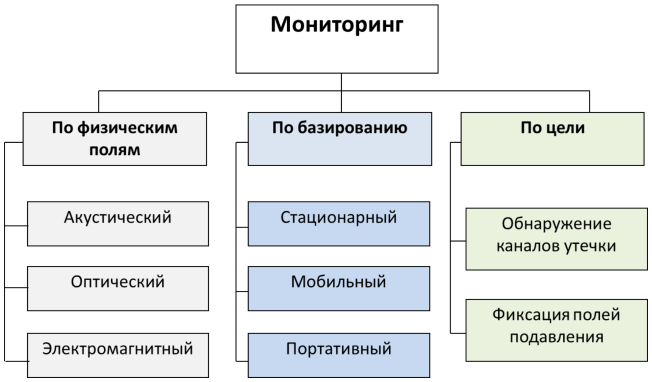
Лекция №4

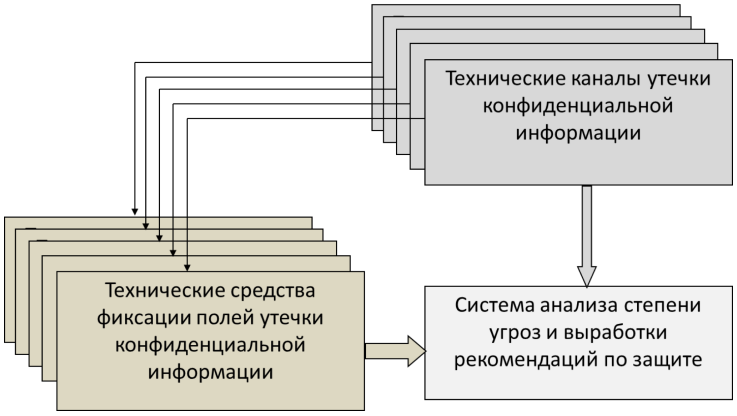
Модель мониторинга утечек информации

Под мониторингом понимают определённую систему наблюдения, оценки и прогноза состояния и развития различных процессов и явлений.



Мониторинг – это постоянный сбор информации, наблюдения и контроль за объектом включающий процедуры анализа риска измерения параметров сигнала способных нести конфиденциальную информацию.

Структура модели комплексной системы мониторинга



Территориальные зоны возможных несанкционированных действий

Для несанкционированного получения информации необходимо одновременное наступление таких событий:

- Нарушитель может получить доступ в ответственную зону;
- Во время пребывания нарушителя в зоне в ней может появляться (существовать) определенный канал несанкционированного получения информации;

- Канал несанкционированного получения информации, которой появился, может быть доступным нарушителям определенной категории;
- В канале не санкционированного получения информации в момент доступа к нему нарушителя может находиться защищаемая информация.

Количественная оценка уязвимости

Методологические подходы к оценки уязвимости информации:

- Эмпирический;
- Теоретический;
- Теоретико-эмпирический.

Исходная посылка при разработке моделей:

- С одной стороны, при нарушении защищенности информации наносится некоторый ущерб
- С другой, обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемость стоимость защиты может быть выражена сумой расходов на защиту и потерь от её нарушения.

Эмпирический подход

На основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирически путём устанавливаются зависимости между потенциально возможных ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при её проявлении размера ущерба.

Для того чтобы воспользоваться данным подходом необходимо знать(или уметь определять):

- Ожидаемы потери при нарушении защищенности информации
- А во-вторых, зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.
- Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации необходимо знать:
  1. Полный перечень угроз информации
  2. Потенциальную опасность для информации каждой из угроз и, в-третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.
- Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равным уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь.

Эмпирический подход (методика IBM)

Эмпирическая зависимость ожидаемых потерь от i-й угрозы информации:

$$R_i = 10^{S_i+V_i-4},$$

(4 – магический коэффициент из опыта)

Где R_i – материальный ущерб по данному каналу;

S_i – коэффициент, характеризующий возможную частоту возникновения i-ой угрозы

V_i- коэффициент, характеризующий значение возможного ущерба при возникновении i-ой угрозы.

возникновении i-ой угрозы.

Общие потери по всем возможным каналам утечки информации:

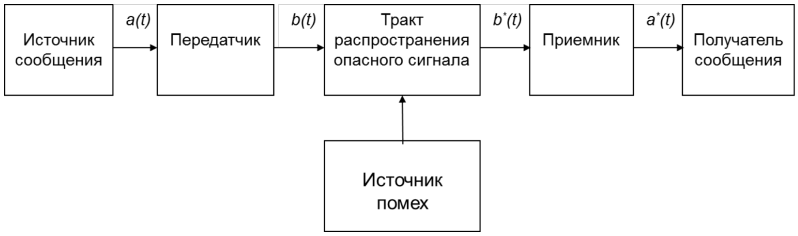
$$R = SUM[i=0..n](R_i)$$

где R – общие потери.

№	Ожидаемая частота появления угрозы	Коэффициент (Si)
1	почти никогда	0
2	1 раз в 1000 лет	1
3	1 раз в 100 лет	2
4	1 раз в 10 лет	3
5	1 раз в год	4
6	1 раз в месяц	5
7	2 раза в неделю	6
8	3 раза в день	7

№	Значение возможного ущерба при появлении угрозы	Коэффициент (Vi)
1	1	0
2	10	1
3	100	2
4	1000	3
5	10000	4
6	100000	5
7	1000000	6
8	10000000	7

Систем передачи информации

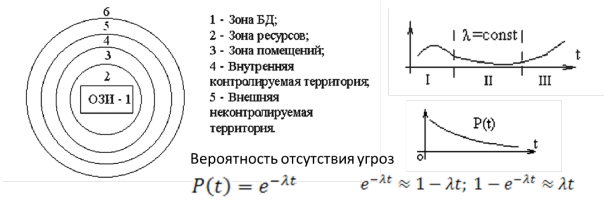


Основные принципы построение защиты:

- Необходимо строить вокруг объекта защиты постоянно действующий замкнутый контур (оболочку) защиты;
- Свойство преграды, составляющие защиту, должны по возможности соответствовать ожидаемой квалификации и осведомленности нарушителя;
- Для входа в систему законного пользователя необходима переменная секретная информация, известная только ему;
- Итоговая прочность защитного контура определяется его слабейшим звеном;
- При наличии нескольких законных пользователей следует обеспечить разграничение их доступа к информации в соответствии с полномочиями и выполняемыми функциями, реализуя, таким образом, принцип наименьшей осведомленности каждого пользователя с целью сокращения возможного ущерба.

Вероятностная модель оценки защищенности по территориальным зонам

Поток случайных событий – это поток угроз и он имеет интенсивность лямбда*т. На достаточно маленьких промежутках она стремится к константе



Вероятность отсутствия угроз $P(t) = e^{-\lambda t}$ $e^{-\lambda t} \approx 1 - \lambda t;\ 1 - e^{-\lambda t} \approx \lambda t$

Вероятность наличия угрозы: $Q(t) = 1 - e^{-\lambda t}$

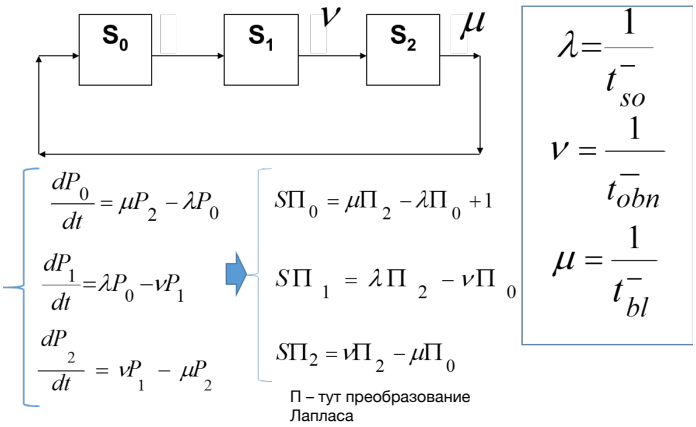
Защищенность *i*-ой зоны защиты:

$\lambda_1, \lambda_2, \lambda_3 \ldots$ – интенсивности угроз (опасностей) для i-го рубежа (зоны ЗИ)

$$P_{уязвим}(t) = P_{наруш} \cdot \left(1 - e^{-\lambda_1 \cdot t}\right) \cdot \ldots \cdot \left(1 - e^{-\lambda_5 \cdot t}\right)$$

- Состояние S_0 – в помещении (на объекте) отсутствуют реальные каналы утечки (КУ), но имеется некоторое множество потенциально возможных КУ;
- Состояние S_1 – на объекте(в помещении возник или специально организован КУ информации и осуществляется перехват циркулирующей на объекте информации;
- Состояние S_2 – каналу утечки информации каким-либо образом обнаружен, но он ещё не устранён и продолжает функционировать.
- Переход объекта(помещения) в состояние возможен только после устранения службой безопасности канала утечки информации.

Применение теоретико-эмпирического подхода – СМО



П – тут преобразование Лапласа

λ – Интенсивность создания
v – Интенсивность выявления
μ – Интенсивность блокировки
t_{so} – среднее время создания канала утечки
t_{obn} – среднее время обнаружения
t_{bl} – среднее блокировки

Уравнения Колмогорова составляют систему Обыкновенных Дифференциальных Уравнений, которую решают операторным методом с помощью преобразования Лапласа

$t \to \infty$

$$\Pi_1 = \frac{\lambda}{S+\nu}\cdot\Pi_0$$

$$\Pi_2 = \frac{\nu}{S+\mu}\cdot\Pi_0 = \frac{\nu\lambda}{(S+\nu)(S+\mu)}\cdot\Pi_0$$

$$\Pi_0 = \frac{(S+\nu)(S+\mu)}{S\left[S^2+S(\mu+\nu+\lambda)+\nu\lambda+\nu\mu+\lambda\mu\right]}$$

Вероятность того, что канал утечки в помещении отсутствует:

$$P_0 = \frac{\mu\nu}{\lambda\mu+\lambda\nu+\nu\mu}$$

Вероятность того, что в помещении имеется канал утечки информации, но СБ не обнаружен:

$$P_1 = \frac{\lambda\mu}{\lambda\mu+\lambda\nu+\nu\mu}$$

Вероятность обнаружения ТКУИ:

$$P_2 = 1 - P_0 - P_1 = \frac{\lambda\nu}{\lambda\mu+\lambda\nu+\nu\mu}$$

Степень защиты (безопасности) объекта от каналов утечки информации:

$$B = 1 - \prod^{n}(1 - P_{on})$$

П – тут умножение

Оценка уязвимости информации по базовым показателям

Вероятность несанкционированного получения информации нарушителем k-ой категории по j-му каналу несанкционированного получения информацц в l-ой зоне i-го структурного компонента информационной системы.

$$\left[P_{ijkl} \right] = P^{Д}_{ikl} P^{Н}_{ijl} P^{П}_{ijkl} P^{З}_{ijl}$$

Базовый показатель уязвимости информации:

$$P^{Б}_{ikl} = 1 - \prod_{l=1}^{5} \left[1 - P_{ijkl} \right] = 1 - \prod_{l=1}^{5} \left[1 - P^{Д}_{ikl} P^{Н}_{ijl} P^{П}_{ijkl} P^{З}_{ijl} \right]$$

$P^{Д}_{ikl}$ – это вероятность доступа нарушителя k-ой категории в зону l i-го компонента информационной системы.

$P^{Н}_{ijl}$- это вероятность наличия(проявления) j-го канала несанкционированного получения информации в l-ой зоне i-го компонента ИС.

$P^{П}_{ijkl}$ – П- вероятность поступления(прорыва) нарушителя k-ой категории j-го канала зоны l i-го компонента ИС.

$P^{З}_{ijl}$-З – вероятность наличия защищаемой информации в j-ом канале несанкционированном получении информации в зон l i-го компонента ИС.

Вероятность несанкционированного получения информации в одном компоненте ИС одним злоумышленником одной категории и по одному каналу называется базовым показателем уязвимости информации.

Поисковые технические устройства:

Детекторы поля – простейшие поисковые устройства. которые необходим для поиска радиоизлучающих подслушивающих устройств.

Нелинейные локаторы – предназначены для выявления и локализации негласно установленные электронных средств съема информации. Предназначен для поиска электронных устройств. содержащих полупроводниковые компоненты. Применяется для обследования легких строительных конструкций, мебели и предметов интерьера.

Поисковые комплексы – предназначены для проведения различных работ по выявлению технических каналов утечки информации. Многофункциональное поисковое устройство ST 131 «Пиранья II» предназначено для проведения мероприятий по обнаружению и определению местоположения специальных технических средств негласного получения информации и выявления естественных и искусственно созданных каналов утечки информации.

Блокираторы беспроводной связи предназначены для блокирования работы устройств несанкционированного получения информации, работающих в стандартах сетей сотовой связи и в стандартах Bluetooth и WiFi.

Принцип работы заключается в генерации помех в заданном частотном диапазоне.

Системы постановки виброакустический и акустических помех предназначена для противодействия специальным средствам несанкционированного съема информации. использующим в качестве канала утечки перегородки и пр.