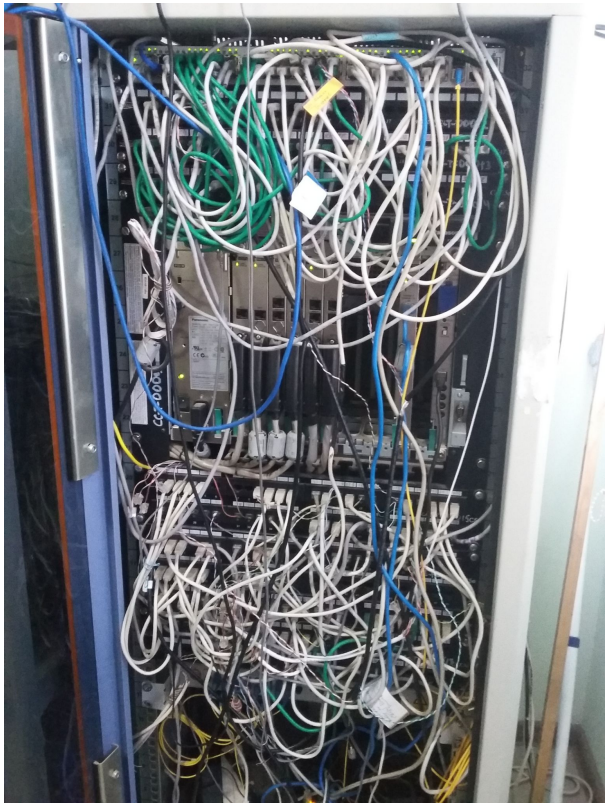
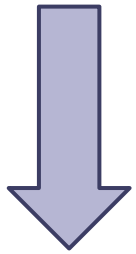
# Вычислительные сети и контроль безопасности в компьютерных сетях

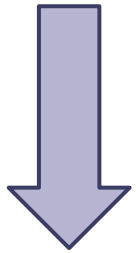


# Структура курса

| |
|---|
| Введение в безопасность КС. Основные понятия. |
| Безопасность физического и канального уровней. |
| Безопасность ARP. Безопасность на уровне порта - 802.1x |
| Безопасность на сетевом уровне. IP, ICMP, IPv6 |
| Прикладная криптография. Виртуальные частные сети. |
| Безопасность транспортного уровня. |
| Анализ защищенности сетевых ресурсов. |
| Фильтрация трафика. Межсетевые экраны. |
| Безопасность протоколов прикладного уровня. |
| Современные проблемы и тенденции развития сетевой безопасности. |



Рубежный контроль



Лабораторный практикум

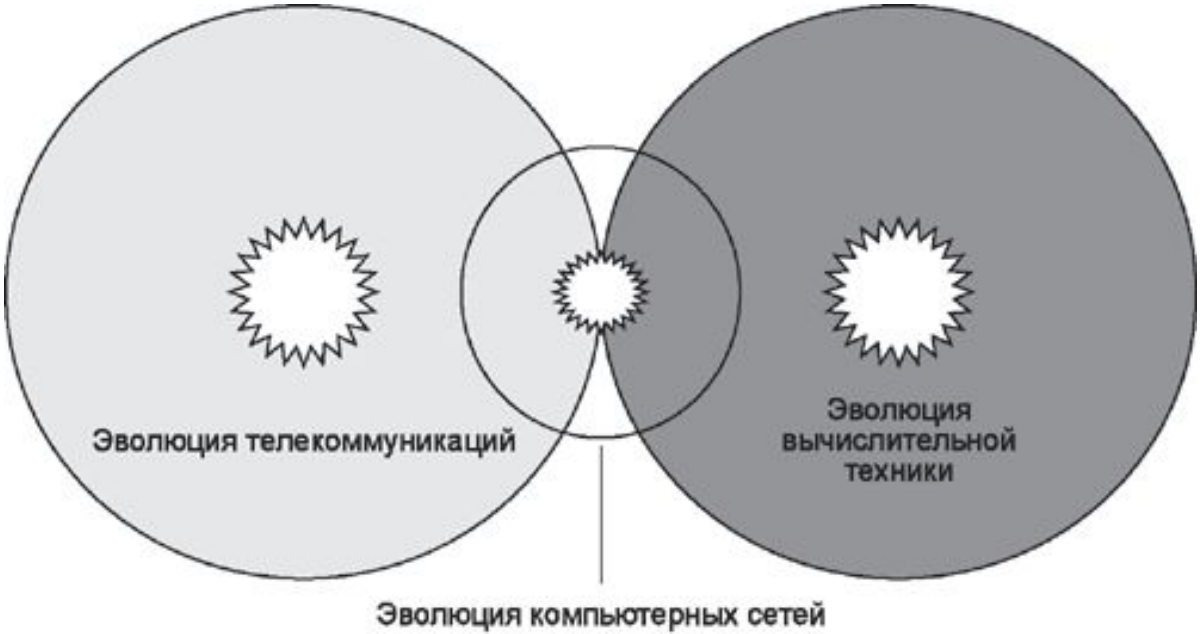
Экзамен

# Вычислительные (компьютерные) сети

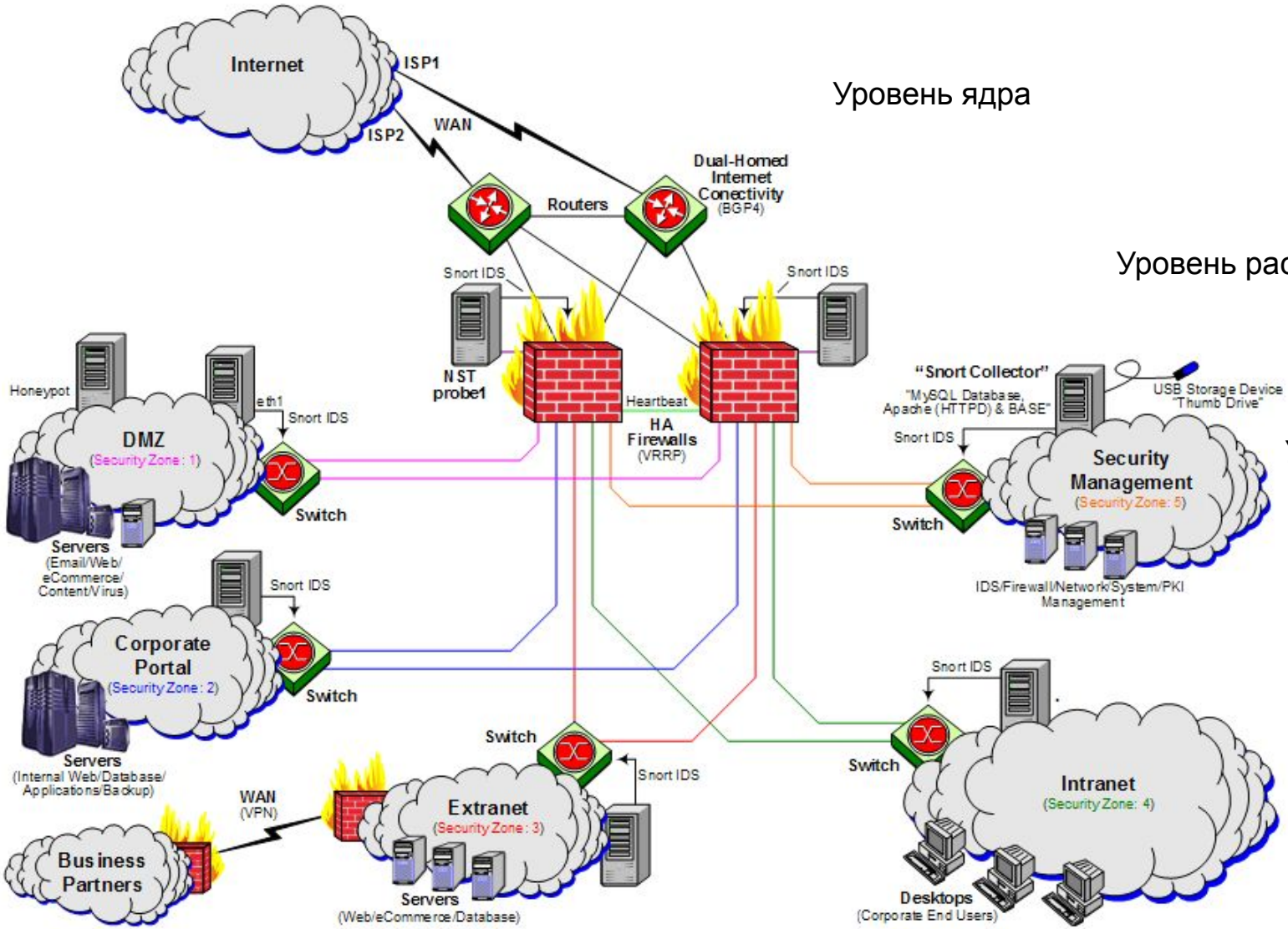
**Вычислительная сеть** - система, обеспечивающая обмен данными между вычислительными устройствами:

- клиенты;
- серверы;
- сетевое оборудование

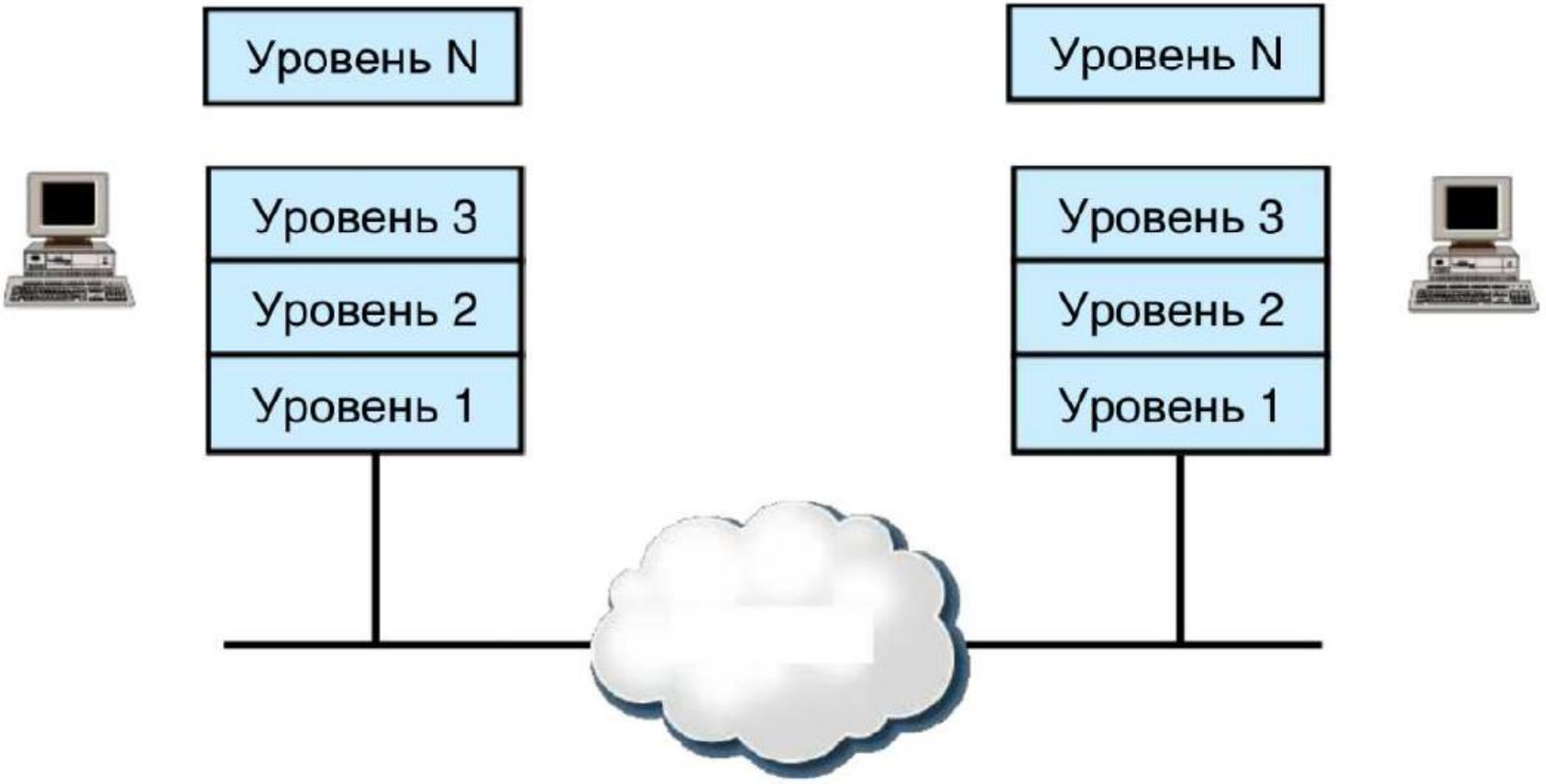
} Линии связи



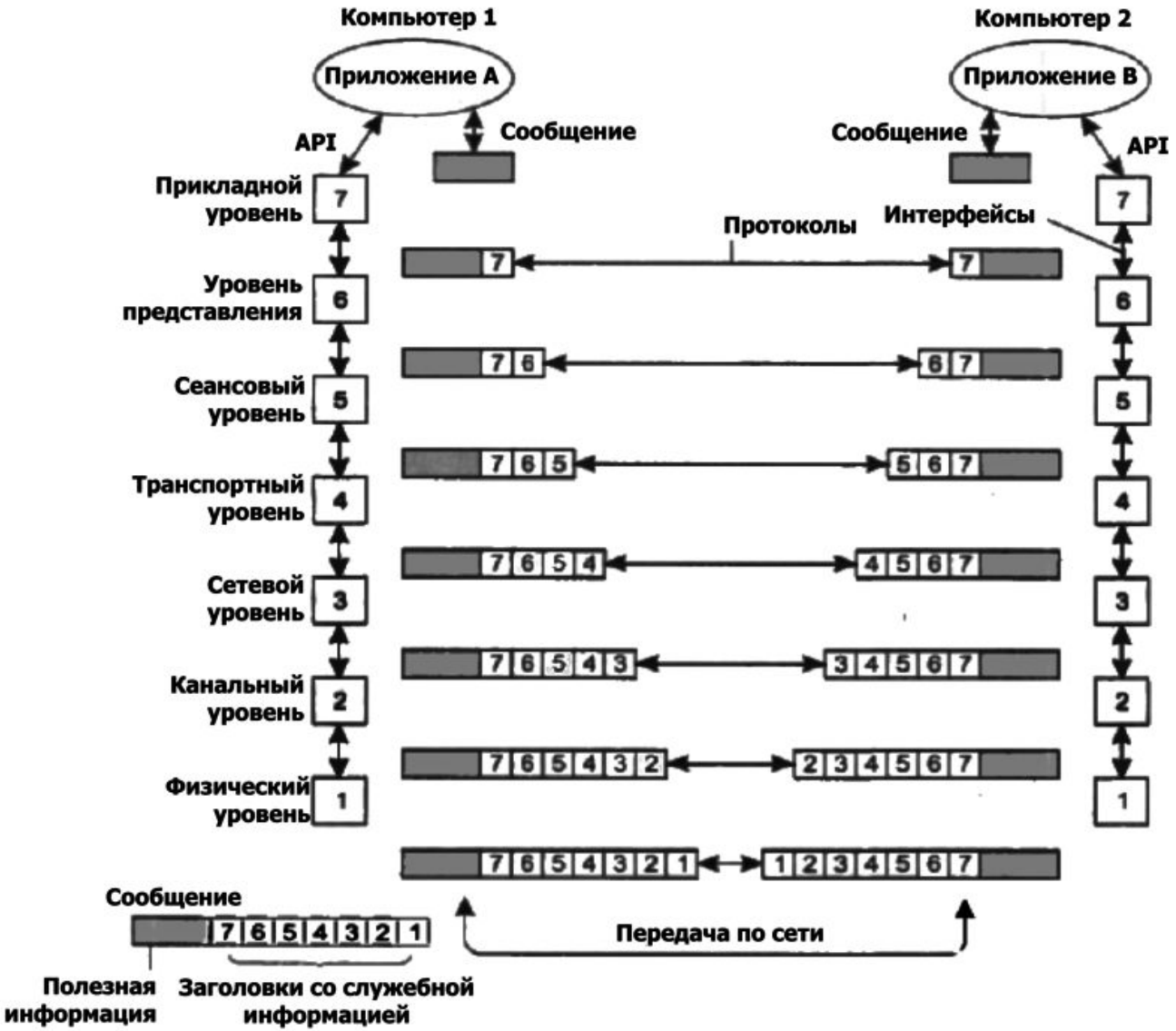
# Типовая IP сеть организации



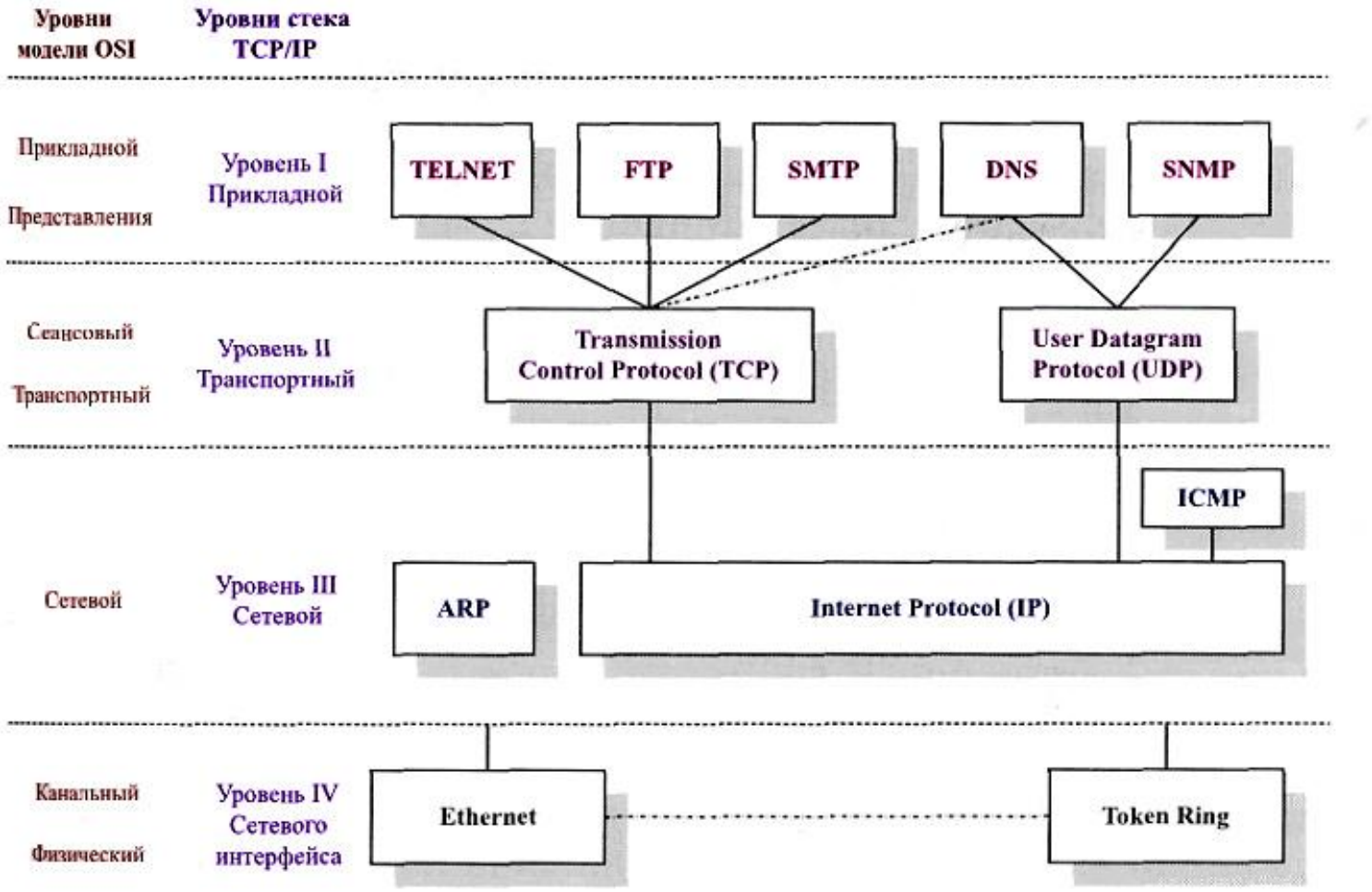
# Сетевое взаимодействие – многоуровневый подход



# Модель OSI


Компьютер 1
Компьютер 2
Приложение A
Приложение B
API
Сообщение
Сообщение
API
Прикладной уровень
Протоколы
Интерфейсы
Уровень представления
Сеансовый уровень
Транспортный уровень
Сетевой уровень
Канальный уровень
Физический уровень
Сообщение
Передача по сети
Полезная информация
Заголовки со служебной информацией

# Структура стека TCP/IP



# Безопасность

- состояние ***защищенности*** жизненно важных интересов личности (1), общества (2), государства (3) от внутренних (a) и внешних (b) ***угроз*** (security)

- способность предмета, явления или процесса *сохраняться при разрушающих воздействиях* (safety)

**- условия, в которых находится сложная система, когда действие внешних и внутренних факторов не приводит к процессам, которые считаются негативными по отношению к данной сложной системе в соответствии с имеющимися на данном этапе потребностям, знаниям и представлениям**

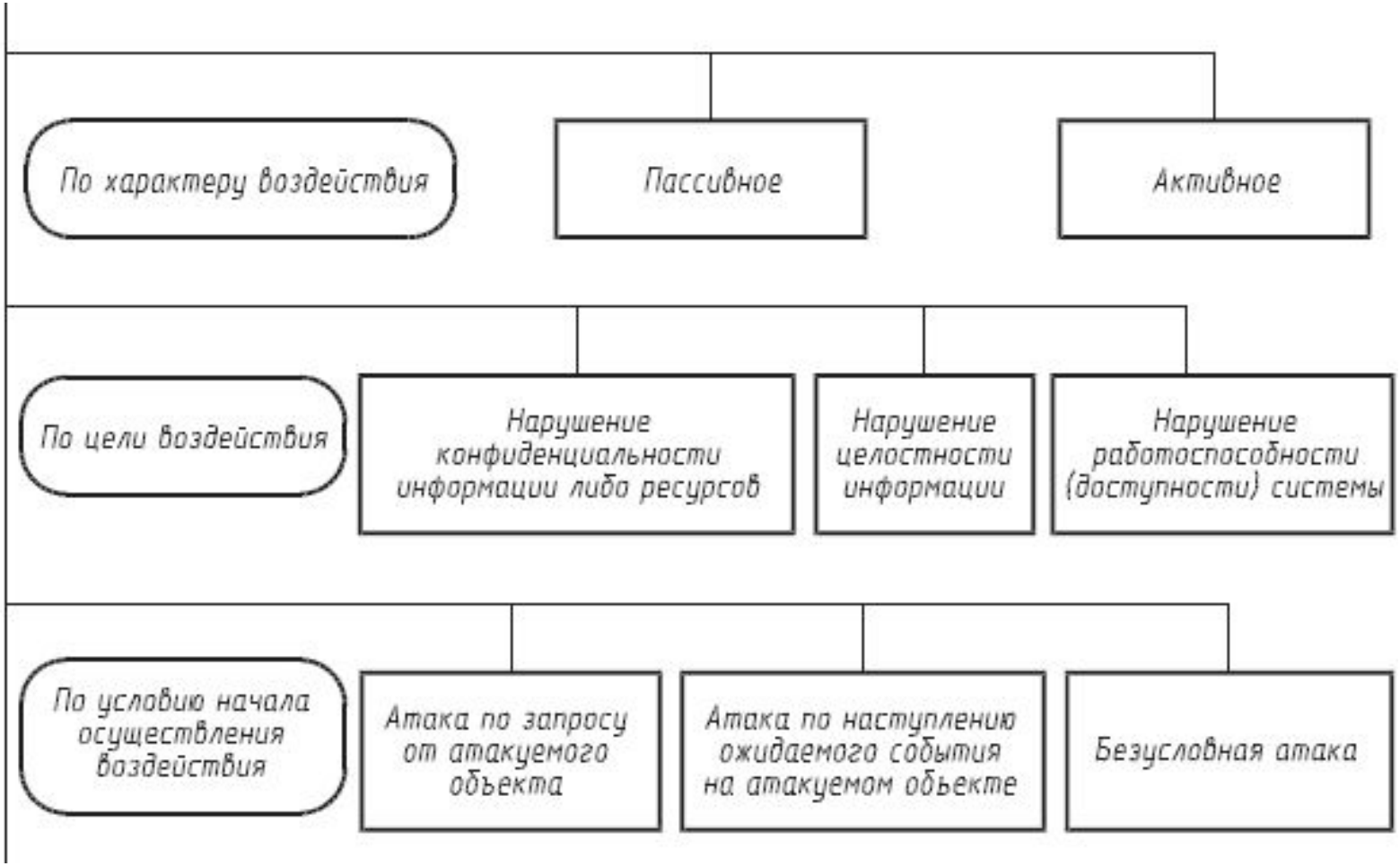
# Составляющие информационной безопасности

- **Конфиденциальность**: Обеспечение доступа к информации только авторизованным пользователям.
- **Целостность**: Обеспечение достоверности и полноты информации и методов ее обработки.
- **Доступность**: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

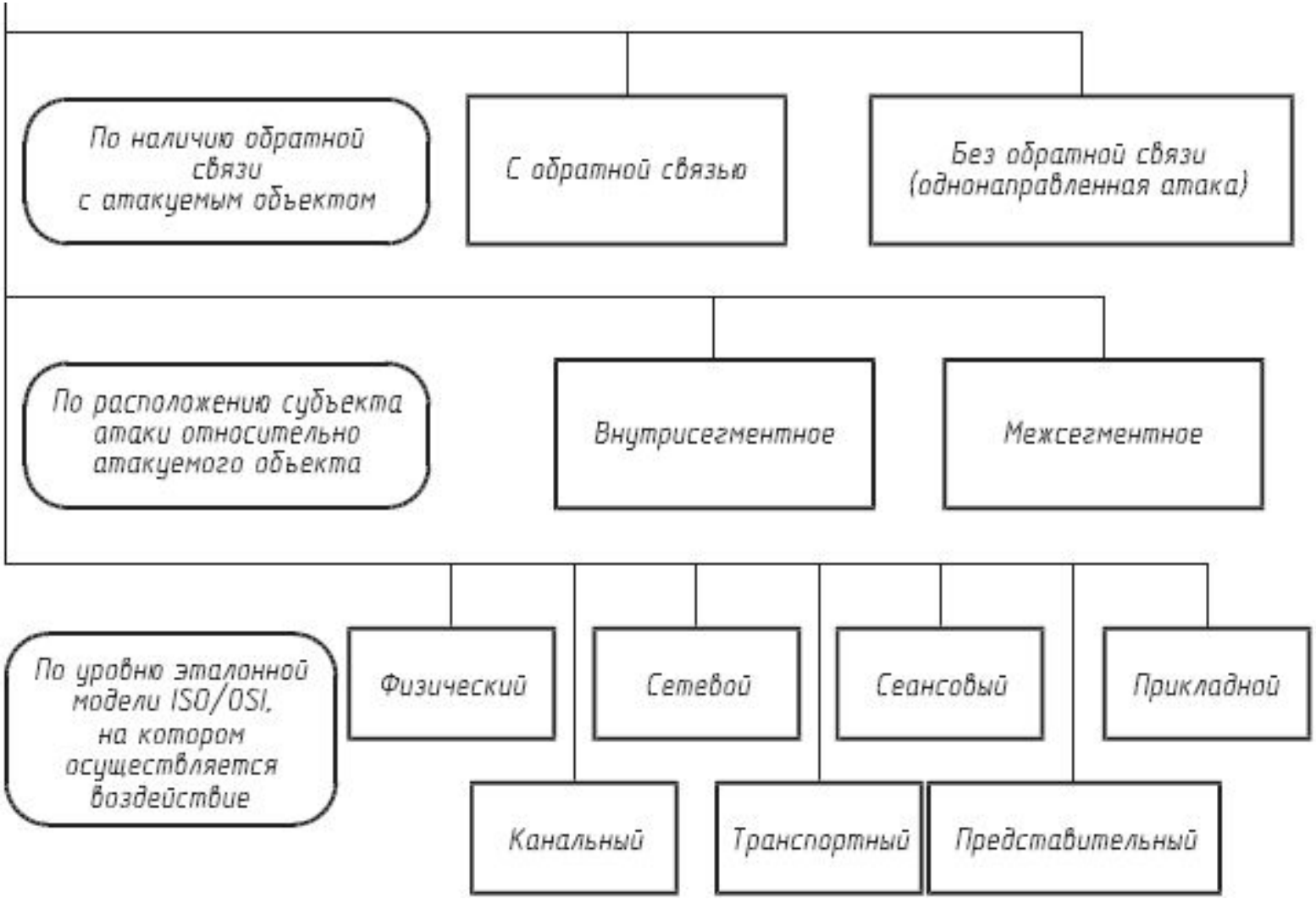
# Угрозы, уязвимости и атаки

- **Угроза** безопасности КС - это потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.
- **Уязвимость** КС - это некая ее характеристика, которая делает возможным возникновение угрозы.
- **Атака** на КС - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака - это реализация угрозы.

# Классификация угроз в КС (1)



# Классификация угроз в КС (2)

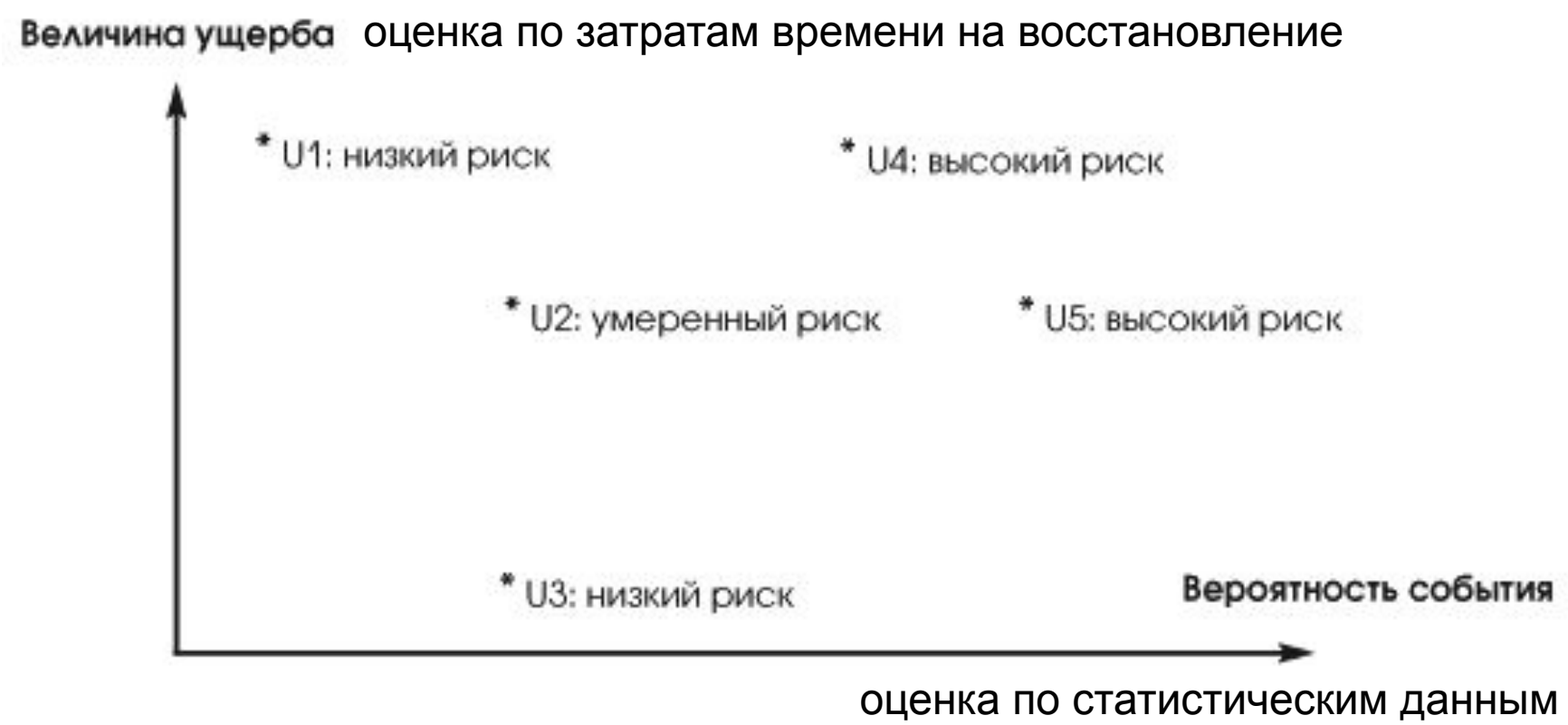


# Источники уязвимостей

- Ошибки проектирования
- Ошибки реализации
- Ошибки обслуживания

# Понятие риска в моделях угроз

Риск - сочетание **вероятности** реализации негативного события и его последствий (**ущерба**)



# Мера риска

- Качественный подход (светофорная модель):
  - Высокий риск
  - Средний риск
  - Низкий риск
- Количественный подход
  - Вероятность негативного сценария
  - Ущерб от негативного сценария

# Каталоги уязвимостей

- SANS Top 20 Internet Vulnerabilities List
  https://www.sans.org/critical-security-controls/
- Common Vulnerabilities and Exposures (CVE)
  http://cve.mitre.org/
- National Vulnerability Database
  https://nvd.nist.gov/

# Механизмы реализации сетевых атак

- Пассивное прослушивание
- Подозрительная активность
- Бесполезное расходование вычислительного ресурса
- Нарушение навигации
- Выведение из строя
- Запуск кода на объекте атаки

# Механизмы защиты

- **Превентивные** (предотвращают использование уязвимости)
- **Детективные** (позволяют своевременно обнаружить атаку)
- **Коррективные** (позволяют восстановить систему за приемлемый срок)

# Контроль безопасности

- Мониторинг - система постоянного наблюдения за событиями в вычислительной сети (оценка->контроль->управление)
- Аудит безопасности - комплексный анализ всех элементов и процессов в вычислительной сети с целью выявления уязвимостей
- Реагирование
  - Политики безопасности
  - Кризисные протоколы

# Выводы

- Необходим комплексный, системный подход к обеспечению безопасности КС.
- На каждом уровне должны обеспечиваться все механизмы защиты.
- Система защиты должна постоянно модифицироваться с учетом информации о новых уязвимостях.