**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ**
Государственное образовательное учреждение высшего профессионального образования
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»**

**А.М. Полонский**

# Информационные технологии в сервисе

Учебное пособие

Санкт-Петербург

2007

Приводятся необходимые теоретические сведения по использованию информационных технологий в сервисе. Приводятся основные понятия и определения, архитектура и состав информационных систем, основные аппаратные и программные средства.

Рассмотрены вопросы безопасности информационных систем.

Настоящие методические указания предназначены для студентов, изучающих курсы «Информационный сервис».

# Содержание

1. Понятие информационных технологий и информационного сервиса ..... 4
2. Информационные системы ..... 7
2.1. Классификация и состав информационных систем ..... 7
2.2. Общие представления об ИС, их компонентах и свойствах ..... 8
2.3. Архитектура информационной системы ..... 9
2.3.1. Техническое обеспечение ИС ..... 10
2.3.2. Программное обеспечение ИС ..... 19
2.3.3. Математическое обеспечение ИС ..... 28
2.3.4. Информационное обеспечение ИС ..... 28
2.3.5. Организационное и правовое обеспечение ИС ..... 29
3. Компьютерные сети (локальные, региональные, глобальные) ..... 30
3.1. Классификация и архитектура компьютерных сетей ..... 30
3.2. Уровни модели OSI ..... 33
3.3. Основные протоколы ..... 35
3.4. Адресация в IP-сетях ..... 37
3.5. Протокол Ethernet ..... 42
3.5.1. Проводные сети ..... 42
3.5.2. Беспроводные сети (RadioEthernet) ..... 44
4. Технологии Интернет и Интранет в системах информационного сервиса ..... 49
4.1. Электронная почта (E-Mail) ..... 49
4.2. Служба WWW ..... 52
4.3. Сервис FTP ..... 54
4.4 Интернет - пейджеры ..... 55
4.5. Организация доступа в Интернет корпоративных сетей ..... 57
4.6. Сайты ..... 59
4.6.1. Назначение сайтов в информационных системах ..... 59
4.6.2. Размещение сайтов (web-хостинг) ..... 60
4.6.3. Основные понятия HTML ..... 61
5. Безопасность информационных систем ..... 66
5.1. Общие положения ..... 66
5.2. Базовые угрозы информации ..... 68
5.3. Основные задачи систем защиты информации ..... 69
5.4. Криптографическая защита информации ..... 70
5.4.1. Технология использования криптографических систем ..... 70
5.4.2. Особенности симметричных и асимметричных криптографических систем ..... 72
5.4.3. Распределение открытых ключей и цифровые сертификаты ..... 73
5.4.4. Защищенный документооборот по открытым каналам связи ..... 74
5.4.5. Формирование и проверка цифровой подписи сообщений ..... 74
Библиографический список ..... 78

# 1. Понятие информационных технологий и информационного сервиса

Современное общество характеризуется широким внедрением информационных технологий во все сферы деятельности, как отдельного индивидуума, так и промышленного производства, финансовой деятельности и торговли, государственного управления, здравоохранения, одним словом - общества в целом. Поэтому с полным правом можно утверждать, что в настоящее время завершается переход от индустриального общества к информационному. К информационным технологиям, или как в настоящее время принято говорить - IT[1] относится совокупность методов и средств сбора, хранения, обработки, передачи и ввода/вывода информации. Целью информационных технологий является снижение трудоемкости процессов использования информационных ресурсов, повышение надежности и оперативности выполнения информационных процессов.

**Информация** - (от латинского informatio - разъяснение, изложение), первоначальное понятие - сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т. д.); с середины XX века. общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; одно из основных понятий кибернетики. Законодательно термин «информация» определен следующим образом: «Информация - сведения (сообщения, данные) независимо от формы их представления»[2].

Сегодня, в век информатизации и компьютеризации, информация является таким же ресурсом, как трудовые, материальные и энергетические. **Информация** - ценнейший ресурс наряду с такими традиционными видами ресурсов, как нефть, газ, полезные ископаемые и др., а значит, процесс ее переработки по аналогии с процессами переработки материальных ресурсов можно воспринимать как технологию.

Общеизвестно, что исторически первым носителем человеческих информации, знаний была речь, представлявшая изначально кодированные звуки для координации действий в человеческом сообществе. Затем появилось наскальное письмо каменного века, далее пиктограммы (“иконы”) бронзового века, иероглифическое письмо (сохраненное до сих пор, например, в Китае) и письмо “обычное” - конкатенацией букв алфавита в слоги (“слоговое письмо”) и т.д.

Объединение систем, процессов, связанных с понятиями “информация”, “управление” привело к появлению нового предмета “**кибернетика** (или науки об управлении в живых организмах и автоматах)” (40-ые годы XX века), изучающей информационные процессы в живых организмах и машинах (автоматах). Кибернетика явилась одной из важных предпосылок появления и развития **информатики**. В последнее время, предмет кибернетики понемногу, видимо, “поглощается” предметом информатики. Но при этом информатика не зачеркивает кибернетику, которая теперь может развиваться сильнее, используя результаты, методы и технологии информатики.

Подлинная информационная революция связана, прежде всего, с созданием электронно-вычислительных машин в конце 40-х годов XX века, и с этого же времени исчисляется эра развития информационной технологии, материальное ядро которой образует микроэлектроника. **Микроэлектроника** формирует элементную базу всех современных средств приема, передачи и обработки информации, систем управления и связи. Сама микроэлектроника возникла первоначально именно как технология: в едином кристалли-

[1] от английского термина «Information Technology»

[2] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 г №149-ФЗ; интересно, что предыдущая версия аналогичного закона «Об информации, информатизации и защите информации» (от 20.02995 г. №24-ФЗ) определял понятие информации следующим образом – «Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

ческом устройстве оказалось возможным сформировать все основные элементы электронных схем.

**Документированная информация (документ)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

**Экономическая информация** – (от англ. economic information) - сведения, уменьшающие неопределенность, недостаток знаний, дополняющие представление о социально-экономических процессах, как в сфере производства, так и в непроизводственной сфере на всех уровнях и во всех органах. Экономической информации отображает факты производственно-хозяйственной деятельности с помощью системы натуральных и стоимостных показателей. Экономическая информация, как правило, передается и обрабатывается в форме знаков, фиксируемых на различных вещественных носителях. Экономическую информацию следует отличать от понятия «экономические данные», которые представляют собой отображение экономических явлений, записанных на определенном языке на конкретных материальных носителях (показатели, записанные в документах, текстах или таблицах), но не связанных с определенной задачей или потребителем. Экономические данные только тогда становятся экономическая информация, когда заключенные в них сведения используются для решения определенные задачи и уменьшают неопределенность условий этой задачи.

Как и любая информация, экономическая информация исследуется в трех аспектах: синтаксическом; семантическом; прагматическом.

*Синтаксический анализ* исследует отношения между знаками, представляющими экономическую информацию, отвлекаясь от их содержания и ценности для получателя. Он устанавливает важнейшие параметры информационных потоков, включая количественные характеристики, необходимые для выбора технических средств, осуществляющих сбор, регистрацию, передачу, хранение и переработку экономической информации.

*Семантический анализ* рассматривает содержание экономической информации и способы его языкового представления (язык человека, компьютерные языки), но также не учитывает ее ценность (т.е. фактически рассматривает экономические данные).

*Прагматический анализ* осуществляется для определения полезности экономической информации в процессе ее использования получателем для различных целей и принятия решений, т.е. именно прагматический анализ применяется в тех условиях, когда экономические данные превращаются в экономическую информацию.

Для каждого вида анализа существуют свои количественной оценки и критерии. Наиболее существенными для практического применения являются оценки полезности экономической информации, поскольку они позволяют определить потребительскую ценность поступившей информации с точки зрения возможности ее использования в процессах прогнозирования и управления экономикой. Ценность экономической информации определяется такой совокупностью ее свойств, как своевременность, достоверность, содержательность, удобство восприятия и т.п. Экономическая информация имеет ряд особенностей, облегчающих применение компьютерных методов анализа: большинство экономических показателей измеряется в количественном выражении (стоимость, объем продукции, прибыль и т.п.); цикличность, характерная для большинства производственных и хозяйственных процессов позволяет многократно использовать созданную программу; объемность информационных потоков (детальная информация об экономических процессах позволяет применять математические модели для прогнозирования и управления ими); возможность контроля за достоверностью информации (передача и обработка экономической информации осуществляется лишь на юридически оформленном носителе - документе с подписью, электронном сообщении с электронной цифровой подписью и т.п.).

**Информационные процессы** - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

**Информационная система** - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

**Информационные ресурсы** - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

**Информация о гражданах** (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность[3];

**Конфиденциальная информация** - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

**Средства обеспечения автоматизированных информационных систем и их технологий** - программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

**Собственник** информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

**Владелец** информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом;

**Пользователь** (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

**Информатизация общества** – совокупность научных, социально-экономических и политических факторов, обеспечивающих каждому члену общества к любым источникам информации[4]. Поэтому к основным проблемам формирования информационного общества относится реализация права доступа к информации, защиты персональных данных, прав и свобод личности, идентификации информации, повсеместное использование электронной цифровой подписи.

**Глобализация информационной сферы** – современное общество, его информационные потоки становятся интернациональными и «не знают границ». Можно сказать, что любая информация, созданная в какой-либо стране, может быть практически мгновенно распространена в сети Интернет (причем, совсем не обязательно с помощью средств именно данной страны) и далее – доступна всему миру[5].

**Информационный сервис** представляет собой вид деятельности, направленный на удовлетворение потребностей клиента путем оказания услуг информационного характера.

Информационный сервис обеспечивает познавательную деятельность общества и может быть представлен в виде двух уровней деятельности: эмпирическом (предоставление информации об отдельных фактах и событиях) и теоретическом (анализ информации, выявление закономерностей в данной сфере явлений).

---

[3] Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных» определяет персональные данные следующим образом «персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация»

[4] За исключением доступа к информации, содержащей сведения, составляющие государственную тайну, или к сведениям конфиденциального характера.

[5] Разумеется, только для пользователей сети Интернет.

На эмпирическом уровне информационного сервиса предоставляется информация (справки) о компаниях (местонахождение, телефонах, адресах электронной почты E-Mail. Web-сайта)[6], о наличии товара, предоставлении услуг, расписаниях, событиях политической, культурной жизни, юридическая информация и т.п. Следует выделить в данном уровне сервиса получение клиентом справки (выписки) о состоянии банковского счета и т.п. информации, очевидно, что данная информация является конфиденциальной и может быть предоставлена только владельцу счета или его доверенному лицу[7].

На теоретическом уровне информационного сервиса осуществляется анализ ситуации в экономике (региона, компании и т.п.), изучение общественного мнения, перспектив развития спроса на товары, услуги и т.п.

***Контрольные вопросы***

1. Приведите несколько определений понятия «информации».
2. Что такое информатизация общества и глобализация информационной сферы?
3. Приведите определение экономической информации.
4. Чем экономическая информация отличается от экономических данных?
5. Что такое «конфиденциальная информация»?
6. В каких аспектах исследуется экономическая информация?

# 2. Информационные системы

## 2.1. Классификация и состав информационных систем

Для предоставления услуг в сфере информационного сервиса любого уровня необходимо на первом этапе обладать и уметь управлять необходимой информацией. Данная информация должна содержаться в информационных системах.

**Информационная система**. Под информационной системой (Computer-aided information system) организации следует понимать совокупность организационных, программных и технических средств, использующих автоматизированные информационные технологии для поддержки информационных методов управления, предоставления управленческому персоналу методов и средств работы с информацией для реализации функций управления

**Информационные системы** могут значительно различаться по типам объектов, характером и объемом решаемых задач и рядом других признаков.

Общепринятой классификации информационных систем по настоящее время не существует, поэтому их можно классифицировать по разным признаками, что приводит к существованию нескольких различных классификаций ИС

**Классификация информационных систем**. Информационные системы (ИС) подразделяются на следующие категории:

- *по масштабам применения*:
    - изолированные ИС – информационная система установлена на компьютере, либо не включенном в локальную или иную сеть компании, либо ИС в своей работе не взаимодействует с ресурсами сети;
    - офисные ИС – информационная система установлена в локальной сети офиса, количество компьютеров от 2 до нескольких десятков; ИС использует выделенный сервер (при количестве компьютеров больше 5-10), технологии

[6] В ряде стран допускается свободное получение полной информации о практически о любом гражданине страны, в Российской Федерации предоставление полной информации (в том числе – номера телефона) – запрещено законодательством. (например, ст.53 Федерального закона от 07.07.2003 г. №126-ФЗ «О связи»). Поэтому не покупайте диски с адресными базами, это противозаконно!

[7] Должна быть выполнена процедура авторизации с помощью электронной цифровой подписи, а сама информация (поскольку она передается по открытым каналам связи) должна быть зашифрована.

файл-сервер (при количестве компьютеров-рабочих станций до 20) или «клиент-сервер» (при большем количестве рабочих станций). Данные ИС для связи компьютеров используют технологию локальной сети;
    - ИС предприятий (или корпоративные) – информационная система установлена на предприятии, как правило, размещена в нескольких зданиях, в том числе – расположенных в разных городах, включают в себя локальные ИС. Данные ИС для объединения компьютеров используют собственные выделенные линии связи либо ресурсами Интернет;
    - глобальные ИС – включают в себя корпоративные ИС, размещены нескольких странах (континентах), ля объединения компьютеров используют ресурсы Интернет.
- по функциональному признаку – *производственные, маркетинговые (анализа рынка, рекламные, снабженческие и т.п.), финансовые (бухгалтерские, статистические, и т.п.), кадровые;*
- по квалификации персонала и уровням управления – *стратегические (топ-менеджеров), функциональные (менеджеров среднего звена) и оперативные (специалистов);*
- по характеру обработки информации: *системы обработки данных, системы управления, система поддержки принятия решений;*
- по оперативности обработки данных – *пакетной обработки и оперативные;*
- по степени автоматизации - *ручные, автоматические, автоматизированные;*
- по характеру использования информации - *на информационно-поисковые, информационно-справочные, информационно-решающие, управляющие, советующие и т.п.;*
- по степени централизации обработки информации — *на централизованные, децентрализованные, информационные системы коллективного использования;*
- по характеру использования вычислительных ресурсов – *на локальные и распределенные;*
- по сфере деятельности - *на государственные, территориальные (региональные), отраслевые, объединений, предприятий или учреждений, технологических процессов;*
- по классу реализуемых технологических операций - *на системы с текстовыми редакторами, системы с табличными редакторами, системы управления базами данных (СУБД), системы управления базами знаний (СУБЗ), системы с графикой, мультимедиа, гипертекстом;*
- по месту в процессе управления предприятия – *на автоматизированные рабочие места (АРМ) специалиста, ИС руководителя, ИС внешнего контролера, интегрированные системы, объединяющие в себе часть или все из этих функций;*
- по концепции построения – *файловые, автоматизированные банки данных, банки знаний.*

## 2.2. Общие представления об ИС, их компонентах и свойствах

ИС называется объект информатизации, который с одной стороны рассматривается как единое целое, а с другой - как множество взаимосвязанных и взаимодействующих между собой составных частей.

Понятие ИС охватывает комплекс взаимосвязанных элементов, действующих как единое целое. В систему входят следующие компоненты:

- структура - множество элементов ИС и взаимосвязей между ними;
- входы и выходы - потоки сообщений, поступающие в ИС и выводимые ею;
- закон поведения ИС - функция, связывающая изменения входа и выхода ИС;
- цель и ограничения на функционирование ИС.

Для ИС характерны такие свойства как сложность, делимость, целостность и структурированность.

***Сложность*** определяется множеством входящих в ИС компонентов, изменяющих внутренние и внешние связи и отношения.

***Делимость*** предполагает, что ИС состоит из подсистем, выделенных по определенному признаку и отвечающих конкретным целям и задачам.

***Целостность*** означает, что функционирование множества элементов ИС подчинено единой цели.

***Структурированность*** предполагает распределение элементов ИС по уровням иерархии.

Создание автоматизированных информационных систем (АИС) - сложное и трудоемкое дело, требующее значительной подготовки и организации. Эффективность функционирования разработанной АИС в значительной мере зависит от научно-обоснованных методов ее создания.

**Создание и функционирование ИС** основывается на следующих принципах:

- ***системность.*** Позволяет четко определить цели создания АИС и общие свойства, присущие системе как единому целому; выявляет критерии декомпозиции системы и многообразные типы связей между ее элементами.
- ***модульность.*** Предусматривает построение АИС в виде взаимосвязанных и взаимно дополняемых модулей; причем замена одного модуля другим не нарушает целостность системы.
- ***адаптируемость*** (гибкость). Обеспечивает приспособление системы к новым условиям функционирования при сохранении ее работоспособности.
- ***непрерывность развития*** (открытость). Предопределяет АИС как систему, способную к развитию и совершенствованию при использовании новейших технологий процесса обработки данных.
- ***стандартизация и унификация.*** Для проектирования АИС следует использовать в разумной мере типовые решения.
- ***«новые задачи».*** Предусматривает решение новых задач, которые ранее не рассматривались.
- ***надежность.*** Предполагает устойчивость работы системы в условиях сбоя отдельных ее элементов.
- ***совместимость.*** Заключается в способности взаимодействия различных АИС, имеющих информационное, техническое и технологическое сопряжение.
- ***однократность ввода.*** Предусматривает одноразовый ввод информации и многократное, многоцелевое ее использование.
- ***«дружелюбность».*** Система должна быть простой и доступной для установки, изучения и эксплуатации.
- ***эффективность*** (окупаемость). АИС не должна разорять пользователя и окупаться как материально, так и морально.
- ***автоматизация.*** Предполагает безбумажную технологию, состоящую в комплексном использовании технических средств на всех стадиях технологического процесса обработки информации.
- ***безопасность.*** Это сохранность и целостность конфиденциальной информации в системе.

## 2.3. Архитектура информационной системы

Архитектура ИС определяется моделью автоматизируемых бизнес-процессов (и порождаемых этими процессами информационными потоками), территориальным расположением компонент ИС, а также предполагаемой совокупной стоимостью владения данной

ИС. Именно последним фактором определяется выбор аппаратных средств, программного обеспечения и т.п.

В состав ИС входят следующие компоненты (подсистемы) ( (рис.1):

- техническое (аппаратное) обеспечение;
- математическое обеспечение;
- программное обеспечение;
- информационное обеспечение;
- организационное обеспечение;
- правовое обеспечение.




**СТРУКТУРА ИС КАК СОВОКУПНОСТЬ ОБЕСПЕЧИВАЮЩИХ ПОДСИСТЕМ**

Рисунок 1.

## 2.3.1. Техническое обеспечение ИС

**Техническое обеспечение** ИС включает в себя:

- компьютерное оборудование (рабочие станции и серверы);
- периферийное оборудование (принтеры, сканеры) и средства оргтехника;
- телекоммуникационное и сетевое оборудование:
- устройства бесперебойного питания.

### 2.3.1.1. Компьютерное оборудование

В зависимости от производительности и функционального назначения выделяют суперкомпьютеры, мэйнфреймы, серверы и персональные компьютеры (ПК).

***Суперкомпьютер*** - компьютер, предназначенный для высокоскоростного выполнения прикладных процессов. Поскольку большие скорости обработки данных можно получить лишь в многопроцессорных системах, увеличивается соответственно и число образующих суперкомпьютер процессоров, что позволяет повысить степень параллельности обработки данных. В системах обработки экономической информации суперкомпьютер чаще всего используется в качестве суперсервера - сервера высокой производительности, выполняющего обработку данных для большего числа клиентов.

***Мэйнфреймы*** (mainframe) по производительности уступают суперкомпьютеру, но охватывают более широкий круг решаемых задач. Мэйнфрейм, как правило, выполняет роль главного компьютера в большой информационной сети и принимает на себя основные потоки данных в финансовой сфере и общих бизнес - расчетах. Мэйнфреймы обладают большим объемом памяти, высокой отказоустойчивостью и производительностью[8].

[8] В качестве мэйнфреймов за рубежом традиционно использовались (и используются по настоящее время) компьютеры класса IBM360/370 и аналогичные «большие ЭВМ». В нашей стране в 70-80-е годы XX века выпускались аналогичные ЭВМ – серии ЕС, однако, с началом повального увлечения персональными компьютерами IBM86/286/386 в России и, соответственно, в постсоветском пространстве практически все существующие ЕС ЭВМ были выведены из эксплуатации.

***Персональные компьютеры*** (ПК) являются наиболее массовым средством обработки информации. Персональные компьютеры характеризуются высокой производительностью, небольшими размерами и массовым производством.

Отметим особенности ПК, важные для построения ИС.

В основном настольные компьютеры различаются по производительности, определяемой, при прочих равных, классом и быстродействием центрального процессора, объемом оперативной памяти, характеристиками видеосистемы.

В зависимости от способа использования персональные компьютеры делятся на настольные (desktop) компьютеры и переносные (notebook). В свою очередь, настольные компьютеры, предназначенные для использования в ИС, часто выпускаются в виде «тонкого клиента». Особенностью такого компьютера является его «упрощенность», связанная с тем, что он не предназначен для самостоятельной (автономной) работы, а используется в качестве терминала пользователя ИС. Соответственно, в «тонком клиенте» отсутствует накопитель на жестком магнитном диске «винчестер», а необходимые программы для первоначальной загрузки записаны либо постоянной памяти, либо на перепрограммируемом запоминающем устройстве. При включении этот компьютер автоматически подключается к серверу и может выполнять определенный набор программ, в зависимости от выполняемой задачи (например, ввод текста, работа с таблицами и т.п.). В результате, корпус компьютера уменьшается в размере (за счет отсутствия винчестера, блока питания меньшей мощности). В «тонком клиенте» отсутствуют традиционные вентиляторы блока питания и системы охлаждения процессора, отсутствуют приводы флоппи-дисков и лазерных дисков, в результате корпус компьютера приобретает более «тонкий» вид и может быть установлен в качестве подставки под монитор. При использовании в качестве рабочих станций ИС «тонких клиентов» пользователи лишены возможности запускать какие-либо программы, кроме заранее определенных[9].

Отметим (как это звучит и не парадоксально!), что для компьютеров - рабочих станций ИС не требуется высоких характеристик по быстродействию, объему памяти и т.п. Эти требования существенно выше у домашних компьютеров[10].

Тем не менее, требования к компьютерам-серверам и компьютерам - рабочим станция существенно различаются.

**Компьютеры-серверы**. Имеют принципиальное значение: быстродействие процессора, объем оперативной памяти и дисковой системы, надежность. Не имеют большого значения: характеристики видеосистемы, современный внешний вид[11]. Для серверов используется набор винчестеров, организованных в дисковых массивов в специальный RAID-массив - набор жестких дисков, образующих единое запоминающее устройство. RAID представляет собой устройство, состоящее из недорогих и небольших жестких дисков со своими процессорами, соединенными скоростными каналами. Массив RAID (Redundant Array of Independent Disks - избыточный массив недорогих дисков)[12] представляет собой набор дисков, воспринимаемых пользователем (или операционной системой) как единое целое. Дисковые массивы обладают высокой отказоустойчивостью. Восстановление данных на любом диске, утратившем работоспособность, происходит незаметно для пользователя. Массивы RAID обладают высокой скоростью обмена с оперативной памятью. Для управления ими используются алгоритмы, обеспечивающие чтение и запись данных сразу на нескольких дисках. Главное достоинство RAID - практически стопроцентная гарантия сохранности данных. Благодаря специализированному процессору, источнику питания и вентилятору эти массивы идеальны для внешнего хранения данных.

---

[9] Но не следует предполагать, что «тонкие клиенты» дешевле традиционных ПК в исполнении «desktop».

[10] Или у компьютера в компьютерном клубе (Интернет-кафе)

[11] Компьютеры-серверы часто имеют сугубо промышленное исполнение – для установки в специальные стойки.

[12] Существует также следующая расшифровка аббревиатуры RAID - Array of Independent Disks — избыточный массив независимых дисков.

Для RAID массивов определены ряд уровней (level):

- **RAID уровня 0** - требует минимально трех дисков и обеспечивает наивысшую производительность, но без защиты от потери и/или повреждения данных. Алгоритм работы основан на разделении данных на "полоски" (striping). В том случае, если от дисковой системы требуется наивысшая производительность, но при этом также требуется защита от выхода из строя жестких дисков, устанавливаются два RAID-контроллера зеркально и каждый конфигурируется под уровень 0.
- **RAID уровня 1** - работает только с двумя дисками и фактически делает только зеркализацию (mirroring). Зеркализация не снижает производительность при чтении, но скорость записи снижается существенно, т.к. контроллеру приходиться выполнять запись на два диска, причем сначала на один, затем на другой.
- **RAID уровня 5** - требует минимально трех дисков и обеспечивает как защиту данных от выхода из строя жестких дисков, так и вполне приемлемую производительность. Применяется как striping, так и parity[13]. Избыточность составляет 1 диск в одном массиве. Т.е. при установке 3-х дисков по 9 GB операционная система увидит только 18 GB. Установив 6 дисков по 9 GB, можно использовать для работы 45 GB и т.д.
- **RAID уровня 7** - требует хотя бы одного диска и представляет собой обычное независимое подключение дисков к RAID-контроллеру. Технологии striping, parity в этом случае не используются. Сами диски могут быть отформатированы и разбиты на логические диски в соответствии с требованиями операционной системе. При использовании RAID других уровней это невозможно. Применение RAID-7 фактически представляет собой использование RAID контроллера в качестве обычного, но очень высокопроизводительного SCSI контроллера с кэш-памятью.
- **RAID уровня 0+1** - использует striping от RAID уровня 0 и mirroring от RAID уровня 1. Отличается повышенной, по сравнению с обычным RAID уровня 1, производительностью, хотя избыточность по-прежнему 100%.
- **RAID уровня 10** - та же архитектура, что и в RAID уровня 0+1, но примененная для дискового массива из нескольких групп дисков. Избыточность, соответственно, составляет 100 %.
- **RAID уровня 30** - используется striping, но "полоска" данных распределяется по большим группам дисков с использованием контроля по четности.
- **RAID уровня 50** - то же, что и RAID уровня 30, но с использованием операции XOR[14] для контроля целостности данных.

**Компьютеры-рабочие станции**. Имеют большое значение: быстродействие процессора, объем оперативной памяти и характеристики видеосистемы. Не имеют существенного значения: объем и надежность дисковой системы ввиду того, что все данные сохраняются на серверах, напомним, что в компьютерах – «тонких клиентах» дисковая подсистема отсутствует. Для компьютера – рабочей станции желательно иметь современный внешний вид, соответствующий общему интерьеру рабочего помещения.

#### 2.3.1.2. Периферийное оборудование и оргтехника

Традиционно к периферийному оборудованию относят следующие «внешние» по отношению к ПК устройства ввода-вывода информации: принтеры и сканеры.

***Принтер*** - устройство вывода на бумажный носитель текстовой и графической информации. Наиболее распространены следующие типы принтеров: матричные, струйные и

[13] Технология контроля четности данных.

[14] Бинарная логическая операция, возвращающая значение true тогда и только тогда, когда один из ее операндов true, а другой - false. Эта операция используется отказоустойчивыми томами RAID-5 операционными системами Windows 2000 Server для вычисления избыточных данных. Они позволяют восстанавливать обычные данные, потерянные на неисправном диске или секторе, используя другие диски, входящие в том RAID-5. Аббревиатура XOR образована от eXclusive OR (исключающее или).

лазерные. В данном методическом пособии не рассматриваются принтеры, предназначенные для домашнего использования, так называемого сегмента SOHO[15], хотя для изолированной (локальной) ИС возможно использование оборудование SOHO-сегмента, но для более серьезных ИС следует использовать исключительно профессиональное оборудование.

**Матричные принтеры** являются одними из первых устройств автоматической печати. Устройство матричных принтеров общеизвестно и не требует дополнительных пояснений. Отметим только, что их конструкция включает в себя печатающую головку (каретку), которая двигается вдоль строки и наносит символы ударами иголок по бумаге через специальную красящую ленту. Собственно, матричными такие принтеры называются потому, что все доступные для печати символы являются частью матрицы, образуемой расположением игл (которых может быть 9 или 24). В целом матричные принтеры считались устройствами недорогими и до 1990-х годов были наиболее распространены на рынке устройств печати. Однако с тех пор цены на них оставались примерно неизменными, создавая благоприятный фон для дешевеющих струйных и лазерных принтеров.

Основные недостатки матричных принтеров:

- низкое качество печати — разрешающая способность, как правило, составляет 140 точек/дюйм (dpi),
- высокий уровень акустического шума, создаваемого работой двигателей привода каретки и ударного механизма привода печатающих иголок,
- низкая скорость печати.

Ввиду перечисленных недостатков матричные принтеры уступили место струйным и лазерным принтерам, сохранив за собой лишь довольно узкую специализацию, определяемую их основным принципом работы – ударный (контактный) метод нанесения изображения на бумажный или иной носитель в виде отдельных точек. Матричные принтеры общего назначения используются для печати многослойных документов для бланках строгой отчетности (например, железнодорожных и авиационных билетов), счетов, квитанций и иных документов на типографских бланках. Специализированные матричные принтеры используются для печати чеков, этикеток, наклеек и т.п. Матричные принтеры используются для печати документов в закрытых конвертах – например, PIN-кода для владельца пластиковой банковской карты, SIM-карты мобильного телефона.

Технология матричной печати обеспечивает долговечность отпечатков и экономичность печати (в 5-10 раз дешевле лазерных).

**Струйные принтеры**. Принцип действия принтеров данного класса основан на технологии безударного точечного высокоскоростного нанесения чернильных капель из микроскопических отверстий на твердый носитель (бумагу) для создания требуемого изображения (текста). Струйные принтеры используются для решения двух принципиально различных задач: первая - печати текста и деловой графики и вторая – печати фотографий и тому подобных высококачественных изображений. При этом следует иметь ввиду, что для профессионального вывода текста и деловой графики в офисной практике преимущественно используются лазерные принтеры, в том числе и цветные, а высококачественная распечатка фотографий требует профессиональных струйных принтеров, которые могут позволить себе лишь компании, занимающиеся профессиональным дизайном.

Соответственно – струйные принтеры SOHO-сегмента используются (как следует из названия их сегмента) исключительно в домашней практике для распечатки фотографий с цифровых фотоаппаратов и видеокамер, данные принтеры могут быть использованы и для распечатки текстов небольшого размера, но в офисной практике для распечаток текстов необходимо использовать лазерный принтер. Наиболее распространенные струйные принтеры сегмента SOHO (ценовой диапазон от $70 до $200) не могут использоваться в больших ИС.

[15] SOHO - Small Office and Home Office, т.е. оборудование для малого офиса и дома.

**Лазерные принтеры.** Принцип действия лазерного принтера основан на электрофотографии, заключающейся в том, что специальное красящее вещество (тонер) первоначально (в соответствии с требуемой распечаткой) наносится на электризованный барабан, а затем переносится на бумажный носитель.

Лазерные принтеры следует разделить на две группы: монохромные («черно-белые») и цветные. Цветные лазерные принтеры существенно превышают по стоимости монохромные, но качество получаемых цветных распечаток несколько хуже профессиональных струйных принтеров.

Первоначально лазерные принтеры использовались исключительно в деловой сфере и были практически недоступны для сегмента SOHO. В настоящее время, в связи с упрощением технологии изготовления данных устройств, их стоимость снизилась для приемлемого (для сегмента SOHO) класса и не намного превышает стоимость струйных принтеров. Однако, профессиональные принтеры, т.е. предназначенные для использования в ИС, существенно превышают по стоимости соответствующие «домашние» модели. Ввиду большого количества предложений лазерных принтеров с практически идентичными (на первый взгляд) характеристиками, следует в первую очередь обращать внимание не на скорость и качество печати, а на удобство эксплуатации, их ресурс (допустимое количество копий в месяц)[16], условия гарантии, емкость, взаимозаменяемость и возможность перезаправки картриджей[17].

Профессиональные лазерные принтеры должны иметь следующие дополнительные возможности – «опции»:

- возможность двухсторонней печати;
- дополнительные лотки для бумаги наиболее распространенных форматов (А4, А3) с возможностью автоматического или программного выбора лотка;
- поддержка основных интерфейсов – USB[18], IEEE 1284 (двунаправленный параллельный порт);
- сетевой интерфейс, т.е. возможность подключения принтера к сети (локальной и даже глобальной) по протоколу Ethernet.

Основные фирмы, предлагающие лазерные принтеры как сегмента SOHO, так и профессиональные: Epson, Canon, Hewlett Packard, Xerox, Panasonic, Lexmark, Brother.

**Сканеры.** Для ввода в компьютер изображений используются ***сканеры*** - устройства для переноса рисунка, текста, штрих-кода, обычно с бумажного листа (реже со слайдов), в компьютер для последующего его применения в прикладных программах (например, в графических базах данных, издательских системах, мультимедийных презентациях, системах складского учета) и, при необходимости, редактирования. Сканеры бывают ручны-

---

[16] Ресурс – очень «лукавый» показатель принтера. Представим себе, что принтер имеет заявленный ресурс (нагрузку) 5000 копий в месяц, а скорость печати принтера – 10 листов в минуту. Мы решили распечатать дипломные работы для двух групп студентов, каждый диплом имеет объем 120 листов, в двух группах 40 студентов, получаем – 4800 листов. По времени печать будет продолжаться 480 минут (8 часов). Сказано - сделано! Записали все дипломы на CD, купили 10 пачек бумаги по 500 листов и запустили процесс. Формально мы правы, принтер должен выполнить месячную нагрузку за 1 день (8 часов), а потом пусть отдыхает (оставшиеся 29 дней), дипломы-то у нас уже есть! Но, к сожалению, принтер у нас сломается, напечатав 1-2 диплома, не более. Под ежемесячным ресурсом следует понимать равномерную нагрузку в течение месяца, т.е. 5000 листов за 30 дней, значит – не более 200 листов в день с равномерной загрузкой в течение рабочего дня. Иными словами – печатать периодически по несколько листов. А для одновременной печати такого количества дипломов нужен профессиональный принтер!

[17] Все компании – производители лазерных принтеров по поводу вторичного использования израсходованных картриджей однозначно декларируют, что все картриджи является **одноразовыми** устройствами и не подлежат перезаправке или какой-либо регенерации (восстановлению). Однако, практика показывает, что большинство картриджей можно 1-2 раза перезаправить, а потом еще и восстановить. При этом, разумеется, теряются все гарантии фирмы-изготовителя.

[18] **USB** (Universal Serial Bus) - тип соединения устройств, поддерживаемый многими современными ПК. USB обеспечивает возможность соединения периферийных устройств, таких как принтер, мышь или цифровая камера к ПК

ми и стационарными (планшетными и рулонными), монохромными и цветными. Различаются разрешающей способностью и числом цветов или оттенков серого цвета (для монохромного сканера), скоростью сканирования и размером сканируемой области. Применяются совместно со специальными программами сканирования для графических и текстовых изображений. Программы для сканирования текстов предусматривают преобразование вводимого в компьютер текста в стандартный текстовый файл.

**Копиры** предназначены для создания копий текстовых и графических документов. Копиры подразделяются по принципу действия на аналоговые и цифровые. Аналоговые копиры являются наиболее простыми устройствами и могут быть рекомендованы для использования в сегменте SOHO.

Принцип получения выходного документа в копирах полностью соответствует лазерным принтерам.

В аналоговых копирах изображение на исходном документе экспонируется и через систему линз попадает на фоторецептор (специальный барабан), далее тонер переносится на лист выходного документа. Более совершенные модели аналоговых копиров позволяют выполнять некоторые процедуры с изображением в процессе копирования: изменять масштаб, яркость, контрастность изображения.

Принцип действия цифровых копиров основан на однократном сканировании оригинала и его сохранении в памяти устройства (это может быть оперативная память и/или жесткий диск) в электронном виде. При этом цифровой копир состоит, по существу, из трех функциональных устройств:

- сканера, который осуществляет считывание изображения с документа (оригинала) и преобразование его в графический файл растрового формата;
- специализированного вычислительно-управляющего устройства (контроллера), осуществляющего распечатку необходимого числа копий отсканированного документа на встроенном лазерном принтере и (при необходимости) масштабирование изображения, изменение яркости, контрастности и т.п. по командам оператора;
- встроенного лазерного принтера.

Соответственно цифровые копиры имеют те же характеристики, что и сканеры и принтеры. Качество изображения для монохромных копиров характеризуется количеством уровней полутонов серого цвета и разрешением в точках на дюйм, которое на сегодняшний день для разных аппаратов составляет от 400 до 1800 dpi, что соответствует качеству печати аналогичных по производительности лазерных принтеров. Разрешение различают оптическое ("истинное") и декларируемое, которое часто бывает более высоким за счет использования специальных приемов: ретуши и др. Аналоговые копиры не имеют такой характеристики, как разрешение, а, как правило, приводятся сведения о качестве копий, которое, в свою очередь, зависит от чувствительности фотобарабана и дисперсности тонера, хотя эти параметры есть и в цифровых аппаратах.

Одним из основных и однозначных преимуществ, которые представляет цифровая технология копирования является возможность редактирования копируемого оригинала. К такого рода возможностям следует отнести: масштабирование от 25 % до 400 % и выше (до 200% у аналоговых); всевозможные штампы типа "конфиденциально", "срочно" или логотип компании, наносимые непосредственно на копию; редактирование отдельных участков изображения (удаление, выделение, фоторежим, обведение контуров, копирование с копии, изменение растра); комбинирование до 16 копий оригинала на одном листе; разворот и наклон изображения; раздельное масштабирование по осям в пределах общего масштабирования и др. Набор операций зависит от имеющихся в цифровом копире программ, изображение можно передать в компьютер и там же обработать.

Еще одно достоинство цифровых копиров - однократное сканирование при изготовлении множества копий, что, кроме непосредственного удобства в пользовании, приводит к снижению энергоемкости и повышает надежность аппаратов. Наличие памяти (оперативной и на жестом диске — винчестере) позволяет сохранить отсканированный документ

и произвести многократное копирование (как правило — до 99 копий). Заметим, что в это время можно пользоваться оригиналом, с которого осуществляется копирование.

Среди преимуществ можно также назвать низкую себестоимость копии у цифровых моделей, которая существенно меньше, чем у сопоставимых по классу аналоговых копиров. Цифровые копировальные аппараты могут подключаться к компьютеру и выполнять функции принтера и сканера, что реализовано в многофункциональных устройствах, по качеству печати они вполне сопоставимы с лазерными принтерами среднего класса.

**Многофункциональные устройства**. В последнее время широкое распространение в офисной практике получили многофункциональные устройства (МФУ), выполняющие функции принтера, сканера, цифрового копира и, для некоторых типов устройств – и факсимильного аппарата (факса). Как следует из описания цифровых копиров, в них имеются все необходимые компоненты для создания такого рода устройства: сканер и принтер. Соответственно, дополненный необходимым оборудованием: как правило, сетевой платой, модемом и контроллером с необходимым программным обеспечением, это МФУ может быть использовано в качестве сетевого лазерного принтера, сканера, а также – факса.

### 2.3.1.3. Сетевое оборудование

Сетевое оборудование предназначено для включения компьютеров (рабочих станций и серверов), а в последнее время – и периферийного оборудования (принтеров, сканеров) в компьютерную сеть. Сетевое оборудование подразделяется на:

- активное: сетевые адаптеры, модемы, аппаратные маршрутизаторы, и концентраторы (hub),[19] переключатели (switch)[20];
- пассивное, представляющее собой специальные конструктивы, кабельные системы и т.п.;
- диагностические и инструментальные средства, приборы и оборудование.

**Сетевые адаптеры** (или сетевые платы) предназначены для включения компьютера в локальную сеть по протоколу Ethernet и устанавливаются в системный блок компьютера[21].

**Модемы** (сокращение от терминов модулятор и демодулятор) предназначены подключения организации связи компьютеров и компьютерных сетей на достаточно большое расстояние. Модем в режиме передачи сигнала осуществляет преобразование (модуляцию) дискретных сигналов компьютера в аналоговые сигналы и посылает их в линию связи. В режиме приема сигнала модем осуществляет обратное преобразование - демодуляцию. Модемы по назначению разделяются на группы:

- dial-up-модемы, предназначенные для работы на коммутируемых телефонных линиях, такие модемы чаще всего используются пользователями для организации сеансового подключения к Интернет-провайдерам; данные модемы используются в основном «в домашнем секторе», поскольку не могут обеспечить надежную и быстродействующую связь;

---

[19] Hub - хаб – (концентратор) является обязательным (кроме двухточечной сети) соединительным элементом сети на витой паре и средством расширения топологических, функциональных и скоростных возможностей для любых сред передачи. Простейшие хабы являются многопортовыми повторителями. К порту хаба можно подключить как отдельный узел, так и другой хаб. Хабы с набором разнотипных портов позволяют объединять сегменты сетей с различными кабельными системами. Существуют более сложные и дорогие варианты Switched HUB, Stackable HUB.

[20] Switch – (переключатель) - сетевое устройство, которое выбирает путь для устройств, пакетов, кадров или ячеек при передаче от локального устройства ввода в указанное локальное устройство вывода со скоростью среды (или чуть меньшей скоростью). Коммутаторы обеспечивают возможность организации множества соединений.

[21] В современных сетевых платах сетевой адаптер уже интегрирован в системную плату, также все современные ноутбуки имеют весь набор сетевых устройств.

- ADSL-модемы, используемые для организации доступа в Интернет по телефонным каналам связи, данная технология требует наличия специального оборудования провайдера на АТС клиента;
- xDSL-модемы, используемые для доступа в Интернет и организации связи компьютерных сетей по специальным выделенным каналам связи.

В последнее время стали активно применяться беспроводные сетевые средства, основанные на так называемой технологии Wi-Fi (Wireless Fidelity)[22]. Технологией Wi-Fi называют один из форматов передачи цифровых данных по радиоканалам. Сеть WLAN (Wireless Local Area Network - беспроводная локальная сеть) - вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение - или альтернатива - кабельной локальной сети внутри одного офиса, здания или в пределах определенной территории. Данная технология позволяет экономить средства за счет отсутствия необходимости производить монтаж кабелей. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры.

Беспроводные сети используют радиочастоты, поскольку радиоволны внутри помещения проникают через стены и перекрытия. Диапазон или область охвата большинства систем WLAN достигает 160 м, в зависимости от количества и вида встреченных препятствий. Беспроводные сети обычно более надежны, чем кабельные. Скорость работы сравнима со скоростью кабельной сети. С помощью перекрывающихся точек доступа, настроенных на разные частоты (каналы), беспроводную сеть можно расширить за счет увеличения числа пользователей в одной зоне.

**Переключатели** (switch), **концентраторы** (hub) и **маршрутизаторы** предназначены для организации локальных сетей.

**Пассивное оборудование** включает в себя кабели, кроссовые устройства, розетки, стойки, шкафы и т.п.

**Диагностические средства** включают в себя специальные приборы-тестеры, позволяющие оценить качество кабельных коммуникаций, определить причины основных неисправностей (обрыв, короткое замыкание, влияние помех и т.п.).

К **инструментальным средствам** относятся специальные инструменты разделки кабелей и соединителей.

### 2.3.1.4. Устройства бесперебойного питания

Примерно через три-шесть месяцев работы стоимость данных, хранящихся на новом рабочем компьютере, начинает превышать стоимость самого компьютера. Для сервера сети такая ситуация может возникнуть уже через несколько недель после его установки. Вместе с тем известно, что только 25-50% проблем от общего числа сбоев компьютерных систем возникают из-за программных или аппаратных сбоев. Во всех остальных случаях (а это почти половина) причиной тому является некачественное электроснабжение. Несмотря на то, что современные файловые системы операционных систем весьма устойчивы к несанкционированному завершению работы, нельзя исключать вероятность того, что одна некорректная сессия записи данных на винчестер может разрушить всю файловую систему, операционная система не будет загружаться и, что чревато еще большими последствиями – данные могут быть потеряны.

Выходом из положения является создание высоконадежных систем электропитания, однако небольшие и даже средние компании не могут по финансовым соображениям полностью реконструировать имеющуюся в их здании, офисе систему электроснабжения, на-

[22] В переводе с английского – «беспроводная преданность»

пример, «развязать» компьютерные и все остальные сети, а также установить на компьютерные сети электропитания дополнительные автономные источники[23].

Более простым и экономически целесообразным способом является использование источников бесперебойного питания, которые от которых получают электропитание серверы, рабочие станции и наиболее ответственное периферийное оборудование.

Существуют две технологии создания источников бесперебойного питания (ИБП)[24]: ***On-line*** и ***Off-line***, каждая из которых делится, в свою очередь, на разные модификации.

ИБП, выполненные по технологии ***Off-line***, более дешевы и подразделяются на **резервные** и **линейно-интерактивные**.

В упрощенном виде работу **резервных** ИБП можно представить следующим образом. ИБП, анализируя напряжение в сети, обязаны своевременно запустить свой преобразователь постоянного напряжения аккумуляторной батареи и подать его в нагрузку. Устройства этого класса обеспечивают лишь базовые возможности защиты оборудования при пропадании напряжения в электросети. Коррекция выходного напряжения не производится, поэтому перед принятием решения о применении ***Off-line*** ИБП следует удостовериться в том, что значение входного напряжения в сети находится в допустимых для используемого оборудования пределах.

Принцип работы **линейно-интерактивных** (Line-interactive) ИБП более сложен. Он заключается в том, что измерительное устройство, входящее в состав ИБП, постоянно анализирует параметры входной сети и в случае понижения либо повышения напряжения питания производит регулировку выходного напряжения, стремясь поддержать его в приемлемых рамках без переключения на батарею. При большем отклонении от номинала линейно-интерактивный ИБП действует аналогично резервному. Простейшей реализацией такого регулирующего устройства является трансформатор с переключаемыми отводами. Выполненные по этой технологии ИБП характеризуются высоким КПД (около 98%), а умеренная цена обусловливается минимальным количеством необходимых комплектующих. Кроме того, ИБП данного типа характеризуются высокой надежностью благодаря тому, что батарея работает только в случае необходимости. Технология оптимальна для ИБП малых мощностей, востребованных в SOHO-условиях. Однако следует учесть, что устройства этого класса плохо защищают от "провалов" напряжения, больших "всплесков" в сети, изменений частоты и формы и нестабильно работают в электросетях с "хронически" заниженным (менее 180 В) входным напряжением.

Ряд устройств, выполненных по технологии Line-interactive, при работе от сети автоматически корректируют выходное напряжение, стараясь оставлять его в пределах нормы. Часто данный класс ИБП называют также Off-line + AVR (Automatic Voltage Regulation). Различные модели могут иметь несколько порогов корректировки (до трех шагов в каждую сторону изменения входного напряжения) либо использовать технологию квазинепрерывного слежения за выходным напряжением. Наличие AVR также облегчает задачу поддержания зарядного тока батарей, чем обусловливает меньшее время их восстановления и более длительный срок службы по сравнению с моделями Off-line, такой функции не имеющих.

В ИБП **непрерывного действия** (или ***On-line***), нагрузка запитывается через постоянно действующий конвертор (преобразователь), который, в свою очередь, питается от источника постоянного тока. В нормальных условиях, когда на входе есть переменное напряжение, входное напряжение конвертора снимается с выпрямителя. Когда же в электро-

---

[23] Но это тоже может не помочь! Автор был свидетелем следующей ситуации. Для электропитания компьютеров очень ответственной информационной системы использовали специальное автономное электропитание. Наступила зима с холодами, основная сеть, перегруженная дополнительными нагревателями, стала периодически отключаться, а компьютеры работали. Наиболее сообразительные сотрудники тут же начали включать радиаторы отопления и электрочайники в розетки с обозначением «только для компьютеров». Что за этим последовало? Можете догадаться…

[24] в англоязычной литературе ИБП называется UPS (Uninterruptible Power Supply)

сети происходит отключение либо входное напряжение становится ниже определенного минимального уровня - снимается с аккумуляторов. Таким образом, процесс переключения питания для нагрузки практически незаметен. Большинство устройств класса ***On-line*** выдают напряжение, близкое к синусоидальному в широком диапазоне входных значений. Платой за эти и многие другие преимущества становятся сложность исполнения, высокая стоимость и, как правило, меньший КПД.

### 2.3.2. Программное обеспечение ИС

Программное обеспечение ИС включает в себя:

- системное программное обеспечение;
- прикладные программы:
- офисные пакеты;
- прикладное ПО (предметно-ориентированные пакеты);
- инструментальное ПО (средства программирования и отладки);
- диагностическое ПО, в том числе антивирусные пакеты программ

#### 2.3.2.1. Правила лицензирования программного обеспечения

Приобретение программного продукта - это приобретение лицензии (права) на его использование. Пользователь, приобретая и устанавливая ПО, должен согласиться с **лицензией**[25] – регламентом использования данного программного продукта..

Программное обеспечение защищено от несанкционированного копирования законами об авторских правах. Законы об авторских правах предусматривают сохранение за автором (издателем) программного обеспечения нескольких исключительных прав, одно из которых - право на производство копий программного обеспечения.

Подтверждением лицензионных прав пользователя является **лицензионное соглашение** (licence agreement), либо "Договор на продажу" или "Именной сертификат".

Все программное обеспечение по методам лицензирования подразделяется на две основные группы:

- лицензионное ПО (коммерческое, условно-бесплатное, бесплатное)
- ПО, распространяемое по «открытой» лицензии, т.е. при условии открытого кода (OpenSource) [26]

**Лицензионное ПО** традиционно является наиболее распространенным видом программного обеспечения и подразделяется в свою очередь на **коммерческое**, у**словно-бесплатное** и **бесплатное** ПО.

**Коммерческое ПО**. Данная лицензия (лицензионное соглашение) определяет условия использования программного обеспечения (например, количество компьютеров, на которых может быть установлено данное ПО, ограничения в использовании ПО[27] и т.п.), содержит требования, запрещающие пользователю копировать и распространять дистрибутив ПО, производить действия, направленные на получение исходных кодов программы (деассемблирование) и т.п. Фактически, приобретая программное обеспечение, мы приобретаем не сам программный продукт, а лишь право на его использование.

Данная лицензия может быть подразделена на:

---

[25] от лат. licentia - право, разрешение

[26] Зачастую считается, что программное обеспечение, поставляемое на условиях открытого кода, является нелицензируемым, это принципиально неверно! Это программное обеспечение является бесплатным (на этапе приобретения), но все равно лицензионным.

[27] Например, только для учебных целей или только в органах государственной власти.

- основную - лицензию для использования ПО на сервере или локальном (изолированном) компьютере. Наличие такой лицензии разрешает использовать программное обеспечение одному пользователю;
- дополнительные лицензии - лицензии на подключение к серверному программному обеспечению дополнительных пользователей (больше одного). Стоимостью дополнительных лицензий на программное обеспечение является суммарная стоимость набора компонент, необходимых для автоматизации конкретного рабочего места (АРМ). Также возможно докупать дополнительные лицензии на использование конкретной компоненты системы.

При приобретении дополнительных лицензий определяется, как правило, количество одновременно работающих пользователей Эти пользователи являются не фиксированными, а «плавающими», т.е. если один из пользователей прекращает работу, то другой может подключиться к серверу.

Пользователь коммерческого ПО имеет право на бесплатную техническую поддержку, возможность получения бесплатных обновлений программы (как правило - через Интернет), приобретения последующих версий программы со значительной скидкой и т.п.

**Условно-бесплатное ПО (Shareware)**. Фактически это программное обеспечение, предлагаемое пользователю для подробнейшего пробного использования.

Если программа пользователю понравилась и он посчитает полезной, то по истечению выделенного срока он должен либо ее зарегистрировать (т.е. произвести оплату), либо удалить. В случае регистрации и оплаты программы она трансформируется в коммерческое ПО, и пользователь получает все возможности, предусмотренные лицензией – бесплатную техническую поддержку, возможность получения обновлений и т.п.

Срок пробного использования составляет, как правило, один месяц, некоторые программы ограничены не только по сроку действия, но и по количеству запусков или времени фактического использования. Кроме того, такие Shareware-программы могут при каждом запуске или по окончанию работы напоминать о необходимости последующей регистрации[28]. В ряде случаев Shareware-программы не имеют ограничений по времени работы, но отличаются от полноценной (коммерческой) версии, например, следующим:

- при распечатке документа выводят надписи (в виде водяных знаков или колонтитулов) о том, что документ создан посредством незарегистрированной версии программы;
- отсутствует возможность сохранения результатов работы в виде файла (например, программа распознавания текста FineReader после «отработки» бесплатного периода отказывается сохранить уже распознанный текст, т.е. программа лишь демонстрирует свои возможности);
- выполняются ограниченные функции при работе программы (например, в антивирусной программе DrWeb отсутствует сигнатурный анализ).

Как правило, Shareware-программы «скачиваются» с сайта разработчика данной программы, но до последнего времени оплата Shareware-программ была затруднена формальностями, связанными с переводом денег в адрес разработчика программы и получения необходимых отчетных документов.

В настоящее время Shareware-программы продают Интернет-магазины, специализирующиеся на продаже ПО, например, известный магазин Softkey (www.softkey.ru).

Приобретение Shareware-программы в таком магазине осуществляется следующим образом. Пользователь скачивает Shareware-версию программы, устанавливает ее на свой компьютер и в последующем принимает решение о приобретении программы. На сайте Интернет -магазина пользователь находит ссылку «купить программу», выбирает способ оплаты, которая различается для физических и юридических лиц. Допускается оплата банковским или почтовым переводом, с помощью электронных платежных систем (на-

[28] Ясно, что такие напоминания носят «раздражающий» характер.

пример, Яндекс-Деньги), с помощью международной платежной системы Visa. После оплаты Интернет-магазин обеспечивает покупателя полноценной рабочей версией программы[29] и высылает по почте необходимый пакет отчетных документов (оригинал счета, счет-фактуру и т.п.), что необходимо для бухгалтерии компании для оформления покупки.

**Бесплатное ПО (Freeware).** Данные программы совершенно бесплатны и могут быть использованы без ограничений по количеству одновременно используемых компьютеров, передаче другим пользователям и т.п.[30]. Как правило, это весьма небольшие программы (по функциональному назначению, объему использования), например, простой (но удобный) текстовый редактор, программа сканирования сети и т.п. Многие авторы распространяют с такой лицензией старые версии своих коммерческих программ или так называемые упрощенные (облегченные - Light) версии своих программ. В ряде случаев программы с freeware-лицензией распространяются лишь для частного использования. При запуске бесплатной программы зачастую выводится сообщение о разработчике данной программы, либо данная информация содержится в пункте меню «О программе», что позволяет автору программы рассчитывать на последующие коммерческие заказы и, в любом случае, способствует его популяризации.

ПО, распространяемое при условии открытого кода (OpenSource).

Пользователь, соглашаясь с такой лицензией, получает не только исполняемые файлы программного средства, но и исходные файлы. Вдобавок к этому часто он получает право на модификацию кода по своему усмотрению, хотя условия дальнейшего распространения переработанных программ строго регламентируются прилагающейся к программе лицензией.

Существует несколько видов лицензий на бесплатное программное обеспечение с открытым кодом. И в первую очередь к ним относятся генеральная открытая лицензия GNU (GNU General Public License, GNU GPL или просто GPL), лицензия BSD (Berkley Software Distribution), а также их многочисленные разновидности.

Наиболее распространенной является лицензия GPL, которая разрешает любую модификацию и дальнейшее распространение ПО при условии соблюдения определенных требований, главное из которых - распространение программы вместе с исходным текстом и лицензией GPL. Данные программные продукты нельзя использовать в коммерческих целях.

В отличие от GPL, лицензия BSD такую возможность вполне допускает. Возможно коммерческое распространение программных продуктов, полученных в результате переработки чужого исходного кода. Техническая поддержка ПО, распространяемого с открытым кодом, осуществляется на коммерческой основе.

**Управление лицензиями** предполагает наличие полных сведений об используемом в компании программного обеспечения. Такой подход дает уверенность в том, что каждый используемый элемент аппаратного и программного обеспечения правильно лицензирован, а связанные с этим элементом затраты точно отвечают текущим потребностям компании. Система управления **лицензиями** анализирует, наглядно описывает и упорядочивает все программное обеспечение в компании.

Программное обеспечение компании может устареть или потерять право на поддержку. Имеющиеся программы могут оставаться в бездействии или устанавливаться дважды в нарушение лицензии. Лицензии могут быть утрачены или просрочены, что делает программы потенциальной мишенью для претензий со стороны правообладателей или правоохранительных органов. Все эти факторы могут повлиять на бизнес через высокий уровень издержек, через штрафы за нарушение законов (и связанное с этим ухудше-

[29] Например, высылается лицензионный файл, осуществляется активация программы или покупателю предоставляется ссылка на ftp-сервер магазина для скачивания рабочей версии программы.

[30] Разумеется, остается самое главное ограничение программ, не распространяемых с открытым кодом, - пользователь обязуется не деассемблировать программу и не пытаться ее любым способом модифицировать.

ние деловой репутации), юридические тяжбы, или просто из-за большого объема неэффективной, тяжелой работы.

Система управления лицензиями решает следующие задачи:

- контроль над имеющимися лицензиями;
- оптимизация лицензионной политики компании;
- минимизация совокупной стоимости владения программными продуктами;
- реорганизация программных активов, в том числе выполнение обновлений (первоочередных, перспективных).

#### 2.3.2.2. Системное программное обеспечение

К системному программному обеспечению относятся операционные системы (ОС). Основные функции операционной системы:

- управление ресурсами компьютера или вычислительной системы, в том числе обеспечение многозадачности;
- поддержка файловой системы;
- обеспечение пользовательского интерфейса.

**Классификация ОС**. Операционные системы могут различаться особенностями реализации внутренних алгоритмов управления основными ресурсами компьютера (процессорами, памятью, устройствами), особенностями использованных методов проектирования, типами аппаратных платформ, областями использования и многими другими свойствами. Далее приведем классификацию ОС по нескольким наиболее основным признакам.

**Особенности алгоритмов управления ресурсами.** От эффективности алгоритмов управления локальными ресурсами компьютера во многом зависит эффективность всей сетевой ОС в целом. Поэтому, характеризуя сетевую ОС, часто приводят важнейшие особенности реализации функций ОС по управлению процессорами, памятью, внешними устройствами автономного компьютера. Так, например, в зависимости от особенностей использованного алгоритма управления процессором, операционные системы делят на многозадачные и однозадачные, многопользовательские и однопользовательские, на системы, поддерживающие многонитевую обработку и не поддерживающие ее, на многопроцессорные и однопроцессорные системы.

**Поддержка многозадачности.** По числу одновременно выполняемых задач операционные системы могут быть разделены на два класса:

- однозадачные (например, MS-DOS);
- многозадачные (Microsoft Windows, UNIX).

Однозадачные ОС в основном выполняют функцию предоставления пользователю виртуальной машины, делая более простым и удобным процесс взаимодействия пользователя с компьютером. Однозадачные ОС включают средства управления периферийными устройствами, средства управления файлами, средства общения с пользователем.

Многозадачные ОС, кроме вышеперечисленных функций, управляют разделением совместно используемых ресурсов, таких как процессор, оперативная память, файлы и внешние устройства.

**Поддержка многопользовательского режима.** По числу одновременно работающих пользователей ОС делятся на:

- однопользовательские (MS-DOS, Windows 3.x, Windows 95/98/ME[31]);
- многопользовательские (UNIX, Windows NT4/2000/XP).

Главным отличием многопользовательских систем от однопользовательских является наличие средств защиты информации каждого пользователя от несанкционированного доступа других пользователей. Следует заметить, что не всякая многозадачная система

[31] Часто семейство операционных систем Windows 95, Windows 98 и Windows Millennium обозначают Windows 9*, подчеркивая единое ядро данных операционных систем.

является многопользовательской, и не всякая однопользовательская ОС является однозадачной.

**Вытесняющая и не вытесняющая многозадачность.** Важнейшим разделяемым ресурсом является процессорное время. Способ распределения процессорного времени между несколькими одновременно существующими в системе процессами (или нитями) во многом определяет специфику ОС. Среди множества существующих вариантов реализации многозадачности можно выделить две группы алгоритмов:

- не вытесняющая (кооперативная) многозадачность (NetWare, Microsoft Windows 3.x, Windows 9*);
- вытесняющая многозадачность (Microsoft Windows NT4/2000/XP, OS/2, UNIX).

Основным различием между вытесняющим и невытесняющим вариантами многозадачности является степень централизации механизма планирования процессов. В первом случае механизм планирования процессов целиком сосредоточен в операционной системе, а во втором - распределен между системой и прикладными программами. При невытесняющей многозадачности активный процесс выполняется до тех пор, пока он сам, по собственной инициативе, не отдаст управление операционной системе для того, чтобы та выбрала из очереди другой готовый к выполнению процесс. При вытесняющей многозадачности решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом[32].

В состав операционной системы входят также управляющие программы (драйверы), предназначенные для организации взаимодействия ОС и прикладных программ с аппаратурой ПК и периферийным оборудованием (принтером, сканером и т.п.).

#### 2.3.2.3. Прикладные программы

К прикладному ПО относятся практически все программные средства, которые использует пользователь компьютера и ИС в своей работе. К такого рода ПО, например, относятся:

- офисное программное обеспечение (Microsoft Office, Open Office);
- графические пакеты (для работы с растровой графикой – Adobe Photoshop, векторной – CorelDraw);
- ПО, предназначенное для автоматизации управления предприятием, автоматизации бухгалтерского, складского учета, кадрового менеджмента (Галактика, 1С:Предприятие, Парус и т.д.);

#### 2.3.2.4. Инструментальные программы

К инструментальному ПО относятся инструментальные средства разработки собственных программ (приложений) – языки программирования (C, Pascal и т.д.). Вообще говоря, в средства прикладного программного обеспечения также входят достаточно мощные инструментальные средства. Например, в состав пакета Microsoft Office входит язык программирования Visual Basic, позволяющий создавать собственные макросы, функции и т.п. В состав 1С:Предприятия входит язык программирования, позволяющий осуществлять редактирование имеющихся информационных баз (конфигураций) и создавать новые.

#### 2.3.2.5. Диагностические и антивирусные программы

К **диагностическому ПО** относятся многочисленные программы, предназначенные для проверки работоспособности (диагностики) составных частей компьютера и периферийного оборудования. К основным диагностическим программным средствам следует

[32] Именно поэтому в ОС WindowsNT/2000/XP (в отличие от Widows 9*) всегда можно завершить «зависшее» приложение и, тем самым, избежать зависания всей ОС. Для завершения работы «зависшего» приложения необходимо комбинацией клавиш Ctrl+Alt+Del вызвать **диспетчер задач**, отметить «зависшее» приложение и выбрать команду «снять задачу».

отнести программы для тестирования процессора, оперативной памяти, винчестера, мониторы. Данные программы позволяют определить, во-первых, исправность испытуемых устройств, и, во-вторых, получить их количественные характеристики (например, быстродействие винчестера в определенных режимах).[33]

**Антивирусное ПО**, как следует из названия, призвано бороться с компьютерными вирусами, т.е. распознавать наличие вредоносного кода в файлах программ, почтовых сообщений, файлах Microsoft Office и т.п., а также удалять (деактивировать) этот вредоносный код. Все современные антивирусные программы в своей работе используют две технологии нахождения вредоносного кода (вирусов): сигнатурный и эвристический анализ.

**Классификация вирусов**. Вирусы можно разделить на классы по следующим основным признакам:

- по среде обитания;
- операционной система (ОС);
- особенностям алгоритма работы;
- деструктивным возможностям.

**По среде обитания** разделяют следующие группы вирусов.

**Файловые вирусы** различными способами внедряются в выполняемые файлы (программные файлы), либо создают файлы-двойники (так называемые компаньон-вирусы), а также могут использовать особенности организации файловой системы (link-вирусы).

**Загрузочные вирусы** записываются либо в загрузочный сектор диска или в сектор, содержащий главную загрузочную область винчестера (MBR, Master Boot Record).

**Макро-вирусы** заражают документы Microsoft Office. Все программы данного пакеты (вне зависимости от версий) позволяют создавать и затем эффективно использовать **макросы** – некие элементы программного кода, написанные на языке Visual Basic, позволяющие получить дополнительные возможности документов Microsoft Office, например, в программе Microsoft Word - выполнять автоматическое форматирование текста по определенным правилам, в Microsoft Excel создавать функции пользователя (в дополнение к уже существующим) и т.п. Соответственно, злоумышленник может создать собственный макрос (интегрированный в документ), который одновременно с полезным действием (или вместо него) будет выполнять и деструктивную функцию[34].

**Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Как правило, данные вирусы могут проникнуть в компьютер в качестве файлов, прикрепленной к письму электронной почты, либо в виде скриптов (исполняемой последовательности команд) при просмотре, например, развлекательных сайтов сомнительного содержания. К таким вирусам относятся "электронные черви" вида I-Worm, файлы- «Трояны» и т.п.

Встречаются комбинированные вирусы, например, файлово-загрузочные. Такие вирусы имеют сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого комбинированного вируса - сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

---

[33] Диагностические программы позволяют зачастую определить и локализовать неисправность устройства, результаты этого теста могут служить основанием для предъявления рекламаций к продавцу (изготовителю) устройства. Однако, хочу предупредить, что «увлекаться» излишней диагностикой устройств, особенно содержащих механические движущиеся части (винчестеры) не стоит, поскольку любой тест чрезвычайно серьезно нагружает устройство, в результате чего именно на штатной работе этого устройства его ресурс и завершится!

[34] Во всех документах Microsoft Office уже имеются встроенные макросы, если эти макросы «блокировать» (что могут делать слишком ретивые антивирусные программы), то могут оказаться недоступными ряд привычных (и полезных!) функций программы.

**По заражаемой операционной системе** следует выделить вирусы, которые заражает файлы какой-либо одной или нескольких систем – Windows 9*/ME, Windows NT/2000/XP.[35]

Третий главный признак классификации - **особенности алгоритма работы вирусов**. В данном случае необходимо выделить: резидентность, использование стелс-алгоритмов, самошифрование и полиморфичность, а также использование нестандартных приемов.

**Вирус-резидент** при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Использование **стелс**-алгоритмов[36] позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо предлагают вместо себя незараженные участки информации.

Методы полиморфичности и самошифрования используются практически всеми типами вирусов для того, чтобы максимально осложнить процесс определения вируса. Полиморфик-вирусы (polymorphic) - это вирусы, не содержащие ни одного постоянного участка программного кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию и затруднить лечение от данного вируса.

По **деструктивным возможностя**м вирусы разделяют на следующие группы:

- **безвредные**, т.е. существенно не влияющие на работу компьютера (кроме уменьшения свободной оперативной памяти на места на винчестере в результате своего распространения), данные вирусы являются результатами «тренировки» разработчиков вирусов[37];
- **неопасные** - влияние ограничивается уменьшением свободной оперативной памяти или места на винчестере, а также графическими, звуковыми эффектами; данные вирусы часто называют «раздражающими»;
- **опасные** вирусы, которые могут привести к серьезным сбоям в работе программного обеспечения компьютера. К этому классу можно отнести вирусы, именуемые "Интернет-червями" (всевозможные I-Worm.Hybris и I-Worm.Tanatos);
- **чрезвычайно опасные**, в алгоритм работы, которых заведомо заложены процедуры, способные вызвать уничтожение или модификацию данных, приведение в неработоспособное состояние прикладных программ и операционной системы, а также перепрограммирование микросхем BIOS. Типичный представитель такого рода вирусов - вирус WIN95.CIH ("Чернобыль"). Примером такого рода вирусов также являются I-Worm.Klez (по 13-м числам чётных месяцев червь ищет на всех дисках заражённого компьютера все файлы и заполняет их случайным содержимым, файлы не подлежат восстановлению), а также вирус "I Love You" с аналогичными функциями. Следует выделить вредоносные программы, которые называются "троянскими программами" или просто "троянами".

---

[35] Обратите внимание, что приведены только операционные системы компании Microsoft. Операционная система OS/2 распространена весьма незначительно и в качестве рабочих станций совершенно не используется. Что касается операционной системы Unix/Linux (и их клонов), то отсутствие для такой среды вирусов объясняется двояко – и тем, что эти системы «не восприимчивы» к вирусам, и тем, что Linux **пока** также не слишком часто используется в качестве системы для рабочих станций, следовательно «вирусописателям» **пока** и не стоит стараться. Вирусы пишут только для наиболее распространенных программных продуктов, тем более – появились вирусы для ПО, установленного в мобильные телефоны!

[36] Stealth – невидимка (англ.)

[37] Вообще-то «разработка» - должна быть деятельностью созидательной.

«Трояны» маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Типичные представители - вирусы семейств Backdoor.Nethief и Trojan.Win32. Данные программы выполняют перечисленные деструктивные действия и, кроме того, передают данные с зараженного компьютера по сети Интернет по заложенным в тело этих программ адресам.

Для обнаружения и удаления вирусов используются антивирусные программы[38]. Данные программы, установленные на компьютере, могут работать либо режиме сканера, либо в режиме проверки «на лету».

**В режиме сканера** пользователь самостоятельно запускает процедуру сканирования оперативной памяти и содержимого винчестера компьютера, либо процедура сканирования запускается специальным планировщиком по расписанию, например, в 9 часов по понедельникам. При обнаружении зараженного файла программа выводит соответствующее сообщение пользователю. Дальнейшие действия антивирусной программы определяются настройками пользователя – программа может автоматически попробовать «вылечить» файл, т.е. удалить фрагмент вредоносного кода[39], либо выдать предупреждающее сообщение пользователю, а дальнейшими действиями (например, «лечение» файла, удаление файла) уже будет управлять в ручном режиме человек.

Во время проверки пользователь имеет возможность работать за компьютером, например, вводить текст, однако работа с пользовательскими программами будет несколько замедленна, т.к. часть ресурсов компьютера будет предоставлена антивирусной программе.

**В режиме проверки «на лету»** антивирусная программа размещается в оперативной памяти (как резидентная программа) и просматривает все файлы, которые пользователь запускает, открывает, копирует, пересылает по почте. При обнаружении вируса процедура работы с «подозрительным» файлом приостанавливается и выводится диалоговое окно, в котором пользователь должен произвести выбор (по аналогии со сканером). В данном режиме работа компьютера также может быть замедленной, однако в отличие от периодического сканирования (во время которого можно, например, прервать работу по вводу текста) уменьшение быстродействия будет постоянно[40].

Отсюда следует вывод – для опытных пользователей целесообразно использовать только режим сканирования диска, оставив проверку «на лету» для поступающей почты, а для менее опытных пользователей или компьютеров «общего пользования» - использовать резидентную проверку всех файлов.

Антивирусные программы при проверке выполняют сигнатурный и эвристический анализ всех файлов.

**При сигнатурном анализе** антивирусная программа просматривает файлы и анализирует их содержимое (коды), при обнаружении совпадений фрагментов кодов программ с известными «штаммами» вирусов (сигнатурами) программа считает, что анализируемый файл заражен вирусом. Очевидно, что при сигнатурном анализе антивирусная программа может найти уже известные для разработчиков программы вирусы.

**Эвристический анализ** сводится к тому, что антивирусная программа «просматривает» проверяемый файл и пытается найти в этом файле фрагменты кода (подпрограммы), потенциально способные вызвать деструктивные действия, например – нарушить функции операционной системы, удалить файлы и т.п. при этом антивирусной программе совсем не

---

[38] На компьютере может быть установлена только одна антивирусная программа, одновременно работающие две (и более) антивирусные программы наверняка будут конфликтовать между собой, что приведет к полной неработоспособности ОС.

[39] При этом работоспособность «вылеченной» программы или возможность чтения вылеченного файла - документа не гарантируется.

[40] Разумеется, можно отключить (при необходимости) проверку «на лету», но для этих действий у пользователя должна быть определенная подготовка (и административные полномочия); кроме того, неопытный пользователь, отключив данную проверку и обрадовавшись увеличению быстродействия ПК наверняка забудет ее включить снова.

обязательно знать фрагмент вредоносного кода (сигнатуру), а достаточно лишь анализировать поведение проверяемой программы.

Можно пояснить отличие сигнатурного и эвристического анализа на таком примере. Представьте себе крупный супермаркет, разумеется, с собственной службой безопасности. Сотрудники службы безопасности с помощью системы видеонаблюдения просматривают всех покупателей на входе и, если очередной посетитель входит в список «неблагонадежных» (например, его фотография размещена на стенде «их разыскивает милиция», он находится в розыске, его фотографию или описание, как подозрительного лица, передали коллеги из службы безопасности соседнего супермаркета и т.п.), то, в зависимости от указаний руководства данного супермаркета, посетитель может быть либо просто не допущен в торговый зал, либо за ним может быть организовано более пристальное наблюдение и т.п. Это сигнатурный анализ, т.е. можно выявить уже известные личности, которые где-то «засветились». Представим себе далее, что служба безопасности супермаркета ведет видеонаблюдение в торговом зале и ее привлекает внимание покупатель, который ведет себя несколько странно, например, все время озирается по сторонам, пытаясь найти видеокамеры и понять, находится ли он в их поле зрения или нет, крутится около стендов с малогабаритным, но дорогостоящим товаром, берет дрожащими руками со стенда какой-либо товар, кладет в корзину (а может быть – и в карман), а потом снова возвращает на полку и т.п. Очевидно, несмотря на то, что личность этого покупателя службе безопасности **пока** не известна, на него будет обращено пристальное внимание, все время, пока он находится в торговом зале – это и есть эвристический анализ.

При этом эвристический анализ носит вероятностный характер, т.е. существует определенная вероятность принятия ошибочного решения. Так служба безопасности супермаркета может напрасно остановить рассеянного или вечно спешащего покупателя, а антивирусная программа сообщить, что вполне «добропорядочная» программа является вирусом. В первом случае служба безопасности принесет извинения нашему покупателю[41], а во втором – мы предложим разработчику программы «договориться» с разработчиками основных антивирусных программ о взаимопонимании.

Соответственно, и антивирусная программа должна иметь базу сигнатур и алгоритмы эвристического анализа. Поскольку каждый день создаются новые вирусы, то какую бы совершенную программу мы не купили бы вчера, завтра она нам уже может не помочь. Отсюда следует чрезвычайно важный вывод – антивирусная программа должна постоянно обновляться. Организационно это производится следующим образом – при покупке программы вы покупаете актуальную программу на день покупки[42] и подписку на определенный период (как правило – на год). Программно обновление программы реализовано следующим образом. Антивирусная программа состоит из исполняемого файла, библиотек и антивирусных баз. Подписка представляет собой специальный файл – «ключ», который размещается в папке с программой. В файле-ключе записаны сведения о подписчике, версия программы, срок подписки и (для корпоративного применения) – количество компьютеров. Имея эту подписку можно бесплатно осуществлять обновления программы, удобнее всего – через Интернет. При выполнении обновления программа автоматически связывается с сервером поддержки и начнет скачивать из Интернета необходимые файлы.

Если вы регулярно производите обновления своей антивирусной программы, то вам придется только «докачивать» антивирусные базы, а это не так сложно. Если же купили очень старую версию, или давно не выполняли все обновления, то программа скачает все необходимые файлы, в том числе и исполняемые файлы и библиотеки, а за трафик (а он может составлять 10 Мб и более) или время нахождения в Интернете (несколько часов) нужно будет платить вам!

---

[41] Наш покупатель после этого может быть никогда не пойдет в этот супермаркет, а может быть … будет вести себя в торговом зале более адекватно.

[42] Правда, не совсем понятно, как может быть актуальной программа в «коробочной» версии, которая пару месяцев уже лежала на полке магазина.

В настоящее время наиболее распространены следующие антивирусные программы: DrWeb (разработчик – ООО «Доктор Вэб», автор программы – Игорь Данилов), «Антивирус Касперского» (разработчик – Евгений Касперский), Norton Antivirus (корпорация Symantec), «Панда» и ряд других. Сравнению антивирусных программ посвящены многочисленные статьи, публикации в Интернете, поэтому мы не будем ставить перед собой задачу такого сравнительного анализа. Все хорошие антивирусные программы работают хорошо[43]. При выборе программы нужно уделить особое внимание ее назначению (для рабочих станций или серверов), на режимы, которые программа поддерживает (сканирование дисков, проверка на вирусы «на лету», проверка почты), требования к версии операционной системы и аппаратуре ПК и, разумеется, условиям подписки[44].

В заключении перечислим основные действия, которые позволят избежать заражения компьютера вирусами:

1. Установить антивирусную программу известных производителей последней версии и обновить антивирусные базы по состоянию на текущий день. Установить необходимый режим работы антивирусной программы[45].
2. Произвести обновление операционной системы и входящих приложений: установить последние сервис-паки и «заплатки» от официальных разработчиков[46].
3. Не открывать файлы, прикрепленные к письму от незнакомого адресата – несмотря на последнюю версию имеющейся у нас антивирусной программы и **новые** обновления антивирусных баз в файле-вложении может быть **новейший** вирус.
4. Любой носитель с информацией, флоппи-диск, CD-ROM, флэш-память, с которых нужно переписать файлы, перед началом работы обязательно проверять антивирусной программой.
5. Все файлы, скаченные с Интернета, проверять антивирусной программой.
6. Не заходить на сайты подозрительного содержания, блокировать всплывающие окна.

### 2.3.3. Математическое обеспечение ИС

**Математическое обеспечение** ИС включает в себя совокупность математических методов, моделей и алгоритмов. Средства математического обеспечения – типовые задачи, средства моделирования, методы математического программирования, математической статистики, теории массового обслуживания и др.

### 2.3.4. Информационное обеспечение ИС

**Информационное обеспечение ИС** можно определить как совокупность единой системы классификации, унифицированной системы документации и информационной базы.

**Информационное обеспечение ИС** включает два комплекса: внешнее («внемашинное») информационное обеспечение (классификаторы технико-экономической информации, документы, методические инструктивные материалы) и внутреннее («внутримашинное») информационное обеспечение (макеты/экранные формы для ввода первичных данных в ПК или вывода результатной информации, структуры информационной базы: входных, выходных файлов, базы данных).

К информационному обеспечению предъявляются следующие общие требования:

---

[43] Как говорится «у хорошего кофе должен быть вкус хорошего кофе»!

[44] Очень часто компьютерные фирмы при продаже компьютеров (особенно – ноутбуков) предлагают бонус – бесплатную антивирусную программу. Но при ближайшем рассмотрении оказывается, что эта «бонусная» программа имеет бесплатную подписку всего лишь на 90 дней.

[45] У меня установлен следующий режим – проверка почты «на лету», а сканирование файлов я запускаю при необходимости.

[46] А для этого нужно иметь лицензионное программное обеспечение!

- информационное обеспечение должно быть достаточным для поддержания всех автоматизируемых функций объекта;
- для кодирования информации должны использоваться принятые у заказчика классификаторы;
- для кодирования входной и выходной информации, которая используется на высшем уровне управления, должны быть использованы классификаторы этого уровня;
- должна быть обеспечена совместимость с информационным обеспечением систем, взаимодействующих с разрабатываемой системой;
- формы документов должны отвечать требованиям корпоративных стандартов заказчика (или унифицированной системы документации);
- структура документов и экранных форм должна соответствовать характеристиками терминалов на рабочих местах конечных пользователей;
- графики формирования и содержание информационных сообщений, а также используемые аббревиатуры должны быть общеприняты в этой предметной области и согласованы с заказчиком;
- в ИС должны быть предусмотрены средства контроля входной и результатной информации, обновления данных в информационных массивах, контроля целостности информационной базы, защиты от несанкционированного доступа.

Фактически информационное обеспечение – это «наполнение» имеющихся баз данных в ИС. Представим себе, что создана информационная справочная система для туристической фирмы – типичный пример системы информационного сервиса. Решены вопросы архитектуры ИС, разработаны все необходимые системы управления базами данных, созданы формы заявок и т.п., но пока в эту систему не внесли всю необходимую информацию по континентам, странам, городам, отелям, расписаниям самолетов и поездов – системой пользоваться нельзя! Несмотря на прекрасно разработанное программное обеспечение. Аналогичный пример можно привести и с ИС бухгалтерского учета. Необходимо ввести сведения (заполнить классификаторы) по счетам, банкам и т.п.

### 2.3.5. Организационное и правовое обеспечение ИС

**Организационное обеспечение ИС** - совокупность мероприятий, регламентирующих функционирование и использование технического, программного и информационного обеспечения и определяющих порядок выполнения действий, приводящих к искомому результату.

**Правовое обеспечение ИС** - совокупность норм, выраженных в нормативных актах, устанавливающих и закрепляющих организацию ИС, их цели, задачи, структуру, функции и правовой статус.

В случае, если при обработке и передаче информации в ИС используются алгоритмы шифрования (криптографии), электронно-цифровые подписи (ЭЦП), то данные вопросы должны быть решены в полном соответствии с законодательством.

Фактически именно корректно решенные вопросы организационно-правового обеспечения позволяют реализовать проект создания ИС и обеспечить ее успешную эксплуатацию. Не умаляя значимости технического и программного обеспечения ИС, следует отметить, что большинство «провалов» при внедрении сложных ИС происходило именно в связи с недостаточной продуманностью организации ввода в эксплуатацию и самой эксплуатации системы. В самом деле, разработкой, монтажом и вводом в эксплуатацию ИС занимаются высококвалифицированные специалисты в области информационных технологий, энтузиасты своего дела, а вот кто должен «подхватить» все это сделанное и продолжить? Сотрудники компании (завода, института)[47], которым и так «жилось неплохо» и без этой информационной системы! И первоначально мотивация на использование в своей

[47] Разумеется, они высококвалифицированные специалисты в своей предметной области.

работе нашей ИС у них отсутствует, более того, человек будет искать недостатки (а они всегда есть!) в системе, объясняя, почему ее нельзя использовать и его действия будет лежать в диапазоне от простого саботажа и неграмотной эксплуатации до нанесения прямого вреда[48].

Следовательно, нужно принять весь комплекс организационных мер, позволяющих нам быть уверенными в том, что ИС будет «на ура» воспринята сотрудниками нашей компании. К таким мерам относятся, в первую очередь, разработка инструкций и/или стандартов предприятия, регламентирующих внедрение и эксплуатацию ИС. Очевидно, что эти инструкции должны быть согласованы как с ранее используемыми бизнес-процессами, так и быть безупречными с правовой точки зрения[49]. Скорее всего, возникнет необходимость организовать обучение сотрудников – конечных пользователей ИС. Обучение может быть организовано либо непосредственно на рабочем месте, либо в специализированном учебном центре. Выбор способа обучения неоднозначен - и тот и другой способы имеют достоинства и недостатки, поэтому зачастую используют комбинированный способ – общим навыкам работы с компьютером и стандартным программным обеспечением обучают в учебном центре, а на рабочем месте – непосредственно с внедряемой ИС. Ввиду того, что основную работу с сотрудником никто, как правило, не снимал, следует предусмотреть и стимулирование оплаты труда.

Организационно-правовые меры являются чрезвычайно важными для обеспечения безопасности ИС, в инструкциях должна быть указана ответственность сотрудников при работе с информационными ресурсами, являющимися собственностью компании, правила работы с паролями, сменными носителями информации и т.п.

***Контрольные вопросы***

1. Что входит в техническое обеспечение ИС?
2. Чем требования, предъявляемые к компьютеру-серверу отличаются от требований, предъявляемых к компьютеру-рабочей станции?
3. Назовите принципиальное отличие изолированной ИС от офисной ИС.
4. Приведите классификацию программного обеспечения по назначения.
5. Приведите серверные операционные системы.
6. каковы основные источники «заражения» компьютерными вирусами.
7. Каковы принципы действия антивирусных программ?
8. Что такое лицензирование программного обеспечения? Виды лицензий?
9. Что относится к информационному и математическому обеспечению ИС?
10. Область применения струйного цветного принтера?
11. Приведите тип принтера, с помощью которого следует распечатки большое количество технических документов (количество цветов – до 256)?

# 3. Компьютерные сети (локальные, региональные, глобальные)

## 3.1. Классификация и архитектура компьютерных сетей

**По территориальной распространенности** компьютерные сети подразделяются на следующие классы.

**Локальные сети - LAN (Local Area Network)** - сети, имеющие замкнутую инфраструктуру и не содержащие в своем составе других сетей. Как правило, под термином

[48] Вспомним действия луддитов (англ. Luddites) во времена первой научно-технической революции, луддиты препятствовали автоматизации производств.

[49] Необходимо привлекать к разработке данных инструкций работников кадровых служб, юристов и руководителей выборных профсоюзных органов (там, где они есть).

"LAN" понимается и небольшая офисная сеть офисную сеть и сеть уровня большого завода, занимающего несколько сотен гектаров. Зарубежные источники дают даже близкую оценку - около шести миль (10 км) в радиусе; использование высокоскоростных каналов.

**Региональные сети** (MAN - Metropolitan Area Network) - связывают абонентов, расположенных на значительном расстоянии друг от друга. Сеть может включать абонентов внутри большого города, экономического региона, отдельной страны. Под абонентами следует понимать как отдельные компьютеры, так и локальные сети. Обычно расстояние между абонентами региональной вычислительной сети составляет десятки - сотни километров

**Глобальные сети - WAN (Wide Area Network)** - глобальные сети, покрывающие большие географические регионы, включающие в себя как локальные сети, так и прочие телекоммуникационные сети и устройства.

Термин "**корпоративная сеть**" также используется в литературе для обозначения объединения нескольких сетей, каждая из которых может быть построена на различных технических, программных и информационных принципах.

**По принадлежности** различают ведомственные и государственные сети. **Ведомственные сети** принадлежат одной организации (ведомству, компании) например, сеть какого-либо национального банка, сеть Российских Железных Дорог и т.п.

**Государственные сети** - сети, используемые в государственных структурах (Вооруженных силах, правоохранительных органах и т.п.).

**По скорости передачи информации** компьютерные сети делятся на низко-, средне- и высокоскоростные.

- низкоскоростные (до 10 Мбит/с),
- среднескоростные (до 100 Мбит/с),
- высокоскоростные (свыше 100 Мбит/с);

**По типу среды передачи** сети разделяются на:

- **проводные** (коаксиальные, на витой паре, оптоволоконные);
- **беспроводные** с передачей информации по радиоканалам, в инфракрасном диапазоне.

**Топологии компьютерных сетей**

Способ соединения компьютеров в сети называется ее **топологией**

**Узел сети** представляет собой компьютер, либо коммутирующее устройство сети.

**Ветвь сети** - это путь, соединяющий два смежных узла.

Узлы сети бывают трёх типов:

- оконечный узел - расположен в конце только одной ветви;
- промежуточный узел - расположен на концах более чем одной ветви;
- смежный узел - такие узлы соединены по крайней мере одним путём, не содержащим никаких других узлов.

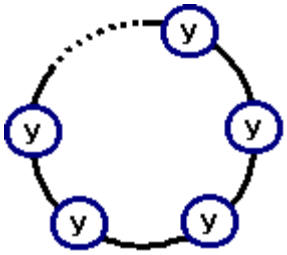
Наиболее распространенные виды топологий сетей:

**Линейная сеть**



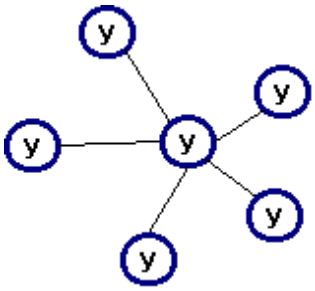

Содержит только два оконечных узла, любое число промежуточных узлов и имеет только один путь между любыми двумя узлами.

**Кольцевая сеть**



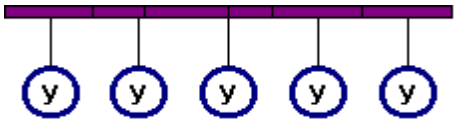
Сеть, в которой к каждому узлу присоединены две и только две ветви.

**Звездообразная сеть**



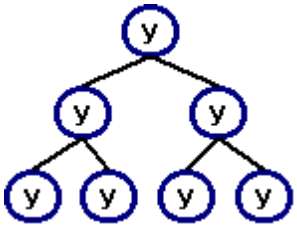
Сеть, в которой имеется только один промежуточный узел.

**Общая шина**



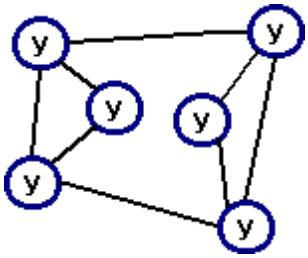
В этом случае подключение и обмен данными производится через общий канал связи, называемый общей шиной.

**Древовидная сеть**



Сеть, которая содержит более двух оконечных узлов и по крайней мере два промежуточных узла, и в которой между двумя узлами имеется только один путь.

**Ячеистая сеть**



Сеть, которая содержит по крайней мере два узла, имеющих два или более пути между ними.

Полносвязная сеть. Сеть, в которой имеется ветвь между любыми двумя узлами.

**Одноранговые и иерархические сети**

С точки зрения организации взаимодействия компьютеров, сети делят на одноранговые (Peer-to-Peer Network) и сети с выделенным сервером (Dedicated Server Network).

**Одноранговые сети**. Все компьютеры (рабочие станции) в одноранговой сети равноправны. Любой пользователь сети может получить доступ к данным, хранящимся на любом компьютере.

Одноранговые сети могут быть организованы также на базе всех современных операционных систем – Windows 9*, Windows NT/2000/XP, Unix/Linux и других.

Достоинством одноранговых сетей является простота в установке и эксплуатации, фактически сеть может быть инсталлирована и успешно эксплуатироваться без привлечения высококвалифицированного специалиста – системного администратора.

Однако в одноранговых сетях чрезвычайно сложно эффективно решать вопросы информационной безопасности и, кроме того, данные сети не являются масштабируемыми, т.е. при необходимости увеличения числа компьютеров проблемы с администрированием сети возрастают многократно.

В связи с этим одноранговые сети используется для сетей с небольшим количеством компьютеров и там, где вопрос защиты данных не является принципиальным.

**Иерархические сети**. В иерархической сети при установке сети заранее выделяются один или несколько компьютеров, осуществляющих регистрацию пользователей, распределением ресурсов и предоставление сервисов. Такие компьютеры называются **серверами**.

Любой компьютер, имеющий доступ к услугам сервера называют клиентом сети или рабочей станцией.

Сервер в иерархических сетях - это постоянное хранилище разделяемых ресурсов. Сам сервер может быть клиентом только сервера более высокого уровня иерархии. Поэтому иерархические сети иногда называются сетями с выделенным сервером.

Серверы обычно представляют собой высокопроизводительные компьютеры, возможно, с несколькими параллельно работающими процессорами, с винчестерами большой емкости, с высокоскоростной сетевой картой.

Иерархическая модель сети является наиболее предпочтительной, так как позволяет создать наиболее устойчивую структуру сети и более рационально распределить ресурсы.

Также достоинством иерархической сети является более высокий уровень защиты данных.

К недостаткам иерархической сети, по сравнению с одноранговыми сетями, относятся:

- Необходимость дополнительной ОС для сервера.
- Более высокая сложность установки и модернизации сети.
- Необходимость выделения отдельного компьютера в качестве сервера

Различают две технологии использования сервера: технологию ***файл-сервера*** и архитектуру ***клиент-сервер***.

В первой модели используется **файловый сервер**, на котором хранится большинство программ и данных. По требованию пользователя ему пересылаются необходимая программа и данные. обработка информации выполняется на рабочей станции.

В системах с архитектурой клиент-сервер обмен данными осуществляется между **приложением-клиентом** (front-end) и **приложением-сервером** (back-end). Хранение данных и их обработка производится на мощном сервере, который выполняет также контроль за доступом к ресурсам и данным. Рабочая станция получает только результаты запроса. Разработчики приложений по обработке информации обычно используют эту технологию.

Использование больших по объему и сложных приложений привело к развитию многоуровневой, в первую очередь трехуровневой архитектуры с размещением данных на отдельном сервере базы данных (БД). Все обращения к базе данных идут через сервер приложений, где они объединяются.

## 3.2. Уровни модели OSI

Взаимодействие всех компонент компьютерной сети (любого уровня сложности) и сетей между собой возможно лишь в том случае, если каждый участник обмена информацией взаимодействует друг с другом в соответствии с принятыми протоколами. Информационные системы являются в этом смысле открытыми, т.е. каждый разработчик (аппаратуры и программного обеспечения) ознакомившись с протоколами может создать свою аппаратуру и ПО, взаимодействующие с остальными компонентами ИС.

В настоящее время общепринятой является семиуровневая модель архитектуры открытых систем (Open System Interconnection), разработанная Международной Организацией по Стандартам (International Organization for Standardization - ISO)

Модель **ISO OSI** предписывает стандартизацию вертикальных межуровневых взаимодействий. Такая стандартизация гарантирует совместимость продуктов, работающих по стандарту какого-либо уровня, с продуктами, работающими по стандартам соседних уровней, даже в том случае, если они выпущены разными производителями. Количество уровней может показаться избыточным, однако же, такое разбиение необходимо для достаточно четкого разделения требуемых функций во избежание излишней сложности и создания структуры, которая может подстраиваться под нужды конкретного пользователя, оставаясь в рамках стандарта

В этой модели рассматриваются так называемые «уровни»:

Уровень 1. Физический уровень (управление физическим каналом).

Уровень 2. Канальный уровень (управление информационным каналом).

Уровень 3. Сетевой уровень (управление сетью).

Уровень 4. Транспортный уровень (управление передачей).

Уровень 5. Сеансовый уровень (управление сеансом).

Уровень 6. Представительный уровень (управление представлением).

Уровень 7. Прикладной уровень (управление сервисом).

Какие же задачи решаются на различных уровнях протоколов открытых систем? Рассмотрим этот вопрос несколько подробнее.

**Физический уровень** отвечает за тип физической среды (например, кабель типа «витая пара» или радиоканал), тип передачи, метод кодирования и скорость передачи данных для различных типов локальных сетей. К его функциям, кроме того, относится установление физического соединения между двумя коммуникационными устройствами, формирование сигнала и обеспечение синхронизации этих устройств.

**Канальный уровень** обрабатывает информацию, поступающую с сетевого уровня, и подготавливает ее к передаче, формируя «кадры» (блоки) соответствующего размера. В процессе перемещения информации вверх по уровням модели OSI канальный уровень должен принимать информацию в виде потока битов, поступающих с физического уровня, и производить ее обработку. Этот уровень обязан определять, где начинается и где заканчивается передаваемый блок, а также обнаруживать ошибки передачи. Если обнаружена ошибка, канальный уровень должен инициировать соответствующие действия по восстановлению потерянных, искаженных и даже дублированных данных.

**Сетевой уровень** осуществляет маршрутизацию передаваемых пакетов. Поскольку в процессе обмена информацией между двумя сетями физические соединения время от времени могут изменяться, сетевой уровень поддерживает виртуальные каналы и обеспечивает правильную сборку пакетов, прибывающих в неправильной последовательности. Работа этого уровня осуществляется с помощью таблиц маршрутизации, которые служат для определения пути продвижения того или иного пакета. Во многих случаях сообщение, состоящее из нескольких пакетов, идет по нескольким путям. Сетевой уровень предоставляет соответствующую «отгрузочную» информацию, необходимую для этих пакетов (например, общее число пакетов в сообщении и порядковый номер каждого из них).

**Транспортный уровень** осуществляет управление передачей пакетов, и именно он определяет качество сервиса, которое необходимо обеспечить посредством сетевого уровня.

**Сеансовый уровень** отвечает за режим передачи и установку точек синхронизации. Иными словами, на этом уровне определяется, какой будет передача между двумя прикладными процессами: полудуплексной (процессы будут передавать и принимать данные по очереди) или дуплексной (процессы будут передавать и принимать данные одновременно). В полудуплексном режиме сеансовый уровень выдает тому процессу, который первым начинает передачу, маркер данных. Когда второму процессу приходит время от-

вечать, маркер данных передается ему. Сеансовый уровень, таким образом, разрешает передачу только той стороне, которая обладает маркером данных.

**Представительский уровень** (или уровень представления данных) отвечает за физическое отображение (представление) информации. Так, в полях базы данных информация должна быть представлена в виде букв и цифр, а зачастую — и графических изображений. Обрабатывать же эти данные нужно, например, как числа с плавающей запятой. Уровень представления данных обеспечивает возможность передачи данных с гарантией, что прикладные процессы, осуществляющие обмен информацией, смогут преодолеть любые синтаксические различия. Для того чтобы обмен имел место, эти два процесса должны использовать общее представление данных или язык.

**Прикладной уровень** обеспечивается программами-приложениями (Web-браузером, клиентом электронной почты и т.п.). В модели OSI прикладная программа, которой нужно выполнить конкретную задачу (например, обновить базу данных на компьютере), посылает конкретные данные на прикладной уровень. Одна из основных «обязанностей» этого уровня — определить, как следует обрабатывать запрос прикладной программы, иными словами — какой вид должен принять данный запрос. Если в запросе прикладной программы определен, например, дистанционный ввод заданий, то это потребует работы нескольких программ, которые будут собирать информацию, организовывать ее, обрабатывать и посылать по соответствующему адресу

## 3.3. Основные протоколы

**Протоколом** называется набор правил и соглашений для передачи данных по сети. Такие правила определяют содержимое, формат, параметры времени, последовательность и проверку ошибок в сообщениях, которыми обмениваются сетевые устройства. В соответствии с рассмотренной семиуровневой моделью OSI каждый протокол (группа протоколов) поддерживают несколько уровней OSI.

На нижних уровнях (уровни 1-3) в компьютерных сетях используются следующие виды протоколов.

**Протокол NetBIOS**. Базовый сетевой протокол сетей компании Microsoft. Как правило, он используется в небольших (охватывающих подразделение предприятия) локальных сетях от 1 до 200 клиентов. Единственным способом маршрутизации, разрешенным при использовании этого протокола, является использование исходной маршрутизации сети Token Ring. Этот протокол является реализацией стандарта NetBIOS. В настоящее время в больших сетях не используется.

**Протокол IPX/SPX**. Протокол IPX (Internet Packet Exchange) был разработан для сетевой операционной системы NetWare и широко используется во многих сетях Novell. PX/SPX - транспортные протоколы, используемые в сетях Novell NetWare, соответствующие протоколам TCP и IP в наборе TCP/IP. Реализация протокола IPX в Windows осуществляется протоколом NWLink. В настоящее время в сетях Microsoft Windows и UNIX не используется.

**Протокол Ethernet**. Основной протокол для построения локальных сетей.

**Протоколы семейства PPP** (Point-to-Point Protocol). Используются для удаленного подключения (через модем) отдельных клиентов и целых сетей.

На следующих уровнях модели OSI используется протоколы семейства TCP/IP.

**Протоколы TCP/IP** - набор широко используемых в Интернете сетевых протоколов, поддерживающий связь между объединенными сетями, состоящими из компьютеров различной архитектуры и с разными операционными системами. Протокол TCP/IP включает в себя стандарты для связи между компьютерами и соглашения о соединении сетей и правилах маршрутизация сообщений. Собственно этот протокол состоит из двух протоколов:

**TCP (Transmission Control Protocol)** – протокол, отвечающий за формирование и отправку пакетов

**IP (Internet Protocol)** – маршрутизируемый протокол семейства TCP/IP, отвечающий за IP-адресацию, маршрутизацию, а также за разбиение на сегменты и повторную сборку пакетов IP.

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем ISO/OSI, то, хотя он также имеет многоуровневую структуру, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Структура протоколов TCP/IP приведена на рисунке 2. Протоколы TCP/IP делятся на 4 уровня.

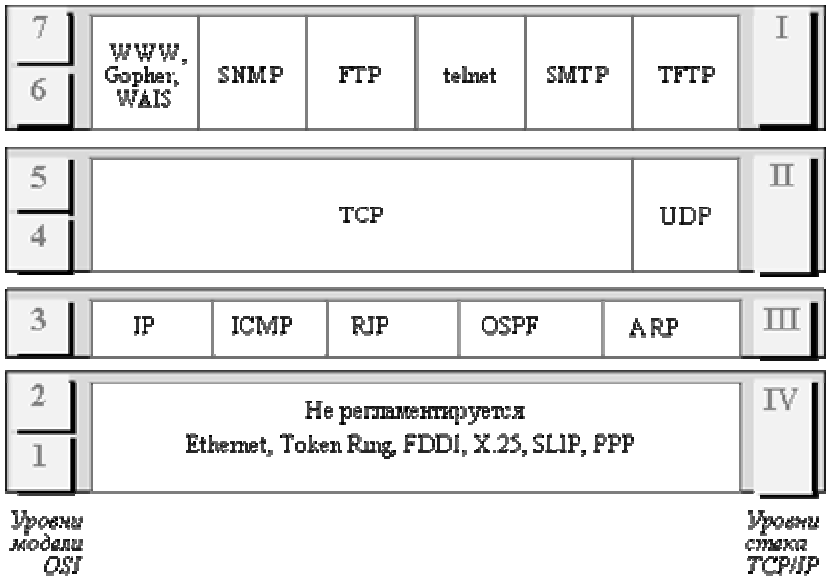



Рис. 2.. Стек TCP/IP

Самый нижний (***уровень IV***) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений "точка-точка" SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня. Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP за счет разработки соответствующего стандарта RFC, определяющего метод инкапсуляции пакетов IP в ее кадры.

Следующий уровень (***уровень III***) - это уровень межсетевого взаимодействия, который занимается передачей пакетов с использованием различных транспортных технологий локальных сетей, территориальных сетей, линий специальной связи и т. п.

В качестве основного протокола сетевого уровня (в терминах модели OSI) в стеке используется протокол **IP**, который изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так и глобальными связями. Поэтому протокол IP хорошо работает в сетях со сложной топологией, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Протокол IP является дейтаграммным протоколом, то есть он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся и все протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации **RIP** (Routing Internet Protocol) и **OSPF** (Open Shortest Path First), а также протокол межсетевых управляющих сообщений **ICMP** (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между

маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов ICMP сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т.п.

Следующий уровень (***уровень II***) называется основным. На этом уровне функционируют протокол управления передачей **TCP** (Transmission Control Protocol) и протокол дейтаграмм пользователя **UDP** (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и IP, и выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

Верхний уровень (***уровень I***) называется прикладным. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество протоколов и сервисов прикладного уровня. К ним относятся такие широко используемые протоколы, как протокол копирования файлов **FTP**, протокол эмуляции терминала **telnet**, почтовые протоколы **SMTP** и **POP3**, используемые в электронной почте, гипертекстовые сервисы доступа к удаленной информации, такие как WWW и многие другие.

Протокол пересылки файлов **FTP** (File Transfer Protocol) реализует удаленный доступ к файлу. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Кроме пересылки файлов протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде, чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов Internet парольная аутентификация не требуется, и ее обходят за счет использования для такого доступа предопределенного имени пользователя Anonymous.

**HTTP** (Hyper Text Transfer Protocol) – протокол передачи гипертекста, используется для передачи данных через Интернет. Один из компьютеров является сервером, на этом компьютере должна работать программа – web-сервер, а второй – клиентом с программой – браузером. Существует разновидность данного протокола – HTTPS, используется для связи с web-сервером по защищенному каналу, например, при осуществлении платежей через Интернет.

Протокол **telnet** обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Поэтому серверы telnet всегда используют как минимум аутентификацию по паролю, а иногда и более мощные средства защиты, например, систему Kerberos.

## 3.4. Адресация в IP-сетях

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней:

- MAC-адрес сетевого адаптера или порта маршрутизатора;
- IP-адрес;
- символьное имя.

### MAC-адрес

**MAC-адрес** для всех существующих технологий построения локальных сетей имеет формат 6 байтов, например: 00-17-9A-51-BF-D0. Старшие 3 байта являются идентифика-

тором фирмы-производителя[50], младшие – назначаются самим производителем. Теоретически, двух совпадающих MAC-адресов сетевых устройств быть не должно, однако ряд современных сетевых устройств допускают их переназначение.

**IP-адрес** — это логический 32-разрядный адрес, однозначно определяющий узел TCP/IP. Каждый IP-адрес состоит из двух частей: идентификатора сети и идентификатора узла, первый служит для обозначения всех узлов в одной физической сети, второй обозначает конкретный узел сети.

**IP-адрес** назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

P-адрес имеет длину 32 бита (4 байта) и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:

128.10.11.31 - традиционная десятичная форма представления адреса, каждое число может находиться в диапазоне от 0 до 255.

10000000 00001010 00001011 00011111 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

- Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей) В сетях класса A количество узлов должно быть больше $2^{16}$, но не превышает $2^{24}$.
- Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов $2^8$ - $2^{16}$. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
- Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше $2^8$. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
- Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

| Класс | Наименьший адрес | Наибольший адрес |
|---|---|---|
| **A** | 01.0.0 | 126.0.0.0 |
| **B** | 128.0.0.0 | 191.255.0.0 |
| **C** | 192.0.1.0 | 223.255.255.0 |
| **D** | 224.0.0.0 | 239.255.255.255 |
| **E** | 240.0.0.0 | 247.255.255.255 |

[50] Поэтому нужно с большим подозрением относиться к сетевым устройствам, у которых в MAC-адресе старшие 3 байта – нули. Скорее всего – это подделка!

### Соглашения о специальных адресах

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов - **broadcast**, **multicast**, **loopback**.

Широковещательный адрес или broadcast определяется следующим образом.

Если IP-адрес состоит только из нулей – 0.0.0.0, то он обозначает адрес того узла, который сгенерировал этот пакет.

Если в поле номера сети стоят нули, а в поле адреса узла – реальный адрес узла, например, 0.0.0.128, то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет.

Если все двоичные разряды IP-адреса равны 1 (в десятичной интерпретации – 255) - 255.255.255.255, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета и такая рассылка называется ограниченным широковещательным сообщением (**limited broadcast**).

Если в поле сети указан реальный адрес сети, а в поле адреса назначения стоят двоичные единицы (десятичное значение – 255), например – 217.15.24.255, то пакет, имеющий такой адрес, будет рассылаться всем компьютерам в сети 217.15.24.1 – 217.15.24.254.

Если в поле адреса назначения стоят сплошные 1. Такая рассылка называется широковещательным сообщением (**broadcast**).

Адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название **loopback**[51].

Уже упоминавшаяся форма группового IP-адреса - multicast - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп. Такие сообщения в отличие от широковещательных называются мультивещательными. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом.

### Статические и динамические IP-адреса

Статические IP-адреса назначаются (присваиваются) сетевому интерфейсу (как правило – сетевой карте) при установке операционной системы и настройке ее сетевых функций, разумеется, в дальнейшем можно произвести замену адреса[52]. Этот статический адрес нам сообщает администратор локальной сети или провайдер Интернет.

Динамические адреса присваиваются сетевому интерфейсу на один сеанс работы. Для назначения динамических IP-адресов у администраторов сетей или провайдеров Интернет используется специальное программное средство – сервер DHCP. Протокол DHCP (Dynamic Host Configuration Protocol) предназначен для динамического назначения IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (а также, при необходимости, другие параметры конфигурации клиента) из пула наличных

[51] Любой компьютер с современной сетевой операционной системой, даже, если в компьютере не установлен сетевой интерфейс (сетевая плата, модем) имеет данный адрес обратной связи, или «короткого замыкания». Вы можете ввести команду *ping 127.0.0.1* – и убедитесь в том, что этот адрес существует.

[52] Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в сети и должны поэтому полагаться на администраторов.

IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра «продолжительности аренды» (lease duration), которая определяет, как долго компьютер (клиент) может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHCP в аренду.

Примером работы протокола DHCP может служить ситуация, когда компьютер, являющийся клиентом DHCP, удаляется из подсети. При этом назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это свойство очень важно для мобильных пользователей.

Однако, централизация процедуры назначения адресов снижает надежность системы: при отказе DHCP-сервера все его клиенты оказываются не в состоянии получить IP-адрес и другую информацию о конфигурации. Последствия такого отказа могут быть уменьшены путем использовании в сети нескольких серверов DHCP, каждый из которых имеет свой пул IP-адресов.

### Маска подсети

Маска подсети выделяет часть IP-адреса и позволяет TCP/IP отличить идентификатор сети от идентификатора узла. Пытаясь связаться, узлы TCP/IP используют маску подсети (например, 255.255.255.0), чтобы определить, находится узел-получатель в локальной или удаленной сети.

### Шлюз по умолчанию

Для того чтобы установить соединение с узлом из другой сети, необходимо сконфигурировать IP-адрес шлюза по умолчанию. TCP/IP посылает пакеты, предназначенные для удаленных сетей, на шлюз по умолчанию, но только в том случае, если на локальном узле не сконфигурирован другой маршрут к сети получателя. Если не указать шлюз по умолчанию, то связь может быть ограничена локальной сетью.

### Публичные и приватные IP-адреса

Анализ использования IP-сетей показал, что большая часть устройств (компьютеров, маршрутизаторов, сетевых принтеров и т.п.) функционируют в исключительно изолированных сетях, и доступ к ним из других сетей Интернет не предполагается. Однако идеология распределения IP-адресов предполагает, что каждое устройство должно иметь уникальный адрес. Для «экономии» диапазонов IP-адресов для устройств, функционирующих в изолированных сетях было предложено зарезервировать 3 диапазона так называемых «приватных» адресов (см. таблицу), а остальные адреса (за исключением адреса loopback) являются публичными.

| Класс сети | Маска | Диапазон приватных адресов | |
|---|---|---|---|
| **A** | 255.0.0.0 | 10.0.0.0 | 10.255.255.255 |
| **B** | 255.255.0.0 | 172.16.0.0 | 172.31.255.255 |
| **C** | 255.255.255.0 | 192.168.0.0 | 192.168.255.255 |

Принципиальное отличие приватных от публичных адресов заключается в том, что приватные адреса не маршрутизируются в Интернете и могут многократно повторяться в несвязанных Интранет-сетях.

### Символьные имена узлов IP-сетей

**Символьные имена узлов IP-сетей** (компьютеров, маршрутизаторов, сетевых принтеров) имеют иерархическую структуру, например:

computer-masha.market.company.ru или computer-andy.dep-25.company.local

В первом случае компьютер имеет реальное имя в глобальной сети Интернет в домене **company.ru**, во втором – компьютер имеет имя в локальном домене компании – **company.local**.

Для определения (разрешения) соответствия символьного имени компьютера и его IP-адреса используется система DNS (*Domain Name System*) - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен - в нем определены DNS-серверы и DNS-клиенты. DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Интернет. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес.

Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет - то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос, либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически, в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов, для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена. Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе.

### Утилита Ipconfig

Для проверки параметров конфигурации узла, включая IP-адрес, маску подсети и шлюз по умолчанию в операционных системах Microsoft Windows 2000/XP используется

утилита **Ipconfig**[53]. Это полезно при выяснении, успешно ли прошла инициализация TCP/IP и не дублируется ли IP-адрес, указанный в конфигурации. Синтаксис команды:

*ipconfig*

Если протокол инициализировался успешно с заданной конфигурацией, то на экране отобразятся IP-адрес, маска подсети и шлюз по умолчанию. Если адрес, заданный в конфигурации уже используется другим узлом в сети на том же сегменте, то отобразится заданный IP-адрес, но маска подсети будет равна 0.0.0.0

#### Утилита Ping

После проверки конфигурации утилитой Ipconfig Вы можете запустить утилиту Ping (Packet Internet Groper) для тестирования соединений. Это диагностическое средство тестирует конфигурации TCP/IP и позволяет определить неисправности соединения. Утилита Ping использует пакеты эхо-запроса (echo request) и эхо-ответа (echo reply) протокола ICMP (Internet Control Message Protocol) для проверки доступности и работоспособности определенного узла TCP/IP. Синтаксис команды:

*ping IP_адрес*

#### Если проверка прошла успешно, то отобразится сообщение типа:

*Pinging IP_адрес with 32 bytes of data:*
*Reply from IP_адрес: bytes= x time<10ms TTL= x*
*Reply from IP_адрес: bytes= x time<10ms TTL= x*
*Reply from IP_адрес: bytes= x time<10ms TTL= x*
*Reply from IP_адрес: bytes= x time<10ms TTL= x*

Если при загрузке операционной системы обнаруживается, что заданный IP-адрес уже используется, то даже после его изменения в конфигурации протокол не инициализируется, пока система не будет перезагружена.

## 3.5. Протокол Ethernet

Протокол Ethernet является наиболее распространенным протоколом, используемым в локальных и глобальных компьютерных сетях. Ethernet представляет собой протокол с состязательным доступом и в качестве метода управления доступа к физической среде использует метод CSMA/DC (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением коллизий). Протокол Ethernet реализуется в проводных и беспроводных сетях.

### 3.5.1. Проводные сети

В качестве физической среды являются кабели, как на основе медных проводников (коаксиальные и типа «витая пара»), так и волоконно-оптические.

Стандарт IEEE[54] 802.3 (и его спецификации) определяют проводные сети Ethernet. Сеть Ethernet по данному стандарту использует топологию шины или звезды. Сетевые узлы, как уже отмечалось, могут быть соединены кабелем либо на основе медных проводников (коаксиальным или типа «витая пара») либо волоконно-оптическим кабелем.

---

[53] Для вызова утилиты следует вызвать окно командной строки (Пуск→ Программы→ Командная_строка) и в окне командной строки ввести требуемую утилиту.

[54] Institute of Electrical and Electronic Engineers (IEEE) - Институт инженеров по электротехнике и электронике (профессиональное объединение, выпускающие свои собственные стандарты; членами IEEE являются ANSI и ISO).

Существуют следующие параметры спецификаций физического уровня протокола для стандарта Ethernet:

**10Base5.** Этот стандарт определяет максимальную пропускную способность 10 Мбит/с при использовании толстого коаксиального кабеля. При этом максимальная длина сегмента составляла 500 метров. Благодаря большой длине сегмента он занял свою нишу на рынке сетевого оборудования. В настоящее время практически не используется.

**10Base-2.** Стандарт IEEE 802.3a, пропускная способность также составляла 10 Мбит/с, но использовался тонкий коаксиальный кабель (диаметр около 6 мм). Физическая топология - шина, что обуславливает сравнительно небольшие затраты кабеля, но при выходе одного узла из строя, вся сеть переставала функционировать. Он был более удобен для прокладки, чем толстый коаксиальный кабель и получил достаточно широкое распространение. Максимальная длина сегмента составляет 185 метров. В настоящее время, как и толстый коаксиал, он практически не используется.

**10BaseT.** Является наиболее удобным стандартом из всей группы 10Base, что можно объяснить тем, что в нем используется витая пара (UTP) третьей категории (Cat3) и выше. Такой кабель более удобен для прокладки, чем коаксиальный, но из-за того, что используется физическая топология звезда (необходимо центральное устройство), расход кабеля больше, чем при использовании коаксиального кабеля и физической топологии шина. Хотя такой недостаток компенсируется более высокой надежностью сети - при выходе из строя одного канала связи или узла, остальная часть сети продолжает работать. Максимальная длина сегмента составляет 100 метров. Сегодня используется только в старых сетях и постепенно исчезает.

**10BaseF.** Этот стандарт сегодня абсолютно не актуален, поскольку использование оптоволокна для создания сети с пропускной способностью всего 10 Мбит/с явно нецелесообразно, хотя различные спецификации поддерживают расстояние до 2000 метров.

**100BaseTX**. Этот стандарт использует две пары кабеля пятой категории (Cat5) и выше. Хотя для построения сети с использованием этого стандарта третья категория кабеля не подойдет, но сегодня это не является проблемой, в случае построения локальной сети с нуля. Кабель пятой категории имеет достаточно низкую стоимость, и может обеспечивать пропускную способность 100 Мбит/с при использовании двух пар проводников. Максимальная длина сегмента также составляет 100 метров. Именно этот стандарт сегодня является наиболее популярным.

**100BaseFX**. Эта спецификация определяет работу по двум многомодовым оптоволокнам со скоростью 100 Мбит/с. Здесь же определены спецификации 100BaseSX и 100BaseLX, работающие при разных длинах волн, кроме того, 100BaseLX может работать и на одномодовом оптоволокне.

**1000BaseT.** Основой этого стандарта, утвержденного в 1998 году, является стандарт IEEE 802.3z. Этот стандарт длительное время использовался исключительно для магистральных каналов, до тех пор, пока в 1999 году не вышло его дополнение для гигабитного Ethernet по кабелю «витая пара» - 1000BaseT. Именно это дополнение помогло этому стандарту выйти практически на тот же рынок, что и 10/100 Мбит Ethernet. В итоге получился стандарт, превышающий по скорости 100BaseT в десять раз, и обратно совместимые с более ранним оборудованием для сетей Ethernet. Он использует традиционный для сегодняшних сетей кабель CAT-5 (или лучше). По мере снижения цен на гигабитное Ethernet оборудование, область применения его расширялась. Сегодня его можно встретить на рабочих станциях, где требования к пропускной способности высоки.

Отметим, что для сетевых приложений, разработанных с учетом возможности работы через Интернет, такая скорость оказывается невостребованной. Для мультимедиа потоков также не требуется гигабитная сетью. Максимум, что потребуется - 40 Мбит/с (для профессионального качества), - 20 Мбит/с (для обычного же пользователя), а при использовании формата MPEG-4 –не более 4 Мбит/с. Поэтому переход на гигабитную сеть ну-

жен в том случае, если требуется одновременная обработка нескольких потоков профессионального качества.

Актуальность гигабитного Ethernet для копирования и резервирования стоит рассмотреть немного подробнее. При копировании больших файлов по стомегабитной сети, а именно такое копирование более наглядно показывает пропускную способность, можно столкнуться с нехваткой пропускной способности. А при том, что скорость выше пятидесяти мегабит в секунду на сети Fast Ethernet достичь весьма сложно, переход на гигабитный Ethernet может исправить дело. При резервировании по сети, равно как при одновременном копировании с нескольких компьютеров на один, переход на гигабит поможет лишь в том случае, если производительность компьютеров и их дисковых систем будет достаточной.

Клиент-серверные бизнес-приложения, использующиеся в сетях предприятий могут быть достаточно критичными к пропускной способности сети, но здесь все зависит от конкретного приложения и для определения необходимости перехода на гигабит следует проанализировать нагрузку на сеть.

Можно сделать вывод, что десятимегабитный Ethernet уже практически не используется, поскольку его скорость недостаточна для большинства сегодняшних сетевых приложений.

### 3.5.2. Беспроводные сети (RadioEthernet)

Как уже отмечалось, в последнее время стали активно применяться беспроводные сетевые средства, основанные на так называемой технологии Wi-Fi (Wireless Fidelity). Соответственно, данная технология передачи данных основана на семействе стандартов (спецификаций) Ethernet IEEE 802.11. Бурное развитие беспроводного Ethernet определяется следующими обстоятельствами:

- разработаны эффективные программные (в составе современных операционных систем) и аппаратные (в составе сетевых адаптеров и точек доступа) средства обеспечения безопасности;
- существенно снизилась стоимость оборудования для беспроводных сетей (беспроводных сетевых адаптеров, точек доступа и т.п.);
- при проектировании локальной сети в пределах здания (компании) выгоднее развернуть сеть на основе беспроводного Ethernet, чем выполнять достаточно дорогостоящие работы по прокладке кабельной сети[55];
- с помощью беспроводного Ethernet достаточно просто решить проблему оперативного подключения удаленного офиса, либо подключения к Интернет-провайдеру[56];
- «по умолчанию» средства Wi-Fi установлены практически во все современные ноутбуки, карманные портативные компьютеры и коммуникаторы (смартфоны), мобильные телефоны достаточно высокого класса;
- доступ к Интернет с помощью W-Fi предоставляют своим клиентам многочисленные кафе и рестораны, отели, бизнес -центры;

**Стандарт IEEE 802.11** (1997 г.), является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей (WLAN). Основные из них - протокол управления доступом к среде MAC (Medium Access Control - нижний подуровень канального уровня) и протокол PHY передачи сигналов в физической среде, в качестве которого допускается использование радиоволн и инфракрасного излучения.

[55] Тем более – сразу же после выполненного ремонта!

[56] Разумеется, данные подключения можно выполнить и с помощью волоконно-оптических линий связи (в ряде случаев это будет и более эффективно), но прокладка любого кабеля (особенно в условиях современного города) – процесс длительный и дорогостоящий.

**Протокол доступа к среде (MAC)**. Стандартом 802.11 определен единственный подуровень MAC, взаимодействующий с тремя типами протоколов физического уровня, соответствующих различным технологиям передачи сигналов - по радиоканалам в диапазоне 2,4 ГГц с широкополосной модуляцией с прямым расширением спектра (DSSS) и перескоком частоты (FHSS) , а также с помощью инфракрасного излучения[57]. Спецификациями стандарта предусмотрены два значения скорости передачи данных - 1 и 2 Мбит/с.

По сравнению с проводными локальными сетями Ethernet возможности Radio-Ethernet подуровня MAC расширены за счет включения в него ряда функций, обычно выполняемых протоколами более высокого уровня, в частности, процедур фрагментации и ретрансляции пакетов. Это вызвано стремлением разработчиков стандарта повысить эффективную пропускную способность системы благодаря снижению накладных расходов на повторную передачу пакетов.

В качестве основного метода доступа к среде стандартом 802.11 определен механизм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance - множественный доступ с обнаружением несущей и предотвращением коллизий).

В основу стандарта 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и нескольких ячеек. Каждая сота управляется базовой станцией, называемой *точкой доступа* (Access Point, AP), которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует *базовую зону обслуживания* (Basic Service Set, BSS) Точки доступа мультисотовой сети взаимодействуют между собой через *распределительную систему* (Distribution System, DS), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему образует *расширенную зону обслуживания* (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняются непосредственно рабочими станциями.

**Роуминг**. Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в мультисотовых системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга базовая версия стандарта 802.11 (в отличие от последующих спецификаций) не предусматривает.

**Обеспечение безопасности**. Для защиты WLAN стандартом IEEE 802.11 предусмотрен целый комплекс мер безопасности передачи данных под общим названием Wired Equivalent Privacy (WEP). Он включает средства противодействия несанкционированному доступу к сети (механизмы и процедуры аутентификации), а также предотвращение перехвата информации (шифрование).

П**равовые аспекты использования Wi-Fi**. Частотный диапазон от 2.4ГГц до 2.4835 ГГц, в основном используемый беспроводными сетями[58], относится к так называемым «частотам ISM» (международному диапазону частот для промышленности, науки и медицины) и в большинстве стран мира не требует какого либо лицензирования.

В Российской Федерации использование радиоэлектронных средств различного назначения регламентируется Государственной комиссией по радиочастотам (ГКРЧ)[59]. В

[57] В дальнейшем рассматриваем только радиоканал

[58] Используется, но значительно реже, и диапазон частот в районе частоты 5 ГГц. Для данного диапазона частот порядок лицензирования более затруднен.

[59] Государственная комиссия по радиочастотам является межведомственным координационным органом, действующим при Министерстве информационных технологий и связи Российской Федерации и осуществляющим на коллегиальной основе регулирование использования радиочастотного спектра в РФ. Комиссия действует в составе представителей Министерства информационных технологий и связи Российской Федерации, Министерства юстиции Российской Федерации, Министерства обороны Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы охраны Российской Федерации, Службы внешней разведки Российской Федерации, Федеральной службы по надзору в сфере связи, Федеральной службы по гидрометеорологии и монито-

соответствии с действующим законодательством, регламентирующим порядок использования радиочастотного ресурса в России (Положениями и Решениями ГКРЧ), можно выделить три типа оборудования беспроводного доступа. Для каждой из групп характерны свои особенности использования радиочастотного ресурса в полосе частот 2400-2483,5 МГц и свой порядок получения разрешительных документов.

1. **Внутриофисные системы беспроводной передачи данных**. Станции (устройства) внутриофисных систем передачи данных разрешается использовать только внутри зданий, закрытых складских помещений и производственных территорий. Максимальная излучаемая мощность любой станции не должна превышать 100 мВт, для станций разрешается использование только интегральных или специализированных антенн и запрещено использование каких-либо внешних антенн. При вводе в эксплуатации внутриофисных систем действует упрощенный порядок лицензирования, заключающийся в том, что допускается использование сертифицированного оборудования без оформления разрешения на использование радиочастот при обязательной регистрации используемых радиоэлектронных средств в установленном в РФ порядке.
2. **Уличные операторские сети беспроводной передачи данных**. Станции (устройства) уличных операторских сетей разрешено использовать вне офисных и производственных помещений, например, на стадионах, в жилых кварталах и т.п. При этом операторами данных сетей не должны предъявляться претензии на возможные помехи от радиоэлектронных средств военного и другого назначения, а также от высокочастотных установок промышленного, научного, медицинского и бытового применения, использующих данную полосу радиочастот. максимальная излучаемая мощность любой станции не должна превышать 1000 мВт, разрешено использовать внешние антенны, входящие в состав сертифицированных устройств, или имеющие сертификаты ГКРЧ. В отношении указанных систем беспроводной передачи данных действует общий порядок назначения радиочастот, частичное упрощение процедуры состоит в том, что разработка и производство, закупка за границей, приобретение на внутреннем рынке, а также эксплуатация рассматриваемых радиоэлектронных средств не требуют оформления частных решений ГКРЧ. В диапазоне 5 ГГц порядок назначения радиочастот одинаков как для уличных операторских сетей, так и для внутриофисных сетей беспроводной передачи данных. Он определен Положениями "О порядке выделения полос радиочастот в Российской Федерации для радиоэлектронных средств всех назначений и высокочастотных устройств" и "О порядке назначения (присвоения) радиочастот в Российской Федерации".
3. **Персональные беспроводные системы**. Данную категорию оборудования Wi-Fi представляют маломощные радиоэлектронные средства технологии Bluetooth. Большинство из них интегрированы в другие электронные системы: периферия персональных компьютеров, сотовые телефоны, видеокамеры и др.Максимальная излучаемая мощность любой станции не должна превышать 2,5 мВт, антенная должна быть интегральной, т.е. встроенной в устройство. Данные устройства согласно Решению ГКРЧ могут реализовываться через торговую сеть без оформления разрешений органов государственной радиочастотной службы на приобретение и эксплуатацию. Также не требуется их регистрировать в органах радиочастотной

---

рингу окружающей среды, Федерального агентства по техническому регулированию и метрологии, Федерального агентства связи, Федерального агентства по информационным технологиям, Федерального агентства по промышленности, Федерального космического агентства и Федерального агентства по печати и массовым коммуникациям.

службы. Фактически речь идет о безлицензионном порядке использования такого оборудования.

В настоящее время наиболее распространены следующие спецификации стандарта **IEEE 802.11**

**Стандарт IEEE 802.11b** - техническая спецификация, определяющая функционирование беспроводных локальных вычислительных сетей, работающих в диапазоне 2,4 ГГц со скоростью 1, 2, 5,5 и 11 Мбит/с по протоколу Direct Sequence Spread Spectrum. В соответствии со стандартом 802.11b передача данных осуществляется на частоте 2,4 ГГц в виде маломощного шумоподобного сигнала, причем предусмотрено более 10 каналов шириной 22 МГц.

**Стандарт 802.11g** является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Стандарт IEEE 802.11g предусматривает скорости соединения: 1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48 и 54 Мбит/с. Одни из них являются обязательными для стандарта, а другие — опциональными для конкретного устройства. Кроме того, для различных скоростей соединения применяются разные методы модуляции сигнала.

Стандарт 802.11g полностью совместим с 802.11b, т.е. любое устройство стандарта 802.11g должно поддерживать работу с устройствами 802.11b[60]. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодняшний день данный стандарт беспроводной связи является наиболее перспективным.

Ряд производителей предлагают собственные расширения стандарта 802.11g с целью повышения скорости передачи данных до 108 Мб/с, например, компания D-Link выпускает беспроводное сетевое оборудование, поддерживающее стандарт «802.11g –Turbo». Но данные преимущества могут быть реализованы при работе оборудования одного производителя. Отметим также, что при ухудшении условий распространения радиоволн беспроводные устройства автоматически снижают скорость передачи данных и восстанавливают ее при восстановлении уровня радиосигнала.

Радиус действия устройств Wi-Fi определяется мощностью передатчиков, чувствительностью приемников, условиями распространения радиоволн в диапазоне 2,4 ГГц и составляет:

- для сетевых адаптеров ноутбуков, персональных компьютеров и точек доступа SOHO-класса — до 400 м вне помещений и до 100 м в пределах помещения[61], причем на радиус охвата могут влиять факторы окружающей среды (например, наличие электромагнитных помех), климатические факторы (туман, дождь, снегопад), наличие препятствий на пути распространения радиосигнала;
- для профессионального оборудования — до 30 км (в режиме «радиомоста»).

**Архитектура беспроводных сетей**. На MAC-уровне определяются два основных типа архитектуры сетей - Ad Hoc и Infrastructure Mode.

В **режиме Ad Hoc**, который называется также Independent Basic Service Set (IBSS) или режимом Peer to Peer (точка-точка), станции непосредственно взаимодействуют друг с другом напрямую без участия точки доступа. Для этого режима требуется минимум оборудования: каждая станция должна быть оснащена беспроводным адаптером. При такой конфигурации не требуется создания сетевой инфраструктуры. Основным недостатком режима Ad Hoc является ограниченный диапазон действия возможной сети и невозможность подключения к внешней сети (например, к Интернету).

---

[60] Для такой совместимости и введена скорость 11 Мбит/с.

[61] Данные значения заявляют изготовители аппаратуры и являются несколько завышенными, поскольку получены в идеальных условиях. Практически ноутбук, снабженный адаптеров Wi-Fi, устойчиво работает на расстоянии 30-40 м от точки доступа (в одном помещении) или в помещении, отделенным от точки доступа двумя-тремя кирпичными стенками или одной железобетонной.

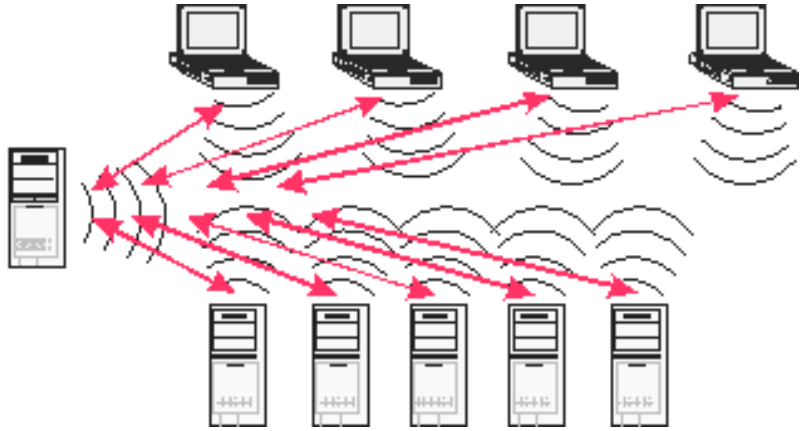


Рис.3. Режим Ad Host

**Режим взаимодействия Infrastructure** — все узлы беспроводной сети взаимодействовали с точкой доступа. Сама же точка доступа служит мостом между беспроводной сетью и внешней сетью Ethernet и подключалась к сегменту внешней кабельной сети.

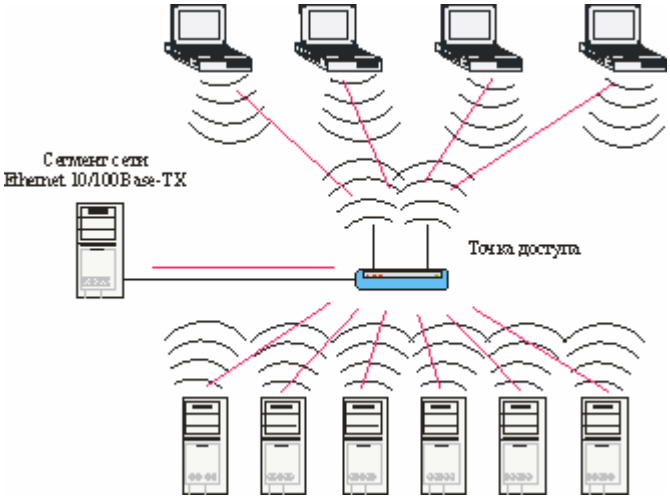



Рис.4. Режим с точкой доступа

**Режим «мост»** — два беспроводных устройства связаны в режиме «точка-точка», а данные устройства будут, в свою очередь, шлюзами для сегментов локальных сетей.

***Контрольные вопросы***

1. Что такое архитектура ИС?
2. Что такое топология ИС?
3. Принципиальные отличия топологий «общая шина» и «звезда»
4. Область применения топологии «кольцо»
5. Что такое уровни модели OSI
6. Области использования протоколов Ethernet и TCP/IP
7. Примеры физической реализации протокола Ethernet
8. Какую максимальную скорость передачи данных можно получить в беспроводной сети?

# 4. Технологии Интернет и Интранет в системах информационного сервиса

Системы информационного сервиса в своей работе должны широко использовать ресурсы и технологии всемирной сети Интернет.

Для получения актуальной информации используются:

- сайты государственных, муниципальных организаций;
- сайты коммерческих компаний и некоммерческих организаций;
- поисковые системы.

Для размещения информации о собственной компании следует создать собственный сайт с одновременным его «продвижением» - анонсированием в ведущих поисковых системах.

Для оперативного обмена информацией следует использовать электронную почту.

**К перспективным технологиям Интернет относятся:** IP-телефония, web-телевидение, технологии online-общения, видео и аудиоинформация по заказу. Мобильные мультимедийные технологии. Видео и аудио IP- мобильная телефония, телевидение на основе мобильной связи, голосовая почта.

Все перечисленные возможности Интернет целесообразно использовать и в информационной системе компании в том случае, если она не имеет выхода в Интернет. Использование методов и технологий Интернет в сети компании называется Интранет.

Принципиально различия между Интернет и Интранет отсутствуют. Даже в локальной сети небольшой компании можно установить собственный web-сервер, на котором будет размещен корпоративный сайт, доступный исключительно сотрудникам компании со своих рабочих мест. В такой сети можно установить почтовый сервер и организовать обмен почтовыми сообщениями между сотрудниками, сервер обмена сообщениями и т.п.

## 4.1. Электронная почта (E-Mail)

Электронная почта традиционно считается первым и по настоящее время наиболее значимым ресурсом Интернет. Электронная почта предназначена для передачи текстовых сообщений (писем), в которые могут быть вложены произвольные файлы (текстовые, табличные, графические, мультимедиа и т.п.).

Как и любые ресурсы Интернет, электронная почта базируется на программах-серверах, клиентах и протоколах.

Для использования сервиса электронной почты пользователь должен получить почтовый адрес. Данный адрес (или имя почтового ящика) состоит из двух частей, разделенных символом @[62] – первая часть: имя почтового ящика, вторая часть - почтовый домен, например yulya@company.ru.

В имени почтового ящика допустимы символы латинского алфавита, цифры, дефис и точка. Имя домена присваивает владелец почтового сервера.

Почтовый ящик пользователь может создать:

- на корпоративном почтовом сервере, в этом случае адрес расположен в домене корпорации (user@company.ru) и доступ к почтовому ящику (в целях безопасности) может быть осуществлен только с компьютеров компании (или даже с компьютера конкретного пользователя);
- на почтовом сервере провайдера, соответственно почтовый адрес будет располагаться в домене провайдера (user@provider.ru), доступ к почтовому ящику может быть осуществлен только в случае входа в Интернет с использованием учетной записи, выданной данным провайдером;
- на одном из бесплатных почтовых серверов (mail.ru, yandex.ru и т.п.), почтовый адрес будет иметь вид user@mail.ru, доступ к данному почтовому ящику

[62] правильное название символа @: «эт», коммерческое «а», амперсанд

может быть осуществлен с любого компьютера, имеющего доступ в Интернет, вне зависимости от провайдера.

Сравнивая перечисленные способы организации почтового ящика, отмечаем, что первый способ (корпоративный почтовый ящик) является единственным способом организации служебного (официального) почтового адреса. В данном случае, во-первых, почтовый адрес явно показывает компанию и (иногда) организационную структуру, в которой работает владелец ящика, во-вторых, обеспечена безопасность хранения писем, и, в третьих, доступ к ящику может быть осуществлен только с компьютеров компании.

Почтовый ящик у провайдера обычно организовывают небольшие компании, которые не имеют собственного почтового сервера. Как правило, все корпоративные пользователи имеют постоянного провайдера. В этом случае провайдер должен обеспечивать все аспекты безопасности почтовой системы компании. В случае, если провайдер организовал на своем сервере почтовый домен компании, то и имя почтового ящика может быть company.ru. Достоинством данного способа является отсутствие необходимости иметь в составе компании почтовый сервер и, соответственно, высококвалифицированного специалиста по его обслуживанию, недостатком – дополнительные финансовые затраты за поддержку почтового сервера[63] и отсутствие оперативного управления им.

Бесплатные почтовые серверы очень удобны для организации личных почтовых ящиков, которыми можно пользоваться с любого компьютера, подключенного к Интернету. Это и будет основным достоинством. Недостатки: почтовый адрес трудно связать с компанией, отсутствие явного договора с владельцем почтового сервера, а также наличие рекламных сообщений и баннеров, которые мы должны читать, оплачивая «бесплатность» этого почтового сервиса.

**Почтовые серверы**. Задачей почтового сервера является прием почтовых сообщений от клиентов и других почтовых серверов по протоколу SMTP и передачи почтовых сообщений клиентам по протоколам POP3 и IMAP4. Бесплатные почтовые сервера предлагают в качестве основного web-интерфейс.

**Протокол SMTP** (Simple Mail Transport Protocol - Простой протокол электронной почты) используется для передачи сообщений от клиента к почтовому серверу получателя. Особенностью протокола SMTP является то обстоятельство, что протокол требует постоянная (круглосуточная) доступность почтового сервера – получателя. Очевидно, что от компьютера – рабочей станции этого требовать практически невозможно, поэтому с помощью протокола SMTP письмо доставляется до почтового сервера, на котором почтовый сервер организовал почтовый ящик. Протокол SMTP встроен в программу – почтовый клиент и отправка писем с помощью протокола SMTP происходит автоматически, пользователь должен при настройке почтового клиента указать адрес сервера SMTP. Авторизация пользователя выполняется, как правило, автоматически, т.е. владелец почтового ящика использует IP-адрес пользователя (в случае использования корпоративной почты или почты, предоставленной провайдером) или данные пользователя (имя и пароль) при использовании бесплатного почтового адреса. Получатель должен получить письма с помощью протокола POP3 или IMAP4.

**Протокол POP3** (Post Office Protocol - Почтовый протокол) предназначен для получения писем с почтового сервера. Авторизация на сервере POP3 осуществляется с помощью ввода регистрационных данных (имени и пароля). Особенностью протокола POP3 является то обстоятельство, что при входе на почтовый ящик POP3-клиент получает список всех сообщений и обязан их все получить. После этого сеанса связи почтовый ящик POP3 «очищается». Если произойдет разрыв связи, то при следующем сеансе почтовый клиент обязан будет снова взять все письма, а если в почтовом ящике находится достаточно большое письмо, то попытка взять все письма может закончиться неудачей.

[63] Но эти затраты все равно меньше, чем зарплата системного администратора почтового сервера.

**Протокол IMAP4** (Interactive Mail Access Protocol - Протокол интерактивного доступа к электронной почте). IMAP4 позволяет клиенту получать доступ к электронным сообщениям на сервере и совершать с ними различные действия. Этот протокол можно рассматривать как расширенный протокол POP3. IMAP — развивающаяся технология, по функциональности превосходящая предыдущую среду POP, поскольку позволяет просмотреть все письма в почтовом ящике и произвести (не скачивая письма на клиентский компьютер) необходимые действия: удалить явно ненужные письма и скачать только нужные.

**Почтовые сервера** инсталлируют на платформах Unix (FreeBSD, Linux) или Microsoft Windows Server. Приведем наиболее распространенные почтовые серверы.

На платформе Unix (FreeBSD, Linux).

**Sendmail** – почтовый сервер, входит в состав дистрибутивов, поддерживает протоколы SMTP, POP3 и IMAP4, работает на платформе Unix (FreeBSD, Linux).

**Microsoft Exchange Server 2003** – мощный сервер обмена сообщениями для электронной почты (поддерживает протоколы SMTP, POP3 и IMAP4), а также осуществляет планирование работы групп, сотрудничества, приложений управление документооборотом и маршрутизацию документов.

**EservAgava mail server** функционирует на платформе Microsoft Windows NT4/2000/XP (для NT4/2000 – на рабочих станциях и серверах). В состав сервера включены:

- почтовый сервер (SMTP, POP3, IMAP4), веб-сервер (HTTP),
- файловый сервер (FTP),
- SNMP сервер,
- SSL/TLS-версии всех серверов (HTTPS, SMTPS, POP3S, IMAPS, FTPS),
- программы управления комплектом серверов,
- статистический спам-фильтр SpamProtexx.

**Courier Mail Server** – достаточно простой почтовый сервер, поддерживает все протоколы почты (SMTP, POP3 и IMAP4), позволяет организовать обмен сообщениями электронной почты в локальной сети и Интернете. Сервер работает на платформах Microsoft Windows NT4/2000/XP, не требователен к аппаратуре. Упрощенный вариант данного почтового сервера можно бесплатно получить с сайта разработчика.

**Почтовые клиенты** позволяют осуществить:

- подготовку электронных писем, вложение в письма файлов произвольного формата;
- отправку и получение писем по протоколам SMTP и POP3 (IMAP4) соответственно;
- ведение баз данных (папок) писем: входящих, исходящих, отправленных, удаленных;
- ведение адресной книги.

Принципиальной особенностью почтового клиента является то обстоятельство, что с помощью почтового клиента можно работать «off-line»[64], т.е. не будучи подключенным к Интернет, и все письма (как полученные, так и отправленные) находятся на локальном компьютере – рабочей станции[65].

**Microsoft Outlook Express** является наиболее распространенным почтовым клиентом, поскольку данная программа интегрирована в операционную систему Microsoft Windows. Outlook Express позиционируется в качестве приложения к Internet Explorer для работы с почтой. Фактически Outlook Express – является облегченной версией Outlook, ко-

[64] Ввиду того, что все большее распространение приобретает оплата услуг провайдеров по трафику, это обстоятельство (по сравнению с web-интерфейсом почты) уже нельзя считать неоспоримым достоинством.

[65] В какой то степени сомнительное достоинство (по сравнению с web-интерфейсом): мы скачали письма на свой рабочий компьютер, а затем поехали в командировку. А как нам прочитать письмо, которое мы забыли переписать или оно отправлено после отъезда? Зато безопасность выше!

торая является уже коммерческим продуктом и поставляется Microsoft в составе пакета Microsoft Office 2000 и последующих версий.

**The Bat!** - простой, и одновременно мощный почтовый клиент. Программа имеет существенное количество дополнительных возможностей и характеризуется весьма удобным интерфейсом. Программа является коммерческим продуктом.

**Eudora**. Этот почтовый клиент считается на западе признанным лидером среди подобных программ, являясь наиболее функциональным продуктом в своем классе. Особо нужно отметить прекрасно реализованные и в таком объеме нигде больше не встречающиеся возможности для работы с почтой на «наладонных компьютерах» (КПК).

## 4.2. Служба WWW

**WWW** (World Wide Web) - служба в Интернет, которая позволяет легко получать доступ к информации на серверах, расположенных по всему миру. Документы в WWW структурированы с помощью HTML (HyperText Markup Language - язык гипертекстовой разметки) и могут включать в себя многочисленные приложения (или взаимодействовать с ними).

Служба WWW построена по принципу «клиент-сервер» и основана следующих стандартах:

- HTML (HyperText Markup Language) - язык гипертекстовой разметки документов;
- URL (Universal Resource Locator) - универсальный способ адресации ресурсов в сети;
- HTTP (HyperText Transfer Protocol) - протокол обмена гипертекстовой информацией;
- HTTPS (HyperText Transfer Protocol Secure) – протокол обмена гипертекстовой по защищенному каналу.

Сервером службы WWW является web-сервер, клиентом - Web-обозреватель (браузер). Упрощенно процедура обмена информацией клиента и сервера происходит следующим образом. Пользователь в программе-браузере в специальном поле – «строке адреса» вводит адрес требуемого ресурса в формате Universal Resource Locators - URL (например, http://www.yandex.ru или http://213.180.204.11). По умолчанию происходит к обращение к главной (основной, индексной) странице сайта. Разумеется, используя технологию гиперссылок посетитель этой страницы может перейти к необходимой «внутренней» странице сайта, однако, в случае необходимости в URL можно указывать также путь к данной конкретной странице, например http://guap.ru/guap/priem/prav_main.shtml.

В ряде случаев после IP-адреса или доменного имени компьютера (в адресной строке браузера) вводится набор символов, состоящих из двоеточия и целого неотрицательного числа. Это число показывает номер **порта TCP**, к которому производится обращение. Дело в том, что программа-клиент, которая посылает ответ на запрос ждёт его именно на вполне определенном порту (по умолчанию для протокола HTTP используется порт 80, поэтому, как правило, номер порта в адресной строке браузера и не вводят).

Таким образом, URL, набираемый в строке браузера, имеет следующий вид:

протокол://адрес:порт/путь.[66]

Клиентский компьютер связывается с web-сервером, на котором размещается требуемый сайт, проверяет возможность обслужить данного клиента (например, доступ к сайту возможен при успешной авторизации по имени пользователя, компьютера) и, при положительном решении, предоставляет возможность загрузить страницу сайта, т.е. документ, созданный с помощью языка HTML. Браузер является интерпретатором языка HTML и, по мере загрузки документа, осуществляет исполнение директив языка («тэ-

[66] Все современные браузеры самостоятельно подставляют протокол HTTP, либо выбирают необходимый протокол самостоятельно (HTTPS, FTP), поэтому вводить протокол, как правило, не требуется.

гов»): размещение на экране отформатированного текста и графических объектов, дальнейший обмен с web-серверами и т.д.

В простейшем случае браузер посылает запрос WEB-серверу, который возвращает содержимое файла, имя которого содержится в URL (такой сайт называют **статическим**). Однако, возможен другой случай: WEB-сервер запускает программу (скрипт, запускаемый на стороне сервера) и возвращает результат его работы. В этом случае сайт называется **динамическим**, так как результат работы скрипта может меняться с течением времени (и в зависимости от пользователя). Кроме того, указанный скрипт может, например, обращаться к базам данных. С другой стороны, не каждое действие пользователя нужно обрабатывать на стороне сервера, поэтому некоторые действия могут выполняться скриптами на стороне клиента (например, проверка правильности ввода даты). Скрипты на стороне клиента пишутся обычно на языках JavaScript, Java. Могут использоваться VBScript, ActionScript (Flash) и вообще любые языки программирования. В некоторых случаях текст скрипта встроен в HTML-документ, в других случаях загружается из отдельного файла. На стороне сервера чаще всего используют PHP, Perl, ASP, но можно использовать любые языки**.**

Основные используемые программы-клиенты - это Internet Explorer (Microsoft), Firefox и Mozilla, Opera. Браузеры являются также и многопротокольными клиентами, т.е. при необходимости они могут осуществлять обмен информацией с web-серверами по протоколу HTTPS, ftp и другими.

Протокол HTTPS создан для безопасного обмена по сети. Этот протокол аналогичен обычному протоколу HTTP, но он дополнительно использует технологию SSL (Secure Socket Layer), что позволяет аутентифицировать клиента и делает обмен данными с сервером полностью недоступным для несанкционированного перехвата или искажения.

Протокол SSL использует общеизвестный методы шифрования, в том числе и метод шифрования открытым ключом. Основой для этого служат сертификаты: сертификат сервера и сертификат клиента. Сертификат сервера, который получает клиент, содержит только открытый ключ сервера, а сертификат клиента содержит как открытый, так и закрытый ключи. Сертификат клиента подписывается закрытым ключом сервера.

Web-сервера устанавливаются на компьютерах, имеющих круглосуточный доступ в Интернет[67] и постоянный (фиксированный) IP-адрес. В качестве программного обеспечения web-серверов используются сервер Apache и Internet Information Server.

**Apache** работает на платформах UNIX/Linux и Microsoft Windows. Данный сервер распространяется по открытой лицензия GNU и, поэтому, в большинстве случает устанавливается на UNIX-платформах, поставляемых по аналогичной лицензии. Apache позволяет создать мощный и производительный web-сервер, позволяющий обслужить на одном компьютере достаточно большое количестве независимых web-серверов, т.е. создать так называемые «виртуальные серверы», имеет мощные средства администрирования и обеспечения безопасности.

**Internet Information Server** интегрирован в серверные операционные системы Microsoft: Windows 2000 и 2003 Server, соответственно – является полностью коммерческим программным продуктом. Internet Information Server (IIS) в составе Windows 2000 Server и 2003 Server содержит в своем составе также файловый сервер (FTP-server) и почтовый сервер. Справедливости ради следует отметить, что IIS в «облегченной» версии имеется и в составе и операционных систем рабочих станций: Windows 2000 professional и Windows XP professional, что можно использовать для отладки сайта, например, на своем локальном компьютере перед установкой на web-сервере в Интернет[68].

---

[67] Это требование относится к Интернет-серверу, для Интранет-сервера необходимо, чтобы компьютер был доступен в пределах рабочего времени компании.

[68] Данный программный компонент не устанавливается «по умолчанию» при установке операционной системы. Для его инсталляции необходимо воспользоваться режимом «Добавление и удаление компонентов Windows».

В качестве клиентом используются браузеры - Internet Explorer (интегрирован в Microsoft Windows), Mozilla, Opera и другие позволяют пользователям просматривать Web-страницы и получить доступ к гипертекстовой и мультимедийной информации.

## 4.3. Сервис FTP

Сервис FTP (File Transfer Protocol) используется для передачи файлов между компьютерами в глобальных и локальных сетях с использованием протокола TCP/IP. Данная технология также построена по технологии «клиент-сервер». На FTP-сервере размещаются файлы произвольного типа, которые могут быть скопированы[69] на компьютер-клиент. На FTP-сервере файлы, как правило, структурированы, т.е. расположены в каталогах, при этом клиент может «скачать» не все имеющиеся файлы с сервера, а только те, на которые у него имеется разрешение. Соответственно, и клиент может скопировать[70] на FTP-сервер свои файлы и целые каталоги (при наличии разрешений, предоставленных администратором FTP-сервера). Следовательно, для работы с FTP-сервером пользователю необходимо на этом сервере зарегистрироваться, т.е. ввести имя и пароль. В соответствии с введенным именем подключившемуся пользователю будет доступна, разумеется, не вся файловая система компьютера-сервера, а лишь определенный каталог. В Интернете имеются многочисленные публичные файловые архивы (программы, драйверы, музыкальные файлы, книги, документация и т.п.). Вся эта информация расположена на многочисленных FTP-серверах и предназначена для свободного скачивания, для доступа к данной информации пользователь должен зарегистрироваться на FTP-сервере под именем **anonymous** (анонимный пользователь), в качестве пароля обычно администраторы FTP-серверов просят ввести адрес своей электронной почты. С помощью протокола FTP обычно владельцы сайтов «закачивают» свою информацию на компьютер, осуществляющий web-хостинг. Разумеется, система безопасности web-хостера допускает каждому владельцу сайта управление только собственным сайтом![71]

Например, в Windows чтобы подключиться к FTP-узлу, следует запустить Internet Explorer и набрать в адресной строке **URL** вида ftp://имя_пользователя@сервер

**FTP-сервера**, как и web-сервера устанавливаются на компьютерах, имеющих круглосуточный доступ в Интернет и фиксированный IP-адрес. Программное обеспечение, необходимое для создания полноценного FTP-сервера входит в состав дистрибутива UNIX/Linux, на платформе Microsoft Windows, как уже отмечалось, следует использовать Internet Information Server (IIS).

**FTP-клиенты**. Поддержка **FTP-клиента** есть в каждой современной операционной системе. Например, в Microsoft Windows (любой современной версии) используется утилита командной строки ftp, для вызова данной утилиты следует перейти в режим командной строки и ввести ftp. Далее, используя встроенные команды этой утилиты (их можно узнать из документации по операционной системе или непосредственно из программы, введя команду **?** (помощь) можно подключиться к FTP-серверу, копировать файлы с сервера на свой компьютер или наоборот и т.п. Однако использование данной утилиты ввиду отсутствия привычного для большинства пользователей графического интерфейса весьма неудобно. Поэтому разработано достаточно большое количество FTP-клиентов (например, CuteFTP) либо возможности работы по протоколу ftp встроены в большинство программ работы с файлами (файловых менеджеров) и браузеров.

В качестве такого рода файловых менеджеров можно рекомендовать Windows Commander (или Total Commander), являющихся по своей сути развитием идей всем известного Norton Commander`a. Удобство использование данных файловых менеджеров в качестве FTP-клиентов заключается в том, для пользователя каталоги и файлы удаленного FTP-

[69] В Интернет - сообществе используют термин «скачены».
[70] Соответственно, используется термин «закачать».
[71] В качестве мер обеспечения безопасности является аутентификация владельца сайта по имени и паролю, а также (при необходимости) по IP-адресу компьютера-клиента, с которого происходит «закачка».

сервера размещаются на одном из окон файлового менеджера и пользователь может работать с удаленными файлами практически так же, как и с файлами на дисках собственного компьютера.

В качестве FTP-клиента использовать и Интернет-браузер (например, Internet Explorer). Например, для подключения в публичному FTP-серверу компании (например, company.ru) следует в адресной строке браузера ввести адрес в следующем формате fttp://ftp.company.ru. Очень часто пользователь, «путешествуя» по www-сайтам незаметно для себя попадает на такого рода адрес и может открыть или сохранить файл (например, драйвер) с публичного сервера.

## 4.4 Интернет - пейджеры

Электронная почта, несмотря на ее распространенность и общедоступность зачастую не может удовлетворить потребность бизнес – партнеров (пользователей Интернет) в оперативности связи. Очень часто при обсуждении вопросов возникает необходимость проведения «живого» общения (голосом по аналогии с обычным телефоном, а желательно – и иметь возможность видеть собеседника) и с возможностью передачи файлов – документов. Также программы-пейджеры используются в службах технической поддержки пользователей (аппаратуры, программного обеспечения).

Данные программы относятся к классу Интернет-пейджеров, представителями программ-пейджеров являются Windows Messenger, ICQ, Skype.

Принцип работы такого рода программ отличается от работы электронной почты. Если в электронной почте два компьютера общаются друг с другом через систему серверов электронной почты (разумеется, за исключением случая, когда получатель и отправитель почтовых сообщений обслуживается одним и тем же почтовым сервером), то в данном случае оба компьютера непосредственно общаются друг с другом. Такие программы называют «пиринговые» от термина “peer-to-peer”. Принцип действия пиринговых программ следующий. Первоначально пользователь должен запустить программу и ввести необходимые сведения о себе, как абоненте данной системы обмена информацией: имя (псевдоним или «ник»), пароль для последующего редактирования личных сведений и личные сведения, проверка которых не осуществляется и корректность их ввода полностью зависит от нового абонента. При каждом запуске, а как правило такие программы автоматически запускаются вместе с операционной системы, программа определяет, подключен ли данный компьютер к Интернет, и если подключен – то связывается с сервером данной пиринговой системы и регистрируется на нем, т.е. сообщает IP-адрес компьютера. Соответственно, сервер пиринговой системы отмечает факт появления активного абонента и его статус (включен). Если другой абонент пиринговой системы захочет вызвать нашего абонента, то сервер передаст ему IP-адрес абонента и этот компьютер сможет непосредственно к нему обратиться. В дальнейшем эти компьютеры смогут вести разговор уже в режиме «точка-точка» без помощи сервера.

В таких системах существуют все дополнительные возможности и сервисы, предлагаемые операторами обычной телефонной связи: абонент видит имя (вернее, псевдоним) вызывающего абонента, может отказаться от разговора, составить адресную книгу, «черный список» нежелательных абонентов, устанавливать статус программы: «свободен для разговора», «нет на месте» и т.п.

**Программа Windows Messenger** входит в состав Microsoft Windows XP и позволяет общаться в режиме реального времени с другими пользователями службы .NET Messenger Service. С помощью программы Windows Messenger можно выполнять следующие действия.

- «звонить» на компьютер, вести голосовую или видеобеседу[72];

[72] Компьютер должен быть оборудован мультимедийным оборудованием: динамиками, микрофоном, а для видеобеседы – дополнительно видеокамерой. Все из перечисленных устройств входят в большинство современных ноутбуков и могут быть легко подключены к настольным ПК.

- создать список контактов, состоящий из бизнес - партнеров, коллег по работе, друзей и т.п.;
- видеть, находятся ли ваши контакты в сети и доступны ли они, а также отправлять и принимать текстовые сообщения;
- отправлять по своим контактам файлы-документы (в том числе – графические и музыкальные файлы);
- использовать рукописный ввод для написания мгновенных сообщений (требуется операционная система Windows XP Tablet PC Edition);
- пригласить кого-нибудь посмотреть программу, установленную на вашем компьютере, или вместе использовать средство «Доска»;
- использовать средство «Удаленный помощник» для привлечения посторонней помощи в устранении неполадок в компьютере;

**Программа ICQ**[73] является популярным Интернет-пейджером. Саму программу можно бесплатно скачать с сайта www.icq.com , при установке и первом запуске программы и регистрации пользователю будет назначен уникальный идентификатор ICQ UIN, который и будет являться именем (псевдонимом) абонента в ICQ.

Далее пользователь может выбрать необходимый режим работы;

- голосовое общение с собеседником;
- chat (беседу), в данном режиме «собеседники» обмениваются текстовыми сообщениями;
- посылку сообщений, в данном режиме «собеседник» увидит сообщения при запуске программы ICQ;
- передачу файла.

**Программа Skype™** является одним из самых совершенных Интернет-пейджеров. Программа обеспечивает сервис VoIP[74]. Саму программу можно бесплатно получить с сайта www.skype.com. Программа является мультиязычной и поддерживает практически все языки мира, интересно, что первоначально сайт предлагает скачать версию программы на языке той страны, с территории которой обратились к сайту программы, а затем (при необходимости) можно выбрать наиболее удобный язык меню и диалоговых окон программы, в том числе – и русский.

С целью обеспечения безопасности ведения переговоров программа Skype осуществляет шифрование передаваемой информации.

Программа Skype позволяет бесплатно[75] выполнять следующие действия:

- «звонить» на компьютер, вести голосовую беседу или видеобеседу (при наличии соответствующего мультимедийного оборудования);
- организовывать конференции, т.е. одновременный разговор трех и более участников;
- создавать список контактов (адресную книгу);
- устанавливать свой статус («в сети», «не в сети», «нет на месте», «не беспокоить» и и.д.).

Кроме перечисленных функций (во многом совпадающих с возможностями Windows Messenger) существуют и коммерческие возможности программы Skype – это возможность звонить на обычный (стационарный или мобильный) телефон практически в любой стране мира (эта функция называется Skype Out) и принимать звонки на телефон, произведенные из системы Skype (соответственно – Skype In). Считается, что с использованием Skype Out и Skype In можно значительно дешевле вести международные телефонные переговоры. Для активизации данных функций необходимо внести определенную сумму на счет компании Skype Кредит, пользователю будет открыт «бюджет», которым можно

[73] Аббревиатура расшифровывается следующим образом - I Seek You – перевод с англ. - Я Ищу Тебя
[74] Voice-over-IP («звук поверх IP») – технология передачи звуковой информации с помощью протокола IP.
[75] Разумеется, за трафик Интернет-провайдеру необходимо будет заплатить.

пользоваться для реализации платных услуг. В России эта возможность Skype не пользуется большой популярностью ввиду того, что внесение денежных средств на Skype Кредит сопровождается достаточно большими расходами на оформление этой операции, но в остальном – программа Skype уверенно занимает первое место в рейтинге Интернет-пейджеров[76].

## 4.5. Организация доступа в Интернет корпоративных сетей

Для эффективного использования Интернет-технологий компьютеры, входящие в состав информационной системы компании, должны быть подключены к Интернет по высокоскоростному надежному каналу. Подключение к Интернет и предоставление Интернет-услуг обеспечивают компании – провайдеры[77].

Для доступа в Интернет корпоративных сетей используются следующие технологии:

- подключение по выделенной линии (медной паре проводов);
- подключение по волоконно-оптической линии связи;
- подключение по радиоканалу;
- использование услуг, предлагаемых операторами мобильной связи;
- использование услуг, предлагаемых операторами кабельного телевидения.

**Подключение по выделенной линии**. В качестве выделенной линии используется одна (как правило) или две пары проводов. Выделенная линия обычно организуется оператором стационарной телефонной связи по отдельному договору. Выделенная линия должна соединять место нахождения компании (как правило – помещение, в котором расположены сервера) с ближайшей «точкой присутствия» провайдера. На обоих концах выделенной линии устанавливается специальное оборудование - модемы[78]. Данные модемы принципиально отличаются от модемов, используемых для подключения к Интернет «домашних» компьютеров, т.к. такие модемы предназначены для работы на коммутируемых телефонных линиях связи и не могут обеспечить скорость передачи данных выше 56кбит/с.

Для подключения по выделенной линии используются следующие технологии:

1. **ADSL** – Asymmetric Digital Subscriber Line (ассиметричная линия передачи данных). Для организации такого подключения провайдеры организовывают на автоматической телефонной станции (АТС) клиента «точку присутствия» и устанавливают ADSL-модемы. Соответственно, любой клиент данной АТС может во взаимодействии с провайдером и оператором телефонной связи установить на своей стороне тоже ADSL-модем и организовать «выделенную» линию связи. Строго говоря, данная линия связи не будет «выделенной», поскольку ее никто «не выделял», а она существовала (и существует) для обеспечения обычной телефонной связи. Наличие двух ADSL-модемов практически не препятствует работе обычного телефонного оборудования[79], при этом компьютер клиента оказывается подключенным к Интернет (без необходимости производить набор номера, так называемый «дозвон». Принципиальной особенностью такой технологии является ее «несимметричность», т.е. скорость информационного потока от провайдера многократно превышает скорость передачи данных к провайдеру. Данное обстоятельство практически не препятствует работе с www-сайтами, но может существенно затруднить пе-

[76] Разработаны и появились в продаже специальные «скайп-телефоны». Данная телефонная трубка содержит программное обеспечение, в том числе - идентификатор пользователя, и может быть подключена к USB-порту компьютера.

[77] Провайдер (англ. Provider) - поставщики удаленных подключений к Интернет, предоставляющие услуги конечным пользователям. Используется также аббревиатура ISP (Internet Service Provider).

[78] Модем (Modem) – оконечное устройство компьютера, позволяющий выполнять передачу цифровых данных с помощью аналоговых каналов передачи данных, например, телефонных линий.

[79] Хотя абонент должен подписать обязательство «не жаловаться» на качество телефонной связи!

редачу данных по электронной почте, работе Интернет - пейджера. Скорость передачи данных существенно зависит от сопротивления телефонной линии и, следовательно, от расстояния до АТС. При средних расстояниях достижимы входящие скорости от 500 кб/с до 5 Мб/с, исходящие скорости в 4-8 раз меньше. Несмотря за преимущества ADSL-модемов такой способ подключения к Интернет практически не используется в корпоративном секторе, а применяется исключительно в SOHO-сегменте.

2. **xDSL-модемы** для работы на выделенной линии. Использование профессиональных кабельных xDSL модемов позволяет получить симметричный цифровой канал связи с провайдером, обеспечивающий скорость передачи данных от 1 до 10Мбит/с.

Общим недостатком выделенной линии является недостаточно высокая надежность и зависимость качества связи от состояния системы коммуникаций оператора телефонной связи.

**Подключение по волоконно-оптической линии связи** позволяет получить высококачественный доступ в Интернет со скоростью до 1Гб/с, недостатком данной технологии является высокая стоимость прокладки оптоволоконного кабеля.

**Подключение по радиоканалу**. Беспроводная связь, или связь по радиоканалу, сегодня используется и для построения магистралей (радиорелейные линии), и для создания локальных сетей, и для подключения удаленных абонентов к сетям и магистралям разного типа. Весьма динамично развивается в последние годы стандарт беспроводной связи Radio Ethernet. Изначально он предназначался для построения локальных беспроводных сетей, но сегодня все активнее используется для подключения удаленных абонентов к магистралям. С его помощью решается проблема "последней мили" (правда, в отдельных случаях эта "миля" может составлять от 100 м до 25 км). Radio Ethernet сейчас обеспечивает пропускную способность до 54 Мбит/с и позволяет создавать защищенные беспроводные каналы для передачи мультимедийной информации. Данная технология соответствует стандарту 802.11, разработанному Международным институтом инженеров по электротехнике и радиоэлектронике (IEEE) в 1997 году и описывающему протоколы, которые позволяют организовать локальные беспроводные сети (Wireless Local Aria Network, WLAN).

Передача сигналов производится на частоте 2,4 ГГц, данный радиосигнал распространяется практически по прямой, поэтому необходимо выполнить условие «прямой видимости» между провайдером и клиентом. Система состоит из двух комплектов, состоящих из параболической антенны и усилительного устройства, один комплект устанавливается у провайдера, второй – у клиента. Если точка антенна провайдера вынесена на специальную мачту, а клиент расположен в высотном здании, то можно получить надежную и качественную связь. Преимущество подключения по радиоканалу заключается также и в отсутствии «невозвратных» капитальных затрат. Дело в том, что затраты, связанные с прокладкой медного или оптического кабеля, как правило, не могут быть компенсированы, если наша компания будет вынуждена отказаться от услуг данного провайдера или сменит место своего расположения. Можно считать, что деньги на прокладку кабеля, как и сам кабель «зарыты в землю», в то время как антенну системы радиодоступа всегда можно демонтировать и использовать на новом месте. К недостаткам данной технологии доступа в Интернет следует отнести:

- необходимость согласования использования частот и последующая регистрация аппаратуры беспроводной сети в Государственной комиссии по радиочастотам и Федеральном агентстве связи;
- возможные перерывы в связи при наличии сильных индустриальных помех, неблагоприятных атмосферных условиях и т.п.

**Операторы мобильной связи**, работающие по протоколам CDMA, предлагают услугу Sky Turbo – услуга высокоскоростной передачи данных и работы в Интернет в мо-

бильном режиме на основе технологии EV-DO в сети стандарта IMT-MC-450 . скорость в сети «Скай Линк» составляет:

- максимально возможная скорость – до 2,4 Мб/с
- средняя скорость – 600 Кбит/с

Данная услуга, в основном, востребована SOHO-сегментом.

**Операторы кабельного телевидения** предоставляют услуги Интернет с использованием специальных модемов. Скорость доступа достигает 1Мб/с. Такой вид доступа также в основном востребован SOHO-сегментом и может служить альтернативой ADSL-модемам.

## 4.6. Сайты

### 4.6.1. Назначение сайтов в информационных системах

Типичные цели, ставящиеся перед сайтом:

- поддержка и продвижение имиджа компании в Интернет (имиджевая составляющая)
- предоставление наиболее подробной информации об услугах фирмы (информационная составляющая)
- реклама фирмы в Интернет (рекламная составляющая)г) Привлечение новых клиентов и партнеров, продажа услуг и товаров с сайта компании (коммерческая составляющая)

Рассмотрим каждый из этих пунктов более подробно:

**Имиджевая составляющая**. XXI век – век информационных технологий. Громадное количество людей в России и за рубежом используют Интернет для бизнеса. На визитке уважающей себя фирмы помимо адреса и телефона всегда присутствует адрес сайта, на котором можно ознакомиться с услугами компании и email. Сайт в Интернет для нормальной компании сродни офису, а компания без офиса – это просто несолидно не говоря уже о том, что вряд ли о такой фирме можно сказать хотя бы что-то положительное. Наличие у компании сайта – это поддержка имиджа фирмы. Это говорит о том, что компания идет в ногу со временем и использует все достижения технического прогресса. Фирма без сайта всегда имеет меньший вес в глазах потенциального клиента и эта тенденция неуклонно растет.

**Информационная составляющая**. Новым клиентам приходится рассказывать одну и ту же информацию об услугах и тонкостях работы фирмы. Сейчас часто можно услышать: “Более подробную информацию о нашей компании, предлагаемых товарах и услугах Вы можете получить на нашем сайте www.имя_фирмы.ru . Адрес нашего сайта указан на визитной карточке”. Информация многих компаний периодически меняется, о новых изменениях нужно информировать растущее число клиентов и зачастую это превращается в обузу, если не использовать сайт. На сайте удобно отображать все последние изменения компании, новости фирмы, изменения цен, услуг, условий и т. д., тогда каждый текущий клиент легко может посмотреть всю новую информацию на сайте. Работа с клиентской базой упрощается и становится дешевле.

**Рекламная составляющая.** Все большее количество компаний вкладывают деньги в Интернет рекламу и это неудивительно, ведь это самая дешевая реклама, которая позволяет охватить огромную аудиторию и получить максимальную отдачу. Оговорюсь, что реклама в Интернет выгодна не всем компаниям, это надо понимать и предварительно проконсультироваться в агенстве Интернет-рекламы. Интернет позволяет донести большому числу людей информацию (рекламу) о товарах и услугах компании и это огромный плюс.

**Коммерческая составляющая.** С сайта можно продавать товары и услуги компании. Громадное количество потенциальных покупателей (Россия и весь мир) делают Интернет привлекательной торговой площадкой. Непросто наладить свой бизнес в Интернет,

но это очень выгодно. Знаменитые Интернет-магазины России PORTA.RU, OZON.RU, BOOKS.RU, уже многие годы успешно продают товары покупателям всей России. Для наглядности отмечу, что посещаемость PORTA.RU составляет около 20.000 посетителей в сутки! Вряд ли физический офис выдержит такое количество покупателей. Вторым несомненным плюсом является автоматизация торговли через Интернет. Все операции по выписке документов, счетов, записи информации в базу данных происходят в автоматическом режиме и не требуют большого количества персонала.

Сайт (web-сайт, www-страница) компании, организации любой формы собственности и рода деятельности призван либо привлечь внимание потенциальных покупателей (клиентов) к данной компании, либо дать возможность получить посетителю сайта, а также получить необходимую и объективную информацию. Как правило, на сайте коммерческой компании представлена продукция фирмы, ее характеристики, цены на выпускаемую продукцию и оказываемые услуги, справочная техническая информация, советы покупателю, сопроводительные графические рисунки, юридический адрес, почтовый адрес, схема проезда, контактная информация, банковские реквизиты, сведения об имеющихся вакансиях.

Сайт способствует увеличению притока покупателей при одновременном снижении расходов на рекламу. Сайт должен способствовать также привлечению деловых партнеров.

### 4.6.2. Размещение сайтов (web-хостинг)

**Web-хостинг**. Размещение сайтов на web-серверах Интернет носит название web-hosting (web-хостинга). Как правило, роль компьютера-сервера, выполняющего функции web-хостинга, совмещены с компьютером, являющимся web-сервером.

Возможны следующие варианты реализации web-хостинга:

- использование собственного (корпоративного) web-сервера для размещения Интернет-сайта компании;
- использование web-сервера провайдера;
- использование специализированного коммерческого web-хостинга;
- использование бесплатного web-хостинга.

Использование для web-хостинга собственного сервера компании имеет определенные достоинства, а именно: упрощена процедура обновления информации на сайте, отсутствуют затраты на хостинг, однако имеются и существенные недостатки: компании необходимо иметь компьютер (или даже несколько компьютеров) с круглосуточным и надежным доступом в Интернет и фиксированным IP-адресом, необходимо иметь собственную службу администрирования web-сервера, трафик, вызванный посещением корпоративного сайта будет вынуждена оплачивать наша компания. Как правило, такой вид хостинга используют крупные компании, имеющие развитую IT-инфраструктуру.

Использование web-сервера провайдера представляет интерес для многих средних и мелких компаний, поскольку большинство провайдеров предлагают для корпоративных клиентов бесплатно (вернее – в составе основного пакета услуг) web-хостинг. В этом случае все проблемы, связанные с безопасностью сайта и трафиком, вызванным его просмотром, решает web-хостер, т.е. провайдер. Обновление сайта выполняет его владелец, т.е. наша компания по протоколу FTP. Недостатком данного вида хостинга является то обстоятельство, что провайдеры не всегда являются специализированными web-хостерами и, следовательно, программное обеспечение, используемое в web-серверах зачастую не в полной мере может удовлетворить требовательных клиентов, например, может отсутствовать поддержка активных форм, возможность работы с базами данных и т.п.

Использование специализированных web-хостеров позволит создать самые современные сайты, обновление сайта, как и в варианте с хостером - провайдером, выполняет владелец сайта по протоколу FTP. В настоящее время в России имеется достаточно много хорошо себя зарекомендовавших компаний, предлагающих web-хостинг. Необходимо с

компанией – хостером заключить договор, в котором должна быть указана ответственность сторон за ненадлежащее исполнение своих обязанностей.

Бесплатный web-хостинг может использован небольшими компаниями, индивидуальными предпринимателями и т.п. на так называемых «бесплатных ресурсах». К ним относятся www.narod.ru, www.mail.ru и ряд других. Имя сайта в этих случаях будет следующим www.company.narod.ru , что в определенным образом снизит его представительские функции. Явными недостатками данного вида web-хостинга (кроме имени сайта) будут, во-первых, наличие рекламы хостера на нашем сайте[80], во-вторых, - отсутствие явного оформленного договора с хостером, т.е. в случае некачественной работы web-сервера будет невозможно предъявить какие-либо претензии, и в-третьих – отсутствие гарантий безопасности размещения информации о нашей компании на web-сервере.

### 4.6.3. Основные понятия HTML

HyperText Markup Language (HTML) является стандартным языком, предназначенным для создания гипертекстовых документов в среде WEB. HTML-документы могут просматриваться различными типами WEB-браузеров. Когда документ создан с использованием HTML, WEB-браузер может интерпретировать HTML для выделения различных элементов документа и первичной их обработки. Использование HTML позволяет форматировать документы для их представления с использованием шрифтов, линий и других графических элементов на любой системе, их просматривающей.

Большинство документов имеют стандартные элементы, такие, как заголовок, параграфы или списки. Используя тэги HTML вы можете обозначать данные элементы, обеспечивая WEB-броузеры минимальной информацией для отображения данных элементов, сохраняя в целом общую структуру и информационную полноту документов. Для чтения (просмотра) HTML-документа необходима программа - WEB-браузер, который и интерпретирует тэги HTML и воспроизводит на экране документ в виде, который ему придает автор. Фактически HTML-документ является «электронным» документом и в основном ориентирован для просмотра на экране монитора. Как правило, «читатель» данного документа может (в зависимости от размеров экрана и его разрешающей способности и своих личных пристрастий) изменять размер шрифтов, использовать полосу прокрутки и т.п. Разумеется, автор HTML-документа, создавая документ, подразумевал определенный размер экрана, создавая для читателя наиболее комфортные условия работы. Основное преимущество HTML как раз и заключается в том, что один и тот же документ может быть просмотрен на WEB-браузерах различных типов, с использованием различных операционных систем и аппаратных платформ.

Основой языка HTML являются элементы разметки или «тэги»[81]. Тэги определяют, как будут выглядеть текст, табличные формы, графические объекты странице, и как они будут располагаться относительно друг друга.

HTML-документы могут быть созданы при помощи любого текстового редактора (например, Блокнота Microsoft Windows) или специализированных HTML-редакторов. Собственно говоря, именно при разработке HTML-документа с помощью простого текстового редактора автор и должен знать язык HTML. Для «облегчения» данной работы были созданы более сложные редакторы, позволяющие работать в режиме WYSIWYG[82] т.е. разрабатывать документ и не думать (казалось бы!) о тэгах. Однако знание основ языка HTML считается необходимым условием создания любых, даже самых сложных доку-

---

[80] Это и будет платой за хостинг.

[81] Tag – (англ.) признак

[82] (произносится как *визивиг*) — сокращение для *What You See Is What You Get* (англ. *что видишь, то и получишь*). Применяется для описания способа редактирования, при котором редактируемый материал в процессе редактирования выглядит в точности так же, как и конечный результат. Обычно этот термин используется в отношении текстовых процессоров, но может применяться и к другим типам прикладных программ

ментов с помощью самых совершенных редакторов, например, Microsoft Front Page, Macromedia Dreamweaver и др[83].

HTML-тэги могут быть условно разделены на две категории:

- тэги, определяющие, как будет отображаться WEB-браузером тело документа в целом
- тэги, описывающие общие свойства документа, такие как заголовок или автор документа.

Все тэги HTML начинаются с "<" (левой угловой скобки) и заканчиваются символом ">" (правой угловой скобки). В скобках записывается сам «признак» - команда для разметки страницы. Как правило, существуют стартовый и завершающий тэг. Завершающий тэг выглядит также, как стартовый, и отличается от него прямым слэшем перед текстом внутри угловых скобок.

Для примера приведем тэги заголовка, определяющие текст, находящийся внутри стартового и завершающего тэга и описывающий заголовок документа:

<TITLE> Заголовок документа </TITLE>

Завершающий тэг выглядит также, как стартовый, и отличается от него прямым слэшем перед текстом внутри угловых скобок. В данном примере тэг <TITLE> говорит WEB-броузеру об использовании формата заголовка, а тэг </TITLE> - о завершении текста заголовка.

Некоторые тэги, такие, как <P> (тэг, определяющий абзац), не требуют завершающего тэга, но его использование придает исходному тексту документа улучшенную читаемость и структурируемость. В языке HTML регистр символов, описывающих тэг, не распознается, следовательно тэги <TITLE>, <Title> и <title> эквивалентны.

Дополнительные пробелы, символы табуляции и возврата каретки, добавленные в исходный текст HTML-документа для его лучшей читаемости, будут проигнорированы WEB-браузером при интерпретации документа. HTML-документ может включать вышеописанные элементы только если они помещены внутрь тэгов <PRE> и </PRE>.

Как отмечалось, **Тег** - оформленная единица HTML-кода. Например, HEAD, FONT ..., BODY, HTML и так далее. Теги бывают начальными (открывающими) и конечными (закрывающими, начинающимися со знака "/"). Например, вышеуказанным тегам соответствуют закрывающие теги /HEAD, /FONT, /BODY, /HTML.

**Элемент** - понятие, введенное для удобства. Например, элемент HEAD состоит из двух тегов - открывающего HEAD и закрывающего /HEAD. Следовательно, элемент - более емкое понятие, обозначающее пару тегов и участок документа между тегами, на который распространяется их влияние

HTML-тэги могут быть условно разделены на две категории:

- тэги, определяющие, как будет отображаться WEB-браузером тело документа в целом
- тэги, описывающие общие свойства документа, такие как заголовок или автор документа

Основное преимущество HTML заключается в том, что документ может быть просмотрен на WEB-браузерах различных типов и на различных платформах.

HTML-документы могут быть созданы при помощи любого текстового редактора или специализированных HTML-редакторов и конвертеров. Выбор редактора, который будет использоваться для создания HTML-документов, зависит исключительно от понятия удобства и личных пристрастий каждого автора.

Все тэги HTML начинаются с "<" (левой угловой скобки) и заканчиваются символом ">" (правой угловой скобки). Как правило, существует стартовый тэг и завершающий тэг. Для примера приведем тэги заголовка, определяющие текст, находящийся внутри стартового и завершающего тэга и описывающий заголовок документа:

[83] Все перечисленные HTML-редакторы имеют возможность вывести в специальном окне содержимое создаваемого документа в виде тэгов и производить в данном окне редактирование.

<TITLE> Заголовок документа </TITLE>

Завершающий тэг выглядит также, как стартовый, и отличается от него прямым слэшем перед текстом внутри угловых скобок. В данном примере тэг <TITLE> говорит WEB-браузеру об использовании формата заголовка, а тэг </TITLE> - о завершении текста заголовка.

Некоторые тэги, такие, как <P> (тэг, определяющий абзац), не требуют завершающего тэга, но его использование придает исходному тексту документа улучшенную читаемость и структурируемость.

HTML не реагирует на регистр символов, описывающих тэг, и приведенный ранее пример может выглядеть следующим образом:

<title> Заголовок документа </title>

Дополнительные пробелы, символы табуляции и возврата каретки, добавленные в исходный текст HTML-документа для его лучшей читаемости, будут проигнорированы WEB-браузером при интерпретации документа. HTML-документ может включать вышеописанные элементы только если они помещены внутрь тэгов <PRE> и </PRE>. Более подробно о тэгах <PRE> будет написано ниже.

Когда WEB-браузер получает документ, он определяет, как документ должен быть интерпретирован. Самый первый тэг, который встречается в документе, должен быть тэгом <HTML>. Данный тэг сообщает WEB-браузеру, что ваш документ написан с использованием HTML. Минимальный HTML-документ будет выглядеть так:

<HTML> ...тело документа... </HTML>

Заголовочная часть документа <HEAD>

Тэг заголовочной части документа должен быть использован сразу после тэга <HTML> и более нигде в теле документа. Данный тэг представляет из себя общее описание документа. Избегайте размещать какой-либо текст внутри тэга <HEAD>. Стартовый тэг <HEAD> помещается непосредственно перед тэгом <TITLE> и другими тэгами, описывающими документ, а завершающий тэг </HEAD> размещается сразу после окончания описания документа. Например:

<HTML> <HEAD>

<TITLE> Список сотрудников </TITLE> </HEAD> ...

Стартовые и завершающие тэги типа <HTML>, <HEAD> и <BODY> необязательны. Но настоятельно рекомендуется их использовать, поскольку использование данных тэгов позволяет WEB-браузеру уверенно разделить заголовочную часть документа и непосредственно смысловую часть.

Заголовок документа <TITLE>

Большинство WEB-браузеров отображают содержимое тэга <TITLE> в заголовке окна, содержащего документ и в файле закладок, если он поддерживается WEB-браузером. Заголовок, ограниченный тэгами <TITLE> и </TITLE>, размещается внутри <HEAD>-тэгов, как показано выше на примере. Заголовок документа не появляется при отображении самого документа в окне.

**Комментарии**. Как любой язык, HTML позволяет вставлять в тело документа комментарии, которые сохраняются при передаче документа по сети, но не отображаются броузером. Синтаксис комментария:

```
<!-- Это комментарий -->
```

Комментарии могут встречаться в документе где угодно и в любом количестве.

**Тэги тела документа**. Тэги тела документа идентифицируют отображаемые в окне компоненты HTML-документа. Тело документа может содержать ссылки на другие документы, текст и другую форматированную информацию.

**Тело документа** <BODY>

Тело документа должно находиться между тэгами <BODY> и </BODY>. Это та часть документа, которая отображается как текстовая и графическая (смысловая) информация вашего документа.

**Уровни заголовков** <Hx>

Когда пишется HTML-документ, текст структурно делится на просто текст, заголовки частей текста, заголовки более высокого уровня и т.д. Первый уровень заголовков (самый большой) обозначается цифрой 1, следующий - 2, и т.д. Большинство браузеров поддерживает интерпретацию шести уровней заголовков, определяя каждому из них собственный стиль. Заголовки выше шестого уровня не являются стандартом и могут не поддерживаться браузером. Заголовок самого верхнего уровня имеет признак "1". Синтаксис заголовка уровня 1 следующий:

```
<H1> Заголовок первого уровня </H1>
```

Заголовки другого уровня могут быть представлены в общем случае так:

```
<Hx> Заголовок x-го уровня </Hx>
```

где x - цифра от 1 до 6, определяющая уровень заголовка.

**Тэг абзаца** <P>

В отличии от большинства текстовых процессоров, в HTML-документе обычно игнорируются символы возврата каретки. Физический разрыв абзаца может находиться в любом месте исходного текста документа (для удобства его читаемости). Однако броузер разделяет абзацы только при наличии тэга <P>. Если вы не разделите абзацы тэгом <P>, ваш документ будет выглядеть как один большой абзац.

Дополнительные параметры тэга <P>:

```
<P ALIGN=left|center|right>
```

позволяют выравнивать абзац по левому краю, центру и правому краю соответственно.

Центрирование элементов документа

Можно центрировать все элементы документа в окне браузера. Для этого можно использовать тэг <CENTER>.

Все элементы между тэгами `<CENTER>` и `</CENTER>`
будут находиться в центре окна

**Тэг преформатирования** <PRE>

Тэг преформатирования, <PRE>, позволяет представлять текст со специфическим форматированием на экране. Предварительно сформатированный текст заканчивается завершающим тэгом </PRE>. Внутри предварительно сформатированного текста разрешается использовать:

- перевод строки

- символы табуляции (сдвиг на 8 символов вправо)
- непропорциональный шрифт, устанавливаемый браузером

Использование тэгов, определяющих формат абзаца, таких как <Hx> или <ADDRESS>, будет игнорироваться браузером при помещении их между тэгами <PRE> и </PRE>.

Далее идет несколько более подробный пример, собранный из предыдущих:

```
<HTML>
<HEAD>
<TITLE> Список сотрудников </TITLE>
</HEAD>
<BODY>
<H2> Список сотрудников нашей фирмы </H2>
<H3> Составлено : 30 июля 2006 года </H3>
Данный список содержит фамилии, имена и отчества
всех сотрудников нашей компании. <P>
Список может быть использован только в служебных целях. <P>
</BODY>
</HTML>
```

Вот, что вы увидите на экране браузера:

**Список сотрудников нашей фирмы**
**Составлено : 30 июля 2006 года**

Данный список содержит фамилии, имена и отчества всех сотрудников нашей компании.

Список может быть использован только в служебных целях.

Заголовок "Список сотрудников" не отображен браузером как часть документа. Он появится в заголовке окна браузера.

**Разрыв строки** <BR>

Тэг <BR> извещает браузер о разрыве строки. Наилучший пример использования данного тэга - форматированный адрес или любая другая последовательность строк, где браузер должен отображать их одну под другой. Например:

```
Александр Полонский <BR>
пр. Просвещения, <BR>
д.85, офис 415 <BR>
```

## Список базовых тэгов HTML

| Стартовый | Завершающий | Описание |
|---|---|---|
| <HTML> | </HTML> | Обозначение HTML-документа |
| <HEAD> | </HEAD> | Заголовочная часть документа |
| <TITLE> | </TITLE> | Заголовок документа |
| <BODY> | </BODY> | Тело документа |
| <H1> | </H1> | Заголовок абзаца первого уровня |
| <H2> | </H2> | Заголовок абзаца второго уровня |
| <H3> | </H3> | Заголовок абзаца третьего уровня |
| <H4> | </H4> | Заголовок абзаца четвертого уровня |

| | | |
|---|---|---|
| <H5> | </H5> | Заголовок абзаца пятого уровня |
| <H6> | </H6> | Заголовок абзаца шестого уровня |
| <P> | </P> | Абзац |
| <PRE> | </PRE> | Уже отформатированный текст |
| <BR> | | Перевод строки без конца абзаца |
| <BLOCKQUOTE> | </BLOCKQUOTE> | Цитата |

***Контрольные вопросы***

1. Перечислите задачи, решаемые системами электронной почты
2. По какому принципу выбирается (назначается) адрес электронной почты
3. Программы-клиенты электронной почты
4. Какие протоколы используются для отправки и получения сообщений электронной почты?
5. Назначение www-сайта компании
6. Приведите основные тэги языка HTML, как расшифровывается данная аббревиатура?
7. Задачи, решаемые Интернет-пейджерами?
8. Приведите наиболее распространенные Интернет-пейджеры.
9. Как организовать доступ в Интернет для корпоративной сети (более 10 компьютеров) с использованием одного публичного IP-адреса?

# 5. Безопасность информационных систем

С развитием информационных технологий на основе внедрения локальных и глобальных сетей вопросы обеспечения безопасности обрабатываемой информации приобретают все большую актуальность. Обеспечение безопасности автоматизированных систем является одной из главных задач для любой компании, так как от сохранения локальных или корпоративных информационных ресурсов во многом зависит скорость принятия решений и эффективность работы компании.

Задачи обеспечения информационной безопасности привлекают уже внимание не только руководителей предприятий, программистов, администраторов безопасности и других специалистов в области компьютерных систем, но и обычных пользователей. Безопасность обработки информации обеспечивается различными мерами: физическими, организационными, техническими и другими.

В настоящем пособии рассматриваются вопросы защиты информации с помощью технических (аппаратно-программных) мер защиты, которые основаны на использовании различных электронных устройств и специальных программ, входящих в состав компьютерных систем и выполняющих (самостоятельно или вместе с другими средствами) функции защиты.

## 5.1. Общие положения

В настоящее время автоматизированные системы (АС), построенные на базе различных средств вычислительной техники, являются основным инструментом накопления, хранения и обработки различной информации. Современные компьютеры могут обрабатывать текст, звук, графику и другие виды информации. Различные виды информации в АС представлены в виде специальным образом закодированных данных - файлов различных форматов, которые в совокупности образуют информационное обеспечение АС.

Для обработки этих данных и управления работой в ходе информационно-вычислительного процесса в каждой АС имеется набор программ, которые образуют про-

граммное обеспечение. Совокупность информационного и программного обеспечения образует информационно-программное обеспечение (ИПО) автоматизированной системы.

Широкое распространение и повсеместное применение АС привело к созданию сетей, и АС стали удобным и мощным средством для организации обмена различной информацией - текстовой, звуковой, графической, мультимедийной и др. В составе ИПО АС появились компоненты, обеспечивающие реализацию различных сетевых сервисов - электронной почты, обмена различными данными в реальном масштабе времени, доступа к сетевым базам данных и т. п. Вместе с тем возрастает количество случаев получения ущерба в связи с применением АС для обработки различных видов информации.

Под ***угрозой*** АС будем понимать потенциально возможное событие действие или процесс, которое посредством воздействия на компоненты АС может привести к нанесению ущерба как техническим средствам так и информационно-программному обеспечению АС. Обычно различают угрозы случайного и преднамеренного характера. К случайным угрозам относятся угрозы потерь данных и нарушений работоспособности АС, возникающие вследствие:

- ошибок и сбоев в работе программных и технических средств АС;
- стихийных бедствий;
- ошибок в работе пользователей и т.п

Угрозы преднамеренного характера исходят со стороны нарушителей (злоумышленников), т. е. лиц, которые сознательно стремятся получить несанкционированный доступ к ресурсам АС или нарушить ее работоспособность. К такого рода угрозам можно отнести:

- внесение изменений в финансовые документы;
- незаконное копирование компонентов ИПО;
- нарушение работоспособности АС с целью нанесения ущерба компании.

Под ***уязвимостью*** АС будем понимать любую характеристику или свойство АС, использование которой нарушителем может привести к реализации угрозы.

Под ***атакой*** будем понимать любое действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей АС.

Основными факторами, способствующими повышению уязвимости АС являются:

- постоянное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью АС;
- возрастание степени автоматизации обработки данных вАС;
- интеграция в единых базах данных информации больших объемов, различного назначения и различной принадлежности;
- усложнение режимов функционирования технических средств АС и увеличивающаяся сложность программного обеспечения;
- долговременное хранение данных на внешних носителях информации;
- постоянное расширение круга пользователей, имеющих доступ к ресурсам АС;
- возрастающая важность и ответственность решений, принимаемых на основе автоматизированной обработки данных в АС;
- большая концентрация и широкая территориальная расположения АС;
- повышение интенсивности циркуляции информации между АС, объединенными в сети, расположенными друг от друга, как на малом, так и на большом расстоянии.

Эти и другие факторы позволяют сделать вывод, что по мере развития средств вычислительной техники, уязвимость АС постоянно возрастает.

В связи с этим проблема защиты информационно - программного обеспечения автоматизированных систем стала одной из главных проблем в области автоматизированной обработки данных.

## 5.2. Базовые угрозы информации

Наиболее ценным и критичным ресурсом АС является информационное обеспечение (ИО). В общем случае имеется широкий спектр угроз информационному обеспечению от различных стихийных бедствий до неправильных действий законных пользователей. Все эти многочисленные угрозы можно свести к нескольким базовым угрозам.

К хранящимся в АС данным в общем случае возможны только два вида доступа: чтение или запись. Этот доступ может быть санкционированным - осуществляться по желанию владельца соответствующего информационного ресурса и в соответствии с установленными им правилами разграничения доступа к нему, или несанкционированным - в противном случае.

Доступ пользователей к компонентам ИО, хранящимся в АС, возможен только с помощью программ. Для организации доступа пользователя к ИО обычно используется несколько различных программ. Например, для работы пользователя с некоторым текстовым файлом необходимо запустить на выполнение программу - текстовый редактор. В ходе выполнения своих функций эта программа будет вызывать и передавать управление различным программам операционной системы (осуществляющим ввод данных с клавиатуры, отображение данных на дисплее, ввод-вывод данных на магнитный диск и т.п.).

Совокупность программ, которая обеспечивает доступ пользователя к ИО будем называть системой доступа к информационному обеспечению. В общем случае эта система доступа может быть достаточно сложной, например, если информационный ресурс расположен на удаленной АС и доступ к нему осуществляется через телекоммуникационную сеть.

Если система доступа по каким-либо причинам перестанет функционировать, то оперативный доступ пользователя к ИО станет невозможен. Таким образом, можно выделить следующие три базовых угрозы:

- угроза несанкционированного чтения данных;
- угроза несанкционированной записи данных;
- угроза отказа в обслуживании.

***Угроза несанкционированного чтения данных*** - интересующие нарушителя файлы могут быть несанкционированно (в обход установленных правил разграничения доступа или вопреки желанию владельца) прочитаны (скопированы) с целью незаконного использования - ознакомления с текстовыми данными, прослушивания звуковых данных, просмотр графических данных, выполнения программных файлов и т.п. С этой базовой угрозой связаны:

- угроза нарушения конфиденциальности хранимой в АС информации;
- угроза несанкционированного использования и распространения программного обеспечения и ряд других аналогичных угроз.

У***гроза несанкционированной записи данных*** - файлы могут быть несанкционированно модифицированы или уничтожены. Несанкционированная модификация компонент ИПО может быть проведена с целью внедрения ложных данных в информационное обеспечение или изменения алгоритмов функционирования программ. С этой угрозой связаны:

- угрозы нарушения целостности и достоверности информации;
- угроза внедрения скрытых режимов функционирования программных систем;
- угроза отказа в обслуживании в ходе работы программных систем, и другие.

**Угроза отказа в обслуживании** (угроза нарушения работоспособности АС) - система доступа пользователя к ИО может перестать выполнять запросы пользователя по доступу к ИО (чтение или запись) или сделать время выполнения этих запросов неприемлемо большим. Эта угроза может возникать вследствие:

- ошибок, сбоев или отказов в работе программно-технических средств АС;

- несанкционированной модификации программ, образующих систему доступа пользователя к информационному обеспечению;
- поступлении слишком большого количества запросов на доступ к ИО со стороны пользователей и др.

Несмотря на использование различных систем защиты информации, в современных АС невозможно перекрыть все потенциально возможные каналы несанкционированного доступа к ее информационно-программным ресурсам.

## 5.3. Основные задачи систем защиты информации

В процессе обеспечения защиты информации, как правило, необходимо решать следующие комплексные задачи:

- создание системы органов, ответственных за защиту информации;
- разработка теоретико-методологической основы защиты информации;
- решение проблемы управления системой защиты информации и ее автоматизации;
- создание и совершенствование нормативно-правовой базы, регламентирующей решение различных задач защитыинформации;
- разработка и налаживание производства программно-технических средств защиты информации;
- организация подготовки специалистов по защите информации.

**Создание системы органов, ответственных за защиту информации**. На различных уровнях - общегосударственном, региональном (ведомственном) и уровне компаний, должна быть создана система органов, которые должны эффективно решать все задачи, связанные с защитой информации. Эти органы должны осуществлять:

- управление процессами защиты информации;
- проведение НИР и ОКР соответствующей тематики;
- разработку и производство программно-технических средств защиты информации;
- практическое решение всех задач защиты информации на объектах автоматизации;
- подготовку, повышение квалификации и переподготовку кадров в области защиты информации.

**Разработка теоретико-методологической основы защиты информации.** Для эффективного решения всех задач, связанных с защитой информации, необходимо разработать научно обоснованный базис. Для этого необходимо:

- разработать и обосновать единую терминологию (понятийный аппарат) в области защиты информации;
- проводить накопление и аналитическую обработку всех данных, относящихся к защите информации;
- разработать и обосновать стратегические подходы к решению различных задач защиты информации в современных условиях;
- разрабатывать научно-обоснованные методы решения различных задач защиты информации;
- обосновать структуру и содержание инструментально-методологической базы решения различных задач защиты информации.

**Решение проблемы управления системой защиты информации и ее автоматизации.** Должны быть разработаны методы и технологии управления системами защиты информации различного уровня и назначения. Должна быть предусмотрена возможность управления системами защиты на следующих основных уровнях:

- на общегосударственном уровне (структуры государственной власти);
- на региональном уровне (территориально-промышленные зоны);

- на уровне предприятия.

При этом должно быть предусмотрено два режима управления:

- повседневный - режим планового осуществления мер по защите информации;
- экстренный - режим принятия оперативных решений и осуществления мер по защите информации.

**Создание и совершенствование нормативно-правовой базы.** Должны быть созданы условия, для правового и нормативного регулирования решения всех задач защиты информации. Для этого необходимо:

- обоснование структуры и содержания нормативно - правовой базы;
- разработка и принятие законов, регламентирующих деятельность в области защиты информации;
- разработка, утверждение и распространение системы общегосударственных руководящих и методических материалов по защите информации;
- определение порядка разработки и утверждения руководящих документов по защите информации регионального уровня и уровня предприятия;
- разработка, утверждение и распространение комплектов типовых инструкций по различным аспектам защиты информации.

**Разработка и налаживание производства программно-технических средств защиты информации.** В стране должна быть создана мощная индустрия производства и распространения программно-технических средств защиты информации. Для этого необходимо:

- обоснование и разработка перечня средств защиты информации;
- создание системы предприятий и учреждений, производящих средства защиты информации;
- определение эффективного порядка разработки, производства, сертификации и распространения средств защиты информации, и т. д.

**Организация подготовки специалистов по защите информации.** Необходимо создание системы подготовки специалистов по защите информации, которая должна выпускать необходимое количество специалистов требуемых специализаций. Для решения этой задачи необходимо:

- разработать и научно обосновать концепцию подготовки кадров по защите информации;
- определить перечень учебных заведений, уполномоченных готовить кадры по защите информации, и распределить между ними специализации выпускаемых специалистов,
- организовать набор и подготовку молодых специалистов;
- организовать переподготовку и повышение квалификации специалистов по защите информации;
- организовать подготовку научно-педагогических кадров в области защиты информации.

## 5.4. Криптографическая защита информации

### 5.4.1. Технология использования криптографических систем

Термин "криптография" в переводе с греческого языка означает "тайнопись", что вполне отражает ее первоначальное предназначение.

Задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, называемую шифртекстом или криптограммой. При этом шифтекст может содержать как новые, так и имеющиеся в открытом сообщении знаки. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является то, что, используя некоторые логические замены символов в шифртексте, можно однозначно и в полном объеме восстановить исходную информацию.

Наряду с развитием криптографических систем совершенствовались и методы, позволяющие восстанавливать исходное сообщение, исходя только из шифртекста (криптоанализ). Успехи криптоанализа приводили к ужесточению требований к криптографическим алгоритмам.

Голландец Огюст Керкхофф (Auguste Kerckhoffs) (1835 - 1903 гг.) впервые сформулировал правило: стойкость шифра, т.е. криптосистемы - набора процедур, управляемых некоторой секретной информацией небольшого объема, должна быть обеспечена в том случае, когда криптоаналитику противника известен весь механизм шифрования за исключением секретного ключа - информации, управляющей процессом криптографических преобразований.

Это требование отразило понимание необходимости испытания, разрабатываемых, криптосхем в условиях, более жестких по сравнению с условиями, в которых мог бы действовать потенциальный нарушитель.

Правило Керкхоффа стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нем содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. С позиций сегодняшнего дня это правило можно интерпретировать более, широко - все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику. В последнюю формулировку криптосистемы входят как частный случай механизмов защиты. В этой формулировке предполагается, что все элементы систем защиты подразделяются на две категории - долговременные и легко сменяемые.

К долговременным элементам относятся те элементы, которые относятся к разработке систем защиты и для изменения требуют вмешательства специалистов или разработчиков.

К легко сменяемым элементам относятся элементы системы, которые предназначены для произвольного модифицирова ния или модифицирования по заранее заданному правилу, исходя из случайно выбираемых начальных параметров. К легко сменяемым элементам относятся, например, ключ, пароль, идентификатор и т.п. Рассматриваемое правило отражает тот факт, что надлежащий уровень секретности может быть обеспечен только по отношению к легко сменяемым элементам.

Несмотря на то, что, согласно современным требованиям к криптосистемам, они должны выдерживать криптоанализ на основе известного алгоритма, большого объема известного открытого текста и соответствующего ему шифртекста, шифры, используемые специальными службами, сохраняются в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточна сложную проблему.

Обоснование надежности используемых систем осуществляется, как правило, экспериментально при моделировании криптоаналитических нападений с привлечением группы опытных специалистов, которым предоставляются значительно более благоприятные условия по сравнению с теми, которые могут иметь место на практике в предполагаемых областях применения криптоалгоритма. Например, кроме шифртекста и алгоритма преобразований криптоаналитикам предоставляется весь или часть исходного текста, несколько независимых шифртекстов, полученных с помощью одного и того же ключа, или шифртексты, получаемые из данного открытого текста с помощью различных ключей. Оценивается стойкость испытываемой системы ко всем известным методам криптоанализа, разрабатываются новые подходы к раскрытию системы. Если в этих, благоприятствующих взлому условиях, криптосистема оказывается стойкой, то она рекомендуется для данного конкретного применения.

### 5.4.2. Особенности симметричных и асимметричных криптографических систем

Построение современных криптографических систем защиты информации основано на использовании различных методов шифрования. Эти методы можно разделить по характеру применения ключей шифрования:

- симметричные (одноключевые, с секретным ключом);
- несимметричные (двухключевые, с открытым и закрытым ключом);
- составные (комбинация симметричных и несимметричных).

Криптография делится на два класса: с симметричными ключами и с открытыми ключами. В криптографии с симметричными ключами отправитель и получатель информации используют один и тот же общий ключ для шифровки и дешифрации сообщений. Криптография с симметричными ключами отличается высокой стойкостью, т.е. невозможностью несанкционированной дешифрации, но имеет ограниченную область применения, так как изначально предназначена для целей ограничения доступа посторонних лиц к передаваемой информации.

## Симметричные криптографические системы

Данные системы являются классическими. Для шифрования и расшифрования текста в них используется один и тот же секретный ключ, сохранение которого в тайне обеспечивает надежность защиты информации.

Процесс работы данной системы можно представить следующим образом:
Пусть Zc- секретный ключ, EZc(X) - функция шифрования, а DZc(Y) - функция расшифрования, тогда Y=EZc(X),
X=EZc(Y)=DZc(EZc(X)), где X - открытый текст, Y - зашифрованный текст.

Все известные симметричные криптографические системы подразделяются по методам шифрования:

- блочные;
- поточные;
- комбинированные.

**Блочные шифры.** Поскольку открытый текст сообщения имеет произвольную длину, то он разбивается на более мелкие блоки фиксированной длины. Далее каждый блок шифруется отдельно, причем независимо друг от друга.

Симметричные блочные шифры подразделяются на шифры перестановки, замены и составные шифры.

При использовании *шифров перестановки* устранение смысла сообщения происходит путем изменения порядка чередования его символов, т.е. знаки открытого текста переставляются по некоторому правилу в пределах заданного блока. Различают шифры простой и сложной перестановки.

Шифры простой перестановки изменяют группу букв текста в соответствии с выбранным ключом перестановки. Ключом может быть размер таблицы, слово или фраза и т.д.

**Поточные шифры.** Основным достоинством поточного шифрования является высокая скорость преобразования данных, практически соизмеримая со скоростью поступления информации.

Поточные (потоковые) шифры осуществляют поэлементное шифрование потока данных без задержки в криптосистеме. Каждый символ открытого текста шифруется (дешифруется) либо независимо от других символов, либо с учетом ограниченного числа предыдущих символов.

Поточные шифры основываются на использовании ключевой последовательности с заданными свойствами случайности и двоичном представлении информационных сообщений. Шифрование (дешифрование) в основном осуществляется с использованием операции сложения по mod 2 элементов шифруемого (дешифруемого) текста и псевдослучайной

ключевой последовательности. Последние состоят из сгенерированных последовательностей символов с заданными свойствами случайности появления очередного символа

### 5.4.3. Распределение открытых ключей и цифровые сертификаты

Одной из главных сфер применения схемы с открытым ключом является решение проблемы распределения открытых ключей. Такое распределение может осуществляться двумя способами:

- путем создания центра генерации и распределения ключей;
- путем прямого обмена ключами между абонентами.

Главной особенностью шифрования с открытым ключом является тот факт, что открытый ключ должен быть известен всем. И если имеется некоторый общепринятый алгоритм шифрования с открытым ключом, то любая сторона может послать свой открытый ключ любой другой стороне. Этот подход очень удобен, но он имеет большой недостаток: публикацию может фальсифицировать кто угодно. И до того как пользователь обнаружит подлог и предупредит об опасности остальных, фальсификатор сможет читать весь шифрованный поток данных и использовать фальсифицированные ключи для аутентификации своих сообщений.

Эта проблема решается с помощью сертификатов открытых ключей. Сертификат состоит из открытого ключа и идентификатора владельца этого ключа, а весь блок подписывается надежной третьей стороной (Уполномоченный Центр Сертификации).

Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их, ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей под писей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

Пользователь предоставляет свой открытый ключ в уполномоченный центр и получить соответствующий сертификат. После чего он может опубликовать данный сертификат. Любой, кому потребуется открытый ключ данного пользователя, может получить сертификат и убедиться в его подлинности, проверив присоединенную подпись надежного источника.

Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи; наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи; наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи; сведения об

отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра

### 5.4.4. Защищенный документооборот по открытым каналам связи

Использование технологии несимметричного шифрования позволяет создать систему защищенного документооборота, использующую открытые каналы связи – Интернет и общеизвестные программы – клиенты электронной почты.

Первоначально участник защищенного документооборота, планирующий получать электронные письма от корреспондентов, должен в удостоверяющем центре получить пару ключей: закрытый и открытый ключ шифрования. Закрытый ключ шифрования данный участник документооборота хранит у себя, а открытый ключ должен по открытым каналам связи передать своим корреспондентам. В принципе, он может даже опубликовать открытый ключ на своем сайте.[84]

Корреспонденты шифруют сообщения с помощью открытого ключа. Предварительно следует убедиться в том, что открытый ключ принадлежит именно тому лицу, с которым мы планируем вести переписку. Для этого нужно изучить сертификат открытого ключа и, при необходимости, - обратиться в удостоверяющий центр за подтверждением статуса сертификата[85]. Далее с помощью открытого ключа и специальных программных средств осуществляется шифрование сообщения и передача его по обычной электронной почте. Зашифрованное сообщение с помощью открытого ключа уже не может быть расшифровано и для перехватчика (если таковой найдется) оно будет представлять собой набор бессмысленный символов. Получатель корреспонденции – владелец закрытого ключа расшифровывает сообщение.

### 5.4.5. Формирование и проверка цифровой подписи сообщений

Развитие цифровых и компьютерных и сетевых технологий привело к тому, что обмен электронными документами находит все более широкое применение в сфере бизнеса и в административной практике.

За рубежом заключение договоров на основании обмена информацией без использования бумажного носителя стало получать широкое распространение уже в начале 70-х годов. С появлением цифровых интерактивных компьютерных сетей, в том числе Интернета, развитие электронной коммерции совершило качественный скачек.

Однако появление новых технологий наряду с ускорением процессов обмена информацией значительно усложнило решение вопросов о достоверности такой информации, поскольку процесс обмена электронными документами существенным образом отличает-

[84] Открытый ключ потому и называется открытым, что в нем нет никакого секрета.

[85] Сертификат должен быть действующим, но он может быть и недействующим (например, по истечению срока), отозванным, дискредитированным и т.д.

ся от обычного обмена документами на бумажных носителях. Можно привести множество примеров злоупотреблений и мошенничества, совершаемых с использованием новых технологических возможностей. В то же время очевидно, что для широкого применения электронного обмена информацией необходимо обеспечить достаточную степень доверия к содержанию электронных документов, передаваемых с использованием новых технологических средств.

Технически проблема подтверждения подлинности информации, содержащейся в электронном документе, решается путем использования средств электронной цифровой подписи (ЭЦП), которая позволяет установить автора электронного документа и гарантировать неизменность его содержания.

ЭЦП - это специфический "цифровой код", связанный с содержанием электронного документа и позволяющий идентифицировать его отправителя (автора), а также установить отсутствие искажений информации в электронном документе, поскольку в случае внесения в него изменений ЭЦП теряет силу. результате специального криптографического преобразования текста электронного документа. Оно осуществляется с помощью так называемого "закрытого ключа" - уникальной последовательности символов, известной только отправителю электронного документа. Эти "данные" передаются вместе с текстом электронного документа его получателю, который может проверить ЭЦП, используя так называемый "открытый ключ" отправителя - также уникальную, но общедоступную последовательность символов, однозначно связанную с "закрытым ключом" отправителя. Успешная проверка ЭЦП показывает, что электронный документ подписан именно тем, от кого он исходит, и что он не был модифицирован после наложения ЭЦП.

Таким образом, подписать электронный документ с использованием ЭЦП может только обладатель "закрытого ключа", а проверить наличие ЭЦП - любой участник электронного документооборота, получивший "открытый ключ", соответствующий "закрытому ключу" отправителя. Подтверждение принадлежности "открытых ключей" конкретным лицам осуществляет удостоверяющий центр - специальная организация или сторона, которой доверяют все участники информационного обмена. Обращение в удостоверяющие центры позволяет каждому участнику удостовериться, что имеющиеся у него копии "открытых ключей", принадлежащих другим участникам, используемых им для проверки их ЭЦП, действительно принадлежат этим участникам.

Сегодня доверие к ЭЦП, используемым в закрытых (корпоративных) системах обмена информацией, достигается путем заключения специальных соглашений между участниками таких систем. Но для открытых, общедоступных систем электронного документооборота эту проблему возможно решить только путем создания развитой инфраструктуры, опирающейся на надежный правовой фундамент.

Широкое развитие электронного документооборота невозможно, если его участникам не будет предоставлена возможность совершать юридически значимые действия с применением средств электронной связи и защищать свои права, в частности, в случае необходимости представлять электронные документы в качестве судебных доказательств наравне с документами на бумажных носителях. Для этого необходимо законодательно закрепить условия, при которых ЭЦП признается равнозначной собственноручной подписи в документах на бумажных носителях.

ЭЦП основывается на криптографии с открытыми ключами, в которой используются два ключа (коды, уникальные последовательности символов) - закрытый ключ и открытый ключ, причем открытый ключ должен соответствовать закрытому.

Закрытый (секретный, частный, личный) ключ имеется только у отправителя сообщения, а открытый (публичный) предоставляется адресату сообщения. Известный только владельцу ЭЦП закрытый ключ используется для выработки ЭЦП, а общедоступный предназначен для проверки ЭЦП.

Сообщение, преобразованное (зашифрованное) с использованием закрытого ключа, можно проверить с помощью соответствующего открытого ключа, который позволяет ус-

тановить, что сообщение подписано именно обладателем закрытого ключа. Однако с помощью такого открытого ключа невозможно вычислить, определить закрытый ключ, используемый для создания шифрованных сообщений.

При криптографическом преобразовании электронного документа получается так называемое "хэш-значение" этого документа, иногда именуемое "сверткой сообщения" или "цифровым дайджестом сообщения" (message digest), причем вычисляемое с применением определенного алгоритма "хэш-значение" каждого электронного документа. При внесении малейшего изменения в электронный документ его "хэш-значение" изменяется.

Получатель электронного документа может с помощью открытого ключа отправителя расшифровать указанное отправителем "хэш-значение" и сравнить его с фактическим "хэш-значением" полученного документа. Совпадение обоих "хэш-значений" гарантирует, что электронный документ был подписан именно отправителем (обладателем закрытого ключа) и что в этот документ после подписания не вносились никакие изменения. Если проверяемое соотношение оказывается выполненным, то документ признается подлинным, в противном случае он считается недействительным.

Алгоритм криптографического преобразования должен соответствовать ГОСТу 28147-89 "Процедуры выработки и проверки ЭЦП", а также "хэш-функции" должны соответствовать алгоритмам, определяемым ГОСТами Р 34.10-94 и Р 34.11-94

ЭЦП позволяет гарантировать подлинность информации, содержащейся в электронном документе, а также дает возможность доказать любой третьей стороне (партнеру по сделке, суду), что электронный документ был подписан именно отправителем или по его поручению и именно в том виде, в каком он предъявляется.

Без знания закрытого ключа невозможно подделать ЭЦП или незаметно изменить содержание электронного документа, удостоверенного ЭЦП.

Общедоступный открытый ключ используется для проверки подлинности документа и ЭЦП, а также лишает подписавшее электронный документ лицо возможности оспорить факт его подписания.

Однако получателю сообщения необходимо быть уверенным в том, что предоставленный ему открытый ключ не просто соответствует конкретному закрытому ключу, но и в том, что оба эти ключа принадлежат именно тому лицу, которого получатель сообщения считает отправителем сообщения. Существует возможность распространять свой открытый ключ под чужой фамилией, в связи с чем возникла необходимость в сертификации таких открытых ключей.

Сущность сертификации ключей заключается в том, что открытый ключ вместе с именем владельца соответствующего закрытого ключа подписывается третьей стороной, известной обоим пользователям - удостоверяющим центром. Без такой дополнительной защиты злоумышленник может представить себя отправителем подписанных данных. Поэтому криптография с открытыми ключами требует наличия развитой инфраструктуры открытых ключей (PKI - Public Key Infrastructure) - системы удостоверяющих центров, основы для создания которой закреплены в Законе об ЭЦП. Открытый ключ, подписанный цифровой подписью удостоверяющего центра, называется сертификатом ключа подписи.

Таким образом, для заверения электронного документа используется ЭЦП его отправителя, а для заверения электронного сертификата, подтверждающего принадлежность используемого для проверки ЭЦП открытого ключа конкретному лицу, применяется ЭЦП удостоверяющего центра, являющегося основным элементом системы использования ЭЦП.

Удостоверяющий центр (сертифицирующий центр, англ. - certification authority, используются также термины Trust Center и Trustcenter) - это лицо, которое удостоверяет связь открытых ключей подписи с определенным физическим лицом. Любое лицо - пользователь открытого ключа ЭЦП (лицо, которое желает идентифицировать владельца ЭЦП при помощи сертификата ключа ЭЦП) вправе обратиться к удостоверяющему центру, выдавшему сертификат данного ключа, за подтверждением информации, содержащейся в

сертификате, а также за проведением проверки ЭЦП. В соответствии с требованиями Закона об ЭЦП и Федерального закона "О лицензировании отдельных видов деятельности" деятельность удостоверяющих центров подлежит лицензированию.

Законом об ЭЦП предусмотрено создание трехуровневой системы использования ЭЦП: обменивающиеся электронными документами владельцы и пользователи сертификатов ЭЦП ("клиенты"), выдающие сертификаты ЭЦП удостоверяющие центры и контролирующий деятельность этих центров федеральный орган исполнительной власти. Причем в отношении удостоверяющих центров такой федеральный орган исполнительной власти сам выполняет роль своеобразного удостоверяющего центра, ведущего реестр сертификатов ключей ЭЦП, которыми пользуются остальные удостоверяющие центры при работе с клиентами.

Заслуживает особого рассмотрения вопрос об определении владельца ЭЦП, именуемого в Законе об ЭЦП владельцем сертификата ключа подписи. В соответствии с российским Законом об ЭЦП ее владельцем может быть только физическое лицо. Такой подход принят и в европейском законодательстве. Так, по германскому законодательству ЭЦП может принадлежать только физическому лицу.

Как и в случае с собственноручной подписью, физическое лицо может действовать от имени юридического лица, но на такое полномочие обязательно должно быть указано в сертификате ключа подписи.

***Контрольные вопросы***

1. Перечислите базовые угрозы информации.
2. Основные задачи, решаемые системами защиты информации.
3. Задачи, возложенные на Удостоверяющие центры.
4. Особенности симметричных и ассиметричных криптографических систем.
5. Процесс подписания документа электронной цифровой подписью.
6. Процесс передачи шифрованных сообщений с использованием ассиметричных криптографических алгоритмов по открытым каналам связи.

# Библиографический список


1. Советов Б.Я., Информационные технологии. Учебник для ВУЗов, М.: Высшая школа, 2005
2. Козырев А.А., Информационные технологии в экономике и управлении, СПб.: Изд-во Михайлова, 2005
3. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2005.
4. Молдовян Н.А., Введение в криптосистемы с открытым ключом. СПб.: БХВ-Петербург, 2005.
5. Хорошилов А.В., Селетков С.Н., Мировые информационные ресурсы, СПб.:Питер, 2004
6. Поляк-Брагинский А.В. Администрирование сети на примерах. СПб.: БХВ-Петербург, 2006
7. Сергеев А.П. Беспроводная сеть в офисе и дома. Самоучитель. СПб.:Питер, 2007.
8. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. СПб.:Питер, 2006