Основы локальных вычислительных сетей

Принципы организации и основные топологии вычислительных сетей

Что такое компьютерная сеть

Совокупность:

- **узлов (компьютеров, рабочих станций или других устройств)**
- **соединенных коммуникационными каналами**
- **набор оборудования, обеспечивающего соединение станций и передачу между ними информации**

Преимущества сетей

1. Мощь и гибкость совместной работы
2. Свобода выбора
3. Эффективное совместное использование ресурсов (Sharing)
4. Обеспечение безопасности информации
5. Возможность получения информации из любой точки мира

Клиент-серверная архитектура

Сервер

узел сети, предоставляющий свои ресурсы другим абонентам, но сам не использующий ресурсы других узлов

Клиент (рабочая станция)

абонент сети, который только использует сетевые ресурсы

Виды компьютерных сетей

LAN – Locate Area Network

WAN – Wide Area Network

MAN – Metropolitan Area Network

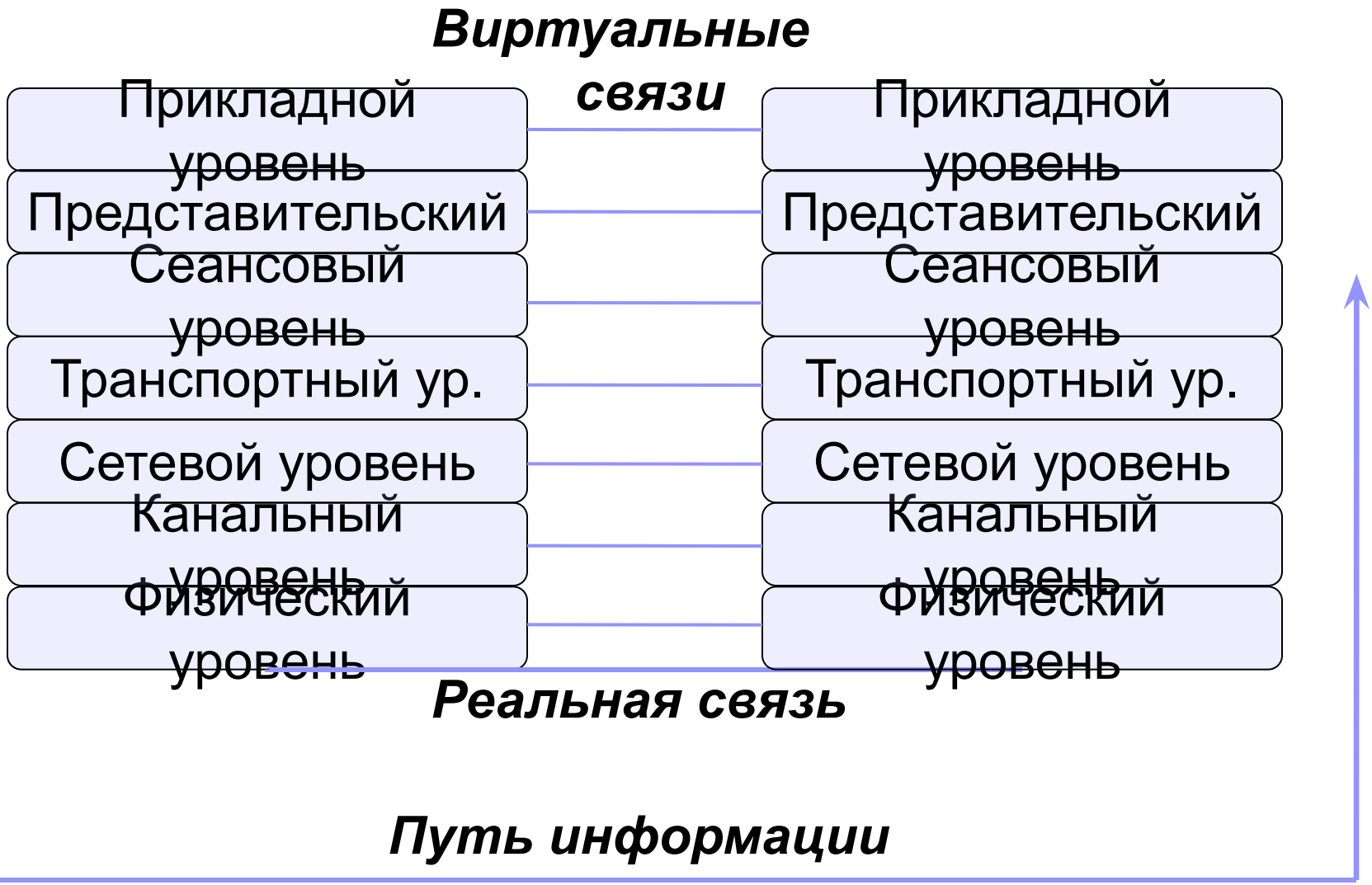
Однозначной границы нет!!!

Модель ISO/OSI

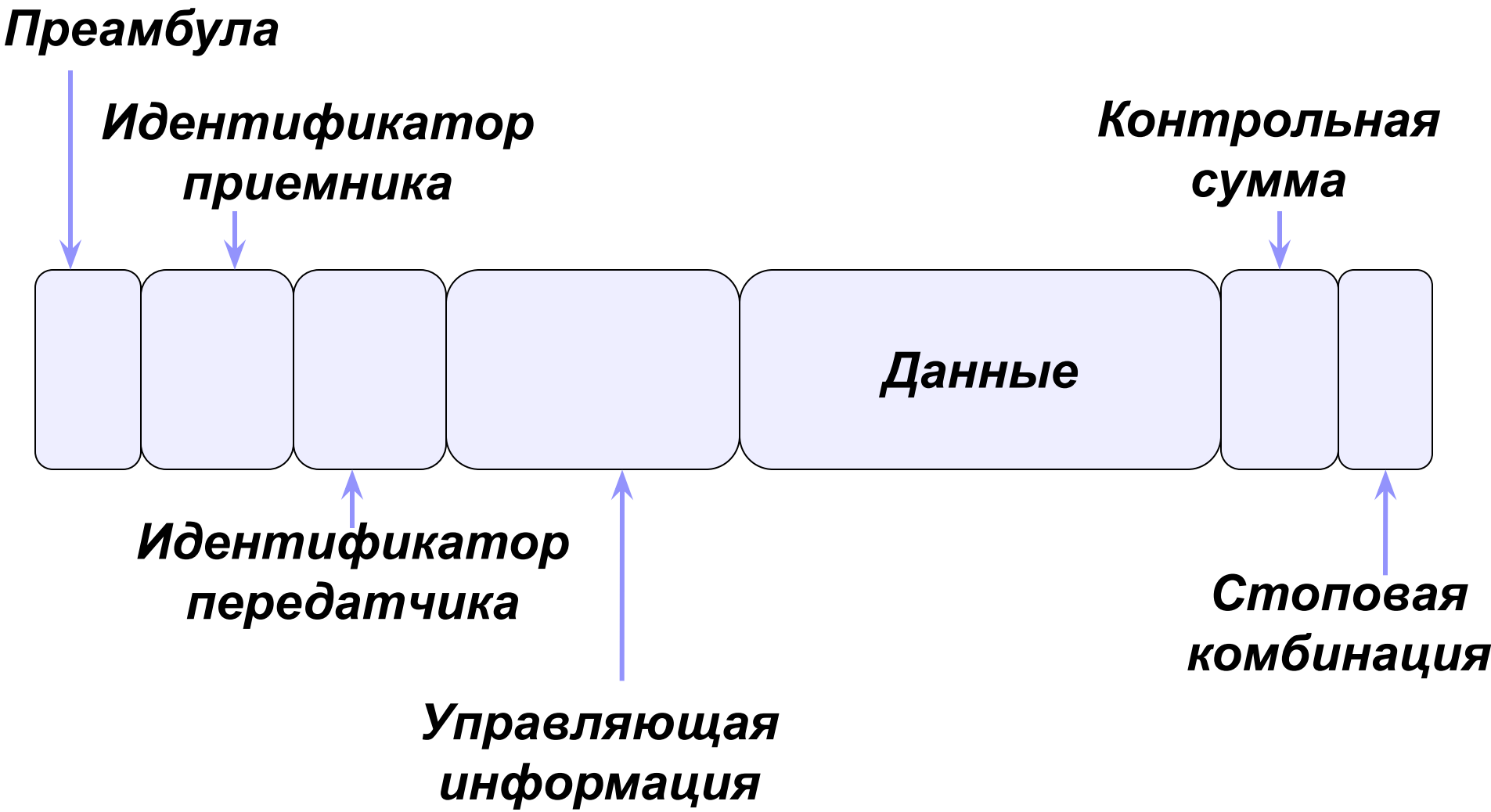
ISO – International Organization for Standardization

OSI – Open System Interconnection

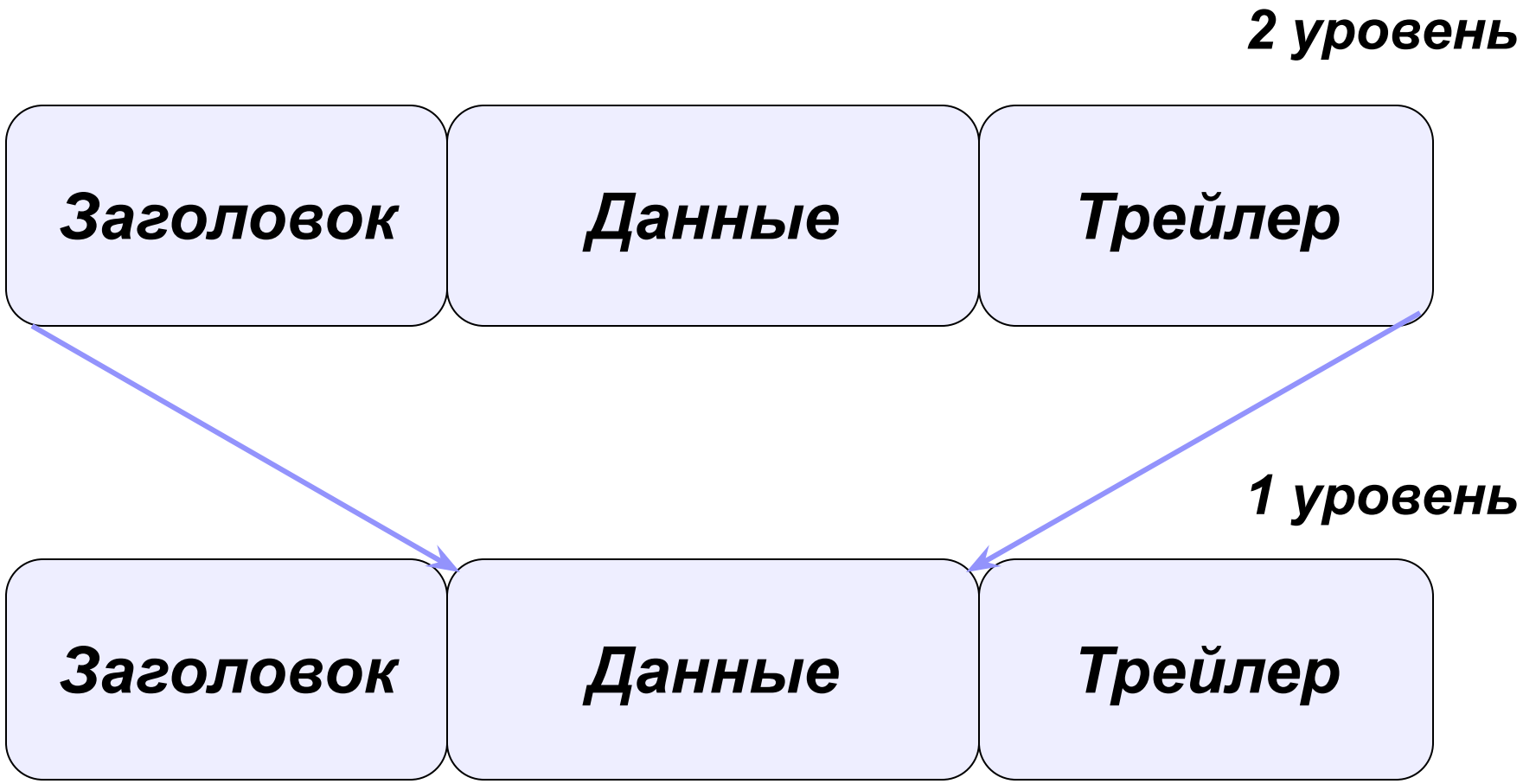
Путь информации от абонента к абоненту



Структура пакета



Структура пакета



7 – Прикладной (Application)

- *Программные средства передачи файлов, средства эл. почты, доступ к БД*

6 – Представительский (Presentation)

- *Преобразование форматов данных*
- *Шифрование/дешифрование данных*
- *Сжатие*

5 – Сеансовый (Session)

- *Устанавливает, поддерживает, прекращает связь*
- *Распознает логические имена абонентов*
- *Контролирует права доступа абонентов*

4 – Транспортный (Transport)

- *Доставка пакетов*
- *Сегментация данных*
- *Восстановление принимаемых данных*

3 - Сетевой (Network)

- *Отвечает за адресацию пакетов*
- *Перевод логических имен в физические сетевые адреса и обратно*
- *Выбор маршрута отправления пакета*

2 - Канальный (Data Link)

- *Управление линией передачи*
- *Проверка доступности среды передачи*
- *Формирование кадров*

1 - Физический (Physical)

- *Физические характеристики среды передачи*
- *Прием и передача данных по линиям связи*
- *Управление каналом*
- *Кодирование информации в уровни сигналов*
- *Декодирование*

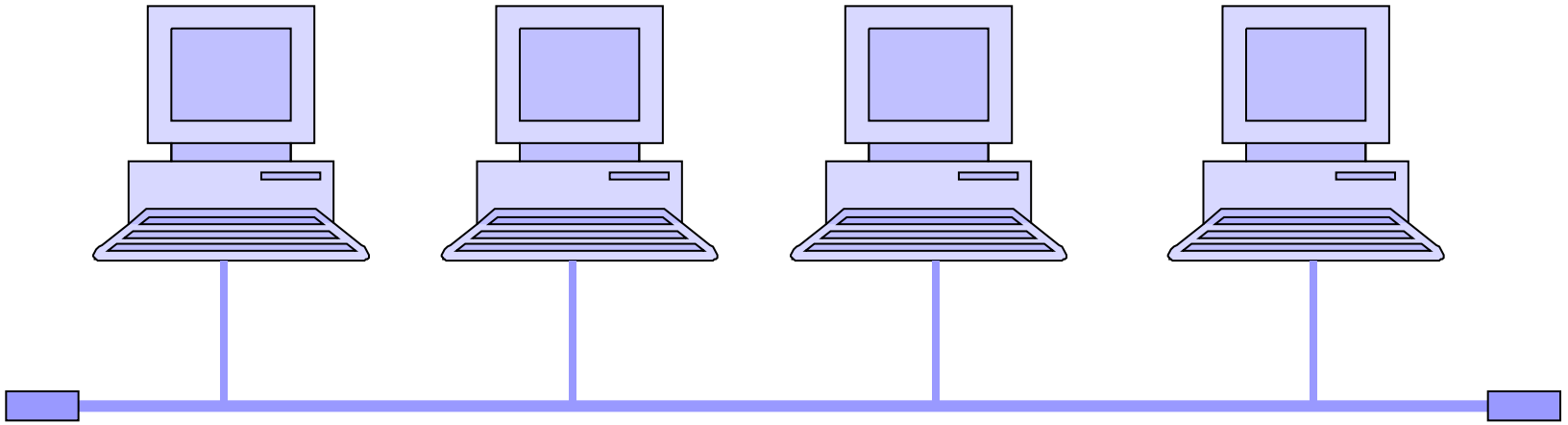
Топология локальных сетей

Топология (компоновка, конфигурация)

физическое расположение компьютеров сети относительно друг друга и способ соединения их линиями связи

Определяет требования к оборудованию, тип используемого кабеля, возможность расширения

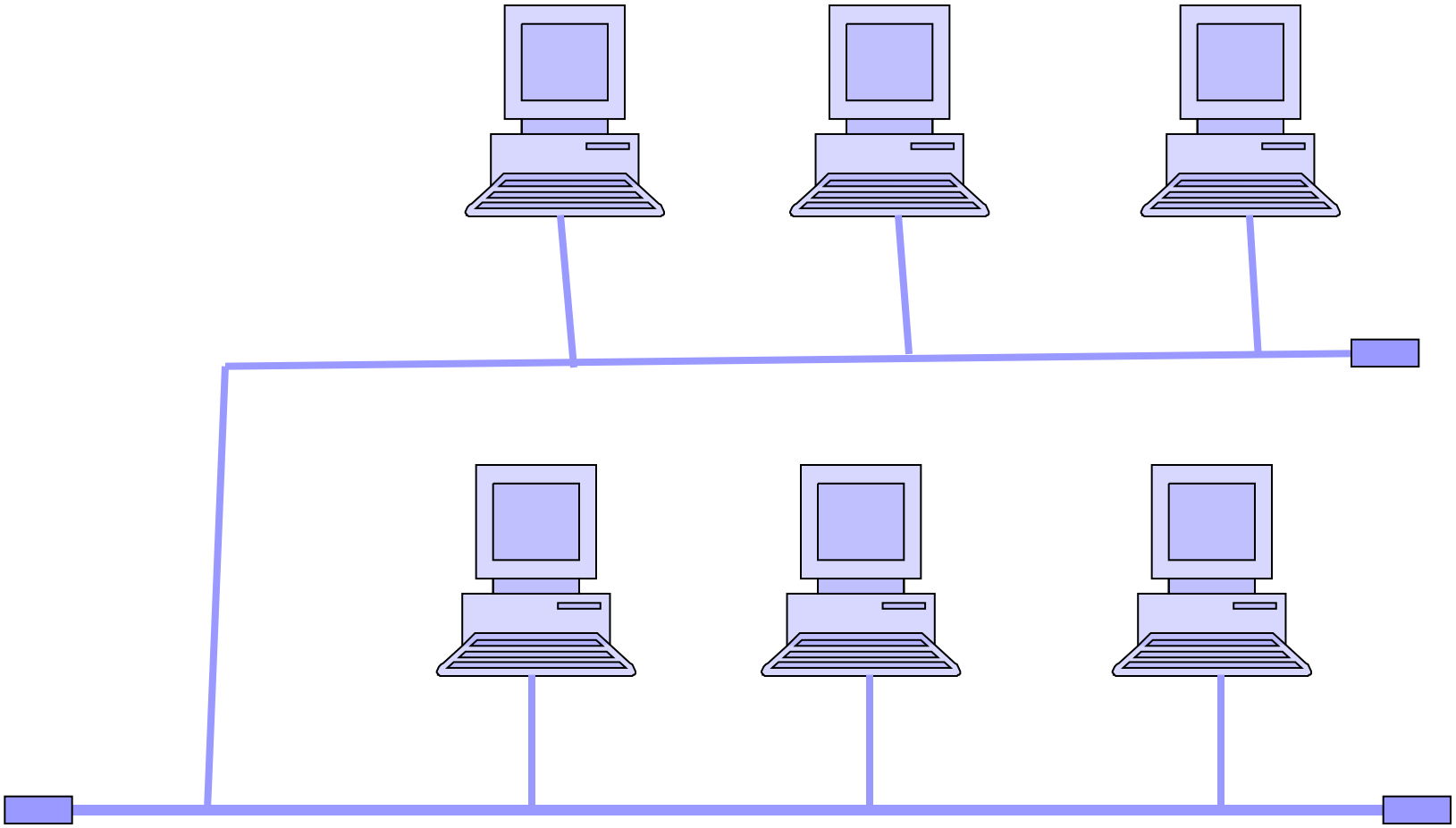
Топология «шина»



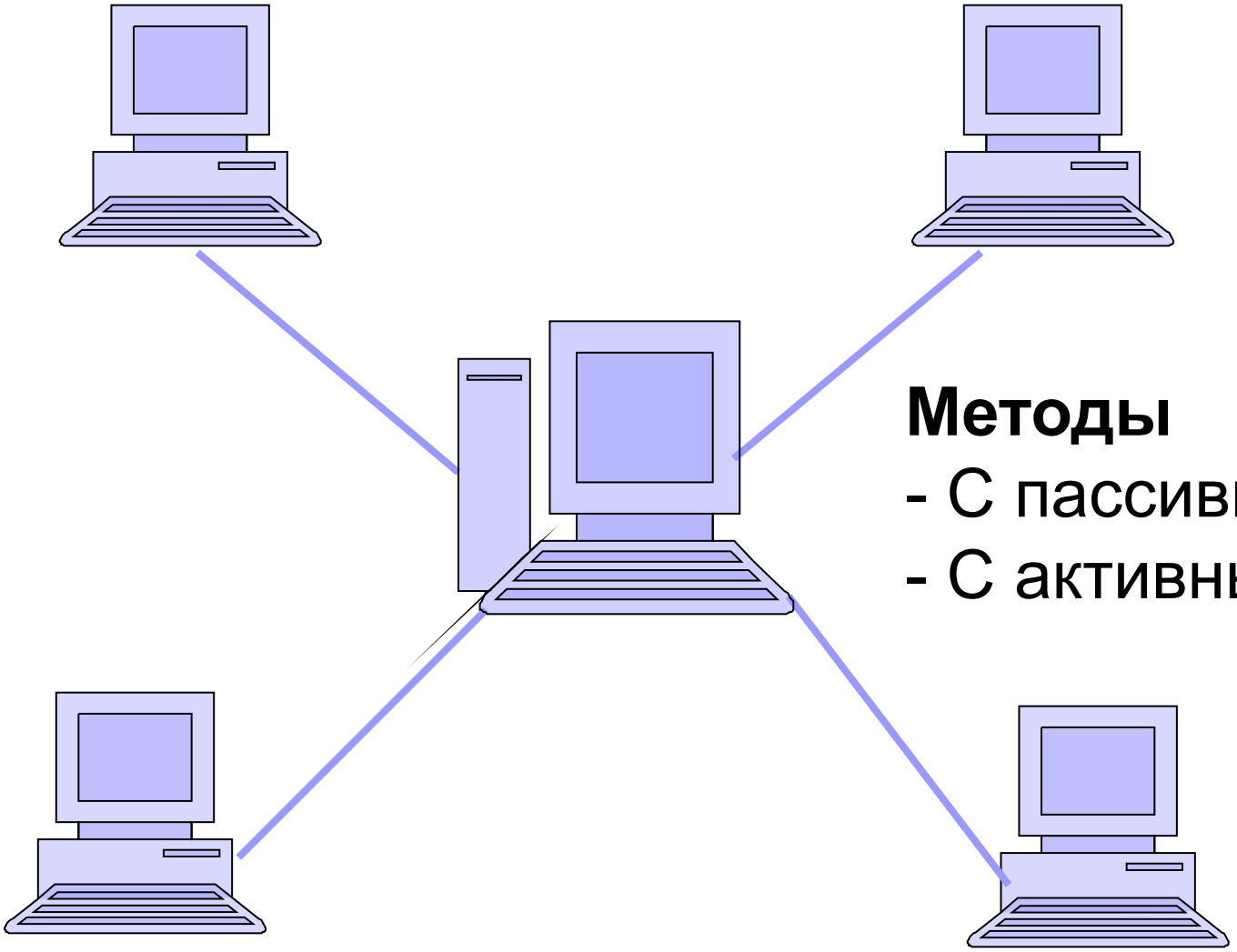
Управление обменом в сети с топологией шина

Централизованные методы
Децентрализованные методы
Случайные методы (коллизии)

Топология «распределенная шина»



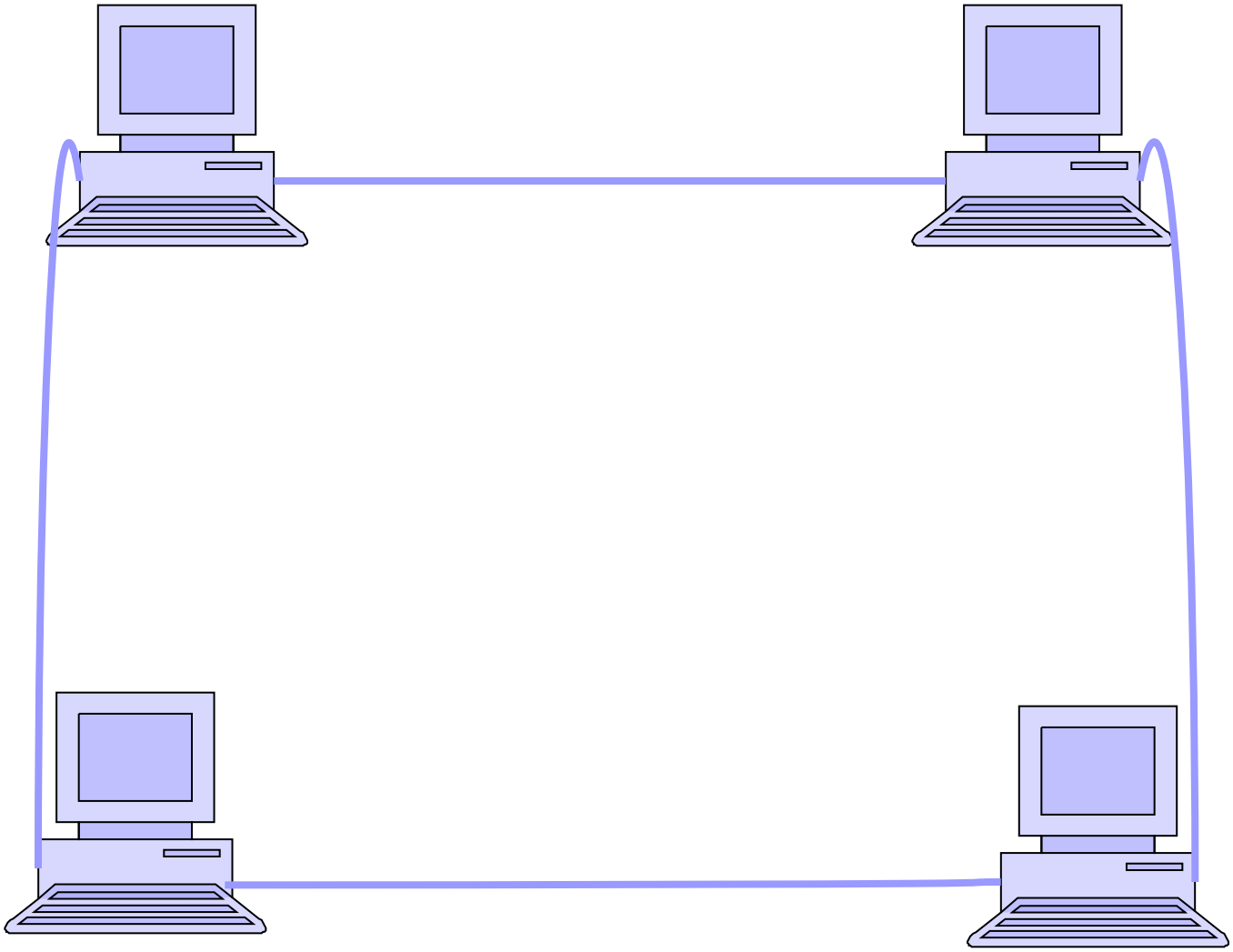
Топология «звезда»



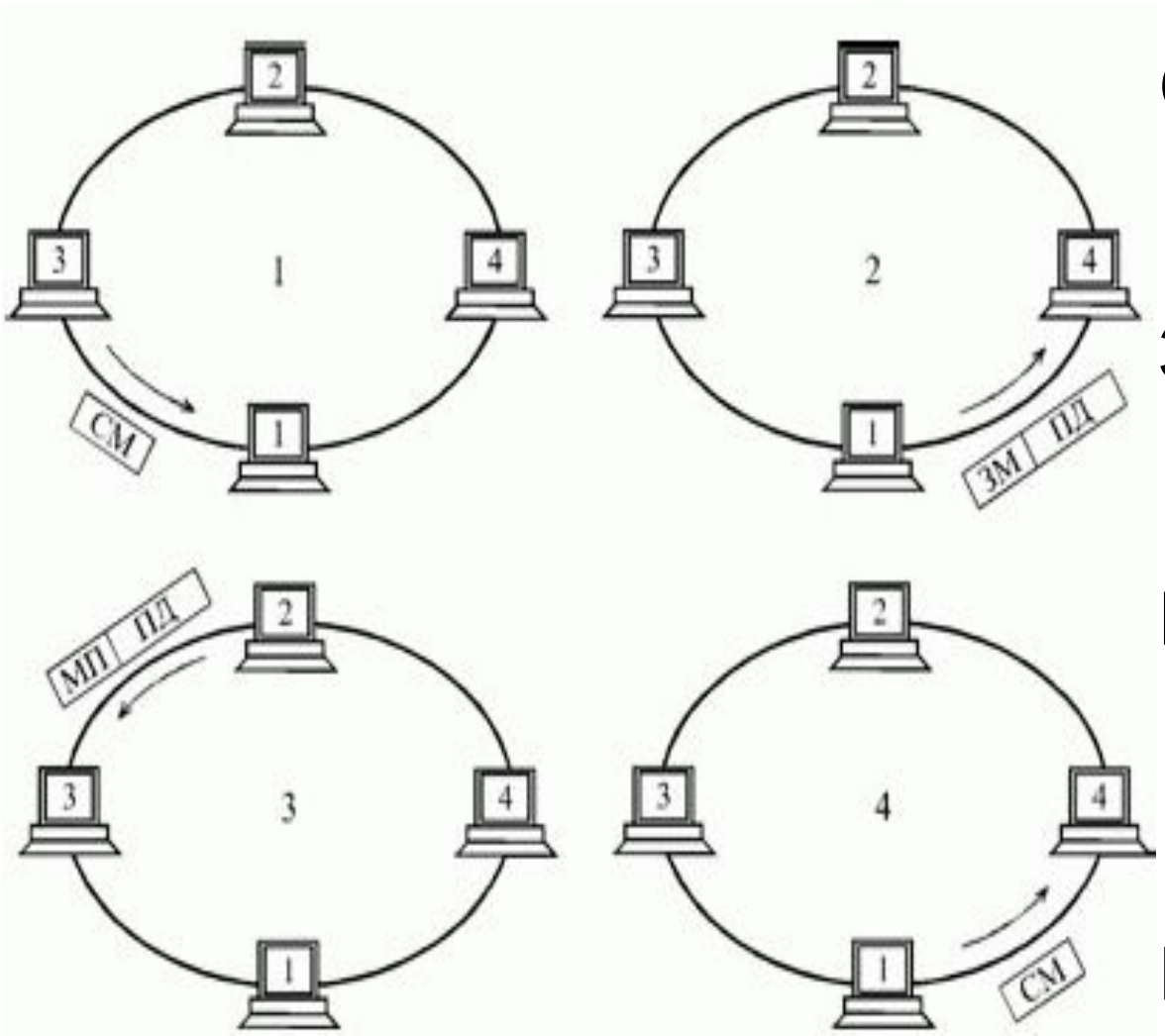
Методы

- С пассивным центром
- С активным центром

Топология «кольцо»



Маркерный метод



СМ – свободный маркер

ЗМ – занятый маркер

МП – занятый маркер с подтверждением

ПД – пакет данных

Многозначность понятия топологии

Физическая топология *– схема расположения компьютеров и прокладки кабеля*

Логическая топология *– структура связей, характер распространения сигнала по сети*

Вредоносное ПО
Вирусы, черви, трояны
Антивирусная защита

Вредоносная программа

- компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе (КС), либо для скрытого нецелевого использования ресурсов КС, либо иного воздействия, препятствующего нормальному функционированию КС

Типы вредоносных программ

- Вирусы
- Трояны
- Черви

Вирусы

Отличительная особенность - способность к размножению в рамках одного компьютера (создание копий, необязательно совпадающих с оригиналом)

<u>Процесс размножения</u>:

- **Проникновение на компьютер**
- **Активация вируса**
- **Поиск объектов для заражения**
- **Подготовка вирусных копий**
- **Внедрение вирусных копий**

Классификация вирусов

по способу заражения:

- Резидентные
- Нерезидентные

по степени воздействия:

- Неопасные
- Опасные
- Очень опасные

по типам объектов, которые могут быть заражены:

- Загрузочные вирусы
- Файловые вирусы
- Файлово-загрузочные

Червь (сетевой)

— тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Черви. Жизненный цикл

1. **Проникновение в систему**
2. **Активация**
3. **Поиск "жертв"**
4. **Подготовка копий**
5. **Распространение копий**

Для активации:

- *необходимо активное участие пользователя*
- *достаточно лишь пассивного участия*

Сетевые черви
использующие для распространения протоколы Интернет и локальных сетей

Почтовые черви
распространяющиеся в формате сообщений электронной почты

IRC-черви
распространяющиеся по каналам IRC (Internet Relay Chat)

P2P-черви
распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей

IM-черви
использующие для распространения системы мгновенного обмена сообщениями (IM-Instant Messenger, ICQ, MSN Messenger, AIM)

Троян (троянский конь)

- тип вредоносных программ, цель которых - вредоносное воздействие по отношению к КС

- Отличаются отсутствием механизма создания собственных копий
- В общем случае попадает в систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника
- Некоторые способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы

Трояны. Жизненный цикл

- Проникновение на компьютер
- Активация
- Выполнение заложенных функций

Функций размножения и распространения отсутствуют!

Маскировка

выдает себя за полезное приложение, которое пользователь самостоятельно загружает из Интернет и запускает

Кооперация с вирусами и червями

путешествует вместе с червями или с вирусами

Трояны. Выполняемые функции

- Клавиатурные шпионы
- Похитители паролей
- Утилиты удаленного управления
- Люки (backdoor)
- Утилиты дозвона
- Модификаторы настроек браузера
- Логические бомбы

Угрозы безопасности информации

❑ Нарушение конфиденциальности

- Кража информации и ее распространение
- Кража паролей доступа, ключей шифрования
- Удаленное управление

❑ Нарушение целостности

- Модификация без уничтожения (изменение информации)
- Модификация посредством уничтожения либо шифрования
- Модификация путем низкоуровневого уничтожения носителя (форматирование носителя)

❑ Нарушение доступности

- Загрузка каналов передачи данных большим числом пакетов
- Любая деятельность, результатом которой является невозможность доступа к информации
- Вывод компьютера из строя путем уничтожения, либо порчи критических составляющих (уничтожение BIOS)

Антивирус

- программное средство,
предназначенное для борьбы с вирусами

Задачи антивируса:

- Препятствование проникновению вирусов в КС
- Обнаружение наличия вирусов в КС
- Устранение вирусов из КС без нанесения повреждений другим объектам системы
- Минимизация ущерба от действий вирусов

Ни один антивирус не обеспечивает полную защиту от всех вредоносных программ

Признаки присутствия вредоносных программ

Явные

- Вывод на экран сообщений, страниц

Изменение настроек браузера

Косвенные (ошибки авторов вред.прогр.)

- Провоцирование сбоев, перезагрузка ПК
- Отключение или попытка удаления антивируса
- Блокировка антивирусных сайтов

Сообщение об ошибке при загрузке компьютера

Скрытые

- Наличие дополнительных процессов в памяти
- Изменения системного реестра Windows

Незнакомые файлы

Необычная сетевая активность (ни одно сетевое приложение не запущено, а значок сет.соед. сигнализирует об обмене данными)

История вопроса

1940-е г. – теоретические основы
самораспространяющихся программ
Джон фон Нейман, Л.С.Пенроуз, Ф.Ж.Шталь

Первые самораспространяющиеся программы не были вредоносными в понимаемом ныне смысле.
Это были программы-шутки, либо последствия ошибок в программном коде.

История вопроса

Основная характеристика компьютерного вируса — способность к самораспространению.

Подобно биологическому вирусу для жизни и размножения он активно использует внешнюю среду:

- память компьютера;
- операционную систему.

1983 (84) г. – Фред Коэн при исследовании самовоспроизводящихся (саморазмножающихся) программ впервые ввел термин «компьютерный вирус»

Вирусы. Техники (1990е)

Stealth (**стелс**, **невидимость**) – способность вируса заражать файлы скрытно, не давая пользователю повода заподозрить неладное

Polymorph (**полиморфизм**) – способность вируса шифровать свое тело так, чтобы никакие две копии вируса не были похожи друг на друга

Armored (**защита**, **бронирование**) – способность вируса сопротивляться отладке и дизассемблированию

Multipartite (**многосторонность**) – способность вируса заражать и программы, и загрузочные сектора дисков

Червь Морриса

ноябрь 1988

первая эпидемия, вызванная сетевым червем.

Из-за ошибок в коде безвредная по замыслу программа (вскрытие паролей) неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы.

Заразил 6000 - 9000 компьютеров в США
(+ Исследовательский центр NASA)

4 мая 1990 года - суд над автором

- 3 года условно
- 400 часов общественных работ
- штраф в 10 тысяч долларов США.

Криптография. История развития

Информационная безопасность

- защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Составляющие ИБ

Доступность

возможность за приемлемое время получить требуемую информационную услугу.

Целостность

актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность

защита от несанкционированного доступа к информации.

Термины

Угроза - потенциальная возможность определенным образом нарушить ИБ

Атака - попытка реализации угрозы

Злоумышленник - тот, кто предпринимает такую попытку

Источники угрозы - потенциальные злоумышленники

Окно опасности - промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.

Для ликвидации окна опасности:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Классификация угроз

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность);

- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Наиболее распространенные угрозы доступности:

- непреднамеренные ошибки
- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры

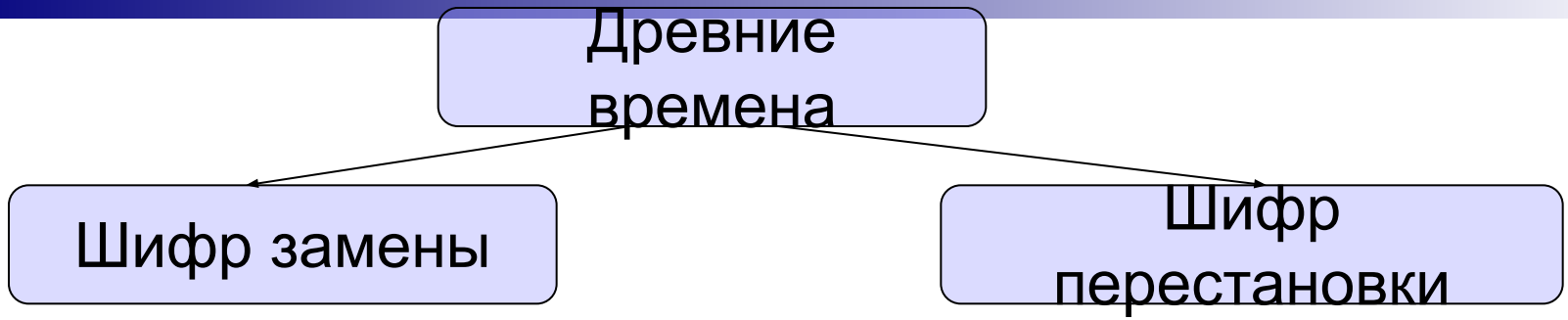
Программные атаки на доступность:

Агрессивное потребление ресурсов
- локальное
- удаленное

Вредоносное ПО
- вирусы
- черви
- трояны

Способы защиты информации

- Силовые методы защиты
- Стеганография – сокрытие самого факта наличия секретной информации
- Криптография – преобразование смыслового текста в некий хаотический набор знаков (букв алфавита)



Шифр Гая Юлия Цезаря (I в.до н.э.)

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У

РИМ → УЛП

Ключ – величина сдвига второй строки (3)

Цезарь Август – ключ сдвиг 1

РИМ → ???

Развитие шифра Цезаря

Произвольное расположение букв 2-й строки

33 варианта ключей при стандартном расположении

33! – при произвольном (подбор ключа займет столетия)

Шифр перестановки

1 2 3 4 5

3 2 5 1 4 ***- подстановка***

(перестановка)

5 – степень

РИМСКАЯ ИМПЕРИЯ

РИМСК АЯИМП ЕРИЯЪ

СИРКМ МЯАПИ ЯРУЪИ

Расшифровка – разбиваем текст на 5-ки

- обратная перестановка

Прибор Сцитала

Древняя Спарта V в. до н.э.

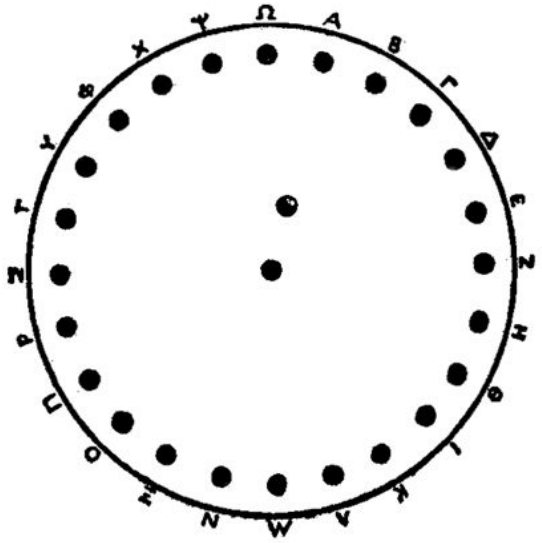
Шифр маршрутной перестановки

Ключ – диаметр цилиндра

Антисцитала - Аристотель

Античность

- **Диск Энея**



- **Линейка Энея**

(шифрование по линейке с использованием узелков)

- **Узелковое письмо**

Античность

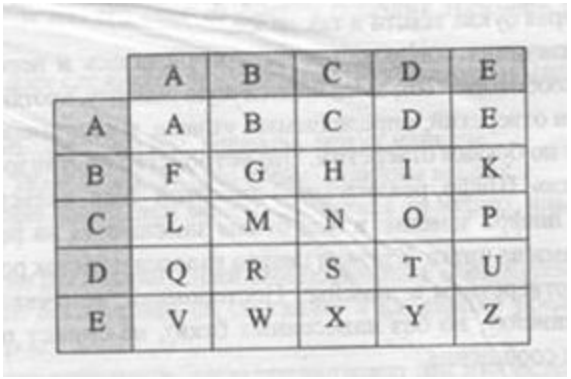
- **Книжный шифр (Эней)**

дырочки в книге над буквами секретных сообщений (исп. в 1 Мировую войну = газета+чернила)

- **Квадрат Полибия**

(др. греч. гос. деятель)

BALL →***ABAACACA***



	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

- **Усложненный квадрат Полибия**

Ключ THE TABLE

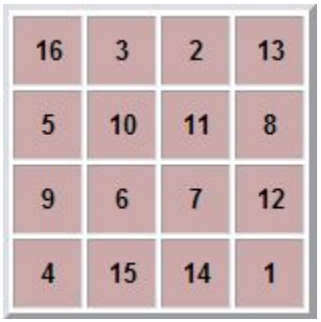
T	H	E	A	B
L	C	D	F	G
I	K	M	N	O
P	Q	R	S	U
V	W	X	Y	Z

Античность

- **Тюремный шифр**

(Полибий, но с числами. Простукивается позиция по строке и столбцу)

- **Магические квадраты**



Приезжаю сегодня

Ъирдзегюсжаоеянп

16 Ъ	3И	2Р	13Д
5З	10Е	11Г	8Ю
9С	6Ж	7А	12 О

Исторические книги по криптографии

Абу Вакр Ахмед бен Али бен Вахшия ан-Набати

«Книга о большом стремлении человека разгадать загадки древней письменности»

1412 – Шехаб аль Кашканди

«Относительно сокрытия в буквах тайных сообщений»

XI – XII Омар Хайям

XIV – XV Чикко Симонетти

XV – Габриель де Лавинда

«Трактат о шифрах» - 1ый европейский учебник

Леон Альберти (частота появления букв в текстах, итал.)

«сеновалитр»

Шифр Тритемия

XV – аббат Тритемий, Германия

«Периодически сдвигаемый ключ»

Таблица Тритемия

- Введение произвольного порядка расположения букв исходного алфавита
- Применение усложненного порядка выбора строк таблицы при шифровании

Шифры. Продолжение

1940г. – Германия, Гуттенберг
книгопечатание

Книжный шифр
n/m/t (номер страницы, строки, буквы)

Шифр вольных каменщиков

(исп. Наполеон)

A:	B:	C:
D:	E:	F:
G:	H:	I:

J.	K.	L.
M.	N.	O.
P.	Q.	R.

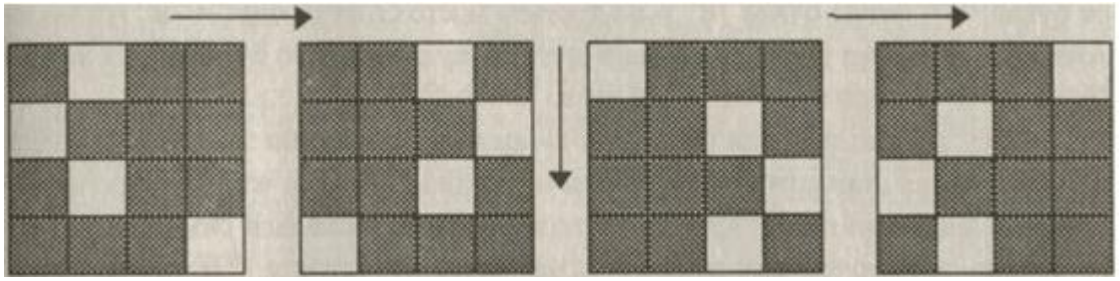
S	T	I
V	W	X
Y	Z	

Шифры. Продолжение

Диск Альберти – XVI в.

«двойное шифрование»

Шифры Кардано



Шифры. Продолжение

Библия (осмысленные слова)

Шифр «Атбаш»

A B C ….X Y Z

Z Y X …..C B A

Шифр «Альбам»

A B C …. K L

M N O…..Y Z

Шифр Фальконера

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЪЬЭЮЯ

1 3 5 67

2 4

Ключ – ЛИЛИПУТ (3142576)

3	1	4	2	5	7	6
ш	и	ф	р	в	е	р
т	и	к	а	л	ь	н
о	й	п	е	р	е	с
т	а	н	о	в	к	и

Выписываем по столбцам:

Иийараеоштот…….

Черные кабинеты

XVI в. – органы дипломатической службы

XVII-XVIII – эра «черных кабинетов»

перехват, дешифрование переписки

Д. Кан

«Криптография является наиболее важной формой разведки в современном мире. Она дает намного больше и намного более достоверной информации, чем шпионаж»