**Курс «СЕТИ ЭВМ и ТК»**

**В. ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ СЕТЕЙ**

В середине 90-х огромное количество разнообразных сетей LAN и WAN. К 2003 г. – единственной построенной на проволочной технологии остается Ethernet, а большинства WAN составляют сеть сетей Internet.

Наблюдается рывок в беспроводных сетях. Актуальной становится тема защиты информации в сетях, тема объединения локальных сетей (зачастую разнородных) в корпоративную сеть, ведомственную сеть.

Нормативная УПРАВЛЕНИЕ Информационная

модель (план) (ЛПР) модель

**возмущения**

Система

обработки

информации

# Канал

взаимодействия

# Объект

управления

**Рис.В.1. Структура РАС**

<программно-технические средства ВТ>+<средства связи>

Некоторые области применения:

• сети в организациях – использование общего аппаратного и информационного ресурса;

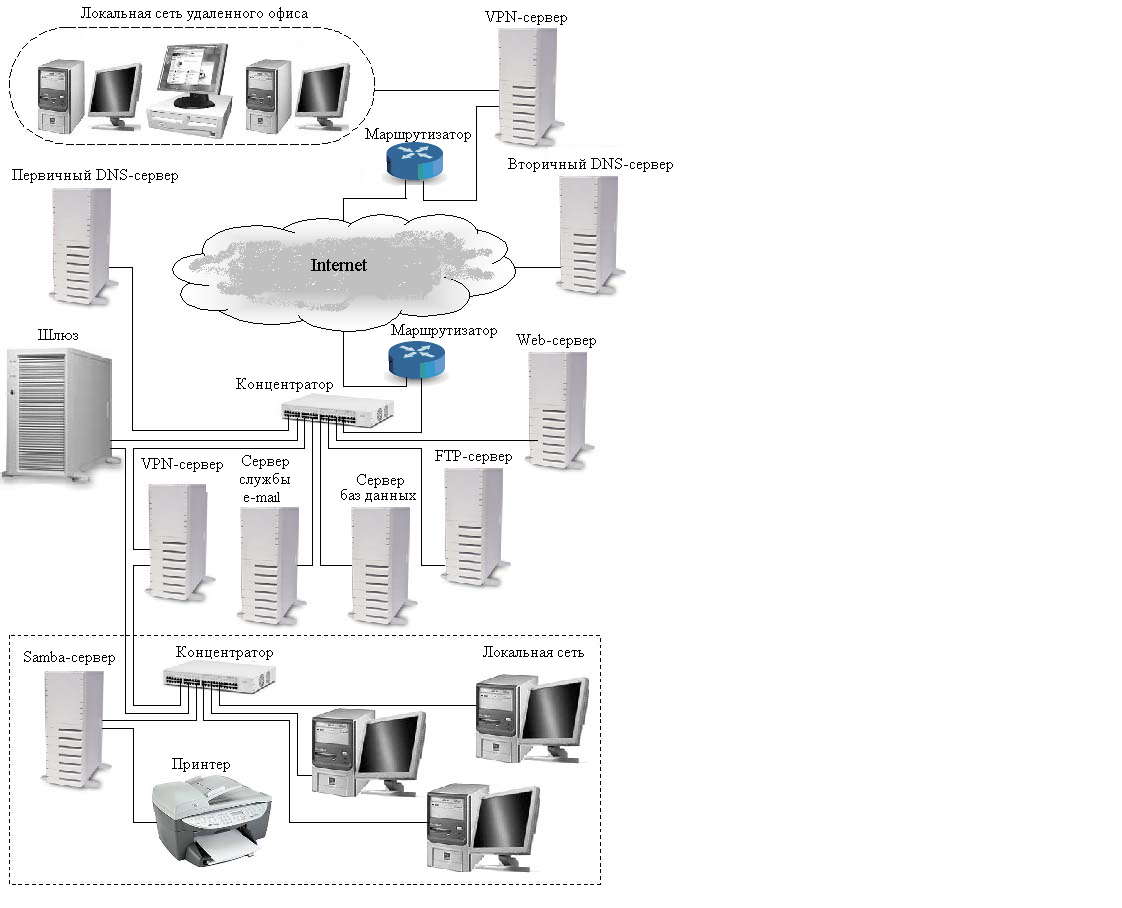
• замечательная коммуникационная среда для коллективного и частного общения людей;

• деловое общение между компаниями;

• коммерция;

• сети в системах управления.

# Угрозы безопасности корпоративным сетям



**Рис. 1.1. Структура корпоративной сети**

**Samba** — [пакет программ](http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC), которые позволяют обращаться к [сетевым дискам](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA) и [принтерам](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BD%D1%82%D0%B5%D1%80) на различных операционных системах по [протоколу](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [SMB/CIFS](http://ru.wikipedia.org/wiki/SMB). Имеет [клиентскую и серверную](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80) части.

А*така - это совокупность действий злоумышленника, приводящих к нарушению информационной безопасности компьютерной сети (КС).*

*В качестве потенциальных целей могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование сети.*

Любая атака может быть разделена на четыре стадии:

*рекогносцировки, вторжения в систему, атакующего воздействия на систему, стадия дальнейшего развития атаки* (жизненный цикл типовой атаки).

***Рекогносцировка.*** Получение информации об объекте атаки, чтобы на ее основе спланировать этапы вторжения.

*Примеры такой информации: тип и версия операционной системы, установленной на хостах информационной системы (ИС), список пользователей, зарегистрированных в системе, сведения об используемом прикладном программном обеспечении (ПО) и др.*

***Вторжение****.* На этом этапе нарушитель получает *несанкционированный доступ к ресурсам тех хостов, на которые совершается атака*.

***Атакующее воздействие****.* Реализуются атаки. Например, *нарушение работоспособности ИС; кража конфиденциальной информации, хранимой в системе; удаление или модификация данных и др*.

***Развитие атаки****.* З*лоумышленник стремиться расширить объекты атаки,* чтобы продолжить несанкционированные действия на других составляющих ИС.

Рассмотрим как могут реализовываться эти стадии.

На этапе **рекогносцировки** действия нарушителя могут быть нацелены на получение информации о:

* ***структуре и топологии*** компьютерной сети. *Информацию о структуре ИС злоумышленник может получить и путём обращения к DNS-серверу;*
* ***типе ОС***. При одних и тех же сетевых запросах разные ОС отправляют в ответ отличные друг от друга данные, используя которые можно с большой долей вероятности определить характеристики атакуемой ОС и даже тип аппаратной платформы;
* ***типе прикладных сервисов***. Эти знания нарушитель получить путём сканирования открытых портов и анализа заголовков ответов, полученных от этих служб;
* ***зарегистрированных пользователях***. Данные этого типа злоумышленник может извлечь из *базы данных SNMP MIB,* установленной на рабочих станциях и серверах компьютерной сети.

*SNMP* (Simple Network Management Protocol – простой протокол управления сетью);

*MIB* (management Information Base –информационная база управления).

***Вторжение****.* *Любое вторжение основано на наличии в компьютерной сети уязвимостей, и использование хотя бы одной из них открывает злоумышленнику вход в систему.*

Примеры уязвимостей:

– ***ошибки при конфигурировании*** ***сетевых служб*** компьютерной сети,

– ***использование*** «слабых» и «нестойких» ***паролей***,

– ***отсутствие*** необходимых ***средств защиты***.

Результат: нарушитель получает несанкционированный доступ к ресурсам атакованного узла.

На стадии ***атакующего воздействия,***  например, ***извлекает*** из СУБД атакованного узла сети ***конфиденциальную информацию***.

Перевод атаки в фазу её ***дальнейшего развития***.

Для этого в систему обычно несанкционированно внедряться программа, с помощью которой можно организовать атаку на другие узлы ИС. После установки такой программы опять начинается первый этап атаки - сбор информации о следующей цели.

Атаки имеют распределенный массовый характер. На  информационный узел сети осуществляется одновременное с десяток тысяч (и более) атакующих обращений. Узел выходит из строя. Данный вид атаки именуется *«Отказ в обслуживании» или DoS атакой (Denied of Service attack-* Отвергнутое атаки Услуги) . По статистике, 90% всех отказов атакуемых узлов были инициированы именно DoS-атаками.

По объему наносимого ущерба угрозы компьютерной сети классифицируются на следующие типы:

###### – Отказ в обслуживании;

– Попытка несанкционированного доступа;

– Предварительное зондирование;

– "Подозрительная" сетевая активность.

**Класс угроз «Отказ в обслуживании».**

Отказ в обслуживании - это любое действие или последовательность действий, которая приводит любую часть атакуемой системы к выходу из строя, при котором та перестает выполнять свои функции.

**(SYN flooding** (НАВОДНЕНИЕ SYN) - разновидность сетевых атак типа «отказ в обслуживании», которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок).

***Класс атак «Попытка несанкционированного доступа».***

ЭТО любое действие (последовательность действий), которая приводит к попытке чтения файлов или выполнения команд в обход установленной политики безопасности.

**(Переполнение буферов** )

***Класс атак «Предварительное зондирование».***

***Предварительное зондирование*** - любое действие или последовательность действий по получению информации из или о сети (например, имена и пароли пользователей), используемые в дальнейшем для осуществления неавторизованного доступа.

**(Сканирование сети посредством DNS** – выявление компьютеров, которые будут жертвами атаки.

**Сканирование TCP портов** – представляет собой распознавание конфигурации компьютера и доступных сервисов.

**Сканирование UDP портов**  позволяет за короткое время сканировать все порты на компьютере-жертве).

***Класс атак «Подозрительная сетевая активность***» представляет класс атак, характерной особенностью которых является наличие сетевого трафика, выходящего за рамки определения "стандартного" трафика. К данной группе угроз относятся:

(**Использование маршрутизации источника** злоумышленником для обхода элементов защиты (например, межсетевого экрана) локальной сети.

* **Дублирующий IP-адрес**. (Совпадение IP адресов может применяться атакующей стороной для незаметной подмены работающей "доверенной" системы и осуществления атак от ее имени).

1. ПРИНЦИПЫ ПОСТРОЕНИЯ ИНФОРМАЦИОННЫХ СЕТЕЙ

1.1. Концептуальная модель информационной сети

Главная обобщенная задача ТКС: ***бесыскаженная доставка заданного вида и объема информации в заданное время между заданными точками пространства.***

**Инф. Сети -р**езультат слияния средств обработки и обмена информацией В роли элементов ИС выступают **информационные и прикладные процессы.**

***Информационные процессы* (ИП)** – совокупность взаимосвязанных процессов выявления, отбора, формирования информации, ее ввода в техническую систему, обработки, хранения и передачи.

***Прикладные процессы* (ПП)** – тип ИП, ориентированных на выполнение конкретной прикладной задачи.

Информационная сеть

Транспортная сеть

Телекоммуникационная сеть

Абонентская система

ПП

Абонентская система

Сеть каналов связи

(передачи)

ПП

Рис. 1.5. Концептуальная модель информационной сети

Абонентская система

ПП

Абонентская система

ПП

***первый уровень*** (внутренний): функции и правила доставки информации между удаленными АС через физические КС (***транспортная сеть***);

***второй уровень*** (промежуточный): описывает функции и правила обмена информацией в интересах взаимосвязи прикладных процессов различных абонентских систем и реализуется ***телекоммуникационной сетью***.

***третий уровень*** (внешний) образуется совокупностью *прикладных процессов*, размещенных в территориально удаленных *абонентских системах*.

**1.2. КЛАССИФИКАЦИЯ СЕТЕЙ**

**Табл. 1**

|  |  |  |
| --- | --- | --- |
| Расстояние между  процессорами | Процессоры  расположены | Тип  сети |
| 1 м | На одном кв.метре | персональная |
| 10 м | комната | **LАN – Lосаl Агеа Networks** |
| 100 м | Здание | **LАN – Lосаl Агеа Networks** |
| 1 км | кампус | **LАN – Lосаl Агеа Networks** |
| 10 км | город | **МАN–Меtropolitan А Networks** |
| 100 км | страна | **WAN Wide Агеа Networks** |
| 1000 км | континент | **WAN Wide Агеа Networks** |
| 10 000 км | планета | Интернет **(Internet)** |

Два подхода решения проблемы предельной дальности.

***Первый подход*.** За дальность отвечают внешние технологии передачи, которые предоставляют готовый цифровой канал. Такой подход дает возможность строить ***глобальные сети*** (***WAN – Wide Area Network***) с неограниченной дальностью между сетевыми элементами.

***Второй подход*** предполагает добавление к функциям физического уровня функций формирования и обработки сигналов для передачи через конкретную физическую среду на конкретные максимальные дальности. Такие сетевые технологии применяются для построения ***локальных сетей*** (***LAN – Local Area Network***) с ограниченной дальностью между сетевыми элементами.

Сети ***MAN*** (***Metropolitan Area Network***)– ***городские сети***.

Другая отличительная особенность LAN от WAN: *способ разделения физической среды* *передачи между отдельными парами сетевых элементов* при обеспечении передачи информации между ними.

Для WAN типично использование поделенной (на отдельные каналы) физической среды системами передачи. Принцип «***точка-точка***». Соединение любой конкретной пары АС осуществляется в соответствии с протоколами маршрутизации сетевого уровня, *минимум*, *через один узел коммутации* (максимум, через все).

Для LAN АС связаны через общую физическую среду по принципу «***точка-многоточка***». Протоколы уровня звена данных регулируют поочередное использование общей среды передачи всеми АС.

Принцип «точка-многоточка» – «один передает – все принимают», но если информация предназначена кому-то одному, то только он ее и воспринимает, а остальные игнорируют.

Носителем адресных признаков АС источника и АС получателя в LAN являются специальные адресные поля кадров, которые не используются в WAN.

**1.4. Технология «клиент – сервер»**

Цель создания сети коллективное использование ресурсов (ресурсы – диски, файлы, принтеры, модемы, факс – аппараты и т.п.).

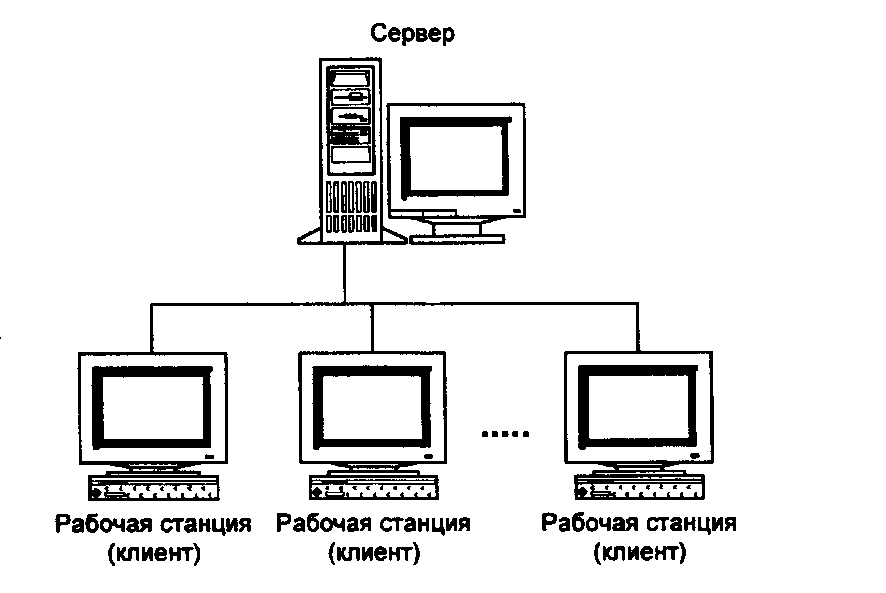
Специальные программные модули в режиме ожидания запросов называются **программными серверами** (serve – обслуживать).

Специальные программные модули, вырабатывающие запросы - **программные клиенты** (klient).

Это части операционных систем. **Пара клиент-сервер, обеспечивая доступ к определенному ресурсу, «образует» определенную службу**: файловая служба, служба печати, служба электронной почты, служба удаленного доступа и др. (прикладной уровень ЭМ ВОС).

Термины «клиент», «сервер» используются и для обозначения компьютеров

**1.4. Модели архитектуры «клиент – сервер»**



## Рис.1.8. Типовая архитектура «клиент-сервер»

## (одноранговая)

Рабочая станция Компьютер-сервер

Компонент Прикладной Менеджер Представления компонент ресурсов

данные

Модель файл-сервер

Модель сервера базы данных 

 Модель сервера приложений

Рис.1.9. Модели двухранговой архитектуры «клиент-сервер»

**1.5. ТОПОЛОГИИ СЕТЕЙ**

**Сетевая тополо́гия** (от [греч.](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) τόπος, - место) — способ описания конфигурации [сети](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), схема расположения и соединения [сетевых устройств](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0). Сетевая топология может быть **физической** — описывает реальное расположение и связи между узлами сети; **логической** — описывает направление потоков информации, передаваемых по сети.

Существует множество способов соединения сетевых устройств, из них можно выделить ряд базовых топологий: [Шина](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D0%BD%D0%B0_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8)), [Кольцо](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8)), [Звезда](http://ru.wikipedia.org/wiki/%D0%97%D0%B2%D0%B5%D0%B7%D0%B4%D0%B0_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8)), [Ячеистая топология](http://ru.wikipedia.org/wiki/%D0%AF%D1%87%D0%B5%D0%B8%D1%81%D1%82%D0%B0%D1%8F_%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F), [Дерево](http://ru.wikipedia.org/w/index.php?title=%D0%94%D0%B5%D1%80%D0%B5%D0%B2%D0%BE_(%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D1%81%D0%B5%D1%82%D0%B8)&action=edit&redlink=1), Сотовая. Остальные способы являются комбинациями базовых.

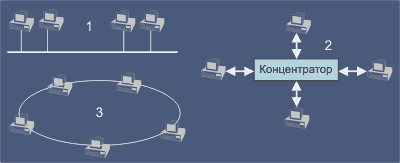


Рис.1.10. Примеры сетевых топологий ЛС

.

5

4

Рис.1.11. Ячеистая (4) и сотовая (5)сетевые топологические схемы

1.6. Уровневая организация ЭМВОС

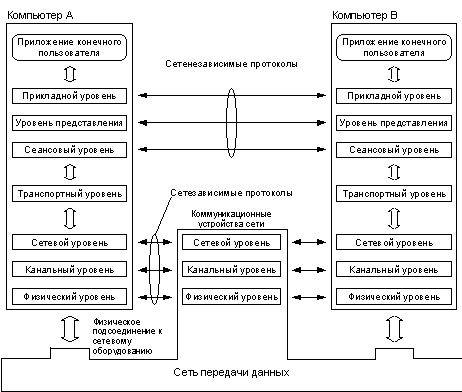


Рис. 1.12. *Сетезависимые и сетенезависимые уровни модели OSI*

OSI TCP/IP

|  |  |  |
| --- | --- | --- |
| Прикладной | Прикладной | Различия моделей OSI и TCP/IP: |
| Представительный | Не присутствует | 1). Количество уровней  2).OSI на сетевом уровне поддерживает возможности использования |
| Сеансовый | Не присутствует | связи с *установлением соединения* и |
| Транспортный | Транспортный | *без установления соединения*, на тра- |
| Сетевой | Межсетевой | транспортном уровне – только на основе *установления соединения* |
| Канальный  Физический | От хоста  к сети | TCP/IP – на сетевом уровне только без *установления соединения, на транспортном уровне* – оба режима, предоставляя пользователю выбор |

Описание уровней ЭМВОС опирается на ряд формализованных понятий.

***N-уровень; N-логический объект*** (***N-объект***); ***Равноправные логические объекты; N-услуги*** и ***N-функции; Протокол***; **Межуровневый интерфейс**; **Сервис**; ***Ассоциация***.

1.7. Структуры передаваемых данных

(*N*+1)-уровень

*N*-

уровень

(*N*+1)-УИП

(*N*+1)-УИИ

(*N*+1)-объект

(*N*+1)-СБД

*N*-СБД

*N*-УИП

*N*-объект

*N*-УИИ

(*N*+1)-ПБД

(*N*+1)-СБД

(*N*+1)-объект

(*N*+1)-

УИП

*N*-УИИ

*N*-СБД

(*N*+1)-УИИ

*N*-УИП

*N*-объект

(N+1)-ИБД

*N*-ПБД

*N*-ИБД

*N*-ИБД

*N*-ПБД

(*N*+1)-ИБД

(*N*+1)- ПБД

Рис. 1.13. Последовательность формирования и обработки блоков данных

***Протокольные блоки данных* (ПБД); Сервисные блоки данных** **(СБД)**; **Интерфейсные блоки данных** **(ИБД); Управляющая информация интерфейса (УИИ).**

Протокольная избыточность разных телекоммуникационных технологий

|  |  |  |  |
| --- | --- | --- | --- |
| **Протокольная избыточность** | ATM | ***IP*** | Ethernet |
| **Lprot/Ltotal, %** | 10 | **0,1** | 1,0 |

Lprot – объем заголовка (и хвостовика);

Ltotal – общий объем протокольного блока данных.

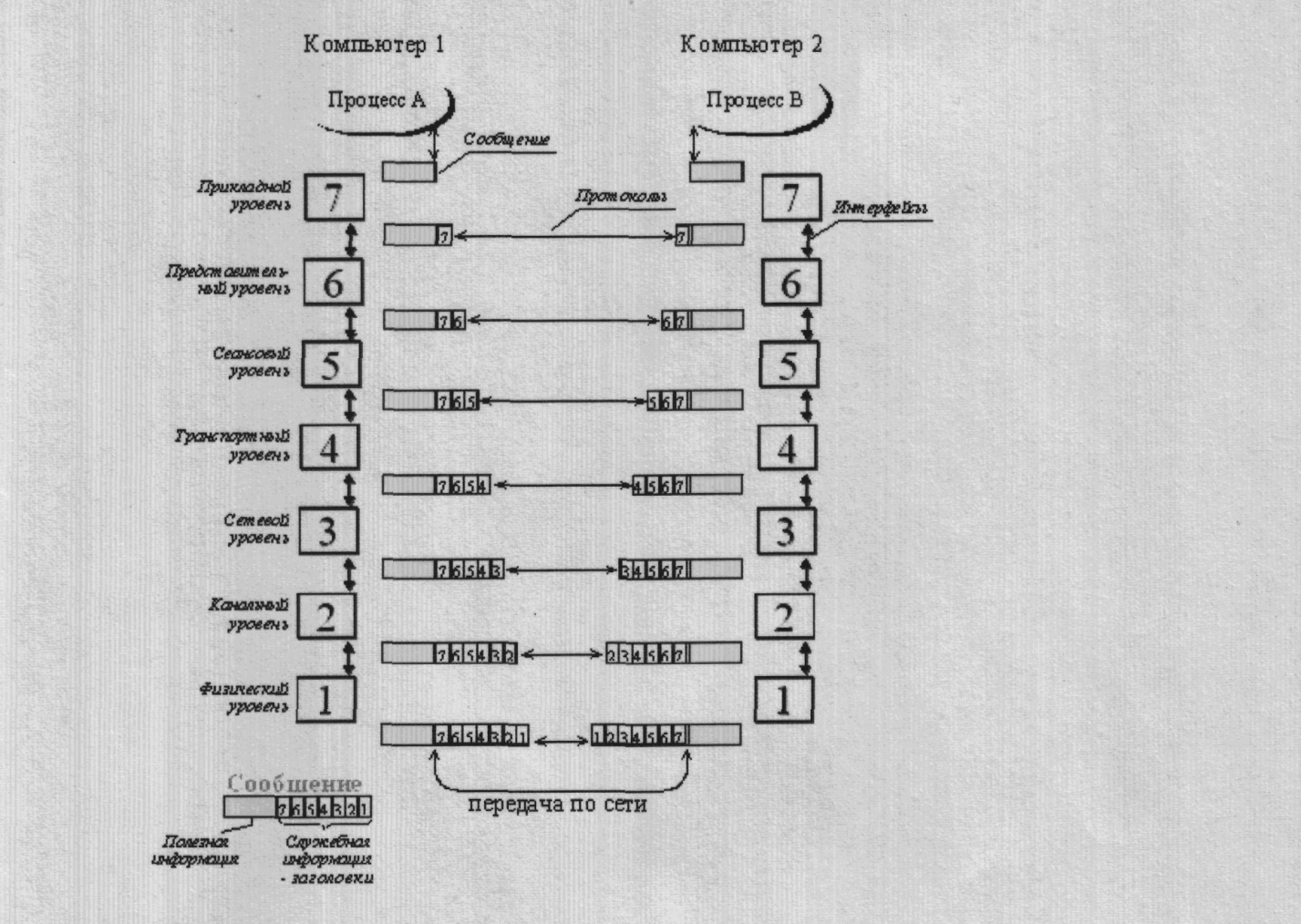


Рис. 1.14. Вложенность пакетов различных уровней

*N*-СБД

*N*-ПБД

*N*-СБД

*N*-СБД

*N*-СБД

*N*-ПБД

*N*-ПБД

*N*-ПБД

Фрагментация / дефрагментация

Блокирование / деблокирование

**1.8. Расход ресурсов пропускной способности среды передачи**:

*W*с.сум

*W*с.сум

+ на повторную передачу искаженных ПБД

+ на передачу служебных полей ПБД

на передачу полезной информации

*Т*min

*T*

*W*и

*Т*min = *W*и / *V*

*V*min = *W*и / *T*

*W*и

+ на технологические паузы

+ на передачу служебных ПБД

Рис. 1.16*.* Оценка расхода ресурсов пропускной способности среды передачи

*Т*mах = (*W*с.сум + *W*и) / *V*

*V*mах = (*W*с.сум + *W*и) / *T*

Эффективность *E* использования пропускной способности среды передачи:

*E* = *V*min/*V*max = *T*min/*T*max = *W*и / (*W*и + *W*с.сум) < 1,

где *W*с.сум – эквивалентный суммарный объем служебной информации, необходимой для передачи объема полезной информации *W*и .

**1.9. Характеристики сетевых систем**

Две группы характеристик: *производительность* и *надежность*.

Показатели **производительности**:

- *временные* (**задержка** и **вариации задержки, время реакции);**

- *пропускной способности* (объем данных, переданных сетью или ее частью в единицу времени)*.*

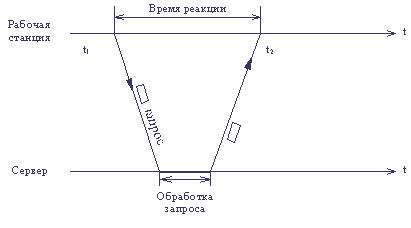


Рис. 1.17. Время реакции - интервал между запросом и ответом

Смысл и значение этого показателя зависят от загруженности сегментов, через которые проходит запрос, загруженности сервера, коммутатора, моста, маршрутизатора и т.п.

Вариантами критерия могут служить времена реакции, измеренные при различных, но фиксированных состояниях сети (крайние значения):

A) *Полностью ненагруженная сеть*.

B) *Нагруженная сеть*.

При оценке производительности сети по отношению ко всем узлам в целом используются критерии двух типов: *средно-взвешенные* и *пороговые*.

*Эффективная скорость передачи всегда меньше номинальной.*

**Надежность** - способность правильно функционировать в течение продолжительного периода времени. Это свойство имеет три составляющих: *собственно надежность, готовность и удобство обслуживания*.

Надежность измеряется ***интенсивностью отказов*** и ***средним временем наработки на отказ*.**

***Удобство обслуживания*** включает такие понятия как:

• *расширяемость (масштабируемость*)

• *Мобильность (переносимость) –* поддержка разных программно-аппаратных платформ;

• *Интероперабельность* – способность к взаимодействию с другими системами;

• *Управляемость* – адекватность сетевому администрированию;

**1.10. Резюме**

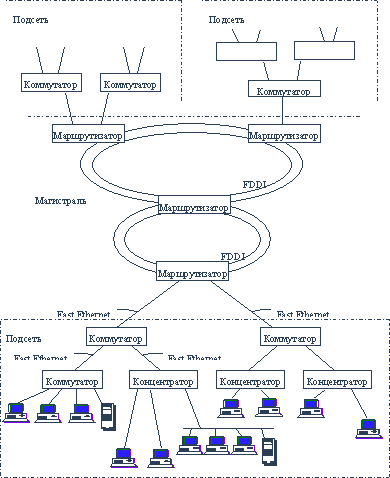


Рис. 1.18 .Структура локальной сети

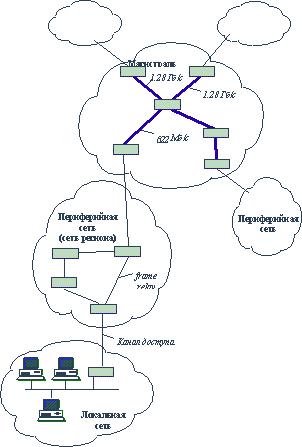


Рис. 1.19. Структура глобальной сети