на рынке, число продаж; количество комплексных внедрений в России. Имеются ли внедрения на родственных предприятиях?;
- терминология и качество русификации западной системы;
- качество адаптации западной системы к российским стандартам;
- цена;
- функциональная полнота;

- модульность – необходимо иметь возможность покупать и внедрять систему по частям и только на нужное число пользователей;

- гибкость – система должна позволять легко менять бизнес - процессы и алгоритмы путем параметрической настройки и т.п. Система должна также легко интегрироваться с другими модулями;

- архитектура – желательна клиент-серверная архитектура;

- техническая платформа – система должна уметь мигрировать с платформы на платформу;

- операционная среда – обязательно должны быть версии на UNIX;

- СУБД – в набор обязательно должен входить Oracle, желательны также Informix и SQL Server, остальные СУБД – по желанию.

Есть еще один очень важный вопрос, связанный с выбором набора модулей ERP решения, предназначенных для внедрения. Большая часть потребителей предполагает внедрить на первом этапе минимальный набор модулей, оценить эффективность их внедрения, и лишь потом принять решения о комплексном внедрении. К сожалению, мнения поставщиков ERP решений различается на счет так называемого «минимального интегрированного решения». Одни предлагают любой набор модулей. Другие выделяют минимальные интегрированные решения. Третьи рассматривают свою систему как принципиально целостную.

Методологии внедрения ERP-систем

Традиционно в России, как и во всем мире, промышленные предприятия информатизируются в два этапа. Первой создается система автоматизированного проектирования (САПР). А уже на втором этапе приступают к внедрению ERP систем. Как правило, этому предшествует реинжиниринг бизнес-процессов – либо «с чистого листа», либо «под выбранный продукт». В первом случае бизнес-процессы предприятия анализируются и перестраиваются с использованием традиционных средств, основываясь на собственных критериях оптимальности. На выходе получаются идеально подходящие для данного предприятия стандарты и процессы управления, хотя для их реализации может не оказаться необходимого ПО. Во втором случае бизнес-процессы предприятия

в процессе оптимизации «подгоняются» под реализованные в конкретной ERP-системе стандарты. При таком подходе возможно неполное удовлетворение нужд предприятия, но зато обеспечивается автоматическая программная реализация выбранных процессов и гарантируется успешность применяемой бизнес-практики.

В зависимости от масштабов изменений бизнес-процессов выделяют 4 варианта внедрения систем ERP класса:

1) минимальные изменения бизнес-процессов и минимальная доработка ERP-системы. Этот вариант удобен при совпадении используемой бизнес-практики с заложенной в систему. Внедрение происходит в сжатые сроки, требуя минимума затрат на реорганизацию предприятия и на доработку ПО. Как правило, так поступают фирмы, внедряющие только учетные модули, либо средние и мелкие фирмы, не стремящиеся достичь конкурентного преимущества за счёт автоматизации или ограниченные в средствах.

2) серьёзные изменения бизнес-процессов и минимальная доработка ERP-системы. При этом внедрение ERP предваряется перестройкой процессов функционирования предприятия под одну или несколько бизнес-практик, выбранных из базы. Само внедрение происходит быстро и безболезненно, но реинжиниринг бизнес-процессов может потребовать значительных финансовых и временных затрат. Обычно к этому варианту внедрения прибегают предприятия, убедившиеся в неэффективности ранее существовавших на предприятии бизнес-процессов. Корректное внедрение может привести к значительному повышению эффективности работы предприятия, но использование уже опробованных бизнес-практик означает, что предприятие не может использовать ERP-систему как средство внесения инноваций в процесс управления.

3) минимальные изменения бизнес-процессов и серьёзная доработка ERP-системы. Данный подход необходим в тех случаях, когда изменение структуры предприятия затруднительно из-за размеров и/или уникальности процессов управления, либо в случае принятия предприятием бизнес-практик, отсутствующих в базе внедряемой ERP-системы. Обычно именно так происходит внедрение модулей управления производством и автоматизация других специфичных для предприятия процессов. Переработка ПО связана со значительными затратами труда и времени, сопряжена с

риском неудачного внедрения, а также предполагает дополнительные затраты на адаптацию новых версий. Как правило, такой вариант внедрения используют только крупные компании.

4) серьёзные изменения бизнес-процессов и серьёзная доработка ERP-системы. Этот вариант внедрения выбирается в результате реинжиниринга «с чистого листа». Такой подход является самым затратным и рискованным. Перестройка бизнес-процессов с одновременной переработкой ПО обычно требуется при первом внедрении ERP-системы в новой для неё отрасли. Это даёт компании серьёзное конкурентное преимущество, так как она какое-то время будет на шаг опережать всех своих конкурентов. Кроме того, поставщик системы может принять эту специфическую для отрасли реализацию как основу для выпуска специальной версии своего ПО. Соответственно, компания, внедрившая ERP-систему, будет практически избавлена от необходимости модифицировать новые версии под свои нужды. Однако все указанные преимущества уравновешиваются высокими затратами на реализацию подобной стратегии, а также риском провала.

Кроме различных вариантов внедрения существуют разные методы их реализации – единовременный и поэтапный. При единовременном внедрении старая система управления «отключается», и ERP-система «ставится» сразу во всех подразделениях. Преимуществом этого метода является отсутствие необходимости работать со старой системой управления – пользователям можно сразу предоставить полную функциональность системы. Сроки внедрения системы достаточно сжаты. В то же время, это требует очень высоких затрат ресурсов, внимание разработчиков оказывается «размыто» по всем внедряемым модулям, скрытые ошибки могут вызвать провал всего проекта, в то время как откат к старой системе управления становится сложным и экономически невыгодным.

Поэтапное внедрение предполагает внедрение системы отдельными модулями и/или в отдельных подразделениях. Указанный метод обеспечивает постепенную замену старой системы управления на новую. В этом случае каждый отдельный модуль проектируется, реализуется и тестируется, после чего добавляется к уже внедрённым компонентам ERP-системы. Поэтапное внедрение позволяет распределить затраты организации по времени. В процессе разработки внимание уделяется лишь одному или

нескольким модулям, что позволяет повысить качество их проработки. При неудаче внедрения какого-то из модулей возможен практически безболезненный откат на предыдущую позицию внедрения. В свою очередь пользователи могут изучить функциональность внедряемых модулей значительно раньше полного внедрения системы. Однако плавность поэтапного внедрения требует дополнительных затрат на создание интерфейсов между новой и старой системами управления, а также поддержку старой системы. Общие затраты на внедрение, как правило, выше, чем при единовременном внедрении.

Обычно, чем крупнее организация, тем более она склонна к выбору поэтапного внедрения. Это связано, как со сложностью автоматизируемых процессов, так и с высокой степенью риска провала внедрения.

Проблемы развития и внедрения КИС на российских предприятиях

Внедрение ERP-системы на предприятии нередко занимает несколько лет. По оценкам экспертов, не более 20 % всех проектов по внедрению ERP-решений заканчивается в оговоренное контрактом время и с сохранением бюджетов. Часто ограничивается функциональность решения, либо проект завершается досрочно, когда внедрена только часть модулей.

Можно сформулировать несколько основных причин неудачных внедрений ERP-систем на российских предприятиях.

1. В большинстве случаев полностью отсутствует какая бы то ни было политика или стратегия построения КИС на промышленных предприятиях. Решения по выбору КИС и партнера по ее созданию принимаются без какого-либо серьезного обоснования. Решения о выделении средств и об их расходовании на ИТ и создание КИС в большинстве случаев принимаются лицами, не ориентирующимися в проблемах данной области. При этом никто не отвечает за конечный результат и окупаемость израсходованных средств.

2. Хорошо зарекомендовавшие себя на западе дорогостоящие решения не дают ожидаемого эффекта на российских предприятиях – в основном из-за ориентации подобных решений на западные стандарты управления, а не российские, например, отсутствие экономической стабильности и т.п.

3. Недостаток высококвалифицированных кадров и т.п.

Эффекты от внедрения ERP-систем

Внедрение систем ERP-класса на промышленном предприятии дает ряд экономических выгод, в том числе, уменьшение страховых запасов, увеличение оборачиваемости ТМЗ, увеличение поставок точно в срок, сокращение НЗП, сокращение производственного цикла, сокращение цикла разработки новых продуктов и т.д. Таким образом, увеличивается ликвидность предприятия.

Существуют и не денежные эффекты:

- Повышение «интеллектуальности» бизнеса (оперативное наличие больших объемов релевантной информации позволяет управленцу принять перспективное, упреждающее решение).

- Оптимизация планирования (своевременный доступ всех заинтересованных пользователей к важной информации, находящейся в одной централизованной БД).

- Усовершенствование процессов принятия решений. Решения становятся более обоснованными, если они подкреплены достоверной и оперативной информацией. Кроме того, экономится время.

- Повышение рыночной привлекательности компании (т.н. «бонус Wall Street») – рынок благосклонен к тем компаниям, которые демонстрируют внимание к деталям своей деятельности, и, более того, их полноценному анализу.

- Расширение информационной компетентности – чем большее количество сотрудников имеет доступ к корпоративным данным, тем «умнее» и мобильнее становится организация в целом.

- Создание единой среды сотрудничества (организация приобретает мощный заряд развития, ведь каждый из ее членов работает на достижение прозрачных, понятных и, главное, общих целей).

3.3. Контрольные вопросы

1. Классификация АРМ
2. Принципы конструирования АРМ
3. Типовая структура АРМ
4. Понятие и классификация КИС
5. Основные стандарты управления предприятием
6. Функции MRP II системы
7. Сравнительный анализ систем MRP и MRP II
8. Характеристика стандарта ERP
9. Краткая характеристика линейки стандартов ERP: ERP, ERP II, Collaborative ERP
10. Характеристика стандарта ERP II
11. Характеристика стандартов CSRP и MES
12. Современный рынок КИС

4. ТЕХНОЛОГИЯ БАЗ ИНФОРМАЦИИ, СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ, МОДЕЛИ ДАННЫХ. ПОНЯТИЕ ХРАНИЛИЩА ДАННЫХ

4.1. Системы управления базами данных (СУБД)

Основные понятия баз данных

Под ***информацией*** понимают любые сведения о каком-либо событии, сущности, процессе и т.п., являющиеся объектом некоторых операций: восприятия, передачи, преобразования, хранения или использования.

Данные можно определить как информацию, фиксированную в определенной форме, пригодной для последующей обработки, хранения и передачи.

База данных (БД) – поименованная совокупность структурированных данных, относящихся к определенной предметной области.

Объекты реального мира, сведения о которых хранятся в базе данных, называются ***сущностями*** – entities, а их актуальные признаки – ***атрибутами*** (attributes). Каждый признак конкретного объекта есть значение атрибута.

В базе данных могут отражаться не только физические объекты. Она способна вобрать в себя сведения об абстракциях, процессах, явлениях, т.е. обо всем, с чем сталкивается человек в своей деятельности.

В состав базы данных входит также ***метаинформация*** (т.е. информация об информации), включающая описание базы данных (схема БД), информацию о предметной области, необходимую для проектирования системы, о пользователях БД, о проектных решениях и др.

Централизованное хранилище метаинформации называется ***словарем данных*** (словарь-справочник, энциклопедия, репозиторий).

Система управления базами данных (СУБД) – это комплекс программных и языковых средств, необходимых для создания баз данных, поддержания их в актуальном состоянии и организации поиска в них необходимой информации.

Виды моделей БД

Ядром любой базы данных является модель данных. Модель данных – совокупность структур данных и операций их обработки.

СУБД основывается на использовании иерархической, сетевой или реляционной модели, на комбинации этих моделей или на некотором их подмножестве.

Иерархическая модель данных.

К основным понятиям иерархической структуры относятся: узел, уровень, элемент, связь. Узел – это совокупность атрибутов, описывающих некоторый объект. На схеме иерархического дерева узлы представляются вершинами графа. Каждый узел на более низком уровне связан только с одним узлом, находящимся на более высоком уровне. Иерархическое дерево имеет только одну вершину (корень дерева), не подчиненную никакой другой вершине и находящуюся на самом верхнем (первом) уровне (рис. 4.1):

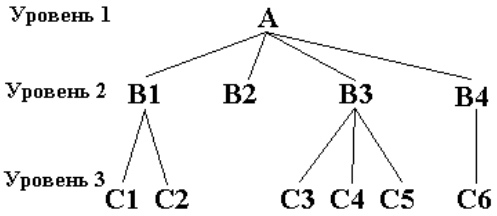


Рис. 4.1. Иерархическая модель данных

Пример иерархической структуры: каждый студент учится в определенной (только одной) группе, которая относится к определенному (только одному) факультету (рис. 4.2):

Рис. 4.2. Пример иерархической структуры

Сетевая модель данных.

В сетевой структуре каждый элемент может быть связан с любым другим элементом:

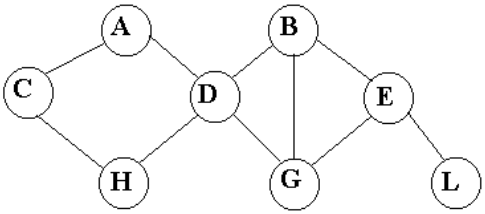


Рис. 4.3. Сетевая модель данных

Пример сетевой структуры: база данных, содержащая сведения о студентах, участвующих в научно-исследовательских работах (НИРС). Возможно участие одного студента в нескольких НИРС, а также участие нескольких студентов в разработке одной НИРС (рис. 4.4):

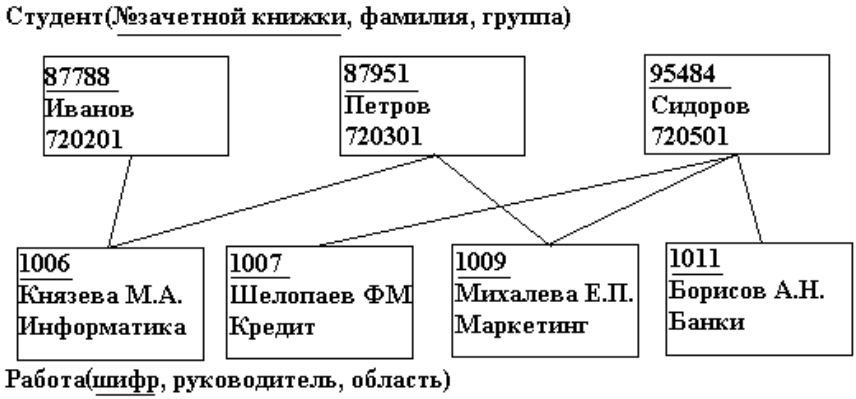


Рис. 4.4. Пример сетевой структуры

Реляционная модель данных

Ориентирована на организацию данных в виде двумерных таблиц. Каждая реляционная таблица (отношение) обладает следующими свойствами:

- каждый элемент таблицы – один элемент данных;
- все столбцы в таблице однородные, т.е. все элементы в столбце имеют одинаковый тип (числовой, символьный и т.д.) и длину;
- каждый столбец имеет уникальное имя;
- одинаковые строки в таблице отсутствуют;
- порядок следования строк и столбцов может быть произвольным.

Пример: реляционной таблицей можно представить информацию о студентах, обучающихся в вузе (таблица):

Пример реляционной структуры

№ зачетной книжки	Фамилия	Имя	Отчество	Дата рождения	Группа
155125	Сергеев	Петр	Михайлович	01.01.1996	720581
154652	Петрова	Анна	Владимировна	31.12.1996	720591
178535	Анохин	Андрей	Борисович	20.06.1996	720682

В настоящее время наибольшее распространение получили СУБД, реализующие именно реляционную модель данных, например, Microsoft Access.

Кроме этого также выделяют многомерные СУБД. ***Многомерная СУБД*** – одна из моделей организации системы управления БД, основанная на многомерном представлении данных.

Многомерные базы данных отличаются от реляционных прежде всего трехмерностью – поддержкой неограниченного числа значений в поле, и находят свое применение там, где необходима эффективная и простая работа с большими массивами символьной информации. В многомерных СУБД данные организованы в виде упорядоченных многомерных массивов, удовлетворяющих требованиям защиты от несанкционированного доступа в организации. Они обеспечивают более быструю реакцию на запросы данных за счет того, что обращения поступают к относительно небольшим блокам данных, необходимых для конкретной группы пользователей. Для достижения сравнимой производительности реляционные системы требуют тщательной проработки схемы базы данных, определения способов индексации и специальной настройки. Ограничения SQL остаются реальностью, что не позволяет реализовать в реляционных СУБД многие встроенные функции, легко обеспечиваемые в системах основанных на многомерном представлении данных.

Рис. 4.5. Пример трехмерной модели

Классификация СУБД

По языкам общения СУБД делятся на *открытые*, *замкнутые* и *смешанные*. Открытые системы – это системы, в которых для обращения к базам данных используются универсальные языки программирования. Замкнутые системы имеют собственные языки общения с пользователями БнД. Открытые системы в настоящее время используются редко.

По *выполняемым функциям* СУБД делятся на *информационные* и *операционные*. Информационные СУБД позволяют организовать хранение информации и доступ к ней. Для выполнения более сложной обработки необходимо писать специальные программы. Операционные СУБД выполняют достаточно сложную обработку, например, автоматически позволяют получать агрегированные показатели, не хранящиеся непосредственно в базе данных, могут изменять алгоритмы обработки и т. д.

По *сфере возможного применения* различают *универсальные и специализированные*, обычно проблемно-ориентированные СУБД.

Системы управления базами данных поддерживают разные типы данных. Набор типов данных, допустимых в разных СУБД, различен. СУБД, позволяющие разработчику добавлять новые типы данных и новые операции, называются расширяемыми системами баз данных (РСБД). Дальнейшим развитием концепции РСБД являются объектно-ориентированные системы баз данных, позволяющие моделировать сложные объекты.

Существуют и другие направления классификации СУБД.

4.2. Хранилища данных

Принятие решений должно основываться на реальных данных об объекте управления. Такая информация обычно хранится в оперативных базах данных OLTP-систем. Но эти данные не подходят для анализа и принятия стратегических решений, так как для этого в основном нужна агрегированная информация. Также, для целей анализа необходимо иметь возможность быстро манипулировать информацией, представлять ее в различных аспектах, производить различные нерегламентированные запросы к

ней, что затруднительно реализовать на оперативных данных по соображениям производительности и технологической сложности.

Решением данной проблемы является создание специального хранилища данных, содержащего агрегированную информацию в удобном виде.

Хранилище данных (data warehouse, DWH) – это предметно-ориентированное, привязанное ко времени и неизменяемое собрание данных для поддержки процесса принятия управляющих решений. ***Целью*** построения хранилища данных является интеграция, актуализация и согласование оперативных данных для физической реализации единого интегрированного источника данных.

По своей сути, Хранилище данных, представляет собой центр, в который собирается вся необходимая информация из различных подразделений предприятия (а также из внешних источников, например статистических отчетов). Прежде чем попасть в Хранилище, данные должны быть соответствующим образом обработаны штатными средствами Хранилища. При этом осуществляется контроль корректности поступающих данных, разноформатные данные приводятся к единой структуре.

Компоненты, входящие в типичное ХД, представлены на рис. 4.6.

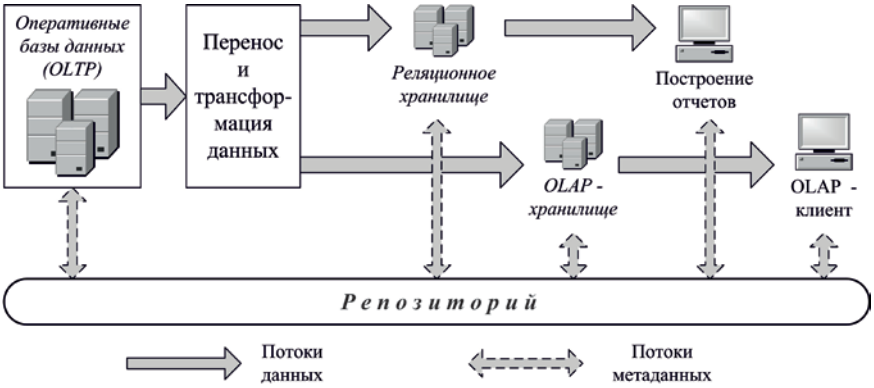


Рис. 4.6. Типичная структура Хранилища данных

Как уже говорилось выше, основными источниками данных Хранилища данных служат оперативные транзакционные системы, которые обслуживают повседневную учетную деятельность компании. Детальные данные из источников могут либо напрямую поступать в хранилище, либо предварительно очищаться, интегрироваться и агрегироваться до требуемого уровня обобщения.

При этом для их промежуточного хранения используется Оперативный склад данных (***ODS*** – *Operational Data Store*). В отличие от хранилища данных информация в складе данных может изменяться со временем в соответствии с изменениями, происходящими в источниках данных.

Конструкция оперативного склада аналогична конструкции хранилища данных. Идентичность оперативного склада и хранилища данных состоит в их предметной ориентированности и хранении детальных данных. Отличие от хранилища данных состоит в том, что оперативный склад данных:

- имеет изменяемое содержимое;
- содержит только детальные данные (данные из оперативных и внешних систем, не подвергавшиеся операциям обработки;
- содержит текущие значения данных.

Данные оперативного склада регулярно обновляются. Каждый раз, когда данные изменяются в оперативных системах и внешних источниках, соответствующие им данные из оперативного склада также должны быть изменены. Частота обновления оперативного склада зависит как от частоты обновления источников, так и от регламента загрузки данных в склад. Данные, хранящиеся в оперативном складе данных, уже доступны для предварительного анализа.

Важнейшим элементом ХД являются метаданные, т.е. информация о структуре, размещении и трансформации данных. Благодаря им обеспечивается эффективное взаимодействие различных компонентов хранилища. Обычно выделяют три вида метаданных, которые должны присутствовать в системе:

1. С точки зрения пользователей:
- метаданные для бизнес-аналитиков;
- метаданные для администраторов;
- метаданные для разработчиков.

2. С точки зрения предметных областей:
- структуры данных хранилища;

- модели бизнес-процессов;
- описания пользователей;
- технологические и пр.

3. С точки зрения функциональности системы:
- метаданные о процессах трансформации;
- метаданные по администрированию системы;
- метаданные о приложениях;
- метаданные о представлении данных пользователям.

Наряду с большими корпоративными хранилищами данных широкое применение находят также витрины данных (***Data Mart***). Под витриной данных понимается небольшое специализированное хранилище для некоторой узкой предметной области, ориентированное на хранение данных, связанных одной бизнес-тематикой. Иногда эти структуры хранения данных называют также ***киосками данных***. Витрины данных можно рассматривать как небольшие хранилища, которые создаются с целью информационного обеспечения аналитических задач конкретных управленческих подразделений. Как правило, витрина содержит значительно меньше данных, охватывает всего несколько предметных областей и имеет более короткую историю.

Источником данных для витрин служат данные из Хранилища данных, которые, как правило, агрегируются и консолидируются по различным уровням иерархии. Детальные данные могут также помещаться в витрину или присутствовать в ней в виде ссылок на данные хранилища.

Различные витрины данных содержат разные комбинации и выборки одних и тех же детализированных данных хранилища.

Методика (методология) построения Хранилищ данных

Существуют различные подходы к стратегии построения корпоративного хранилища данных: построение сверху вниз; снизу вверх; динамическая интеграция данных и др.

Считается, что наиболее эффективным подходом является подход, при котором в процессе разработки и внедрения хранилища данных осуществляется его пошаговое наращивание на основе единой системы классификаторов и общей среды передачи и хранения данных – спиральная модель процесса разработки (рис. 4.7).

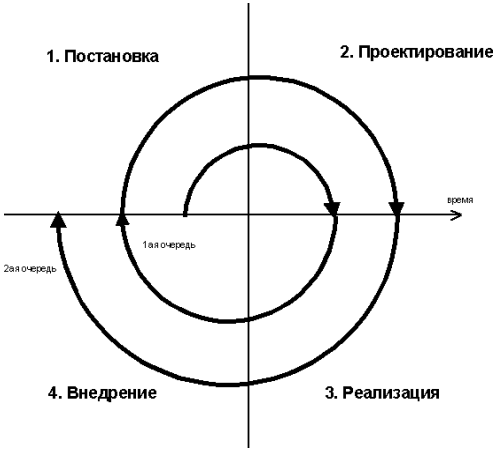


Рис. 4.7. Спиральная модель разработки

На каждом шаге развертывания осуществляется реализация одной или ограниченного числа витрин данных по следующему технологическому циклу:

- постановка задачи;
- проектирование;
- реализация;
- внедрение.

Стратегия пошагового наращивания позволяет по завершении каждого цикла ввести в кратчайшие сроки в промышленную эксплуатацию законченную систему, с определенной ограниченной функциональностью. Небольшие масштабы каждого проектного цикла существенно уменьшают потери при возможных проектных ошибках по сравнению с полномасштабным проектированием и созданием системы в целом. Кроме того, поскольку в каждом цикле применяются одни и те же методологические и технологические подходы, а также средства разработки, то время реализации каждой новой витрины будет сокращаться за счет повышения опыта проектной группы и постепенной отладки механизма взаимодействия между заказчиком и разработчиком системы.

4.3. Современный рынок хранилищ данных (DWH)

На рынке ПО предлагается ряд продуктов, которые имеют принципиально разную функциональность, назначение, степень готовности к применению, однако все они позиционируются как хранилища данных. Это затрудняет понимание описаний этих продуктов поставщиками, их сравнение и в конечном итоге выбор продукта для конкретной организации.

Продукты, которые относят к категории хранилищ данных, можно разделить на следующие группы:

- Специальная СУБД;
- Инструмент программиста;
- Отраслевые заготовки хранилищ данных;
- Конструктор;
- Специализированное приложение;
- Комплексная платформа разработки.

Специальная СУБД. Иногда хранилищем данных называют системы управления базами данных (СУБД). Например, СУБД Sybase IQ, предназначенную для создания хранилищ данных, или многомерные СУБД, такие как MS Analysis Services, Oracle Explorer. В этом случае нужно понимать, что речь идет о системе управления базой данных, которая может стать платформой хранилища данных, также как и любая промышленная реляционная СУБД.

Инструмент программиста. К этой группе можно отнести инструменты проектировщика баз данных. Они являются специальными CASE-средствами, ориентированными на создание реляционных баз данных в идеологии хранилищ.

Data warehouse Architect (Sybase). Среда проектировщика базы данных базируется на идеологии хранилищ данных. В ней предлагается создание не просто таблиц, а таблиц фактов или таблиц измерений. В систему заложены знания о структурах «звезда» и «снежинка». Результатом работы системы является логическая и физическая модель базы данных, сгенерированная реляционная база данных будущего хранилища данных. Для завершения работы над хранилищем данных требуется использовать ETL-систему для извлечения, очистки и загрузки данных и OLAP-систему для визуализации данных. По этой технологии можно достаточно быстро создавать простые «фотографические» хранилища данных, уникальные для предприятия, а также с равным

успехом использовать ее в софтверной компании (software company – компании-разработчики программного обеспечения) при создании тиражного хранилища данных.

Ascential DataStage (Ascential Software). Система является ETL-инструментом и предназначена для проектирования стадий извлечения данных из исходной базы, преобразования и загрузки в базу данных приемник.

Однако, как это часто бывает, развитие инструмента привело к появлению в нем функции проектирования и генерации приемной базы данных, что позволяет использовать этот инструмент не только как классический ETL, но и как инструмент проектировщика хранилища данных.

Отраслевые заготовки хранилищ данных. Ряд компаний предлагает набор заготовок отраслевых приложений, применение которых сокращает сроки разработки хранилища данных и позволяет использовать опыт других предприятий.

Industry Warehouse Studio (Sybase). Система предоставляет инструменты дизайна хранилища данных и набор заголовок отраслевых решений, которые можно использовать при построении хранилища данных. Система базируется на специализированной СУБД Sybase IQ, оптимизированной для создания хранилища данных. Инструменты дизайна хранилища ориентированы на программиста.

Готовые хранилища данных. Эти системы обладают всеми свойствами конечных клиент-серверных продуктов. Они имеют инсталлятор, готовую базу данных, инструменты настройки информационной модели, предназначенные не для программиста, а для аналитика, административные и пользовательские интерфейсы, встроенные инструменты создания отчетов. Такие системы содержат готовые информационные объекты, свойственные всем деловым хранилищам данных, например, Организационная иерархия, Финансовый показатель, Валюта и др.

CFO Vision (SAS). Система финансовой консолидации, реализованная как готовое хранилище финансовых показателей, включающее технологию сбора данных, структуры хранения данных, алгоритмы консолидации показателей и другие необходимые функции хранилища данных.

Платформа хранилищ данных «Контур» (Intersoft Lab). Финансовое хранилище данных, включающее базу данных,

объектно-ориентированную библиотеку классов, наборы административных, дизайнерских, технологических и пользовательских интерфейсов. В системе реализован комплект бизнес-объектов, характерных для деловых хранилищ данных, таких как Организационная структура, Контрагенты, Счета и показатели. Финансовые инструменты, Документы, Бюджеты и др. Система позволяет создавать конечные управленческие приложения при помощи дизайнерских интерфейсов, ориентированных на аналитика.

Конечные приложения. Конечные приложения реализуют одну или несколько задач на платформе хранилищ данных. Они требуют лишь установки и кастомизации. Как правило, при внедрении не изменяется информационная модель, заложенная в приложение, не требуется (или почти не требуется) программирование. Приложения строятся на основе анализа предметной области и опыта решения данной задачи на вертикальном рынке, например:

- *BPM-платформа «Контур».* Бюджет хозяйственных расходов. (Intersoft Lab). Приложение для комплексной автоматизации бюджетирования административно-хозяйственных расходов банка. Реализует технологию коллективного планирования сметы и оперативного контроля расходования бюджета.

- *BPM-платформа «Контур».* Управленческий учет (Intersoft Lab). Приложение для ведения управленческого учета на основе данных бухгалтерского и операционного учета, что обеспечивает комплексное решение задач финансового управления банком и подготовки управленческой отчетности.

- *BPM-платформа «Контур».* Трансфертное управление ресурсами (Intersoft Lab). Приложение предназначено для автоматизации трансфертноИ управления ресурсами банка.

- *BPM-платформа «Контур».* Функционально-стоимостный soft Lab). Приложение реализует метод функционально-стоимостного анализа Activity Based Costing (ABC) и обеспечивает точную калькуляцию и анализ себестоимости банковских продуктов, проектов (целевых программ), каналов сбыта, бизнес-процессов.

Лидеры рынка

В основном хранилища данных функционируют на базе реляционных СУБД. Широко известны следующие производители хранилища данных:

- ***Teradata.*** Платформа хранилищ данных компании Teradata включает широкий набор решений для хранилищ данных, в том числе три аппаратно-программные модели с разной функциональностью предназначенные для различных категорий компаний.

В состав платформы входит база данных Teradata Database, а также Teradata Manager – большой набор инструментов и средств для контроля над операциями базы данных, управления и сервисного обслуживания.

- ***Oracle.*** Компания предлагает аппаратно-программные решения, тесно интегрируя их с продуктами других производителей, таких как Hyperion Fusion Middleware, Siebel.

- ***IBM.*** Комплекс программно-аппаратных решений IBM интегрируется с программными продуктами InfoSphere, Rational, Cognos, WebSphere, FileNet, Optim и др.

- ***Netezza.*** Компания предлагает идеальную платформу для хранения данных четвёртого поколения, обеспечивающую совмещение хранения данных и проведение аналитики. TwinFin Netezza – это самый “быстрый” продукт на сегодняшний день, у которого скорость обработки данных до 100 раз быстрее, чем у ближайших аналогов.

В сентябре 2010 г. IBM приобрела компанию Netezza. В настоящее время на рынке представлено семейство IBM Smart Analytics System (ISAS) и бренд Netezza. Программное обеспечение хранилищ данных IBM – InfoSphere Warehouse доступно для Unix, Linux, Windows и z/OS. IBM имеет тысячи клиентов баз данных по всему миру и более 500 клиентов на устройства (комбинация Netezza и ISAS)

- ***EMC/Greenplum.*** Greenplum является частью подразделения компании EMC – Data Products, разрабатывающего хранилища данных СУБД массово-параллельной архитектуры (MPP), работающих на Linux и Unix. Продукт реализуется в виде устройства или автономной СУБД. Компания имеет в мире более 400 клиентов.

- ***Microsoft.*** Платформы хранилищ данных Microsoft Data Warehouse Platform включает реляционную СУБД MS SQL Server, многомерную СУБД MS Analysis Services, ETL-систему Data Transformation Services (DTS), MS Office как среду отображения данных и выпуска отчётов.

- ***Sybase.*** Программно-аппаратные решения Sybase включают высокопроизводительную реляционную базу данных СУБД IQ, набор инструментов для мониторинга систем обработки данных (СУБД и др.).

В 2010 г. Sybase была приобретена компанией SAP. В квадранте Gartner рассматривается СУБД Sybase IQ, ставшая первой колоночной СУБД. Она же является основным хранилищем данных СУБД SAP / Sybase. У Sybase тысячи клиентов Sybase IQ во всём мире.

Основные преимущества Хранилищ данных:

- единый источник информации: компания получает выверенную единую информационную среду, на которой будут строиться все справочно-аналитические приложения в той предметной области, по которой построено хранилище. Эта среда будет обладать единым интерфейсом, унифицированными структурами хранения, общими справочниками и другими корпоративными стандартами, что облегчает создание и поддержку аналитических систем. Также, при проектировании информационного хранилища данных особое внимание уделяют достоверности информации, которая попадает в хранилище;

- производительность: физические структуры хранилища данных специальным образом оптимизированы для выполнения абсолютно произвольных выборок, что позволяет строить действительно быстрые системы запросов;

- быстрота разработки: специфическая логическая организация хранилища и существующее специализированное ПО позволяют создавать аналитические системы с минимальными затратами на программирование;

- интегрированность: интеграция данных из разных источников уже сделана, поэтому не надо каждый раз производить соединение данных для запросов требующих информацию из нескольких источников. Под интеграцией понимается не только

совместное физическое хранение данных, но и их предметное, согласованное объединение; очистку и выверку при их формировании; соблюдение технологических особенностей и т.д.;

- историчность и стабильность: OLTP-системы оперируют с актуальными данными, срок применения и хранения которых обычно не превышает величины текущего бизнес-периода (полугода-год), в то время как информационное хранилище данных нацелено на долговременное хранение информации (обычно временные рамки данных, находящихся в хранилище, лежат в пределах от 15-ти месяцев до пяти лет. Данные большей давности, как правило, переносятся в архив). Стабильность означает, что фактическая информация в хранилище данных не обновляется и не удаляется, а только специальным образом адаптируется к изменениям бизнес-атрибутов. Таким образом, появляется возможность осуществлять исторический анализ информации;

- независимость: выделенность информационного хранилища существенно снижает нагрузку на OLTP-системы со стороны аналитических приложений, тем самым производительность существующих систем не ухудшается, а на практике происходит уменьшение времени отклика и улучшение доступности систем.

Альтернативным по отношению к концепции Хранилищ данных способом формирования единого взгляда на корпоративные данные является создание виртуального источника, опирающегося на распределенные базы данных различных систем обработки данных. При этом каждый запрос к такому источнику динамически транслируется в запросы к исходным базам данных, а полученные результаты на лету согласовываются, связываются, агрегируются и возвращаются к пользователю. Однако такой способ обладает рядом существенных недостатков: время обработки запросов значительно больше, требуется постоянная связь всех источников данных в сети, задействован большой объем ресурсов сервера БД, данные могут иметь разные форматы и кодировки данных, а значит, могут быть несогласованны и т.п. Главным же недостатком следует признать практическую невозможность обзора длительных исторических последовательностей, ибо при физическом отсутствии центрального хранилища доступны только те данные, которые на момент запроса есть в реальных базах данных.

4.4. Контрольные вопросы

1. Основные понятия баз данных
2. Виды моделей данных
3. Реляционная модель данных
4. Классификация СУБД
5. Характеристика хранилищ данных
6. Современный рынок хранилищ данных (DWH)
7. Основные преимущества Хранилищ данных

5. КЛАССЫ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРЕДПРИЯТИИ. АВТОМАТИЗАЦИЯ ОПЕРАЦИОННЫХ ЗАДАЧ. СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ. СИСТЕМЫ АНАЛИЗА ДАННЫХ. OLAP-ТЕХНОЛОГИИ

5.1. Аналитическая пирамида

Информационную инфраструктуру предприятия можно представить в виде нескольких иерархических уровней, каждый из которых характеризуется степенью агрегированности информации и своей ролью в процессе управления. Примером схематического представления информационной инфраструктуры может служить «аналитическая пирамида» (analytical stack), предложенная компанией Gartner (рис. 5.1).

Рис. 5.1. Аналитическая пирамида

Аналитическая пирамида представляет собой иерархическую структуру, в которой различные классы информационных систем располагаются на разных уровнях.

К числу таких уровней относятся:

− уровень транзакционных систем;

− уровень хранилищ данных;

− уровень витрин данных;

− уровень OLAP-систем;
− уровень аналитических приложений.

В основании аналитической пирамиды расположены транзакционные системы, предназначенные для управления текущими операциями и, таким образом, являющиеся источниками первичной информации для анализа. По мере движения от основания пирамиды к ее вершине происходит преобразование детальных операционных данных в агрегированную информацию, предназначенную для поддержки принятия управленческих решений.

Отметим, что передача данных из транзакционных систем в аналитические приложения может производиться как последовательно, через все обозначенные ярусы аналитической пирамиды, так и более коротким путем, минуя один или несколько уровней (это отражено на схеме в виде стрелки “bypass” – «прямая передача»). Способ передачи данных зависит как от технических возможностей программных продуктов, так и от того, каким образом предполагается использовать те или иные данные.

Кроме этого, заметим, что отнести тот или иной программный продукт к какому-либо одному классу не всегда возможно, поскольку многие системы позволяют решать аналитические задачи нескольких категорий. Например, OLAP-системы многих производителей способны выступать в роли аналитических приложений или использоваться для построения многомерных хранилищ и витрин данных.

5.1. Классы ИС на предприятии

Как известно, существуют три уровня управления – оперативный, тактический и стратегический. Оперативный уровень – наиболее детальный, здесь планированию и учету подлежат отдельные операции (транзакции), выполняемые различными подразделениями организации. Горизонт оперативного планирования, как правило, не превышает одного месяца, а планирование ведется в разрезе недель, дней, смен. На тактическом уровне решаются задачи более общего характера, а внимание руководителя сосредоточено в основном на эффективности использования ресурсов. Горизонт планирования, как правило, год, с разбивкой по кварталам и месяцам. А стратегический уровень –

наиболее глобальный: на этом уровне решаются задачи формирования стратегических целей, оценки путей их достижения и определения так называемых стратегических инициатив – реальных программ действий по реализации стратегии.

По мере перехода от оперативного управления к тактическому и далее к стратегическому информация становится более агрегированной и охватывает все большие временные периоды. И именно это явление привело к тому, что в области информационных систем исторически сложились два класса – транзакционные и аналитические системы (рис. 5.2).

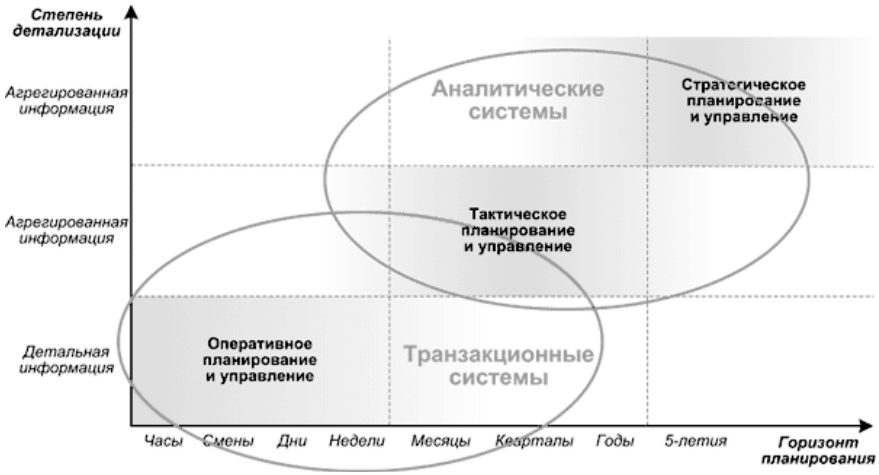


Рис. 5.2. Классы ИС на предприятии

К транзакционным относятся системы, осуществляющие обработку данных на уровне отдельных операций (*транзакций*) (ERP-системы, учетные системы и некоторые другие). Эти программные продукты иногда называют ***OLTP***–системами (*On–Line Transaction Processing* – обработка транзакций в режиме реального времени – системы операционной обработки данных).

К аналитическим приложениям относятся прикладные информационные системы, удовлетворяющие следующим трем критериям:

- *поддержка процессов управления* – возможности автоматизации задач анализа и оптимизации деятельности организации, а также выявления возможностей развития бизнеса;

- *разграничение функций* – независимость от ключевых транзакционных систем, но с возможностью двустороннего обмена данными с ними;

- *интеграция данных и учет фактора времени* – возможность извлечения, преобразования и обобщения данных из различных источников.

В качестве примера аналитических приложений, расположенных на вершине «аналитической пирамиды» следует выделить:

- системы, реализующие методологию сбалансированных систем показателей (BSC-системы, Balanced Scorecard);

- системы корпоративного планирования и бюджетирования;

- системы формирования и анализа консолидированной финансовой отчетности;

- другие аналитические приложения (системы бизнес-интеллекта (BI-приложения), системы бизнес-моделирования, системы статистического анализа данных, экспертные системы поддержки принятия решений).

Кроме того, особую категорию аналитических систем составляют системы бизнес-интеллекта (*business intelligence*), или BI-системы.

В своей совокупности транзакционные и аналитические системы образуют так называемую аналитическую пирамиду (*термин Gartner*). Основанием такой пирамиды служат ERP-системы и другие транзакционные системы. По мере движения от основания пирамиды к ее вершине, где располагаются аналитические приложения, происходит постепенное преобразование детальных операционных данных в агрегированную информацию, достаточную и удобную для принятия экономически обоснованных управленческих решений.

5.3. OLTP-системы

Системы операционной обработки данных (*обработки транзакций в режиме реального времени*) рассчитаны на быстрое обслуживание относительно простых запросов большого числа пользователей.

Транзакция может состоять из операций чтения, удаления, вставки или модификации данных.

Чтобы использование механизмов обработки транзакций позволило обеспечить целостность данных и изолированность пользователей, транзакция должна обладать четырьмя основными свойствами:

- атомарности (atomicity),
- согласованности (consistency),
- изолированности (isolation),
- долговечности (darability).

Транзакции, обладающие перечисленными свойствами, иногда называют ACID-транзакциями по первым буквам их английских названий.

Свойство атомарности означает, что транзакция должна выполняться как единая операция доступа к БД. Она должна быть выполнена полностью либо не выполнена совсем. То есть должны быть выполнены все операции манипулирования данными, которые входят в транзакцию, либо, если по каким-то причинам выполнение части операций невозможно, ни одна из операций не должна выполняться.

Свойство согласованности гарантирует взаимную целостность данных, то есть выполнение ограничений целостности БД после окончания обработки транзакции.

В многопользовательских системах с одной БД одновременно могут работать несколько пользователей или прикладных программ. Поскольку каждая транзакция может изменять разделяемые данные, данные могут временно находиться в несогласованном состоянии. Доступ к этим данным другим транзакциям должен быть запрещен, пока изменения не будут завершены. Свойство изолированности транзакций гарантирует, что они будут выполняться отдельно друг от друга.

Свойство долговечности означает, что если транзакция выполнена успешно, то произведенные ею изменения в данных не будут потеряны ни при каких обстоятельствах.

Результатом выполнения транзакции может быть ее фиксация или откат.

Фиксация транзакции – это действие, обеспечивающее запись в БД всех изменений, которые были произведены в процессе ее выполнения.

До того как транзакция зафиксирована, возможна отмена всех сделанных изменений и возврат базы данных в то состояние, в котором она была до начала выполнения транзакции. Для фиксации транзакции необходимо успешное выполнение всех ее операторов. Если нормальное завершение транзакции невозможно, происходит откат. При этом база данных возвращается в исходное состояние, все изменения аннулируются.

Применение транзакций – эффективный механизм организации многопользовательского доступа к БД. Однако при реализации этого механизма в СУБД приходится сталкиваться с целым рядом проблем. Для их решения должна быть использована специальная дисциплина совместной обработки (***сериализации***) транзакций.

Современные информационные системы работают с распределенными БД, поэтому в одной транзакции могут модифицироваться отношения, физически хранящиеся на удаленных вычислительных системах. При этом существует два подхода к выполнению транзакций в распределенных системах – механизм двухстадийной фиксации транзакций и технология тиражирования данных.

5.4. BPM-системы

90-е годы прошлого века ознаменовались интенсивным развитием аналитических систем, включая BI-системы и аналитические приложения. На определенном этапе была признана необходимость их интеграции – как методологической (функциональной), так и технологической. Так появилось новое направление, получившее название Business Performance Management (BPM), что на русский язык обычно переводится как «управление эффективностью бизнеса» (хотя такой перевод

представляется не вполне корректным). В общих чертах, BPM – это целостный, процессно-ориентированный подход к принятию управленческих решений, направленный на улучшение способности компании оценивать свое состояние и управлять эффективностью своей деятельности на всех уровнях, путем объединения собственников, менеджеров, персонала и внешних контрагентов в рамках общей интегрированной среды управления.

Сегодня концепция BPM признана мировым сообществом, в том числе такими известными аналитическими компаниями, как IDC, Gartner и META Group.

Business Performance Management (BPM) – это методология, направленная на оптимизацию реализации стратегии, и состоящая из набора интегрированных циклических аналитических процессов, поддерживаемых соответствующими технологиями и имеющих отношение как к финансовой, так и к операционной информации. BPM позволяет предприятию определять, измерять и управлять эффективностью своей деятельности, направленной на достижение стратегических целей. Ключевые финансовые и операционные процессы BPM включают планирование, консолидацию и отчетность, анализ ключевых показателей эффективности и их распространение в рамках организации.

В соответствии с документом, разработанным Группой по стандартизации BPM, в качестве основных процессов, охватываемых BPM-системами, можно выделить следующие:

− формализация стратегии;
− планирование;
− мониторинг и анализ;
− корректирующие воздействия.

В части *формализации стратегии* BPM-системы позволяют менеджерам разрабатывать стратегии и доводить их до подразделений компании, выявлять возможности создания стоимости и формировать системы метрик, позволяющих оценивать эффективность бизнеса и ее динамику.

В части *планирования* BPM-системы позволяют менеджерам всех подразделений компании устанавливать свои локальные цели, разрабатывать и моделировать сценарии планирования, разрабатывать программы и бюджеты, поддерживающие бизнес-стратегию, а также формировать целевые значения определенных показателей для различных временных периодов.

В части *мониторинга и анализа* BPM-системы позволяют оценивать индивидуальную и групповую эффективность с применением соответствующих ключевых показателей на всех организационных уровнях, а также предоставляют пользователям дополнительную информацию, помогающую им предпринимать те или иные действия.

В части *корректирующих воздействий* BPM-системы помогают менеджерам своевременно реагировать на возникающие ситуации и отклонения.

Исследовательская фирма Gartner разделила поставщиков BPM-инструментов на три группы – это разработчики базовых аналитических (BI, business intelligence) систем, ERP-комплексов и отдельных BPM-приложений.

В первой группе выделяются компании Cognos и Hyperion Solutions.

Некоторые разработчики ERP-комплексов выпускают также и BPM-комплекты. Особенность их подхода – обеспечение легкой консолидации данных из своих ERP-систем в хранилище данных CPM-комплекта и/или даже реализация прямого доступа BPM-приложений к базам данных ERP-систем.

Так, компания SAP AG предлагает модуль Strategic Enterprise Management (SEM) для поддержки стратегического управления предприятием. Этот компонент аналитики Gartner относят к классу BPM, но он, однако, не продается отдельно, а предлагается только в составе системы mySAP ERP.

На российском рынке BPM-систем помимо перечисленных компаний выделяется московская фирма InterSoft Lab, предлагающая BPM-систему на основе собственных базовых инструментов OLAP-анализа и консолидации данных.

5.5. Системы поддержки принятия решений (СППР)

Для поддержки и обеспечения системы принятия управленческих решений на всех уровнях управления возможно использование современных информационных технологий. Спектр подобных решений очень широк. Это и системы принятия решений на основе сбора данных, и корпоративные порталы, и системы для обработки функциональной информации, и огромное множество подобных систем разного уровня. Однако наибольший интерес в

системах данного направления вызывают специализированные решения класса СППР (систем поддержки принятия решений). Их применение дает возможность более точно моделировать ситуации, качественно оценивать опасности, моделировать их воздействие, а также выполнять анализ с большей точностью.

Рассмотрим характеристики программных продуктов класса СППР.

Интерактивность СППР. Означает, что система откликается на разного рода действия пользователя в диалоговом режиме.

Интегрированность СППР. Обеспечивает совместимость составных систем относительно управления данными и средствами общения с пользователями в процессе поддержки принятия решений.

Мощность СППР. Означает способность системы отвечать на самые важные вопросы.

Доступность СППР. Это способность обеспечивать выдачу ответов на запросы пользователя в нужной форме и в необходимое время.

Гибкость СППР. Характеризует возможность системы адаптироваться к изменениям потребностей и ситуаций.

Надежность СППР. Означает способность системы выполнять нужные функции на протяжении заданного периода времени.

Робастность (robustness) СППР. Это степень способности системы восстанавливаться в случае возникновения ошибочных ситуаций как внешнего, так и внутреннего происхождения.

Управляемость СППР. Означает, что пользователь может контролировать действия системы, вмешиваясь в ход решения задачи.

Основу СППР составляет комплекс взаимосвязанных моделей с соответствующей информационной поддержкой исследования, экспертные и интеллектуальные системы, включающие опыт решения задач управления и обеспечивающие участие коллектива экспертов в процессе выработки рациональных решений.

На рисунке 5.3 приведена архитектурно-технологическая схема информационно-аналитической поддержки системы принятия управленческих решений:

Первоначально информация хранится в оперативных базах данных OLTP-систем, но ее сложно использовать в процессе

управления. Агрегированная информация организуется в многомерное хранилище данных Data Warehouse. Затем она используется в процедурах многомерного анализа (OLAP) и для интеллектуального анализа данных Data Mining.

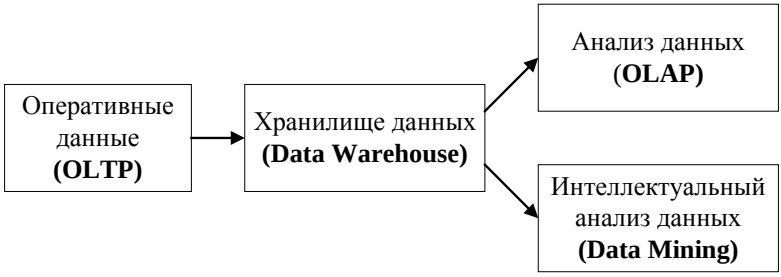


Рис. 5.3. Архитектурно-технологическая схема информационно-аналитической поддержки системы принятия управленческих решений

Современных рынок ПО предлагает довольно широкий спектр готовых решений класса СППР. Западные: «CONCORDE», «ORET», «Y&R», «Quick Rating». Российские: «Эксперт», «ИКСИ», «ИСИС», «Парус», «КОНФЛИКТ», «МАИ», «РИСК-1», «КОНСЕНСУС».

5.6. OLAP-технологии

В основе концепции оперативной аналитической обработки (OLAP) лежит многомерное представление данных. Формальное определение OLAP-технологии впервые было дано в статье Е.Ф. Кодда (E.F.Codd), которая вышла в свет в 1993 году, получила большой резонанс и привлекла внимание к возможностям многомерного анализа. По Кодду, многомерное представление данных представляет собой множественную перспективу, состоящую из нескольких независимых измерений, вдоль которых могут быть проанализированы определенные совокупности данных. Одновременный анализ по нескольким измерениям данных определяется как многомерный анализ. Каждое измерение включает направления консолидации данных, состоящие из серии последовательных уровней обобщения, где каждый вышестоящий уровень соответствует большей степени агрегации данных по

соответствующему измерению. В этом случае становится возможным произвольный выбор желаемого уровня детализации информации по каждому из измерений.

К характеристикам OLAP-систем относятся:

- основные характеристики: многомерность модели данных, интуитивные механизмы манипулирования данными, доступность данных, пакетное извлечение данных, архитектура «клиент-сервер», прозрачность, многопользовательская работа;

- специальные характеристики: обработка ненормализованных данных, хранение результатов отдельно от исходных данных, выделение отсутствующих данных, обработка отсутствующих значений;

- характеристики построения отчетов: гибкое построение отчетов, стабильная производительность при построении отчетов, автоматическое регулирование физического уровня;

- управление размерностью: общая функциональность, неограниченное число измерений и уровней агрегирования, неограниченные операции между данными различных измерений.

Большинство современных OLAP-систем нельзя однозначно отнести ни к средствам разработки, ни к готовым приложениям. С одной стороны, их использование не требует длительного изучения теории и практики построения аналитических приложений. Но, с другой стороны, они не являются готовыми программными продуктами для решения аналитических задач, поскольку требуют определенной настройки на источники данных, алгоритмы анализа и формы представления итоговой информации. Эта двойственность приводит к многовариантности внедрения, которое может осуществляться как системным интегратором, так и квалифицированными специалистами компании-пользователя.

Универсальным критерием определения OLAP как аналитического инструмента является тест ***FASMI*** (*Fast Analysis of Shared Multidimensional Information – Быстрый анализ разделяемой многомерной информации*). Рассмотрим детально каждую из составляющих этой аббревиатуры.

- *Fast (быстрый)*. Это свойство означает, что OLAP-система должна обеспечивать ответ на запрос пользователя в среднем за пять секунд, при этом большинство запросов обрабатываются в пределах одной секунды, а самые сложные запросы должны обрабатываться в пределах двадцати секунд.

- *Analysis (аналитический).* OLAP-система должна справляться с любым логическим и статистическим анализом, характерным для бизнес-приложений, и обеспечивать сохранение результатов в виде, доступном для конечного пользователя. Средства анализа могут включать процедуры анализа временных рядов, распределения затрат, конверсии валют, моделирования изменений организационных структур и другие.

- *Shared (разделяемый).* Система должна предоставлять широкие возможности разграничения доступа к данным и одновременной работы многих пользователей.

- *Multidimensional (многомерный).* Система должна обеспечивать концептуально многомерное представление данных, включая полную поддержку множественных иерархий.

- *Information (информация).* Мощность различных программных продуктов характеризуется количеством обрабатываемых входных данных. Разные OLAP-системы имеют разную мощность: наиболее мощные из них могут оперировать, по крайней мере, в тысячу раз большим количеством данных по сравнению с самыми маломощными. При выборе OLAP-инструмента следует учитывать целый ряд факторов, включая дублирование данных, требуемую оперативную память, использование дискового пространства, эксплуатационные показатели, интеграцию с информационными хранилищами и т.п.

В настоящее время на рынке ПО предлагается большое число OLAP-систем. Западные: Arbor Software, IBM, Informix, Microsoft, Oracle, SAS Institute, Sybase и т.д. Однако, наибольшее распространение в России получили решения только Oracle и Microsoft. Российские: Intersoft Lab, Институт Открытых Систем, BaseGroup Labs.

Разновидности многомерного хранения данных

Обсуждая тему OLAP, следует упомянуть и о разновидностях многомерного хранения данных. Дело в том, что информационные массивы, логически упорядоченные по аналитическим направлениям и, таким образом, являющиеся многомерными с точки зрения конечных пользователей, не обязательно являются многомерными с точки зрения технологической реализации. Как правило, выделяют три разновидности хранения данных:

- многомерный OLAP (multidimensional OLAP, MOLAP) представляет собой «OLAP в чистом виде», т.е. технологию, основанную на хранении данных под управлением специализированных многомерных СУБД;

- реляционный OLAP (relational OLAP, ROLAP) – технология, основанная на хранении многомерной информации в реляционных базах данных, на основе одной или нескольких схем типа «звезда» или «снежинка»;

- гибридный OLAP (hybrid OLAP, HOLAP) – технология, при которой одна часть данных хранится в многомерной базе, а другая часть – в реляционной. При этом инструментальные средства, поддерживающие эту технологию, обеспечивают прозрачность данных для пользователя, который на логическом уровне всегда работает с многомерными данными.

Одной из причин, объясняющих необходимость различных подходов к хранению данных, является то, что в многомерных структурах хранятся довольно большие объемы агрегированных данных (например, данные продаж могут агрегироваться по временным интервалам, категориям товаров или регионам продаж). Эти данные очень важны, поскольку в большинстве случаев аналитика интересуют именно агрегированные, а не детальные цифры.

Любые данные (как исходные, так и агрегированные) могут храниться либо в реляционных, либо в многомерных структурах, в зависимости от применяемой технологии. Например, MOLAP подразумевает хранение всей информации в многомерной базе данных. Это позволяет манипулировать данными как многомерным массивом, но в этом случае многомерная база данных оказывается избыточной, поскольку и агрегированные показатели, и лежащие в их основе исходные данные хранятся вместе. При технологии ROLAP исходные данные остаются в той же реляционной базе, где они находились изначально, а агрегированные данные помещаются в специальные служебные таблицы в той же базе данных. Наконец, при гибридной технологии (HOLAP) исходные данные остаются в реляционной базе данных, а агрегированные показатели хранятся в многомерной базе данных.

Выбор способа хранения зависит от нескольких факторов, таких как объем и структура данных, скорость выполнения запросов, частота обновления OLAP-кубов.

5.7. Интеллектуальный анализ данных

Интеллектуальный анализ данных *(Data Mining*) – это процесс поддержки принятия решений, основанный на поиске в данных скрытых закономерностей. При этом накопленные сведения автоматически обобщаются до информации, которая может быть охарактеризована как знания.

В общем случае процесс интеллектуального анализа данных состоит из трёх стадий (рис. 5.4):

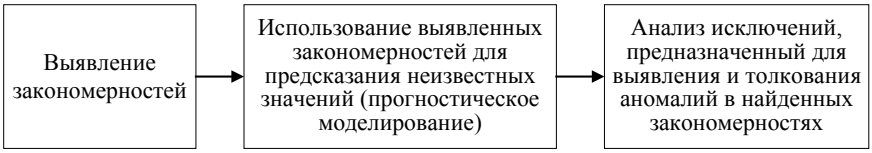


Рис. 5.4. Процесс интеллектуального анализа данных

Компьютерными технологиями, образующими Data Mining являются:

Статистические пакеты. Полезны главным образом для проверки заранее сформулированных гипотез и для "грубого" разведочного анализа, составляющего основу оперативной аналитической обработки данных. Хорошо известны пакеты SPSS, STATGRAPHICS, STATISTICA, STADIA.

Нейронные сети и их вариации. Представляют собой сеть взаимосвязанных элементов, которые являются математической моделью нейронов головного мозга. Используются для определения априорно неизвестных сложных функциональных зависимостей на основании статистических данных. Наиболее известные примеры - BrainMaker, NeuroShell, OWL, NeuroScalp, Эврика+.

Экспертные системы. Позволяют на основании опыта экспертов моделировать процесс принятия решений и выдавать эффективный результат. Наиболее известные примеры: Acquire, Active AgentX, ReThink.

Байесовы (вероятностные) сети. Моделируют вероятностные причинно-следственные связи. Позволяют рассчитывать вероятность наступления того или иного события при известной априорной вероятности причин, строить модели в режиме реального

времени с учетом неполноты данных и возможностью корректировки результата при появлении новой информации.

Методы эвристической самоорганизации. Методы данной группы позволяют моделировать сложные нелинейные процессы и системы при отсутствии априорных знаний о структуре системы.

Теория игр. Позволяет формализовать описание процессов принятия сознательных целенаправленных решений при участии одной или нескольких сторон в условиях неопределенностей, риска и конфликта, которые возникают при столкновении интересов. Задача теории игр заключается в предложении рекомендаций рационального образа действий участников процесса принятия решений, т.е. в определении оптимальной стратегии для каждого из них.

Теория хаоса. Предлагает новые методы анализа данных, позволяющие выявлять скрытые зависимости там, где раньше систему считали случайной, и не имеющей каких-либо закономерностей. Применение аппарата теории хаоса позволяет качественно изучать нестабильное апериодическое поведение в нелинейных динамических системах, например, в экономических процессах.

Многозначные логики. Нечеткая логика. Логика антонимов. Расширяет возможности “обычной” двоичной логики, оперирующей только понятиями “1-да” и “0-нет”. Позволяет оперировать с нечеткой, неточной, "размытой" информацией. Дает возможность использования качественных, а не количественных характеристик, что позволяет манипулировать лингвистическими понятиями и знаниями, выражаемыми на обычном языке (например, для описания процессов: “плохо”-“средне”-“хорошо” и т.д.).

Эволюционные алгоритмы. Адаптивные методы поиска, используемые для решения задач функциональной оптимизации. Основаны на эволюционном принципе "выживает сильнейший". Моделируя этот процесс, эволюционные алгоритмы, в частности генетические, способны "развивать" решения реальных задач. Такой подход является динамическим и позволяет довольно быстро находить оптимальные, с определенной точки зрения, решения. Примером такой системы является PolyAnalyst.

Деревья решений и Алгоритмы классификации (decision trees). Создается иерархическая структура классифицирующих правил типа "ЕСЛИ..., ТО...", имеющая вид дерева. Недостаток: деревья решений

принципиально не способны находить "лучшие" (наиболее полные и точные) правила в данных. (IDIS, KnowledgeSEEKER, See5/C5.0).

Системы рассуждений на основе аналогичных случаев. Вывод путем сопоставления (Memory-based Reasoning, MBR) или вывод, основанный на прецедентах (Case-based Reasoning, CBR). Эти алгоритмы основаны на обнаружении некоторых аналогий в прошлом, наиболее близких к текущей ситуации, с тем, чтобы оценить неизвестное значение или предсказать возможные результаты (последствия). Эти методы называют еще методом "ближайшего соседа". В выборе решения они основываются на всем массиве доступных исторических данных, поэтому невозможно сказать, на основе каких конкретно факторов строятся ответы. Примеры: KATE tools (Франция), Pattern Recognition Workbench (США), КОРА (Россия).

Ассоциативные правила. Алгоритмы ограниченного перебора. Выявляют причинно-следственные связи и определяют вероятности или коэффициенты достоверности, позволяя делать соответствующие выводы. (Пример, WizWhy).

Методы экспертных оценок. Применяются при отсутствии возможности или трудо-ресурсной нецелесообразности получения данных в количественном выражении. В таких случаях обращаются к использованию знаний и опыта экспертов - методам экспертных оценок, которые включают в себя методы получения, формализации и интеграции экспертных знаний.

Существуют и другие технологии, применяемые в Data Mining, например, генетические алгоритмы, роевой интеллект и т.д.

Среди западных систем класса Data Mining наиболее известно решение Microsoft Data Mining. Наиболее известная российская система класса Data Mining - PolyAnalyst.

5.8. Контрольные вопросы

1. Аналитическая пирамида
2. Характеристика транзакционных и аналитических систем
3. Системы операционной обработки данных
4. Основные свойства транзакций
5. Принципы сериализации транзакций
6. Подходы к выполнению транзакций в распределенных системах

7. Характеристика систем управления эффективностью бизнеса BPM

8. Основные характеристики систем класса СППР

9. Структура систем СППР

10. Понятие OLAP-технологий

11. Характеристика компьютерных технологий в интеллектуальном анализе данных

6. ГЛОБАЛЬНАЯ СЕТЬ ИНТЕРНЕТ

6.1. История создания Интернет

В 1961 году DARPA (агентство перспективных научных исследований в области обороны) приступило к проекту по созданию экспериментальной сети передачи информационных пакетов. Эта сеть, названная ***ARPANET***, предназначалась первоначально для изучения методов обеспечения надежной связи между компьютерами различных типов, причем в условиях частичных повреждений, получаемых во время ведения военных действий, в том числе и ядерной войны. С самого начала предполагалось, что связь в сети является ненадежной: любой ее сегмент может быть поврежден или уничтожен. И, тем не менее, сеть должна была обеспечивать связь между уцелевшими компьютерами.

Следующим этапом в развитии Интернет следует считать создание сети научного фонда США (NSF). Сеть, названная ***NSFNET*** и объединяющая научные центры США, основывалась на пяти суперкомпьютерах, соединенных между собой высокоскоростными линиями связи. Сеть NSFNET быстро заняла место ARPANET, которая в 1990 году была ликвидирована.

Быстрый рост числа пользователей сети требовал ее постоянной реорганизации, и в 1987 году был создан ***NSFNET Backbon*** – базовая часть, или хребет сети. Хребет состоял из тринадцати центров, соединенных друг с другом высокоскоростными линиями связи. Центры располагались в разных частях США. Одновременно создавались национальные сети в других странах. Компьютерные сети разных стран стали объединяться, и в 90-х годах сформировалась сеть Интернет в сегодняшнем виде.

Одним из последних и наиболее важных событий в истории Интернет стала разработка так называемой всемирной паутины – среды ***World Wide Web*** (WWW). История WWW началась в марте 1989 года, когда ученый Tim Bernes Lee выступил с проектом телекоммуникационной среды для проведения совместных исследований в области физики высоких энергий. И уже в 1991 году Европейская лаборатория практической физики (CERN) объявила на

весь мир о создании новой глобальной информационной среды WWW.

Суть этой среды состоит в том, что документ, к которому будет возможен доступ через Интернет, определенным образом форматируется с помощью гипертекстового языка. Информация может быть найдена в сети посредством так называемого универсального локатора ресурсов и отображена с помощью навигационных ***программ-браузеров***.

Рейтинг использования браузеров для компьютеров и планшетов на конец 2014 г.: Google Chrome – 40-47 %; Firefox – 17-18 %; Safari – 8-11 %; Opera – 1-2 %; прочие (Яндекс.Браузер, Internet Explorer и др.) – 2-3 %.

Международная статистика мобильных браузеров на конец 2014 г.: Google Chrome – 24-28 %, iPhone – 23-25 %, Android – 20-22 %, UC Browser – 8-10 %, Opera Mini/Mobile – 8-11 %, Nokia Browser – 2,5-4 %, IEMobile – 2-3 %, прочие – 4-5,5 %.

Административное устройство Интернет

Можно говорить только о некоторых элементах управления и регулирования Интернета, поскольку участие в Сети добровольное и в ней нет единого хозяина и централизованного управления.

По существу идет речь о совокупности сетей, подчиняющихся некоторым общим правилам, которые определяются особенностями используемой технологии, государственного регулирования и экономическими факторами.

Интернет – иерархическая структура, каждая из сетей которой отвечает за трафик (время передачи), за передачу информации в сеть более высокого уровня, а также за свое финансирование.

Укажем на следующие ***компоненты управления и регулирования Интернет в мировом сообществе***:

- *Внутренние правила сетей, входящих в Интернет*. На практике понятие регулирования с учетом различных источников финансирования привели к оформлению Правил приемлемого использования (Accepted Use Policy – AUP) для сетей, имеющих бюджетную поддержку.

- *Общественное регулирование Интернета.* Основным органом, осуществляющим регулирование Интернета, является Internet Society (ISOC) – общественная организация, ее финансовой

основой являются взносы участников и пожертвования спонсоров. ISOC проводит ежегодные конференции (INET), выпускает информационные материалы (Internet Society News), поддерживает информационные сервера.

Технические комитеты, поддерживающие системы стандартов, на которых базируется вся сеть:

Комиссия по архитектуре сети Интернет (Internet Architecture Board – IAB), ее основная задача – разработка и оформление стандартов взаимодействия готовых информационных систем.

IETF (Internet Engineering Task Force) – непосредственно отвечает за разработку протоколов и архитектуры Интернета.

IRTF (Internet Research Task Force) – исследовательское подразделение по развитию перспективных технологий Интернета.

IANA (Internet Assigned Numbers Authority) – ведет реестр всех идентификаторов, связанных с протоколами Интернета, поддерживает хранилище документов.

CERT (Internet Computer Emergency Response Team) – специализируется на вопросах безопасности сети.

RIPE (Reseaux IP Euopeens) – координация развития сетей в Европе, занимается распределением IP-номеров, развивает технические виды сервиса по маршрутизации и системы доменных имен.

InterNIC – центр сетевой информации, контролирует ресурсы Интернета (IP-номера, доменные имена, справочные службы и хранилища документов).

Информационный центр MERIT – центр специализированной информации, по маршрутизации, оптимизации адресного пространства и пр.

В России создано отделение ISOC – “РАЙНЕТ”. В рамках Ассоциации документальной электросвязи в России Интернет-комитет будет выполнять функции по сертификации Интернет-операторов.

Функции по администрированию домена RU, присвоению IP-номеров, поддержанию хранилища документов выполняет Российский НИИ развития общественных сетей (РосНИИРОС).

6.2. Структура и основные принципы построения сети Интернет

Internet – всемирная информационная компьютерная сеть, представляющая собой объединение множества региональных компьютерных сетей и компьютеров, обменивающих друг с другом информацией по каналам общественных телекоммуникаций (выделенным телефонным аналоговым и цифровым линиям, оптическим каналам связи и радиоканалам, в том числе спутниковым линиям связи).

Информация в Internet хранится на серверах. Серверы – это "мощные" компьютеры, работающие круглосуточно и постоянно подключенные к Интернету. Серверы имеют свои адреса и управляются специализированными программами. Серверы защищены от сбоев электропитания и работают под управлением операционной системы Unix. Они позволяют пересылать почту и файлы, производить поиск в базах данных, хранить и пересылать информацию по запросу компьютеров, отвечая при этом на десятки и сотни запросов одновременно и выполнять другие задачи.

Обмен информацией между серверами сети выполняется по высокоскоростным каналам связи (выделенным телефонным линиям, оптоволоконным и спутниковым каналам связи). Доступ отдельных пользователей к информационным ресурсам Internet обычно осуществляется через провайдера или корпоративную сеть.

Провайдер – поставщик сетевых услуг – лицо или организация предоставляющие услуги по подключению к компьютерным сетям. В качестве провайдера выступает некоторая организация, имеющая модемный пул для соединения с клиентами и выхода во всемирную сеть.

Основными ячейками глобальной сети являются локальные вычислительные сети. Если некоторая локальная сеть непосредственно подключена к глобальной, то и каждая рабочая станция этой сети может быть подключена к ней.

Существуют также компьютеры, которые непосредственно подключены к глобальной сети. Они называются хост - компьютерами (host – хозяин). Хост – это любой компьютер, являющийся постоянной частью Internet, т.е. соединенный по Internet – протоколу с другим хостом, который в свою очередь, соединен с другим, и так далее.

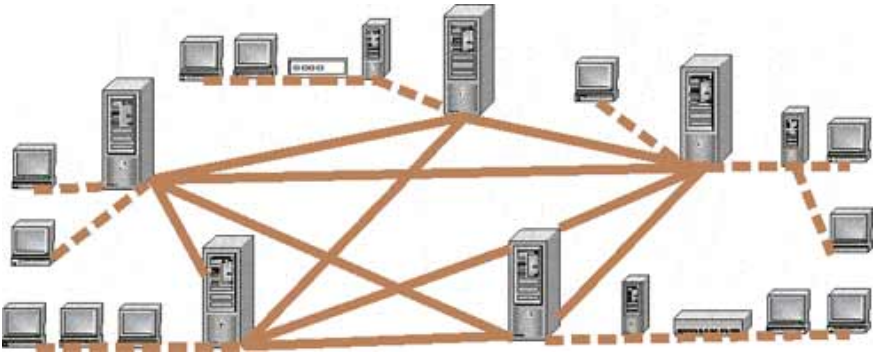


Рис. 6.1. Структура глобальной сети Internet

Для подсоединения линий связи к компьютерам используются специальные электронные устройства, которые называются сетевыми платами, сетевыми адаптерами, модемами и т.д.

Практически все услуги Internet построены на принципе клиент-сервер. Вся информация в Интернет хранится на серверах. Обмен информацией между серверами осуществляется по высокоскоростным каналам связи или магистралям. Серверы, объединенные высокоскоростными магистралями, составляют базовую часть сети Интернет.

Отдельные пользователи подключаются к сети через компьютеры местных поставщиков услуг Интернета, Internet-провайдеров (Internet Service Provider – ISP), которые имеют постоянное подключение к Интернет. Региональный провайдер, подключается к более крупному провайдеру национального масштаба, имеющего узлы в различных городах страны. Сети национальных провайдеров объединяются в сети транснациональных провайдеров или провайдеров первого уровня. Объединенные сети провайдеров первого уровня составляют глобальную сеть Internet.

Передача информации в Интернет обеспечивается благодаря тому, что каждый компьютер в сети имеет уникальный адрес (IP-адрес), а сетевые протоколы обеспечивают взаимодействие разнотипных компьютеров, работающих под управлением различных операционных систем.

В основном в Интернет используется семейство сетевых протоколов (стек) TCP/IP. На канальном и физическом уровне стек

TCP/IP поддерживает технологию Ethernet, FDDI и другие технологии. Основой семейство протоколов TCP/IP является сетевой уровень, представленный протоколом IP, а также различными протоколами маршрутизации. Этот уровень обеспечивает перемещение пакетов в сети и управляет их машрутизацией. Размер пакета, параметры передачи, контроль целостности осуществляется на транспортном уровне TCP.

Прикладной уровень объединяет все службы, которые система предоставляет пользователю. К основным прикладным протоколам относятся:

- протокол удаленного доступа telnet,
- протокол передачи файлов FTP,
- протокол передачи гипертекста HTTP,
- протоколы электронной почты: SMTP, POP, IMAP, MIME.

6.3. Способы доступа в Интернет

В настоящее время известны следующие способы доступа в Интернет:

1. Dial-Up (когда компьютер пользователя подключается к серверу провайдера, используя телефон) – коммутируемый доступ по аналоговой телефонной сети скорость передачи данных до 56 Кбит/с;

2. DSL (Digital Subscriber Line) – семейство цифровых абонентских линий, предназначенных для организации доступа по аналоговой телефонной сети, используя кабельный модем. Эта технология (ADSL, VDSL, HDSL, ISDL, SDSL, SHDSL, RADSL под общим названием xDSL) обеспечивает высокоскоростное соединение до 50 Мбит/с (фактическая скорость до 2 Мбит/с). Основным преимуществом технологий xDSL является возможность значительно увеличить скорость передачи данных по телефонным проводам без модернизации абонентской телефонной линии. Пользователь получает доступ в сеть Интернет с сохранением обычной работы телефонной связи;

3. ISDN – коммутируемый доступ по цифровой телефонной сети. Главная особенность использования ISDN – это высокая скорость передачи информации, по сравнению с Dial-Up доступом. Скорость передачи данных составляет 64 Кбит/с при использовании одного и 128 Кбит/с, при использовании двух каналов связи;

4. Доступ в Интернет по выделенным линиям (аналоговым и цифровым). Доступ по выделенной линии – это такой способ подключения к Интернет, когда компьютер пользователя соединен с сервером провайдера с помощью кабеля (витой пары) и это соединение является постоянным, т.е. некоммутируемым, и в этом главное отличие от обычной телефонной связи. Скорость передачи данных до 100 Мбит/с.

5. Доступ в Интернет по локальной сети (Fast Ethernet). Подключение осуществляется с помощью сетевой карты (10/100 Мбит/с) со скоростью передачи данных до 1 Гбит/с на магистральных участках и 100 Мбит/сек для конечного пользователя. Для подключения компьютера пользователя к Интернет в квартиру подводится отдельный кабель (витая пара), при этом телефонная линия всегда свободна.

6. Спутниковый доступ в Интернет или спутниковый Интернет (DirecPC, Europe Online). Спутниковый доступ в Интернет бывает двух видов – ассиметричный и симметричный:

- Обмен данными компьютера-пользователя со спутником двухсторонний;
- Запросы от пользователя передаются на сервер спутникового оператора через любое доступное наземное подключение, а сервер передает данные пользователю со спутника. Максимальная скорость приема данных до 52,5 Мбит/с (реальная средняя скорость до 3 Мбит/с).

7. Доступ в Интернет с использованием каналов кабельной телевизионной сети *(Кабельный Интернет (“coax at a home”))*. Скорость приема данных от 2 до 56 Мб/сек. В настоящее время известны две архитектуры передачи данных это симметричная и асимметричная архитектуры. Кроме того, существует два способа подключения: а) кабельный модем устанавливается отдельно в каждой квартире пользователей; б) кабельный модем устанавливается в доме, где живет сразу несколько пользователей услуг Интернета. Для подключения пользователей к общему кабельному модему используется локальная сеть и устанавливается общее на всех оборудование Ethernet.

8. Беспроводные технологии последней мили:

- WiFi
- WiMax
- RadioEthernet

- MMDS
- LMDS
- Мобильный GPRS-Интернет
- Мобильный CDMA- Internet

WiFi (Wireless Fidelity – точная передача данных без проводов) – технология широкополосного доступа к сети Интернет. Скорость передачи информации для конечного абонента может достигать 54 Мбит/с. Радиус их действия не превышает 50 – 70 метров. Беспроводные точки доступа применяются в пределах квартиры или в общественных местах крупных городов. Имея ноутбук или карманный персональный компьютер с контроллером Wi-Fi, посетители кафе или ресторана (в зоне покрытия сети Wi-Fi) могут быстро соединиться с Интернетом.

WiMAX (Worldwide Interoperability for Microwave Access), аналогично WiFi – технология широкополосного доступа к Интернет. WiMAX, в отличие от традиционных технологий радиодоступа, работает и на отраженном сигнале, вне прямой видимости базовой станции. Информацию можно передавать на расстояния до 50 км со скоростью до 70 Мбит/с.

В настоящее время WiMAX частично удовлетворяет условиям сетей 4G, основанных на пакетных протоколах передачи данных. К семейству 4G относят технологии, которые позволяют передавать данные в сотовых сетях со скоростью выше 100 Мбит/сек. и повышенным качеством голосовой связи. Для передачи голоса в 4G предусмотрена технология VoIP.

RadioEthernet – технология широкополосного доступа к Интернет, обеспечивает скорость передачи данных от 1 до 11 Мбит/с, которая делится между всеми активными пользователями. Для работы RadioEthernet-канала необходима прямая видимость между антеннами абонентских точек. Радиус действия до 30 км.

MMDS (Multichannel Multipoint Distribution System). Эти системы способна обслуживать территорию в радиусе 50—60 км, при этом прямая видимость передатчика оператора является не обязательной. Средняя гарантированная скорость передачи данных составляет 500 Кбит/с – 1 Мбит/с, но можно обеспечить до 56 Мбит/с на один канал.

LMDS (Local Multipoint Distribution System) – это стандарт сотовых сетей беспроводной передачи информации для фиксированных абонентов. Система строится по сотовому

принципу, одна базовая станция позволяет охватить район радиусом в несколько километров (до 10 км) и подключить несколько тысяч абонентов. Сами базовые станции объединяются друг с другом высокоскоростными наземными каналами связи либо радиоканалами (RadioEthernet). Скорость передачи данных до 45 Мбит/с.

Мобильный GPRS-Интернет. Для пользования услугой "Мобильный Интернет" при помощи технологии GPRS необходимо иметь телефон со встроенным GPRS-модемом и компьютер. Технология GPRS обеспечивает скорость передачи данных до 114 Кбит/с. При использовании технологии GPRS тарифицируется не время соединения с Интернетом, а суммарный объем переданной и полученной информации.

Технология GPRS – это усовершенствование базовой сети GSM или протокол пакетной коммутации для сетей стандарта GSM. EDGE является продолжением развития сетей GSM/GPRS. Технология EDGE (улучшенный GPRS или EGPRS) обеспечивает более высокую скорость передачи данных по сравнению с GPRS (скорость до 200 Кбит/сек). EDGE (2,5 G) – это первый шаг на пути к 3G технологии.

Мобильный CDMA-Internet. Сеть стандарта CDMA – это стационарная и мобильная связь, а также скоростной мобильный интернет. Для пользования услугой "Мобильный Интернет" при помощи технологии CDMA необходимо иметь телефон со встроенным CDMA – модемом или CDMA модем и компьютер. Технология CDMA обеспечивает скорость передачи данных до 153 Кбит/с или до 2400 Кбит/с – по технологии EV-DO Revision 0.

В настоящее время технология CDMA предоставляет услуги мобильной связи третьего поколения. Технологии мобильной связи 3G (third generation – третье поколение) – набор услуг, который обеспечивает как высокоскоростной мобильный доступ к сети Интернет, так и организовывает видеотелефонную связь и мобильное телевидение. Мобильная связь третьего поколения строится на основе пакетной передачи данных. Сети третьего поколения 3G работают в диапазоне около 2 ГГц, передавая данные со скоростью до 14 Мбит/с.

Сети третьего поколения 3G реализованы на различных технологиях, основанных на следующих стандартах: W-CDMA (Wideband Code Division Multiple Access) и его европейском

варианте – UMTS (Universal Mobile Telecommunication System), который является приемником GSM/GPRS/EDGE; CDMA2000 1X, являющимся модификацией стандарта CDMA; китайским вариантом – TD-CDMA/TD-SCDMA.

9. В настоящее время для “последних метров” доступа в Internet применяются технологии ***Home PNA (HPNA)*** и ***HomePlug***. Доступ в Интернет по выделенным линиям Home PNA или HPNA (телефонным линиям) и доступ через бытовую электрическую сеть напряжением 220 вольт (HomePlug, Plug – это штепсель).

Обычно доступ к Интернету по выделенным линиям Home PNA и HomePlug комбинируется с такими методами доступа как DSL, WiFi, и другими, т.е. для “последних метров” доступа применяются технологии Home PNA и HomePlug, а в качестве “последней мили” доступа используются DSL, WiFi и другие технологии.

Скорость передачи данных HPNA 1.0 составляет 1 Мбит/с, а расстояние между наиболее удаленными узлами не превышает 150 метров. Спецификация HomePNA 2.0 обеспечивает доступ со скоростью до 10 Мбит/с и расстояние до 350 м.

Технология Home PNA применяется в основном для организации домашней сети с помощью сетевых адаптеров. Подключение к глобальной сети можно осуществить с помощью роутера через сети общего доступа. Кроме того, технология HPNA предназначена для организации коллективного доступа в Интернет (например, для подключения жилого дома или подъезда дома к Интернет по существующей телефонной проводке). Телефонную линию при этом можно использовать для ведения переговоров.

Стандарт HomePlug 1.0 доступ к Интернет через бытовую электрическую сеть поддерживает скорость передачи до 14 Мбит/с. максимальная протяжённость между узлами до 300 м. Компания Renesas, выпустила модем в виде штепсельной вилки для передачи данных по электросетям.

Технология PLC (Power Line Communication) позволяет передавать данные по высоковольтным линиям электропередач, без дополнительных линий связи. Компьютер подключается к электрической сети и выходит в Интернет через одну и ту же розетку. Для подключения к домашней сети не требуется никаких дополнительных кабелей. К домашней сети можно подключить

различное оборудование: компьютеры, телефоны, охранную сигнализацию, холодильники и т.д.

Основные сервисы Интернет

Электронная почта (E-mail) – это метод передачи сообщений электронным способом. Поставщик услуг Интернет (провайдер) открывает клиенту электронный почтовый ящик, в который будет попадать направляемая пользователю корреспонденция. Этому почтовому ящику ставится в соответствие адрес почты, так называемый E-mail и пароль. На самом деле пользователю предоставляется возможность сохранять определенный объем информации на компьютере провайдера. При обмене почтовыми сообщениями отправителю и получателю не нужно одновременно быть на линии связи. Отправляемые сообщения попадают в почтовый ящик, откуда их можно взять в удобное для себя время.

Для работы с электронной почтой используются несколько протоколов.

Протокол ***SMTP*** – Simple Mail Transfer Protocol был разработан для обмена почтовыми сообщениями в сети Интернет.

Протокол ***POP3*** – Post Office Protocol предназначен для разбора почты из почтовых ящиков пользователей на их рабочие места при помощи программ-клиентов. Если по протоколу SMTP пользователи отправляют корреспонденцию через Интернет, то по протоколу POP3 (после проверки прав доступа) пользователи получают корреспонденцию из своих почтовых ящиков на почтовом сервере в локальные файлы.

Протокол ***IMAP*** – Interactive Mail Access Protocol является другим протоколом разбора почты, который по своим возможностям очень похож на POP3, но был разработан как более надежная альтернатива последнего и к тому же обладает более широкими возможностями по управлению процессом обмена с сервером. Главным отличием от POP3 является возможность поиска нужного сообщения и синтаксический анализ сообщений.

В последнее время наиболее популярными программами для работы с электронной почтой являются Outlook Express и TheBat.

Группы новостей USENET NEWS – это огромная, базирующаяся на сообщениях, электронная доска объявлений.

Группы новостей сегодня чаще называют телеконференциями. В отличие от электронной почты информация в группах новостей доступна для всеобщего обозрения. Для удобства дискуссий образованы различные группы, участники которых посылают и принимают сообщения по определенной тематике.

NetMeeting – программа, позволяющая общаться голосом через Интернет. Если хорошая скорость, разговор идет как по телефону. Поддерживает одновременно несколько собеседников. Кроме голосового обмена информацией есть возможность использовать "доску" (типа Paint), где каждый может что-то нарисовать, и все остальные это увидят.

Iphone – похож на NetMeeting, но поддерживает видео передачу.

Telnet – позволяет превращать компьютер пользователя в удаленный терминал другого компьютера, т.е. предоставляет в распоряжение пользователя большинство ресурсов удаленного компьютера. Этот сервис еще называется эмуляцией удаленного терминала. На практике он используется нечасто.

FTP (File Transfer Protocol) – протокол передачи файлов – позволяет получать и передавать файлы. Этот сервис и сегодня является самым распространенным для получения программных продуктов и другой информации негиперстекстового характера.

WWW (World Wide Web) – ***Всемирная паутина*** – сервис, позволяющий работать с гипертекстовыми и гипермедиа документами. Для работы с WWW используется специальный протокол HTTP – Hyper Text Transfer Protocol (протокол передачи гипертекста). Гипертекстовые документы создаются с помощью специального языка HTML – Hyper Text Markup Language (язык разметки гипертекста). Документ, подготовленный с помощью этого языка и доступный для просмотра пользователем, называется Web-страницей.

Archie – позволяет найти файл в Интернет по его имени. Однако в последнее время этот сервис стал менее популярным, т.к. в WWW появились поисковые системы, позволяющие выполнить поиск более простым способом.

Gopher – это система файловых серверов, которая служит для хранения и поиска только текстовой информации. В настоящее время используется редко.

WAIS (Wide Area Information Service) – ***Информационный сервис*** широкой области - система поиска информации по ключевому слову.

IRC (Интернет Chat Relay) – ***Беседа через Интернет***. Эта система чем-то похожа на группы новостей, но обмен сообщениями ведется без задержек. Подключившись к группе пользователей, обсуждающих ту или иную проблему, можно набрать свое сообщение на клавиатуре, и оно мгновенно станет доступным другим участникам беседы. В свою очередь вы видите вопросы и ответы, вводимые другими пользователями, подключившимися к вам в одной разговорной группе или комнате (chat room), которые сейчас часто называют просто "чатами".

ICQ (I seek you) – ***"Я ищу тебя"***. Эта служба также предназначена для организации общения через Интернет, но предоставляет и ряд дополнительных возможностей, например, поиск сетевого IP-адреса человека, подключенного в данный момент к Интернет.

Интернет-телефония (IP-телефония) – технология, в которой голосовой трафик частично передается через телефонную сеть общего пользования, а частично – через Интернет. Именно таким образом осуществляются звонки с телефона на телефон, с компьютера на телефон, с телефона на компьютер (здесь вместо номера телефона используется IP-адрес), а также ставший в последнее время особенно популярным Surf'n'Call – звонок с Web-браузера на телефон.

Существует еще много интересных направлений использования Интернет, например ***получение радио- и телепередач***.

Сервисы глобальных сетей

Какие услуги доступны в Интернете?

1. Веб-сервис. Коллективный доступ в режиме чтения с разных компьютеров к одному хранилищу информации (сайту или веб-сайту), представленной в "человеческом" медиаформате – в виде комбинации текста, звука, изображения, видео.

Сайт – комплект связанных гиперссылками документов (веб-страниц), доступных в Интернете, для просмотра с помощью программы-обозревателя.

Гиперссылка – это часть электронного документа, указывающая на другое место в данном документе (внутренняя гиперссылка) либо на другой документ или файл (внешняя гиперссылка).

Веб-сервис, как правило, доступен в режиме online – во время работы пользователя в сети. Новостные сайты предлагают подписку на новостные ленты или тематические новости и рассылку их пользователям. Доступ к информации однонаправленный: группа специалистов готовит информацию для широкого круга пользователей и поддерживает ее обновление. Пользователи (читатели) не могут оказывать непосредственного влияния на создателей сайта и на его содержимое. Хотя могут создателям или владельцам сайта посылать письма по электронной почте или делать отметки о качестве просмотренных материалов.

2. Форум – двусторонний обмен текстовой и графической информацией в режиме offline. Информация, как правило, определенной тематической направленности "выкладывается" одними пользователями в "общее" место и в любой момент времени доступна другим пользователям. Естественно, что выкладывание сообщения и его чтение происходят в режиме online. Разновидностью форумов является другая форма диалогового обмена информацией в сети – *FAQ*, (часто задаваемые вопросы), которые представляют собой списки ранее заданных пользователями форума вопросов с "готовыми" ответами.

3. Хостинг – услуга размещения файлов сайта на сервере в сети (как правило, Интернет), на котором запущено программное обеспечение для обработки запросов к файлам (веб-сервер). Владелец сайта должен заниматься продвижением сайта (чтобы сайт стал заметным, посещаемым) и его постоянным обновлением (поддержкой).

4. Электронная почта – пересылка текстовых сообщений с возможностью приложения к письму файлов. Режим доступа – при отправке и получении писем online, отправка и получение могут быть разнесены во времени на интервал до нескольких суток.

5. Чат – обмен текстовыми сообщениями в условиях Double Online, т.е. все "разговаривающие" должны быть в сети одновременно. В настоящее время, как и форумы, чат вытесняется программами универсального мультимедийного online-общения. Программы *Google Talk* и *Skype* позволяют не только обмениваться

текстовыми сообщениями, но одновременно и разговаривать и видеть собеседника.

6. Пересылка файлов – однонаправленное копирование (т.е. режим только чтение) с удаленного компьютера файлов и структуры папок. Обычно переход к скачиванию файлов осуществляется по гиперссылке с веб-сайта. Возможен как режим online, так и режим offline для пользователя, когда обновление системного и прикладного программного обеспечения проводится автоматически по определенному расписанию.

7. Файлообменные сети – одноранговые полносвязные сети, работающие по протоколу P2P (peer-to-peer, P2P – равный-равному, клиент-клиенту). Иногда этот протокол называют *BitTorrent* (битовый поток). Каждый клиент такой сети может запросить и получить файлы целиком или их фрагменты от другого клиента, который на момент передачи становится “де-факто” отдающим – сервером. Число клиентов и отдающих серверов в сети велико и постоянно меняется.

8. Удаленный доступ к ресурсам и программному обеспечению другого компьютера, включая удаленное администрирование (т.е. удаленную настройку компьютера и запуск на нем исполняемых программ).

9. Телеконференции – обмен информацией в режиме online для всех участников. Пример использования телеконференции в профессии – телеконференции в практике проведения судебных заседаний для общения с “виртуально присутствующим” осужденным или свидетелем, находящимся “под защитой”.

10. Социальная сеть в Интернете – сообщество из людей со схожими интересами и (или) деятельностью. Связь осуществляется через сервис внутренней почты или путем мгновенного обмена сообщениями. На сайте сети можно указать информацию о себе (дату рождения, школу, вуз, любимые занятия и др.), по которой аккаунт пользователя найдут другие участники. Различаются открытые и закрытые социальные сети. Используется система “друзей” и “групп”. Популярные русскоязычные: В Контакте (vkontakte.ru), Одноклассники.ru.

11. Блог (от “веб” и “лог”, т.е. веб-дневник) – сетевой дневник, минисайт, создаваемый, редактируемый, наполняемый постингами (записями) самим пользователем и его комментаторами. Создание блога и выбор дизайна не требует профессиональных знаний и

занимает несколько минут. При правильном выборе тематики и содержания можно объединить большие сообщества пользователей (корпоративные блоги, блог города, студенческий блог и т.п.). Популярные русскоязычные площадки размещения блогов: Живой журнал (livejournal.com), Liveiternet.ru, mail.ru.

К недостатку блогов относится возможность размещения ложной, клеветнической информации, искажения авторской информации из-за низкой защищенности.

6.4. Системы адресации в Интернет

Для однозначного определения компьютера в Интернет применяется система адресов, называемая ***IP-адресами***. Адреса компьютеров в Интернет состоят из разделенных точками четырех чисел, каждое из которых не превышает 255. Например: 194.85.26.130.

IP-адрес может быть постоянным или изменяемым. Изменяемый IP-адрес обычно назначается сервером провайдера для тех компьютеров, которые используют коммутируемое IP-соединение.

Вся доступная IP-адресация в Интернет разделена на несколько групп сетей, часть из них используется непосредственно для адресации компьютеров – A, B, C; часть для служебных и иных целей – D, E.

Существует несколько специальных IP-адресов. Так, например, адрес 127.0.0.1 определяет локальную машину пользователя и используется для тестирования программ. При этом данные не передаются.

Из-за огромного роста числа компьютеров в Интернет привел к тому, что сети классов A и B можно считать исчерпанными и еще осталась некоторая свобода в множестве сетей класса C.

Числовые адреса используются компьютерами для связи между машинами, но они неудобны для запоминания и использования людьми. Поэтому в Интернет поддерживается ***система имен доменов*** (Domain Name System – DNS), в которой каждому компьютеру наряду с IP-адресом присваивается уникальное имя. DNS иногда еще называют ***региональной системой наименований***. Компьютеры при пересылке используют цифровые адреса, а пользователи применяют доменные имена.

В имени может быть любое число доменов, но более пяти встречается редко. Каждый последующий домен в имени (если смотреть слева направо) больше предыдущего. В имени ***ux.cso.uiuc.edu*** элемент ***ux*** – имя реального компьютера с IP – адресом. Имя этого компьютера создано и курируется группой ***cso,*** которая есть не что иное, как отдел, в котором стоит этот компьютер. Отдел ***cso*** является отделом университета штата Иллинойс (***uiuc***). ***uiuc*** входит в национальную группу учебных заведений (***edu***). Таким образом, домен ***edu*** включает в себя все компьютеры учебных заведений США; домен ***uiuc.edu*** – все компьютеры университета штата Иллинойс и т.д. Каждая группа может создавать и изменять все имена, находящиеся под её контролем.

Домены верхнего уровня бывают двух типов.

• Географические (двухбуквенные – каждой стране соответствует двухбуквенный код). Например, ***ru*** – код России; ***ca*** – код Канады и т.п. Общее число кодов стран – 300.

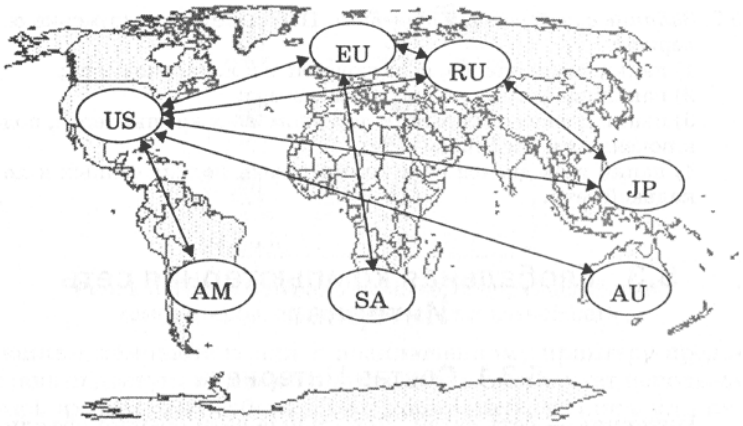


Рис. 6.2. Региональные компьютерные сети, объединенные в глобальную сеть Интернет

• Административные (трехбуквенные). Домены этого типа были созданы, когда была изобретена доменная система. Изначально было шесть организационных доменов высшего уровня и все они относились к сетям США (таблица):

Домены высшего уровня

№ п/п	Домен	Использование
1	com	Коммерческие организации
2	edu	Учебные заведения (университеты, средние школы и т.д.)
3	gov	Правительственные учреждения (кроме военных)
4	mil	Военные учреждения (армия, флот и т.д.)
5	org	Прочие организации
6	net	Сетевые ресурсы

Однако на сегодняшний день по доменам второго типа уже нельзя определить национальную принадлежность адреса, к тому же их список был значительно расширен, появились 4-х и 5-ти буквенные домены:

• ***firm*** – для деловых ресурсов Сети;

• ***store*** – для торговли;

• ***web*** – для организаций, имеющих отношение к регулированию деятельности в WWW;

• ***arts*** – для ресурсов гуманитарного образования;

• ***rec*** – игры и развлечения;

• ***info*** – предоставление информационных услуг;

• ***nom*** – для индивидуальных ресурсов.

При работе в Интернет используются не просто доменные имена, а универсальные указатели ресурсов URL (Uniform Resource Locator). URL-адрес – это адрес любого ресурса в Интернет с указанием того, с помощью какого протокола к нему следует обращаться. Иными словами, в указателе кроме собственно адреса имеются сведения, какую программу следует запустить на сервере и к какому файлу следует обратиться. Например:

http:// указатель на гипертекстовую страницу;

ftp:// указатель на доступ через FTP.

Например: ***http://www.whitehouse.gov*** – США, Белый дом.

Если имена начинаются на аббревиатуру WWW, то это говорит о гипертекстовом характере материала, поэтому при вводе этих имен протокол HTTP можно не указывать, он подразумевается. Например, ***www.whitehouse.gov***.

Часто адрес дополняется символами, записанными после имени домена старшего уровня через косую черту “/”. Это дальнейшая детализация адреса ресурса в Интернет. Обычно это имя каталога на указанном сервере и, возможно, имя конкретного файла. Так, адрес www.microsoft.com/ru указывает на каталог ru на Web-сервере корпорации Microsoft.

Построение почтовых адресов в Интернет имеет свои особенности. Как ранее отмечалось, адрес электронной почты принято называть E-mail. Он включает в себя имя конкретного пользователя, знак @ и несколько сегментов, разделенных точками, как в ссылках на WWW-страницы. Например, адрес службы технической поддержки одного из популярных в Москве провайдеров выглядит следующим образом: ***support@mtu.ru***

В данном случае в качестве имени использовано слово support, а местом расположения почтового ящика является сервер mtu.ru.

6.5. Понятие Интернет-протокола TCP/IP

Протокол – это правила, предписанные компьютерам для работы в сети Интернет. Сетевые протоколы строятся по многоуровневому принципу. На нижнем уровне используются два основных протокола: ***IP***-Интернет Protocol (Протокол Интернет) и ***TCP***-Transmission Control Protocol (Протокол управления передачей).

Протокол ***IP*** обеспечивает маршрутизацию (доставку по адресу) сетевых пакетов. Протокол ***TCP*** отвечает за надежность передачи больших объемов информации, обрабатывает и устраняет сбои в работе сети. ***TCP-протокол*** делит длинные сообщения на несколько пакетов (от 1 до 1500 байт каждый), каждый из которых помещается в TCP-конверт и после этого в IP-конверт. Каждый TCP-конверт помечается определенным образом, чтобы после разбивки сообщение вновь можно было собрать в единое целое.

Протоколы TCP и IP тесно взаимосвязаны, и их часто объединяют, говоря, что в Интернет базовым является протокол ***TCP/IP***. Схема функционирования протокола TCP/IP представлена на рисунке 6.3.

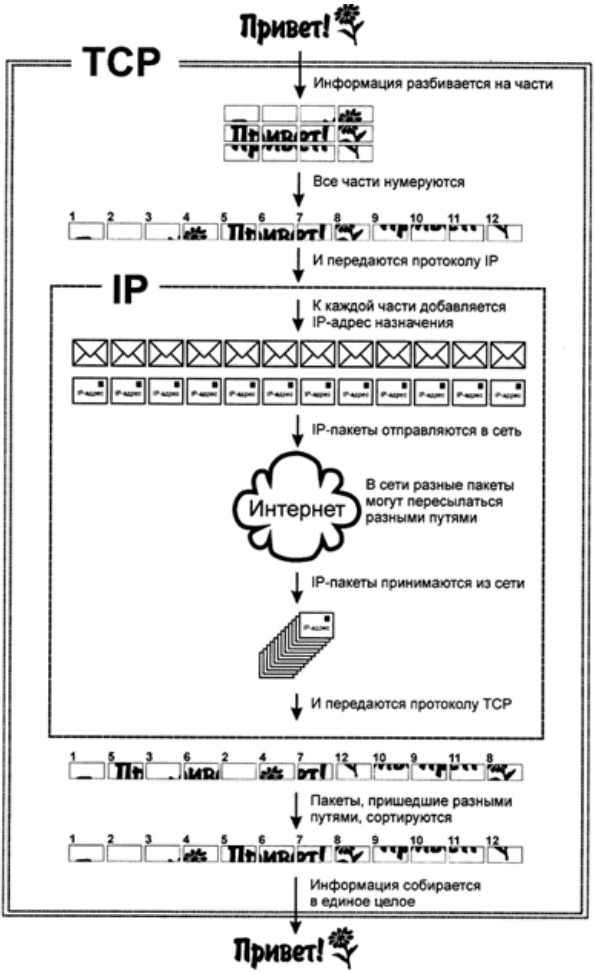


Рис. 6.3. Схема функционирования протокола TCP/IP

Имеется другой стандартный протокол транспортного уровня, который не отягощен такими накладными расходами, как TCP.

Этот протокол называется ***UDP*** – User Datagram Protocol – протокол пользовательских дейтаграмм. UDP проще TCP, поскольку он не заботится о возможной пропаже данных, пакетов, о сохранении правильного порядка данных и т.д. UDP используется для клиентов, которые посылают только короткие сообщения и

могут просто заново послать сообщение, если отклик подтверждения не придет достаточно быстро. Протокол UDP сохраняет границы сообщений, определяемые прикладным процессом. Он не объединяет несколько сообщений в одно целое и не делит одно сообщение на части.

6.6. Поиск информации в Интернет

Информационный поиск – последовательность операций, направленных на предоставление информации заинтересованным лицам. Поиск выполняется в четыре этапа:

1) определение информационной потребности и держателя информационного массива;

2) формулировка запроса;

3) извлечение информации из информационного массива;

4) ознакомление с полученной информацией и оценка результатов поиска.

Информационный поиск в совокупности информационных ресурсов, массивов документов, базах данных, знаний реализуется с помощью автоматизированных информационно-поисковых систем.

В обычной библиотеке информационный массив подразумевает наличие классификации и специализации знаний по областям. В Интернете нет глобального каталога всех ресурсов и главного редактора, часть информации имеет низкое качество.

Поэтому там легко потратить время впустую. Однако есть средства и методы вести эффективный поиск.

К основным средствам поиска информации в Интернете относятся (таблице):

• поисковые и метапоисковые системы (поиск конкретных документов);

• индексированные каталоги (поиск тематических сайтов по структуре рубрик);

• адреса популярных поисковых систем и каталогов сети Интернет;

• рейтинги (топы) наиболее посещаемых ресурсов;

• тематические списки ссылок (тематические порталы-указатели);

• сетевые энциклопедии и справочники с определениями понятий и справочными данными.

Российские поисковые системы

Поисковые системы	Основные характеристики поисковой системы
1	2
Яндекс (www.yandex.ru, www.ya.ru.) *Поисковая система и каталог*	В настоящее время – лучшая поисковая система России. На середину 2010 года декларирована индексация более 10 миллиардов оригинальных документов (страниц) с российских и зарубежных русскоязычных серверов, а также серверов на территории бывшего СССР. Яндекс – единственная российская поисковая система, индексирующая документы в форматах PDF, DOC, RTF, PPT, XLS и SWF. Обладает большим количеством сервисных функций.
Google (www.google.ru) *Международная поисковая система и каталог*	Локализованный российский вариант глобальной поисковой системы, которая на сегодня является абсолютным мировым лидером по объему проиндексированных документов (порядка 3 триллионов), быстроте обработки запроса и корректности ранжирования результатов поиска.
Bing! (www.bing.com) *Поисковая система*	Русскоязычный вариант бета-версии поисковой системы, запущенной компанией Microsoft в середине 2009 года. Пока не обладает преимуществами, позволяющими ей опередить Google. Объем индексного файла в настоящее время сопоставим с аналогичными показателями Google, однако по всем остальным параметрам и, прежде всего, по степени определения релевантности результатов, Bing значительно уступает своему главному конкуренту.
Рамблер (www.rambler.ru) *Поисковая система и каталог Top 100*	Является первой российской профессиональной поисковой системой, действующей с 1996 года. В конце 2002 года была произведена коренная модернизация, после которой Rambler вновь вошел в группу лидеров сетевого поиска. В настоящее время объем индекса составляет порядка 150 миллионов документов. Интерфейс без рекламы расположен по адресу http://www.r0.ru.
Mail.ru (www.mail.ru) *Поисковая система и каталог*	Поисковый модуль компании Mail.ru, запущенный в 2008 году. В качестве программного “движка” используется не собственная разработка компании, а поисковый модуль Google. Это обеспечивает данной поисковой системе высокие качественные характеристики. Сбор и индексирование информации осуществляется системой самостоятельно – этим определяются разные результаты запроса в Google и ПОИСК@mail. Форма "Расширенного поиска" также дает возможность ограничить разыскания определенными типами файлов (PDF, DOC, XLS, PPT), местом положения искомых слов в документе или определенным доменом.

Продолжение таблицы

1	2
Nigma (www.nigma.ru) *Метапоисковая система и каталог*	Экспериментальный проект в области сетевого поиска (мета-поисковая система), в основе которого заложено применение искусственного интеллекта. Nigma в ряде случаев способна интуитивно предвидеть запрос и выдавать ответ без обращения к первоисточникам, решать формулы, расшифровывать сокращения, давать уточняющие подсказки при разысканиях на английском языке. Также осуществляется поиск иллюстраций и аудиофайлов.

Поисковая система в Интернете – специальный вебсайт, на котором можно сделать запрос и получить ссылки на документы и сайты, соответствующие запросу. В состав поисковой системы может входить несколько мощных серверов (в системе Google – более 10 000 компьютеров).

Интерфейс поисковой страницы обеспечивает возможность формулировать в строке текстовый запрос, посылать его, просматривать полученный в ответ список ссылок и переходить по их адресам.

Программное обеспечение поисковой системы состоит из трех компонентов:

- поисковый робот,
- индекс системы,
- классификатор.

Поисковый робот – программа-анализатор, непрерывно посещающая веб-адреса в Интернете, просматривает и исследует содержание документов, индексирует слова из текста и заносит в базу данных (обновляет её).

База данных индексов – создаваемая по результатам поиска таблица: “слово – адрес документа, где слово встречается”. Поисковый робот периодически обновляет базу данных, находя новые материалы, убирая неработающие ссылки. Когда посетитель делает запрос, поиск адресов ведется не в Интернете, а в заготовленной базе данных сервера.

Классификатор – программа, которая:

а) обрабатывает запрос пользователя;

б) находит и извлекает с помощью индекса слов из базы данных ссылки, отвечающие критериям запроса;

в) выводит список ссылок на найденные документы в порядке убывания релевантности (определяет их соответствие, “вес”,

значимость и выполняет сортировку), сверху списка самые подходящие адреса.

Особо мощные поисковые системы учитывают популярность сайта по числу посещений и ссылок на него с других сайтов, оценивают страницы по числу других связанных важных страниц. Алгоритмы ранжирования (оценивания) важности могут отличаться, сайт может занимать 5-е место по одним рейтингам и 30-е – по другим.

Поисковые системы в списке ссылок могут предложить не только прямой переход к документу и его сайту, но и текст с выделением слов, заявленных в запросе, а также сохраненную копию основного текста документа из своего архива (без рисунков и гиперссылок, иногда без форматирования). Сохраненная в архиве поисковой системы копия удобна тем, что загружается быстрее, можно получить документ, недоступный на исходном сервере, или преобразование формата doc, pdf в формат HTML.

Метапоисковая система – система поиска, не имеющая собственной базы данных, но обладающая программными возможностями запрашивать данные у нескольких других поисковых сайтов, анализировать полученное, следуя собственному алгоритму обработки, предоставлять сводный результат.

Напомним, что метаданные – данные о данных: каталоги, справочники, реестры, базы метаданных, содержащие сведения о составе данных, содержании, статусе, происхождении, местонахождении, качестве, форматах и формах представления, условиях доступа. Метаинформация – описание информации, информация об информации.

Некоторые каталоги содержатся в поисковых системах и позволяют поиск и по ключевым словам, и по иерархическому дереву разделов. Если же необходимо найти конкретный документ, то каталог малоэффективен. Иногда часть приводимых в тематических коллекциях ссылок не работает.

Полезно обращаться к топам (tops) – спискам наиболее посещаемых сайтов по конкретной тематике. Высокая посещаемость сайта свидетельствует о качественном содержании, сервисе.

Крупные поисковые системы и каталоги ресурсов Интернета стали порталами – предлагают разнообразную информацию, новости, дополнительные услуги: бесплатную электронную почту, место для размещения веб-страниц, поддерживают форумы.

Поисковые системы Интернета на первых позициях списка ресурсов, предлагаемых по запросу посетителя, размещают так называемые оплаченные и «управляемые результаты» и коммерческую рекламу товаров и услуг различных компаний, искусственно повышая их рейтинг. Рекламодатели покупают право контекстной рекламы на конкретные темы запросов. Оплаченные ссылки не обязательно отличаются оформлением от обычных результатов поиска.

Особая деятельность поисковых систем

Поисковые системы вносят в базы данных оказавшиеся доступными страницы, в том числе и те, которые им удалось найти из-за неосторожности или программных ошибок администратора сервера, сайта. Новые возможности возникли с появлением современных продвинутых поисковых систем. Организации, применяющие электронный документооборот, часто размещают на серверах файлы для внутреннего пользования (скрытые файлы). Поисковые программы ведут поиск не только веб-страниц, но и связанных с ними ссылками файлов документов форматов RTF, Word, Excel, PowerPoint, Works, Write, Adobe PostScript. Язык запросов поисковой системы Google позволяет проникать на серверы глубже веб-содержания и даже находить скрытые документы, преодолевая не очень сложные средства защиты от постороннего доступа. В результате такого “углубленного” поиска поисковая система сохраняет копии документов внутреннего назначения (того, что не получить при прямом посещении сайта) и предоставляет их просмотр из своей базы данных. Поэтому, когда не приняты дополнительные меры защиты, на сервер, к которому есть доступ из Интернета, не следует выносить документы, не предназначенные для посторонних.

6.7. Контрольные вопросы

1. История создания Интернет
2. Административное устройство Интернет
3. Структура и основные принципы построения сети Интернет
4. Способы доступа в Интернет
5. Основные сервисы Интернет

6. Принципы работы с e-mail
7. Системы адресации в Интернет
8. Понятие Интернет-протокола TCP/IP
9. Поиск информации в Интернет

7. СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Локальная вычислительная сеть (ЛВС) – набор аппаратных и программных средств, обеспечивающих соединение нескольких отдельных компьютерных рабочих мест (рабочих станций) и других периферийных устройств (принтеров, дисковых контроллеров и т.п.) к единому каналу передачи данных и позволяющих им совместно использовать общую дисковую память, периферийные устройства, обмениваться данными.

Определение сети компьютеров дано в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» гласит (п. 4): «...информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». В определении имеются три квалифицирующих признака – использование компьютеров или иных устройств, ими управляемых, наличие линии связи для передачи информации, присутствие телекоммуникационной аппаратуры, которая в сочетании с линиями связи и образует единую технологическую систему для передачи информации.

Для эффективной работы сетей используются специальные операционные системы (ОС), которые, в отличие от персональных операционных систем, предназначены для решения специальных задач по управлению работой сети компьютеров. Это *сетевые операционные системы*. Одними из наиболее распространенных являются UNIX, OS/2, Novell NetWare и Windows Server.

7.1. Аппаратные средства ЛВС

Все устройства, подключаемые к сети, можно разделить на три функциональные группы:

- рабочие станции;
- серверы сети;
- коммуникационные узлы.

Рабочая станция, или хост (host), – компьютер, подключенный к сети и имеющий в сети собственный адрес. Каждая рабочая станция обрабатывает свои локальные файлы и использует

свою операционную систему. Это может быть как *сервер*, так и *клиентский компьютер*.

Клиент – компьютер в локальной сети, на котором пользователь запускает прикладные программы и с которого обращается к серверу за обеспечением связи с другими компьютерами и доступом к сетевым ресурсам (файлам, программам и устройствам). В отличие от сервера клиент хотя и подключен физически к сети, в отдельные моменты времени может быть логически (программно) отключен от нее. Еще одно отличие – у клиента в разные моменты времени может быть как постоянный, так и разный (меняющийся в каждом сеансе работы в сети) адрес.

Сервер – компьютер, «руководящий обслуживанием» в сети с помощью своих устройств, программ и данных, предоставляющий другим компьютерам (рабочим станциям сети, клиентам) услуги по связи, получению, пересылке и обработке информации, а также совместно используемые ресурсы.

Строго говоря, сервером называется программа, устанавливаемая на компьютер для обслуживания совместной работы в сети других компьютеров. Но поскольку через подобный компьютер «протекает» большое количество информации, его аппаратную часть стараются сделать более мощной. Увеличивают объемы оперативной и дисковой памяти, применяют более быстродействующие процессоры, устанавливают либо несколько обычных сетевых карт, либо сетевые устройства: коммутаторы (свитчи), маршрутизаторы (роутеры). По этой причине сервером называют и компьютер, «руководящий обслуживанием» в сети. Обычно сервер работает круглосуточно для обеспечения бесперебойного доступа к размещенной на нем информации.

Существуют сетевые, файловые, терминальные и серверы баз данных:

С*етевой сервер* поддерживает выполнение следующих функций сетевой операционной системы: управление вычислительной сетью, планирование задач, распределение ресурсов, доступ к сетевой файловой системе, защиту информации.

Файловый сервер (file server – файл-сервер) – компьютер, хранящий данные пользователей сети и обеспечивающий доступ пользователей к этим данным. Так, файл-сервер обеспечивает доступ к центральной базе данных удалённым пользователем. Как

правило, этот компьютер имеет большой объем дискового пространства.

Терминальный сервер поддерживает выполнение функций многопользовательской системы.

Сервер баз данных (data base server) – многопользовательская система, обеспечивающая обработку запросов к базам данных. Он является средством решения сетевых задач, в которых локальные сети используются для совместной обработки данных.

Также *по выполняемым функциям* можно выделить следующие группы серверов:

- *коммуникационный сервер* (communications server) – устройство или компьютер, который предоставляет пользователям локальной сети прозрачный доступ к своим последовательным портам ввода/вывода.

- *сервер прикладных программ* (application server) – компьютер, используемый для выполнения прикладных программ пользователей.

- *сервер доступа* (access server) – позволяет организовать защищенное беспроводное подключение рабочих станций к корпоративным сетям и сетям операторов при полном контроле за параметрами соединения.

- *факс-сервер* (fax server) – устройство или компьютер, который выполняет рассылку и прием факсимильных сообщений для пользователей локальной сети.

- *сервер резервного копирования данных* (back up server) – устройство или компьютер, который решает задачи создания, хранения и восстановления копий данных, расположенных на файловых серверах и рабочих станциях. В качестве такого сервера может использоваться один из файловых серверов сети.

Следует отметить, что все перечисленные типы серверов могут функционировать на одном выделенном для этих целей компьютере.

При построении больших сетей однородная структура связей превращается из преимущества в недостаток. В таких сетях использование типовых структур порождает различные ограничения, важнейшими из которых являются:

• ограничения на длину связи между узлами;

• ограничения на количество узлов в сети;

• ограничения на интенсивность трафика, порождаемого узлами.

Для снятия этих ограничений используются специальные методы структуризации сети и специальное структурообразующее оборудование – ***коммуникационные узлы***:

- повторители (концентраторы);
- мосты;
- коммутаторы;
- маршрутизаторы;
- шлюзы.

Часть сети, в которую не входит устройство расширения, принято называть *сегментом* сети.

Повторитель (repeater) – устройство, усиливающее или регенерирующее пришедший на него сигнал.

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют *концентратором* или *хабом* (hub).

Существуют активные и пассивные концентраторы. Активные концентраторы дополнительно содержат усилитель для подключения от 4 и более рабочих станций. Пассивный концентратор является исключительно разветвительным устройством (максимум на 3 рабочие станции и максимально возможное расстояние до рабочей станции не должно превышать нескольких десятков метров).

Концентратор, приняв пакет из одного сегмента, передает его во все остальные. При этом концентратор не выполняет развязку присоединенных к нему сегментов. В каждый момент времени во всех связанных концентратором сегментах поддерживается обмен данными только между двумя станциями.

Мост (bridge) – программное или аппаратное средство для преобразования информации при обмене ею между однотипными сетями или их частями (логическими сегментами). При этом он передает информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима. Таким образом, мост изолирует трафик одной подсети от трафика другой, повышая общую производительность передачи данных в сети. Именно мост обычно используется для связи сетей между собой, а также для подключения удаленных РС к ЛВС.

Коммутатор, или *свитч* (switch, switching hub), – коммуникационное устройство, в котором возможна параллельная независимая обработка информации, поступающей на разные порты (входы). Это отличает его от моста, где информация, поступающая с разных портов, обрабатывается друг за другом (последовательно).

Однако применение мостов и коммутаторов приводит к значительным ограничениям на конфигурацию связей сети – сегменты должны быть соединены таким образом, чтобы в сети не образовывались замкнутые контуры. Для снятия этого и других ограничений используются маршрутизаторы и шлюзы.

Маршрутизатор (router) – комплекс программных и аппаратных средств, обеспечивающих в сети передачу по назначению (по заданному маршруту) пакетов данных и разделяющий информационные потоки отдельных частей сети друг от друга. Маршрутизатор анализирует адрес назначения и направляет данные по оптимально выбранному маршруту. При этом маршрутизаторы могут работать в сети с замкнутыми контурами. Также очень важной функцией маршрутизатора является возможность связывать в единую сеть подсети, использующие разные сетевые технологии.

Шлюз (gateway) – устройство для соединения разнотипных сетей, работающих с отличающимся сетевым программным обеспечением и по разным протоколам. Впрочем, шлюз, также как и другое коммуникационное оборудование, тоже обеспечивает локализацию трафика.

7.2. Средства коммуникации в компьютерных сетях

В качестве средств коммуникации наиболее часто используются кабельные соединения (витая пара, коаксиальный кабель, оптоволоконные линии); радиоканалы наземной и спутниковой связи.

При выборе учитывают следующие показатели:

- стоимость монтажа и обслуживания;
- скорость передачи информации;
- ограничения на величину расстояния передачи информации (без дополнительных усилителей-повторителей (репитеров));
- безопасность передачи данных.

Главная проблема – в одновременном обеспечении этих показателей.

Витая пара

Наиболее дешевым кабельным соединением является витое двухжильное проводное соединение, часто называемое “витой парой” (***UTP***). Позволяет передавать данные со скоростью до 100 Мбит/с, легко наращивается. Длина кабеля не может превышать 1000 м для обеспечения минимальной скорости передачи в 1 Мбит/с.

Кабель витой пары очень чувствителен к электромагнитным помехам. Для повышения помехозащищенности информации часто используют экранированную витую пару (***STP***).

Кабели неэкранированной витой пары классифицируются по производительности передачи данных по 5 уровням. Категории 1 и 2 позволяют получать невысокое качество передачи и используются исключительно для передачи речевой информации. Категория 3 является минимальным требованием для сетей со скоростью передачи 10 Мбит/с. Категория 4 используется в сетях со скоростями до 16 Мбит/с, а категория 5 – до 100 Мбит/с. Кабели категории 5 наиболее долговечны и надежны.

Кабели экранированной витой пары также классифицируются по стандартам (Type1 – Type9). Основным типом является кабель Type1 стандарта IBM. По своим характеристикам соответствует параметрам кабеля UTP категории 5.

Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара – один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и в компьютерных сетях в качестве физической среды передачи сигнала во многих технологиях, таких как Ethernet, Arcnet и Token ring. В настоящее время, благодаря своей дешевизне и лёгкости в монтаже, является самым распространённым решением для построения проводных (кабельных) локальных сетей.

Рис. 7.1. Витая пара

На рисунке 7.1 представлена витая пара категории 6 (между парами виден разделительный корд, у каждой пары свой шаг скрутки).

Коаксиальный кабель

Обеспечивает скорость до 10 Мбит/сек. На сегодня это далеко не самая распространенная, и не самая удобная технология.

Различают несколько разновидностей коаксиального кабеля.

Ethernet-кабель.

Первые сети Ethernet были построены на протоколе 10base5, использующей в качестве электрической среды передачи данных “толстый” (thick) Ethernet коаксиальный кабель или желтый кабель (yellow cable). Вследствие высокой помехозащищенности является дорогой альтернативой обычным коаксиальным кабелям. Максимально доступное расстояние без повторителей не превышает 500 м, а общее расстояние сети – около 3 км.

Cheapernet-кабель.

Так, использовать “толстый” коаксиальный кабель практически оказалось не слишком удобно, и практически сразу появился более простой и дешевый вариант 10base2, использующий

соединение Cheapernet-кабель или, как его часто называют, “тонкий” (thin) Ethernet коаксиальный кабель.

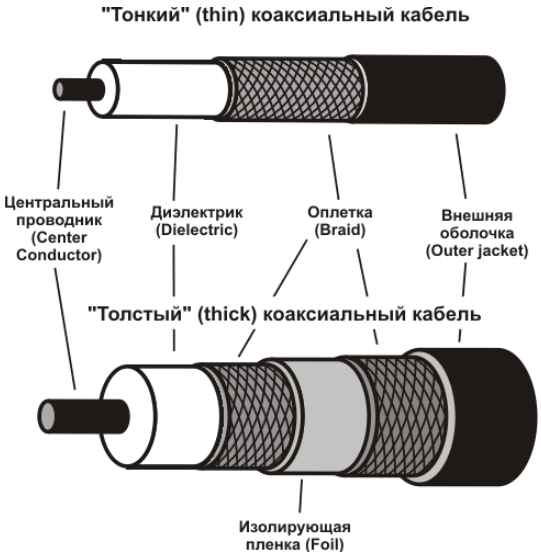


Рис. 7.2. “Тонкий” и “толстый” коаксиальный кабель

При соединении сегментов Cheapernet-кабеля требуются повторители. Вычислительные сети с Cheapernet-кабелем имеют небольшую стоимость и минимальные затраты при наращивании.

Расстояние между двумя рабочими станциями без повторителей максимум 300 м, а общее расстояние – около 1 км.

Оптоволоконные линии

Наиболее дорогим кабельным соединением являются оптопроводники, называемые также стекловолоконным кабелем.

В волоконно-оптическом (fiber-optic cable) кабеле для передачи данных используются световые импульсы. Сердечник такого кабеля изготовлен из стекла или пластика и окружен слоем отражателя, который направляет световые импульсы вдоль кабеля. Такой кабель не подвержен воздействию электромагнитных помех и обеспечивает секретность передаваемой информации (техника

ответвлений в оптоволоконных кабелях очень сложна). Производительность оптоволокна – до 10 Гбит/с.

Рис. 7.3. Некоторые разновидности оптических кабелей

Различают одномодовые и многомодовые кабели. В одномодовом кабеле используется очень тонкий центральный проводник. Луч света почти не отражается от внешнего отражателя. В многомодовом кабеле более толстый центральный проводник, в котором одновременно существует несколько световых лучей с разными углами преломления – модами. Допустимое удаление более 50 км.

Передача данных выполняется только в *симплексном* режиме, поэтому для организации обмена данными устройства необходимо соединять двумя оптическими волокнами (на практике оптоволоконный кабель всегда имеет четное, парное количество волокон).

Применяются там, где возникают электромагнитные поля помех или требуется передача информации на очень большие расстояния без использования повторителей. Оптопроводники объединяются в ЛВС с помощью звездообразного соединения.

Радиоканалы наземной и спутниковой связи

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ), по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких и сверхвысоких волн (УКВ и СВЧ). В диапазоне СВЧ (свыше 4 ГГц) сигналы уже не отражаются ионосферой Земли и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы.

Радиорелейные каналы связи состоят из последовательности станций, являющихся ретрансляторами. Связь осуществляется в пределах прямой видимости, дальности между соседними станциями – до 50 км. Цифровые радиорелейные линии связи применяются в качестве региональных и местных систем связи и передачи данных, а также для связи между базовыми станциями сотовой связи.

В ***спутниковых сетях*** используются три основных типа спутников, которые находятся на геостационарных, средних или

низких орбитах. Спутники запускаются, как правило, группами. Разнесенные друг от друга они могут обеспечить охват почти всей поверхности Земли. Работа спутникового канала передачи данных представлена на рисунке 7.4.

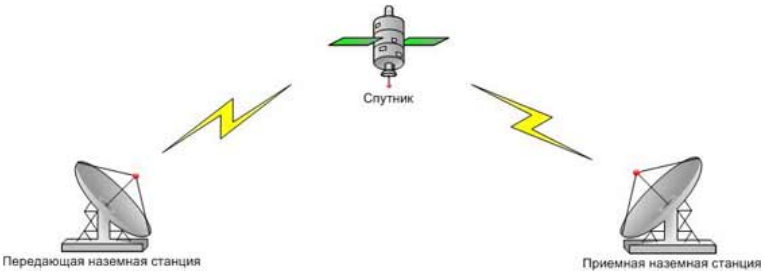


Рис. 7.4. Работа спутникового канала передачи данных

Целесообразнее использовать спутниковую связь для организации канала связи между станциями, расположенными на очень больших расстояниях, и возможности обслуживания абонентов в самых труднодоступных точках. Пропускная способность высокая – несколько десятков Мбит/с.

Беспроводные ЛС считаются перспективным направлением развития ЛВС. Их преимущество – простота и мобильность. Исчезают проблемы, связанные с прокладкой и монтажом кабельных соединений.

7.3. Принципы передачи данных в сетях

Кодирование информации

Для передачи информации по коммуникационным линиям данные преобразуются в цепочку следующих друг за другом битов (двоичное кодирование с помощью только лишь двух крайних состояний:"0" и "1").

Передаваемые алфавитно-цифровые знаки представляются с помощью битовых комбинаций. Битовые комбинации располагают в определенной кодовой таблице, содержащей 4-, 5-, 6-, 7- или 8-битовые коды.

Количество представленных знаков зависит от количества битов, используемых в коде: код из четырех битов может представить максимум 16 значений, 5-битовый код - 32 значения, 6-битовый код – 64 значения, 7-битовый – 128 значений и 8-битовый код – 256 алфавитно-цифровых знаков.

На международном уровне передача символьной информации осуществляется с помощью 7-битового кодирования, позволяющего закодировать заглавные и строчные буквы английского алфавита, а также некоторые спец-символы. Национальные и специальные знаки с помощью 7-битового кода представить нельзя. Для представления национальных знаков применяют 8-битовый код.

Методы передачи информации

Передача данных (обмен данными, цифровая передача, цифровая связь) – физический перенос данных(цифрового битового потока) в виде сигналов от точки к точке или от точки к нескольким точкам средствами электросвязи по каналу передачи данных, как правило, для последующей обработки средствами вычислительной техники.

1. При обмене данными между узлами обычно используются *три метода передачи данных*:

• ***симплексная*** (однонаправленная) передача (например, радио, телевидение);

• ***полудуплексная*** – прием/передача информации осуществляется поочередно;

• ***дуплексная*** (двунаправленная) – каждая станция одновременно передает и принимает данные.

2. Мультиплексирование.

Как в локальных, так и в крупномасштабных сетях имеются случаи, когда пропускная способность передающей среды превышает требуемую для передачи единичного сигнала. Экономичное использование высокоскоростного магистрального канала связи для одновременной передачи нескольких сигналов известно как *мультиплексирование*.

Использование ***мультиплексирования с разделением частот*** (*Frequency Division Multiplexing* – ***FDM***) основывается на том, что общая полоса полезных частот одного высокоскоростного канала связи разделяется на несколько непересекающихся подполос,

называемых каналами. В рамках каждого из каналов осуществляется взаимонезависимая передача только одного сигнала со своей несущей, а общее число одновременно передаваемых сигналов определяется количеством каналов.

Технология FDM, применяемая в оптоволоконных линиях, получила название *разделения по длине волны* (*Wave Time Division Multiplexing* – ***WDM***).

Мультиплексирование с временным разделением (*Time Division Multiplexing* – ***TDM***) основывается на том, что скорость передачи двоичных данных по магистральному каналу значительно превосходит требуемую скорость для передачи единичного дискретного сигнала. В этом случае порции нескольких дискретных сигналов могут поочередно передаваться по общей среде, тем самым совместно используя ее. Последовательность временных интервалов использования общей передающей среды определенным сигналом, по аналогии с FDM, называется каналом.

Технология TDM имеет и другое название – *техника синхронного режима передачи* (*Synchronous Transfer Mode* – ***STM***).

Следует отметить, что существуют случаи совместного применения FDM и TDM. Общая полоса частот передающей среды может быть разбита на несколько отдельных частотных каналов, каждый из которых далее подразделяется на подканалы с помощью временного разделения.

3. Синхронная и асинхронная передача данных.

Для передачи данных в информационных системах наиболее часто применяется последовательная передача. Широко используются следующие методы последовательной передачи: ***асинхронная*** и ***синхронная***, которые позволяют получателю знать момент начала и временной период передачи каждого получаемого бита.

В ***асинхронной*** схеме данные передаются по одному символу за раз. Каждому передаваемому символу предшествует передача стартового кода (предупреждает приемник о начале передачи), затем передается символ. Для определения достоверности передачи используется бит четности (бит четности = 1, если количество единиц в символе нечетно, и 0, в противном случае. Последний бит "стоп бит" сигнализирует об окончании передачи.

Преимущества: несложная отработанная система; недорогое (по сравнению с синхронным) интерфейсное оборудование.

Недостатки: третья часть пропускной способности теряется на передачу служебных битов (старт/стоповых и бита четности); невысокая скорость передачи по сравнению с синхронной; при множественной ошибке с помощью бита четности невозможно определить достоверность полученной информации.

Асинхронная передача используется в системах, где обмен данными происходит время от времени и не требуется высокая скорость передачи.

При использовании ***синхронного*** метода данные передаются блоками. Для синхронизации работы приемника и передатчика в начале блока передаются биты синхронизации. Затем передаются данные, код обнаружения ошибки и символ окончания передачи. При синхронной передаче данные могут передаваться и как символы, и как поток битов. В качестве кода обнаружения ошибки обычно используется *Циклический Избыточный Код Обнаружения Ошибок* (*CRC*). Он вычисляется по содержимому поля данных и позволяет однозначно определить достоверность принятой информации.

Преимущества: высокая эффективность передачи данных; высокие скорости передачи; надежный встроенный механизм обнаружения ошибок.

Недостатки: интерфейсное оборудование более сложное и, соответственно, более дорогое.

7.4. Организация взаимодействия устройств в сети

В зависимости от способа организации обработки данных и взаимодействия пользователей, который поддерживается конкретной сетевой операционной системой, выделяют два типа информационных систем:

- иерархические сети;
- сети клиент/сервер.

В ***иерархических сетях*** все задачи, связанные с хранением, обработкой данных, их представлением пользователям, выполняет центральный компьютер. Пользователь взаимодействует с центральным компьютером с помощью терминала. Операциями ввода/вывода информации на экран управляет центральный компьютер.

Достоинства иерархических систем:

• отработанная технология обеспечения отказоустойчивости, сохранности данных;

• надежная система защиты информации и обеспечения секретности.

Недостатки:

• высокая стоимость аппаратного и программного обеспечения, высокие эксплуатационные расходы;

• быстродействие и надежность сети зависят от центрального компьютера.

Примеры иерархических систем: SNA, IBM Corp., DNA, DEC.

В системах ***клиент/сервер*** обработка данных разделена между двумя объектами: клиентом и сервером.

Так, к***лиент*** – это задача, рабочая станция, пользователь. Он может сформировать запрос для сервера: считать файл, осуществить поиск записи и т.п. В системах клиент/сервер требования к производительности компьютеров значительно ниже, чем в иерархических системах.

Напомним, что с***ервер*** – устройство или компьютер, выполняющий обработку запроса. Отвечает за хранение данных, организацию доступа к этим данным и передачу данных клиенту.

Выделяются четыре подхода, реализованные в моделях системы ***клиент/сервер***:

• модель файлового сервера (File Server – FS);

• модель доступа к удаленным данным (Remote Data Access – RDA);

• модель сервера базы данных (DataBase Server – DBS);

• модель сервера приложений (Application Server – AS).

В зависимости от метода взаимодействия устройств в сети различают два типа систем, использующих метод клиент/сервер: равноправную сеть и сеть с выделенным сервером.

Равноправная сеть (одноранговая) – это сеть, в которой нет единого центра управления взаимодействием рабочих станций, нет единого устройства хранения данных. Операционная система такой сети распределена по всем рабочим станциям, поэтому каждая рабочая станция одновременно может выполнять функции как сервера, так и клиента. Пользователю в такой сети доступны все устройства (принтеры, жесткие диски и т.п.), подключенные к другим рабочим станциям.

Достоинства: низкая стоимость (используются все компьютеры, подключенные к сети, и умеренные цены на программное обеспечение для работы сети); высокая надежность (при выходе из строя рабочей станции, доступ прекращается лишь к части информации).

Недостатки: работа сети эффективна только при количестве одновременно работающих станций не более 10; трудности организации эффективного управления взаимодействием рабочих станций и обеспечение секретности информации; трудности обновления и изменения ПО рабочих станций.

Сеть с выделенным сервером – здесь один из компьютеров выполняет функции хранения данных общего пользования, организации взаимодействия между рабочими станциями, выполнения сервисных услуг – сервер сети.

Достоинства: выше скорость обработки данных; обладает надежной системой защиты информации и обеспечения секретности; проще в управлении по сравнению с равноправными.

Недостатки: такая сеть дороже из-за отдельного компьютера под сервер; менее гибкая по сравнению с равноправной.

Сети с выделенным сервером являются более распространенными. Примеры сетевых операционных систем такого типа: LAN Server, IBM Corp., VINES, Banyan System Inc., NetWare, Novell Inc.

7.5. Требования к современным ЛВС

Вычислительная сеть создается для обеспечения потенциального доступа к любому ресурсу сети для каждого пользователя сети. Качество доступа к ресурсу, как глобальная характеристика функционирования сети, может быть описана многими показателями, выбор которых зависит от задач, стоящих перед вычислительной сетью. Среди основных показателей можно выделить следующие:

- ***Производительность***. Важным показателем производительности сети является время реакции системы – это время между моментом возникновения запроса и моментом получения ответа. Время реакции зависит от многих факторов, таких как используемая служба сети, степень загруженности сети или отдельных сегментов и др. Поэтому при оценке производительности

работы сети определяется среднее время реакции. *Пропускная способность* сети определяется количеством информации, переданной через сеть или ее сегмент в единицу времени. Пропускная способность сети характеризует, насколько быстро сеть может выполнить свою основную задачу передачи информации. Пропускная способность определяется в битах в секунду.

- ***Надежность и безопасность.*** *Надежность* работы вычислительной сети определяется надежностью работы всех ее компонентов. Для повышения надежности работы аппаратных компонентов обычно используют дублирование, когда при отказе одного из элементов функционирование сети обеспечат другие. Важное значение имеет другая сторона надежности – *безопасность*. Это способность сети обеспечить защиту информации от несанкционированного доступа.

- ***Управляемость***. Система управления сетью должна предоставлять возможность воздействовать на работу любого элемента сети. Должна быть обеспечена возможность осуществлять мероприятия по управлению с любого элемента сети. Управлением сетью занимается администратор сети или пользователь, которому поручены эти функции.

- ***Расширяемость и масштабируемость***. Любая вычислительная сеть является развивающимся объектом, и не только в плане модернизации ее элементов, но и в плане ее физического расширения, добавления новых элементов сети (пользователей, компьютеров, служб). Существование таких возможностей, трудоемкость их осуществления входят в понятие *расширяемости*. Другой похожей характеристикой является *масштабируемость* сети, которая определяет возможность расширения сети без существенного снижения ее производительности.

- ***Прозрачность.*** *Прозрачность* вычислительной сети является ее характеристикой с точки зрения пользователя. Прозрачность сети предполагает скрытие особенностей сети от конечного пользователя. Пользователь обращается к ресурсам сети как к обычным локальным ресурсам компьютера, на котором он работает. Другой важной стороной прозрачности сети является возможность распараллеливания работы между разными элементами сети. Вопросы назначения отдельных параллельных заданий

отдельным устройствам сети также должны быть скрытыми от пользователя и решаться в автоматическом режиме.

- ***Интегрируемость (совместимость)***. *Интегрируемость* означает возможность подключения к вычислительной сети разнообразного и разнотипного оборудования, программного обеспечения от разных производителей.

Основным направлением развития интегрируемости вычислительных сетей является стандартизация сетей, их элементов и компонентов.

Работы по стандартизации вычислительных сетей ведутся большим количеством организаций. Среди них необходимо выделить Международную организацию по стандартизации (International Organization for Standardization – ISO). Эта организация известна разработкой модели взаимодействия открытых систем Open Systems Interconnection (OSI), которая в настоящее время является основной, своего рода «эталонной» моделью вычислительной сети. Эта модель является основой стандартизации в области вычислительных сетей.

На основе модели OSI вычислительная сеть предстает как распределенная вычислительная среда, включающая в себя большое число разнообразных аппаратных и программных средств. Данная среда представляется рядом логических уровней, на каждый из которых возложена одна из задач сети.

Модель OSI представляет собой *семиуровневую модель*, которой соответствует и программная структура:

1. *Физический* (Physical Layer) – осуществляет как соединения с физическим каналом, так и расторжение, управление каналом; также на этом уровне определяется скорость передачи данных и топология сети.

2. *Канальный* (Data Link) – осуществляет обрамление передаваемых массивов информации вспомогательными символами и контроль передаваемых данных.

3. *Сетевой* (Network Layer) – определяет маршрут передачи информации между сетями (ПЭВМ), обеспечивает обработку ошибок, а так же управление потоками данных.

4. *Транспортный* (Transport Layer) – связывает нижние уровни (физический, канальный, сетевой) с верхними уровнями, которые реализуются программными средствами. Здесь осуществляется разделение информации по определенной длине и уточняется адрес

назначения. Транспортный уровень позволяет мультиплексировать передаваемые сообщения или соединения.

5. *Сеансовый* (Session Layer) – на данном уровне осуществляется управление сеансами связи между взаимодействующими пользователями.

6. *Представительский* (Presentation Layer) – управляет представлением данных в необходимой для программы пользователя форме, генерацию и интерпретацию взаимодействия процессов, кодирование/декодирование данных, компрессию и декомпрессию данных. Разрешает организовать обмен данными между станциями с разными операционными системами.

7. *Прикладной* (Application Layer) – в его ведении находятся прикладные сетевые программы, обслуживающие файлы, а также выполняет вычислительные, информационно-поисковые работы, логические преобразования информации, передачу почтовых сообщений и т.п. Главная задача этого уровня – обеспечить удобный интерфейс для пользователя. С этим может справиться системное и пользовательское прикладное программное обеспечение.

Модель OSI представляет хотя и очень важную, но только одну из многих моделей коммуникаций. Эти модели и связанные с ними стеки протоколов могут отличаться количеством уровней, их функциями, форматами сообщений, службами, поддерживаемыми на верхних уровнях, и прочими параметрами.

7.6. Классификация вычислительных сетей

Классификация по территориальному признаку

В настоящее время информационно-вычислительные системы принято делить на 3 основных типа:

- ***LAN*** (Lokal Area Network) – локальная сеть в пределах предприятия, учреждения, одной организации. Размер локальной сети не превышает нескольких километров. Пропускная способность современных локальных сетей достигает нескольких Гбит/с. Время обращения к сетевым ресурсам соизмеримо со временем обращения к локальным ресурсам рабочей станции. Локальные сети обладают плохой масштабируемостью, так как используемые технологии накладывают жесткие ограничения на длину линий связи и количество компьютеров.

- ***MAN*** (Metropolitan Area Network) – городская или региональная сеть, т.е. сеть в пределах города, области и т.п.. Обычно они используют цифровые магистральные линии связи, часто оптоволоконные, со скоростями от 45 Мбит/с, и предназначены для связи локальных сетей в масштабах города и соединения локальных сетей с глобальными.

- ***WAN*** (Wide Area Network) – глобальная сеть, соединяющая абонентов страны, континента, всего мира. Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, то, обычно, при организации WAN-сетей используются уже существующие линии связи, например, телефонные линии. Скорость обмена данными существенно ниже, чем в LAN-сетях. Глобальные сети обладают хорошей масштабируемостью. Подключение дополнительных компьютеров почти не влияет на общие показатели всей сети.

Сейчас наблюдается взаимное проникновение технологий LAN и WAN. Процесс переноса технологий глобальных сетей в локальные сети получил в последнее время широкое развитие. Появилось понятие *intranet-технология*, которое обозначает применение служб глобальных сетей для реализации целей локальных сетей. Масштабы локальных сетей перестали определяться лишь территориальными признаками.

Классификация по масштабу сети

Еще одним популярным способом классификации сетей является их классификация по масштабу производственного подразделения, в пределах которого действует сеть. Различают *сети отделов*, *сети кампусов* и *корпоративные сети*.

Сети отделов – это сети, которые используются сравнительно небольшой группой сотрудников, работающих в одном отделе предприятия.

Главной целью сети отдела является разделение локальных ресурсов, таких как приложения, данные, принтеры и т.п. Обычно сети отделов имеют один или два файловых сервера и не более 30 пользователей. Сети отделов обычно не разделяются на подсети. В этих сетях локализуется большая часть трафика предприятия.

Существует и другой тип сетей, близкий к сетям отделов, – *сети рабочих групп*. К таким сетям относятся совсем небольшие

сети (до 10 – 20 компьютеров). Характеристики сетей рабочих групп практически не отличаются от описанных выше характеристик сетей отделов.

Сети кампусов – это название используют сейчас для обозначения сетей любых предприятий и организаций.

Сети этого типа объединяют множество сетей различных отделов одного предприятия в пределах отдельного здания или в пределах одной территории, покрывающей площадь в несколько квадратных километров. При этом глобальные соединения в сетях кампусов не используются. Службы такой сети включают взаимодействие между сетями отделов, доступ к общим базам данных предприятия, доступ к общим факс-модемам и т.п. Главной целью сети кампусов является оперативный обмен информацией между отделами.

Однако именно на уровне сети кампуса возникают проблемы интеграции неоднородного аппаратного и программного обеспечения, которое может отличаться в каждом отделе.

Информационные системы, в которых средства передачи данных принадлежат одной компании и используются только для нужд этой компании принято называть *Сеть Масштаба Предприятия* или ***Корпоративная сеть*** (*Enterprise Network*). Они могут покрывать город, регион или даже континент. Число пользователей и компьютеров может измеряться тысячами, а число серверов – сотнями, расстояния между сетями отдельных территорий могут оказаться такими, что становится необходимым использование глобальных связей.

Классификация по способу передачи информации

В компьютерных сетях для передачи данных между узлами сети можно использовать три технологии: *коммутацию каналов*, *коммутацию сообщений* и *коммутацию пакетов*.

Метод ***коммутации каналов*** используется в сетях в том случае, если между двумя станциями необходимо установить непосредственное физическое канальное соединение. Это соединение устанавливается в коммуникационных узлах сети до начала передачи данных. Типичным примером использования коммутации каналов является обычная телефонная сеть.

Предварительное резервирование сетевых каналов на всем пути от передатчика к приемнику при коммутации каналов предусматривает, что узлы должны обладать способностью распределять ресурсы и выбирать маршруты при установке соединений.

Предварительное резервирование всего пути имеет существенные недостатки, к основным из которых относятся:

- неэффективность использования ресурсов (каналы резервируются даже на то время, когда данные не передаются);
- высокая вероятность получения отказа при резервировании пути, включающего много транзитных узлов;
- значительная задержка при установлении соединения и склонность сети к перегрузке;
- лавинообразный рост отказов установления соединений в случае перегрузки сети.

Однако данный способ имеет и некоторые преимущества. Так, после установления соединения в сети с коммутацией каналов передача данных идет очень эффективно и практически без задержек.

Метод ***коммутации сообщений*** представляет собой реализацию принципа поэтапной передачи данных с промежуточным хранением. Здесь нет необходимости заранее резервировать весь путь между двумя станциями.

При коммутации сообщений устройства, называемые коммутаторами и выполненные на базе универсальных или специализированных компьютеров, позволяют накапливать (буферизировать) сообщения и посылать их в соответствии с заданной системой приоритетности и принципами маршрутизации другим узлам сети. Для маршрутизации каждое сообщение снабжается заголовком с сетевыми адресами станции-передатчика и станции-приемника.

Использование коммутации сообщений может увеличить время доставки сообщений по сравнению с коммутацией каналов, однако при этом сглаживаются пиковые нагрузки в сети и повышается живучесть сети.

Коммутация сообщений увеличивает эффективность использования линий связи; позволяет избежать блокировок сети при увеличении сетевого трафика; обеспечивает возможности установления приоритетного обслуживания сообщений, и т.д. В то

же время задержки передачи, которые связаны, в первую очередь, с ожиданием длинных сообщений в очередях узлов, значительно возрастают при увеличении нагрузки, что не подходит для интерактивного сетевого взаимодействия в режиме реального времени.

Пакетная коммутация подразумевает обмен небольшими пакетами, которые не дают возможности образования очередей в узлах коммутации. Достоинства: быстрое соединение, надежность, эффективность использования сети. При данном методе проблема передачи пакета решается способом фиксированной маршрутизации.

Метод пакетной коммутации в настоящее время используется в двух модификациях: в режиме ***дейтаграмм*** и в режиме ***виртуальных каналов***.

Режим дейтаграмм является прямым развитием коммутации сообщений, где сообщения предварительно разбиваются на пакеты. Каждый пакет при передаче по коммуникационной сети является полностью независимой единицей. Для этого он снабжается своим заголовком, где указываются сетевые адреса отправителя и получателя сообщения, а также порядковый номер отдельного пакета во всем сообщении.

В некоторых дейтаграммных сетях может отсутствовать функция упорядочения пакетов на выходном узле – тогда эту функцию берет на себя станция назначения. Пакет может повредиться при передаче по сети. Например, если один из узлов в сети вышел из строя, то все пакеты, находящиеся на этом узле в очереди на передачу, будут потеряны. Опять же, функцию обнаружения потерянных пакетов может брать на себя как конечный узел маршрута, так и станция-получатель. В такой сети каждый пакет передается независимо от остальных и называется дейтаграммой.

Уменьшение размера передающихся порций информации и возможность одновременной передачи нескольких пакетов одного сообщения по альтернативным путям при данном подходе существенно уменьшают сетевые задержки при передаче данных. Кроме того, коммутационные узлы могут иметь не столь большие, как при коммутации сообщений, размеры буферов для временного размещения транзитных пакетов, поэтому скорость обработки информации в этих узлах может быть повышена. На уменьшение

задержек влияет и то, что при обнаружении ошибок передачи в режиме коммутации пакетов повторно передаются лишь отдельные пакеты, а не целые сообщения.

Пакетная коммутация, однако, имеет и негативные стороны. С одной стороны, при ее использовании увеличивается объем дополнительной, служебной информации, передающейся по сети (заголовки отдельных пакетов). С другой стороны, в режиме дейтаграмм существует проблема организации сборки переданного сообщения в узле назначения. Эта проблема связана с тем, что отдельные пакеты, проходя различными маршрутами по подсети связи, будут приходить в конечный узел назначения в неупорядоченной последовательности.

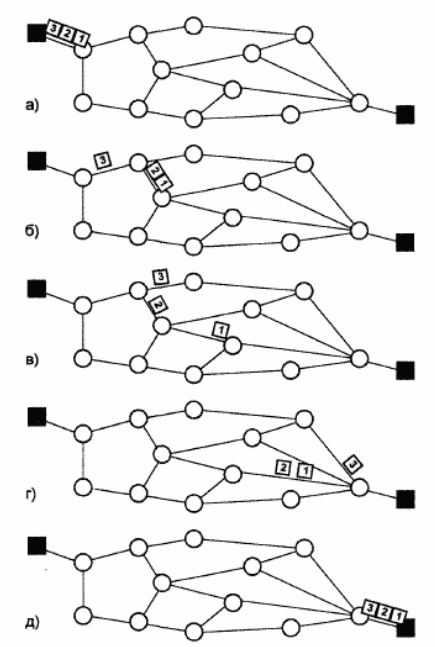


Рис. 7.5. Пакетная коммутация – дейтаграммная сеть

Режим виртуальных каналов является попыткой соединить воедино преимущества метода коммутации каналов и метода коммутации сообщений. При этом подходе, еще до посылки по сети первого информационного пакета, между двумя конечными точками

организуется *логическое соединение*, связанное с реализацией трех фаз, присущих методу коммутации каналов. Вызывающая станция сначала посылает по сети служебный пакет запроса на установление виртуального канала, связывающего станцию-инициатор с вызываемой станцией. Подсеть связи маршрутизирует этот пакет как обычную дейтаграмму, содержащую в заголовке сетевые адреса двух конечных станций. Передвигаясь по сети, пакет закрепляет за пройденным маршрутом номер устанавливаемого виртуального канала. Номер логического канала, запоминаемый в транзитных узлах, закрепляется за двунаправленным маршрутом для каждого конкретного вызова обмена данными.

После установления логического соединения, т.е. после получения вызывающей станцией пакета-ответа на запрос, по установленному виртуальному каналу начинается пересылка информационных пакетов сообщения. Последовательная передача пакетов по установленному логическому каналу полностью обеспечивает их получение в правильной последовательности. Поэтому заголовок каждого информационного пакета уже не нуждается в порядковом номере, а также и в указании сетевых адресов обеих станций-абонентов (достаточно лишь указания номера логического канала). Следовательно, при коммутации виртуальных каналов не только уменьшается объем передачи дополнительной служебной информации, но и обеспечивается интерактивный режим взаимодействия двух станций-абонентов.

Заметим, что весь путь целиком между двумя станциями-абонентами здесь не резервируется. Пакеты передаются от узла к узлу с промежуточным хранением и ожидают в общих очередях к каналам, связывающим эти транзитные узлы. Однако маршрутизация осуществляется только один раз при установлении соединения.

Конечно, если отдельной станции необходимо передать по сети всего несколько пакетов, то режим дейтаграмм будет более быстрым и предпочтительным. Однако, если между станциями необходим обмен данными на протяжении значительного периода времени, предпочтение следует отдать виртуальным соединениям. Поэтому в вычислительных сетях на практике применяются сочетания различных методов коммутации в зависимости от требований приложений, количественных и качественных характеристик узлов, линий связи и трафика.

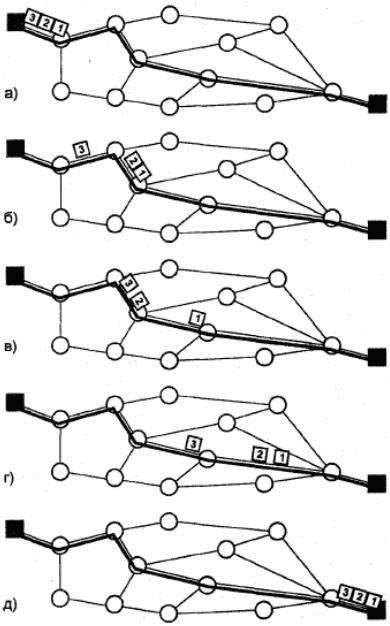


Рис. 7.6. Пакетная коммутация – сеть с виртуальными каналами

Преимущества сети с виртуальными каналами:

1. Сеть может поддерживать ряд служб, связанных с виртуальными каналами, включая порядок следования, контроль ошибок и контроль потока. Правильный порядок следования легко поддерживается, поскольку все пакеты двигаются одним и тем же маршрутом и прибывают в первоначально установленной последовательности. Служба контроля ошибок гарантирует не только то, что пакеты прибывают в нужной последовательности, но и то, что все пакеты на приемной стороне корректны. Например, если один из пакетов в последовательности, двигаясь от узла 4 к узлу 6 (рис. 5.14) потерялся или пришел на узел 6 с ошибкой, то узел 6 может послать запрос на узел 4 с просьбой повторить «соответствующий пакет последовательности. Служба контроля потока гарантирует, что отправитель не может «завалить» получателя данными. Например, если станция Е буферизует данные от станции А и видит, что приемный буфер близок к переполнению, то она может просигнализировать через обратный виртуальный

канал о необходимости уменьшить или временно прекратить передачу данных от станции А.

2. Преимущество этой сети состоит в том, что пакеты передаются через узел быстрее, когда узел не принимает решения о маршрутизации пакета.

Сети, одновременно осуществляющие коммутацию каналов, сообщений и пакетов, называются *интегрированными*. К таким сетям относится сетевая технология ***ATM*** (Asynchronous Transfer Mode – асинхронный способ передачи данных).

7.7. Топологии вычислительной сети

Существует ряд принципов построения ЛВС на основе разных типов и модификаций соединений. Такие принципы еще называют топологиями. Топология определяется физическими связями между компьютерами, которые могут отличаться от логических связей, представляющих собой маршруты передачи данных между узлами сети.

Полносвязная топология

В сети, построенной по данному принципу, каждый компьютер сети связан со всеми остальными. При этом для каждой пары компьютеров сети должна быть выделена отдельная линия связи. Очень неэффективная и дорогая топология, поэтому чаще всего она используется в глобальных сетях при небольшом количестве компьютеров.

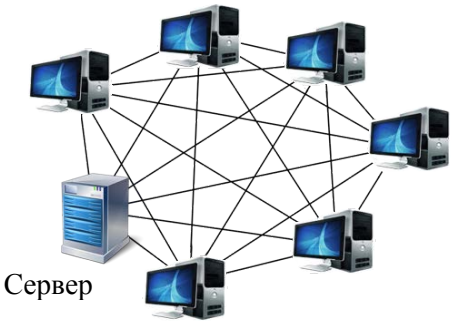


Рис. 7.7. Полносвязная топология

Ячеистая топология

Получается из полносвязной путем удаления некоторых возможных связей. В подобной топологии непосредственно связываются только те компьютеры, между которыми происходит интенсивный обмен данными, а остальные используют транзитную передачу через промежуточные узлы.

Топология типа звезда

Здесь вся информация между двумя периферийными рабочими местами проходит через центральный узел вычислительной сети.

Пропускная способность сети определяется вычислительной мощностью узла и гарантируется для каждой рабочей станции. Коллизий (столкновений) данных не возникает.

Кабельное соединение довольно простое, т.к. каждая рабочая станция связана с узлом. Однако затраты на прокладку кабелей высокие, особенно когда центральный узел географически расположен не в центре топологии. При расширении вычислительных сетей не могут быть использованы ранее выполненные кабельные связи: к новому рабочему месту необходимо прокладывать отдельный кабель из центра сети.

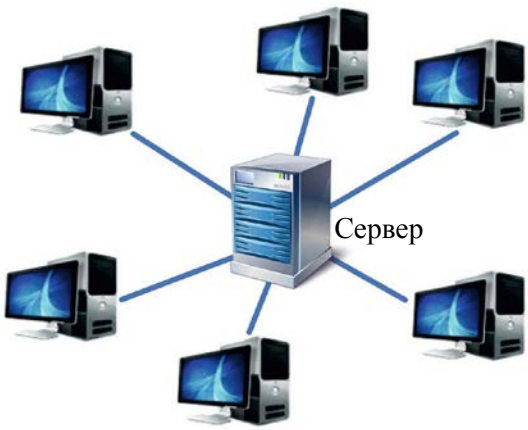


Рис. 7.8. Топология типа звезда

Топология в виде звезды является наиболее быстродействующей из всех топологий вычислительных сетей, поскольку передача данных между рабочими станциями проходит через центральный узел по отдельным линиям, используемым только этими рабочими станциями. Частота запросов передачи информации от одной станции к другой невысокая, по сравнению с достигаемой в других топологиях.

Главное преимущество топологии «звезда» – большая надежность, т.к. дефект кабеля касается только того компьютер, к которому он подсоединен, и только неисправность концентратора может вывести из строя всю сеть. К преимуществам также относится возможность реализации оптимального механизма защиты против несанкционированного доступа к информации, т.к. вся вычислительная сеть может управляться из ее центра.

К недостаткам топологии типа «звезда» относится более высокая стоимость сетевого оборудования. Также, недостатком является то, что возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора.

Кольцевая топология

При кольцевой топологии сети рабочие станции связаны одна с другой по кругу, т.е. рабочая станция 1 с рабочей станцией 2, рабочая станция 3 с рабочей станцией 4 и т.д. Последняя рабочая станция связана с первой. Коммуникационная связь замыкается в кольцо.

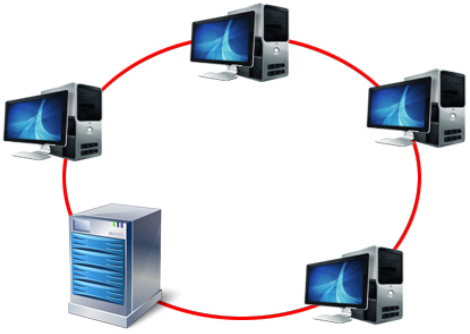


Рис. 7.9. Кольцевая топология

Прокладка кабелей от одной рабочей станции до другой может быть довольно сложной и дорогостоящей, особенно если географически станции расположены далеко от кольца (например, в линию).

Сообщения циркулируют регулярно по кругу (обычно только в одном направлении). Пересылка сообщений является очень эффективной, т.к. большинство сообщений можно отправлять по кабельной системе одно за другим. Очень просто можно реализовать кольцевой запрос на все станции. Продолжительность передачи информации увеличивается пропорционально количеству рабочих станций, входящих в вычислительную сеть.

Основная проблема при кольцевой топологии заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них вся сеть парализуется. Однако неисправности в таких соединениях локализуются легко.

Подключение новой рабочей станции требует краткосрочного выключения сети, т.к. во время установки кольцо должно быть разомкнуто. Ограничения на протяженность вычислительной сети не существует, т.к. оно, в конечном счете, определяется исключительно расстоянием между двумя рабочими станциями.

Логическая кольцевая топология

Специальной формой кольцевой топологии является логическая кольцевая сеть (рис. 7.10).

Физически она монтируется как соединение звездных топологий. Отдельные звезды включаются с помощью специальных коммутаторов. Разрыв соединения происходит только для нижерасположенного (ближайшего) узла сети, так что лишь в редких случаях может нарушаться работа всей сети.

Шинная топология

При шинной топологии (рис. 7.11) среда передачи информации представляется в форме коммуникационного пути, доступного для всех рабочих станций и к которому они все должны быть подключены. Все рабочие станции могут непосредственно

вступать в контакт с любой другой рабочей станцией, имеющейся в сети.

Рис. 7.10. Логическая кольцевая топология

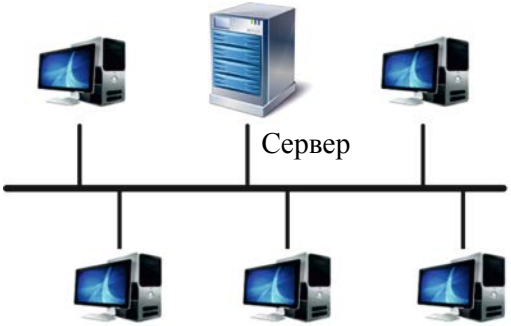


Рис. 7.11. Шинная топология

Основным преимуществом такой схемы являются дешевизна и простота разводки кабеля по помещениям. Также обеспечивается возможность почти мгновенного широковещательного обращения ко всем станциям сети. Самые серьезные недостатки – низкая надежность (любой дефект кабеля или разъема полностью парализует всю сеть) и невысокая производительность, т.к. при

таком подключении в каждый момент времени только один компьютер может передавать данные в сеть.

Благодаря тому, что рабочие станции можно включать без прерывания сетевых процессов и коммуникационной среды, очень легко прослушивать информацию, т.е. ответвлять информацию из коммуникационной среды.

Древовидная структура ЛВС

Для крупных сетей характерно наличие произвольных связей между компьютерами. В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют сетями со *смешенной топологией*. Примером может служить древовидная структура. Она образуется в основном путем комбинаций вышеназванных топологий вычислительных сетей. Основание дерева вычислительной сети располагается в точке (корень), в которой собираются коммуникационные линии информации (ветви дерева).

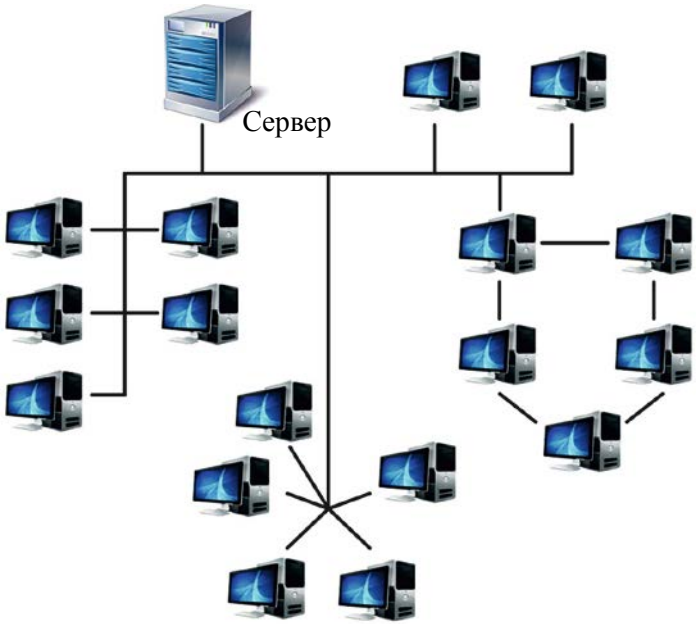


Рис. 7.12. Древовидная структура ЛВС

Вычислительные сети с древовидной структурой применяются там, где невозможно применение базовых сетевых структур в чистом виде.

7.8. Типы построения сетей по методам передачи информации

В проектировании локальных сетей основная роль отводится протоколам физического и канального уровней модели OSI. Канальный уровень подразделяют на два подуровня: логической передачи данных LLC (Logical Link Control) и управления доступом к сети MAC (Media Access Control). В современных вычислительных сетях имеют распространение несколько протоколов уровня MAC: ARCnet, Token Ring, Ethernet, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, FDDI.

Локальная сеть Arcnet

Эта сетевая технология разработана фирмой Datapoint Corp. в середине 80-х годов. Она получила широкое распространение, в основном благодаря тому, что оборудование Arcnet дешевле, чем оборудование Ethernet или Token Ring.

В качестве доступа к передающей среде используется одна из разновидностей детерминированного метода – маркерный метод, а именно *маркерная шина* (Token Bus). Один из компьютеров создает специальный маркер (сообщение специального вида), который последовательно передается от одного компьютера к другому. Если станция желает передать сообщение другой станции, она должна дождаться маркера и добавить к нему сообщение, дополненное адресами отправителя и назначения. Когда пакет дойдет до станции назначения, сообщение будет “отцеплено” от маркера и передано станции, а маркер продолжит движение.

Локальная сеть Token Ring

Технология *Token Ring* была разработана в 1984 году фирмой IBM.

В общем случае сеть Token Ring имеет комбинированную звездно-кольцевую конфигурацию. Конечные узлы подключаются к концентратору (MSAU) по топологии звезда, а сами концентраторы

объединяются по кольцу. Все станции работают на одной скорости – либо 4 Мбит/с, либо 16 Мбит/с.

Для доступа к среде передачи данных, как и в технологии Arcnet, также применяется разновидность маркерного метода – *маркерное кольцо* (Token Ring). При использовании этого метода маркер передается от узла к узлу путем ретрансляции. Если нет необходимости в передаче, то узел передает маркер следующему узлу. Если такая необходимость есть, то маркер изымается из сети и узел посылает свой кадр данных по кольцу. Получив обратно посланный кадр с подтверждением получения, узел-отправитель отправляет в сеть новую копию маркера для передачи доступа к сети. Время доступа к сети ограничивается временем удержания маркера, в течение которого узел может послать несколько кадров данных и после чего узел обязан передать маркер в сеть. Этот алгоритм маркерного доступа используется в сетях Token Ring, которые работают на скорости 4 Мбит/с. В сетях Token Ring, которые работают на скорости 16 Мбит/с, используется алгоритм раннего освобождения маркера, суть которого заключается в отправке маркера сразу после передачи кадра данных. В этом случае по сети одновременно могут продвигаться кадры нескольких станций.

Контроль за работой сети, за наличием маркера в сети осуществляет *активный монитор*. Функции активного монитора выполняет один из узлов сети. В частности, в случае отсутствия маркера в сети в течение достаточно длительного времени, активный монитор генерирует новую копию маркера. Одновременно в сети не может быть больше одной копии маркера.

Компания IBM предложила новую технологию High-Speed Token Ring, которая поддерживает скорости 100 и 155 Мбит/с и сохраняет основные особенности технологии Token Ring.

Локальная сеть Ethernet

Сетевой стандарт Ethernet был разработан фирмой Xerox в 1975 году. В 1980 году фирмы DEC, Intel, Xerox разработали стандарт Ethernet DIX на основе коаксиального кабеля. Эта последняя версия фирменного стандарта послужила основой стандарта IEEE 802.3. Стандарт IEEE 802.3 имеет модификации, ко¬торые различаются типом используемой физической среды:

• *10Base-5* – «толстый» коаксиальный кабель диаметром 0,5 дюйма.

• *10Base-2* – «тонкий» коаксиальный кабель диаметром 0,25 дюйма.

• *10Base-T* – неэкранированная витая пара (UTP).

• *10Base-F* – волоконно-оптический кабель.

Локальные сети, построенные по всем перечисленным стандартам, обеспечивают пропускную способность до 10 Мбит/с.

В стандарте 802.3, включая Fast Ethernet (IEEE 802.3u) и Gigabit Ethernet (IEEE 802.3z) (они рассмотрены ниже), в качестве метода доступа к среде передачи данных используется недетерминированный метод – метод коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-miltiply-access with collision detection), *метод CSMA/CD*.

Стандарт Ethernet не позволяет одновременную передачу/прием более одного кадра. На практике в сетях Ethernet возможны ситуации, когда два узла пытаются передать свои кадры. В таких случаях происходит искажение передаваемых данных, потому что методы стандарта Ethernet не позволяет выделять сигналы одного узла из общего сигнала и возникает так называемая коллизия. Передающий узел, первым обнаруживший коллизию, временно прекращает передачу кадра, делает паузу случайной длины и повторяет попытку захвата передающей среды и передачи кадра. После 16 неудачных попыток передачи кадра данный кадр отбрасывается.

При увеличении количества коллизий, когда передающая среда заполняется повторными кадрами, реальная пропускная способность сети резко уменьшается. В этом случае необходимо уменьшить трафик сети любыми доступными метода ми (уменьшение количества узлов сети, использование приложений с меньшими затратами сетевых ресурсов, реструктуризация сети).

Технологии Fast Ethernet и 100VG-AnyLAN

В 1995 году было принято два стандарта: IEEE 802.3u – *Fast Ethernet* и IEEE 802.12 – *100VG-AnyLAN*, с пропускной способностью до 100 Мбит/с.

Технология Fast Ethernet использует метод доступа CSMA/CD, такой же, как в технологии Ethernet.

Отличия Fast Ethernet от Ethernet наблюдаются только на физическом уровне. Установлены три спецификации для физического уровня:

• 100Base-TX – неэкранированная витая пара 5 категории (две пары в кабеле) и экранированная витая пара.

• 100Base-T4 – неэкранированная витая пара 3, 4 или 5 категорий (четыре пары в кабеле).

• 100Base-FX – многомодовое оптоволокно (два волокна в кабеле).

В технологии 100VG-AnyLAN для доступа к разделяемой среде используется приоритетный доступ по требованию *Demand Priority*. Сеть состоит из корневого концентратора и присоединенных к нему узлов и других концентраторов. Концентратор играет роль арбитра доступа к сети. Узел запрашивает у концентратора разрешение на передачу кадра. Если сеть свободна, концентратор отправляет кадр узлу назначения. Если сеть занята, то запрос ставится в очередь.

Технология Gigabit Ethernet

Стандарт IEEE 802.3z Gigabit Ethernet был принят в 1998 году на основе согласованных усилий группы компаний, образовавших объединение Gigabit Ethernet Alliance. Скорость передачи данных до 1000 Мбит/с. Разработчики стандарта максимально сохранили преемственность предыдущих стандартов Ethernet: сохраняются все форматы кадров; поддерживается тот же метод доступа CSMA/CD с минимальными изменениями.

Для многомодового оптоволокна стандарт IEEE 802.3z определил две спецификации: 1000Base-SX и 1000Base-LX.

Технология FDDI

Сеть FDDI состоит из двух колец для повышения отказоустойчивости. Данные передаются по первичному кольцу сети в одном направлении, по вторичному кольцу – в противоположном. В обычном режиме используется только первичное кольцо. В случае отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), происходит процесс сворачивания колец (Wrap-режим), при

котором первичное кольцо объединяется с вторичным, образуя новое кольцо. При множественных отказах сеть распадается на несколько колец.

Кольца сети FDDI являются разделяемой средой передачи данных, для доступа которой применяется маркерный метод, аналогичный используемому в сетях Token Ring. Различия в некоторых деталях. Время удержания маркера является переменной величиной и зависит от степени загрузки сети. При небольшой загрузке сети время удержания маркера больше, при большой загрузке – уменьшается.

Сеть FDDI поддерживает скорость 100 Мбит/с. Стоимость реализации данной технологии значительна, поэтому область применения стандарта FDDI – магистрали сетей и крупные сети.

7.9. Контрольные вопросы

1. Определение ЛВС и характеристика ее основных компонентов
2. Коммуникационное оборудование ЛВС
3. Классификация и назначение серверов в составе ЛВС
4. Средства коммуникации в ЛВС
5. Принципы кодирования информации
6. Методы передачи информации (симплексная, дуплексная, полудуплексная)
7. Характеристика методов мультиплексирования
8. Синхронный и асинхронный методы передачи информации
9. Организация взаимодействия устройств в сети
10. Структура базовой модели OSI
11. Классификация ЛВС по территориальному признаку и масштабу
12. Классификация ЛВС по масштабу сети
13. Классификация ЛВС по способу передачи информации
14. Основные топологии построения ЛВС
15. Типы построения сетей по методам передачи информации

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В БУХГАЛТЕРСКОМ УЧЕТЕ, ФИНАНСОВОЙ, МАРКЕТИНГОВОЙ И ЛОГИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИТЯ

8.1. Информационные технологии в бухгалтерском учете предприятия

Информационная система предприятия состоит из взаимосвязанных подсистем (конструкторской, технологической, экономической и др.). Наибольшее значение для управления имеет экономическая информация. Она подразделяется на следующие виды: плановая, нормативная, учетная и прочая (материалы ревизий или аудиторских проверок, объяснительных и докладных записок, деловая переписка с другими организациями и т. п.).

В совокупности экономической информации наибольший удельный вес занимает учетная, базирующаяся в основном на данных бухгалтерского учета. Учетную систему предприятия можно представить в виде схемы

На долю бухгалтерской информации приходится свыше 70% общего объема экономической информации. Именно бухгалтерский учет фиксирует и накапливает всестороннюю синтетическую (обобщающую) и аналитическую (детализированную) информацию о состоянии и движении имущества предприятия, источниках его образования, хозяйственных процессах, конечных результатах финансовой и производственно-хозяйственной деятельности.

Бухгалтерская информация широко используется в оперативно-техническом и статистическом учете, а также в налогообложении, планировании, прогнозировании, выработке тактики и стратегии деятельности предприятия.

Выбор программного обеспечения для бухучета проводится по различным признакам и правилам. Существенные признаки классификации программных комплексов – размер предприятия, на который они рассчитаны и, соответственно, масштаб задач бухгалтерского учета, а также определенная специализация некоторых бухгалтерских программ. С учетом масштаба задач бухучета можно выделить программы для ***малых, средних*** и ***крупных предприятий***.

Автоматизированные информационные технологии в мини-бухгалтериях на малых предприятиях и предприятиях без образования юридического лица характерны тем, что бухучет ведется на одном компьютере. Вместе с тем может встречаться и сетевой вариант на два-четыре места. Функции ведения синтетического и стоимостного аналитического учета позволяют вводить и обрабатывать бухгалтерские записи, оформлять небольшой набор первичных документов и формировать отчетность. Для таких предприятий существует широкий спектр бухгалтерских тиражных программ, таких как: ***«1С:Бухгалтерия», «Инфо-Бухгалтер», «Инфин-Бухгалтерия», «БЭСТ-Офис», «Турбо-Бухгалтер», «Парус-бухгалтерия», «СБИС, Инотек», «Контур», «ИП:Бухгалтерия», «Финансы без проблем», «Бухгалтерия малого предприятия»*** и др.

Для автоматизированных информационных технологий бухгалтерий средних предприятий типично наличие сетевой программы автоматизации бухгалтерии на пять-десять мест, которые относятся к классу интегрированных бухгалтерских систем. Эти программы объединяют и поддерживают ведение всех основных учетных функций и разделов. Они работают в режимах «файл-сервер» или «клиент-сервер». На таких предприятиях бухгалтерский учет часто организован по основным участкам бухучета. К этому классу можно отнести следующие бухгалтерские программы: ***«1С:Бухгалтерия», «БЭСТ-5», «Фин-Эко», «Abacus», «Парус-7», «Компас+SQL», «Инфософт», «Инотек», «ТурбоБухгалтер», «ПК Суперменеджер», «Партнер бухгалтера»*** и др.

Автоматизацию бухгалтерского учета в управлении крупными фир-мами, как правило, отличает использование систем управления БД, например, SQL, Oracle, Atlantis и др. Для такого класса фирм почти всегда необходимо вести бухгалтерский учет нескольких предприятий в составе холдинга. Кроме того, должна быть предусмотрена возможность настройки бухгалтерской системы на специфику конкретного предприятия. Автоматизированная информационная технология бухучета рассматривается здесь как функциональная подсистема, встроенная в автоматизированную систему управления крупной корпоративной фирмы со сложной организационно-производственной структурой. Корпорация может объединять различные управленческие, производственные,

финансовые и другие структуры, иметь несколько территориально удаленных филиалов, предприятий с разнообразными видами деятельности. Обмен данными может выполняться по схеме «клиент-сервер».

В качестве компонентов системы присутствуют различные функциональные подсистемы бухучета с возможностью использования международных стандартов, а также подсистемы оперативного учета, учета кадров, планирования и прогнозирования, анализа и принятия решений, контроля, анализа и оптимизации финансово-хозяйственной деятельности предприятий и др. Здесь подсистема бухучета не имеет главенствующего положения, здесь важна гармонизация всех подсистем для достижения наивысшего эффекта от управления компанией в целом. В данных условиях программный комплекс должен иметь гибконастраиваемую бизнес-логику, позволяющую настраивать систему на работу в самых разных областях предприятия.

Крупные организации используют программные продукты фирм *«Галактика», «Росэкспертиза», «Парус», «Бизнес-Консоль», «Информконтакт», «Инфософт», «Интеллект-Сервис», «БЭСТ-5», «АйТи»* и др.

Класс так называемых адаптивных автоматизированных информационных технологий бухгалтерского учета базируется на специализированных программных продуктах, обладающих расширенными инструментальными возможностями. Они построены по принципу «бухгалтерский конструктор», в частности, имеют модульную, гибкую структуру. При наличии основных бухгалтерских функций имеется специальный встроенный процедурный язык и средства настройки, ориентированные на возможность адаптации к конкретным условиям учета и дополнительным требованиям со стороны пользователя, либо дилера разработчика. К этому классу можно отнести программные продукты фирм *«1С», «Информатик», «Аквилон», «Порт»*.

Имеются системы технологий класса *«Эккаунт кутюр»*. Они, как правило, развиваются на базе типового бухгалтерского ядра для индивидуального заказчика. Доработка дополнительных функций и модулей увеличивают потенциал технологии предприятия-заказчика. Доработка, внедрение и эксплуатация обеспечивается четким сопровождением программных систем разработчиком-исполнителем с учетом конкретных требований заказчика, что

влечет сравнительно высокую стоимость работ. Программы подобного класса разрабатывают фирмы *«Ост-Ин», «БИТ», «Никос-Софт», «Экософт»*.

Автоматизированные информационные технологии бухгалтерского комплекса построены по признаку модульности разделов бухучета. Каждый модуль реализован соответствующим АРМ бухгалтера. Таким образом, достигается явное разделение функций между ними. Комплекс АРМ (пять и более) ориентирован на реализацию бухучета в целом силами персонала различной квалификации. К этому классу относятся программные продукты фирм *«Интеллект-Сервис», «Инфософт», «Комтех+», «Инфин», «АСВП»* и др.

8.2. Информационные технологии в финансовой деятельности предприятия

Высокая роль финансовой информации в подготовке и принятии эффективных управленческих решений предъявляет соответственно высокие требования к её качеству при формировании информационной системы финансового менеджмента.

Исходя из этого, у предприятий и организаций возникает необходимость в автоматизации их финансовой и инвестиционной деятельности.

Присутствующее сегодня на рынке финансово-экономическое прикладное программное обеспечение весьма разнообразно. Так, к числу наиболее распространённых относят следующие:

Программные продуты группы компаний "ИНТАЛЕВ"

"ИНТАЛЕВ" – международная группа компаний, специализирующаяся на разработке и внедрении современных информационных систем управления предприятием.

"ИНТАЛЕВ: Корпоративный менеджмент" ориентирован на применение в крупных и средних организациях различных направлений деятельности и форм собственности, в том числе и в географически-распределенных компаниях. Возможности продукта независимы от отраслевой специфики предприятия. Продукт особенно полезен для компаний, использующих "1С: Предприятие 8", ввиду возможности полной интеграции с 1С.

Эффекты от внедрения «ИНТАЛЕВ: Корпоративный менеджмент» определяются составом его модулей, а также взаимосвязями между ними.

Так, модуль ***“ИНТАЛЕВ: Корпоративные финансы”*** – программно-методический комплекс для управления финансами и эффективностью компаний и холдингов (Finance Management и Business Performance Management).

Продукт позволяет автоматизировать такие области финансового управления как:

- бюджетирование по всей системе бюджетов;
- управленческий и бухгалтерский учет по нескольким стандартам:

• МСФО – международные стандарты финансовой отчетности;

• РСБУ – Российский стандарт ведения бухгалтерского учета;

• НСБУ – Национальный стандарт ведения бухгалтерского учета в Украине;

• КСБУ – Стандарты бухгалтерского учета Республики Казахстан;

• возможно ведение учета по корпоративному стандарту;

- платежный календарь (управление ликвидностью, казначейство);
- финансовый анализ;
- финансовый контроль;
- прогнозирование.

<u>Программные продуты компании “Альт-Инвест”</u>

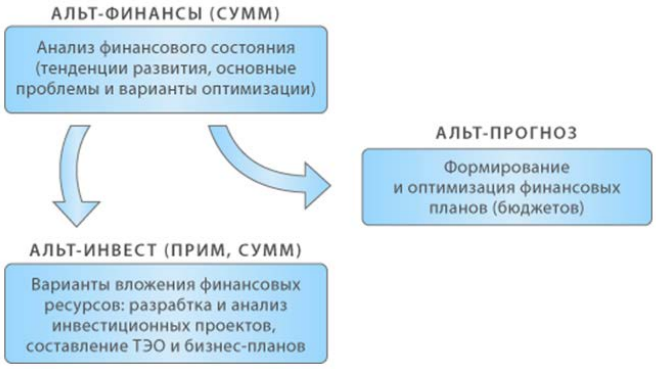


Рис. 8.1. Программные продуты компании “Альт-Инвест”

Компания «Альт-Инвест» работает на рынке консалтинговых услуг и программного обеспечения для аналитиков с 1992 года. До 2004 года компания действовала как департамент экономического анализа исследовательско-консультационной фирмы «Альт», в мае 2004 года этот бизнес выделен в самостоятельную структуру.

Сегодня "Альт-Инвест" – это не только ведущий в России разработчик программного обеспечения для оценки инвестиционных проектов, но и единственная компания, предлагающая в комплексе программные продукты и обучение, а также консультационные услуги в области инвестиционно-финансового анализа и планирования.

Основные направления деятельности компании:

- создание методического и программного обеспечения для инвестиционного и финансового анализа;
- подготовка специалистов по инвестиционному проектированию и управлению финансами;
- финансовый консалтинг.

Программный продукт ***"Альт-Финансы"*** предназначен для выполнения комплексной оценки деятельности предприятия, выявления основных тенденций его развития, расчета базовых нормативов для планирования и прогнозирования, оценки кредитоспособности предприятия.

Программный продукт «Альт-Финансы» использует основные методы проведения анализа:

- горизонтальный – анализ тенденций, при котором показатели сравниваются с аналогичными за другие периоды;
- вертикальный – анализ, при котором исследуется структура показателей путем постепенного углубления и детализации;
- сравнительный – анализ, при котором исследуемые показатели сравниваются со значениями, допустимыми для данного предприятия;
- факторный – анализ, позволяющий определить влияние различных факторов деятельности предприятия на основные финансовые показатели.

Программные продуты компании "ИНЭК"

Группа ИНЭК – одна из крупнейших IT и консалтинговых компаний в России.

Основные направления деятельности компании:

- разработка информационно-аналитического программного обеспечения;

- консалтинг, аудит и оценка;

- бизнес-обучение.

Программные продукты серии “Аналитик” предназначены для автоматизации профессиональной деятельности финансовых директоров, риск-менеджеров и аналитиков, занимающихся оценкой, анализом и планированием деятельности организаций.

Программные продукты серии Аналитик это:

1. Анализ финансово-экономической деятельности предприятий и их мониторинг;

2. Бюджетирование, план-фактный контроль, анализ отклонений исполнения бюджетов;

3. Разработка и анализ бизнес-плана предприятия, плана внешнего управления, инвестиционного проекта, ТЭО кредита;

4. Коммерческая оценка эффективности инвестиций;

5. Оценка стоимости предприятия (бизнеса);

6. Бюджетная эффективность;

7. Консолидация данных предприятий и анализ консолидированной отчетности;

8. Сортировка предприятий по различным показателям;

9. Сравнение деятельности предприятий, отбор предприятий по различным показателям.

Программы, входящие в серию "Аналитик", решают задачи разного уровня сложности:

- Анализ финансового состояния.

Программа ***“ИНЭК-АФСП”*** предназначена для анализа финансового состояния организаций всех видов деятельности и мониторинга хозяйствующих субъектов с использованием данных внешней бухгалтерской отчетности (формы № 1,2,4) и произвольных форм пользователя.

Базовая программа “ИНЭК-АФСП” – содержит минимальный набор расчетов, а каждая последующая по иерархии сложности включает в себя наряду с возможностями предыдущей новые функции.

- Анализ финансового состояния и анализ экономической деятельности.

Программа ***“ИНЭК-АДП”*** (включает все возможности программы “ИНЭК-АФСП”) проводит анализ финансово-

экономической деятельности предприятий всех видов деятельности. Исходной информацией для анализа служат не только формы внешней бухгалтерской отчетности и произвольные формы пользователя, но и данные управленческой отчетности.

- Анализ финансового состояния, анализ экономической деятельности и бизнес-план.

Программный комплекс ***"ИНЭК-Аналитик"*** (включает все возможности программы "ИНЭК-АДП") – решает задачи анализа финансово-экономической деятельности предприятия, разработки и оценки планов его развития, анализа отклонений плана от факта (производство, торговля, услуги, и др.).

Кроме этого, к прикладным программным продуктам, решающим те или иные задачи финансовой деятельности предприятия, относятся:

- ***"КИС:Финанализ"*** и ***"КИС:Бюджетирование"*** компании ЗАО "КИС";
- ***"ФинЭкАнализ 2011"*** Южной аналитической компании (ООО ЮАК);
- ***"Project Expert"*** консалтинговой компании "Эксперт Системс";
- ***"Финансовый анализ:Проф"*** и ***"Финансовый анализ:Проф + Оценка бизнеса"*** компании "Константа";
- ***"ИТ: Финансовое Планирование"***;
- ***"Мастер Финансов. Планирование", "Мастер Финансов. Анализ", "Мастер Финансов. Бюджет предприятия" консультационной группы "Воронов и Максимов"***;
- ***и другие***.

8.3. Информационные технологии в маркетинговой деятельности предприятия

Сегодня на российском программном рынке предлагается достаточно широкий спектр информационных систем, предназначенных для автоматизации маркетинговой деятельности и маркетинговых исследований. По функциональной направленности можно выделить несколько направлений, которые автоматизируются с помощью этих систем. При этом конкретные продукты могут одновременно решать несколько проблем: визуальное объектное моделирование, аудит маркетинга,

комплексная оценка рынка, прогнозирование рыночных тенденций, финансово-организационное планирование маркетинга, оперативный учет маркетинговой деятельности, поддержка маркетинговой деятельности. К числу таких относятся:

Программные продуты компании "КонСи"

КонСи – лидер рынка разработки программного обеспечения для проведения маркетинговых исследований и принятия бизнес-решений.

КонСи выпускает следующую серию программных продуктов:

- поддержка процедур анкетирования и проведения массовых опросов (***KonSi-Simple Anketter*** – КонСи-Простой Анкетер; ***KonSi-Anketter for Positioning Brands*** – КонСи-Анкетер для позиционирования брендов; ***KonSi-Benchmarking Prices*** – Бенчмаркинг цен, сравнение цен конкурентов; ***KonSi-Price Sensitivity Meter van Westendorp*** – Определение оптимальной цены по методу van Westendorp; ***KonSi-Price Sensitivity Meter by Gabor/Granger*** – Определение оптимальной цены по методу Gabor/Granger; ***KonSi-Brand Price Trade Off*** – Определение цены переключения покупателя с бренда на бренд);

- выделение целевых сегментов рынка с применением различных технологий в том числе кластерного и факторного анализа и позиционирование продукта на целевых сегментах рынка с построением карты позиционирования (***KonSi-Segmentation&Positioning*** – КонСи-Сегментирование рынка и позиционирование бренда);

- анализ временных рядов для построения прогнозов продаж и экономических показателей (***KonSi-Forexsal*** (Forecasting Expert Sales System) – Прогнозирование продаж трендовыми и сезонными методами анализа временных рядов);

- формирование оптимального ассортимента для торговых компаний и промышленных предприятий (***KonSi Assortment Optimization***). Пользователями программы KonSi-Assortment Optimization являются отделы снабжения, закупки и сбыта;

- анализ конкурентов, накопления и анализа разведывательных данных о конкурентах, поиска лучшей практики с применением технологии бенчмаркинга (***KonSi-Competitive Intelligence&Benchmarking*** – КонСи-Конкурентная разведка и конкурентный бенчмаркинг; ***KonSi-Benchmarking Prices*** – Бенчмаркинг цен, сравнение цен конкурентов; ***KonSi-Multi SWOT***

Analysys – КонСи-SWOT анализ для изучения многих конкурентов и анализ их стратегий стратегий);

- SWOT анализ для изучения ситуации на рынке и разработки стратегий поведения (***KonSi-Simple SWOT Analysys*** – КонСи-SWOT анализ для изучения одного объекта и разработки стратегий; ***KonSi-Multi SWOT Analysys*** – КонСи-SWOT анализ для изучения многих конкурентов и анализ их стратегий стратегий);

- анализ эффективности торговых сетей, DEA (Data Envelopment Analysis) анализ, планирование улучшений в работе (***KonSi-DEA Analysys*** – КонСи-DEA анализ);

- ценовой мониторинг и сравнение цен (на промышленное сырье и материалы, станки и оборудование и пр.), анализ цен конкурентов и поставщиков (***KonSi-Price Monitoring for Marketing*** – Ценовой мониторинг для отделов продаж и маркетинга; ***KonSi-Price Monitoring for LOGISTICS*** – Ценовой мониторинг для отделов снабжения и логистиков; ***KonSi-Benchmarking Prices*** – Бенчмаркинг цен, сравнение цен конкурентов);

- ценообразование и определение оптимальной цены на новый продукт (***KonSi-Price Sensitivity Meter van Westendorp; KonSi-Price Sensitivity Meter by Gabor/Grander; KonSi-Brand Price Trade Off***);

Работа с клиентами (CRM) – обеспечивает компьютерную поддержку работы персонала отдела маркетинга и сбыта по выполнению контактов с клиентами (так называемая технология CRM – Customer Relationship Management – управление взаимоотношениями с клиентами) - ***KonSi-Marketing 9.7*** – ведение работы с клиентами при продвижении продукции CRM;

- региональный маркетинг и анализ продаж и рынка с применением географических карт (***KonSi-Regional Marketing*** – КонСи-Региональный маркетинг – представление данных о продажах на географических картах).

Программные продуты компании "БЭСТ"

Программная система "БЭСТ-Маркетинг" представляет собой удобный и эффективный инструментарий, позволяющий оценить рыночные позиции предприятия в условиях конкуренции. Система может использоваться на предприятиях производства, торговли и сферы услуг.

В числе методик, на которых базируется "БЭСТ-Маркетинг" – SWOT-анализ и модель Розенберга, метод 4P, матрица Ансоффа.

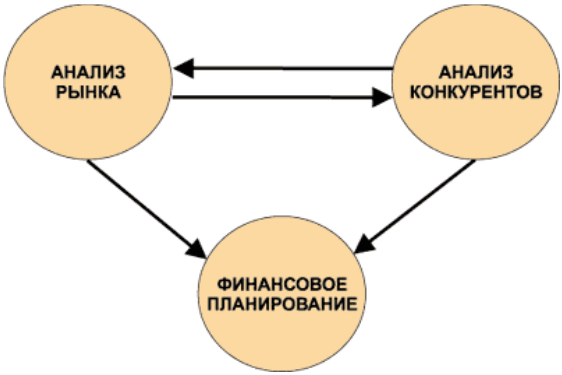


Рис. 8.2. Возможности системы “БЭСТ-Маркетинг”

Возможности системы “БЭСТ-Маркетинг”

- *Анализ рынка:*

• определение перспективных рыночных ниш;

• анализ конкурентоспособности товара;

• анализ рекламы, рекомендации по повышению ее эффективности;

• рекомендации по стимулированию продаж;

- *Анализ конкурентов:*

• степень присутствия конкурентов на рынке;

• сравнительный анализ по товару;

• сравнительный анализ рекламных компаний;

- *Финансовое планирование маркетинговой деятельности:*

• прогноз продаж;

• бюджет рекламы;

• сводный бюджет;

• подготовка бюджета затрат по продвижению продукции и контроль за его исполнением.

Программные продуты компании “Курс”

Программный комплекс ***“Marketing Analytic”*** предназначен для информационно-аналитической поддержки управления маркетингом и коммерческой деятельностью компании на стратегическом, тактическом и оперативном уровне.

На стратегическом уровне “Marketing Analytic” помогает решить следующие ключевые задачи:

- сегментация базовых рынков,

- анализ текущего положения компании на рынке (привлекательность сегментов для компании, конкурентоспособность компании на сегментах, доходность и прибыльность сегментов),

- оценка будущего положения компании при различных стратегиях развития.

На тактическом уровне “Marketing Analytic” оказывает информационно-аналитическую поддержку при решении следующих задач:

- планирование комплекса маркетинга: формирование ассортимента, ценообразование, подготовка программы мероприятий по продвижению, планирование работы сбытовой сети,

- анализ результативности и эффективности мероприятий комплекса маркетинга,

- среднесрочное прогнозирование объема продаж.

На оперативном уровне “Marketing Analytic” используется для решения следующих задач:

- автоматизация работы персонала продаж (управление контактами с клиентами, подготовка стандартных документов и другие рутинные операции),

- планирование и контроль текущей работы персонала продаж и партнеров по сбыту;

- планирование мероприятий по продвижению и контроль их выполнения;

- оперативное планирование объема продаж и закупок (для торговых компаний).

Кроме этого, к прикладным программным продуктам, решающим задачи маркетинговой деятельности предприятия на основе концепции управления отношениями с клиентами (CRM) в условиях активной конкуренции, относятся:

- CRM-система ***“Маркетинг и менеджмент”*** компании “Компас”, обеспечивающая автоматизацию управления взаимоотношениями с клиентами;

- ***“SugarCRM”*** компании “АйТи” предлагает богатый набор возможностей, использование которых повышает эффективность маркетинговых мероприятий, способствует росту производительности труда менеджеров по продажам, улучшает качество обслуживания клиентов и делает прозрачными бизнес-процессы компании. Обеспечивая эффективное взаимодействие

сотрудников и новые возможности для управления, настраиваемые в соответствии со спецификой предприятия, “SugarCRM” успешно работает в сотнях компаний всех размеров, ведущих свою деятельность в различных отраслях бизнеса;

- ***“1С:Управление торговлей 8”*** компании “1С”;

- ***“NetSuite CRM”*** компании “Systematic Software Solutions (Russia)”. Помимо фундаментальных принципов CRM-системы, таких как: автоматизация продаж, автоматизация маркетинга и служба поддержки и обслуживания клиентов, которые стали еще более эффективными благодаря возможностям индивидуальной пользовательской настройки, “NetSuite CRM” включает также web-сервисы через NetFlex, масштабные системные маркетинговые кампании, расширенное прогнозирование, управление контактами и управление возможностями;

- ***и другие***.

8.4. Информационные технологии в логистической деятельности предприятия

В настоящее время на российском рынке программных продуктов, предусматривающих автоматизацию управления логистическими процессами, представлено огромное количество систем и пакетов прикладных программ (ППП). Рассмотрим наиболее известные программные продукты отечественных производителей, которые уже достаточно широко внедрены в бизнес-практику.

Программные продуты компании “БЭСТ”

Система управления предприятием ***БЭСТ-5*** разрабатывается с 2001 года большим коллективом специалистов по информационным технологиям, управлению, бухгалтерскому и налоговому учету.

Система располагает всеми необходимыми средствами для эффективного ведения учета и принятия выверенных управленческих решений по всем направлениям деятельности современного торгового или производственного предприятия и др.

Система БЭСТ-5 состоит из набора взаимосвязанных функциональных компонентов – приложений. Каждое приложение автоматизирует отдельную область учета или управления на предприятии. Приложения могут работать как в автономном

режиме, так и совместно друг с другом, образуя единое информационное пространство предприятия.

Приложение ***"БЭСТ-5"-Логистика*** – это группа приложений для эффективного управления закупками, запасами и продажами. Реализует полнообъемный учет товаров, сырья, материалов, полуфабрикатов и готовой продукции. Обеспечивает управление продажами в оптовой и розничной торговле, а также в мобильной торговле. Решает задачи учета реализации работ/услуг и управления работой автотранспортных служб предприятия.

Программные продуты компании "Корпорация ПАРУС"

Система ***"ПАРУС-Предприятие 7"*** предназначена для малых и средних хозрасчетных предприятий различной отраслевой принадлежности.

Система построена по модульному принципу и представляет собой набор модулей, каждый из которых предназначен для автоматизации одного из основных видов деятельности предприятия и может работать как в автономном режиме, так и совместно с другими модулями комплекса, образуя единое информационно-управленческое пространство масштаба предприятия.

Основные возможности по автоматизации торговой и складской деятельности (модуль ***"Реализация и склад"***):

- полная поддержка мультивалютного учета;
- поддержка оптовой продажи любых видов товаров и услуг;
- полный учет и контроль не только за движением товаров, но и за взаиморасчетами и состоянием финансов без привлечения бухгалтерии;
- ведение учетных регистров заказов, приходных ордеров, счетов, накладных;
- учет и отработка результатов инвентаризации и возвратов;
- ведение журнала товарных запасов:
- настраиваемый партионный учет с возможностью автоматического учета сроков годности;
- резервирование товара;
- ведение журнала платежей;
- учет товаров в натуральном и стоимостном выражении с момента его поступления до продажи и списания вне зависимости от его местонахождения (на складах, в торговых залах, в отделах);
- работа с лицевыми счетами контрагентов, ведение лимита кредитования;

- ведение многих тарифов, автоматизированное формирование цен реализации;

- прямая обработка торговых документов в бухгалтерской подсистеме;

- учет нормативных затрат по картам;

- создание актов комплектации и разукомплектации;

- отработка актов разукомплектации со списанием комплектующих;

- списание комплектующих с оприходованием готового изделия;

- списание изделия с оприходованием комплектующих;

- получение полной отчетности по складу.

Программные продуты компании "1С"

Выпуск совместно с партнерами отраслевых и специализированных решений на платформе "1С:Предприятие" является одним из ключевых направлений стратегии развития и продвижения программ экономического назначения фирмы "1С".

Программный продукт ***"1С-Логистика: Управление складом 3.0"*** – специализированное тиражное решение на платформе "1С:Предприятие 8" для автоматизации управления складским хозяйством предприятия. Продукт позволяет эффективно автоматизировать управление технологическими процессами современного складского комплекса. Программный продукт "1С-Логистика: Управление складом 3.0" – совместный продукт фирмы "1С" и компании "AXELOT", созданный в результате анализа опыта автоматизации и управления складских хозяйств ряда российских и зарубежных компаний, а также на основе анализа опыта внедрения продукта "1С-Логистика: Управление складом" редакции 1 и 2.

К функциональным возможностям "1С-Логистика: Управление складом 3.0" относится:

- задание топологии склада и учет товара на складе;

- приемка и размещение товара;

- отбор, упаковка и отгрузка товара;

- внутрискладские операции;

- инвентаризация;

- управление задачами;

- штрихкодирование;

- расчет услуг ответственного хранения.

“1С-Логистика:Управление перевозками” – программный продукт на технологической платформе “1С-Предприятие 8”, предназначенный для автоматизации транспортной логистики, с целью повышения рентабельности логистических операций.

Система предоставляет возможности управления процессом перевозки товарно-материальных ценностей по цепи “поставщик – склад – клиент”.

Система ориентирована на предприятия, которые стремятся оптимизировать и наилучшим образом управлять транспортными перевозками, и может использоваться:

- Транспортными компаниями, которые осуществляют перевозки любым видом транспорта, в том числе и смешанные перевозки (интермодальные). При этом компания может задействовать как собственный парк транспортных средств, так и пользоваться услугами сторонних организаций для перевозки на отдельных участках маршрута;

- Транспортно-логистическими подразделениями предприятий (торговых, производственных и т.д.), обеспечивающих как доставку ТМЦ от поставщиков, так и доставку ТМЦ покупателям. При этом подразделение может использовать услуги сторонних транспортных компаний и/или использовать свои собственные транспортные мощности;

- Отделом закупок для планирования и контроля процесса доставки товара в случае доставки товара поставщиком. В этом случае система позволяет учитывать и контролировать все предстоящие и текущие доставки, позволяя тем самым планировать связанную с этим торгово-производственную деятельность;

- Отделом продаж для планирования и контроля отгрузки товара со склада организации, если предприятие оказывает услуги доставки товара клиентам;

- Подразделениями компаний, отвечающими за организацию межскладского перемещения товаров в рамках предприятия, что особенно актуально при наличии нескольких территориально-распределенных складов.

Система позволяет решить наиболее типовые транспортно-логистические проблемы:

• Неэффективное использование моделей и типов транспортных средств по причине отсутствия алгоритмов подбора с

учетом максимального использования грузоподъемных характеристик;

• Увеличенный пробег транспортных средств по причине отсутствия алгоритмов оптимальной маршрутизации;

• Отсутствие контроля за местоположением транспортного средства и состоянием груза в процессе перевозки;

• Отсутствие или недостаток обмена информацией между подразделениями компании, участвующими в процессе перевозки;

• Отсутствие системы формирования актуальной отчетности для оценки эффективности и качества выполняемых работ с целью принятия необходимых управленческих решений.

Система «1С-Логистика:Управление перевозками» реализована в среде «1С:Предприятие 8» и использует все достоинства этой современной технологической платформы: масштабируемость, открытость, простоту администрирования и конфигурирования, и т.д.

"1С:Предприятие 8. МТО Материально-техническое обеспечение"

Конфигурация "МТО Материально-техническое обеспечение" разработана на базе типовой конфигурации "Управление производственным предприятием" ред. 1.3 системы программ "1С:Предприятие 8" с сохранением всех возможностей и механизмов этого типового решения.

В дополнение к возможностям типовой конфигурации "Управление производственным предприятием", конфигурация "МТО Материально-техническое обеспечение" учитывает специфику материально-технического обеспечения холдингов и крупных промышленных предприятий и обеспечивает следующие возможности:

- Управление процессом централизованного формирования потребностей в материалах и оборудовании по статьям расхода и направлениям деятельности в соответствии с выделенным бюджетом (лимитом) на основе единого Классификатора материально-технических ресурсов (МТР);

- Управление процессом формирования потребностей в материалах и оборудовании на промышленные объекты в соответствии с запланированными мероприятиями по направлениям деятельности;

- Анализ соответствия потребностей в МТР планам, проектам, бюджетам, программам, планово-предупредительным работам и т.д.;

- Управление подготовкой и утверждением Плана МТО;

- Планирование закупочной деятельности в соответствии с Планом МТО;

- Организация конкурентных закупок МТР и формирование спецификации к контрактам на поставку с победителями торгов;

- Управление процессом контроля наличия остатков МТР на складах и их распределения в соответствии с потребностями;

- Управление процессом контроля наличия запасов на аварийные и непредвиденные ситуации и за своевременностью их пополнения;

- Формирование оперативной и управленческой отчетности о выполнении планов обеспечения и закупок на основе единого Классификатора НСИ;

- Интеграция с web-площадкой электронных торгов.

Программные продуты компании "ФОЛИО"

Корпоративная информационная система (КИС) ***ФОЛИО Купец*** – современный программный комплекс для автоматизации учета в торговле, производстве и на складах ответственного хранения.

Модульная структура системы, способной решать, практически, все задачи контроля и управления, обеспечивает ей необходимую гибкость – т.е. возможность использования только необходимых пользователю программ-модулей системы, а также простоту подключения новых модулей, по мере возникновения надобности в них.

Корпоративная информационная система ФОЛИО Купец включает следующие основные модули, связанные с логистической деятельностью:

ФОЛИО WinСклад. Проф – профессиональная версия программ складского учета и торговли, предназначенная для автоматизации учета и анализа движения товаров и денежных средств, формирования различных отчетов, подготовки и печати первичных складских и платежных документов, экспорта данных в бухгалтерские программы ФОЛИО, 1С и других производителей, а также в MS Excel. Поддерживается обмен данными и работа в режиме on-line с удаленными рабочими местами, филиалами, складами, магазинами. Обеспечивает полную автоматизацию

технологии складирования на больших складах со сложной системой хранения товаров.

ФОЛИО Заказ-Поставка (ФОЛИО CSM) – система управления цепочками поставок, автоматизирующая работу отделов закупки и логистики предприятия, предназначена для отслеживания перемещения товара от заказа поставщику до прихода на склад.

SCM система фолио состоит из ряда модулей, отвечающих за сбор заявок, их консолидацию, выбор поставщика, согласование заказов, контроль исполнения поставок, формирование отчетов. Являясь модулем КИС "ФОЛИО Купец", ФОЛИО SCM (ФОЛИО Заказ-Поставка) может работать либо самостоятельно, либо – в составе корпоративной системы, обмениваясь данными с программами – модулями: складского учета, складской логистики, бухгалтерского учета и управления взаимоотношениями с клиентами (CRM).

В отличие от других модулей корпоративной системы, отвечающих за автоматизацию внутренних бизнес-процессов, SCM система отвечает за взаимодействие с "внешним миром", обеспечивая полный цикл документооборота, связанного с закупками.

Программные продукты компании Никос-Софт

Компания Никос-Софт – одна из ведущих российских компаний-разработчиков программного обеспечения в области автоматизации процессов коммерческой логистики, финансово-экономической и торговой деятельности предприятий.

Система ***NS2000*** представляет собой программный конструктор, состоящий из нескольких комплектов функциональных модулей. Комбинируя эти модули можно создавать оригинальные системы управления предприятием, учитывающие все особенности функционирования компании. При этом достигается, с одной стороны, значительная экономия средств, так как используются стандартные модули, с другой стороны – гибкость индивидуального проекта, сделанного под заказ.

В модулях направления логистика системы NS2000 реализован полный набор всех операций от первого запроса клиента до окончательного выставления счета и оформления отгрузочных документов. Гибкая, легко настраиваемая система расчета цен отвечает самым взыскательным требованиям и позволяет осуществлять временной резервирование товаров на складе под

заказ, делать выбор специальной конфигурации цены, осуществлять контроль оплат и анализ задолженности.

Кроме этого задачи логистической деятельности решают такие программы, как:

- ***"Галактика ERP"***. Контур логистика системы Галактика ERP позволяет интегрировать в единую систему основные функции логистики: управление заказами и закупками, снабжением и сбытом, управление запасами, складами, взаимоотношениями с поставщиками и получателями продукции и услуг, а также контроль взаиморасчетов;

- ***"AVACCO"***. Основные задачи автоматизация логистики выражены в транспортной логистике данной системы и могут быть сформулированы как:

- выбор типа транспортных средств,

- совместное планирование транспортного процесса со складским и производственным процессами,

- совместное планирование транспортных процессов на различных видах транспорта (в случае смешанных перевозок),

- обеспечение технологического единства транспортно-складского процесса,

- определение рациональных маршрутов доставки.

- ***"Бизнес Про"***. Решения "Бизнес Про" позволяют сформировать эффективную систему управления для предприятий различных сфер деятельности: транспортная логистика, оптовая торговля, цепочки поставок, розничная торговля.

Все отраслевые решения надежно интегрируются с базовыми подсистемами "Бизнес Про", что обеспечивает полную автоматизацию бизнес-процессов компаний на базе одной системы. Автоматизация предприятий, имеющих холдинговую структуру, одно из достоинств "Бизнес Про".

- ***и другие***.

8.5. Контрольные вопросы

1. ИТ в бухгалтерском учете предприятия
2. ИТ в финансовой деятельности предприятия
3. ИТ в маркетинговой деятельности предприятия
4. ИТ в логистической деятельности предприятия

9. ЗАЩИТА ИНФОРМАЦИИ

9.1. Необходимость защиты информации

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость: с одной стороны, возможность уничтожения или искажения информации (т.е. нарушение ее физической целостности), а с другой – возможность несанкционированного использования информации (т.е. опасность утечки информации ограниченного пользования). Второй вид уязвимости вызывает особую озабоченность пользователей ЭВМ.

Безопасность данных включает обеспечение достоверности данных и защиту данных и программ от несанкционированного доступа, копирования, изменения.

Под *угрозой безопасности* автоматизированных систем обработки информации понимают возможность воздействия на информационную систему, которое прямо или косвенно может нанести ущерб её безопасности.

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Основными каналами *"утечки"* информации являются:

1. Прямое хищение носителей и документов.

2. Запоминание или копирование информации.

3. Несанкционированное подключение к аппаратуре и линиям связи или незаконное использование "законной" (т.е. зарегистрированной) аппаратуры системы (чаще всего терминалов пользователей).

4. Несанкционированный доступ к информации за счет специального приспособления математического и программного обеспечения.

К настоящему времени разработано много различных средств, методов, мер и мероприятий, предназначенных для защиты информации. Сюда входят ***аппаратные*** и ***программные*** средства, ***криптографическое*** закрытие информации, ***физические*** меры (различные устройства и сооружения, а также мероприятия, которые затрудняют или делают невозможным проникновение потенциальных нарушителей в места, в которых можно иметь доступ к защищаемой информации), ***организационные*** мероприятия (нормативно-правовые акты, которые регламентируют процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется), ***законодательные*** меры.

Виды защищаемой информации

В соответствии с п. 2 ст. 5 Федерального закона «Об информации, информационных технологиях и защите информации» информация в зависимости от категории доступа к ней подразделяется на общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

В п. 2 ст. 7 того же Закона отмечается, что общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

В п. 2 ст. 1 говорится, что действие данного Закона, в том числе в вопросах защиты информации, не распространяется «...на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации». Следовательно, защита общедоступной информации должна осуществляться в соответствии с требованиями части четвертой Гражданского кодекса РФ.

В ст. 16 уже не подчеркивается, что защите подлежит только информация ограниченного доступа. В отношении некоторых видов информации ограниченного доступа (государственной, коммерческой, банковской, врачебной тайны, персональных данных) существуют отдельные законодательные акты, регламентирующие порядок обращения с ней. На основании этого можно сделать вывод, что защите подлежит как общедоступная информация, которая может подвергнуться подмене или искажению, так и информация ограниченного доступа.

Классификация мер защиты информации

Классификация мер по защите информации в соответствии с п. 1 ст. 16 Федерального закона № 149-ФЗ представляет собой сочетание правовых, организационных и технических мер. При широкой трактовке понятия защита информации, которое в этом случае правильнее заменить на сочетание "*информационная безопасность*", в перечень мер защиты должны быть включены и физические меры защиты.

9.2. Законодательные меры защиты информации

Законодательные меры занимают около 5% объема средств, расходуемых на защиту информации. Это меры по разработке и практическому применению законов, постановлений, инструкций и правил эксплуатации, контроля как аппаратного, так и программного обеспечения компьютерных и информационных систем, включая линии связи, а также все объекты инфраструктуры, обеспечивающие доступ к этим системам. В России деятельность в информационной сфере регулируют более 1000 нормативных документов. Уголовное преследование за преступления в этой сфере осуществляется в соответствии с гл. 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», содержащей три статьи.

1. Ст. 272 – несанкционированный доступ к информации. ***Несанкционированный доступ к информации*** – нарушение установленных правил разграничения доступа с использованием штатных средств, предоставляемых ресурсами вычислительной техники и автоматизированными системами (сетями). Отметим, что

при решении вопроса о санкционированности доступа к конкретной информации необходимо наличие документа об установлении правил разграничения доступа, если эти правила не прописаны законодательно.

2. Ст. 273 – создание, использование и распространение (включая продажу зараженных носителей) вредоносных программ для ЭВМ, хотя перечень и признаки их законодательно не закреплены. ***Вредоносная программа*** – специально созданная или измененная существующая программа, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети.

3. Ст. 274 – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это – нарушение работы программ, баз данных, выдача искаженной информации, а также нештатное функционирование аппаратных средств и периферийных устройств; нарушение нормального функционирования сети, прекращение функционирования автоматизированной информационной систем в установленном режиме; сбой в обработке компьютерной информации.

Уголовное преследование за незаконные действия с общедоступной информацией осуществляется в соответствии со ст. 146 «Нарушение авторских и смежных прав» и 147 «Нарушение изобретательских и патентных прав» гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» Уголовного кодекса РФ.

Ответственность за соблюдением сотрудниками организации или компании законодательных мер по защите информации лежит на каждом сотруднике организации или компании, а контроль за их соблюдением – на руководителе.

9.3. Аппаратные методы защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. Наибольшее распространение получили:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

- генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;

- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

- специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;

- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (*криптографические методы*).

Криптографическое закрытие (шифрование) информации заключается в таком преобразовании защищаемой информации, при котором по внешнему виду нельзя определить содержание закрытых данных.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований, в том числе: достаточная стойкость (надежность закрытия), простота шифрования и расшифровывания, способ внутримашинного представления информации, нечувствительность к небольшим ошибкам шифрования, возможность внутримашинной обработки зашифрованной информации, незначительная избыточность информации за счет шифрования и ряд других. В той или иной степени этим требованиям отвечают некоторые виды шифров замены, перестановки, гаммирования, а также шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование ***заменой*** (иногда употребляется термин "подстановка") заключается в том, что символы шифруемого текста заменяются символами другого или того же алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование ***перестановкой*** заключается в том, что символы шифруемого текста переставляются по какому-то правилу в пределах какого-то блока этого текста.

Шифрование ***гаммированием*** (данный способ считается одним из основных для шифрования информации в автоматизированных системах) заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой.

Шифрование ***аналитическим преобразованием*** заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).

Особенно эффективными являются комбинированные шифры, когда текст последовательно шифруется двумя или большим числом систем шифрования (например, замена и гаммирование, перестановка и гаммирование). Считается, что при этом стойкость шифрования превышает суммарную стойкость в составных шифрах.

Каждую из рассмотренных систем шифрования можно реализовать в автоматизированной системе либо программным путем, либо с помощью специальной аппаратуры. Программная реализация по сравнению с аппаратной является более гибкой и обходится дешевле. Однако аппаратное шифрование в общем случае в несколько раз производительнее.

Физические меры защиты информации

Физические меры (доля 15-20%) обеспечивают ограничение физического доступа к компьютеру, линии связи, телекоммуникационному оборудованию и контроль доступа. Физические меры защиты направлены на управление доступом физических лиц, автомобилей, грузов в охраняемую зону, а также на противодействие средствам агентурной и технической разведки. Эти меры включают: охрану периметра, территории, помещений; визуальное и видеонаблюдение; опознавание людей и грузов; идентификацию техники; сигнализацию и блокировку; ограничение физического доступа в помещения.

Выделяют три основные макрофункции физической защиты (рис. 9.1):

- внешнюю защиту;
- опознавание;
- внутреннюю защиту.

Перечисленные средства служат для обнаружения угроз и оповещения сотрудников охраны или персонала объекта о появлении и нарастании угроз.

Из 12 разбитых по функциональному признаку групп более детально рассмотрим четыре группы, использующие в своей технической реализации собственные компьютерные средства либо пригодные для защиты самих рабочих помещений с компьютерами.

Рис. 9.1. Основные макрофункции физической защиты

Охранная сигнализация. Основной элемент сигнализации – датчики, фиксирующие изменение одного или нескольких физических параметров, характеристик.

Датчики классифицируют по следующим группам:

• *объемные*, позволяющие контролировать пространство помещений, например внутри компьютерных классов;

• *линейные*, или поверхностные, для контроля периметров территорий, зданий, стен, проемов (окна, двери);

• *локальные*, или *точечные*, для контроля состояния отдельных элементов (закрыто окно или дверь).

Датчики устанавливаются как открыто, так и скрытно. Наиболее распространены:

• *выключатели* (размыкатели), механически или магнитным способом замыкающие (размыкающие) управляющую электрическую цепь при появлении нарушителя. Бывают напольные, настенные, на касание;

• *инфраакустические*, устанавливаемые на металлические ограждения для улавливания низкочастотных колебаний, возникающих во время их преодоления;

• *датчики электрического поля*, состоящие из излучателя и нескольких приемников. Выполняются в виде натянутых между столбами проводов-кабелей. Изменение поля при появлении нарушителя и фиксируется датчиком;

• *инфракрасные датчики* (излучатель – диод либо лазер), используемые для сканирования поверхностей или объемов помещений. Тепловая "фотография" запоминается и сравнивается с последующей для выявления факта перемещения объекта в защищаемом объеме;

• *микроволновые* – сверхвысокочастотный передатчик и приемник;

• *датчики давления*, реагирующие на изменение механической нагрузки на среду, в которой они уложены или установлены;

• *магнитные датчики* (в виде сетки), реагирующие на металлические предметы, имеющиеся у нарушителя;

• *ультразвуковые датчики*, реагирующие на звуковые колебания конструкций в области средних частот (до 30— 100 кГц);

• *емкостные*, реагирующие на изменение электрической емкости между полом помещения и решетчатым внутренним ограждением при появлении инородного объекта.

Средства оповещения и связи. Всевозможные сирены, звонки, лампы, подающие постоянный или прерывистые сигналы о том, что датчик зафиксировал появление угрозы. На больших расстояниях используют радиосвязь, на малых специальную экранированную защищенную кабельную разводку. Обязательное требование – наличие автоматического резервирования электропитания средств сигнализации.

Охранное телевидение. Распространенное физическое средство защиты. Главная особенность – возможность не только фиксировать визуально факт нарушения режима охраны объекта и контролировать обстановку вокруг объекта, но и документировать факт нарушения, как правило, с помощью видеомагнитофона.

В отличие от обычного телевидения, в системах охранного ТВ монитор принимает изображение от одной или нескольких видеокамер, установленных в известном только ограниченному кругу лиц месте (так называемое закрытое ТВ). Естественно, что

кабельные линии для передачи сигналов охранного ТВ не должны быть доступны иным лицам, кроме охраны. Мониторы располагаются в отдельных помещениях, доступ в которые должен быть ограничен.

Рассмотренные выше три группы относятся к категории средств обнаружения вторжения или угрозы.

Естественные средства противодействия вторжению. Сюда относятся естественные или искусственные барьеры (водные преграды, сильно пересекающаяся местность, заборы, спецограждения, особые конструкции помещений, сейфы, запираемые металлические ящики для компьютеров и т.п.).

Средства ограничения доступа, в состав которых входит компьютерная техника. Сюда относятся биометрические или иные, использующие внешние по отношению к компьютеру носители паролей или идентифицирующих кодов, пластиковые карты, флеш-карты, таблетки Touch Memory и другие средства ограничения доступа.

Биометрические средства ограничения доступа. Особенность биометрических методов допуска состоит в их статистической природе. В процессе проверки объекта при наличии ранее запомненного кода устройство контроля выдает сообщение по принципу “совпадает” или “не совпадает”. В случае считывания копии биологического кода и его сравнения с оригиналом речь идет о вероятности ошибки, которая является функцией чувствительности, разрешающей способности и программного обеспечения контролирующего доступ прибора. Качество биометрической системы контроля доступа определяется следующими характеристиками:

• вероятностью ошибочного допуска “чужого” ошибка первого рода;

• вероятностью ошибочного задержания (отказа в допуске) “своего” легального пользователя – ошибка второго рода;

• временем доступа или временем идентификации;

• стоимостью аппаратной и программной частей биометрической системы контроля доступа, включая расходы на обучение персонала, установку, обслуживание и ремонт.

Большая часть биометрических средств защиты реализована на трех компонентах: сканер (датчик) – преобразователь (сигналы датчика в цифровой код для компьютера) компьютер (хранитель

базы биометрических кодов – характеристик объекта, сравнение с принятой от датчика информацией, принятие решения о допуске объекта или блокировании его доступа).

В качестве уникального биологического кода человека в биометрии используются параметры двух групп.

Поведенческие, основанные на специфике действий человека, – это тембр голоса, подпись, индивидуальная походка, клавиатурный почерк. Главный недостаток поведенческих характеристик – временная неустойчивость, т.е. возможность значительного изменения со временем. Это в значительной степени ограничивает применение поведенческих характеристик как средств ограничения доступа. Однако на протяжении относительно короткого временного интервала они применимы как идентифицирующие личность средства. Пример – фиксация клавиатурного почерка работающего в процессе осуществления им сетевой атаки и последующий (после задержания злоумышленника) контрольный набор определенного текста желательно на изъятой у него клавиатуре (лучше на его же компьютере).

Физиологические, использующие анатомическую уникальность каждого человека, - радужная оболочка глаза, сетчатка глаза, отпечатки пальцев, отпечаток ладони, геометрия кисти руки, геометрия лица, термограмма лица, структура кожи (эпителия) на пальцах на основе ультразвукового цифрового сканирования, форма ушной раковины, трехмерное изображение лица, структура кровеносных сосудов руки, структура ДНК, анализ индивидуальных запахов. Справедливости ради отметим, что большая часть перечисленных биометрических средств пока не производится в массовых масштабах.

Устройства биометрического контроля начали распространяться в России еще до 2000 г. Однако из-за высокой цены на российских рынках (десятки тысяч долларов за устройство) подобная техника была экзотикой. Сегодня цены на подобное оборудование снизились в 10 раз, биометрические средства стали более доступны и имеют устойчивый спрос в России. Иная причина – осознание необходимости защиты от преступности у нас в стране. Как показывает опыт, сложность применяемых устройств контроля допуска растет. Раньше в России на режимных предприятиях применялись замки с PIN-кодом, затем появились магнитные пластиковые карты, которые необходимо было провести

через специальные устройства считывания, еще позднее – карточки дистанционного считывания. Опыт, в том числе и российский, показывает, что данные средства эффективны только от случайного посетителя и слабы при жестких формах преступности, когда похищаются и пароли входа в информационную систему, и пластиковые карточки, оказывается давление на отдельных сотрудников служб охраны и безопасности.

Уровень современной биометрической защиты весьма высок: он исключает возможность взлома даже в ситуации, когда злоумышленник пытается использовать труп или изъятые органы. Возможность технического взлома базы эталонов или их подмены на этапе идентификации, как правило, исключена: сканер и каналы связи сильно защищены, а компьютер дополнительно изолирован от сети и не имеет даже терминального доступа.

Известная компания Identix, занимающаяся автоматизированным дактилоскопическим оборудованием, прошла регистрацию в 52 странах. Ее серийно выпускаемое оборудование решает следующие идентификационные задачи:

- контроль физического доступа в здание, на стоянки автомашин и в другие помещения;
- контроль компьютерных станций (серверов, рабочих мест) и систем телекоммуникаций;
- контроль доступа к сейфам, складам и т.п.;
- идентификация в электронной коммерции;
- контроль членства в различных организациях и клубах;
- паспортный контроль;
- выдача и контроль виз, лицензий;
- контроль времени посещения;
- контроль транспортных средств;
- идентификация кредитных и смарт-карт.

В таблице сопоставлены характеристики промышленных биометрических систем контроля доступа.

Характеристики промышленных биометрических систем контроля доступа

Модель	Принцип действия	Вероятность допуска “чужого”, %	Вероятность ложного задержания “своего”, %	Время идентификации, с
EyeDentify	Параметры глаза	0,001	0,4	1,5 – 4,0
Iriscan	Параметры зрачка	0,00078	0,00046	2
Identix	Отпечаток пальца	0,0001	1	0,5
StartekBioMet	Отпечаток пальца	0,0001	1	1
Partners Recognition	Геометрия руки	0,1	0,1	1

Ограничителем распространения биометрических средств контроля доступа в ряде стран выступает действующее на их территории законодательство. В России действует закон о персональных данных (*Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»*, введен в действие с 26 января 2007 г.). Подобные законы существуют в других странах, а в некоторых отсутствуют. Статья 11 «Биометрические персональные данные» указанного Закона не содержит исчерпывающего перечня параметров, которые можно отнести к этим данным.

Несомненно, что создание пусть небольших, локальных баз данных, содержащих идентифицирующую гражданина информацию, должно регулироваться законодательно с обязательными мерами ответственности за несанкционированное раскрытие или искажение подобной информации.

Пластиковые карты. Лидером среди переносных носителей персональных идентификационных кодов (PIN) и кодов физического доступа остаются пластиковые карты.

Пластиковая карта представляет собой пластину стандартных размеров (85,6х53,9х0,76 мм), изготовленную из специальной устойчивой к механическим и термическим воздействиям пластмассы. Основная функция пластиковой карты обеспечение идентификации владельца карты как субъекта системы физического доступа или платежной системы.

По принципу действия карты делятся на две группы – пассивные и активные.

*Пассивные карт*ы только хранят информацию на носителе, но не обеспечивают ее автономной обработки. Пример – широко распространенные во всем мире карты с магнитной полосой на обратной стороне. Данный вид карт уязвим для мошенничества, поэтому, например, системы Visa и MasterCard/Europay используют дополнительные средства защиты карт голограммы и нестандартные шрифты для эмбоссирования.

Активные пластиковые карты содержат встроенную микросхему и допускают разную степень обработки информации. Типичный пример – карты-счетчики и карты с памятью. Но они уступают место интеллектуальным или смарт-картам.

Смарт-карты (англ. smart card) – пластиковые карты со встроенной микросхемой (англ. integrated circuit card, ICC – карта с интегрированными электронными цепями). В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления.

Назначение смарт-карт – одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

Смарт-карты находят всё более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов, телефонов стандарта GSM и проездных билетов.

Однако, например, имеются случаи искажения информации, хранимой в смарт-картах, а также нарушения их работоспособности за счет воздействия высокой или низкой температуры, ионизирующих излучений и т.п. Данный вид карт обладает высокой надежностью и вытесняет другие виды карт.

9.4. Программные методы защиты информации

Программная защита информации – система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации. Защитный программный код может выступать как отдельно, в качестве

отдельного защитного программного продукта, так и включаться в состав других, многофункциональных программ, с целью защиты обрабатываемых ими данных или самозащиты от вредоносного кода. Так как защитные функции многофункциональных программ зачастую даже не имеют существенных средств самозащиты и по определению проигрывают специализированному защитному программному обеспечению, любая значимая компьютерная система требует развёртывания и полноценной интеграции программных средств защиты информации на всех или хотя бы самых уязвимых элементах системы.

Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п.

Так, Не следует путать программную защиту информации с защитой компьютеров от несанкционированного использования или защитой сети компьютеров, не смотря на то, что их функции во многом пересекаются. При использовании данного подхода защищается сама информация, будь то операционная система, специализированное программное обеспечение или некий документ в цифровом виде. При этом такая защита подразделяется на защиту данных и защиту программ.

Полноценная программная защита информации на сервере или рабочем компьютере требует использования различных типов защитных программ или специализированных защитных решений, совмещающих в себе несколько типов защиты одновременно.

Например, важно понимать, что господствующий на данный момент антивирусный подход, обычно объединяющий в себе антивирусы, анти-шпионы, анти-эксплуататоры и анти-модификаторы, недостаточен против целевых атак, так как он основан на сравнении программного кода с имеющимися у производителя сигнатурами вредоносного кода. Имеющаяся в некоторых случаях возможность применения поведенческого анализа также не даёт гарантии сохранности данных и сохранения работоспособности системы. Аналогично, контроль доступа сам по себе не способен гарантировать использование программ и данных исключительно имеющими право на это лицами, так как помимо программных уязвимостей такой тип защиты может быть «вскрыт»

обычной социальной инженерией без использования высокотехнологичных способов нападения в принципе. Системы обнаружения вторжений могут помочь при последующем расследовании инцидента, но без систем предотвращения вторжений повреждения, полученные при атаке, могут оказаться слишком серьёзными, чтобы расследование в принципе понадобилось. Шифрование данных может помочь против попыток украсть эти данные, но не остановит злоумышленника, желающего эти данные уничтожить.

Подобные недостатки узкоспециализированной защиты можно найти в любой комбинации малого числа схожих типов программных средств защиты информации, поэтому защита всегда должна быть основана на множестве параллельных и зачастую пересекающихся алгоритмах. При использовании нескольких решений это чревато внутренними конфликтами в системе, поэтому наиболее логичным выводом является использование комплексных защитных систем, использующих большинство упомянутых типов защиты информации для защиты данных, защиты программ и самозащиты от вторжений, копирования, модификации и уничтожения.

Желательно чтобы защитные программные решения обладали модульной структурой и единым управляющим сервером, что может гарантировать возможность полноценной интеграции в ИТ-инфраструктуру предприятия или организации, при этом защищая именно те области системы, которые защищены слабее всего. Кроме этого необходимо, чтобы программные средства были совместимы с уже установленными защитными решениями сторонних производителей, позволяющие, тем самым, исключить стандартную дилемму построения защищённой инфраструктуры о выборе того или иного производителя решений.

Классификация программных средств защиты информации

По ***функциональному назначению*** их можно разделить на следующие группы:

- идентификация технических средств (терминалов, устройств группового управления вводом-выводом ЭВМ, носителей информации), задач и пользователей;

- определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей;

- контроль работы технических средств и пользователей;

- регистрация работы технических средств и пользователей при обработке информации ограниченного использования;

- уничтожения информации в запоминающем устройстве (ЗУ) после использования;

- сигнализации при несанкционированных действиях;

- вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

По ***назначению программного обеспечения*** следует выделить:

- встроенные средства защиты информации. Примером может служить встроенные системы обеспечения безопасности операционных систем-производителей;

- антивирусная программа (антивирус) – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом;

- специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых решений следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.

- межсетевые экраны (также называемые брандмауэрами или файрволами – от нем. Brandmauer, англ. firewall – “противопожарная стена”). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

- proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью – маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы, код Java и JavaScript).

- защищённые сетевые соединения. Примеров может служить технология VPN (Virtual Private Networks – виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec. Создание защищённых сетевых соединений рассмотрено в параграфе 9.9.

Кроме этого программные средства защиты информации делятся на такие типы так:

- контроль доступа;
- анти-кейлоггеры;
- анти-шпионы (anti-spyware);
- анти-эксплуататоры (anti-subversion)
- анти-модификаторы (anti-tampering)
- антивирусы
- шифрование
- брандмауэры (firewall)
- системы обнаружения вторжений
- системы предотвращения вторжений
- песочница.

9.5. Организационные (административные) меры защиты информации

Программно-аппаратные средства защиты обязательно должны дополняться организационными (административными) мерами защиты информации.

Так, административные меры (доля 50 – 60%) включают:

• разработку политики безопасности применительно к конкретной информационной системе (какие профили, какие пароли, какие атрибуты, какие права доступа);

• разработку средств управления безопасностью (кто, когда и в каком порядке изменяет политику безопасности);

• распределение ответственности за безопасность (кто и за что отвечает при нарушении политики безопасности);

• обучение персонала безопасной работе и периодический контроль за деятельностью сотрудников;

• контроль за соблюдением установленной политики безопасности;

• разработку мер безопасности на случай природных или техногенных катастроф и террористических актов.

Ответственность за соблюдением в организации или компании организационных (административных) мер по защите информации лежит на руководителе, начальнике службы безопасности (информационной безопасности), системном (сетевом) администраторе.

Кроме этого, отметим, что без постоянной квалифицированной поддержки со стороны администратора даже надёжная программно-аппаратная защита может давать сбои.

9.6. Понятие вредоносных программ

Вредоносная программа (на жаргоне некоторых специалистов “зловред”, англ. malware – сокращение от malicious software – “злонамеренное программное обеспечение”) – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.

Так, например, почти все антивирусы считают вредоносными программами “кряки” (crack), “кейгены” (keygen) и прочие программы взлома.

Кряк (жарг. от крэк от англ. crack /kræk/) – специальная программа (или файл) для взлома программного обеспечения, как правило, проприетарного. Проприета́рное программное обеспечение (англ. proprietary software; от proprietary - частное, патентованное, в составе собственности и software – программное обеспечение) –

программное обеспечение, являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободного программного обеспечения.

Генератор ключей (жарг. кейген, киген) (от англ. keygen, key generator) – небольшая программа, которая генерирует:

- криптографический ключ для шифрования данных;
- псевдоподлинные CD-ключи или серийные (регистрационные, активационные) номера для регистрации (активирования) программного обеспечения.

Команды, специализирующиеся на взломе программного обеспечения, предлагают их на различных сайтах, посвященных распространению программного обеспечения без соблюдения лицензии.

Сформулированные выше определения вредоносных программ (см. параграф 9.2, 9.6) не отражены законодательством Российской Федерации. В законодательстве Российской Федерации отсутствует определение вредоносных программ. Однако появились программы, действия которых нельзя классифицировать по ст. 272 или 274 УК РФ, но которые мировым сообществом специалистов по информационной безопасности и сотрудниками антивирусных компаний уже отнесены к разряду вредоносных.

Поэтому при классификации вредоносных программ будем исходить из главного классифицирующего признака в Широкой трактовке – нанесения вреда работе пользователя.

Классификация вредоносных программ

Существуют различные классификации вредоносных программ. Например, по способу распространения – почтовые, сетевые и переносимые вместе с носителями. Чаще применяется классификация, основанная на систематизации мест нахождения вредоносных программ, объектов заражения и следов их действия в компьютере, на сервере и прочих устройствах.

1. Черви. Вредоносные программы, которые несанкционированно (т.е. без ведома или без уведомления пользователя) создают свои копии на доступных носителях информации, включая и сетевые диски, постепенно занимая все свободное место. Этим способом они снижают скорость работы компьютера, вплоть до полной неработоспособности операционной

системы. Черви не совершают деструктивных разрушительных действий, не “заражают” другие программы и не проводят изменения хранимой на носителе информации, но могут блокировать работу отдельной программы или компьютера в целом. Лечение от червей сводится к поиску их или частей на носителях информации с последующим их удалением.

2. Вирусы. Вредоносные программы, которые несанкционированно создают свои копии, размещаемые, как правило, в объектах файловой системы. Вирусы заражают эти объекты, внедряя свой машинный код внутрь этих объектов, причем таким образом, чтобы код вируса исполнялся до начала работы зараженного объекта. Вирусы обладают (хотя и не все, но большинство) деструктивными действиями: нарушение работы операционной системы, прикладного программного обеспечения, разрушение файлов, разрушение каталогов, уничтожение файлов и папок, форматирование носителей полностью или частично. Лечение от вирусов сводится к поиску и удалению заранее известного кода вируса внутри объектов файловой системы. После удаления вируса может потребоваться процедура восстановления работоспособности объекта, особенно файла с документом или программного файла. Удаление кода вируса, который способен шифровать код заражаемого объекта, может приводить к невозможности расшифрования и, следовательно, к потере “вылеченным” объектом работоспособности.

Вирусы классифицируют по *местам заражения* и *местам нахождения следов вредоносной деятельности*.

• *Вирусы-спутники* исполняемых файлов с, расширением *.exe. Создается одноименная копия *.com вируса, которая из-за особенностей операционной системы всегда запускается раньше, чем основной *.exe файл.

• *Файловые вирусы.* Поражают все виды двоичных исполняемых файлов, драйверы, объектные модули и системные библиотеки, записывая свое тело внутрь исполняемой программы таким образом, чтобы при запуске зараженной программы первоначально «приступал к работе» вирус.

• *Загрузочные вирусы.* Записывают в загрузочные сектора носителей информации головку вируса, размещая тело (большую часть кода) внутри отдельных файлов или программ, почти как файловые вирусы. Загрузочные сектора носителей читаются всегда

при обращении к носителю, это позволяет активизировать вирус без открытия файла при вызове окна диска, выводе списка файлов, просмотре структуры дерева каталогов.

• *Dir-вирусы* (от слова директорий – каталог). Размещают свою "головку" таким образом, чтобы активизироваться при просмотре зараженного каталога или структуры дерева каталогов.

• *Макровирусы*. Способны проникать и заражать неисполняемые файлы, например файлы с документами и шаблонами, подготовленные с помощью текстового редактора MS Word, табличного процессора MS Excel. Переносятся и копируются вместе с зараженными документами.

Более подробно вирусы рассмотрены в параграфе 9.7.

3. Троянцы. Вредоносные программы, не осуществляющие на зараженном компьютере деструктивных, разрушающих действий и, как правило, проводящие шпионскую работу по сбору информации ограниченного доступа. Обычно, в отличие от других вирусов, не занимаются несанкционированным копированием, а стараются резидентно, т.е. постоянно во время каждого сеанса работы, прописаться в оперативной памяти компьютера и отслеживать оттуда операции по вводу паролей. При наличии подключения компьютера к локальной или глобальной сети троянцы пытаются несанкционированно и незаметно для пользователя переслать перехваченные пароли хозяину, внедрившему его на компьютер.

Лечение от троянцев аналогично лечению от червей, сводится к поиску и удалению файлов с троянской программой.

4. Программы AdWare/SpyWare. Функционально похожи на троянцев, но их интерес не информация ограниченного доступа, а "простое" слежение за работой пользователя. Подобное слежение не наказуемо по российскому законодательству, но приносит ощутимый вред пользователю: сильно замедляет работу компьютера, занимает оперативную и дисковую память, увеличивает интернет-трафик. Лечение схоже с лечением от червей или троянцев, но осложняется скрытностью присутствия программ данного типа и их активным противодействием как лечению, так и удалению.

5. Программы обманщики (Hoax). Еще одна группа не наказуемых по российскому законодательству программ, которые изображают (симулируют) работу легальных программ, сообщая о наличии ошибок в их работе и требуя платы реальными деньгами за

якобы лицензионный ключ для устранения ошибок и лечения. Например, Hoax. Renos подделывает работу антивирусной программы, постоянно сообщая о наличии десятков вредоносных программ даже в лицензионных версиях “Windows”. За лечение от псевдовирусов, создаваемых самим Hoax, естественно, предлагается заплатить.

6. Root Kit. Программы, позволяющие прятать, скрывать другие программы или процессы от операционной системы, файловых менеджеров и антивирусных программ. Лечение от Root Kit программ аналогично лечению от червей, сводится к поиску и удалению файлов. Сложность в том, что Root Kit технология изначально предназначена для сокрытия своих действий и действий других вредоносных программ от операционной системы и для противодействия антивирусным программам. Положение осложняется тем, что программы этого класса могут использоваться для благих целей – скрытному установлению и включению защитных механизмов на конкретном компьютере. Ряд фирм работает над созданием Root Kit программ, подключающих защиту до загрузки собственно операционной системы. А если эти программы подправить так, чтобы они “вздумали” отключить защиту или “включить” ненужные пользователю сервисы? Напомним, что антивирусные программы работают только под управлением операционной системы и лечить “до её загрузки” не могут.

Прочие вредоносные программы представляют собой комбинации вышеперечисленных программ. Современные вредоносные программы практически все относятся именно к гибридным вредоносным программам.

Классификация вредоносных программ по наносимому ущербу

Вредоносные программы по наносимому ущербу делятся на:

Безопасные – программы, которые не причиняют явного вреда операционной системе, файловой системе, носителям информации. К этой группе, как ни покажется странным, относятся почти все современные мошенники – AdWare/SpyWare, Hoax и подобные программы.

Программы, уничтожающие и (или) изменяющие данные на носителях, – практически все вирусные и отдельные троянские

программы. Так, к примеру, такие программы могут зашифровать важную информацию на винчестере (жёстком диске) и потребовать плату за возможность её расшифровки.

Программы, организующие утечку конфиденциальной информации с компьютера, – это, как правило, троянцы.

Программы, взламывающие защиту компьютеров, – это shell-код для изменения уровня доступа до администраторского; backdoor-программы, обеспечивающие скрытное управление работой компьютера; killer-программы (убийцы), активно противодействующие работе антивирусных программ и других защитных механизмов, вплоть до их полного уничтожения.

Основные пути заражения

Когда можно заразиться вредоносными программами?

Это возможно при запуске на компьютере зараженной программы; загрузке операционной системы с зараженного носителя; подключении к системе зараженного драйвера или системной библиотеки; чтении зараженного документа или приложения к незнакомому электронному письму; посещении сомнительного сайта в Интернете; скачивании новой программы, игрушки или их обновления с незнакомого сайта.

9.7. Компьютерные вирусы и средства защиты информации

Компьютерный вирус – это своеобразное явление, возникшее в процессе развития компьютерной техники и информационных технологий. Суть его состоит в том, что программы-вирусы обладают свойствами, присущими живым организмам, – они рождаются, размножаются и умирают. Термин “*компьютерный вирус*” впервые употребил сотрудник Университета Южной Калифорнии Фред Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Этим термином был назван вредоносный фрагмент программного кода. Конечно, это была всего лишь метафора. Фрагмент программного кода похож на настоящий вирус не больше, чем человек на робота. Однако это один из тех редких случаев, когда значение метафоры становилось со временем менее метафорическим и более буквальным.

Компьютерные вирусы способны делать практически то же, что и настоящие вирусы: переходить с одного объекта на другой, изменять способы атаки и мутировать. Проникнув в информационную систему, компьютерный вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае информационная система, пораженная вирусом, окажется под полным контролем злоумышленника. Сегодня компьютерам доверяют решение многих критических задач. Поэтому выход из строя информационной системы может иметь весьма тяжелые последствия, вплоть до человеческих жертв.

Существует много определений компьютерного вируса. Исторически первое определение, как уже отмечалось выше, было дано в 1984 г. Фредом Коэном: "*компьютерный вирус* – это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению".

Таким образом, ***компьютерный вирус*** – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

К концу XX в. в мире насчитывалось более 14 300 модификаций вирусов.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

- способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
- наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Следует отметить, что эти свойства являются необходимыми, но не достаточными. Указанные свойства следует дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

Классификация компьютерных вирусов

На сегодняшний день известны десятки тысяч различных компьютерных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, достаточно ограничено. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы можно разделить на следующие классы:

- по среде обитания;
- операционной системе (ОС);
- особенностям алгоритма работы;
- деструктивным возможностям.

Основной и наиболее распространенной классификацией компьютерных вирусов является ***классификация по среде обитания***, или по типам объектов компьютерной системы, в которые внедряются вирусы (рис. 9.2). По среде обитания компьютерные вирусы можно разделить:

- на файловые (программные);
- загрузочные;
- макровирусы;
- сетевые.

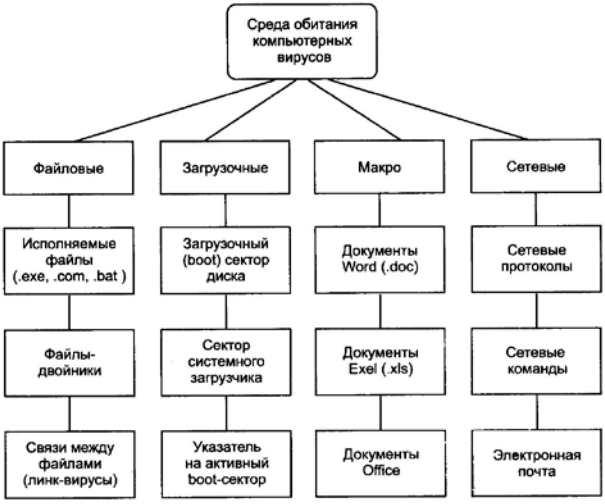


Рис. 9.2. Классификация компьютерных вирусов по среде обитания

Файловые вирусы (программные) либо внедряются в выполняемые файлы (или прикладные программы) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Так, при *"запуске!"* программы, несущей вирус, происходит запуск имплантированного в неё вирусного кода. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ. Вирусный код может воспроизводить себя в теле других программ (*размножение*). По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям: нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется *вирусной атакой*.

Считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение компьютера. Однако бывают случаи, когда аппаратное и программное обеспечение настолько взаимосвязаны, что программные повреждения приходится устранять заменой аппаратных средств (например, при атаке на *BIOS*).

Напомним, что BIOS (англ. basic input/output system – "базовая система ввода-вывода") – реализованная в виде микропрограмм часть системного программного обеспечения, которая предназначается для предоставления операционной системе доступа к аппаратуре компьютера и подключенным к нему устройствам. Так в персональных IBM PC-совместимых компьютерах, BIOS представляет собой набор записанных в микросхему EEPROM (ЭСППЗУ – электрически стираемое перепрограммируемое постоянное запоминающее устройство) персонального компьютера микропрограмм (образующих системное программное обеспечение), обеспечивающих начальную загрузку компьютера и последующий запуск операционной системы.

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в

какой-либо другой сектор диска. Иногда загрузочные вирусы называют бутовыми вирусами.

От программных вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей. Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти. Обычно заражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус.

Макровирусы заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла, если в нём не отключена возможность исполнения макрокоманд, и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения (Microsoft Word, Microsoft Excel и пр.). Как и для других типов вирусов, результат атаки может быть как относительно безобидным, так и разрушительным.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа “червь”. Сетевые черви подразделяются на Internet-черви (распространяются по Internet), LAN-черви (распространяются по локальной сети), IRC-черви Internet Relay Chat (распространяются через чаты).

Существуют много ***комбинированных типов компьютерных вирусов***, например, известен сетевой макро-вирус, который заражает редактируемые документы, а также рассылает свои копии по электронной почте. В качестве другого примера вирусов комбинированного типа можно указать файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы имеют усложненный алгоритм работы и применяют своеобразные методы проникновения в систему.

Другим признаком деления компьютерных вирусов на классы является *операционная система* (ОС), объекты которой подвергаются заражению. Каждый файловый или сетевой вирус

заражает файлы какой-либо одной или нескольких ОС – MS DOS, Windows 95/98, Windows NT/2000 и т. д. Макро-вирусы заражают файлы форматов Microsoft Office (Word, Excel и др.). На определенные форматы расположения системных данных в загрузочных секторах дисков также ориентированы загрузочные вирусы.

Естественно, эти схемы классификации не являются единственно возможными, существуют много различных схем типизации вирусов. Одна из таких классификаций, например, представлена в параграфе 9.6.

Однако ограничимся пока классификацией компьютерных вирусов по среде обитания, поскольку она является базовой, и перейдем к рассмотрению

Средства антивирусной защиты

Существуют три рубежа защиты от компьютерных вирусов:

- предотвращение поступления вирусов;
- предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;
- предотвращение разрушительных последствий, если атака все-таки произошла.

Существуют три метода реализации защиты:

- программные методы защиты;
- аппаратные методы защиты;
- организационные методы защиты.

Основным средством защиты информации является резервное копирование наиболее ценных данных. При этом резервные копии (не менее 2-х копий) должны храниться отдельно от компьютера. Между копиями необходимо осуществлять постоянную *ротацию*. Относительно новым и достаточно надежным приемом хранения ценных, но не конфиденциальных данных является их хранение в Web-папках на удаленных серверах в Интернете.

Вспомогательными средствами защиты информации являются антивирусные программы и средства аппаратной защиты. Так, например, простое отключение перемычки на материнской плате не позволит осуществить стирание BIOS, независимо от того, кто будет пытаться это сделать: компьютерный вирус, злоумышленник или неаккуратный пользователь.

Существует достаточно много программных средств антивирусной защиты. Они предоставляют следующие возможности.

1. *Создание образа жесткого диска на внешних носителях (резервирование, резервное копирование)*. В случае выхода из строя данных в системных областях жесткого диска сохраненный «образ диска» может позволить восстановить если не все данные, то по крайней мере, их большую часть. Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.

2. *Регулярное сканирование жестких дисков в поисках компьютерных вирусов*. Сканирование обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве. При сканировании следует иметь в виду, что антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящимися в базе данных. Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит.

3. *Контроль изменения размеров и других атрибутов файлов*. Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.

4. *Контроль обращений к жесткому диску*. Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, так или иначе обращены на модификацию данных, записанных на жестком диске, антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.

Классификация антивирусных программ по типу действия

1. Сторожа. Не выявляют вредоносных программ и тем более не проводят лечения. Сторожа контролируют выполнение некоторых операций на диске, которые часто используют вредоносные программы, и сообщают пользователю об этих операциях. Перечень операций, какая программа и когда их “заставила” выполняться, записывается в журнал. Проанализировав записи в журнале, пользователь может сделать вывод о

несанкционированности некоторых операций, о возможном воздействии вредоносных программ.

2. Детекторы (сканеры). Программы, содержащие внутри себя или в отдельных подключаемых библиотеках базы данных с цепочками кодов (сигнатурами), присущими ранее выявленным вирусам. Проверяя файлы на наличие таких цепочек, детекторы находят и, вырезая вредоносный код, убивают вирусы. Недостаток детекторов – невозможность обнаружения и лечения новых, незнакомых вирусов, вирусов-невидимок (стелс) и самомодифицирующихся (полиморфных) вирусов. Примерами детекторов служат программы VirusScan, AidTest, V-Hunter, но в настоящее время они не применяются. Детектирующие функции встроены во все современные антивирусные программы.

3. Полиморфные детекторы. Программы, создающие на основе одной сигнатуры полиморфного вируса базу данных, содержащую до миллиона его модификаций, что позволяет обнаружить практически все полиморфные вирусы. Типичный представитель – программа Nod32.

4. Программы-мониторы, или модули многофункциональных программ. Позволяют постоянно за счет размещения в оперативной памяти компьютера контролировать все процессы в реальном времени, в течение всего сеанса работы пользователя. Мониторы входят в состав практически всех современных антивирусных программ.

5. Эвристические доктора. Программы, способные находить группу вирусов по каким-либо общим признакам, даже если они [вирусы] имеют разное внутреннее строение (разные сигнатуры). Типичный общий признак для большинства вирусов – несанкционированное копирование, которое доктора и фиксируют. В сочетании с поиском и удалением известных сигнатур можно найти ранее выявленные вирусы либо заподозрить новый неизвестный вирус. Эвристические подходы используют большинство современных антивирусных программ, лучшими являются отечественные DrWeb, AVP Касперского.

6. На особо опасных участках заражения используются ***карантинные доктора*** *(“виртуальные песочницы”*). Они позволяют вновь прибывшим на компьютер программам работать, но только в отдельной изолированной области памяти. За ними в это время наблюдают программы-доктора. Если в течение

определенного времени “гости” не заявят о себе плохо, то карантин заканчивается и они пускаются в “общую компанию”. В противном случае при подозрении “гости” удаляются с компьютера. Типичные представители карантинных докторов – программы семейства eSafeProtect, AVZ.

7. Проактивная защита. Представляется программами, которые кроме эвристического анализа проводят мониторинг системного реестра, работы приложений с оперативной памятью, контроль целостности наиболее важных системных файлов. Пример – антивирусный пакет AVP Касперского.

Приведем перечень наиболее покупаемых в 2009 г. антивирусных программ:

- Антивирус Касперского;
- ESET NOD32;
- Avast! Professional Edition;
- AVG Anti-Virus Free Edition;
- Avira AntiVir Personal Edition;
- BitDefender Antivirus;
- DrWeb Антивирус;
- F-Prot Antivirus for Windows;
- F-Secure Anti-Virus;
- Norton AntiVirus;
- Panda Antivirus;
- Sophos Norman Virus Control;
- McAffee VirusScan.

Указать лучшую из перечисленных антивирусных программ невозможно по двум причинам.

Во-первых, у каждой программы свой принцип работы и свои “любимые типы” вредоносных программ. Как и для всех болезней человека нет единого лекарства, так и нельзя назвать универсальную антивирусную программу.

Во-вторых, в отличие от вредоносных программ антивирусные программы, к сожалению, несовместимы для одновременной установки на один компьютер и не могут работать одновременно.

По данным тестирования, проведенного многими группами программистов, можно условно определить лучших в отдельных “антивирусных” группах:

- лучший (самый быстрый) сканер – ESET NOD32;
- лучший эвристик – Avira AntiVir Personal Edition или DrWeb;

• лучший проактив – Антивирус Касперского.

Виды антивирусных программ

Различают следующие виды антивирусных программ:
• программы-фаги (сканеры);
• программы-ревизоры (CRC-сканеры);
• программы-блокировщики;
• программы-иммунизаторы.

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги (сканеры, детекторы), как уже отмечали выше, осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и “лечат” их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к “лечению” файлов. Среди фагов выделяют полифаги – программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС.

CRC-сканеры, использующие алгоритмы анти-стелс, являются довольно мощным средством против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их

появления на компьютере. Однако у CRC-сканеров имеется недостаток, заметно снижающий их эффективность: они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их БД отсутствует информация об этих файлах.

К числу CRC-сканеров относится широко распространенная в России программа ADinf (Advanced Diskinfoscope) и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для их восстановления после поражения неизвестными вирусами. В состав ревизора AVP Inspector также входит лечащий модуль, способный удалять вирусы.

Программы-блокировщики реализуют метод антивирусного мониторинга. Антивирусные блокировщики – это резидентные программы, перехватывающие “вирусо-опасные” ситуации и сообщающие об этом пользователю. К “вирусо-опасным” ситуациям относятся вызовы, которые характерны для вирусов в моменты их размножения (вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков или MBR (англ. master boot record – главная загрузочная запись) винчестера, попытки программ остаться резидентно и т. п.).

При попытке какой-либо программы произвести указанные действия блокировщик посылает пользователю сообщение и предлагает запретить соответствующее действие. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что бывает особенно полезно в случаях, когда регулярно появляется давно известный вирус. Однако они не “лечат” файлы и диски. Для уничтожения вирусов требуется применять другие программы, например фаги. К недостаткам блокировщиков можно отнести существование путей обхода их защиты и их “назойливость” (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла).

Следует отметить, что созданы антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера.

Программы-иммунизаторы – это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два гипа:

- иммунизаторы, сообщающие о заражении,
- иммунизаторы, блокирующие заражение каким-либо типом вируса.

Иммунизаторы первого типа обычно записываются в конец файлов и при запуске файла каждый раз проверяют его на изменение. У таких иммунизаторов имеется один серьезный недостаток – они не могут обнаружить заражение стелс-вирусом. Поэтому этот тип иммунизаторов практически не используются в настоящее время.

Иммунизатор второго типа защищает систему от поражения вирусом определенного вида. Он модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, вирус при этом воспринимает их зараженными и поэтому не внедряется. Такой тип иммунизации не может быть универсальним, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако в качестве полумеры подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

9.8. Защита информации в глобальных и локальных сетях

Защита информации, передаваемой по каналам удаленного доступа, требует особого подхода. В мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов – их разделение и передача параллельно по двум линиям, – что делает невозможным “перехват” данных при незаконном подключении “хакера” к одной из линий. Используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки “перехваченных” данных.

В настоящее время разработаны специальные устройства контроля доступа к вычислительным сетям по коммутируемым линиям.

Прямое отношение к теме безопасности имеет стратегия создания резервных копий и восстановления баз данных. Обычно эти операции выполняются в нерабочее время в пакетном режиме.

Рассмотрим основные направления защиты в компьютерных сетях.

Угроза удаленного администрирования

Под удаленным администрированием понимается несанкционированное управление удаленным компьютером. Удаленное администрирование позволяет брать чужой компьютер под свое управление. Это может позволить копировать и модифицировать имеющиеся на нем данные, устанавливать на нем произвольные программы, в том числе и вредоносные, использовать чужой компьютер для совершения преступных действий в Сети «от его имени».

Для эффективной защиты от удаленного администрирования необходимо представлять себе методы, которыми оно достигается. Таких методов два. Первый метод – установить на компьютере “жертвы” программу (аналог сервера), с которой злоумышленник может создать удаленное соединение в то время, когда “жертва” находится в сети. Программы, используемые для этого, называются ***троянскими***. По своим признакам они в значительной степени напоминают компьютерные вирусы. Для защиты от них следует ограничить доступ посторонних лиц к сетевым компьютерам. Доступ закрывается обычными административными способами (физическое ограничение доступа, парольная защита и т. п.).

Второй метод удаленного администрирования основан на использовании уязвимостей (ошибок), имеющихся в программном обеспечении компьютерной системы партнера по связи. Программы, используемые для эксплуатации уязвимостей компьютерных систем, называются ***эксплоитами***. Обычно их атакам подвергаются серверы. Для защиты используются специально выделенные компьютеры или программы, выполняющие функцию ***межсетевых экранов*** (*щитов*). Такие средства также называют ***брандмауэрами*** (*firewall*). Такая программа не позволяет просматривать извне состав программного обеспечения на сервере и не пропускает несанкционированные данные и команды.

Угроза активного содержимого

Активное содержимое – это активные объекты, встроенные в Web-страницы. В отличие от пассивного содержимого (текстов, рисунков, аудиоклипов и т. п.), активные объекты включают в себя не только данные, но и программный код. Агрессивный программный код, попавший на компьютер “жертвы”, способен вести себя как компьютерный вирус или как агентская программа.

Если предположить, что потребитель ни на какие заманчивые предложения сервера не соглашается, то тогда опасными активными объектами и сценариями для него остаются только апплеты Java, элементы ActiveX, сценарии JavaScript и VBScript. Для защиты необходимо оценить угрозу своему компьютеру и, соответственно, настроить браузер так, чтобы опасность была минимальна. Если никакие ценные данные или конфиденциальные сведения на компьютере не хранятся, защиту можно отключить и просматривать Web-страницы в том виде, как предполагал их разработчик. Если угроза нежелательна, прием Java-апплетов, элементов ActiveX и активных сценариев можно отключить. Компромиссный вариант – в каждом конкретном случае запрашивать разрешение на прием того или иного активного объекта.

Угроза перехвата или подмены данных на путях транспортировки

С проникновением Интернета в экономику очень остро встает угроза перехвата или подмены данных на путях транспортировки. Одновременно с потребностью в защите данных возникает потребность в удостоверении (идентификации) партнеров по связи и подтверждении (аутентификации) целостности данных. Методы защиты – криптографические методы.

Кроме того, через Интернет передаются файлы программ. Подмена этих файлов на путях транспортировки может привести к тому, что вместо ожидаемой программы клиент получит ее аналог с «расширенными» свойствами.

Методы защиты – антивирусные программы, организационные мероприятия.

Угроза вмешательства в личную жизнь

В основе этой угрозы лежат коммерческие интересы рекламных организаций. В желании увеличить свои доходы от рекламы множество компаний организуют Web-узлы не столько для того, чтобы предоставлять клиентам сетевые услуги, сколько для того, чтобы собирать о них персональные сведения. Эти сведения обобщаются, классифицируются и поставляются рекламным и маркетинговым службам. Процесс сбора персональной информации автоматизирован, не требует практически никаких затрат и позволяет без ведома клиентов исследовать их предпочтения, вкусы, привязанности.

При посещении почти любых Web-страниц нам на глаза попадаются рекламные объявления (их называют ***баннерами***). При их приеме браузер устанавливает связь с их владельцем (с рекламной системой) и незаметно для пользователя регистрируется в этой системе. Мы можем не обращать внимания на эту рекламу и никогда ею не пользоваться, но, переходя от одной Web-страницы к другой, мы создаем свой психологический портрет (он называется ***профилем***). По характеру посещаемых Web-узлов и Web-страниц удаленная служба способна определить пол, возраст, уровень образования, род занятий, круг интересов, уровень благосостояния и даже характер заболеваний лица, которое никогда к ней не обращалось. Достаточно хотя бы один раз зарегистрироваться где-то под своим именем и фамилией, и ранее собранные абстрактные сведения приобретают вполне конкретный характер – так образуются негласные персональные базы данных на участников работы в сети.

Сопоставляя данные по разным людям или по одним и тем же людям, но полученные в разное время, следящие системы получают профили не только на отдельных лиц, но и на коллективы: семьи, рабочие группы, предприятия. Полученные данные могут использоваться как легально, так и нелегально.

Наиболее простым и очевидным источником для сбора сведений об активности клиентов Интернета являются маркеры ***cookie***. Они используются для регистрации браузера пользователя на сервере.

Маркеры могут быть временными и постоянными. Временный маркер хранится в оперативной памяти до тех пор, пока браузер

работает. По окончании его работы все временные маркеры, полученные от серверов, уничтожаются.

Постоянные маркеры обрабатываются иначе. Когда браузер завершает работу, все постоянные маркеры, накопившиеся в оперативной памяти, переносятся на жесткий диск в виде файлов cookie. Так происходит маркировка жесткого диска, а можно сказать, что не только его, а вообще компьютера клиента. При последующих выходах в Интернет в момент запуска браузера происходит считывание накопившихся маркеров cookie в оперативную память, откуда браузер предъявляет их серверам, которые их поставили.

Физической угрозы маркеры cookie компьютеру не представляют – это файлы данных, которые не являются программным кодом и потому безвредны в смысле несанкционированных действий. Но они представляют угрозу в смысле вмешательства в личную жизнь. Большинство браузеров имеют специальные средства настройки защиты от cookie.

Кроме маркеров cookie источником для сбора сведений о клиентах сети является информация, легально поставляемая браузером. Во время связи по протоколу HTTP браузер сообщает свое название, номер версии, тип операционной системы компьютера клиента и URL-адрес Web-страницы, которую клиент посещал в последний раз.

Кроме этого, у серверов есть приемы, позволяющие в некоторых случаях получить адрес электронной почты клиента, хотя эти приемы используют только негласно и потому правовой режим их сомнителен.

Еще одним источником персональной информации являются так называемые *активные сценарии JavaScript (Java-скрипты)*.

9.9. Создание защищённых сетевых соединений

Выше отмечалась важность парольной защиты для аутентификации пользователя при работе на одном компьютере. Однако большинство пользователей работают не только со своим компьютером, но и используют его в качестве посредника для доступа к другим компьютерам или серверам в сетях. В этом случае возникают две серьезные проблемы.

Пользователь обращается (посылает запрос) определенному серверу. А от кого получает ответ: от запрашиваемого или “чужого” сервера? То есть первая проблема при работе в компьютерной сети – это аутентификация запрашиваемого сервера.

Если пользователь получил ответ от запрашиваемого сервера, то возникает вопрос, с какими правами он будет на нем работать? Это вторая проблема – авторизация пользователя на сервере.

Применение только паролей здесь непригодно, так как их придется пересылать по сети, рискуя “подарить” злоумышленникам.

Технология VPN

Первый способ решения перечисленных сетевых проблем – защита сетевого трафика с использованием виртуальных частных сетей (Virtual Private Networks, VPN). Технология VPN позволяет создать защищенное соединение при незащищенных каналах связи. Подобные соединения часто называют туннелями. В повседневной жизни своеобразные защищенные туннели создают для быстрого и безопасного перемещения на автомобиле важных персон, руководителей государств.

При помощи VPN соединяют между собой и отдельные компьютеры, и отдельные локальные сети. Для создания VPN-туннелей необходимы не только специальные протоколы, специальное программное обеспечение, но и специфическое оборудование шлюз VPN (VPN Gateway), или VPN-сервер. Особенности использования VPN следующие:

• В заголовки пакетов передаваемой информации закладывается однозначный маршрут их передвижения по сети.

• Осуществляется шифрование трафика, т.е. можно скрыть трафик и от интернет-провайдера.

• VPN-шлюз осуществляет подмену вашего IP-адреса (хотя на самом шлюзе ваш IP-адрес должен, естественно, быть зарегистрирован), фактически скрывая ваше присутствие в сети.

• Основой защиты в данной технологии служит ваше доверие хозяевам VPN-шлюза (сервера), знающим ваши истинные параметры и способным расшифровать ваш трафик.

Система Kerberos

Второй и наиболее распространенный в операционных системах способ аутентификации – система Kerberos (Цербер). Аутентификация по Kerberos применяется во многих операционных системах: Windows, MAC OC, некоторых версия Linux.

Работа системы Kerberos строится на следующих принципах:

• Первичную аутентификацию выполняет пароль пользователя при входе в операционную систему (точнее, его хеш или подобное преобразование, но обязательно несущее информацию о текущей дате и времени).

• Система Kerberos включает аутентифицирующий сервер и расположенную там же службу предоставления билетов.

• Все формируемые в системе билеты-сообщения являются временными, т.е. ограничены во времени своего действия.

• Пользователь и система Kerberos четырехкратно обмениваются билетами-сообщениями, содержащими в том числе и "свежие" с учетом текущего времени аутентификаторы самого сервера. Получая назад билеты-сообщения со своими аутентификаторами, которые не может изменить пользователь, сервер убеждается в его подлинности.

Работа системы напоминает обучение студентов в вузе. После успешной сдачи вступительных экзаменов (передача на сервер аутентификаторов) вуз (сервером Kerberos) издает приказ (первый из билетов Kerberos) о зачислении поступающего в ряды студентов. На основании приказа о зачислении обучающийся получает в деканате (аналог службы выдачи билетов) студенческий билет с определенным временем действия, содержащий аутентификаторы вуза (сервера) и студента (пользователя). Используя этот билет, студент может получить дополнительные услуги (на языке информатики – сервисы): входить в корпуса, посещать аудитории, лаборатории, библиотеку, спортзал, клуб и т.д. Но периодически студент должен предъявить деканату (аналог сервера Kerberos) другой билет, им же выданный, – зачетную книжку. Несоответствие записей, несоответствие времени получения записей в этих своеобразных билетах, и студент (пользователь) не получит больше услуг вуза (сервера).

Недостаток системы Kerberos – возможность передачи или раскрытия пароля пользователя другому лицу. В результате это лицо

аутентифицируется на сервере как законный пользователь и будет допущено ко всем ресурсам и сервисам.

Протоколы SSL/TSL

Третий способ обеспечения безопасной передачи информации по сети – применение для аутентификации сервера сертификатов, которые в отличие от ранее рассмотренных билетов выдаются открытым сетевым центром сертификации (например, VerySign), устанавливаются на сервер (вебсервер) и могут автоматически “интегрироваться” в хранилище сертификатов браузера пользователя.

SSL (Secure Socket Layer – протокол защищенных сокетов) и TSL (Transport Layer Security – протокол защиты транспортного уровня) – это криптографические протоколы, обеспечивающие безопасную передачу данных по сети. TSL-протокол – это версия SSL, предназначенная для использования в сети Интернет. Обмен информацией с сервером происходит в несколько этапов.

Обозреватель пользователя направляет серверу запрос на получение интересующей пользователя информации.

Сервер в ответ на запрос посылает свой сертификат с открытым ключом для несимметричного шифрования программе-обозревателю пользователя.

Программа-обозреватель, используя полученный открытый ключ, сверяет полученный сертификат с копией, имеющейся у него. Если проверка прошла успешно, то сертификат сервера считается подлинным.

На компьютере пользователя создается ключ для симметричного шифрования (им будет шифроваться весь трафик, передаваемый от сервера пользователю). Но как его передать на сервер?

Пользователь шифрует по схеме несимметричного шифрования свой созданный ключ с помощью полученного от сервера открытого ключа. Зашифрованный ключ передается на сервер.

Сервер своим закрытым (секретным) ключом расшифровывает полученное сообщение от пользователя, извлекая присланный им ключ для симметричного шифрования.

Теперь оба участника информационного обмена доверяют друг другу и имеют один общий ключ для симметричного шифрования трафика. Дальнейший обмен информацией между ними можно считать защищенным, безопасным.

К особенностям использования SSL относятся следующие:

• Инициатива на установление защищенного SSL-соединения исходит от сервера, а не от пользователя. Не пользователь выбирает это соединение, а соединение изначально уже может быть настроено на SSL-протокол.

• Как правило, с помощью SSL защищается не весь ресурс, а только отдельные веб-страницы, на которых требуется ввести, например, пароль.

• Пользователю для подключения к защищенным страницам не требуется дополнительных устройств или программного обеспечения. Достаточно иметь современную программу-обозреватель, так как она уже “обучена” работе с SSL-соединениями.

• Перед получением защищенной страницы пользователь должен принять от сервера SSL сертификат, после чего сервер передаст клиенту открытый ключ для шифрования передаваемой от пользователя информации. Расшифровку ведет сам сервер, так как только ему известен секретный ключ.

9.10. Контрольные вопросы

1. Основные каналы утечки информации
2. Классификация и краткая характеристика средств защиты информации
3. Характеристика законодательных мер защиты информации
4. Характеристика аппаратных методов защиты информации
5. Классификация программных средств защиты информации
6. Характеристика организационных (административных) меры защиты информации
7. Понятие и классификация вредоносных программ
8. Классификация компьютерных вирусов
9. Характеристика средств антивирусной защиты
10. Характеристика основных направлений защиты в компьютерных сетях
11. Создание защищённых сетевых соединений

ЗАКЛЮЧЕНИЕ

Совершенствование системы управления предприятия в условиях информационной экономики происходит на базе информационных технологий. Цели организации достигаются путём информированности менеджеров организации о продвижении продукции и услуг на рынок, конкуренции, новых технологиях в условиях изменяющейся рыночной ситуации.

Быстрое изменение параметров внешней среды приводит к увеличению объёмов и скорости распространения информации. В связи с этим для успешного ведения бизнеса необходимо сокращать время принятия решений, что неизбежно приводит к увеличению скорости передачи и переработки информации на базе применения новых информационных технологий.

В пособии представлены основные понятия дисциплины, рассматриваются сущность, значение и закономерности развития информационных технологий и систем, приводятся их свойство и классификация, рассматриваются методы обработки информации при принятии управленческих решений. Кроме этого особое внимание в пособии отведено информационным технологиям и системам в экономике и менеджменте, современным корпоративным информационным системам, системам управления базами данных, транзакционным и аналитическим системам, глобальной сети Интернет и сетевым информационным технологиям и информационной безопасности.

Целью учебного пособия является знакомство студентов с основами организации современных информационных технологий и их применение в экономической и управленческой деятельности предприятий, рассмотрение основных принципов построения, внедрения и ведения специализированных информационных систем, создание у студентов целостного представления о процессах формирования информационного общества, а также формирование у студентов знаний и умений в области экономической и компьютерной подготовки, необходимых для успешного применения современных информационных технологий в сфере своей профессиональной деятельности на практике.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гаврилов, М.В. Информатика и информационные технологии [Текст]: учебник для бакалавров / М.В. Гаврилов, В.А. Климов. – 3-е изд., перераб. и доп. – М.: Издательство Юрайт, 2013. – 378 с.

2. Информационные аналитические системы [Текст]: учебник / Т.В. Алексеева, Ю.В. Амириди, В.В. Дик и др.; под. ред. В.В. Дика. – М.: Московский финансово-промышленный университет “Синергия”, 2013. – 384 с.

3. Информационные системы и технологии в экономике и управлении [Текст]: учебник для бакалавров / С.-Петерб. гос. ун-т экономики и финансов; под ред. В.В. Трофимова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2012. – 521 с.

4. Исаев, Г.Н. Информационные системы в экономике [Текст]: учеб. для студентов вузов, обучающихся по специальностям “Финансы и кредит”, “Бухгалт. учет, анализ и аудит” / Г.Н. Исаев. – 5-е изд., стер. – М.: Омега-Л, 2012. – 462 с.

5. Косиненко, Н.С. Информационные системы и технологии в экономике [Текст]: учеб. пособие / Н. С. Косиненко, И. Г. Фризен. – М.: Дашков и К°, 2012. – 303 с.

6. Сибирская, Е.В., Старцева О.А. Электронная коммерция [Текст]: учебное пособие / Е.В. Сибирская, О.А. Старцева. – М.: ФОРУМ, 2010. – 288 с.

7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учеб. пособие / В.Ф. Шаньгин. – М.: ИД “ФОРУМ”: ИНФРА-М, 2014. – 416 с.

ОГЛАВЛЕНИЕ

Учебное издание

Мандрыкин Андрей Владимирович
Шотыло Денис Михайлович

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕНЕДЖМЕНТЕ

В авторской редакции

Подписано к изданию 23.12.2014.

Объем данных 17,5 Мб.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14