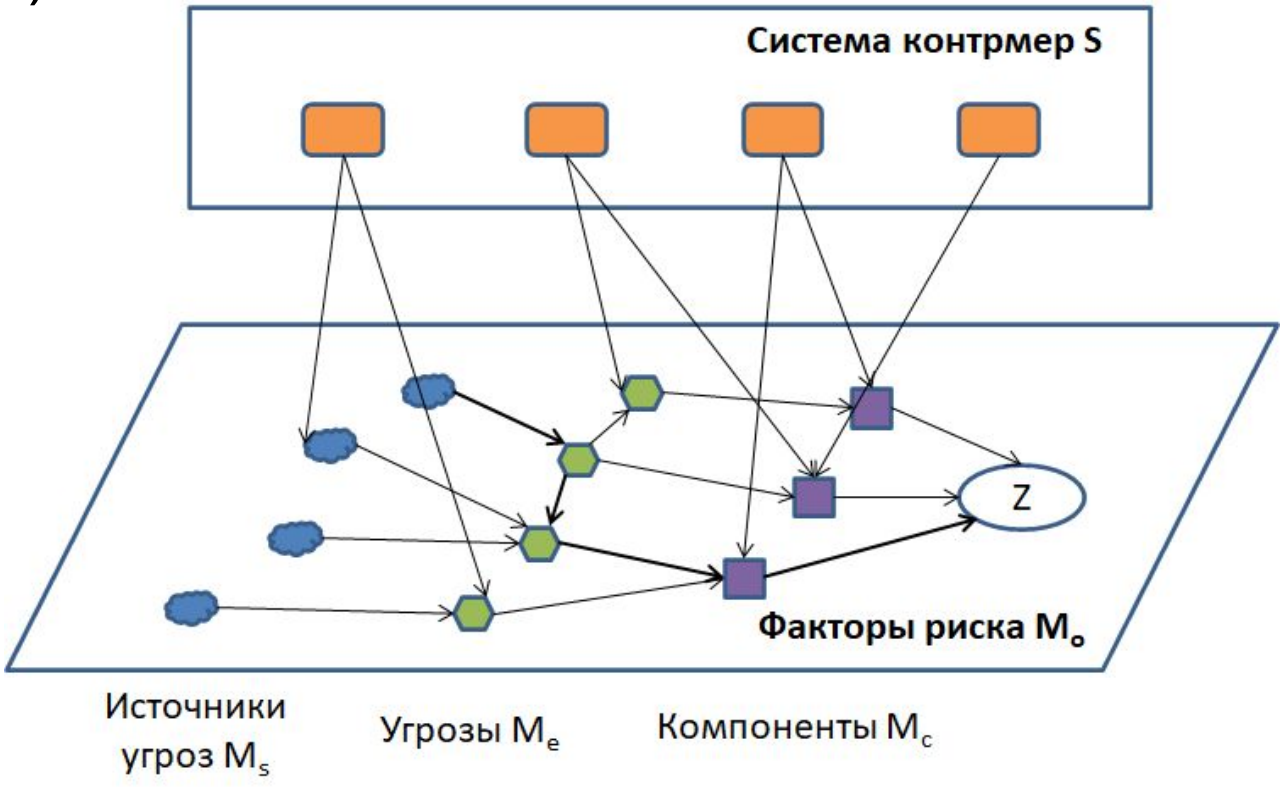
Информационная безопасность - основные понятия

- Безопасность
- Угроза
- Уязвимость
- Риск
- Источник угрозы
- Модель угроз
- СЗИ (контрмера)

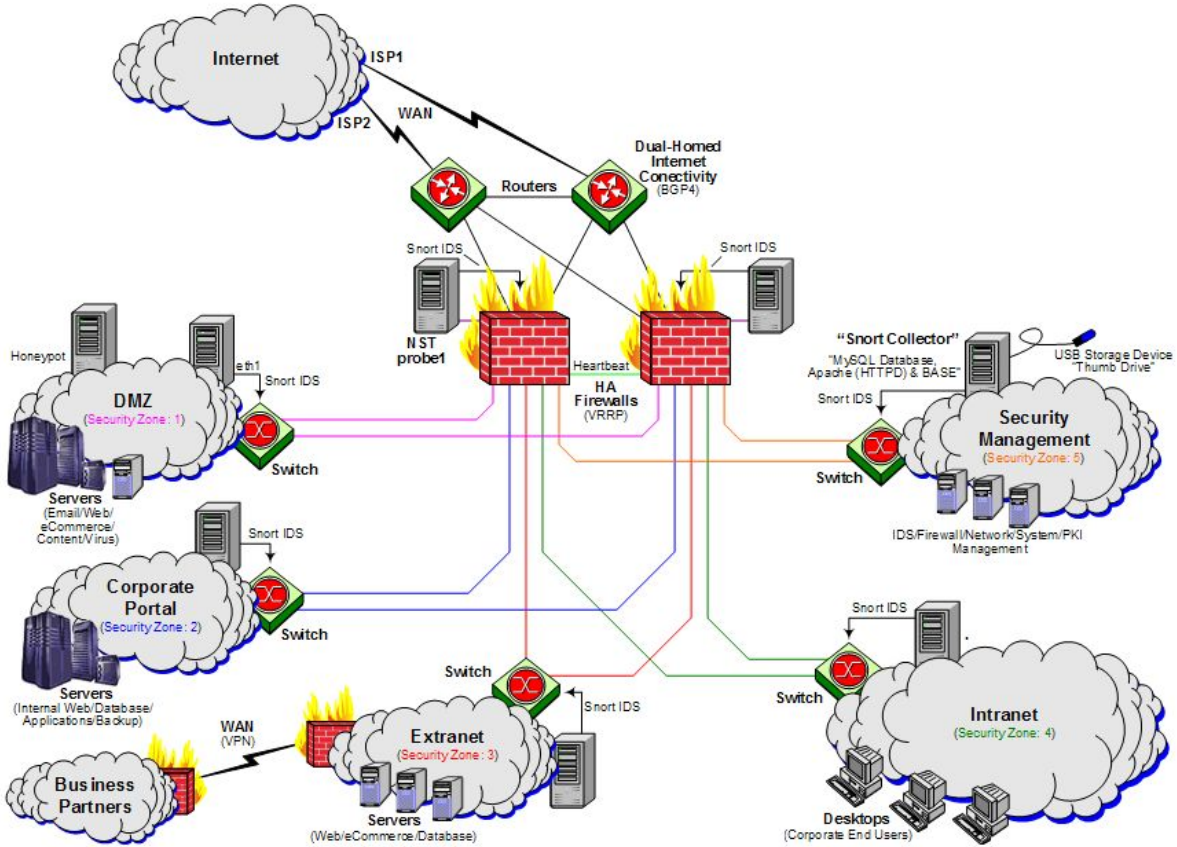
Метрика риска в моделях угроз

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

Структура модели угроз (установление причинно-следственных связей+целенаправленное включение контрмер)



Структурный аспект сетевой безопасности



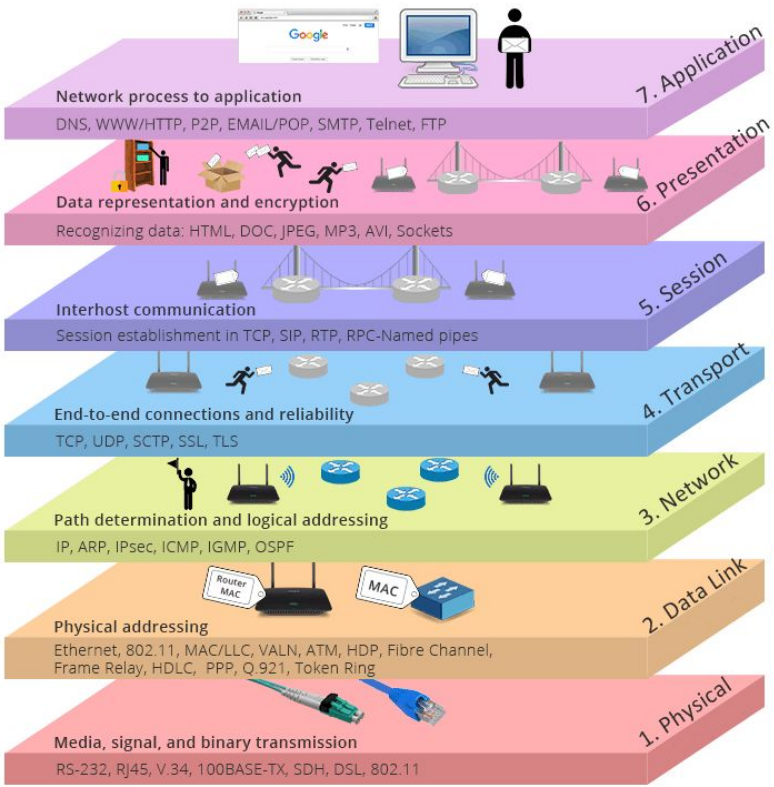
Функциональный аспект сетевой безопасности

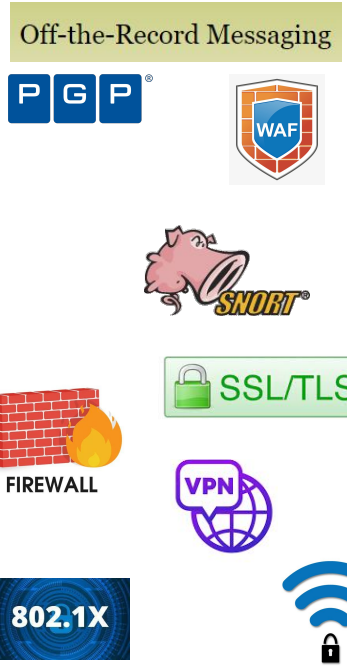
эксплуатация уязвимостей конечного приложения, XSS, SQL-инъекции, HTTP-flood

атаки на уровне сетевого сервиса, подмена TCP сессии, SYN-flood

перехват трафика на транзитных узлах, вмешательство в работу маршрутных протоколов, ICMP-flood

НСД к разделяемой среде, sniffing, сканирование сети, ARP-spoofing





Дано

- объект - сетевая инфраструктура
- компоненты - внутренняя сеть, удаленные устройства, внутренние сервисы, внешние сервисы, каналы коммуникации
- контекст - по группам

Нужно сделать

- модель угроз (каталог угроз)
- оценка угроз (качественная шкала) + обоснование
- система контрмер