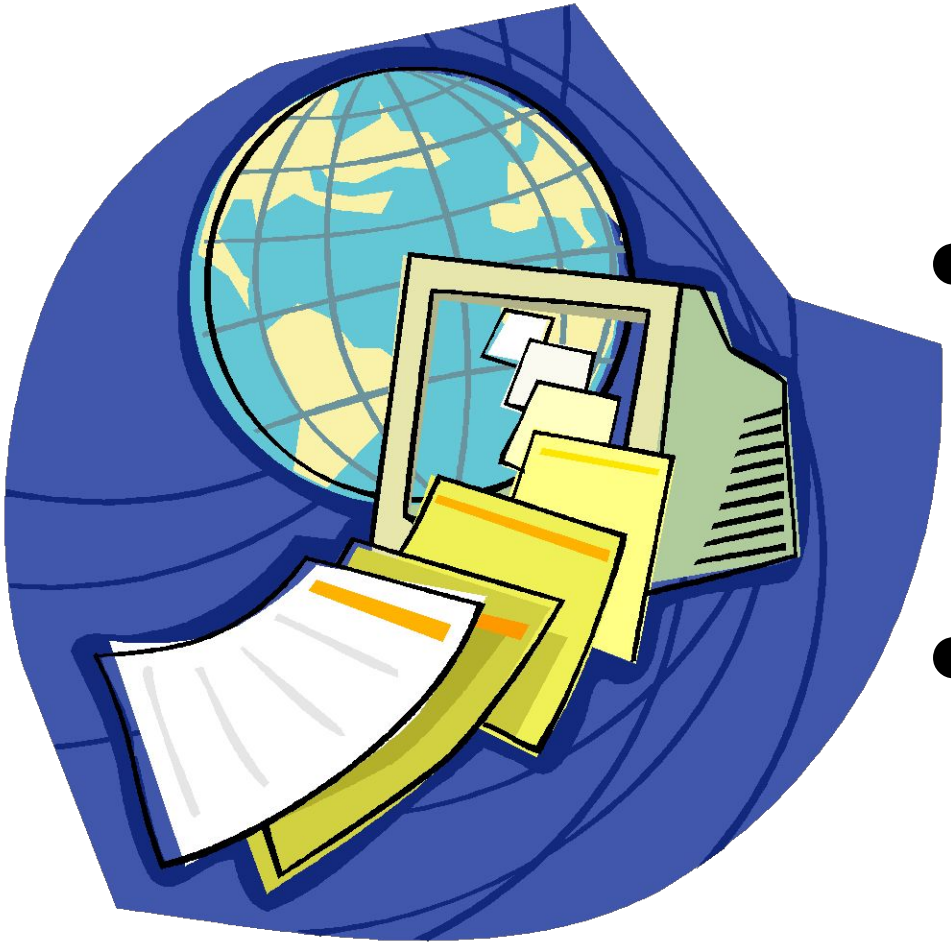
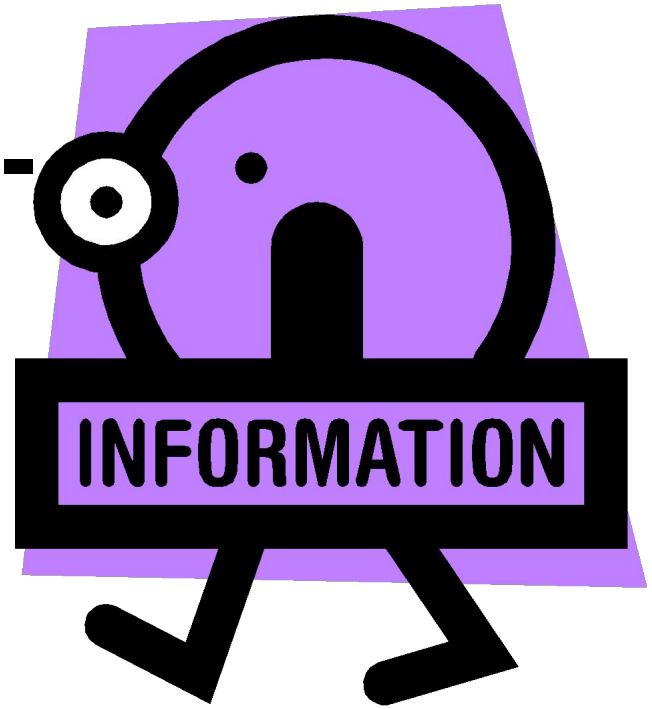
Стратегии и модели информационной защиты

Объекты информационной защиты



- Предприятия, предоставляющие услуги связи
- Банковская сфера

Защита информации - сугубо практическая сфера деятельности, поскольку в каждом случае речь идет о конкретной информации, конкретных опасностях и конкретных способах защиты



Информационные угрозы предприятиям, предоставляющим услуги телефонной связи

- Незаконное подключение к абонентским линиям связи с целью бесплатного пользования ими
- Незаконное подслушивание (запись) телефонных переговоров
- Распространение данных о служебных телефонах и их пользователях
- Сверхнормативное использование ресурсов за обычную абонентскую плату

Информационные угрозы предприятиям, предоставляющим услуги телефонной связи

- Использование незарегистрированных оконечных устройств
- Повреждение линий связи с целью хищения цветных металлов
- Вандализм (повреждение таксофонов и др.)
- Подделка телефонных карточек и жетонов

Направления информационной защиты

- Физическая охрана АТС, линий связи, распределительных устройств, таксофонов
- Законодательные санкции за повреждение линий связи, подслушивание, незаконное подключение к каналам
- Обеспечение конфиденциальности переговоров и регистрационных данных
- Бдительность пользователей

Информационные угрозы предприятиям, предоставляющим услуги мобильной связи

- Слежение за расположением (перемещением) пользователей
- Перехват и расшифровка содержания сообщений и телефонных переговоров
- Изготовление и использование «двойников» абонентских устройств
- Создание радиопомех на частотах сетей сотовой и пейджинговой связи

Направления информационной защиты

- Использование стандартов и протоколов, обеспечивающих надежную криптозащиту сообщений
- Законодательные санкции за перехват информации с помощью СТС
- Обеспечение сохранности компьютерных баз данных с информацией о состоявшихся соединениях и содержании сообщений
- Бдительность пользователей

Информационные угрозы в банковской сфере

- Незаконный доступ к данным о вкладах
- Получение данных о размещении и перемещении наличных денег (выручки, заработной платы и др.)
- Получение незаконного доступа к электронным платежным системам от имени законного клиента или торгового агента
- Подделка кредитных карточек и иных платежных документов

Направления информационной защиты

- Физическая охрана хранилищ, расчетных узлов, транспортных средств и персонала
- Создание и эксплуатация защищенных компьютерных сетей, в которых циркулирует банковская информация
- Изготовление кредитных карт с высокими степенями защиты
- Использование системы ЭЦП
- Использование защищенных протоколов в Интернет

Принципы информационной защиты

- Разрушение опасности (разрушение цепочки условий, приводящей к опасным последствиям, на основе моделирования деревьев угроз)
- Защита расстоянием и движением (в условиях физического или логического пространства)
- Защита временем (или защита на время)
- Создание препятствий нарушителю
- Контроль и аудит
- Прогнозирование
- Ограничение информированности

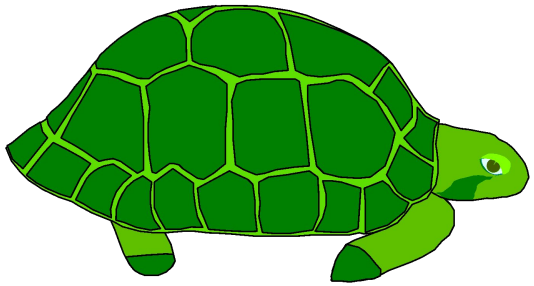
Принципы информационной защиты

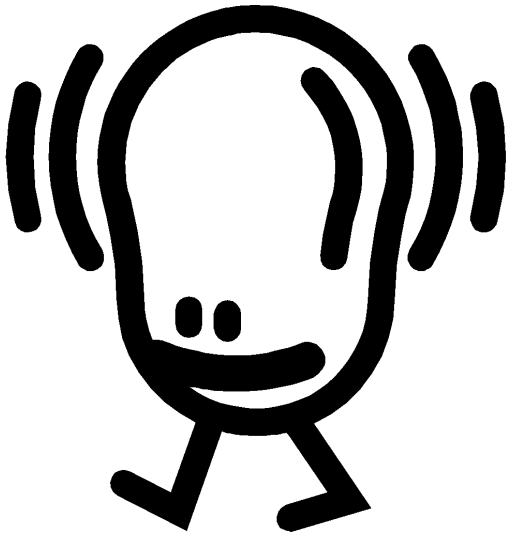
- Защитное блокирование
- Разделение защищаемых ценностей
- Резервирование
- Адекватность угрозам и разумная достаточность
- Управление рисками
- Простота
- Принцип «слабого звена» и др.

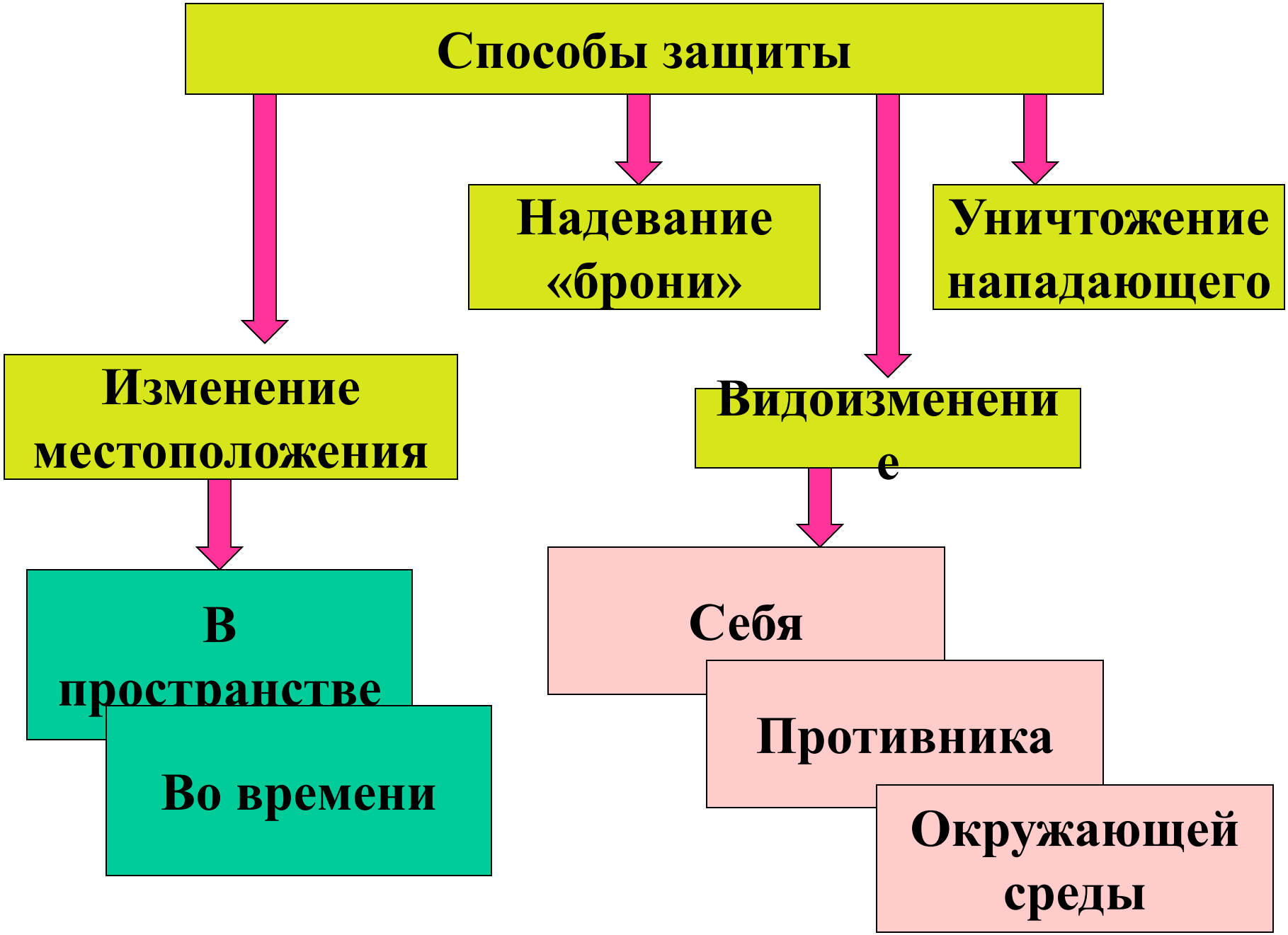
Модель абсолютной защиты

(С. П. Расторгуев)

Модель абсолютной защиты

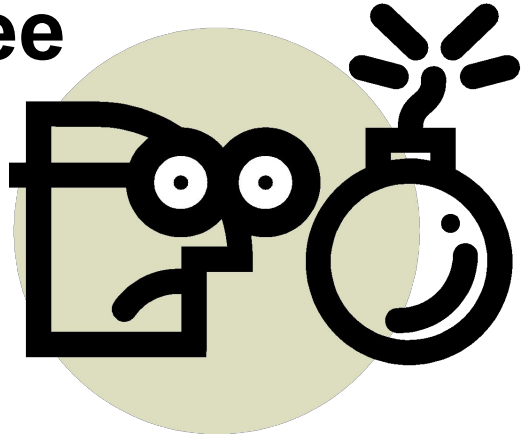


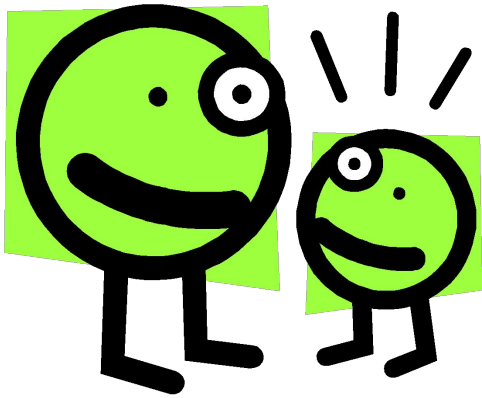



Способы защиты
Надевание «брони»
Уничтожение нападающего
Изменение местоположения
Видоизменение
В пространстве
Во времени
Себя
Противника
Окружающей среды

Этапы информационной защиты

- Прогнозирование потенциальных угроз, выявление наиболее реальных из них
- Выбор разумной стратегии защиты
- Реализация превентивных и контролирующих действий
- Реализация выбранной стратегии противодействия
- Оценка причиненного ущерба и самовосстановление

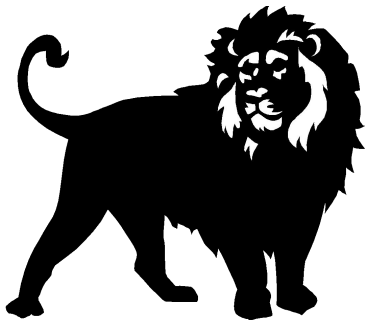




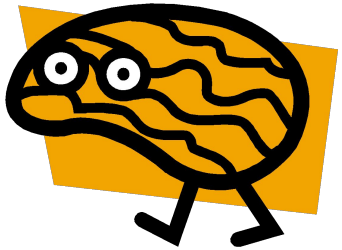
Система защиты информации должна содержать:

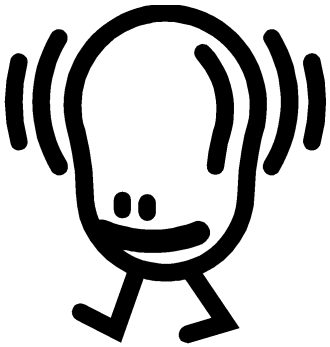
- **Рубежи вокруг источников информации, преграждающих распространение сил воздействия к источникам информации и ее носителей от источников**
- **Силы и средства достоверного прогнози-рования и обнаружения угроз**
- **Механизм принятия решения о мерах по предотвращению и нейтрализации угроз**
- **Силы и средства нейтрализации угроз, преодолевших рубежи защиты**

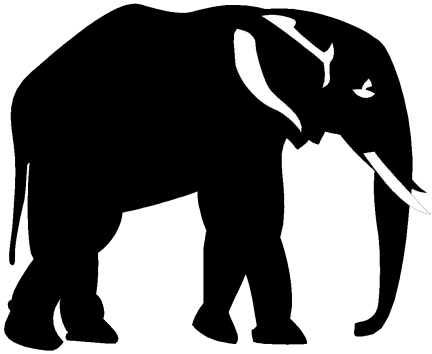
Абсолютной системой защиты следует считать систему, обладающую всеми возможными способами защиты и способную в любой момент своего существования предсказать наступление угрожающего события и вовремя защититься от него



Чем хуже работает механизм прогнозирования, тем более развитыми должны быть способы защиты (чем хуже работают мозги, тем сильнее должны быть мышцы)







Объект, обладающий абсолютной защитой, является потенциально бессмертным

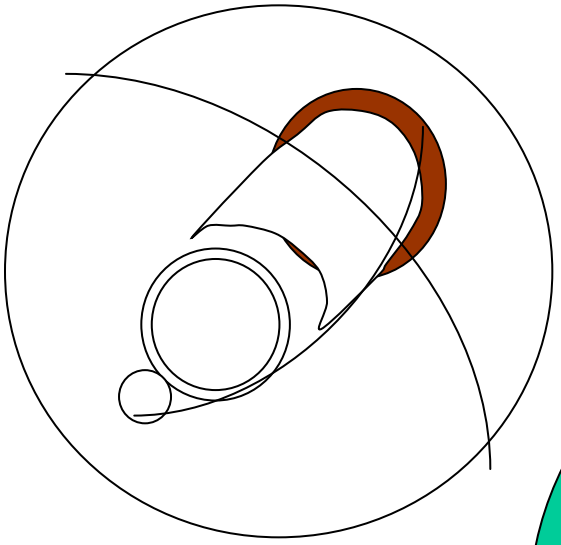
Учитывая такую возможность, Создатель в любую достаточно сложную систему вложил способность к самоуничтожению

Формы биотической защиты

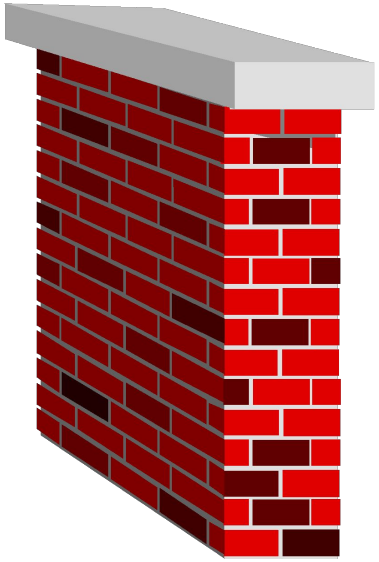
- Защита от опасной внешней среды
- Защита от паразитов, возбудителей болезней, ядов
- Защита от хищников
- Защита от конкурирующих особей

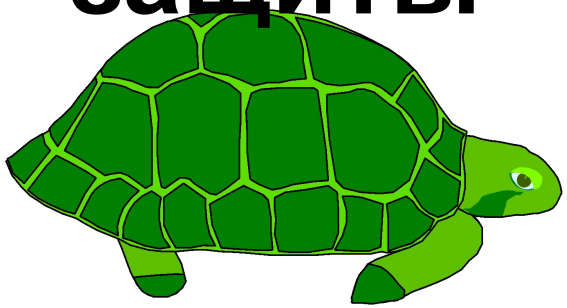
Стратегии биотической защиты

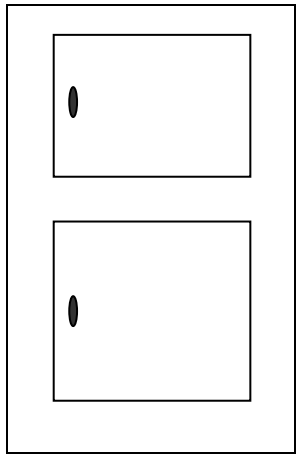
- Пассивная защита (использование убежищ и защитного покрова для индивидуальной защиты и охраны потомства)
- Бегство или маневр (включая расселение и миграцию)
- Маскировка и имитация
- Ликвидация опасности
- Защита жертвой (в индивидуальной и групповой формах)
- Создание запасов на неблагоприятный период
- Временное снижение жизненной активности (спячка, анабиоз)



Стратегия пассивной защиты







Принципы пассивной защиты

- Стратегия пассивной защиты основана на принципах изоляции и защите расстоянием
- Защищаемой ценностью являются люди, материальные ценности, источники и носители информации, каналы связи, территория объектов, на которой циркулирует информация

Принципы пассивной защиты

- Между защищаемой ценностью и источником угрозы (нарушителем) создается слой защитной субстанции (физической, энергетической, логической, смысловой)
- Пассивность защиты заключается в том, что она только сопротивляется внешнему воздействию, ослабляя угрозу до уровня безопасных значений
- Носителю опасности ущерб не причиняется

Формы реализации стратегии пассивной защиты

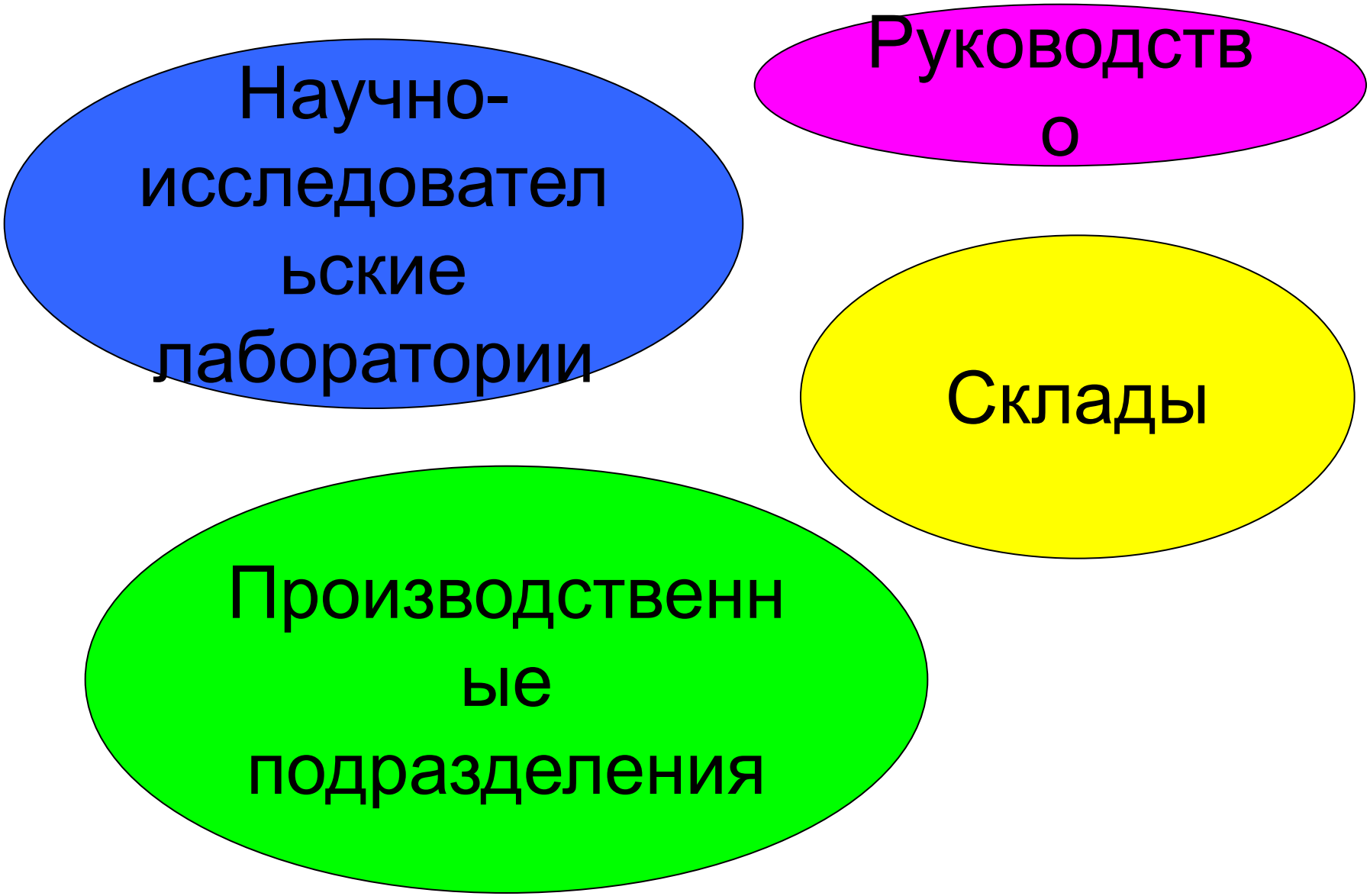
- Область контролируемого пространства
- Преграда (труднопреодолимое препятствие) на пути движения нарушителя, распространения вещества и энергии
- Электромагнитный экран
- Акустический экран

Многозональность защиты

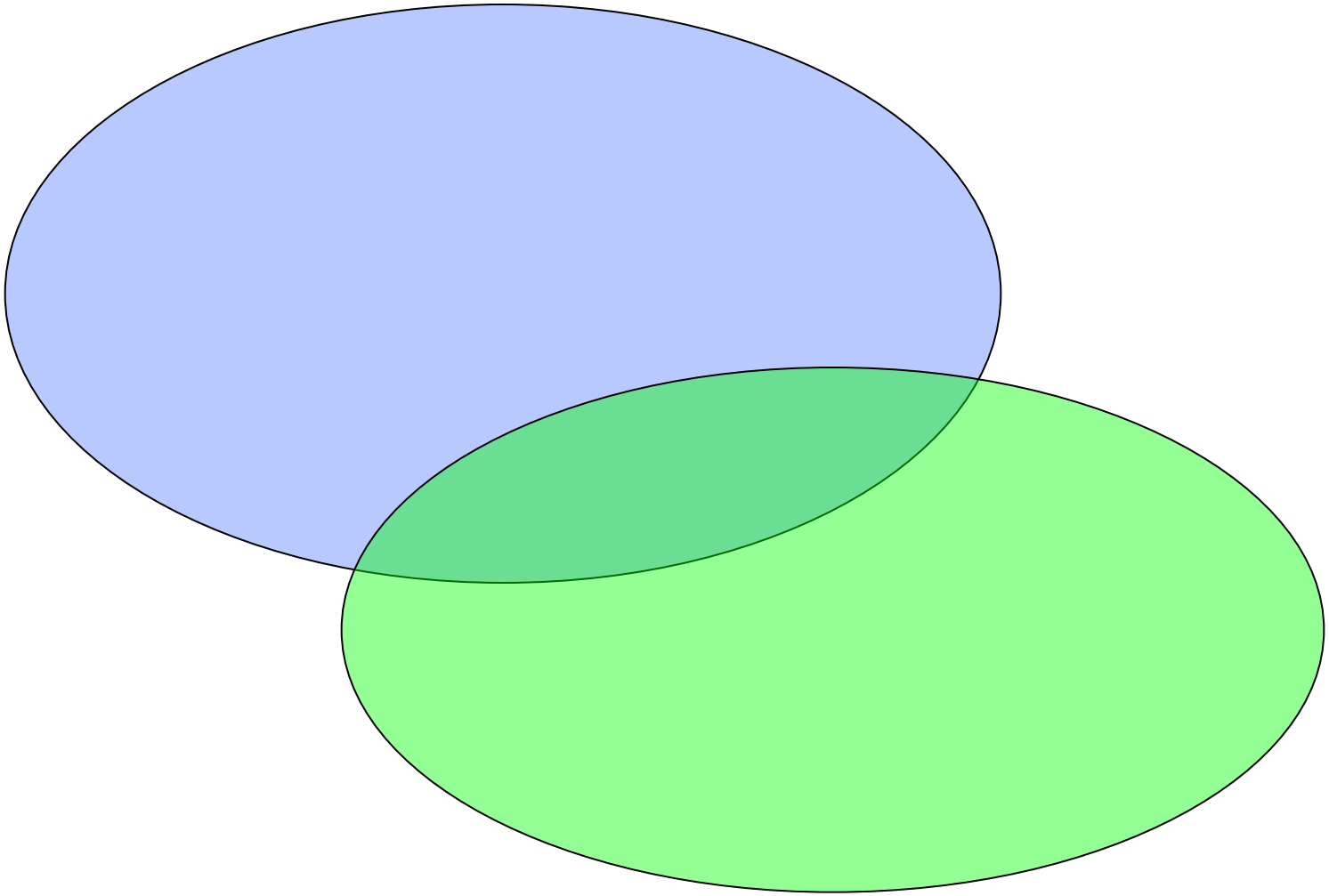
предусматривает разделение территории (государства, предприятия, здания и пр.) на отдельные контролируемые зоны, в каждой из которых обеспечивается уровень безопасности, соответствующий ценности находящейся там информации

чем больше зон, тем более рационально используется ресурс системы, при этом усложняется организация защиты информации

Зоны подразделяют на независимые

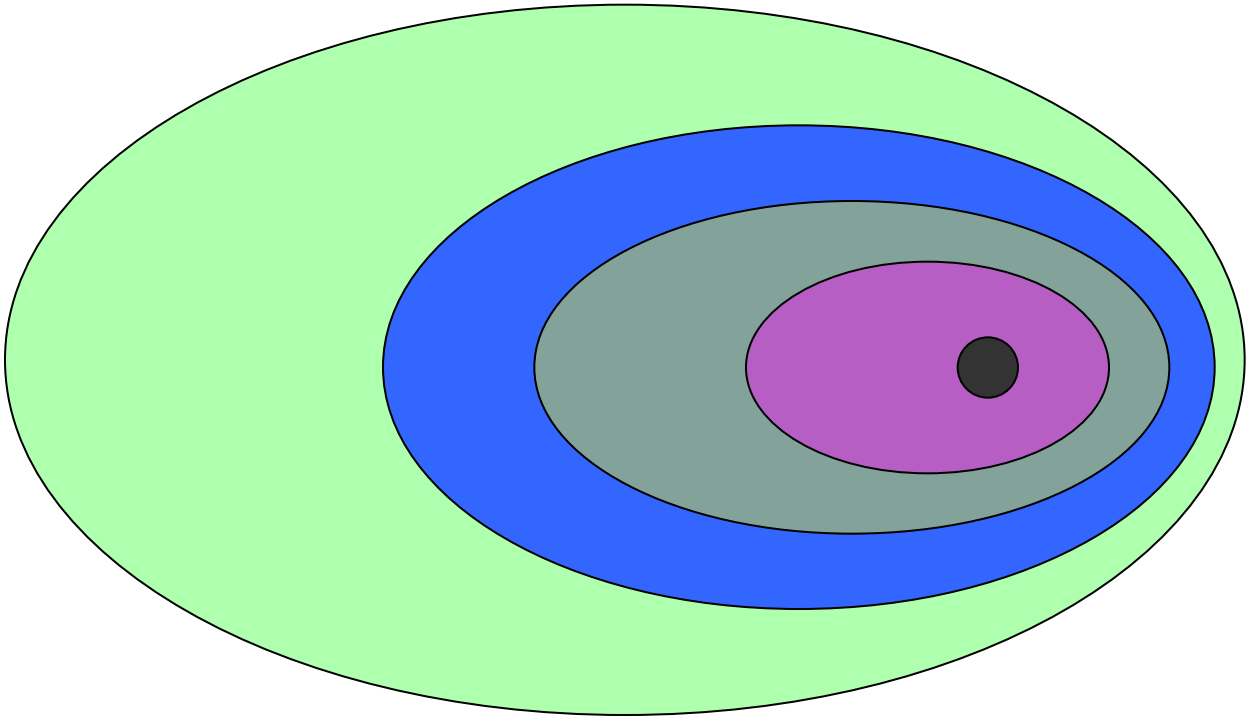


пересекающиеся зоны



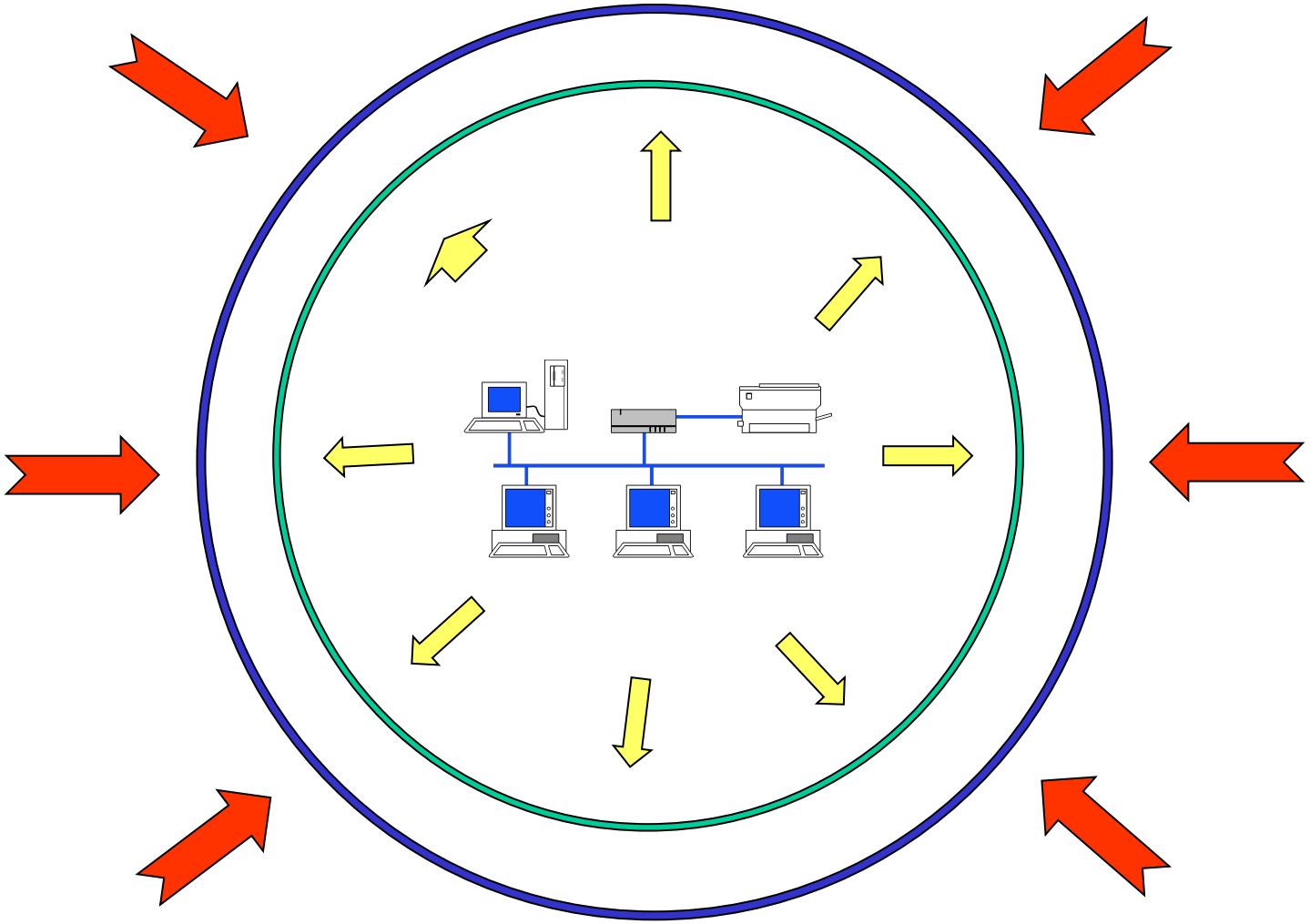
Например, приемная руководителя организации

вложенные зоны



Наиболее распространены, так как позволяют экономнее обеспечивать требуемый уровень безопасности информации – безопасность i-й вложенной зоны обеспечивается уровнями защиты в предшествующих зонах

Многослойная защита



Внешний слой защиты (контролируемая зона)

Внутренний слой защиты

Виды многослойной защиты

- Защита тоталитарного государства от идеологически вредной информации
- Защита секретной информации и секретоносителей
- Защита от использования своих кадров в интересах конкурирующей организации и др.

Задачи наружного слоя изоляции

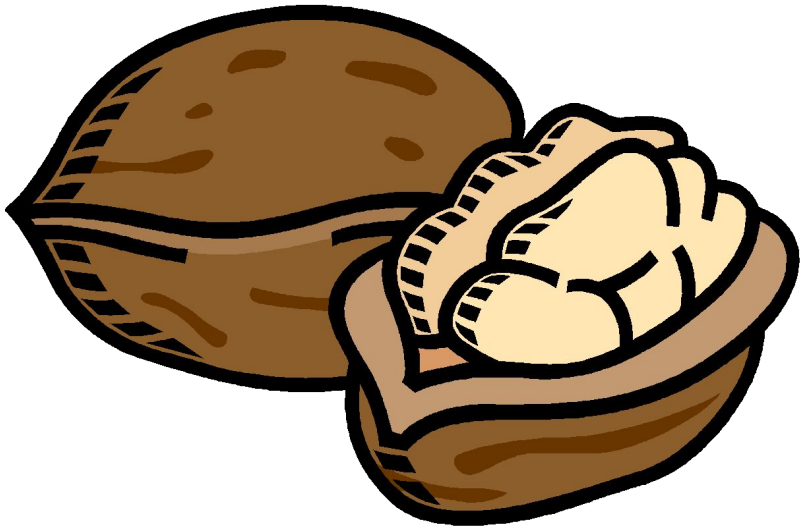
- Создание препятствий для физического доступа на объект посторонних лиц
- Помещение защищаемых вещественных ценностей в надежные хранилища
- Препятствия перемещению на объект автономных средств технической разведки
- Охрана «сетевого периметра»
- Физические и организационные меры противодействия внедрению вредоносных программ

Ослабление модулированной энергии

- в физическом пространстве – оборудование ослабляющих (поглощающих, отражающих) электромагнитных и акустических экранов в виде ограждающих конструкций зданий: стен, плит перекрытия, дверей, тамбуров, остекленных поверхностей, специальных звукопоглощающих слоев, электромагнитных экранов
- в каналах связи – использование поглощающих насадок, нагрузок, аттенюаторов, полосовых и заграждающих фильтров

Требования к пассивной защите

- Эшелонированность (многослойность)
- Надежность (непроницаемость)
- Непрерывность охраны по месту, времени и носителям информации



Изолирующий слой оценивается:

- Коэффициент «прозрачности» или ослабления воздействия, вероятность проникновения через него
- «Толщина» (стены, электромагнитного экрана, радиус контролируемой зоны)
- Стойкость к разрушающим воздействиям
- Зависимость от направления воздействия (крепостная стена, аварийный выход)
- Длительность сопротивления при непрерывном или периодическом воздействии

Стратегия бегства (маневра)

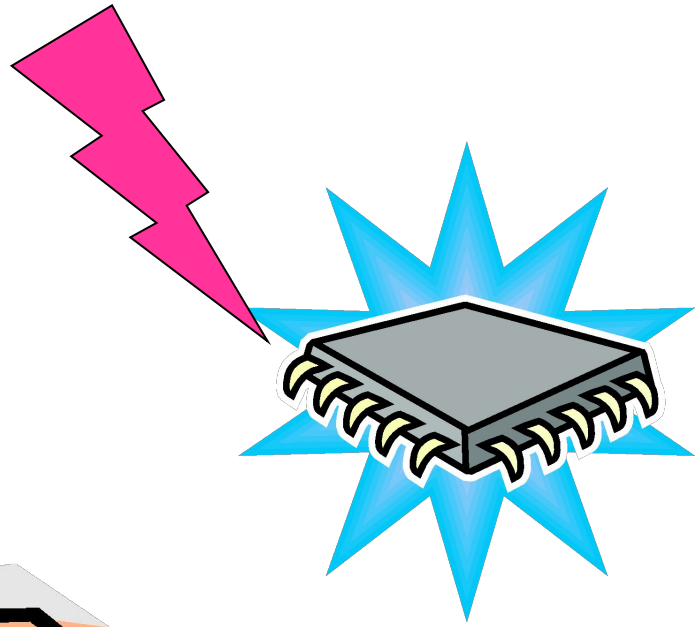
Формы реализации стратегии маневра

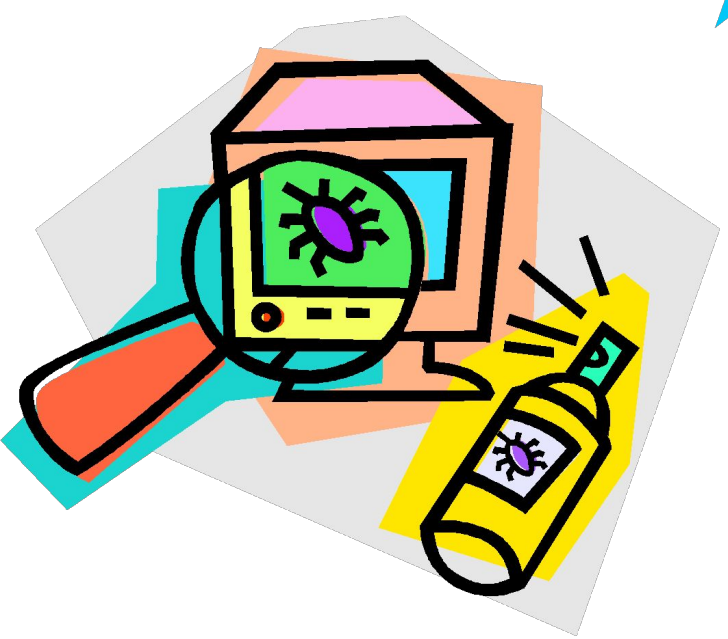
- Эвакуация людей, материальных ценностей, ТСОИ и вещественных носителей информации из зданий и помещений в нештатных ситуациях
- Отключение от источника опасной (недостоверной, избыточной, угрожающей и иной) информации
- Маневр в пространстве памяти как форма сокрытия вредоносных и защитных программ
- Маневр в пространстве радиодиапазона (скачкообразное изменение частоты)

Формы реализации стратегии маневра

- Эвакуация людей, материальных ценностей, ТСОИ и вещественных носителей информации из зданий и помещений в нештатных ситуациях
- Перемещение в пределах здания технических средств обработки информации, создающих ненормированную утечку
- Отключение от источника опасной (недостоверной, избыточной, угрожающей и иной) информации

Ликвидация опасности





Виды ликвидации опасности:

- **Угроза ликвидируется после ее выявления средствами контроля**
- **Угроза ликвидируется «наугад»; ее выявление или установление местонахождения ее источника невозможно, либо нецелесообразно**
- **Ликвидируется не угроза, а уязвимость в системе защиты**
- **Выявляются и ликвидируются последствия реализованной угрозы (атаки). После этого выявляется и ликвидируется причина опасности**
- **Убытки, нанесенные угрозой, возмещаются за счет страховой суммы. Бороться с самой угрозой не имеет смысла**
- **Применяются эффективные превентивные меры, делающие невозможным наступление угрозы**

Формы реализации стратегии ликвидации опасности

- **Угроза применения оружия или санкций против нарушителя или его имущества. «Часовой стреляет без предупреждения!»**
- **Воздействие на нарушителя в формах его физического блокирования, задержания, ареста, ссылки, лишения свободы, привлечения к ответственности, отстранения от должности и др.**
- **Уничтожение или изъятие орудий преступления**
- **Удаление файлов вредоносных программ «Лечение» инфицированных файлов путем удаления опасных фрагментов**

Формы реализации стратегии ликвидации опасности

- **Создание препятствия для нарушителя в виде агрессивной среды или опасного для жизни или здоровья излучения**
- **Излучение, стирающее информацию с ее носителей, либо делающее их непригодными для хранения информации**
- **Повреждение аппаратных закладок в помещении, схеме, проводном канале мощными электромагнитными импульсами**
- **Электромагнитное и акустическое подавление подслушивающих и звукозаписывающих устройств**
- **Ликвидация опасных сетевых пакетов маршрутизатором, межсетевым экраном**

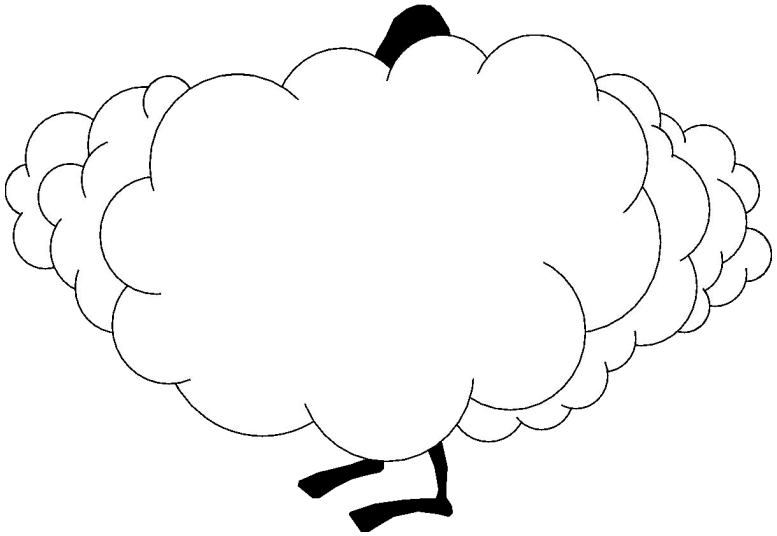
Виды информационного подавления

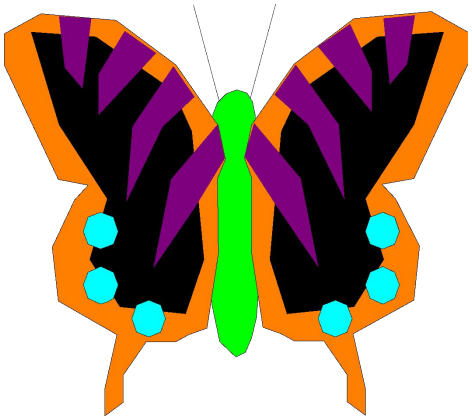
- Создание активных помех радио- и гидролокаторам
- Радиоподавление каналов связи противника в боевых условиях
- Подавление идеологически вредных радиостанций («холодная война»)
- Высылка инакомыслящих из страны
- Имитация тревожных воздействий на технические средства охраны

Ликвидация уязвимостей

- Защита от разглашения конфиденциальной информации мерами внутриобъектового режима
- Очистка компьютерной памяти от «технологического» мусора
- Ликвидация избыточных, потенциально опасных функций операционной системы

Стратегия скрытия, маскировки, дезинформации



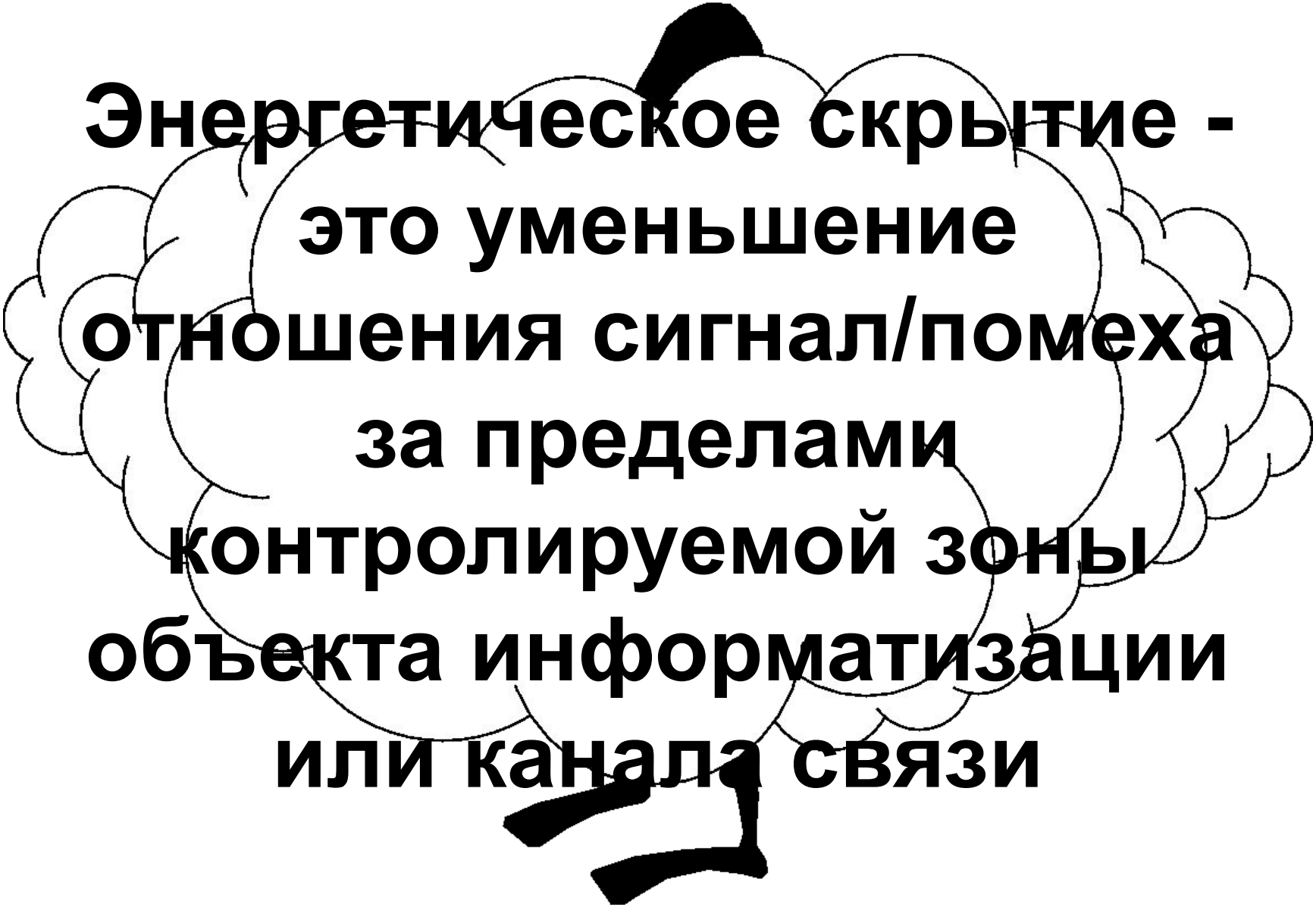


Виды маскировки

- **Маскировка** (masquer - делать незаметным, невидимым) - комплекс мероприятий по введению противника в заблуждение
- **Сокрытие** - устранение или ослабление демаскирующих признаков объектов
- **Демонстративные действия** - действия, имеющие цель ввести противника в заблуждение относительно настоящих намерений
- **Имитация** (imitatio - подражание) - создание эффекта присутствия или деятельности
- **Дезинформация** - преднамеренное распространение ложных сведений

Формы реализации стратегии маскировки

- Электромагнитное и акустическое зашумление «опасных» сигналов (в каналах связи)
- Использование многословия и пустословия для маскировки намерений в политике и дипломатии
- Вибрации ограждающих поверхностей здания
- Скрытие сигнатуры программного кода
- Стеганография («растворение» информации в шуме)
- Маскировка технических средств охраны
- Скрытое несение службы по охране объекта



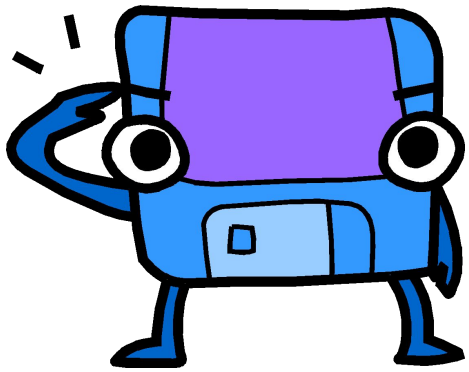
Энергетическое скрытие - это уменьшение отношения сигнал/помеха за пределами контролируемой зоны объекта информатизации или канала связи

За пределами контролируемой зоны или канала связи отношение мощности сигнала и помехи должно быть таким, чтобы выделение модулирующей составляющей сигнала на фоне помех было невозможным

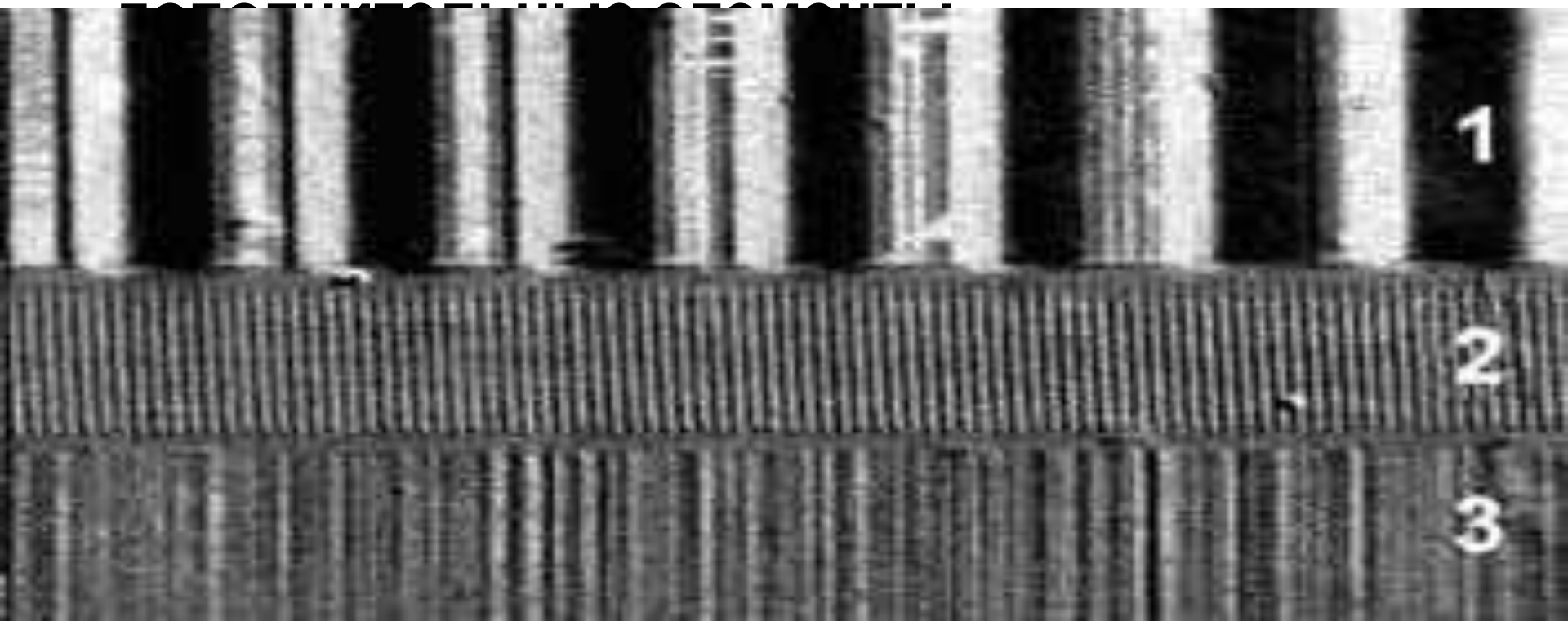
Методы и средства скрытия энергетических носителей информации

- Электромагнитное экранирование и звукоизоляция аппаратуры, каналов связи, рабочих мест, помещений, пространственных объемов (стратегия пассивной защиты)
- Использование оптоволоконных линий с полным внутренним отражением
- Дисциплина приватных бесед и разговоров по телефонным каналам
- Линейное и пространственное зашумление (электромагнитное и акустическое)
- Снижение энергетики «опасных» сигналов
- Обнаружение и ликвидация вторичных антенн

Скрытие информации на уровне взаимодействия с носителем



Используются: сложный физический формат размещения данных (типа защиты от копирования),



Скрытие информации на логическом уровне

- Использование сложных форматов файлов с большим числом заголовков, параметров, ключевой информации, служебных полей, полей данных (текстовых, табличных, графических, звуковых), элементов форматирования и др.
- Использование «непрозрачных» файловых систем
- Скрытие отдельных фрагментов файловой системы (логических дисков, каталогов, файлов) от просмотра с помощью стандартных файловых менеджеров

Скрытие данных на синтаксическом уровне

- Использование различных, в т.числе редких кодировок символов
- Использование различных методов сжатия информации, в т.числе с парольной защитой
- Применение методов криптопреобразования симметричного и асимметричного типа (перестановка, замена, аналитические преобразования, гаммирование)

Информационное скрытие на семантическом уровне

- Прямое скрытие фактов
- Тенденциозный подбор данных
- Нарушение логических (причинно-следственных, временных и др.)
- Смешивание разнородных мнений и фактов
- Использование слов и понятий с разным истолкованием
- Изложение существенных данных на ярком фоне отвлекающих внимание сведений
- Интерпретация услышанного в соответствии со своими знаниями

Скрытие информации на прагматическом уровне

- Превращение информации в неполную, частичную (хранение и обработка по частям, ограниченное информирование сотрудников)
- Использование элементов недостоверности, дезинформация
- Несвоевременная доставка сообщений

Средства пространственного и линейного (канального) зашумления

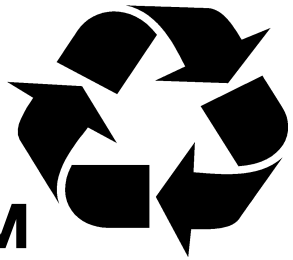
- Широкополосные генераторы электромагнитного излучения («белый» шум)
- Генераторы шума с ограниченным спектром (адаптивные, маскирующие и др.)
- Устройства шумового подавления устройств перехвата
- Использование шумоподобных и псевдослучайных сигналов для кодирования и модуляции

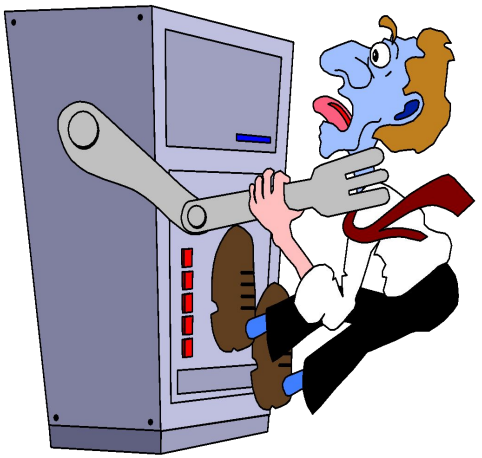
Стеганография - способы сокрытия факта передачи сообщения или его истинного смысла

- Использование невидимых чернил
- Микрофотоснимки
- Специальное условное расположение текстовых или графических символов, предметов
- Цифровые подписи
- Скрытая связь с использованием электромагнитных и акустических волн
- Формы компьютерной стеганографии

Алгоритмы скрытности вредоносных программ

- **Резидентность (постоянное нахождение в оперативной памяти)**
- **Stealth-алгоритмы**
- **Самошифрование и полиморфизм**
- **Нестандартные приемы**





Маскировка средств информационной защиты

- Камуфляж сигнализационных датчиков и телекамер охранного телевидения
- Скрытый мониторинг за средствами электронного подслушивания
- Использование процедур взаимной аутентификации без передачи данных
- Шифрование паролей, скрытие доступа к базам данных учетных записей в ОС
- Тактика скрытой охраны объекта

Дезинформация

- **Дезинформация - процесс создания и распространения ложной информации об объектах, лицах, процессах**
- **Дезинформация может быть массовой или адресной**
- **Хорошая дезинформация должна быть правдоподобной и проверяемой**
- **Легендирование - создание обоснованного, логически завершенного вымысла о якобы происходящих действиях, намерениях, фактах**

Имитация

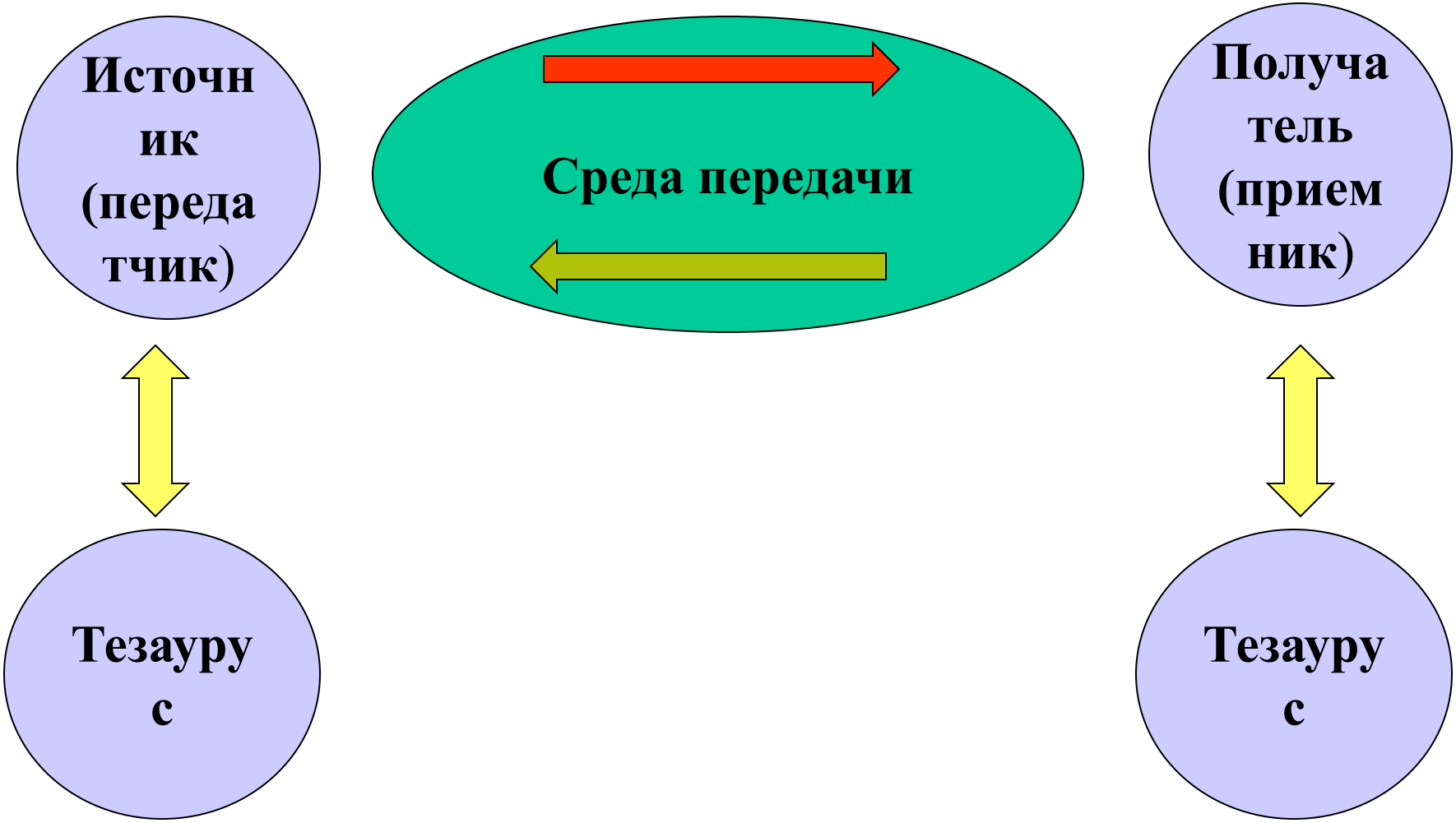
- **Создание эффекта присутствия или деятельности с целью отвлечения на ложный объект сил, средств или внимания противника**
- **Примеры: ложные узлы в компьютерных сетях (Honey Pot), ложные цели для радиолокаторов ПВО, преднамеренно оставленные в доступных для нарушителях местах документы с «важной» информацией, ложные хранилища ценностей и др.**

Модель канала связи

Ограничения и допущения модели

- Защите подлежит информация на этапе ее передачи-приема (транспортирования)
- В общем случае среда передачи считается открытой и общедоступной
- Модель рассматривается с позиций защищенности информации от помех, дезинформации, повреждения канала, ренегатства, целостности, перехвата информации и др.

Элементы канала связи



Основные понятия

Передатчик – устройство, формирующее сигнал и модулирующее его сообщением

Приемник – устройство, получающее смесь сигнал + помеха, выделяющее из смеси полезный сигнал и извлекающее из его иформативных параметров переданное сообщение

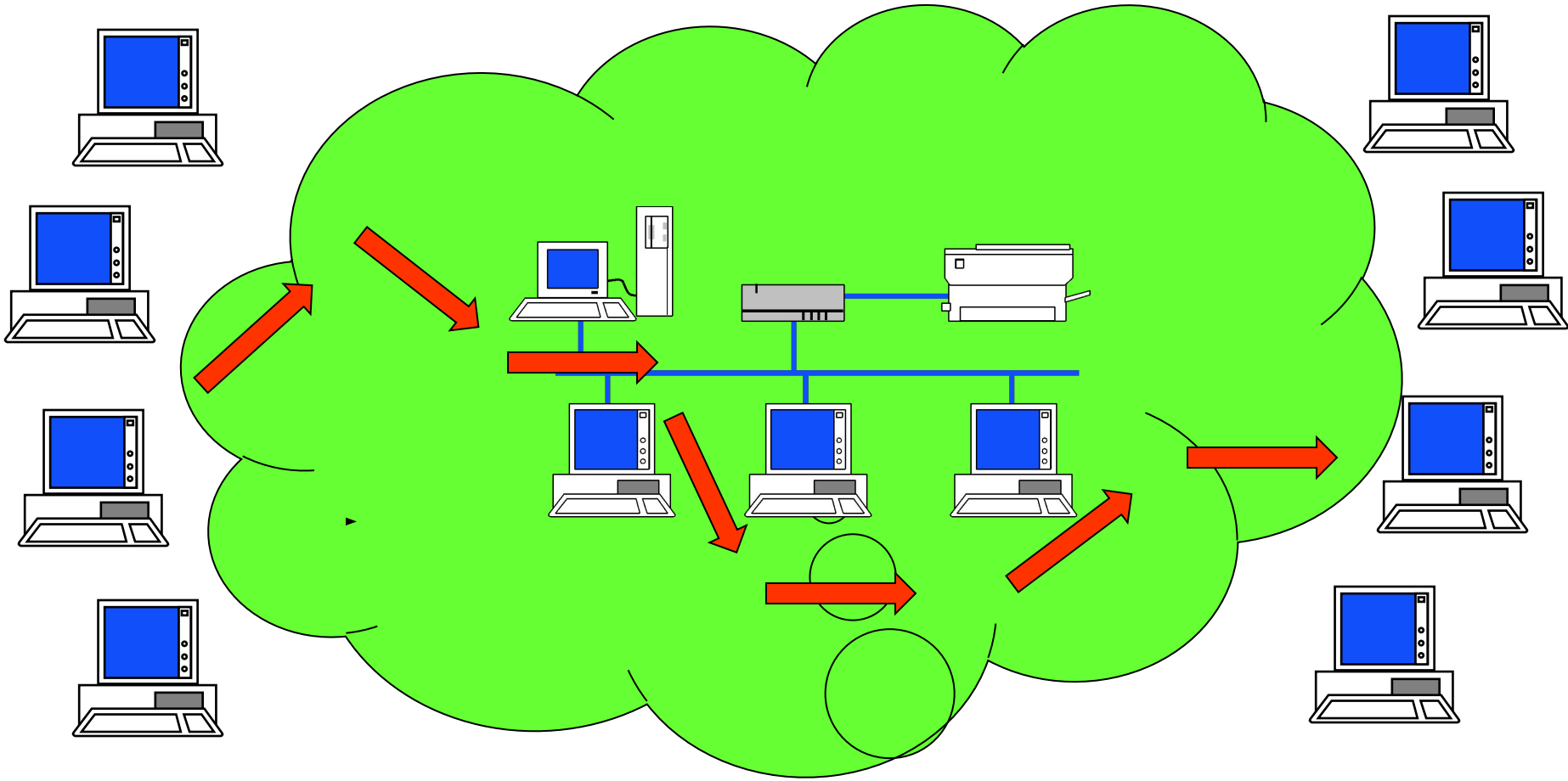
В качестве среды передачи может выступать любая материальная сущность, привносящая наименьшие затухания по уровню и задержки по времени

Основные понятия

- Сигнал в процессе передачи испытывает затухание по уровню и задержку по времени
- Передача детерминированных сообщений не имеет смысла. Детерминированный сигнал не может быть переносчиком информации
- Электрический сигнал обладает набором информативных и селективных параметров

Канал связи - совокупность физической среды распространения сигналов и средств для передачи и приема сообщений

Канал - это тракт движения сигнала с множеством входных и выходных устройств



Основные понятия

Сигнал – это физический процесс, способный изменятся во времени в соответствии с переносимым сообщением и распространяющийся по соответствующей среде передачи

Информация, содержащаяся в любом сигнале, представлена значениями его информационных параметров – т.е. по существу сигнал – это распространяющийся в пространстве носитель с информацией, которая содержится в значениях его физических параметров

Классификация сигналов

По физической природе сигналы делят на:

- акустические
- электрические
- магнитные
- электромагнитные
- корпускулярные
- материально-вещественные

Классификация сигналов

По форме сигналы делят на:

- аналоговые
- дискретные

По регулярности появления сигналы делят на:

- непрерывные
- периодические
- случайные

Основные понятия

- **Модуляция - процесс управляемого изменения параметров носителя по закону передаваемого сообщения**
- **Принцип суперпозиции: выходной сигнал является суммой входных сигналов и помех**
- **В реальных каналах всегда имеет место искажение сигналов**
- **В реальном канале всегда имеются помехи**

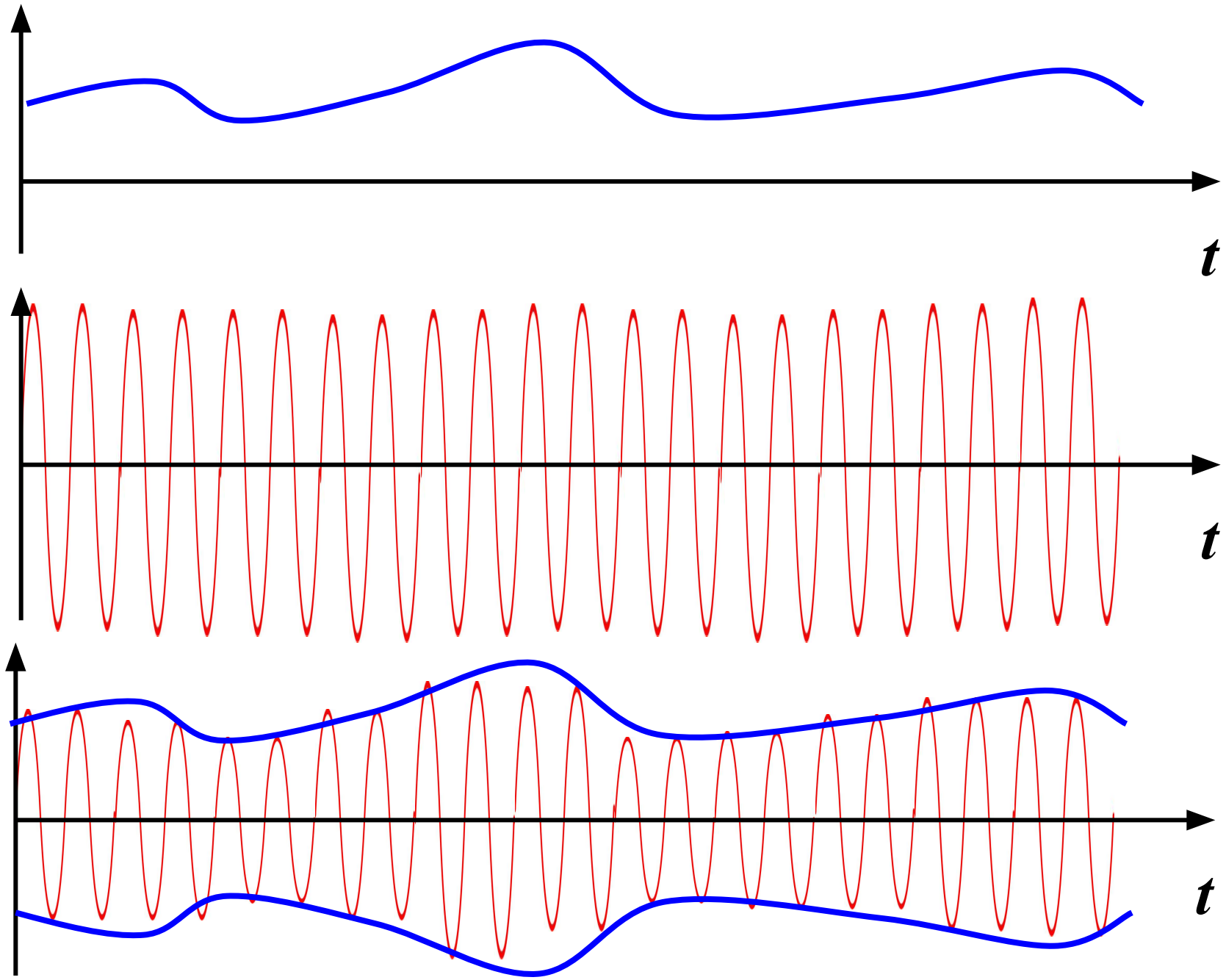
К аналоговым сигналам относят сигналы, уровень (амплитуда) которых может принимать произвольные значения в определенном для сигнала интервале.

Амплитуда простого и достаточно распространенного в природе гармонического сигнала изменяется по синусоидальному закону:

$$s(t) = A \times \sin(\omega \times t + \varphi)$$

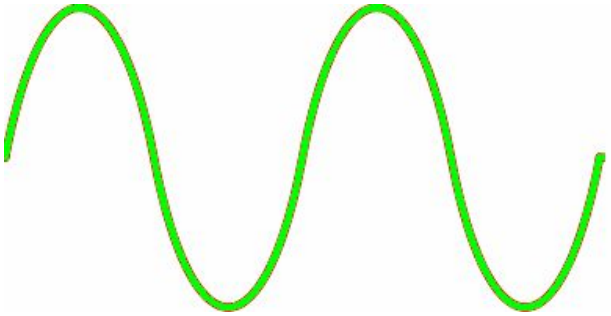
где A – амплитуда; ϕ – фаза колебания;

$\omega = 2 \times \pi \times f$ – круговая частота колебания.

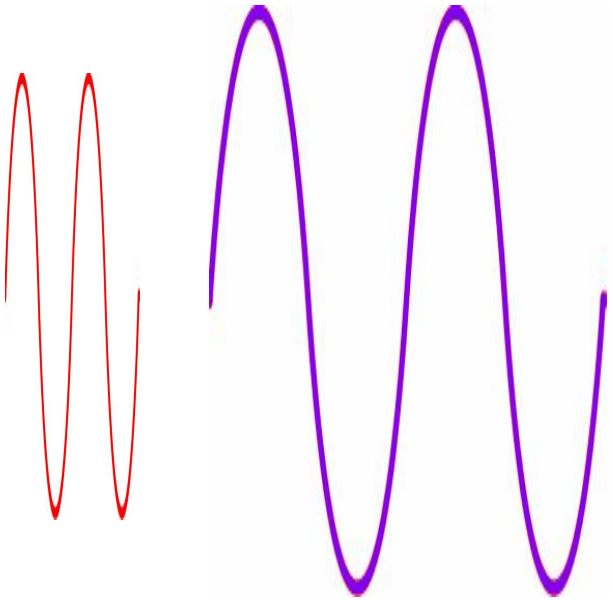

t
t
t

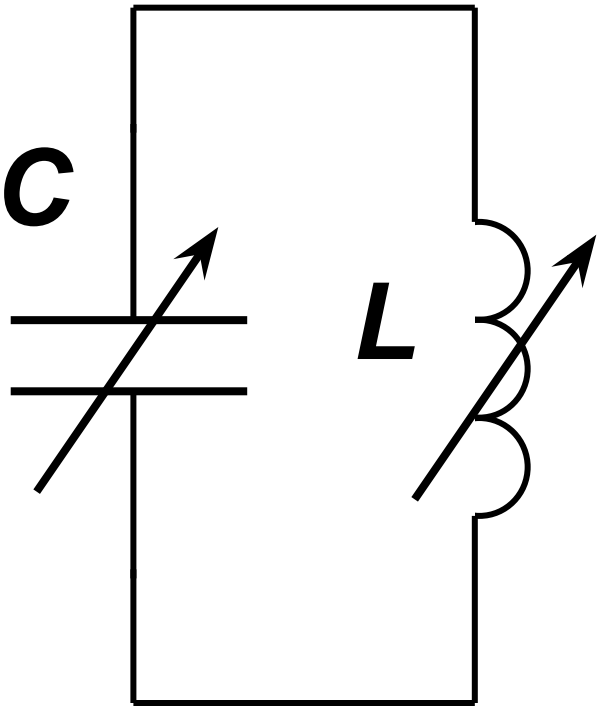
Основные понятия

- Между сигналом и помехой отсутствует принципиальное различие: то, что является сигналом для одного приемника, может являться помехой для других
- В каналах связи решаются две задачи: обнаружение сигнала на фоне помех и различение множества сигналов по их параметрам
- По принятому сигналу можно лишь с некоторой вероятностью определить, какое сообщение передавалось



$$\omega = \frac{1}{\sqrt{L \cdot C}} \qquad f = \frac{1}{2\pi\sqrt{L \cdot C}}$$





Виды каналов

- Моноканалы и каналы с уплотнением сигналов
- Канал «точка-точка» и виртуальный канал
- Составные каналы и сети
- Аналоговые и дискретные каналы
- Симплексные и дуплексные каналы
- Закрытые и открытые каналы

Измерение количества информации

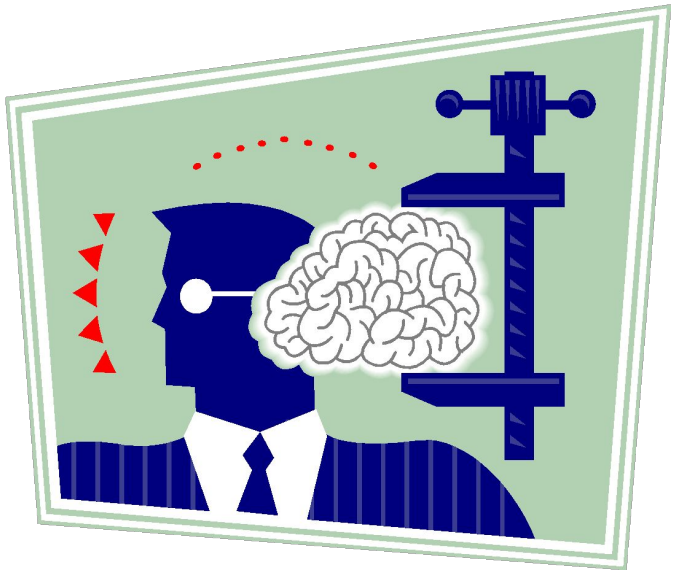
- Структурная мера (количество переданных бит, байт, символов)
- Статистическая мера (мера уменьшения исходной неопределенности у получателя)
- Семантическая мера (содержательность, смысл информации)
- Прагматическая мера (полезность, целесообразность, существенность информации)

Передача информации имеет смысл, если:

- Источник более информирован, чем получатель (его тезаурус больше)
- Передаваемая информация является ценной, достоверной и своевременной
- Получатель нуждается в данной информации и не обладает ею
- Получатель понимает полученную информацию и умеет ее использовать

Свойства тезауруса, как объекта защиты

- Тезаурус - запас знаний, словарь, используемый приемником информации
- Тезаурус - капитал и основная ценность информационной системы
- Для передачи знаний тезаурусы передатчика и приемника должны пересекаться (содержать общие элементы)
- Приобретение новых знаний означает пополнение тезауруса приемника



Пополнение тезауруса вовсе не означает увеличения его объема. За счет образования новых, более совершенных понятий и логических связей старые могут отмирать, а объем тезауруса - сокращаться (сравнить объем научных отчетов и диссертаций с учебными пособиями)

Научное озарение сопровождается эмоциями (обычно – положительными). За счет образования новых логических связей многие старые цепи становятся излишними, лишние нейроны погибают, а энергия, ранее расходовавшаяся на их питание, освобождается.

С.П.Расторгуев

Подключение к каналу своих источников (передатчиков)

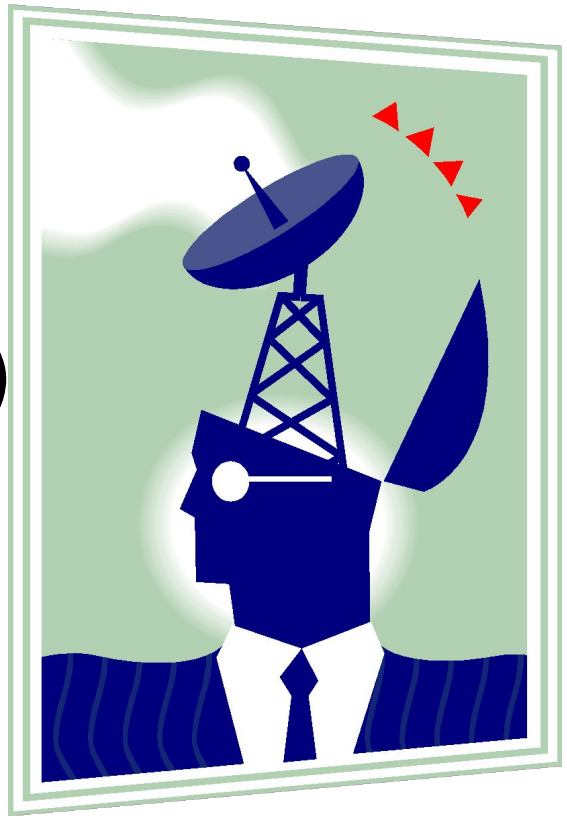
- С целью навязывания ложной информации
- С целью «затопления» (flood) канала неинформативными сигналами на пределе пропускной способности канала
- С задачей зашумления канала для того, чтобы воспрепятствовать нормальной передаче информации

Подключение к каналу своих получателей (приемников)

- Перехват (отвод) всей или выборочной информации
- Контроль трафика (факта, объема, скорости передаваемых сообщений, сведений об используемых протоколах, видах модуляции и др.)

Использование или создание побочных каналов (утечки)

- Подключение к одному из побочных каналов
- Создание внеполосных сигналов (ВЧ навязывание)
- Включение в канал своего ретранслятора (приемопередатчика)



Атаки на линию

- Отключение линии от передатчика
- Отключение линии от приемника
- Вызов повреждения на линии
- Хищение материалов и конструкций на линии связи

Использование канала в своих интересах

- Несанкционированное подключение к чужой линии своих абонентских устройств
- Работа с внеполосными сигналами
- Пользование каналом под чужим именем и за чужой счет
- Обход систем контроля соединений с целью неуплаты за пользование каналом

Способы обмана при передаче сообщения

- Отказ отправителя от посланного им сообщения (ренегатство или отступничество)
- Подмена принятого сообщения в пункте приема с выдачей его за подлинное

Способы обмана при передаче сообщения

- Имитация принятого сообщения в пункте приема при фактическом отсутствии
- Подмена передаваемого сообщения в пути следования
- Повтор нарушителем ранее перехваченного сообщения

- **«Радиоигра» - использование чужого источника (передатчика) в интересах дезинформирования противника**

Защита информации в канале связи включает:

- Защиту источников информации
- Защиту носителей информации
- Защиту линии связи
- Защиту систем обработки информации
- Защиту тезауруса

Направления защиты передаваемой информации

- Физическая защита канала и его элементов от НСД, утечки информации
- Защита от преднамеренных помех, внеполосных сигналов, дезинформации
- Обеспечение конфиденциальности передаваемой информации в открытых каналах
- Маскировка процессов передачи-приема информации

Направления защиты передаваемой информации

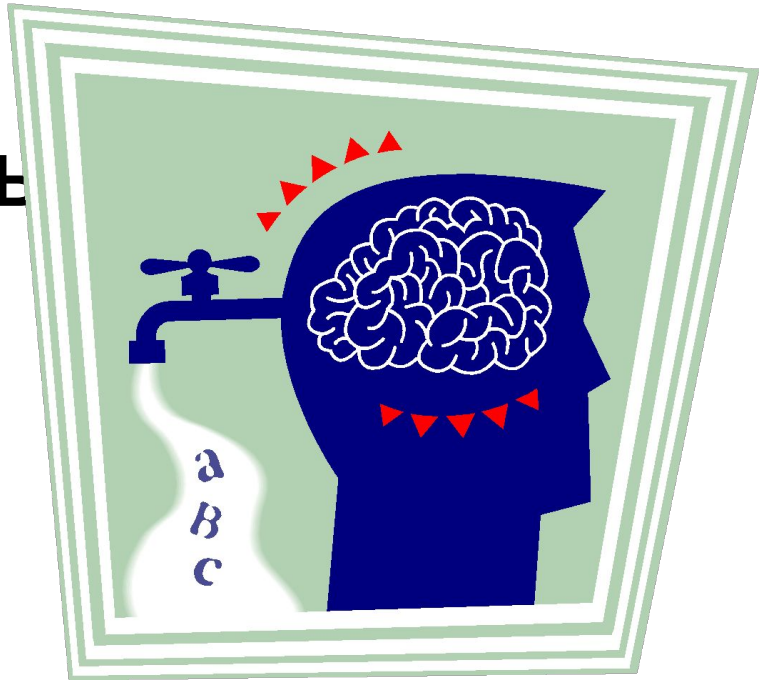
- Установление подлинности источника сообщения
- Установление авторства сообщения
- Проверка достоверности принятого сообщения (соответствия переданных и принятых сигналов)
- Обеспечение помехоустойчивости сигналов при воздействии случайных помех

Физическая защита канала связи

- **Охрана передающей и приемной аппаратуры от НСД**
- **Контроль физической целостности линии связи**
- **Охрана линии связи от хищений аппаратуры и материалов**
- **Контроль пропускной способности**
- **Контроль за параметрами линии и подключениями**

Защита линий связи от утечки информации

- Экранирование проводных линий
- Фильтрация сигналов во вторичных линиях, выходящих за предель объекта
- Использование каналов связи с «узкой» базой



Защита канала от помех и внеполосных сигналов

- Использование сигналов с «широкой» базой
- Применение помехоустойчивых видов модуляции

Фильтрация проходящих сигналов

- Помехоустойчивое кодирование

Обеспечение конфиденциальности передаваемых сообщений

- Использование выделенных линий и физически защищенных каналов
- Криптозащита
- Использование нестандартных сигналов, видов кодирования и модуляции
- Применение шумоподобных сигналов

Маскировка процессов приема-передачи обеспечивается посредством скрытия

- Источника сообщения
- Получателя сообщения
- Тезауруса (языка, кодировки, ключей)
- Факта передачи сообщения (стеганография)
- Маршрута сообщения

Установление подлинности переданных сообщений

- Квитирование сообщений
- Процедуры «рукопожатия»
- Электронная цифровая подпись ее разновидности

Установление подлинности авторства сообщения, достоверности принятого сообщения

- **Электронная цифровая подпись ее разновидности**
- **Использование ассиметричных криптосистем**
- **Эмитовставка**

Обеспечение помехоустойчивости сигналов при воздействии случайных помех

- **Использование помехоустойчивого кодирования**
- **Применение шумоподобных сигналов**