Теория информационной безопасности и методология защиты информации

(лекции)

Введение. Общая характеристика курса

Теория информационной безопасности и методология защиты информации:

– Лекции — 36 часов;

– Практика — 10 часов;

– Лабораторные работы — 8 часов;

– СРС (реферат) — 86 часов;

– экзамен.

Основные разделы курса:

1. Научная терминология. Базовые понятия;
2. Математические основы теории информации;
3. Информационная безопасность. Требования к информации как
4. объекту защиты;
5. Методы и средства защиты информации;
6. Модели и методы оценки защищенности (уязвимости)
7. информации;
8. Анализ риска. Управление риском;
9. Неформальные методы принятия решений в системах ЗИ;
10. Общие принципы проектирования систем ЗИ.

Последующие курсы:

– Правовое обеспечение информационной безопасности;

– Организационное обеспечение информационной безопасности;

– Защита и обработка конфиденциальных документов;

– Инженерно–техническая защита информации;

– Технические средства защиты информации;

– Программно–аппаратная защита информации;

– Защита информационных процессов компьютерных системах;

– Комплексная система защиты информации на предприятии;

– Организация и управление службой защиты информации на предприятии.

Список литературы:

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. — В 2–х кн. — М.: Энергоатомиздат, 1994 (Кн.1 — 400 с., кн. 2 — 176 с.).
2. Организация и современные методы защиты информации. /Под общей ред. Диева С.А., Шаваева А.Г. — М.: Концерн <Банковский Деловой Центр>, 1998. — 472 с
3. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. — М.: Радио и связь, 2000. — 192 с.: ил.
4. Мельников В.В. Защита информации в компьютерных системах. — М.: Финансы и статистика, <Электронинформ>, 1997. — 368с.
5. Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 1999. — 328с.
6. Зегжда А.Н., Ивашко А.М. Как построить защищенную информационную систему; в 2–х томах. — СПб: Мир и семья–95, 1997.
7. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. Серия "Информатизация России на пороге XXI" века. — М.: СИНТЕГ, 1999, 232 с.
8. Большаков А.А., Петряев А.Б., Платонов В.В., Ухминов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях: Учеб.пособие: Часть 1 — Методы, средства и механизмы защиты данных. — Санкт–Петербург, 1996. — 165 с.
9. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Изд–во Агентства "Яхтсмен", — 1996. — 192 с.
10. Теория и практика обеспечения информационной безопасности. / Под ред. П.Д.Зегжды. — М.: Изд–во Агентства "Яхтсмен", — 1996. — 304 с.
11. Информационно–безопасные системы. Анализ проблемы: Учеб.пособие /Алешин Н.В., Козлов В.Н., Нечаев Д.А. и др.; Под ред. В.Н.Козлова — СПб: Изд–во С.–Петербургского гос.тех. унив–та, 1996. — 69 с.

12. Стенг. Д., Мун С. Секреты безопасности сетей. — К.: "Диалектика", 1995.

Периодическая литература:

– Защита информации. Confident

– Безопасность информационных технологий

– Безопасность и достоверность информации

– Проблемы информационной безопасности

– Вопросы защиты информации

– Системы безопасности, связи и телекоммуникаций

– Банковские технологии

и др.

1 Математические основы теории информации.

Теория вероятностей — это наука, изучающая закономерности случайных явлений.

Случайное событие — такое событие, может произойти или не произойти при осуществлении определенного комплекса условий. Примеры: вирусная атака; отказ оборудования, ошибка пользователя.

Случайные события называются несовместимыми, если они не могут появиться одновременно. Случайные события образуют полную группу попарно несовместимых событий, если при каждом испытании (исходе) должно появиться только одно из них.

Достоверное событие — такое, вероятность которого равна 1, т.е. при данном комплексе условий это событие непременно должно произойти: $P\{A\}=1$.

Если полная группа состоит из 2–х несовместимых событий, т.е. наступление одного из них равносильно ненаступлению другого, то такие случайные события называются взаимно противоположными. При этом:

$$P\{A\}+P\{\overline{A}\}=1, \qquad (2.1)$$

т.е. $$\{\overline{A}\}=1-P\{A\} \qquad (2.2)$$

Невозможное событие — такое, которое не может произойти ни при каком повторении испытания: $P\{A\}=0$.

Случайные события A и B называются независимыми, если наступление одного из них не может влиять на наступление другого.

а) Сумма событий: б) Произведение событий:

Рисунок — а) сумма событий; б) произведение событий.

Вероятность $P\{A\}$ (статистическое определение) — это относительная частота появления события при достаточно большом числе одинаковых ситуаций (испытаний): $$P\{A\}=\lim_{N\to\infty}\frac{N_1}{N} \qquad (2.3)$$

Основные свойства вероятностей:

- $0 \le P\{A\} \le 1;$ (2.4)
- $P\{A+B\} = P\{A\} + P\{B\} - P\{A \cdot B\};$ (2.5)
- Для несовместных событий: $P\{A+B\} = P\{A\} + P\{B\};$ (2.6)
- Условная вероятность: $P\{A/B\} = \dfrac{P\{A \cdot B\}}{P\{B\}};$ (2.7)
- Для независимых случайных событий: $P\{A \cdot B\} = P\{A\} \cdot P\{B\};$ (2.8)

Случайные величины.

Случайная величина ξ — это числовая функция, заданная на множестве элементарных событий.

Дискретная случайная величина. Величина ξ называется дискретной случайной величиной, если все ее возможные значения образуют конечную или бесконечную последовательность чисел $x_1, x_2, ..., x_k, ...$ и если принятие ею каждого из указанных значений есть случайное событие с определенной вероятностью.

Возможное значение ξ	1	2		k	
Вероятность (p)	1	2		k	

Закон распределения вероятностей величины ξ.

Закон распределения:

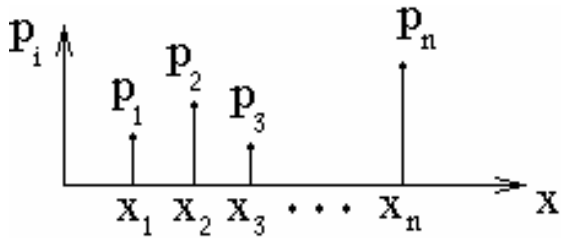


Рисунок — Закон распределения.

Для полной группы событий $\sum_{i=1}^{n} p_i = 1.$ (2.9)

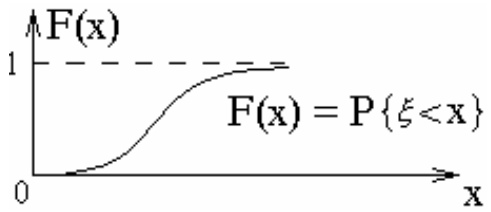
Математическое ожидание: $M[\xi] = \sum_{i=1}^{n} x_i \cdot p_i.$ (2.10)

Дисперсия: $D[\xi] = \sum_{i=1}^{n} (x_i - M[\xi])^2 \cdot p_i$ (2.11) характеризует меру отклонения случайной величины от ее математического ожидания.

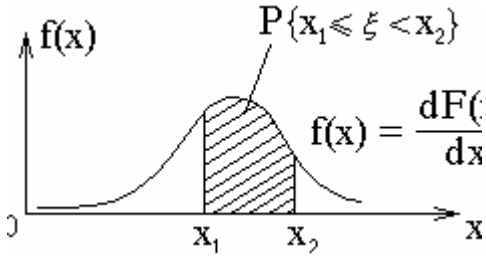
Среднеквадратическое отклонение: $\sigma = \sqrt{D[\xi]}$. (2.12)

Непрерывная случайная величина:

а) Интегрирующая функция распределения:



б) Дифференцирующая функция распределения (плотность распределения вероятности):



Математическое ожидание: $M[\xi] = \int_{\alpha}^{\beta} x \cdot f(x)dx$ (2.13)

Дисперсия: $D[\xi] = \int_{\alpha}^{\beta} (x - M[\xi])^2 \cdot f(x)dx$ (2.14)

Среднеквадратическое отклонение: $\sigma = \sqrt{D[\xi]}$ (2.15)

Статистические оценки:

- Для математического ожидания дискретной случайной величины:

$$\overline{X} = \frac{X_1 + X_2 + ... + X_n}{n}; \qquad (2.16)$$

- Для дисперсии:

$$\overline{D[\xi\xi} = \overline{\delta(\xi)} = \frac{\sum_{k=1}^{n} (X_k - \overline{X})^2}{n-1}. \qquad (2.17)$$

Законы распределения случайных величин:

Распределение Пуассона: $P\{\xi = k\} = \frac{\lambda^k}{k!} \cdot e^{-\lambda}$ (2.18)

Экспоненциальный закон: $f(x) = \lambda \cdot e^{-\lambda x}$ (2.19)

Нормальный закон: $f(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{\frac{-(x-M)}{2\sigma^2}}$ (2.20)

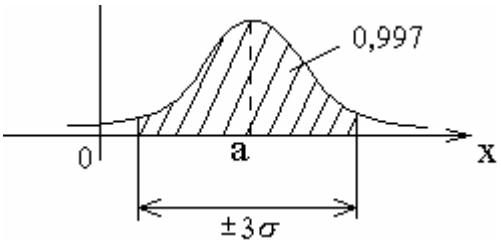


Рисунок — Правило “трех сигм”.

Правило "трех сигм" (для нормального закона распределения):

$P\{-3\sigma + M \le \xi \le 3\sigma + M\} = 0,997;$ (2.21)

В диапазоне $x \in [M \pm 2\sigma\sigma:]$ $P = 0,954;$

Центральная предельная теорема (А.М.Ляпунов, 1900г.):

Сумма достаточно большого количества независимых случайных величин, каждая из которых пренебрежимо мала по сравнению с суммой, стремится в пределе к нормально распределенной случайной величине.

Закон больших чисел:

С ростом числа событий N относительная частота события μ_N приближается к вероятности p этого события. Более строго, справедливо следующее утверждение:

для любого $\varepsilon > 0$ вероятность отклонения частоты от p на величину, меньшую ε, при $N \to \infty$ приближается к 1, т.е. $\lim_{N\to\infty} P(|\mu_N - p| < \varepsilon) = 1.$ (2.22)

Пример 1.

Два стрелка независимо друг от друга стреляют по одной и той же цели; вероятность попадания для первого стрелка равна P{A} = 0,9, для второго: P{B} = 0,8.

Требуется определить вероятность поражения цели, т.е. вероятность того, что хотя бы один стрелок попадет в цель.

Решение: $P\{A,B\} = 0{,}9 + 0{,}8 - 0{,}9 * 0{,}8$.

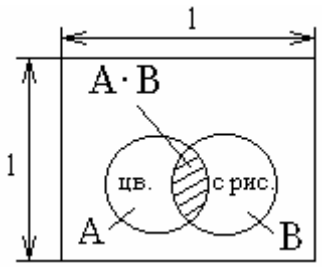
Пример 2. Условная вероятность

Пусть в коробке находится N шаров, одинаковых на ощупь, но различающихся по цвету и по рисунку:

K — количество цветных шаров (N–K белых);

L — количество шаров с рисунком (N–L без рисунка);

M — количество цветных шаров с рисунком.



Допустим, что событие A — заключается в появлении цветного шара; событие B — в появлении шара с рисунком. Тогда A*B — появление цветного шара с рисунком.

Используя данные обозначения, можно записать:

$P\{B/A\} = \frac{M}{K} = \frac{\frac{M}{N}}{\frac{K}{N}} = \frac{P\{A \cdot B\}}{P\{A\}}$ — условная вероятность события B при условии осуществления события A.

Аналогично: $P\{A/B\} = \frac{P\{A \cdot B\}}{P\{B\}}$

Для независимых случайных событий: $P\{A/B\} = P\{A\}; P\{B/A\} = P\{B\};$

Пример 3.

Из колоды (36 карт) достают 2 карты. Какова вероятность того, что обе карты — это тузы?

Решение: Пусть A — появление 1–го туза; B — появление 2–го туза. Тогда вероятность вынуть 2 туза подряд:

$P\{A \cdot B\} = P\{A\} \cdot P(B/A) = \frac{4}{36} + \frac{3}{35} = \frac{1}{105}$, где $P\{A\}$ — вероятность достать 1–й туз, $P\{B/A\}$ — вероятность достать 2–й туз (при условии, что 1–я карта также была тузом).

2 Научная терминология (базовые понятия)

Методология — это часть науки, представляющая собой учение о ее методах и теории, об их создании и практическом применении.

Наиболее важные точки приложения методологии:

– выявление предмета исследования,

– постановка научной задачи или проблемы,

– построение метода или теории решения рассматриваемой

– научной задачи (проблемы),

– проверка достоверности полученных выводов и рекомендаций.

Метод — совокупность приемов или операций практического или теоретического изучения действительности, подчиненных решению конкретной задачи.

Теория — высшая, самая развитая форма организации научного знания, дающая целостное представление о закономерностях и существующих связях, определяющих области действия объекта данной теории.

Необходимыми признаками теории являются:

– систематизация и обобщение знаний о закономерностях и особенностях развития явлений рассматриваемой предметной области;

– неочевидность;

– прагматичность;

Структура теории:

– исходная эмпирическая основа;

– исходная теоретическая основа (гипотезы, концепции, допущения, законы,…);

– логика теории;

– выводы, реконструкции.

Методика исследования — определенная совокупность элементов (методов, приемов, операций, средств), примененных в определенной логической последовательности в ходе проведения исследования или его части, имеющей

относительно самостоятельное значение, для решения конкретной научной задачи или научной проблемы.

Задача — то, что надо решить; при этом, по крайней мере, один метод решения известен.

Проблема — то, что надо решить; при этом метод решения неизвестен.

Постановка проблемы — четкая формулировка данной проблемы, конкретизирующая предмет исследования и требуемый научный результат.

3 Ценность информации.

Чтобы защитить информацию, надо затратить силы и средства, а для этого надо знать какие потери мы могли бы понести. Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери. Для решения этих задач в информацию вводятся вспомогательные структуры — ценность информации. Рассмотрим примеры.

Аддитивная модель. Пусть информация представлена в виде конечного множества элементов и необходимо оценить суммарную стоимость в денежных единицах из оценок компонент. Оценка строится на основе экспертных оценок компонент, и, если денежные оценки объективны, то сумма дает искомую величину. Однако, количественная оценка компонент не всегда объективна даже при квалифицированной экспертизе. Это связано с неоднородностью компонент в целом. Поэтому делают единую иерархическую относительную шкалу (линейный порядок, который позволяет сравнивать отдельные компоненты по ценности относительно друг друга). Единая шкала означает равенство цены всех компонент, имеющих одну и туже порядковую оценку.

Пример 1 $0_1,...,0_n$ — объекты, шкала 1<...<5. Эксперты оценили (2, 1, 3,...., 4) — вектор относительных ценностей объектов. Если есть цена хотя бы одного объекта, например, C_1=100 руб., то вычисляется оценка одного балла C_1/λ.= 50 руб., где λ — число баллов оценки первого объекта, и вычисляется цена каждого следующего объекта: C_2=50руб., C_3=150 руб. и т.д. Сумма дает стоимость всей информации. Если априорно известна цена информации, то относительные оценки в порядковой шкале позволяют вычислить цены компонент.

Анализ риска. Пусть в рамках аддитивной модели проведен учет стоимости информации в системе. Оценка возможных потерь строится на основе полученных стоимостей компонент, исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

Пример 2. Пусть $O_1,...,O_n$ — объекты, ценности которых $C_1,...,C_n$. Предположим, что ущерб одному объекту не снижает цены других, и пусть

вероятность нанесения ущерба объекту O_i равна p_i, функция потерь ущерба для объекта O_i равна

$$Wi=\begin{cases} Ci, \text{ если объекту i нанесен ущерб,} \\ 0, \text{ в противном случае.} \end{cases}$$

Оценка потерь от реализации угроз объекту i равна $EW_i = p_iC_i$.

Исходя из сделанных предположений, потери в системе равны $W = W_1 + ... + Wn$. Тогда ожидаемые потери (средний риск) равны:

$$EW = \sum_{i=1}^{n} p_iC_i \qquad (4.1)$$

Существуют ППП, позволяющие автоматизировать оценку риска, например, RASYS.

Порядковая шкала ценностей. Далеко не всегда возможно и нужно давать денежную оценку информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. Однако подход, связанный со сравнением ценности отдельных информационных элементов между собой, по–прежнему имеет смысл.

Пример 3. При оценке информации в государственных структурах используется порядковая шкала ценностей. Все объекты (документы) государственного учреждения разбиваются по грифам секретности. Сами грифы секретности образуют порядковую шкалу: несекретно < для служебного пользования <секретно < совершенно секретно (НС<ДСП<С<СС) или у американцев : unclassified<confidential<secret<top secret (U<Conf<S<TS). Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

Модель решетки ценностей. Обобщением порядковой шкалы является модель решетки. Пусть дано SC — конечное частично упорядоченное множество относительно бинарного отношения <, т.е. для каждых A, B, C выполняется

1. рефлексивность: A<A, (4.2)
   транзитивность: A<B, B<C==>A<C, (4.3)
2. антисимметричность: A<B, B<A => A=B. (4.4)

Определение. Для A, B∈SC элемент C=A⊕B∈SC называется наименьшей верхней границей (верхней гранью), если:

A<C, B<C;

A<D, B<D⇒C<D для всех D∈SC.

Элемент A⊕B, вообще говоря, может не существовать. Если наименьшая верхняя граница существует, то из антисимметричности следует единственность.

Упражнение. Доказать это.

Определение. Для A, B∈C элемент E=A⊗B∈SC называется наибольшей нижней границей (нижней гранью), если

E<A, E<B;

D<A, D<B⇒D<E.

Эта граница также может не существовать. Если она существует, то из антисимметричности следует единственность.

Упражнение. Доказать этот факт.

Определение. (SC, <) называется решеткой, если для любых A, B∈SC существует A⊕B∈SC и A⊗B∈SC.

Лемма. Для любого набора $S=\{A_1,...,A_n\}$ элементов из решетки SC существуют единственные элементы,:

$\oplus S=A_1\oplus...\oplus A_n$ — наименьшая верхняя граница S; (4.5)

$\otimes S=A_1\otimes...\otimes A_n$ — наибольшая нижняя граница S. (4.6)

Доказательство. Докажем ассоциативность операции ⊕.

$C_1=(A_1\oplus A_2)\oplus A3=A1\oplus(A_2\oplus A_3)=C_2$.

По определению $C_1>A_3$, $C_1>A_1\oplus A_2$. Отсюда следует $C_1>Аз$, $C_1>A_2$, $C_1>A_1$. Тогда $C_1>A_2\oplus A_3$, $C_1>A_1$, следовательно, $C_1>C_2$. Аналогично $C_2>C_1$. Из антисимметричности $C_1=C_2$.

Отсюда следует существование и единственность ⊕S. Такими же рассуждениями доказываем, что существует ⊗S и она единственна. Лемма доказана.

Для всех элементов SC в конечных решетках существует верхний элемент High = ⊕SC, аналогично существует нижний элемент Low = ⊗SC.

Определение. Конечная линейная решетка — это линейно упорядоченное множество, можно всегда считать {0, 1 ,..., n}=SC .

Для большинства встречающихся в теории защиты информации решеток существует представление решетки в виде графа. Рассмотрим корневое дерево на вершинах из конечного множества $X=\{X_1, X_2...X_n\}$ с корнем в X_i. Пусть на единственном пути, соединяющем вершину X_1 с корнем, есть вершина X_j. Положим по определению, что $X_i<X_j$. Очевидно, что таким образом на дереве определен частичный порядок. Кроме того, для любой пары вершин X_i и X_j существует элемент $X_i \oplus X_j$, который определяется точкой слияния путей из X_i и X_j в корень. Однако такая структура не является решеткой, т.к. здесь нет нижней грани. Оказывается, что от условия единственности пути в корень можно отказаться, сохраняя при этом свойства частичного порядка и существование верхней грани. Например, добавим к построенному дереву вершину L, соединив с ней все концевые вершины. Положим i=l,...,n, $L<X_j$. Для остальных вершин порядок определяется как раньше. Построенная структура является решеткой.

Упражнение. Доказать этот факт.

Приведенный пример не исчерпывает множество решеток, представимых в виде графов, однако поясняет, как связаны графы и решетки.

Упражнение. Покажите, что следующие графы определяют решетки.

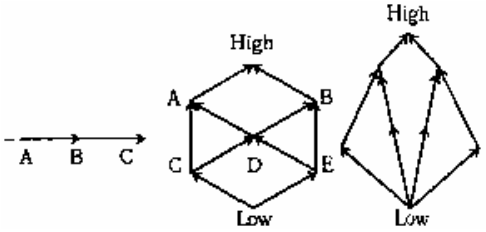


Рисунок — Примеры решеток.

Не всякий граф определяет решетку. Например,

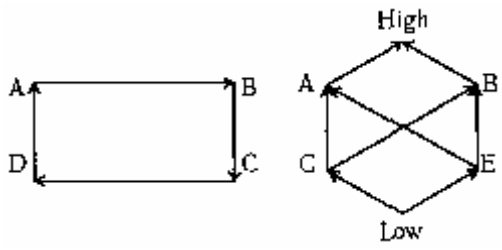


Рисунок — Графы, не являющиеся решеткой.

Упражнение. Доказать, что это так.

Решетка подмножеств x.

Для $\forall A, B \in X$. Определим $A<B \Rightarrow A \subseteq B$. Все условия частичного порядка 1), 2), 3) выполняются. Кроме того, $A \oplus B$ — это $A \cup B$, $A \otimes B = A \cap B$. Следовательно, это решетка.

Пример 4. X={1, 2, 3}.

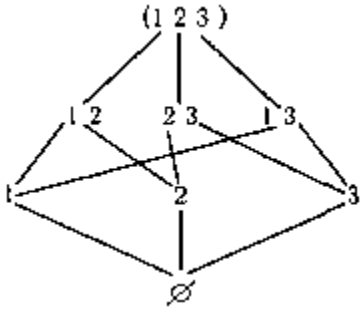
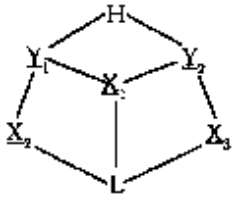


Рисунок — Пример решетки подмножеств.

Пусть программа имеет $X=\{X_1,...,X_m\}$ — входные, $Y_1...Y_n$ — выходные элементы. Каждый выходной элемент зависит от некоторых входных элементов. Отношение вход–выход описывается решеткой рассматриваемого типа. Решетка подмножеств строится по подмножествам X следующим образом. Для каждой $X_i \underline{X_i}=\{X_i\}$. Для каждой $Y_j \underline{Y_j}=\{X_i | X_j \rightarrow Y_j\}$.

Пример 5. X_1, X_2, X_3, Y_1, Y_2. Y_1 зависит только от X_1,X_2; Y_2 зависит от X_1 и X_3.

$Y_1=\{X_1,X_2\}$ $\underline{Y_2}=\{X_1,X_3\}$



MLS решетка

Название происходит от аббревиатуры Multilevel Security и лежит в основе государственных стандартов оценки информации. Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X, т.е. (α,β), (α',β') — элементы произведения, $\beta,\beta' \in L$ линейная решетка, $\alpha,\alpha' \in SC$ — решетка подмножеств некоторого множества X. Тогда

$(\alpha,\beta)<(\alpha',\beta')\Leftrightarrow\alpha\subseteq\alpha',\beta<\beta'$ (4.7)

Верхняя и нижняя границы определяются следующим образом:

$(\alpha,\beta)\oplus(\alpha',\beta')\Leftrightarrow(\alpha\cup\alpha',\max\{\beta,\beta'\})$, (4.8)

$(\alpha,\beta)\otimes(\alpha',\beta')\Leftrightarrow(\alpha\cap\alpha',\min\{\beta,\beta'\})$. (4.9)

Вся информация {объекты системы} отображается в точки решетки {(a,β)}. Линейный порядок, как правило, указывает гриф секретности. Точки множества X обычно называются категориями.

Свойства решетки в оценке информации существенно используются при классификации новых объектов, полученных в результате вычислений. Пусть дана решетка ценностей SC, множество текущих объектов O, отображение C: $0\rightarrow S$, программа использует информацию объектов $0_1,..,0_n$, которые классифицированы точками решетки $C(0_1),...,C(0_n)$. В результате работы программы появился объект O, который необходимо классифицировать. Это можно сделать, положив $C(0)= C(0_1)\oplus...\oplus C(0_n)$. Такой подход к классификации наиболее распространен в государственных структурах. Например, если в сборник включаются две статьи с грифом секретно и совершенно секретно соответственно, и по тематикам: первая — кадры, вторая — криптография, то сборник приобретает гриф совершенно секретно, а его тематика определяется совокупностью тематик статей (кадры, криптография).

4 Роль и место информационных ресурсов в современной жизни

[1]:

Стоимость потока циркулирующей сегодня в мире информации оценивается в 2,3 млрд. долл. в день (1,43 трилл. долл. в год).

Ежегодный прирост всеобщего международного трафика составляет от 11 до 15 %, и количество информации удваивается каждые 5-10 лет.

Установлена устойчивая эмпирическая зависимость между мощностью информационных потоков и зрелостью национальной экономики, согласно которой:

$$T \approx Q^2,$$

где T — трафик, Q — национальный продукт страны.

Литература:

1. Шульцева В. "Золотой" ресурс нации //Мир связи и информации. Connect!, август 1996.- с. 18-21.

[1]: В 60-е гг. во Франции стала очевидна неадекватность информационного обеспечения экономики хозяйственным потребностям.

Тогдашний президент страны Жискар д'Эстен четко сформулировал требования к информатизации страны (которые были провидческими и не потеряли актуальность и по сей день):

"Если наша страна не будет располагать мощной системой телекоммуникаций, разветвленной сетью собственных банков данных и не станет рассматривать информацию как важнейший ресурс, наравне с энергией и пахотной землей (и не привьет вкуса к потреблению этого ресурса), то мы неизбежно отстанем от главных своих конкурентов!"

Ныне страна имеет одну из наиболее прогрессивных систем телекоммуникаций в мире.

5 Информационные ресурсы. Новые технологии

Согласно Федерального Закона "Об информации, информатизации и защите информации", вступившем в действие с января 1995 г. (ст. 2):

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы ее представления;

Информационный ресурс — отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств компьютерной техники и связи.

Особенности информационных ресурсов:

13. они не потребляемы и подвержены не физическому, а моральному износу;
14. они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;
15. их использование позволяет резко сократить потребление остаточных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств;
16. процесс их создания и использования осуществляется особым способом — с помощью компьютерной техники.

Информационный процесс — процесс сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационные технологии — совокупность методов, способов, приемов, средств обработки информации и регламентированного порядка их применения, направленных на удовлетворение информационных потребностей.

[Герасименко В.А. Информационный системотехник — менеджер — новая профессия: сущность, необходимость, содержание //Зарубежная радиоэлектроника, № 11/12, 1994. — с. 48 — 52.]

Проблема обеспечения качества информации — относится к числу сложных проблем, поскольку:

1. само понятие качества информации — очень сложное, многоаспектное и в значительной мере неопределенное;
2. на качество информации оказывает влияние большое количество дестабилизирующих факторов, многие из которых носят неопределенный характер;
3. трудно (если вообще возможно) выразить зависимость показателей качества информации от воздействия всей совокупности дестабилизирующих факторов;
4. средства обеспечения качества информации до настоящего времени разработаны явно недостаточно;
5. в настоящее время нет полных и объективных данных о зависимостях качества информации от применяемых средств его обеспечения.

Информатика — это научно — техническое направление, изучающее информационные проблемы современного общества и разрабатывающее способы, методы и средства наиболее эффективного их решения.

Новые информационные технологии

В журнале "Информационные технологии", издаваемом с 1995 г., дается следующее определение [см.: Колин И.К. Информационные технологии — катализатор процесса развития современного общества, с. 2 — 8 //Информационные технологии, № 0, 1995 г.]:

Информационная технология — это представленное в проектной форме (т.е. в формализованном виде, пригодном для практического использования) концентрированное выражение научных знаний и практического опыта, позволяющее рациональным образом организовать тот или иной достаточно часто повторяющийся процесс.

Там же [Горбатов В.А. Интеллектуальные информационные технологии и стратегии (состояние и перспективы), с. 35 — 38] перечисляются критические технологии, определяющие процветание государства в XXI веке:

1. производство и обработка материалов различных классов;
2. автоматизированное проектирование (САПР), особенно электронных, машиностроительных, организационных систем, а также строительных, банковских, картографических, структур;
3. производство электронных компонентов, в том числе и hardware;
4. создание информационных средств, в том числе и software;
5. двигателестроение.

6 Безопасность информации. Информационная безопасность

[1]:

Безопасность информации (information security) — такое состояние ее в системе обработки, когда несанкционированное получение защищаемой информации лицами и процессами, не имеющими на это специальных полномочий, становится невозможным или сводится к уровню не выше допустимого.

Понятие безопасности информации тесно связано с понятием:

[2]: Безопасность данных (data security) — это также состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Защита данных — совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных.

Таким образом, защита данных есть процесс обеспечения безопасности данных, а безопасность — состояние данных, конечный результат процесса защиты.

[3]:

Информационная безопасность — это состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

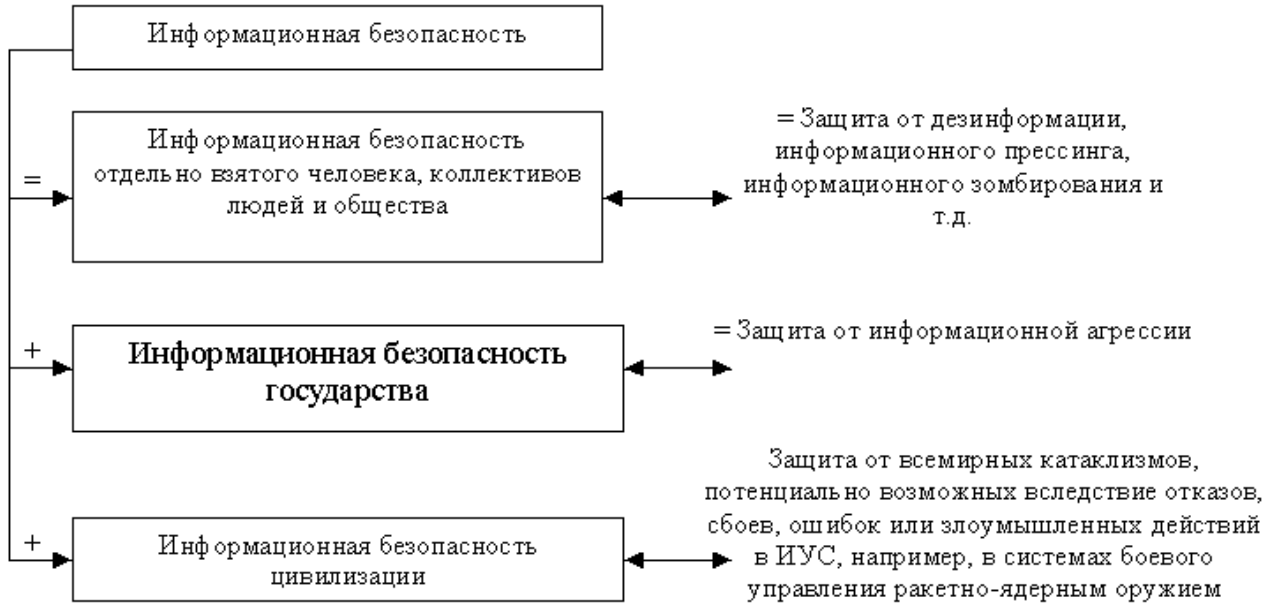


Рисунок — Информационная безопасность

Литература:

1. Герасименко В.А. Информационный системотехник-менеджер — новая профессия: сущность, необходимость, содержание //Зарубежная радиоэлектроника, № 11-12, 1994, с. 48-52.

2. Большаков А.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. Учебное пособие. — С.-П., 1996.- 165 с.

3. Защита информации. Термины и определения. Словарь (составитель — В.И. Парфенов)//Вопросы защиты информации, вып. 3-4, М., 1996.

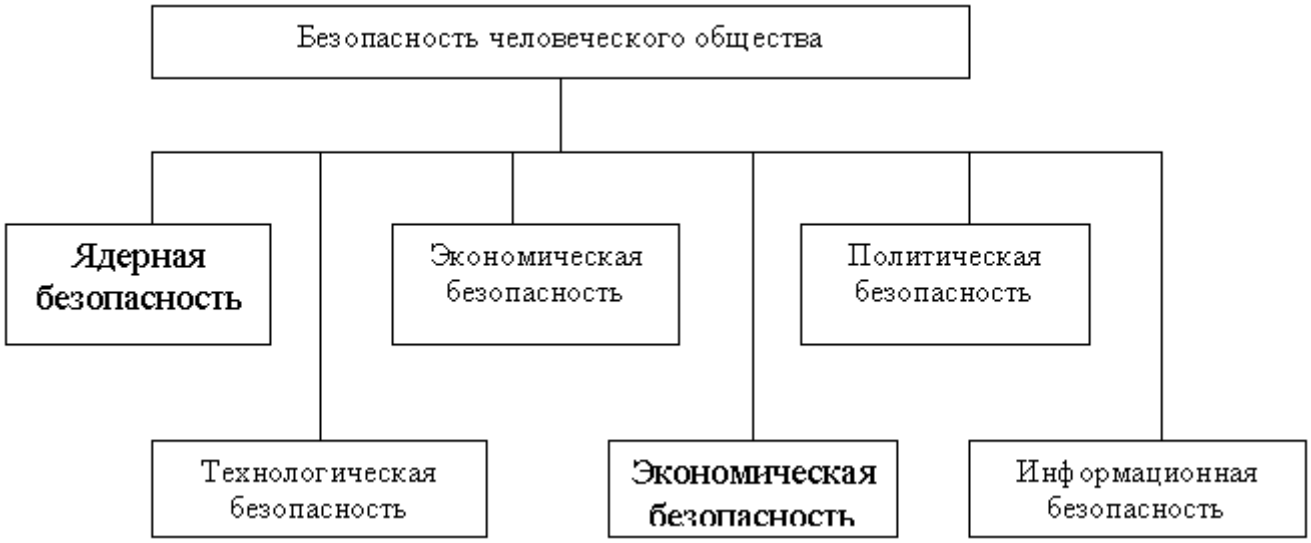


Рисунок — Классификация видов безопасности

Информационная безопасность является основой этих составляющих безопасности человеческого общества.

[1]: Информационная безопасность — состояние защищенности внешней среды от дестабилизирующего воздействия информации, находящейся и обрабатываемой в организованных системах, на окружающую среду.

Понятие информационной безопасности — связано с угрозой интересам личности, общества и государства, возникающей от:

1. воздействия информации на общество, на безопасность государства;

   воздействия на саму информацию;

   нарушения информационных прав и свобод личности.

При этом информационное законодательство выступает как правовое обеспечение информационной безопасности, а концепция информационной

безопасности — как основа, методическое руководство для конструирования информационного законодательства.

Требования к информации с точки зрения ее безопасности

[1]

1. Безопасность (securitiy) — это гарантированная конституционными, законодательными и практическими мерками защищенность и обеспеченность жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Безопасность:

- это наука, которую надо изучать и развивать;
- это искусство, которое надо постигать;
- это культура, которую надо воспитывать у предпринимателей.

Под жизненно важными интересами коммерческих предприятий понимаются:

- экономическая самостоятельность:
- правовое и социальное благополучие;
- структурная целостность;
- стабильное и эффективное функционирование.

Объектами безопасности являются:

- персонал (руководство, ответственные исполнители, сотрудники);
- финансовые средства, материальной ценности, новейшие технологии;
- информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, представленная в виде документов и массивов независимо от формы и вида их представления).

Состояние защищенности представляет собой умение и способность организации надежно противостоять любым попыткам конкурентов нанести ущерб законным интересам коммерческого предприятия.

Литература:

1. Алешенков М.С., Бузанова Я., Ярочкин В.И. Концепция комплексной безопасности предпринимательства. — М.: Паруса, 1997. — 31 с.

7 Концепция информационной безопасности России

[Информационные технологии, #3,1996,с. 8–9; А.П. Курило, Д.С. Черешкин "Проблемы информационной безопасности России и пути их разрешения "]:

Концепция информационной безопасности России, утвержденной Советом Безопасности РФ и президентом, является составной частью Концепции национальной безопасности РФ и служит методологической основой для: разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплексную основу мер по её практической реализации;

- формирование и поведение государственной политики РФ в области обеспечения информационной безопасности;
- разработки целевых программ защиты информационных ресурсов и средств информатизации.

В Концепции впервые осуществлен переход от понятия «защита информации» к более широкому понятию «информационная безопасность». В этом документе подчеркивается необходимость учета и согласования интересов трех основных субъектов, функционирующих в информационной сфере: личности; общества; государства.

- Как следствие изменения подхода, в состав объектов информационной безопасности, наряду с традиционными информационными ресурсами, системами переработки информации, информационной инфраструктурой, включены информационные права граждан и системы формирования общественного сознания.

При разработке данной Концепции принята следующая логика:

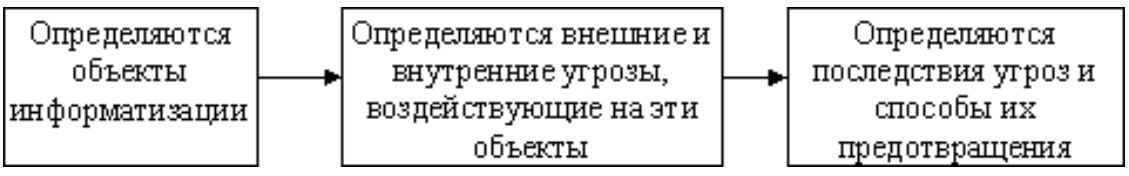


Рисунок — Этапы разработки Концепции

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития.

В соответствии с этими приоритетами, основными целями информационной безопасности являются:

- Защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых информационных сетей и стремления США и других развитых стран к информационному доминированию;
- Концепция информационной безопасности России, утвержденной Советом Безопасности РФ и президентом, является составной частью Концепции национальной безопасности РФ и служит методологической основой для:
- разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплексную основу мер по её практической реализации;
- формирование и поведение государственной политики РФ в области обеспечения информационной безопасности;
- разработки целевых программ защиты информационных ресурсов и средств информатизации.
- обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;
- реализация прав граждан, организаций и государства на получение, распределение и использование информации.

К основным задачам обеспечения информационной безопасности относятся:

- выявление, оценка и прогнозирование источников угроз информационной безопасности;
- регулировка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов ее реализации;
- регулировка нормативно–правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;
- развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств предотвращения,

парирования и нейтрализации угроз информационной безопасности и ликвидности последствий ее нарушения;

- обеспечения активного участия России в процессах создания и использования глобальных информационных сетей и систем.

К числу ключевых проблем в области обеспечения информационной безопасности в России относится:

1. развитие научно–технических основ информационной безопасности, отвечающей современным геополитическим ситуациям и условиям политической и социально–экономического развития РФ;
2. разработка современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации;
3. разработка критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

8 Этапы развития концепции обеспечения безопасности информации

[Мельников В.В., с. 103 -110]; [Герасименко В.А., ч.I, с. 26]; [Большаков А.А. и др., с. 12-15]

1 этап (1960-1970 гг.). Попытка обеспечить надежную защиту информации чисто формальными механизмами, содержащими, главным образом, технические и программные средства. Сосредоточение программных средств в рамках операционных систем и систем управления БД.

Слабым звеном разработанных механизмов защиты оказался механизм защиты доступа пользователя к данным. Попытки создания механизмов дифференцируемого доступа к данным, на пример, систем MULTICS и ADEPT-50, показали, что они также имеют множества недостатков.

2 этап (1970-1976 гг.). Дальнейшее развитее формальных механизмов защиты информации. Выделение упрощенного компонента защиты данных — ядра безопасности. Развитие не формальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных.

Ядро безопасности — это специальный программный компонент, управляющий программными и, частично, аппаратными средствами защиты данных. После нескольких попыток включения ядра безопасности в состав ОС была сформирована, концепция создания функционально самостоятельных подсистемы управления механизмами защиты информации, которые включали в себя технические, программные, информационные и лингвистические средства.

Этот этап характеризуется также интенсивным развитием технических и криптографических средств защиты. Однако, несмотря на принимаемые меры, обеспечение надежной защиты информации оказалось недостижимым, о чем свидетельствовали многочисленные факты нарушения безопасности данных.

3 этап (1976-1990 гг.). Дальнейшее развитие механизмов 2-го этапа. Формирование взглядов на обеспечение безопасности как на непрерывный процесс. Развитие стандартов на средства защиты информации. Усиление тенденции на аппаратные реализации средств защиты информации. Формирование вывода о

взаимосвязи обеспечения безопасности данных, архитектура ИВС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения безопасности данных (защиты информации).

Основной отличительной особенностью этого этапа стала применение принципа системности к проблеме защиты информации. Принцип системности требует, что бы обеспечение ЗИ (безопасности данных) представляло собой регулярный процесс, осуществимый на всех этапах жизненного цикла ИВС при комплексном использовании всех средств и механизмов защиты. При этом все средства и механизмы защиты, используемые для ЗИ, объединяются в систему обеспечения ЗИ, которая должна обеспечить многоуровневую ЗИ не только от злоумышленников, но и от пользователей и обслуживающего персонала ИВС.

4 этап (1990 г. — по настоящее время). Дальнейшее развитие механизмов 3-го этапа. Формирование основ теории обеспечения ЗИ в ИВС. Разработка моделей, методов и алгоритмов управления ЗИ в ИВС.

Данный этап отражает современное представление об интеллектуализации ОСУ. Накопленный опыт в области обеспечения ЗИ, а также усиления тенденции стандартизации и унификации ИВС позволили перейти к разработке методов, моделей и алгоритмов управления ЗИ в ИВС. На данном этапе также были сформулированы основы теории обеспечения ЗИ в ИВС и определенны основные научные направления исследований в рамках указанной теории.

[Большаков А.А., Петряев А.Б., Платонов В.В., Ухлинов Л.М. Основы обеспечения безопасности данных в компьютерных системах и сетях. — учебное пособие, С.-Петербург, 1996. -165с.]:

Теория обеспечения безопасности информации — новое научное направление, изучающее методы предотвращения случайного или преднамеренного раскрытия, искажения или уничтожения хранимой, обрабатываемой и передаваемой информации в системах управления, функционирующих на базе средств вычислительной техники и передачи данных.

9 Классификация защищаемой информации

Информация как объект защиты

Классификационные признаки информации

Информация может быть классифицирована по следующим признакам:

1. Формам представления (носителям): документированная и недокументированная информация;
2. Праву собственности: государственные и негосударственные информационные ресурсы;
3. Условиям правового режима: информация, отнесенная к государственной тайне и конфиденциальная.

Структура классификации информации:

Литература:

1. Василец В.И., Голованов В.Н. Правовая защита результатов интеллектуальной деятельности акционерного общества // Вопросы защиты информации, Вып. 3 (34), 1996. — с. 29 — 33.

Согласно Закона РФ “Об информации, информатизации и защите информации”,

1. **Документированная информация** — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (документирование, осуществляемое в установленном порядке, является обязательным условием для включения информации в информационные ресурсы).
2. **Недокументированная информация** — речевая информация, воспринимаемая ”на слух”, в том числе с использованием технических средств ее приема и передачи, а также опосредствованная информация, находящая свое отображение в технических демаскирующих признаках технологий и факторах производственной среды, косвенно раскрывающих исходящую информацию (законодательное регулирование вопросов, связанных с использованием и защитой недокументированной информации, в настоящее время отсутствует).
3. **Государственная тайна** — (согласно “Закона о государственной тайне”) — это защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно — розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Негосударственные информационные ресурсы создаются или приобретаются АО на законных основаниях за счет его собственных средств.
4. **Конфиденциальная информация** — документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ. Включает в себя информацию, составляющую:

- коммерческую;
- профессиональную;
- служебную и другие тайны;
- а также персональные данные.

Классификация защищаемой информации по характеру сохраняемой тайны

Литература:

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. — Кн. 1, М.: 1994 — С.10-11.
2. Хэфман Л.Дж. Современные методы защиты информации — М.: 1980.

Основными видами информации, подлежащими защите в АСОД (автоматизированных системах обработки данных), могут быть:

- исходные данные, то есть данные, полученные в АСОД на хранение и обработку от пользователей, абонентов и взаимодействующих систем;
- производные данные, то есть данные, полученные в АСОД в процессе обработки исходных и производных данных;
- нормативно-справочные, служебные и вспомогательные данные, включая и данные систем защиты;
- программы, используемые для обработки данных, организации и обеспечения функционирования АСОД, включая и программы системы ЗИ;
- алгоритмы, на основе которых разрабатывались программы (если они находятся на объектах, входящих в состав АСОД);
- методы и модели, на основе которых разрабатывались алгоритмы (если они находятся на объектах, входящих в состав АСОД);
- постановки задач, на основе которых разрабатывались алгоритмы (если они находятся на объектах, входящих в состав АСОД);
- техническая, технологическая и другая документация, находящаяся на объектах АСОД.

Защищенность — способность противостоять НСД к конфиденциальной информации, ее искажению или разрушению.

[2]:Секретность — это понятие, которое употребляется по отношению к отдельным лицам. Это есть право лица решать какую информацию он желает разделить с другими, а какую хочет скрыть от других.

Законодательством России охраняется три основных вида информации, которые одновременно подлежат защите:

1. сведения, отнесенные к государственной тайне соответствующим федеральным законом, под которыми понимается информация в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно–розыскной деятельности, распространение которой может нанести ущерб безопасности России *[1]*;
2. сведения, отнесенные к служебной и коммерческой тайне в соответствии со статьёй 139 Гражданского кодекса России, под которыми понимается информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, если к ней нет законного доступа на законных (санкционированных) основаниях

и обладатель такой информации принимает меры к охране её конфиденциальности *[2]*;

3. сведения, имеющие статус в соответствии со статьёй 11 Федерального Закона “Об информации, информатизации и защите информации” понимается информация о гражданах, включаемая в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, органов местного самоуправления, а также получаемая и собираемая негосударственными организациями *[3]*;

Литература:

1. Закон Российской Федерации “О государственной тайне”//Росс. газета, 1993, 21 сентября.
2. Гражданский кодекс Российской Федерации (часть 1 и 2). Волгоград: ВЮИ МВД России, 1995.
3. Закон Российской Федерации “Об информации, информакизации и защите информации”//Собр.Закон. РФ, №8, 20 фквраля 1995, ст. 609.

К информации составляющей профессиональную тайну (know–how), относятся секреты производства АО и иная производственно–технологическая информация, не запрещенная законодательством РФ.

Служебная тайна связана с понятием служебной информации ограниченного распространения, используемым в федеральных органах исполнительной власти и подведомственных им организациях.

Конфиденциальная информация.

В указе Президента РФ “Об утверждении перечня сведений конфиденциального характера” от 06.03.1997 года приводится перечень сведений конфиденциального характера:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в

средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграмм или иных сообщений и т.д.)
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретений, полезной модели или промышленного образца до официальной публикации информации о них.

[“Защита информации. Confident”, №3, 1997, с.20].

10 Угрозы безопасности информации. Обобщенная модель нарушения защищенности информации. Примеры конкретных видов угроз.

Требования к информации с точки зрения её безопасности (доступа к ней)

Главная цель ЗИ — это контроль за доступом к ней. К просмотру, созданию, удалению или изменению данных должны допускаться только лица, обладающие необходимыми полномочиями.

Основные требования, предъявляемые к информации:

1) Должна обеспечиваться конфиденциальность (confidentiality) сохраняемых личных или других важных данных.	Конфиденциальная (от латинского слова confidential — доверие) информация — доверительная, ограниченного пользования, не подлежащая передаче посторонним лицам.
2) Должна поддерживаться целостность (integrity) и точность хранимой информации и программ, которые её обрабатывают.	Целостность информации — гарантирует отсутствие несанкционированных изменений в сообщении (данных) при их передаче или хранении. Точность (достоверность) — полное соответствие действительности, истине; подлинность, правильность, отсутствие каких–либо отклонений.
3) Должна обеспечиваться доступность систем, данных и служб для тех, кто имеет право доступа.	Отказ в доступе одним пользователям и гарантия легкого доступа другим предполагает очень тщательную и разумную фильтрацию.
4) Должно обеспечиваться соответствие всех направлений деятельности действующему законодательству, инструкциям, лицензиям, контрактам и устным этическим нормам.	Под законодательными мерами понимаются законодательные акты, которыми регламентируются правила использования данных ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Этические нормы — это нормы, несоблюдение которых ведет к потере авторитета, престижа человека или организации.

[Большаков А.А и др. “Основы обеспечения безопасности данных в компьютерных системах и сетях”, с.12]:

Доступ — это процесс использования технических и программных средств, обеспечивающий логическую (физическую) связь с каким–либо ресурсом для его функционального использования или получения (модификации) поддерживаемых этим ресурсом данных.

Ресурс — это любой компонент ИВС (устройство, программа, файл, БД, и т.п.), который может использоваться для выполнения каких–либо операций в ИВС.

Объект доступа — это пассивный ресурс, используемый субъектом доступа для выполнения операций.

Субъект доступа — это актитвный ресурс (оператор, процесс или устройство), осуществляющий какие–либо действия над другими ресурсами.

[Хоффман Л.Дж. “Современные методы ЗИ”, 1980]:

Целостность данных — имеет место только тогда, когда данные в системе не отличаются от данных в исходных документах, т.е. не произошло их случайной или преднамеренной замены или разрушения.

[Герасименко В.А. “ЗИ в АСОД”, часть 1, М.: 1994,с.8]:

Физическая целостность — отсутствие искажений или уничтожения элементов информации.

Угрозы безопасности информации (опасности).

Одной из главных особенностей проблемы ЗИ является требование полноты определения угроз информации, потенциально возможных в современных ИВС. Даже один неучтенный (невыявленный или не принятый во внимание) дестабилизирующий фактор может в значительной степени снизить (и даже свести на нет) эффективность защиты. В то же время, проблема формирования полного множества угроз относится к числу неформализованных проблем, регулярные методы решения которых отсутствуют.

Угроза безопасности информации — это потенциально существующая возможность случайного или преднамеренного действия или бездействия, в результате которого может быть нарушена безопасность информации (данных).

Угроза (threat) — это человек, вещь, событие или идея, которая представляет некоторую опасность для ценностей, нуждающихся в защите.

Возникновение угрозы может подвергать опасности конфиденциальность, целостность или доступность информации через уязвимые и слабые места системы. Угроза необязательно должна быть умышленной или преднамеренной. Угроза может заключаться в таких событиях, как человеческие ошибки, сбои оборудования,

стихийные бедствия и перебои линий связи. К умышленным угрозам относятся воровство, вандализм, диверсии и злоупотребление ресурсами.

Носитель угрозы (threat agent) — это сущность (субъект), которая может инициировать возникновение угрозы.

Последствия угрозы (consequence или outcome) — это нежелательные результаты проявления угрозы по отношению к каким–либо ценностям, которые приводят к ощутимой потере для организации.

[Л.Дж.Хоффман]:

Угроза — это событие или действие, которое может вызвать нарушение функции ИВС, включая искажение, уничтожение или несанкционированное использование (размножение) обрабатываемой информации.

Рисунок — Угрозы и их последствия

Общая модель процесса нарушения защищенности информации:

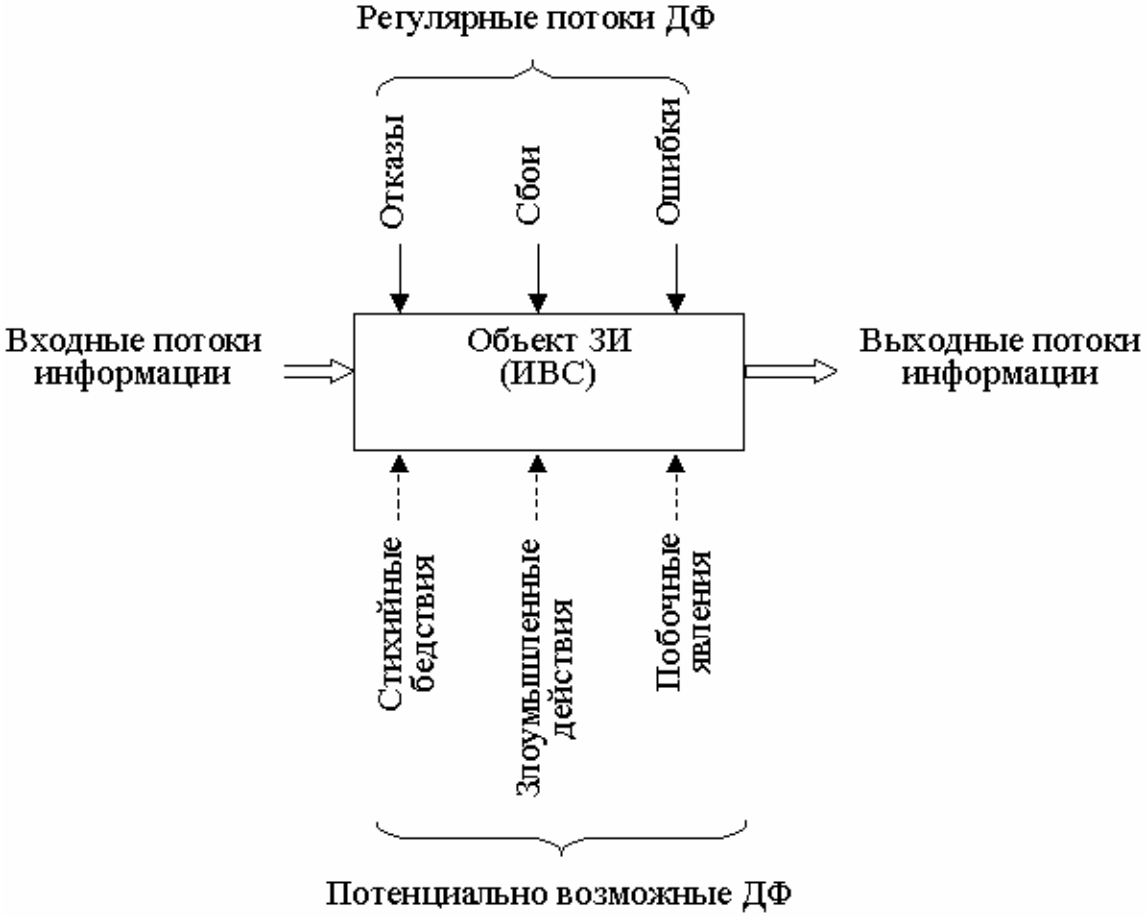


Рисунок — Общая модель процесса нарушения защищенности информации

Дестабилизирующие факторы (угрозы) могут быть разбиты на 2 группы:

- случайные (отказы, сбои, ошибки компонентов ИВС), которые могут появиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов.
- потенциально возможные (стихийные бедствия, действия злоумышленников, побочные явления), которые могут и не случиться, но в случае их возникновения приводят к крайне нежелательным последствиям.

Отказ (failure или fault) — это нарушение работоспособности какого–либо элемента ИВС, приводящее к невозможности выполнения им своих функций.

Сбой (malfunction) — это временное нарушение работоспособности какого–либо элемента ИВС, следствием чего может быть неправильное выполнение им в этот момент своих функций.

Ошибка (вид) — неправильное (одноразовое или систематическое) выполнение элементом ИВС одной или нескольких функций, происходящее вследствие специфического его состояния.

Ошибки включают в себя:

- ошибки основной аппаратуры (неправильный монтаж той или иной схемы);
- ошибки программ;
- ошибки людей;
- ошибки системы передачи данных (например: неправильная схема коммутации канала);

Стихийные бедствия — пожары, наводнения, стихийные бедствия, взрывы и т.д.

Злоумышленные бедствия — связаны главным образом с несанкционированным доступом к ресурсам ИВС.

Побочные явления — электромагнитные излучения устройств ИВС, паразитные наводки, внешние электромагнитные излучения, вибрации, внешние атмосферные условия и т.д.

Несанкционированный доступ к данным (НСД) — злоумышленное или случайное действие, нарушающее технологическую схему обработки данных и ведущее к получению, модификации или уничтожению данных. НСД к данным может быть пассивным (несанкционированное получение или размножение информации) и активным (модификация, уничтожение информации).

Нарушитель — субъект, осуществляющий НСД к данным.

Злоумышленник (противник) — субъект, осуществляющий преднамеренный НСД к данным.

Классификация угроз безопасности данных

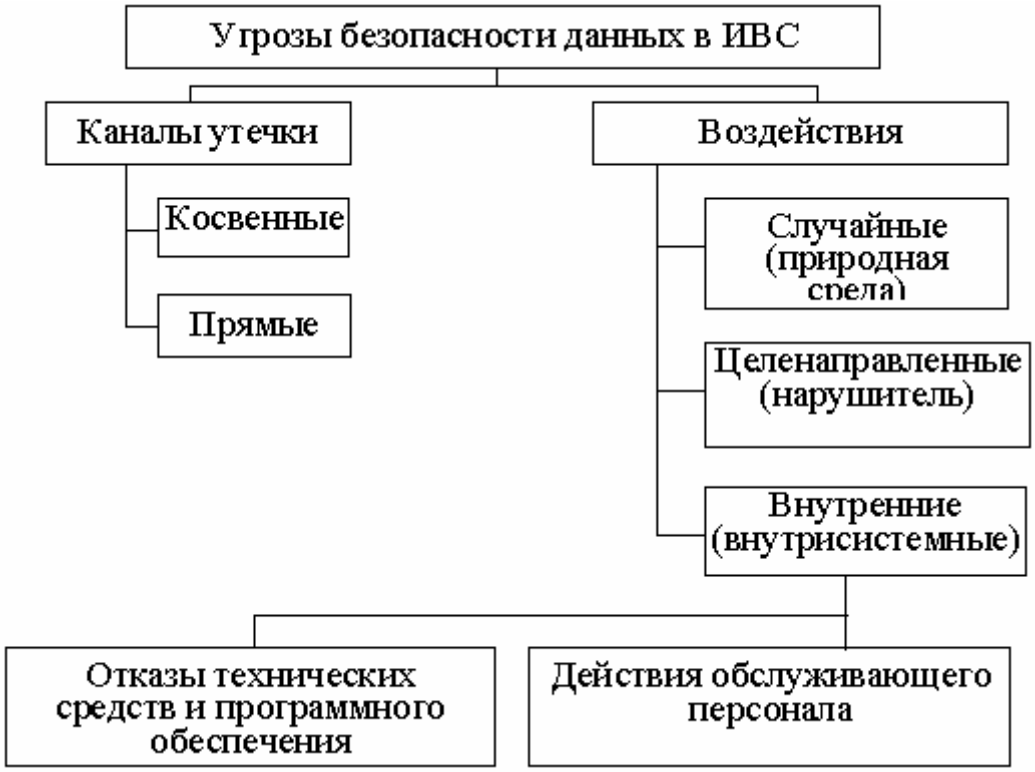


Рисунок — Классификация угроз безопасности данных

[Д. Стенг, С. Мун "Секреты безопасности сетей" стр. 13]

В таблице показано, каким из главных требований защиты угрожают конкретные виды угроз (опасностей) .

Угроза	Конфиденци-альность	Целостность	Доступность	Законность/ Этические нормы
Аппаратные сбои	X	X	X	
Вирусы		X	X	
Диверсии		X	X	
Излучение	X			
Искажение	X			X
Кража	X	X	X	
Логические бомбы	X	X	X	
Мошенничество		X		
Небрежность	X	X	X	
Неправильная маршрутизация	X			

Неточная или устаревшая информация		X		X
Ошибки программирования	X	X	X	
Перегрузка			X	
Перехват	X			
Пиггибекинг	X	X	X	
Пиратство				X
Подлог		X		
Пожары и другие стихийные бедствия		X	X	
Потайные ходы и лазейки	X	X	X	
Препятствие использованию			X	
Различные версии		X		
Самозванство	X	X	X	
Сбор мусора	X			
Сетевые анализаторы	X			
Суперзаппинг	X	X	X	
Троянские кони	X	X	X	
Умышленное повреждение данных или программ		X		
Хищение		X		

1. **Логическая бомба** (logic bomb) — модификация компьютерной программы, в результате которой данная программа может выполняться несколькими способами в зависимости от определенных обстоятельств. При

проверке в обычных условиях бомба никак не проявляется, но при определенном событии программа работает по алгоритму, отличному от заданного.

Логическая бомба может использоваться для хищений. Например, программист может прибавить к программе начисления заработной платы код, слегка повышающий его жалование (IF сотрудник = Я THEN зарплата = часы * ставка * 1,01 ELSE зарплата = часы * ставка). Такое изменение кода может оставаться незамеченным в течение многих лет.

Задача по написанию логических бомб не сложнее любой другой задачи в программировании. Но обнаружение таких бомб это очень трудоемкий процесс.

2. **Небрежность** (bumbling) — именуется также ошибкой человека (human error), случайностью (accident), оплошностью (error of omission), проявлением некомпетентности (error of commission).

“Неумелые пальцы” являются самым распространенным источником несчастий в любой компьютерной системе (до 50 — 60% ежегодных компьютерных потерь).

3. **Перехват** (wiretapping) — может выполняться с применением элементарных зажимов типа “крокодил”, а также путем наблюдения за излучением или спутниковыми передачами с помощью антенн. Пассивный перехват (passive tapping) индуцируемых волн может происходить с использованием кассетного магнитофона, микрофона, коротковолновой радиостанции, модема и принтера.

Характеристика конкретного вида опасности (угрозы)

Рисунок — Характеристика конкретного вида угроз

Вирус — это возможное оружие маленькой нации. Вирус, разработанный в странах третьего мира, может выполнить главное задание по снижению эффективности действий противника (заменяя террористов). Поскольку ведущие государства компьютеризированы в большей степени, чем страны третьего мира, то ущерб для первых будет более значительным.

Тип угрозы	Чему угрожает?	Как обнаруживается?	Как часто проявляется?	Каковы последствия?	Как предотвращается?
Вирус	Целостности Доступности	Очевидно	Очень часто	Потенциально большие	Сложно

4. **Пиггибекинг** (piggybacking) (от слов “piggy” — поросенок, свинка и “back” — спина) — непосредственное проникновение, получение доступа в систему (закрытую зону) после того, как легальный пользователь некорректно завершил сеанс работы. Например, электронные пиггибекеры (piggybacker) могут использовать основной терминал, оставленный без присмотра, либо доступный, нелегально подключенный к тому же кабелю. Физический пиггибекинг — физическое проникновение в закрытую зону (помещение) через дверь, которую забыли закрыть.

5 **Суперзаппинг** (superzapping) — это несанкционированное использование какой–то утилиты для модификации, уничтожения, копирования, вскрытия, применения или запрещения применения компьютерных данных. SUPERZAP — утилита, имеющаяся во многих больших компьютерных системах. Она позволяет оператору запускать, останавливать или модифицировать процедуру. Применительно к ПЭВМ, функциональный эквивалент такой процедуры подобен Norton Utilities или PC Tools.

6 **Троянские кони** (Troyan horse) — это такие программы, которые вместо выполнения действий, для которых они якобы предназначены, на самом деле выполняют другие. Троянский конь, как и любая другая программа, может производить самые разные операции, включая изменение БД, запись в платежные ведомости, отправку E–mail или уничтожение файлов. Когда такая программа запускается, она может разрушить таблицу размещения файлов (FAT) и каталоги, что является эффективным методом удаления файлов на жестком диске.

[Д. Стенг, С. Мун «Секреты безопасности сетей», Киев, 1996, с. 51]

Согласно отчету, подготовленному в 1989 году фирмой Executive Information Network, вероятность возникновения различных угроз безопасности принимает следующие значения:

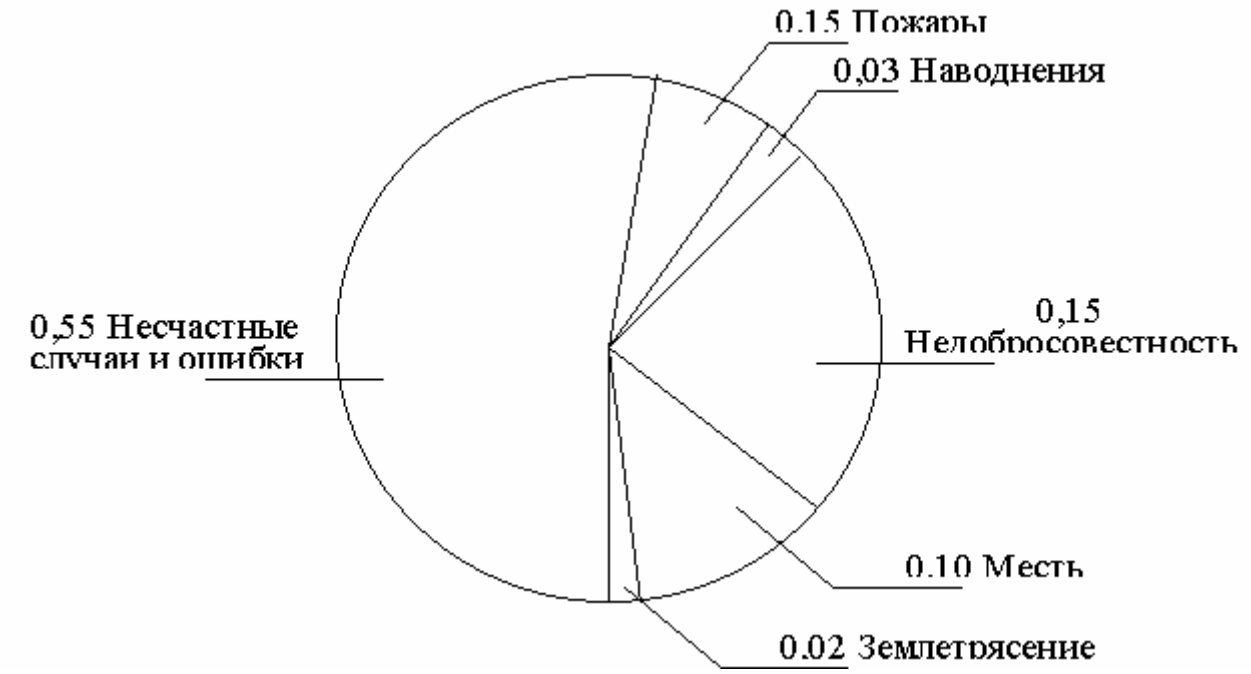


Рисунок — Вероятность возникновения различных угроз безопасности

Таким образом, 80 % всех угроз возникает по вине служащих, а 20 % приходится на стихийные бедствия.

Угрозы информации

Если информация представляет ценность, то необходимо понять, в каком смысле эту ценность необходимо оберегать. Если ценность информации теряется при ее раскрытии, то говорят, что имеется опасность нарушения секретности информации. Если ценность информации теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации. Если ценность информации в ее оперативном использовании, то говорят, что имеется опасность нарушения доступности информации. Если ценность информации теряется при сбоях в системе, то говорят, что есть опасность потери устойчивости к ошибкам. Как правило, рассматривают три опасности, которые надо предотвратить путем защиты: секретность, целостность, доступность. Хотя, как показывают

примеры действий в боевых условиях, развитие сложных систем Hewlett–Packard, Tandem, практически добавляется четвертое направление: устойчивость к ошибкам.

Под угрозами подразумеваются пути реализации воздействий, которые считаются опасными. Например, угроза съема информации и перехвата излучения с дисплея ведет к потере секретности, угроза пожара ведет к нарушению целостности информации, угроза разрыва канала может реализовать опасность потерять доступность. Угроза сбоя электроэнергии может реализовать опасность неправильной оценки ситуации в системе управления и т.д.

В главе рассматриваются вопросы анализа опасностей, выявления угроз. Далее рассматриваются основные угрозы нарушения секретности в ЭСОД и механизмы их предотвращения, угрозы нарушения целостности и механизмы защиты от них. Связь между видом опасности и возможной угрозой состоит в месте, времени и типе атаки, реализующей угрозу. Анализ опасности должен показать, где и когда появляется ценная информация, в каком месте системы эта информация может потерять ценность. Угроза характеризует способ нападения в. определенном месте и в определенный момент. Угроза реализуется через атаку в определенном месте и в определенное время.

Угрозы Секретности

В руководстве по использованию стандарта защиты информации американцы говорят, что существует только два пути нарушения секретности:

- утрата контроля над системой защиты;
- каналы утечки информации.

Если система обеспечения защиты перестает адекватно функционировать, то, естественно, траектории вычислительного процесса могут пройти через состояние, когда осуществляется запрещенный доступ. Каналы утечки характеризуют ту ситуацию, когда–либо проектировщики не смогли предупредить, либо система не в состоянии рассматривать такой доступ как запрещенный. Утрата управления системой защиты может быть реализована оперативными мерами, и здесь играют существенную роль административные и кадровые методы защиты. Утрата контроля за защитой может возникнуть в критической ситуации, которая может

быть создана стихийно или искусственно. Поэтому одной из главных опасностей для системы защиты является отсутствие устойчивости к ошибкам.

Утрата контроля может возникнуть за счет взламывания защиты самой системы защиты. Противопоставить этому можно только создание защищенного домена для системы защиты.

Разумеется, в реальной жизни используются комбинации этих атак.

Большой спектр возможностей дают каналы утечки. Основной класс каналов утечки в ЭСОД — каналы по памяти (т. е. каналы, которые образуются за счет использования доступа к общим объектам системы). Графически канал по памяти можно изобразить следующим образом:

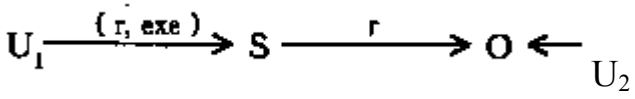


Рисунок — Канал по памяти

Пользователь U_1 активизирует процесс, который может получить доступ на чтение к общему с пользователем U_2 ресурсу O, при этом U_2 может писать в O, а U_1 может читать от S. Приведем примеры таких каналов.

Пример 1. В директорию O внесены имена файлов. Хотя доступ к самим файлам для субъекта S_1 закрыт, доступ к директории возможен. Если субъект S_2 создал закрытые файлы, то информация о файловой структуре стала доступной S_1. Произошла утечка части информации. В частности, существование или нет одного конкретного файла — 1 бит.

Значит, в этом случае создан канал утечки одного бита из той информации, которая принадлежит S_2.

Пример 2. Вирус–архиватор, созданный пользователем U_1, заражает командные файлы пользователя U_2 за счет использования совместных ресурсов объекта в виде компьютерной игры. Съем информации осуществляется при помощи записи архива сделанных U_2 файлов на каждую принесенную дискету. Это гарантирует анонимность истинного получателя информации в случае выявления вируса.

Защитные механизмы основаны на правильном выборе политики безопасности.

Пример 3. Очень важным примером канала утечки по памяти является возможность статистического вывода в базах данных. Обычно в базах данных с ограниченным доступом функции вычисления статистик по закрытым данным являются общедоступными. Это создает ситуацию совместного использования закрытых ресурсов допущенными и незаконными пользователями. Как было показано в разделе "информационные потоки", канал связи от закрытой информации к незаконному пользователю может быть сильно зашумлен. Однако использование различных статистик и модификация запросов могут позволить отфильтровать информацию.

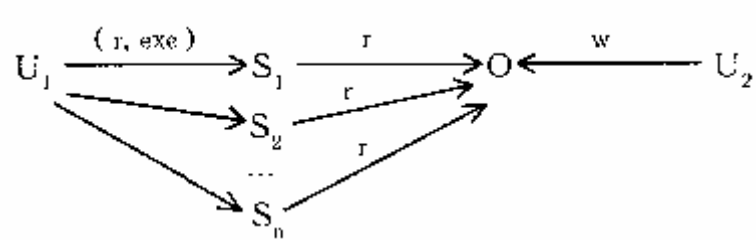


Рисунок — Процессы между законным и незаконным пользователем

где U_1 — незаконный пользователь; U_2 — законный пользователь ценной информации в объекте O; S_1, S_2,...,S_n — процессы вычисления ответов на различные запросы пользователя U_1. Доступ S_i к O разрешен, так как в каждом случае по O вычисляется статистическая характеристика, не дающая достаточно полной информации об объекте O. Защитные механизмы основаны на контроле возможностей вывода и контроле информационных потоков.

Следующий основной класс каналов утечки американцы называют каналами по времени. Канал по времени является каналом, передающим противнику информацию о процессе, промодулированном ценной закрытой информацией. Графически канал по времени можно изобразить следующей схемой

$$U_1 \xrightarrow{(r,exe)} S \xrightarrow{r} S_m \xleftarrow{w} S_u \xleftarrow{exe}$$

Рисунок — Графическое изображение канала времени

где U1 — злоумышленник; U_2 — пользователь, оперирующий ценной информацией; $S_ц$ — субъект, информация о котором представляет интерес; S_m — субъект, процесс которого модулируется информацией процесса $S_ц$; S — процесс от имени пользователя U_1, позволяющий наблюдать процесс S_m.

Функционирование канала утечки определяется той долей ценной информации о процессе $S_ц$, которая передается путем модуляции процессу S_m.

Пример 4. Пусть процесс $S_ц$ использует принтер для печатания результатов очередного цикла обработки информации. Процесс $S_м$ определяется работой принтера, который является общим ресурсом U_1 и U_2 с приоритетом у U_2. Тогда процесс S регулярно с заданной частотой посылает запрос на использование принтера и получает отказ, когда $S_ц$ распечатывает очередную порцию информации. Тогда в единицах частоты запроса пользователь U_1 получает информацию о периодах обработки процессом $S_ц$ ценной информации, то есть получаем канал утечки. Защитные механизмы от таких каналов основаны на контроле информационных потоков в системе.

Пример 5 Перехват информации в канале связи является примером канала утечки по времени. Здесь реализуется непосредственный доступ к процессу обработки (передачи) ценной информации. Съем информации об этом процессе и накопление ее во времени восстанавливают переданную ценную информацию. Защита от этих каналов основана на криптографии.

Пример 6. Побочные каналы утечки по излучению, питанию или акустике являются типичными каналами утечки по времени. Защитные механизмы основаны на экранировании, фильтрах и зашумлении.

Угрозы Целостности

Нарушения целостности информации — это незаконные уничтожение или модификация информации.

Традиционно защита целостности относится к категории организационных мер. Основным источником угроз целостности являются пожары и стихийные бедствия. К уничтожению и модификации могут привести также случайные и преднамеренные критические ситуации в системе, вирусы, "троянские кони" и т.д.

Язык описания угроз целостности в целом аналогичен языку угроз секретности. Однако в данном случаев место каналов утечки удобнее говорить о каналах воздействия на целостность (или о каналах разрушающего воздействия). По сути они аналогичны каналам утечки, если заменить доступ (r) доступом (w).

Пример 1. Канал несанкционированной модификации, использующий "троянского коня", изображен на следующей схеме:

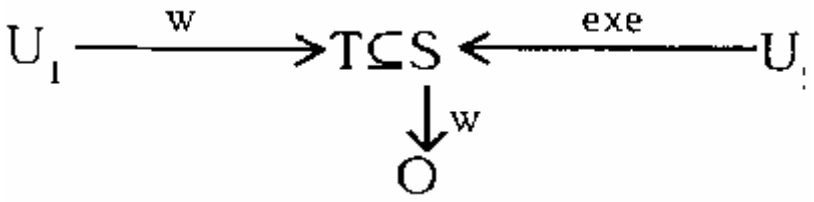


Рисунок — Канал несанкционированной модификации, использующий "троянского коня"

где U_1 — злоумышленник; U_2 – пользователь; O — объект с ценной информацией; S — процесс (программа), являющаяся общим ресурсом U_1 и U_2.

Пользователь U_1, пользуясь правом w, модифицировал общий ресурс S, встроив в него скрытую программу T, модифицирующую информацию в O при запуске ее пользователем U_2.

Исследованием схем примера 1 занимается теория распространения вирусов.

Основой защиты целостности является своевременное регулярное копирование ценной информации.

Другой класс механизмов защиты целостности основан на идее помехозащищенного кодирования информации (введение избыточности в информацию) и составляет основу контроля целостности. Он основан на аутентификации, т.е. подтверждении подлинности, целостности информации. Подтверждение подлинности охраняет целостность интерфейса, а использование кодов аутентификации позволяют контролировать целостность файлов и сообщений. Введение избыточности в языки и формальное задание спецификации позволяет контролировать целостность программ.

Наконец, к механизмам контроля и защиты целостности информации следует отнести создание системной избыточности. В военной практике такие меры называются: повышение "живучести" системы. Использование таких механизмов позволяет также решать задачи устойчивости к ошибкам и задачи защиты от нарушений доступности.

Модели общей оценки угроз информации

[Герасименко В.А., ч.1, гл.4–5]

Данные модели характеризуют меру угроз информации от всей совокупности или от отдельно взятых дестабилизирующих факторов (ДФ), в соотнесении с теми потерями, которые могут иметь место при реализации угроз.

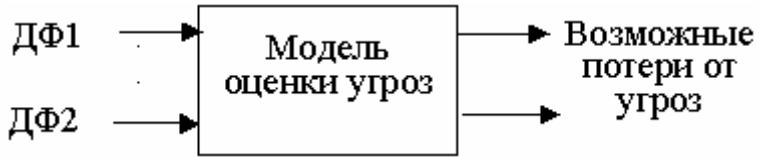


Рисунок — Соотнесение ДФ с потерями при реализации угроз

Исходная предпосылка при разработке моделей:

- с одной стороны, при нарушении защищенности информации наносится некоторый ущерб;
- обеспечение ЗИ сопряжено с расходованием средств.

Полная ожидаемая стоимость ЗИ равна сумме расходов на защиту и потерь от ее нарушения.

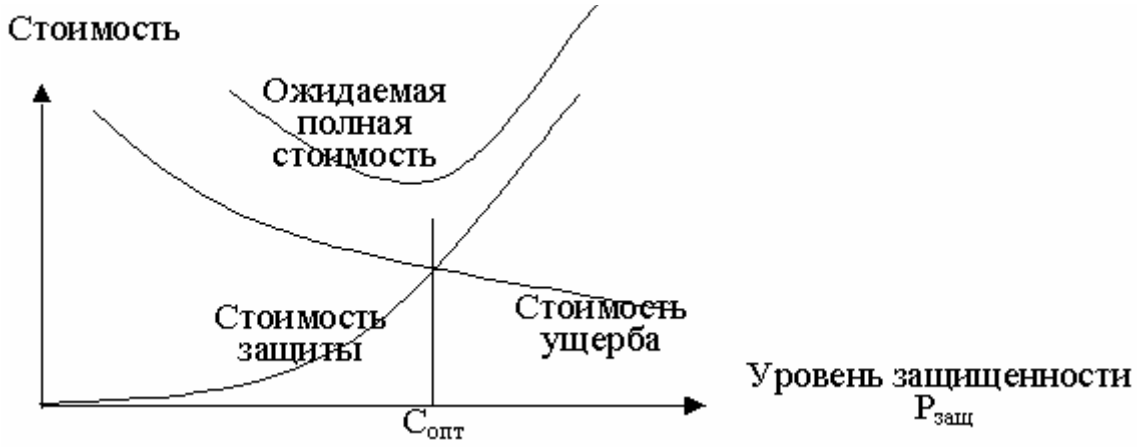


Рисунок — Соотношение между уровнем защищенности истоимостьюзащиты

Следовательно, Оптимальное решение соответствует минимуму общей стоимости ЗИ

Но: трудно дать оценку потерь при нарушении статуса защищенности информации, содержащей государственную, военную или другую подобную тайну

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо знать:

- полный перечень угроз информации;
- потенциальную опасность для информации каждой из угроз;
- размеры затрат, необходимые для нейтрализации каждой из угроз.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту обычно состоит в том, что этот уровень должен быть равным уровню ожидаемых потерь при нарушении защищенности ($C_{защ}=C_{ущерба}$) , то достаточно определить только уровень ожидаемых потерь ($R=C_{ущерба}$).

Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь R_i от i–й угрозы информации:

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

где: Si — коэффициент, характеризующий возможную частоту возникновения i–й угрозы;

V_i — коэффициент, характеризующий значение возможного ущерба при ее возникновении.

(Значения коэффициентов S_i и V_i смотри ниже)

Суммарная стоимость потерь:

$$R = \sum_{i} R_i$$

Но: данный подход является весьма приближенным и условным.

[Герасименко В.А., ч.1, с.136]

Значения коэффициента S_i:

Ожидаемая (возможная) частота появления угрозы	Предлагаемое значение S_i
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 100 лет	3
1 раз в год	4
1 раз в месяц (≈10 раз в год)	5
2 раза в неделю (100 раз в год)	6
3 раза в день (1000 раз в год)	7

Возможные значения коэффициента V_i:

Значение возможного ущерба при проявлении угрозы (долл.)	Предлагаемое значение V_i
1	0
10	1
100	2
1000	3
10000	4
100000	5
1000000	6
10000000	7

Методика вычисления показателей защищённости информации.

Допущения:

Характер и уровень воздействия одних угроз (ДФ) не зависит от характера и уровня воздействий других;

Средства защиты также независимы друг от друга.

Тогда вероятность защищённости (отсутствия нарушений) объекта O_i на оцениваемом интервале времени ΔT равна:

$$P_i = 1 - \sum_k (1 - P_{ik})\alpha_k \text{, где : } \alpha_k = \frac{\Delta t_k}{\Delta T};$$

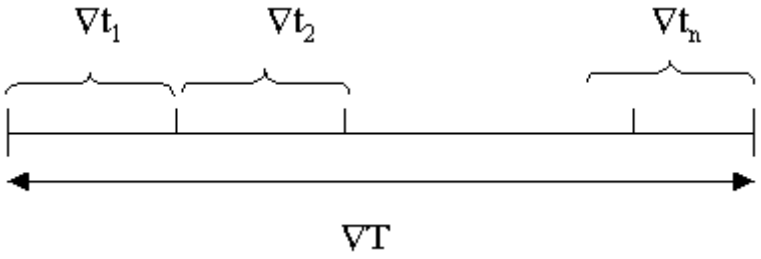


Рисунок — Интервалы нахождения АСОД в своих состояниях

Δt_k — интервал нахождения АСОД в К — м состоянии;

P_{ik} — вероятность защищённости O_i для К — го состояния АСОД;

$(1 - P_{ik})$ — вероятность уязвимости O_i для К — го состояния АСОД.

В свою очередь:

$P_{ik} = P'_{ik} \cdot P''_{ik}$, где: $P'_{ik} = \prod_{j' \in J'} (1 - P^*_{ij'k})$ — вероятность защищённости информации на i — м объекте в К-м его состоянии по отношению к тем ДФ, для противодействия которым не предусмотрены средства защиты;

J' — множество номеров тех ДФ, против которых отсутствуют средства защиты;

$P^*_{ij'k}$ — вероятность уязвимости O_i в К — м его состоянии для угрозы (ДФ) $У_{j1}$.

$P''_{ik} = \prod_{\eta \in H} \prod_{j'' \in J''} (1 - P^*_{ij''\eta k})$ — вероятность защищённости информации на O_i в К–м его состоянии (режиме работы) по отношению к тем $Y_{j''}$, для противодействия которым в системе защиты предусмотрены средства $СЗ_\eta$.

J'' — множество номеров тех ДФ, для противодействия которым в системе предусмотрены средства $СЗ_\eta$;

$P^*_{ij'k}$ — вероятность уязвимости O_i по отношению к $Y_{j''}$ в К-м состоянии объекта при наличии средств защиты $СЗ_\eta$.

В общем случае, для группы объектов(при условии их независимости) вероятность защищённости информации на оцениваемом интервале времени ΔT:

$$P = \prod_{i \in I} P_i .$$

Особенности использования общей модели процесса ЗИ:

- Данная модель предназначена для использования квалифицированными специалистами способнми критически оценить степень адекватности получаемых решений;
- Модель должна использоваться не просто для получения конкретных значений показателей защищённости (уязвимости), а для оценки поведения этих значений при варьировании исходных данных в возможных диапазонах их изменений;
- Эффективное использование модели во многом зависит от объективности (обоснованности) исходных данных, подавляющее большинство которых обладает высокой степенью неопределённости.

Анализ опасностей

ПРИМЕР (см.:[Д. Стенг, С. Мун], с. 44–45)

В отчете GAO (General Accounting Office) приведен анализ состояния дел на 1992 год в DEA (Drug Enforcement Administration) подразделении Министерства Юстиций США, занимающимся борьбой с наркотиками.

По данным GAO, оказалось, что DEA не знает, где находится ее грифованная информация! Когда Министерство Юстиций потребовало представить перечень компьютеров, на которых обрабатывается информация, связанная с национальной безопасностью, DEA оказалась неспособной выполнить это распоряжение.

Ряд других нерешенных проблем в DEA, обнаруженных GAO:

- Для обработки грифованных данных применялась незащищенная и неутвержденная система автоматизации делопроизводства. Любой сотрудник DEA имел доступ к любой информации на любой работающей станции;
- в DEA не анализировались опасности для системы;
- работающие станции DEA находились в открытых незащищенных помещениях;
- в DEA для обработки информации, связанной с национальной безопасностью, использовались работающие станции, не прошедшие проверку TEMPTEST (на устойчивость к внешним воздействиям);
- в DEA использовались открытые каналы связи;
- в DEA не потрудились за 5 лет изменить системные пароли, поставленные производителями;
- управление доступом к грифованным материалам было неадекватным их важности;
- лица, не имеющие допуска к материалам, представляющим угрозу для национальной безопасности, например, уборщики, имели свободный доступ без сопровождающих в зоны особого режима;
- работающие компьютеры оставлялись без присмотра;
- сейфы оставлялись открытыми и без присмотра;
- пропускные устройства на электронных карточках в рабочее время отключались, а двери оставались открытыми;

- украденные или потерянные электронные карточки не изымались из памяти;
- замки на дверях не менялись в течение 5 лет, несмотря на то, что за это время было потеряно (или украдено) 17 ключей, в том числе ключи от компьютерных залов; и так далее.

13 Компьютерные преступления

Компьютерное преступление — предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники.

В качестве предмета или орудия преступления при этом может выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

Наиболее распространенные мотивы совершения компьютерных преступлений:

корыстные соображения — 66 %;

политические цели (шпионаж; дезорганизация валютной системы страны; преступления направленные на подрыв рыночных отношений) — 17 %;

исследовательский интерес — 7 %;

хулиганские побуждения и озорство — 5%;

месть — 5%.

В Уголовном кодексе РФ (принят Государственной Думой 24 мая 1996 г. и введен в действие с 1 января 1997 г.) предусмотрены уголовные наказания за компьютерные преступления:

Как преступления квалифицируются: неправомерный доступ к компьютерной информации (штраф от 200 до 500 минимальных размеров заработной платы,..., лишение свободы на срок до трех лет); использование и распространение вредоносных программ для ЭВМ (лишение свободы на срок до трех лет со штрафом от 200 до 500 минимальных размеров заработной платы,...,лишение свободы на срок от трех до семи лет); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (лишение свободы на срок до четырех лет).

Литература:

1. Вехов В.Б. Компьютерные преступления: Способы совершения. Методики расследования М.: Право и Закон, 1996.- 182 с.

2. Рачук Т.В. Уголовные наказания за информационные преступления //Защита информации. Конфидент, июль-август, 1996, № 4(10).- с. 25-27.

По данным Ю.М. Батурина, выделяются *три группы потерпевших сторон* от компьютерных преступлений:

собственники компьютерных систем — 79 %;

клиенты, пользующиеся их услугами — 13%;

третьи лица — 8%.

По оценкам ведущих зарубежных и отечественных специалистов, 90 % компьютерных преступлений остаются необнаруженными или о них не сообщается в правоохранительные органы по различным причинам, а из оставшихся 10 % обнаруживаемых и зарегистрированных преступлений раскрывается только каждое десятое.

[PC Week/RE, 8 июля 1997, #26, с. 44] = [А. Воробьев, начальник исследовательско-аналитической группы ассоциации "Конфидент"]:

"На территории России только за 1995 г. выявлено 185 случаев хищения с использованием элементарных средств доступа, ущерб от которых составил 250 млрд. рублей, было привлечено к ответственности более 60 человек. Ежегодный рост числа компьютерных преступлений составляет около 20 %.

14 Цели и особенности моделирования процессов и систем защиты информации

Особенности проблем ЗИ:

- сложность систем обработки информации, их неоднородный состав, большое количество элементов и подсистем;
- неопределенность, разнообразие режимов и условий функционирования АСОД (ИУС);
- ограниченность ресурсов в условиях наличия различных вариантов построения систем ЗИ;
- высокая "цена ошибки" (возможность потерь) при принятии решений по обеспечению ЗИ.
- необходимость использования адекватных моделей процессов и систем ЗИ.

Процесс моделирования СЗИ — может быть представлен в общем виде двух составляющих:

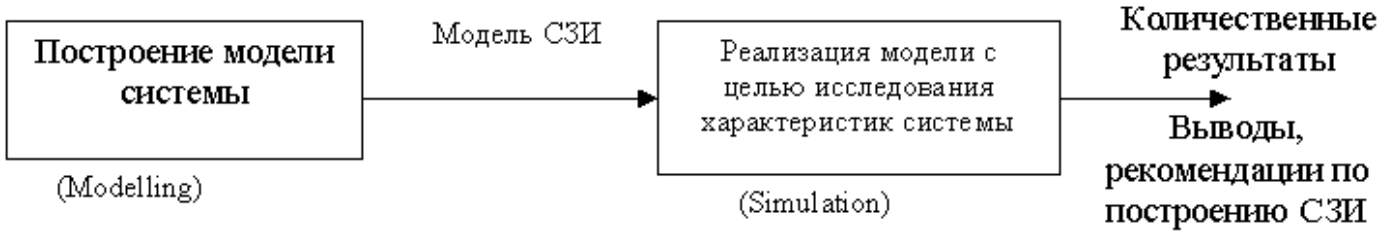


Рисунок — Процесс моделирования СЗИ

Классификация моделей процессов и систем ЗИ:

В основу классификации моделей закладываются два критерия:

характер системы, т.е. характер взаимосвязей между значениями моделируемых характеристик системы и параметрами системы и внешней среды;

масштаб моделирования, т.е. уровень определяемых на модели характеристик.

- аналитические расчеты (точные показатели)
- статистические эксперименты (усредненные характеристики). Метод Монте-Карло

Литература:

1. [Герасименко В.А. ЗИ в АСОД, ч.1, М.: 1994]- с.70-75;

2. [Хоффман Л.Дж. Современные методы ЗИ.- М.: Мир, 1980]:

Приводится следующий вопрос: "Почему пытаются моделировать системы?" и ответ на него (цитата): "Практические ситуации имеют тенденцию к усложнению, а модели выделяют главное и концентрируют внимание на тех проблемах, которые необходимо решить в первую очередь".

Цели моделирования:

Оценка характеристик (показатель качества эффективности) системы;

- Оптимизация характеристик системы;
- Оценка чувствительности характеристик системы к суммированию тех или иных параметров (фактов);
- Прогноз поведения системы в тех или иных условиях.

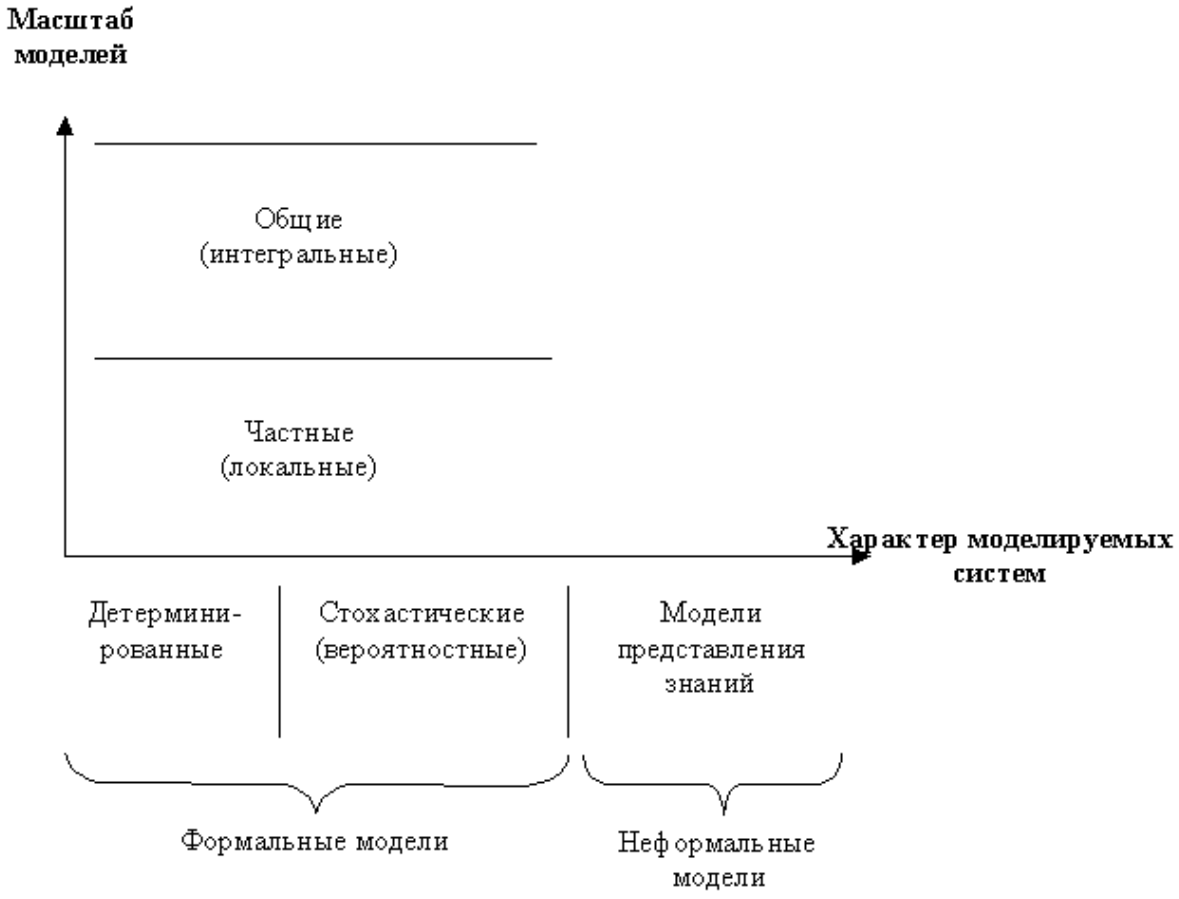


Рисунок — Виды моделей Рисунок — Множество отношений «объект–угроза»

Общие модели процессов и систем ЗИ:

Модель анализа показателей защищенности многоуровневой (многозонной) СЗИ;

Модель анализа риска СЗИ (ресурсная модель);

Функциональная модель СЗИ;

Модель анализа защищенности СЗИ с учетом эффективности перекрытий (барьеров) — (модель Клемента-Хофмана)

Модель анализа риска(возможных потерь) в системе ЗИ.

(Бабиков А.Ю. Бакиров А.А. Васильев В.И.)

При отсутствии барьеров на пути угроз:

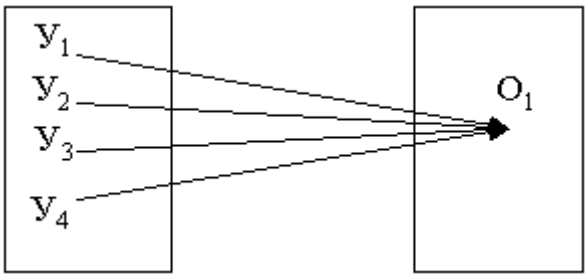


Рисунок — Воздействие угроз при отсутствии баръеров

Средние потери(ушерб): $R = \sum_{i=1}^{n} p(Y_i) r_i$

$p(Y_i)$ — вероятность появления угрозы Y_i;

r_i — средние потери от действия Y_i

В системе ЗИ с полным перекрытием:

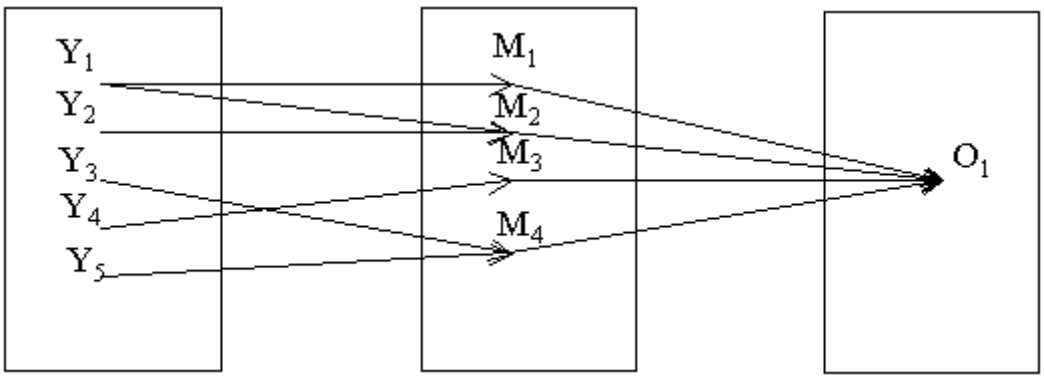


Рисунок — Воздействие угроз при наличии СЗИ

Средние потери (ущерб) от НСД при наличии СЗИ:

$$\tilde{R} = \sum_{i=1}^{n} [p(Y_i) \cdot p(Y_i'/Y_i) r_i + c_i]$$

$p(Y_i)$ — вероятность появления угрозы Y_i;

$p(Y_i'/Y_i)$ — условная вероятность прохождения i-й угрозы через M_i ; характеризует эффективность средства ЗИ M_i (уязвимость M_i);

r_i — средние потери от действия Y_i;

c_i — стоимость средств ЗИ (M_i);

Эффект(экономия) от использования средств ЗИ:

$$\Delta R = R - \tilde{R} = \sum_{i=1}^{n} \{p(Y_i) \cdot r_i \cdot [1 - p(Y_i'/Y_i)] - c_i\} = \sum_{i=1}^{n} [p_i \cdot r_i \cdot (1 - e^{-\gamma_i c_i}) - c_i]$$

Если представить $\tilde{R} = \sum_{i=1}^{n} \tilde{R}_i$, где $\tilde{R}$ — средние потери в СЗИ от действия Y_i, то :

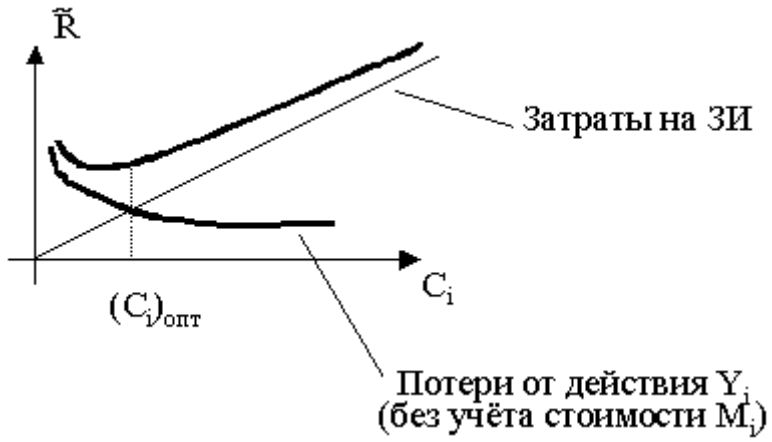


Рисунок — Соотношение затрат на ЗТ и Потерь от реализации угроз

Вывод: затраты на средства ЗИ должны быть оптимальными.

2 задачи оптимизации СЗИ:

а) Задача оптимизации выделения ресурсов ($\nabla R \rightarrow \max$); ($\tilde{R} \rightarrow \min$)

$$\frac{\partial(\Delta\Delta R}{\partial C_i} = p_i r_i \gamma_i e^{-\gamma_i c_i} - 1 = 0;\ e^{-\gamma_i c_i} = \frac{1}{p_i r_i \gamma_i};$$

$$\Rightarrow (C_i)_{опт} = \frac{1}{\gamma_i} \ln(p_i r_i \gamma_i),\ (I=1, 2, \ldots, n).$$

б) задача оптимизации распределения ресурсов ($\nabla R \rightarrow \max$); ($\tilde{R} \rightarrow \min$), при $\sum_{i=1}^{n} C_i = C_0 = \text{const}$.

Задача условной оптимизации — метод неопределённых множителей Лагранжа:

$$F=\Delta R+\alpha\cdot(\sum_{i=1}^{n} C_i - C_0)\rightarrow \max .$$

α — неопределённый множитель.

$$\frac{\partial F}{\partial C_i}=p_i r_i \gamma_i e^{-\gamma_i c_i} - 1+\alpha=0;\ C_i=\frac{1}{\gamma_i}\ln(\frac{p_i r_i \gamma_i}{1-\alpha})=\frac{1}{\gamma_i}\ln(p_i r_i \gamma_i)-\frac{1}{\gamma_i}\ln(1-\alpha);$$

Поскольку: $\sum_{i=1}^{n} C_i = C_0$, то $\sum_{i=1}^{n} \frac{1}{\gamma_i}\ln(p_i r_i \gamma_i) - \sum_{i=1}^{n} \frac{1}{\gamma_i}\ln(1-\alpha)=C_0$

Первую сумму в левой части обозначим через A, вторую через B.

$\ln(1-\alpha)=\frac{(A-C_0)}{B}$ — превышение оптимальных затрат на ЗИ по сравнению с выделяемой суммой

Если C_0=A, то $(C_i)_{опт}$ совпадает с предыдущим решением, поскольку ln(1-α)=0.

$$(C_i)_{опт}=\frac{1}{\gamma_i}\ln(p_i r_i \gamma_i)-\frac{1}{\gamma_i}\frac{(A-C_0)}{B}.$$

15 Модель наиболее опасного поведения потенциального нарушителя (злоумышленника)

Может меняться в зависимости о принципов построения АСОД, вида и ценности обрабатываемой в них информации:

- для военных систем — уровень разведчика–профессионала;
- для коммерческих систем — уровень квалифицированного пользователя;
- для медицинских систем — требуется защита от безответственности пользователей;
- и т. д.

Вводятся 4 класса безопасности:

1–й класс — для защиты жизненно важной информации утечка, разрушение или модификация которой может привести к большим потерям для пользователя. Прочность защиты должна быть рассчитана на нарушителя–профессионала.

2–й класс — для защиты важной информации при работе нескольких пользователей, имеющих доступ к разным массивам данных или формирующих свои файлы, недоступные другим пользователям. Прочность защиты должна быть рассчитана на нарушителя высокой квалификации, но не взломщика-профессионала.

3–йкласс — для защиты относительно ценной информации, постоянный несанкционированный доступ к которой может привести к утечке. Прочность защиты должна быть рассчитана на относительно квалифицированного нарушителя–профессионала

4–й класс — для защиты прочей информации, не представляющей интереса для серьезных нарушителей, однако требующей учета и защиты от преднамеренного НСД .

Реализация перечисленных уровней безопасности — должна обеспечиваться набором соответствующих средств защиты, перекрывающих определенное количество возможных каналов НСД в соответствии с ожидаемым классом потенциальных нарушителей.

Уровень безопасности защиты внутри класса обеспечивается количественной оценкой прочности отдельных средств защиты и оценкой прочности контура защиты от преднамеренного НСД.

Пример постановки и решения задачи:

Исходные данные:

- вероятность угрозы (=$P_{угр}$), т. е. действий со стороны злоумышленника;
- $P_{з1}$, $P_{з2}$, $P_{з3}$ — вероятность правильного функционирования зон защиты 1:3;

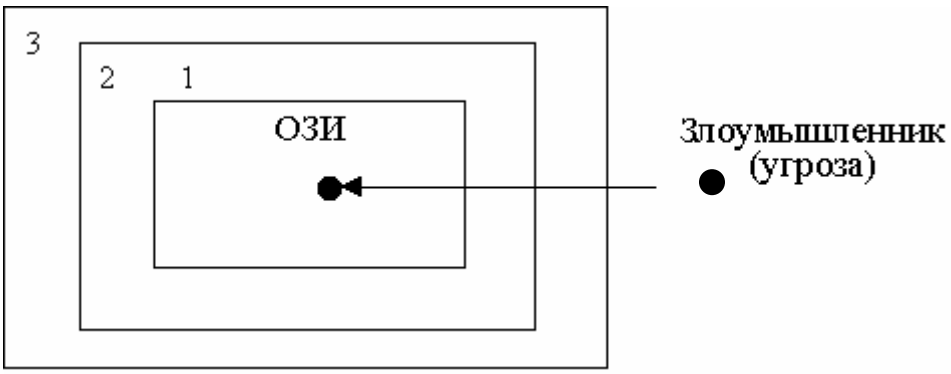


Рисунок — Зоны защиты

Тогда защищенность информации:

$$P_{ЗИ} = P_{УГР} /(1 - P_{З1})(1 - P_{З2})(1 - P_{З3});$$

Уязвимость информации:

$$P^{*}_{УЯЗВ} = 1 - P_{ЗИ}.$$

Основные задачи злоумышленника в информационной борьбе:

- Локализация объектов автоматизации управления и средств связи;
- Внедрение средств, способных осуществить блокировку или искажение как управляющих воздействий, так и информации обратной связи.

Таким образом, объектами информационного нападения (ИН) можно считать:

- средства управления;
- средства сбора, передачи и обработки информации;
- средства и системы защиты информации
- должностные лица органов управления и связи.

К числу задач злоумышленника могут быть отнесены:

- полное разрушение или искажение информации в различных фазах цикла управления;

- создание условий для утечки и нарушения целостности информации;
- перехват информации и ее хищение;
- вывод из строя должностных лиц органов управления.

Анализ задач ИН позволяет выделить следующие возможны способы его осуществления:

- изменение условий распространения электромагнитных, акустических и других волн;
- воздействие на средства разведки и связи (помехи, внедрение ложной информации);
- нарушение энергообеспечения;
- воздействия на средства автоматизации управления;
- хищение носителей и стирание информации;
- создание искажений в ВС, алгоритмах обработки информации;
- снижение производительности ИВС;
- блокирование информации в ЛВС;
- дезорганизация работы сетей запросами информации;
- внедрение программных закладок в ПО ИВС.

Модели защиты информации от несанкционированного доступа

[Мельников В.В. Защита информации в компьютерных системах — М.; 1997, §16.3]

Модель действий (ожидаемого поведения) злоумышленника/ нарушителя:

Поскольку время и место появления преднамеренного НСД предсказать невозможно, рассматривается наиболее опасная ситуация: ОБСТОЯТЕЛЬСТВА (УСЛОВИЯ):

Злоумышленник (нарушитель) может появиться в любое время и в любом месте периметра АСОД;

Квалификация и осведомленность нарушителя может быть на уровне разработчика данной системы;

Постоянно хранимая информация о принципах работы системы, включая секретную, нарушителю известна;

Для достижения своей цели нарушитель выберет наиболее слабое звено в защите;

Нарушителем может быть не только постороннее лицо, но и законный пользователь системы;

Нарушитель действует один.

Отсюда вытекают основные принципы построения защиты:

Необходимо строить вокруг объекта защиты постоянно действующие 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 наличие 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;

Отсюда также следует, что расчет прочности защиты должен производится для двух возможных исходных позиций нарушителя: за пределами контролируемой территории и внутри ее.

Защита от группы нарушителей (группа людей, выполняющих одну задачу под общим руководством) — отдельная проблема.

Нарушение — попытка НСД к любой части подлежащей защите информации, хранимой, обрабатываемой и передаваемой в АСУ.

Модели систем разграничения доступа к ресурсам АСОД

АСОД является системой множественного доступа, то есть к одним и тем же ее ресурсам (техническим средствам, программам, массивам данных) имеет законное право обращаться некоторое число пользователей (абонентов). Если какие-либо из указанных ресурсов объявляются защищенными, то доступ к ним должен осуществляться лишь при предъявлении некоторых полномочий. Система разграничения доступа и является тем механизмом, который регулирует такой доступ. Требования к этому механизму на содержательном уровне состоят в том, что, с одной стороны, не должен быть разрешен доступ пользователям, не имеющим на это полномочий, а с другой — не должно быть отказано в доступе пользователям, имеющим соответствующие полномочия.

Примером системы разграничения доступа является система АДЕПТ-50 (разрешена Корпорацией системного развития). В основе модели функционирования этой системы используются объекты (структурные элементы) следующих типов:

U — пользователь;

j — здание;

t — терминал;

f — файл.

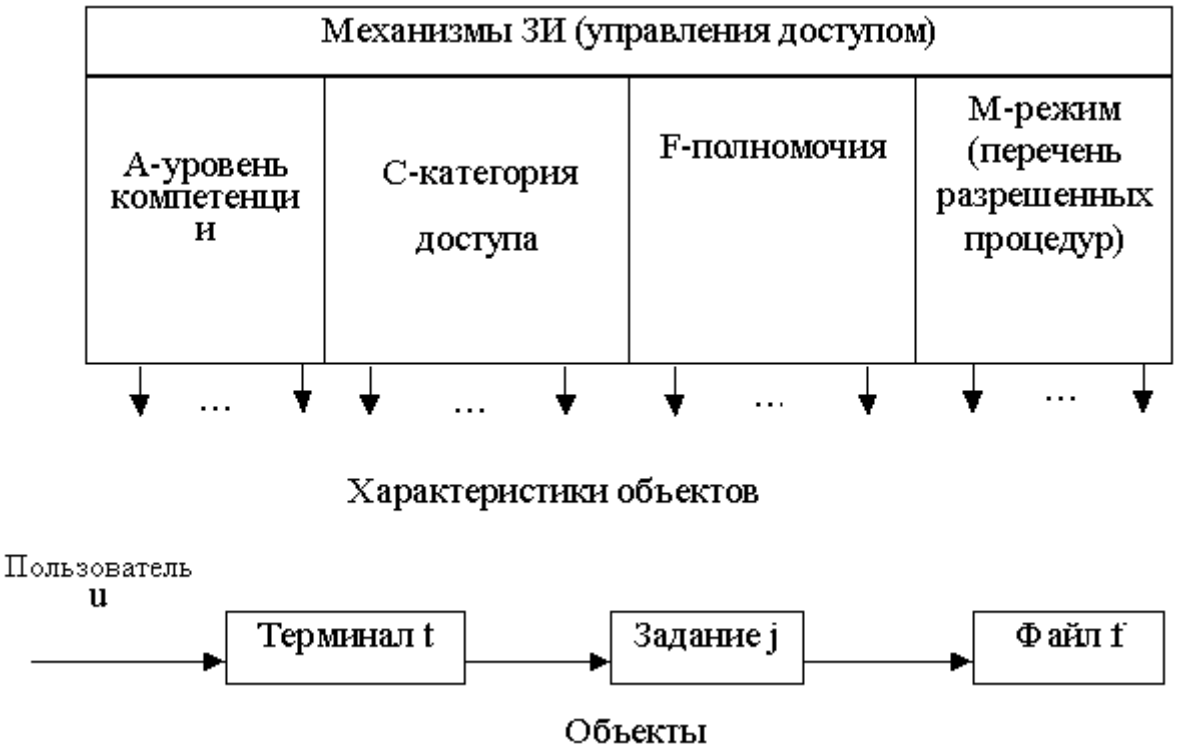


Рисунок — Объекты модели функционирования системы АДЕПТ — 50

Объект каждого типа полностью описывается заданием четырех характеристик (параметров безопасности):

A — уровень компетенции, выраженный наибольшим грифом секретности данных, допустимых для данного объекта;

C — категория доступа, выраженная набором рубрик, к данным по которым разрешен доступ к объекту;

F — полномочия, выраженные списком пользователей, имеющих доступ к объекту;

M — режим, выраженный перечнем процедур, разрешенных для соответствующего объекта.

A, C, F, M — образуют кортеж.

На основе такого формального описания системы можно сформулировать систему формальных правил регулирования доступа:

- пользователь "u" получает доступ к заданию "j" только тогда, когда u принадлежит U, где U — множество всех пользователей, зарегистрированных в системе;
- пользователь "u" получает доступ к терминалу "t" только тогда, когда u принадлежит F(t);

- пользователь "u" получает доступ к файлу "f" только тогда, когда u принадлежит F(t), A(u) ≥A(f), C(u) ≥C(f), M(u) ≥M(f);
- с терминала "t" может быть осуществлен доступ к файлу "f" только тогда, когда:

F(t) ≥F(f), A(t) ≥C(f), C(t) ≥C(f), M(t) ≥M(f).

К подобному типу относятся пятимерная модель безопасности, в которой для описания процесса доступа к данным используется 5 множеств: U — список зарегистрированных пользователей, R — набор имеющихся в системе ресурсов, S — множество возможных состояний ресурсов, A — перечень возможных полномочий пользователей.

Область безопасности: D=U*A*R*S*E.

Любой запрос на доступ может быть описан четырехмерным кортежем: g=(u,r,s,e), где u принадлежит U, r принадлежит R, s принадлежит S, e принадлежит E. Запрос получает право на доступ только тогда, когда он попадает в соответствующую подобласть области безопасности.

Литература:

Герасименко В.А., ЗИ в АСОД, ч. I, §4.5 (с.141-146).

Хоффман Л.Дж. Современные методы ЗИ.- М.: Мир, 1980.

Компетенция (A) — скаляр — элемент из множества иерархически упорядоченных положений о безопасности таких как: НЕСЕКРЕТНО, КОНФИДЕНЦИАЛЬНО, СЕКРЕТНО, СОВЕРШЕННО СЕКРЕТНО.

Категория (C) — дискретный набор рубрик. Категории не зависят от уровня компетенции. Примеры рубрик: {ОГРАНИЧЕНО, ТАЙНО, ТОЛЬКО ДЛЯ ПРОСМОТРА, ЯДЕРНЫЙ, ПОЛИТИЧЕСКИЙ}.

Полномочия (F) — группа пользователей, имеющих право на доступ к определенному объекту.

Режим (M) — набор видов доступа, разрешенных к определенному объекту или осуществляемых объектом. Например: ЧИТАТЬ ДАННЫЕ, ЗАПИСАТЬ ДАННЫЕ, ИСПОЛНИТЬ ПРОГРАММУ и т.д.

16 Определение базовых показателей уязвимости (защищенности) информации:

Под базовым показателем уязвимости (защищенности) информации понимается такой, который характеризует данное свойство информации в одном структурном комплекте АСОД (=объекте защиты) относительно одного дестабилизирующего фактора и (для факторов, связанных с злоумышленными действиями людей) относительно одного нарушителя одной категории.

Введем следующие обозначения (индексы):

i — текущий номер (идентификатор) для объекта защиты O_i;

j — то же, для дестабилизирующего фактора Y_i;

= j–го канала утечки информации;

k — то же, для категории потенциальных нарушителей;

l — то же, для зоны злоумышленных действий.

Тогда — вероятность несанкционированного получения информации нарушителем k–й категории по j–му каналу утечки информации в l–й зоне i–го объекта защиты:

$$P^{*}_{ijkl} = P^{(ддост.\ l)}_{ikl} * P^{(ккан}_{ijl} * P^{(ддост.\ j)}_{ijkl} * P^{(иинф}_{ijl}$$

где:

$P^{(ддостl)}_{ikl}$ — вероятность доступа нарушителя k–й категории в l–ую зону i–го объекта;

$P^{(ккан}_{ijl}$ — вероятность наличия (проявления) j–го канала утечки информации в l–ой зоне I–го объекта;

$P^{(ддостj)}_{ijkl}$ — вероятность доступа нарушителя k–й категории к j–му каналу утечки информации в l–ой зоне i–го объекта при условии доступа нарушителя в зону;

$P^{(ииф)}_{ijl}$ — вероятность наличия защищаемой информации в j–ом канале утечки информации в l–ой зоне i–го объекта в момент доступа туда нарушителя.

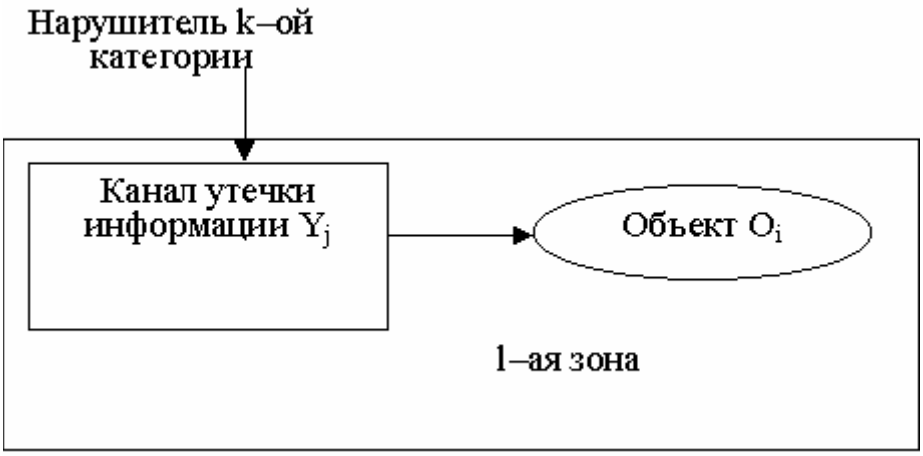


Рисунок — Доступ нарушителя к защищаемому объекту

Окончательно, базовый показатель уязвимости информации, который определяется в данном случае как вероятность несанкционированного получения информации нарушителем k–й категории по j–му каналу утечки информации i–го объекта защиты (в любой, т. е. хотя бы в одной из существующих 5 зон возможных злоумышленных действий), равен:

$$P^{*(\text{ббаз}}_{ijk} = 1 - \prod_{l=1}^{5}[1 - P^{*}_{ijkl}] = 1 - \prod_{l=1}^{5}[1 - P^{(\text{ддост}1)}_{ikl} * P^{(\text{ккан}}_{ijl} * P^{(\text{ддост}j)}_{ijkl} P^{(\text{иинф}}_{ijl}]$$

соответственно базовый показатель защищенности информации (с точки зрения ее несанкционированного получения) находится как:

$$P^{(\text{ббаз}}_{ijk} = 1 - P^{*(\text{ббаз}}_{ijk} = \prod_{l=1}^{5}[1 - P^{*}_{ijkl}]$$

Определение обобщенных показателей уязвимости:

Базовые показатели уязвимости информации имеют ограниченное практическое применение. Часто необходимо знать значения показателей, обобщенных по какому–либо одному индексу (i, j или k) или по их комбинации, или же характеризующие какое–либо экстремальное состояние защищенности.

[Герасименко В.А, ч.I, §5.11]

Значение частично обобщенных показателей могут быть определены следующим образом. Пусть $\{k\}$ — интересующее нас подмножество из полного множества потенциально возможных нарушителей, $\{k\} \subset K$. Тогда вероятность

нарушения защищённости информации указанным подмножеством нарушителей по j–му фактору в i–ом компоненте АСОД определяется как:

$$P^{*}_{ij\{k\}} = 1 - \prod_{k\in\{k\}} [1 - P^{*(\text{ббаз})}_{ijk}].$$

Аналогично, если {j} есть подмножество представляющих интерес дестабилизирующих факторов, то уязвимость информации в i–ом компоненте (объекте) по данному подмножеству факторов относительно k–го нарушителя:

$$P^{*}_{ij\{k\}} = 1 - \prod_{j\in\{j\}} P^{(\text{ббаз})}_{ijk} = 1 - \prod_{j\in\{j\}} [1 - P^{*(\text{ббаз})}_{ijk}]$$

Наконец, если {i} есть подмножество интересующих нас объектов (структурных компонентов) АСОД, то уязвимость информации в них по j–му фактору k–го нарушителя:

$$P^{*}_{i\{jk\}} = 1 - \prod_{i\in\{i\}} P^{(\text{ббаз})}_{ijk} = 1 - \prod_{i\in\{i\}} [1 - P^{*(\text{ббаз})}_{ijk}]$$

Общий показатель уязвимости АСОД:

$$P^{*} = 1 - \prod_{\substack{i\in I \\ j\in J \\ k\in K}} [1 - P^{*(\text{ббаз}}_{ijk}] = 1 - \prod_{i\in I} \prod_{j\in J} \prod_{k\in K} [1 - P^{*(\text{ббаз}}_{ijk}].$$

Выражение для экстремальных показателей уязвимости определяется следующим образом (под экстремальными понимаются такие показатели, которые характеризуют наиболее неблагополучные условия защищенности информации):

а) самый уязвимый объект защиты ($\bar{i}$):

$$\bar{i} = i : P^{*}_{\bar{i}\{j\}\{k\}} = \max_{i\in\{i\}} P^{*}_{i\{j\}\{k\}},$$

где: $P^{*}_{i\{j\}\{k\}} = 1 - \prod_{j\in\{j\}} [1 - P^{*}_{ij\{k\}}] = 1 - \prod_{\substack{j\in\{j\} \\ k\in K}} [1 - P^{*(\text{ббаз}}_{ijk}];$

б) самый опасный дестабилизирующий фактор ($\bar{j}$):

$$\bar{j} = j : P^{*}_{\{i\}\bar{j}\{k\}} = \max_{j\in\{j\}} P^{*}_{\{i\}j\{k\}},$$

где: $P^{*}_{\{i\}j\{k\}} = 1 - \prod_{\substack{i\in\{i\} \\ k\in\{k\}}} [1 - P^{*(ббаз}_{ij\{k\}}]$;

в) самая опасная категория нарушителей ($\bar{k}$):

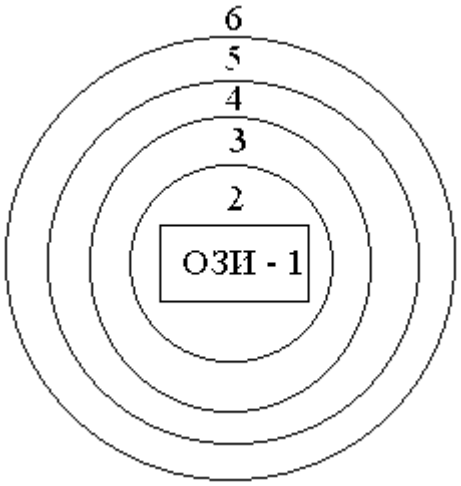
$\bar{k} = k : P^{*}_{\{i\}\{j\}\bar{k}} = \max_{k\in\{k\}} P^{*}_{\{i\}\{j\}k}$,

где: $P^{*}_{\{i\}\{j\}k} = 1 - \prod_{\substack{i\in\{i\} \\ j\in\{j\}}} [1 - P^{*(ббаз}_{ij\{k\}}]$.

В формулах (8) — (10) вместо $\{i\},\{j\},\{k\}$ рассматриваются полные множества соответствующих индексов:

$i \in I, j \in J, k \in K$.

Анализ показателей защиты (уязвимости) многоуровневой СЗИ



1 - Зона БД;
2 - Зона ресурсов;
3 - Зона помещений;
4 - Внутренняя контролируемая территория;
5 - Внешняя неконтролируемая территория.

Рисунок — Зоны многоуровневой СЗИ

Угрозы:

$$\lambda(t) = \frac{\Delta n * l * \Delta t}{N - n(t)}$$

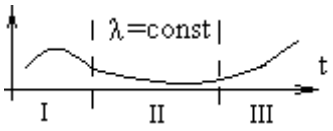
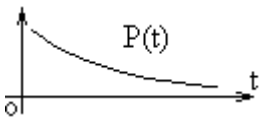


Рисунок — Простейший поток случайных событий

Вероятность отсутствия угроз:



$$P(t) = e^{-\lambda t}$$

Рисунок — Вероятность отсутствия угроз

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

$$e^{-\lambda t} \approx 1 - \lambda t; 1 - e^{-\lambda t} \approx \lambda t$$

Защищенность i — ой зоны защиты — вероятность правильного функционирования i — го рубежа ЗИ:

$$P(t) = P_{(1)}(t) \times P_{(2)}(t) \times P_{(3)}(t) ... = e^{-\lambda_1 t} \times e^{-\lambda_2 t} \times e^{-\lambda_3 t} ... = e^{-\sum_{i=1}^{k} \lambda_i t} = e^{-\lambda t}$$

Понятие наиболее слабого звена:

Рисунок — Понятие наиболее слабого звена

λ_1, λ_2, λ_3,… —— интенсивность угроз (опасностей) для i — го рубежа (зоны ЗИ).

$$P_{уязв}(t) = P_{наруш} \times (1 - у^{-\lambda_1 t}) \times ... \times (1 - e^{-\lambda_5 t})$$

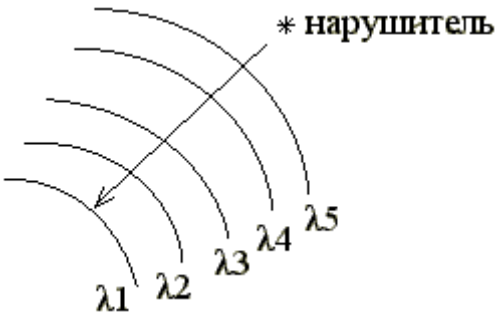


Рисунок — Проникновение нарушителя через рубежи безопасности

17 Функциональная модель СЗИ.

Функционально-структурный подход:

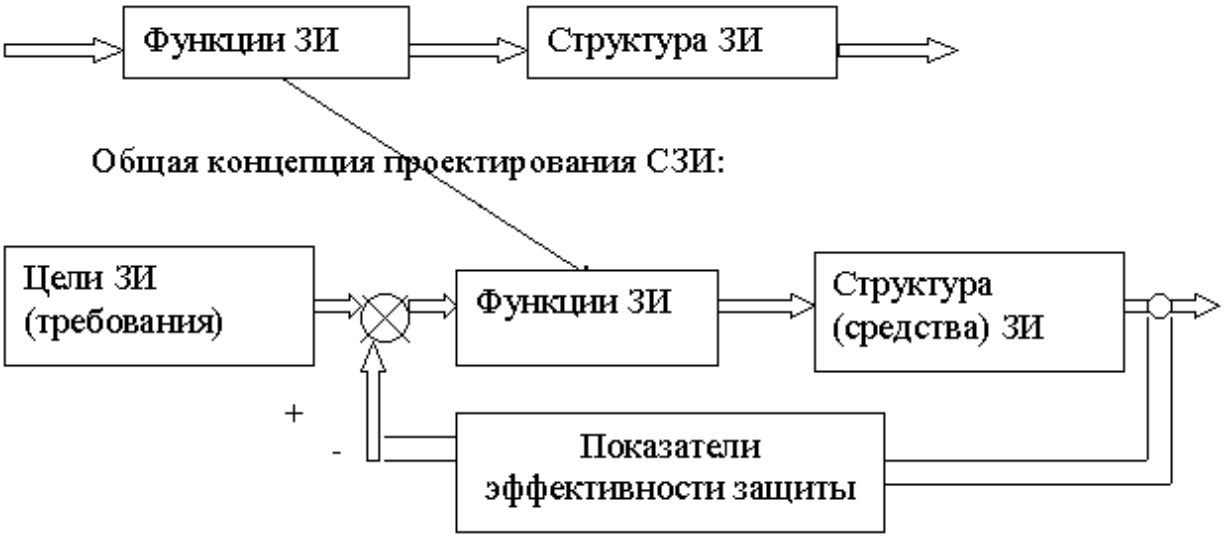


Рисунок — Общая концепция проектирования СЗИ

Что нужно делать?

Функция защиты — совокупность мероприятий проводимых с целью обеспечения условий для ЗИ.

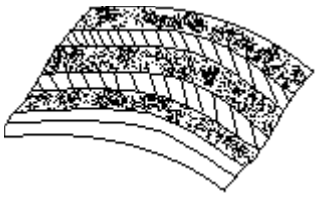


Рисунок — Фрагмент рубежа защиты

Полный набор функций при построении рубежа ЗИ:

1-6 — ЗИ обеспечена;

7,8 — ЗИ нарушена;

9,10 — ЗИ разрушена.

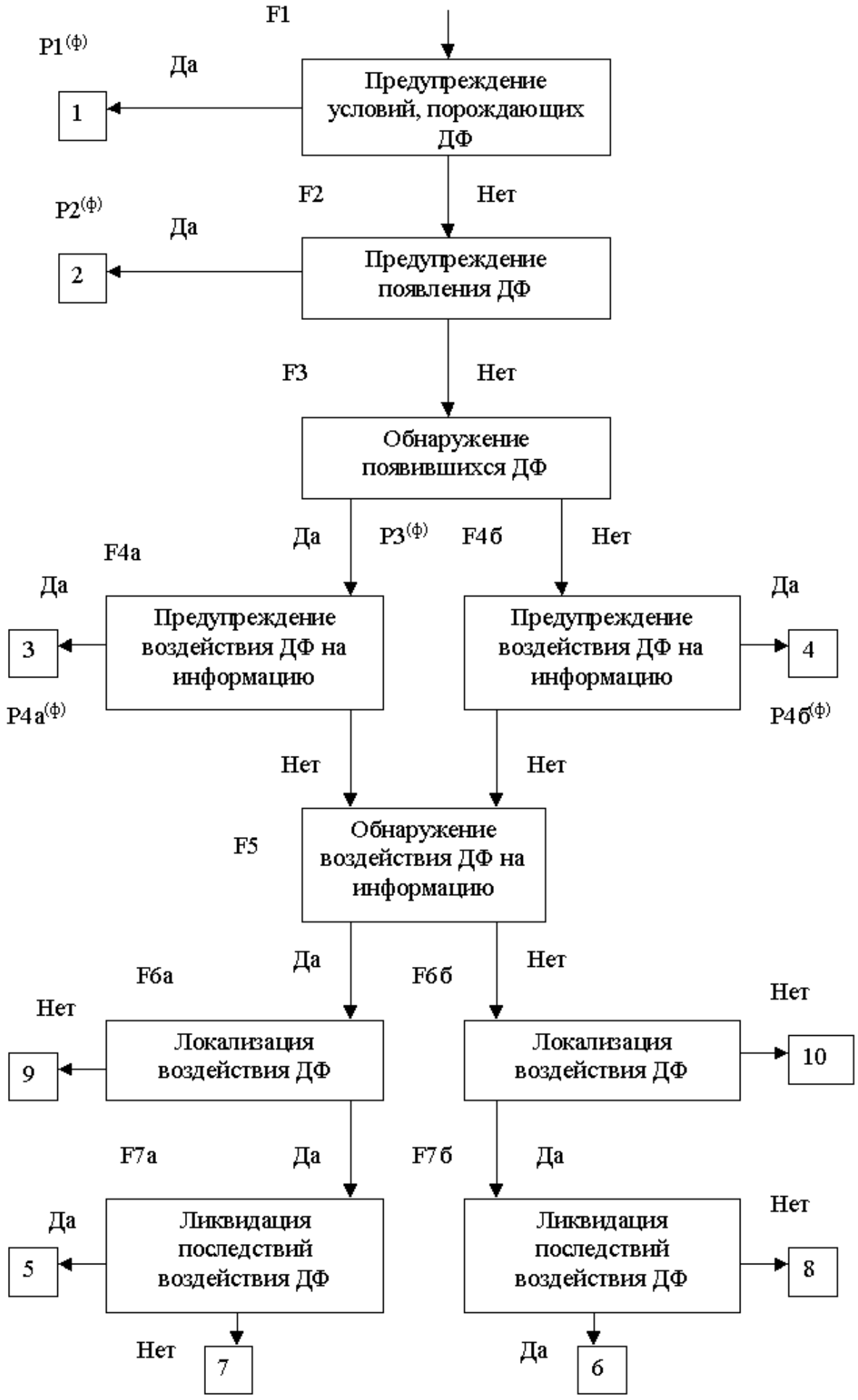


Рисунок — Полный набор функций при построении рубежа ЗИ

18 Модель процесса(системы) защиты информации с полным перекрытием.

(см. Хоффман Л. Дж. Современные методы ЗИ –М. : Мир, 1980).

Множество отношений «объект–угроза» можно представить в виде 2–х дольного графа, в котором ребро $<Y_i, O_j>$ существует только тогда, когда Y_i является средством получения доступа к объекту O_j:

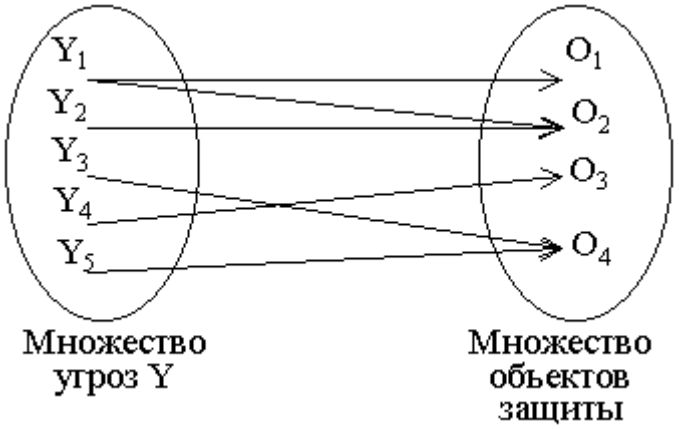


Рисунок — Множество отношений «объект–угроза»

Цель ЗИ состоит в том, чтобы “перекрыть” каждое ребро графа и воздвигнуть барьер для доступа по этому пути.

Основной характеристикой множества угроз является вероятность появления каждой из возможных угроз (злоумышленных действий).

Средства защиты информации $M=(M_1, M_2, \ldots)$ обеспечивают защиту ИВС (объектов $O_1, O_2, \ldots$) от указанных угроз. В идеале каждое средство $M_к$ должно устранять некоторое ребро $<Y_i, O_j>$ из указанного графа. В действительности, эти средства выполняют функцию «брандмауэра» («пожарной стенки», нем.), обеспечивая некоторую степень сопротивления попыткам проникновения. Это сопротивление — основная характеристика присущая всем элементам множества М.

Применение множества средств ЗИ (М) преобразует 2–х дольный граф в 3–х дольный:

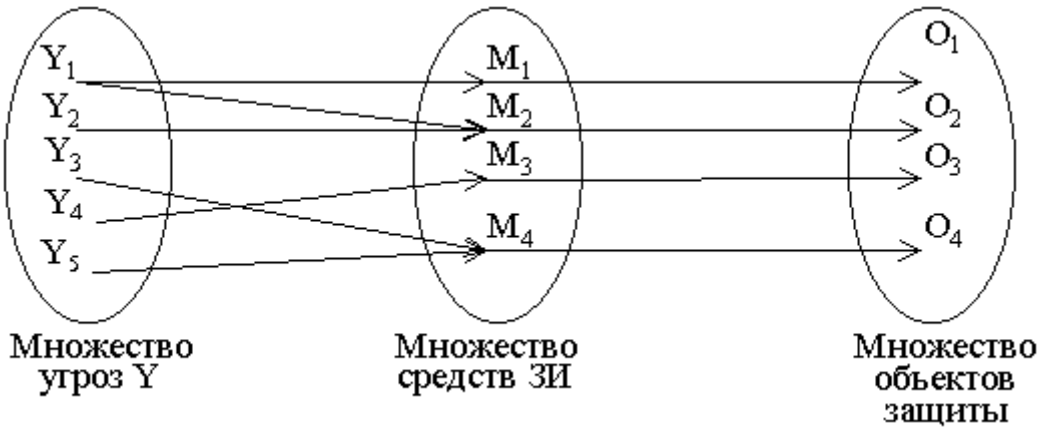


Рисунок — Множество отношений «объект–СЗИ–угроза»

В защищённой системе все рёбра представляются в виде $<Y_i, M_к>$ и $<M_к, O_j>$. При этом одно и то же средство ЗИ может перекрывать более одной угрозы и защищать более одного объекта. Т.о., процесс ЗИ можно представить с помощью 5–мерного кортежа: S={O, Y, M, V, B}, где: O — множество защищаемых объектов; Y — множество возможных угроз; M — множество средств ЗИ; V — множество уязвимых мест, сост. из упорядоченных пар $V_i=<Y_i, O_i>$, представляющих собой пути проникновения в систему; B — множество барьеров, множество упорядоченных троек $B_i=<Y_i, O_i, M_к>$, представляющих собой те точки в которых требуется осуществить ЗИ в системе.

Система защиты с полным перекрытием — предусматривается средства защиты на каждый возможный путь проникновения. В такой системе каждому уязвимому месту V_i соответствует барьер B_i . Если данное условие не выполняется, то объект O_i не защищён для некоторого j.

Согласно данной модели (называемой также моделью Клементса) каждый барьер $B_i=<Y_i, O_i, M_к>$ может быть представлен следующим образом:

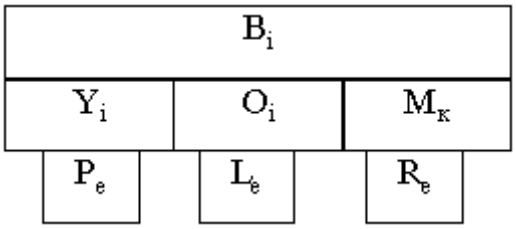


Рисунок — Представление баръера

Здесь: P_e — лингвистическая переменная, характеризующая вероятность появления угрозы; L_e — величина ущерба при проникновении к объекту; R_e — степень сопротивления средства защиты.

Представление процессов с помощью теории графов.

Угроза — случайное событие, подчиняющееся определённому закону распределения.

Экспоненциальный закон:

В технике:

Рисунок — Закон распределения вероятности угрозы

λ — интенсивность отказов; $\lambda = \frac{\frac{\Delta n}{\Delta t}}{N - n(t)}$;

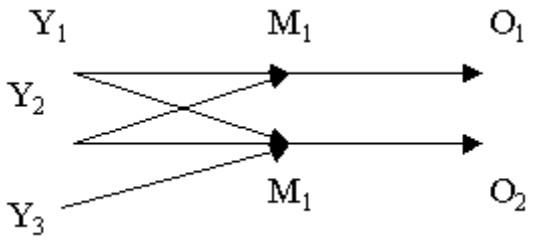
Вероятность возникновения угрозы Y_i:

$$Q(t) = 1 - P(t) = 1 - e^{-\lambda t} \approx \lambda t$$

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

Пример постановки и решения задачи:

Исходные данные:



P_{y1}, P_{y2}, P_{y3} — вероятности возникновения угроз $У_1$, $У_2$, $У_3$;

$P_{м1}$, $P_{м2}$ — вероятности правильного выполнения функций защиты с помощью M_1, M_2;

События: $НСД_{о1}$=[(Угроза У1) или (Угроза У2)] и (неправильное функционирование М1;

$НСД_{о2}$=[(Угроза У1) или (Угроза У2) или (Угроза У3)] и (неправильное функционирование М2;

Тогда: уязвимость информации (НСД) в O_1 и O_2 :

$P_{о1}^{*}=(P_{у1}+P_{у2}-P_{у1}\cdot P_{у2})\cdot(1-P_{м1})$;

$P_{о2}^{*}=(P_{у1}+P_{у2}+P_{у3}-P_{у1}\cdot P_{у2}-P_{у1}\cdot P_{у3}-P_{у2}\cdot P_{у3}+P_{у1}\cdot P_{у2}\cdot P_{у3})\cdot(1-P_{м2})$;

Защищённость информации (отсутствие НСД) в O_1 и O_2:

$P_{о1}=1-P_{о1}^{*}$; $P_{о2}=1-P_{о2}^{*}$;

19 Политика безопасности

Иногда удается достичь общепринятого понимания оптимальности принимаемого решения и доказать его существование. Например, в математической статистике для проверки простой гипотезы против простой альтернативы всеми признано понятие оптимального решения, которое минимизирует ошибку второго рода, а также доказано существование такого критерия (лемма Неймана-Пирсона). Однако, когда решение многоальтернативное, то общепринятого понимания оптимальности не получается, а в тех случаях, когда рассматривается вопрос об оптимальном в каком-то смысле решении, то его существование, чаще всего, удается доказать лишь в частных задачах.

Подобная ситуация существует в задачах защиты информации, поскольку неоднозначно решение о том, что информация защищена. Кроме того, система защиты — не самоцель и должна нести подчиненную функцию по сравнению с главной целью вычислительного процесса. Приведем примеры, поясняющие эти утверждения.

Пример 1. Пусть два инженера ведут разработки двух приборов, которые требуют решения задач $\xi_1, ..., \xi_{n1}$ — первым и задач $\xi'_1, ..., \xi'_{n2}$ — вторым инженером. Предположим, что информация о решении каждой задачи собирается в отдельном файле $O_1,...,O_{n1}$ и $O'_1,...,0'_{n2}$ соответственно. Предположим, что среди множеств задач первого и второго инженеров есть одинаковые. К сожалению, обычный офицер службы безопасности, разрешающий или запрещающий доступ к файлам, не в состоянии решить, что в двух файлах накапливается информация по решению одной задачи. Рассмотрим различные решения офицера по обеспечению безопасности информации.

1. Если он разрешит доступ инженеров к файлам друг друга, то один из них, взяв информацию другого или свою, анонимно и поэтому безнаказанно, продаст эту информацию, так как нет персональной ответственности (невозможно установить, кто продал информацию из данного файла). При этом безнаказанность может стимулировать преступление.

2. Если он не разрешит доступ инженеров к файлам друг друга, то возникает опасность ущерба из-за недоступности информации (один нашел, а второй не нашел

решение одной задачи; тогда вся задача второго инженера оказалась нерешенной, из-за чего возможен большой ущерб для фирмы, т.к. соответствующий прибор сделали конкуренты).

Очевидно, что в обоих случаях достигается снижение одной опасности за счет возрастания другой.

Пример 2. Пример посвящен проблеме компромисса задачи защиты и других задач вычислительной системы. Пусть в базе данных собирается информация о здоровье частных лиц, которая в большинстве стран считается конфиденциальной. База данных нужна, т.к.эта информация позволяет эффективно производить диагностику. Если доступ к этой базе из соображений защиты информации сильно ограничен, то в такой базе не будет пользы для врачей, ставящих диагнозы, и не будет пользы от самой базы. Если доступ открыть, то возможна утечка конфиденциальной информации, за которую по суду может быть предъявлен большой иск. Каким должно быть оптимальное решение?

Результатом решения в приведенных примерах и других аналогичных задачах является выбор правил распределения и хранения информации, а также обращения с информацией, что и называется политикой безопасности. Соблюдение политики безопасности должно обеспечить выполнение того компромисса между альтернативами, который выбрали владельцы ценной информации для ее защиты. Ясно, что, являясь результатом компромисса, политика безопасности никогда не удовлетворит все стороны, участвующие во взаимодействии с защищаемой информацией. В тоже время выбор политики безопасности — это окончательное решение проблемы: что — хорошо и что -плохо в обращении с ценной информацией. После принятия такого решения можно строить защиту, то есть систему поддержки выполнения правил политики безопасности. Таким образом, построенная система защиты информации хорошая, если она надежно поддерживает выполнение правил политики безопасности. Наоборот, система защиты информации — плохая, если она ненадежно поддерживает политику безопасности.

Такое решение проблемы защищенности информации и проблемы построения системы защиты позволяет привлечь в теорию защиты точные математические методы. То есть доказывать, что данная система в заданных условиях поддерживает

политику безопасности. В этом суть доказательного подхода к защите информации, позволяющего говорить о "гарантированно защищенной системе". Смысл "гарантированной защиты" в том, что при соблюдении исходных условий заведомо выполняются все правила политики безопасности. Термин "гарантированная защита" впервые встречается в стандарте министерства обороны США на требования к защищенным системам ("Оранжевая книга").

В данной главе приводятся определения и примеры политик безопасности, показаны последствия плохо выбранных политик. Определены такие политики как дискреционная политика, политика MLS, политика защиты целостности Biba и проведен их анализ. На примере РМ рассмотрены математические проблемы корректного определения политики в данной вычислительной системе.

Определение политики безопасности

Будем следовать общепринятому определению политики безопасности (ПБ), приведенному в стандарте "Оранжевая книга" (1985 г.).

Политика безопасности — это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации .

Полное описание ПБ достаточно объемно даже в простых случаях, поэтому далее будем пользоваться сокращенными описаниями.

Если вспомнить модель защиты, построенную в параграфе 1.1, то смысл политики безопасности очень прост — это набор правил управления доступом. Заметим отличие ПБ от употребляемого понятия несанкционированный доступ (НСД). Первое отличие состоит в том, что политика определяет как разрешенные, так и неразрешенные доступы. Второе отличие — ПБ по своему определению конструктивна, может быть основой определения некоторого автомата или аппарата для своей реализации.

Пример 1. Сформулируем простую политику безопасности в некотором учреждении. Цель, стоящая перед защитой, — обеспечение секретности информации. ПБ состоит в следующем: каждый пользователь пользуется своими и только своими данными, не обмениваясь с другими пользователями. Легко построить систему, поддерживающую эту политику. Каждый пользователь имеет

свой персональный компьютер в персональной охраняемой комнате, куда не допускаются кроме него посторонние лица. Легко видеть, что сформулированная выше политика реализуется в этой системе. Будем называть эту политику тривиальной разграничительной (дискреционной) политикой.

ПБ определяется неоднозначно и, естественно, всегда связана с практической реализацией системы и механизмов защиты. Например, ПБ в примере 1 может полностью измениться, если в организации нет достаточного числа компьютеров и помещений для поддержки этой политики.

Выбор ПБ определяется фазовым пространством, допустимыми природой вычислительных процессов, траекториями в нем и заданием неблагоприятного множества *N*. Корректность ПБ в данных конкретных условиях должна быть, вообще говоря, доказана.

Построение политики безопасности обычно соответствует следующим шагам:

1 шаг. В информацию вносится структура ценностей и проводится анализ риска.

2 шаг. Определяются правила для любого процесса пользования данным видом доступа к элементам информации, имеющим данную оценку ценностей.

Однако реализация этих шагов является сложной задачей. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики. Таким образом, даже хорошая система защиты может быть "прозрачной" для злоумышленника при плохой ПБ.

Рассмотрим следующие примеры.

Пример 2. Пусть банковские счета хранятся в зашифрованном виде в файлах ЭВМ. Для зашифрования, естественно, используется блочная система шифра, которая для надежности реализована вне компьютера и оперируется с помощью доверенного лица. Прочитав в книгах о хороших механизмах защиты, служба безопасности банка убеждена, что если шифр стойкий, то указанным способом информация хорошо защищена. Действительно, прочитать ее при хорошем шифре невозможно, но служащий банка, знающий стандарты заполнения счетов и имеющий доступ к компьютеру, может заменить часть шифртекста в своем счете на

шифртекст в счете богатого клиента. Если форматы совпали, то счет такого служащего с большой вероятностью возрастет. В этом примере игра идет на том, что в данной задаче опасность для целостности информации значительно выше опасности для нарушения секретности, а выбранная политика безопасности хорошо защищает от нарушений секретности, но не ориентирована на опасность для целостности.

Пример 3. Как было описано в примере в конце параграфа 1.4 для государственных структур традиционно принято определять гриф результирующего документа как верхнюю грань грифов и категорий составляющих этот документ частей. Формальное перенесение этого правила традиционной ПБ в ПБ для электронных документов может привести к возникновению канала утечки информации. В самом деле, рассмотрим многоуровневую реляционную базу данных как в параграфе 1.7 с решеткой ценностей {несекретно(Н), секретно (С)}. Пусть R — отношение, A_1,..., A_m — атрибуты, причем A_1- первичный ключ. По запросу строится "обзор" R', который состоит из элементов различной классификации. ПБ может включать одно из двух правил формализованного грифа отношения R':

1. (Привычный для госструктур) R' имеет гриф, равный наибольшему значению из грифов элементов, которые принимают входящие в него атрибуты.

2. (Как это было сделано в параграфе 1.7) R' имеет гриф, равный наименьшему значению из грифов элементов, которые принимают входящие в него атрибуты.

Покажем, что в случае 1 возможна утечка информации с грифом С пользователю, которому разрешен доступ только к информации с грифом Н. Для этого достаточно построить пример базы данных, где такая утечка очевидна.

Пусть реляционная база данных реализует геоинформационную систему. Например, она содержит географическую карту некоторого района пустыни. Базовое отношение РМ имеет три атрибута:

A_1 — ключевой атрибут, содержащий координаты и размеры прямоугольного сектора в некоторой сетке координат;

A_2 — изображение (карта) местности в секторе с координатами, задаваемыми атрибутом A_1;

Аз — координаты колодцев с водой в рассматриваемом секторе.

Для простоты будем считать, что на запрос в базу данных мы получаем на экране изображение карты сектора, определяемого значением атрибута A_1. Пустьзначения атрибутов A_1 и A_2 имеют гриф Н, а значения атрибута A_3 — С.

Если выбрать политику безопасности пункта 1, то мы покажем, как пользователь, не имеющий доступа к секретной информации, реализует канал утечки секретных данных о том, где в пустыне находится колодец с водой (пусть, для простоты, в рассматриваемой местности есть только один колодец). Для получения секретной информации пользователь делает последовательность запросов в базу данных, причем каждый следующий запрос (можно говорить о шагах алгоритма пользователя) определяется ответом на предыдущий.

1 шаг. Разбиваем район (для удобства — квадрат) на полосы и делаем запрос на эти участки в базу данных. Ответ возможен в двух формах:

отказ от показа карты, если она секретная, таккак пользователю, не имеющему допуска к секретнойинформации, база данных, естественно, не должна еепоказывать;

представление карты на экране, если она имеетгриф Н.

_____

I I -------→ отказ

_____

I I -------→ доступ разрешен

_____

Если есть отказ в доступе, то в этом случае в прямоугольнике есть колодец.

2 шаг. Разбиваем полосу, где есть колодец (т.е. где есть отказ в доступе) пополам на две полосы и делаем два запроса в базу данных. Отказ означает, что в данной полосе есть колодец.

И так далее.

В результате вычисляется первая координата колодца с любой заданной точностью. Затем, в оставшейся полосе аналогично вычисляем вторую координату.

Таким образом, ПБ соблюдена, однако, произошла утечка секретной информации.

Если использовать ПБ пункта 2, то любой пользователь получает карту, но пользователь с допуском к секретной информации получает карту с нанесенным колодцем, а пользователь без такого доступа — без колодца. В этом случае канал, построенный выше, не работает и ПБ надежно защищает информацию.

19,23,25 Язык описания политик безопасности

Корт С. С, Боковенко И. Н.

СЦЗИ СПбГТУ

В данной статье рассматривается язык описания политик безопасности, позволяющий на базе логики предикатов составлять спецификации авторизации. В данной статье также исследуется выразительность силы языка описания политик безопасности, т.е. возможность удобного и корректного описания различных классов моделей безопасности на данном языке. В данном случае с его помощью будут описаны следующие мандатные модели безопасности: Белла и Лападулла, Белла и Лападулла с доверенными субъектами, Биба, Биба с понижением уровней субъектов или объектов.

Спецификация авторизации является набором предикатных правил, определяющих правила доступа субъектов к объектам системы для текущего состояния системы. В языке описания политик безопасности правила доступа определяются как отображение четверки (объект, субъект, роль, действие) во множество {авторизован, запрещен}. С точки зрения правил написания спецификации политики безопасности можно классифицировать как:

закрытые политики безопасности — все разрешенные виды доступа должны быть специфицированы;

открытые политики безопасности — все запрещенные виды доступа должны быть специфицированы;

гибридные политики безопасности;

гибридные политики безопасности с разрешенными противоречиями.

Важной характеристикой спецификации авторизации является ее корректность. Спецификация авторизации является корректной, если она непротиворечива и полна. Под непротиворечивостью спецификации понимается наличие только одного решающего правила для каждого доступа (доступ не может быть одновременно разрешен и запрещен). Под полнотой спецификации понимается существование правила для каждого доступа, запрещающего или разрешающего его. Если для некоторого доступа не определена авторизация, должно присутствовать разрешающее правило-умолчание.

Язык описания политик безопасности состоит из следующих компонентов:

1. Множества.

1.1. объектов. Obj — множество объектов. Объекты могут быть сгруппированы по типам T (types).

1.2. субъектов, которым может быть предоставлен доступ:

1.2.1. U — пользователи — отдельные пользователи, работающие с системой;

1.2.2. G — группы — множества пользователей. Субъект s является членом группы G непосредственно, если он определен как член группы G, и косвенно, если существует последовательность s_1, s_2, … ,s_n, n > 1, так что s_i непосредственный член s_{i+1} для i=1, ... n-1. Единственным ограничением на членство в группе является ацикличность, т.е. если s_i член s_j, то s_j, не может быть членом s_i.

1.2.3. R — роли — именованные списки привилегий, необходимые для работы в системе. Роль есть именованный список привилегий, необходимых для выполнения некоторых обязанностей в системе. Также как и группы, роли могут быть организованы в иерархию.

1.2.4. Основное отличие между группами н ролями в том, что последние могут быть активированы и деактивированы пользователями по их желанию, тогда как ограничения, накладываемые группами, применяются всегда.

1.3. действии *A* субъектов над объектами, и множество знаковых авторизованных типов SA = $\{+a, -a \mid a \in A\}$

2.Отношения над множествами субъектов и объектов — предикаты:

2.1. Иерархического членства субъектов и объектов*:*

dirin и in Аргументы — переменные субъектов, s_1 и s_2 Отражают концепцию прямого н

косвенного членства.

typeof. Аргументы — переменные объекта o и типа t. Отражает группирование объектов.

2.2. Доступа субъектов к объектам*:*

done. Первый аргумент данного предиката — переменная объекта, второй — субъекта, третий — множество ролей, четвертый — знаковая авторизация, а пятый — натуральное число. Представляет доступы, выполненные субъектом.

cando Первый аргумент данного предиката — переменная объекта, второй — субъекта, а третий — знаковая авторизация. Данный предикат определяется офицером безопасности системы.

do. Аргументы данного предиката такие же, как у предиката cando. Представляет авторизацию, которую имеет каждый субъект для каждого объекта. Реализует политику разрешения конфликтов.

dorcando. Аргументы данного предиката такие же, как у предиката cando. Представляет авторизацию, определяемую системой с использованием логических правил.

grant. Первый аргумент данного предиката — переменная объекта, второй — субъекта, третий — множество ролей, а четвертый — знаковая авторизация. Представляет разрешенные или запрещенные доступы для каждого субъекта к каждому объекту. Реализует политику контроля доступа.

2.3. Роли субъектов

active. Первый аргумент данного предиката — переменная субъекта, второй — роль. Отражает концепцию активной роли.

2.4. Конфликтов спецификации авторизации

error. Аргументы отсутствуют. Отражает ошибки в спецификации и использовании авторизации.

Если p — описанный выше предикатный символ с корректным количеством и типом переменных

$t_1,...,t_n$ то $p(t_1,...,t_n)$ есть атом. Литеры отображают атомы или их отрицание. Например: cando(OT, ST, SAT) и -¬cando(OT, 5T, 5AT) являются литерами.

3. Правила, составляющие спецификацию политики безопасности (авторизации).

Правило представляет собой импликацию некоторой (возможно, пустой) булевой формулы от литералов, определенных языком, к некоторому предикату, также определенному языком. Язык задает типы и структуру правил, на основе которой составляется конкретный набор правил, специфицирующий конкретную политику безопасности.

В описываемом языке определены следующие правила:

3.1. Осуществленное действие.

done(o, s, R, a, t) <— .

где o, s, R, a, t — элементы Obj,U, 2^R, A и IN соответственно. Правило done является свершившимся фактом, и, как следствие, тело его пусто. Правило done определяется системой при выполнении доступа. Если done(o, s, R, a, t) — истинно, то пользователь s с ролью R осуществил действие a над объектом o во время t. Данное правило полезно для политик безопасности, в которых решение о предоставлении доступа для пользователя базируется на его предыдущих действиях.

3.2. Авторизация.

Правила, задающие начальное состояние системы:

cando (o, s, <sign> a) <— L_1 &L_2...&Ln

где o, s, a, — элементы Obj∪U∪ G∪ R∪ A соответственно, n ≥ 0, <sign> = {+,-}, и для каждого 0 < i < n, L_i есть in или dirin или typeof литерал. Правила авторизации задаются администратором для разрешения или запрещения доступа. Литерал в правой части задаст условия, которые должны быть верифицированы для выполнения авторизации.

Производные правила:

dorcando(o, s, <sign> a) ←L_1 &L_2...&L_n

где o, s, a, — элементы Obj∪U∪ G∪ R∪ A соответственно, n ≥ 0, <sign> = {+, -}, и для каждого 0 < i < n, L_i do, cando, done, in, dirin или typeof литерал. Все dorcando литералы в теле правила должны быть позитивными.

Правила разрешения конфликтов авторизации:

do(o, s, <sign> a) ← L_1 &L_2...&L_n

где o, s, a, — элементы Obj∪U∪ G∪ R∪ A соответственно, n ≥ 0, <sign> = {+, -}, и для каждого 0 < i < n, L_i cando, dorcando, done, in, dirin или typeof литерал. Все dorcando литералы в теле правила должны быть позитивными. Разрешающее правило разрешает или запрещает доступ субъекту системы. Данное правило используется в случае, если правила cando и dorcando не дают положительной или отрицательной авторизации. В этом случае правило do задает принудительную авторизацию или авторизацию по умолчанию.

Правила контроля доступа:

grant(o, u, RS, <sign> a) ← L_1 &L_2...&L_n,

где для каждого 0 < i < n, L_i, cando, dorcando, done, do, in, dirin или typeof литерал. Если grant(o, u, R, +a) — истинно, то пользователь и с активной ролью R может выполнить действие a над объектом o. Аналогично, если grant(o, u, R, +a) — истинно, то действие запрещено.

3.3. Правило целостности.

errorO←L_1 &L_2...&L_n.

где для каждого 0 < i < n, L_i grant, cando, dorcando, done, do, in, dirin или typeof литерал. При добавлении нового правила r вычисляется правая часть правила, и r принимается только, если в результате обработки правила не генерируется ошибка. Данное правило является специфическим для приложения. В общем случае правило целостности говорит о том, что ни один из субъектов не может иметь доступ и отсутствие доступа к объекту.

С использованием описанного языка авторизации закрытые (открытые) политики безопасности могут быть специфицированы с использованием только положительных (отрицательных) авторизации.

Определив язык описания политик безопасности, перейдем к рассмотрению распространения правил авторизации по иерархии субъектов, т.е. как авторизация передается от субъекта к субъекту, если они связаны в иерархии пользователей. При этом существуют две проблемы

- Порождение (правила, регулирующие распространение прав доступа вдоль иерархии субъектов). Для решения этой проблемы могут быть применены следующие подходы:
- запрет распространения прав доступа для потомков;
- запрет перекрытия — все авторизации распространяются, не считаясь с конфликтами;
- перекрытие субъектами-потомками — авторизация для субъекта s перекрывает авторизацию для супер-субъекта s";
- перекрытие путей — авторизация, специфицированная для субъекта s, перекрывает конфликтную авторизацию для супер-субъекта s только для путей, проходящих через s. Перекрытие не имеет эффекта для других путей.

- Разрешение конфликтов (правила, определяющие авторизацию, в случае наличия конфликтной авторизации). Существует четыре подхода к решению данной задачи:
  - запрет конфликтов — наличие конфликта рассматривается как ошибка;
  - запрет имеет преимущество — запрет доступа реализуется преимущественно над его разрешением;
  - разрешение имеет преимущество — разрешение доступа реализуется преимущественно над его запретом;
  - отсутствие преимущества — ничто не имеет первенства, окончательный результат не имеет решения.

После того, как мы рассмотрели язык описания политик безопасности, приступим теперь к исследованию выразительной силы предлагаемого языка на примере мандатных моделей безопасности. Поскольку политики безопасности для данных моделей являются открытыми, то все используемые правила авторизации будут отрицательными. Исключения могут составлять правила разрешения конфликтов (которые не имеют непосредственного отношения к модели безопасности), и специфические правила (в нашем случае это будет правило доопределения уровня объекта — некоторый отход от классической модели мандатного доступа).

Существует ряд моментов, которые следует отметить перед непосредственным описанием политик безопасности:

Поскольку в описываемых моделях роли отсутствуют, предикат grant не используется.

В связи со спецификой (простотой) описываемых моделей политика разрешения конфликтов “фильтрует” только начальное состояния системы, т.к. легко доказать, что любое последующее состояние не будет содержать конфликтных авторизации.

По этой же причине (простота описываемых моделей) предикат error не используется.

В целях более детального исследования выразительной силы языка был произведен некоторый отход от классических мандатных моделей безопасности. Он

заключается в том, что объекту присваивается не конкретный уровень безопасности, а диапазон уровней, который вычисляется системой через уровни и права субъектов, имеющих к нему доступ.

Для всех моделей введем общие положения, касающиеся алфавита языка описания авторизации:

$\exists g_i \subset G \; i \in Z$	Существуют группы пользователей $g_ш$, принадлежащие множеству групп
$g_{i-1} \subset g_i \; i \in Z$	Иерархия групп пользователей, а значит и субъектов, определяется включением одной
$\exists o \in Obj; s \in Subj; s \in G; o \notin G$	Субъекты могут принадлежать к какой-либо группе g_i, объекты не имеют принадлежности к группам, иерархия объектов косвенно
$\exists r, \; w \in A$ ==>+r,-r,+w,	Существуют права чтения и записи, принадлежащие множеству знаковой
$a = r$ v w	Для удобства "a" означает чтение или запись

Операция create (создание объекта субъектом) в данных моделях может рассматриваться как одновременное чтение и запись объекта субъектом.

Рассмотрим общую схему построения набора предикатных правил, составляющих спецификаций авторизации рассматриваемых моделей безопасности:

Начальное состояние системы задается предикатами cando и предикатами вида

in(s,g) ← (принадлежностью субъектов группам g_i). Начальное состояние задает администратор.

Политика разрешения конфликтов реализуется с помощью предикатов do конструкциями вида

$Y \leftarrow X_1 \wedge X_2 \wedge X_3 \wedge$,...,где Y — предикат do(...),

а X_i, предикат cando(...), cando(...), in(...), in(...),dirin(...), dirin(...)

Т.е. на наличие конфликтов проверяется начальное состояние системы.

Собственно правила функционирования модели задаются с помощью предикатов dorcando конструкциями вида

Y ←X_1^ X_2^ X_3^..., где Y-предикат dorcando(...), а X_i, — предикат do(...), do(...), in(...), in(...),dirin(...), dirin(...)

Перейдем к описанию моделей безопасности на языке описания политик безопасности.

Модель Белла и Лападулла

Модель Белла и Лападулла — это модель мандатного доступа, в которой действуют два правила:

=> NoReadUp — Запрет на чтение объекта субъектом более низкого уровня

=> NoWriteDcwn — Запрет на запись в объект субъектом более высокого уровня

Запишем правила, специфицирующие данную модель на языке описания политик безопасности:

Привило: Уровень безопасности группы выше уровня безопасности группы g_i если i>j

Отношения сравнения субъекта с субъектом определяется включением группы одного субъекта в группу другого:

s > s’ <=> dirin(s’,g)^in(s,g)^ ¬in(s’g)

s < s' <=> dirin{s, g')^ in(s, g')^ ¬in(s, g')

s = s' <=> in(s, g) ^ in(s’, g)

Вместо введения решетки уровней безопасности для объектов, иерархия безопасности объектов косвенно задается через права и иерархию субъектов:

s < o <=>∃s’ ^ g' : dorcando(o,s’,+w)^dirin(s,g’)^ in(s’,g')^ ¬in(s,g')

s > o <=>∃s' ^ g : dorcando(o,s’,+r)^ dirin(s’,g)^ in(s,g)^ ¬in(s’,g)

s = o <=> ∃s’ ^ s’’ ^g : dorcando{o, s’,+r)^ dorcando(o, s’’,+w) ^ in{s’,g) ^ in{s’’,g) ^ in(s,g)

Таким образом, уровень объекта определяется нечетко в диапазоне между субъектом с наименьшим уровнем, который может его читать, и наибольшим, могущим в него писать, в соответствии с принципом движения информации вверх по иерархии субъектов в данной модели. В этих трех отношениях и проявляется

Правило 2

Cando(o, s_1 ,+r) ^ cando(o, s_2 ,+w) ^s_2^> s_1 —> do(o, s_2 ,—w)

Если из начальных условий следует, что субъект 2 более высокого уровня может писать в объект и субъект 1 более низкого уровня может читать этот объект, то происходит нарушение принципа модели Белла и Лападулла, гласящего, что информация двигается вверх, и выраженного в правилах NRU и NWD. Для разрешения этого противоречия можно запретить субъекту 1 (более низкого уровня) читать объект (что приведет к истинности отношения S_2<o), либо запретить субъекту 2 (более высокого уровня) писать в объект (что приведет к истинности отношения S_1>o). В данном случае выбран второй вариант, при возникновении противоречия присваивающий объекту наименьший отличие описываемых моделей от классических мандатных, причем классические модели являются частным случаем данных.

Политика разрешения конфликтов.

Правило 1

do(o,s,-a) ← cando{o,s,+a} ^ cando{o,s,—a)

Если начальное состояние системы одновременно авторизует и запрещает какое-либо право субъекта по отношению к объекту, то преобладает запрет.возможный уровень безопасности.

Правило 3

do(o,s,+a)← cando(o,s,+a)^ ¬do{o,s,—ci)

Если в соответствии с начальными условиями субъект имеет право "a" по отношению к некоему объекту, и правила 1 и 2 не отменяют его, то это право сохраняется.

Политика авторизации.

Правило 1

Dorcando(o, s,±a)←do(o, s,±ai)

Правила авторизации выводимы из начальных условий.

Правило 2

dorcando{o,s,+a) ←¬dorcado{o,s,-a)

В связи с открытой политикой безопасности "что не запрещено, то разрешено'

Правило 3 (NRU)

dorcando(o,s,-r) ←s< o

Субъект не может читать объект, если найдется субъект более высокого уровня, имеющий право писать в объект.

Правило 4 (NWD)

dorcando(o,s,-w) ← s > o

Субъект не может писать в объект, если найдется субъект более низкого уровня, имеющий право читать объект.

Правило 5 (Правило доопределения уровней объектов)

dorcando{o,s,+a) ← done{o,s,+a)

Правила построены таким образом, что когда уровень объекта определен нечетко в промежутке между уровнем g_i и g_{i+k}, субъекты, лежащие в данном промежутке уровней, изначально имеют полный доступ (+r и +w) к данному объекту. Однако, при первом обращении какого-либо субъекта из этого промежутка к данному объекту, диапазон уровней, которому принадлежит объект, сужается, чтобы не нарушить принцип движения информации в одном направлении (для модели Белла и Лападулла это — движение информации вверх). Таким образом, уровень объекта доопределяется в процессе работы системы в соответствии с направлением движения информации.

Модель Белла и Лападулла с доверенными субъектами

Доверенный субъект — это субъект, все операции которого над объектами априорно безопасны. Доверенному субъекту разрешено писать и читать любой объект независимо от уровня его секретности. Для описания данной модели к модели Белла и Лападулла добавляется еще одно правило:

Правило введения доверенных субъектов:

∃S : in(s, S)^ ¬dirnn(s,G)

В связи с открытой политикой безопасности (что не запрещено, то разрешено), субъекты, не принадлежащие группе G, имеют полный доступ к любым объектам.

Модель Биба

Данная модель является инверсией модели Белла и Лападулла. В ней действуют два правила:

=> *NoRecidDown* Запрет на чтение объекта субъектом более высокого уровня.

=> *NoWriteUp* Запрет на запись в объект субъектом более низкого уровня.

Поскольку модель Бнба является полной инверсией модели Белла и Лападулла, то для описания данной модели достаточно просто инвертировать правило:

Уровень целостности группы g_i, выше уровня целостности группы g_j, если i<j. Более

высокий уровень целостности соответствует более низкому уровню безопасности. Остальные правила остаются абсолютно идентичными модели Белла и Лападулла:

Модель Биба с понижением уровней субъектов или объектов.

Данные модели аналогичны модели Биба, в них сохраняется закон движения информации вниз, однако правила NoReadDown или NoWriteUp могут быть нарушены. При этом, в зависимости от модели, происходит понижение уровня субъекта или объекта:

Для модели Биба с понижением уровней субъектов:

Правило *NoWriteUp* — такое же, как и в модели Биба, однако субъект может читать объект вопреки правилу *NoReadDown,* при этом уровень субъекта понижается до уровня объекта.

Для модели Биба с понижением уровней объектов:

Правило *NoReadDown* — такое же, как и в модели Биба, однако субъект может писать в объект вопреки *NoWrileUp,* при этом уровень объекта понижается до уровня субъекта.

Опишем правила, дополняющие модель Биба до соответствующей модели:

Для модели Биба с понижением уровней субъектов *dorcando(o,s,-r)*$\leftarrow s > o$ v ($s_1 < s$^ *done*{s_1 ,o,+r'))

Для модели Бнба с понижением уровней объектов

dorcando(o,s,-w) $\leftarrow s <$ o *v* ($o_1 < o$^done(s,o,r))

Модель Биба с понижением уровней объектов является инверсией модели Биба с понижением уровней субъектов относительно принадлежности сущности множеству субъектов или объектов, в связи с чем в дальнейшем возможна коррекция рассмотренного языка таким образом, чтобы объекты и субъекты

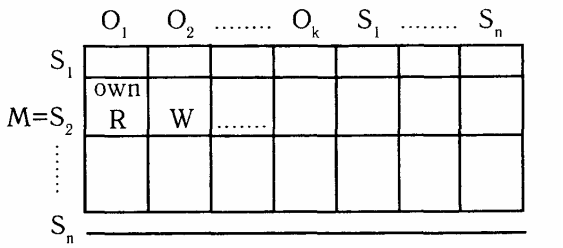
представляли собой одну сущность двух типов, а операции чтения/записи заменены на одну операцию "направленный поток информации", что позволит описывать модели Биба с понижением уровней субъектов и объектов как разновидность (инверсию) одной модели

20 Дискреционная политика

Заглавие параграфа является дословным переводом Discretionary policy, еще одним вариантом перевода является следующий — разграничительная политика. Рассматриваемая политика — одна из самых распространенных в мире, в системах по умолчанию имеется ввиду именно эта политика.

Пусть O — множество объектов, S — множество субъектов, $S \subseteq O$. Пусть $U=\{U_1,...,U_m\}$ — множество пользователей. Определим отображение: own: $0 \rightarrow U$.

В соответствии с этим отображением каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являющийся собственником объекта, имеет все права доступа к нему, а иногда и право передавать часть или все права другим пользователям. Кроме того, собственник объекта определяет права доступа других субъектов к этому объекту, то есть политику безопасности в отношении этого объекта. Указанные права доступа записываются в виде матрицы доступа, элементы которой — суть подмножества множества R, определяющие доступы субъекта S, к объекту 0_i(i = 1, 2,...,; j = 1, 2,...).



Существует несколько вариантов задания матрицы доступа.

1. Листы возможностей: Для каждого субъекта S_i создается лист (файл) всех объектов, к которому имеет доступ данный объект.

2. Листы контроля доступа: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Дискреционная политика связана с исходной моделью таким образом, что траектории процессов в вычислительной системе ограничиваются в каждом доступе. Причем вершины каждого графа разбиваются на классы и доступ в каждом классе определяется своими правилами каждым собственником. Множество неблагоприятных траекторий *N* для рассматриваемого класса политик определяется наличием неблагоприятных состояний, которые в свою очередь определяются запретами на некоторые дуги. Дискреционная политика, как самая

распространенная, больше всего подвергалась исследованиям. Существует множество разновидностей этой политики. Однако многих проблем защиты эта политика решить не может. Одна из самых существенных слабостей этого jкласса политик — то, что они не выдерживают атак при помощи "Троянского коня". Это означает, в частности, что система защиты, реализующая дискреционную политику, плохо защищает от проникновения вирусов в систему и других средств скрытого разрушающего воздействия. Покажем на примере принцип атаки "Троянским конем" в случае дискреционной политики.

Пример 1. Пусть U_1 — некоторый пользователь, а U_2 — пользователь-злоумышленник, O_1 — объект, содержащий ценную информацию, O_2 — программа с "Троянским конем" T, и M — матрица доступа, которая имеет вид:

	O_1	O_2
U_1	own r w	 w
U_2		own r w

Проникновение программы происходит следующим образом. Злоумышленник U_2 создает программу O_2 и, являясь ее собственником, дает U_1 запускать ее и писать в объект O_2 информацию. После этого он инициирует каким-то образом, чтобы U_1 запустил эту программу (например, O_2 — представляет интересную компьютерную игру, которую он предлагает U_1 для развлечения). U_1 запускает O_2 и тем самым запускает скрытую программу T, которая обладая правами U_1 (т.к.была запущена пользователем U_1), списывает в себя информацию, содержащуюся в O_1. После этого хозяин U_2 объекта O_2, пользуясь всеми правами, имеет возможность считать из O_2 ценную информацию объекта O_1.

Следующая проблема дискреционной политики -это автоматическое определение прав. Так как объектов много, то задать заранее вручную перечень прав каждого субъекта на доступ к объекту невозможно. Поэтому матрица доступа различными способами агрегируется, например, оставляются в качестве субъектов только пользователи, а в соответствующую ячейку матрицы вставляются формулы

функций, вычисление которых определяет права доступа субъекта, порожденного пользователем, к объекту O. Разумеется, эти функции могут изменяться во времени. В частности, возможно изъятие прав после выполнения некоторого события. Возможны модификации, зависящие от других параметров.

Одна из важнейших проблем при использовании дискреционной политики — это проблема контроля распространения прав доступа. Чаще всего бывает,что владелец файла передает содержание файла другому пользователю и тот, тем самым, приобретает права собственника на информацию. Таким образом, права могут распространяться, и даже, если исходный владелец не хотел передавать доступ некоторому субъекту S к своей информации в O, то после нескольких шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ. Эта задача иследовалась в модели "take-grant", когда форма передачи или взятия прав определяются в виде специального права доступа (вместо own). Некоторые результаты этих исследований будут приведены в главе "Математические методы анализа политики безопасности".

21 Матричная модель

При использовании матричной модели условия доступа каждого субъекта *s* к каждому объекту *o* определяются содержимым элемента матрицы доступа или матрицы установления полномочий *M*. Каждый элемент m_{ij} матрицы доступа *M* определяет права доступа *i*-го субъекта к *j*-му объекту (читать, писать, выполнять, нельзя использовать и т.п.). Пример матрицы доступа приведен в таблице 1.1.

Таблица 1.1

M	O_1	O_2	…	O_{NO}
S_1	r	w	…	w
S_2	rw	rw	…	∅
…	…	…	…	…
S_{NS}	e	erw	…	ew

Элементы в матрице доступа имеют следующие значения: *r* — чтение, *w* — запись, *e* — выполнение, ∅ -нельзя использовать. Элементы матрицы доступа могут содержать указатели на специальные процедуры, которые должны выполняться при обращении субъекта к объекту. Решение о доступе в этом случае осуществляется на основании результатов выполнения процедур, например:

а) решение о доступе в данный момент времени основывается на анализе предыдущих доступов к другим объектам, например, пользователь *A* может записывать данные в файл *F* только в том случае, если он не читал файл *G*;

б) решение о доступе основывается на динамике состояния системы — права доступа субъекта зависят от текущих прав доступа других субъектов, например, пользователь *B* может открыть файл *H* только в то время, когда база данных, в которой размещен файл, находится в открытом состоянии;

в) решение о доступе основывается на текущем состоянии информации, например, пользователю не разрешено читать поле зарплаты, величина которой превышает 20000 долларов;

г) решение о доступе основывается на значении определенных внутрисистемных переменных, например, доступ может быть осуществлен пользователями определенной группы только во время с 7 до 19 ч, исключая работу со специального терминала.

Отметим, что строка $M[s,*]$ содержит список разрешенных операций субъекта s по отношению ко всем объектам (список возможностей), а столбец $M[*,o]$ — определяет, какие субъекты имеют права доступа к объекту o и какие именно права (список доступа). Размерность матрицы доступа зависит от количества субъектов и объектов в системе и может быть достаточно большой. Для уменьшения размерности матрицы доступа могут применяться различные методы:

а) установление групп субъектов, называемых кликами, каждая из которых представляет собой группу субъектов с одинаковыми правами; установление групп терминалов по классам полномочий (клики терминалов);

б) группировка объектов по уровням категорий (по уровням секретности);

в) хранение списка пар вида (o,f), где o — защищаемый объект, а f — разрешение на использование его субъектом.

Как уже отмечалось, в процессе функционирования системы множества субъектов и объектов могут динамически изменяться. Такие изменения могут происходить, например, в результате появления новых субъектов и объектов, уничтожения субъектов и объектов и изменения прав доступа субъектов к объектам. Соответственно в процессе функционирования системы должна изменяться и матрица доступа. Динамика изменения множеств субъектов и объектов, а также матрицы доступа при выполнении некоторых операций представлена в таблице 1.2.

Таблица 1.2

Исходное состояние	Операция	Результирующее состояние
S,O,M $S' \notin O$	Создание субъекта s'	$S'=S \cup \{s'\}, O \cup \{s'\}$. $M'=[s,o]=M[s,o]$, $s \in S$, $o \in O$. $M'[s',o]=\varnothing$, $o \in O'$. $M'[s',s]=\varnothing$, $s \in S'$.
S,O,M $o' \notin O$	Создание объекта o'	$S'=S$, $O'=O \cup \{o'\}$. $M'[s,o]=M[s,o]$, $s \in S$, $o \in O$. $M'[s',o]=\varnothing$, $s \in S'$.
S,O,M $s'=S$	Уничтожение субъекта s'	$S'=S\setminus\{s'\}$, $O'=O\setminus\{s'\}$. $M'[s,o]=M[s,o]$, $s \in S$, $o \in O'$.
S,O,M $o' \in O$, $o' \notin S$	Уничтожение объекта o'	$S'=S$, $O'=O\setminus\{o'\}$. $M'[s,o]=M[s,o]$, $s \in S'$, $o \in O'$.

S,O,M $s \in S$, $o \in O$	Введение права g в $M[s,o]$	$S'=S$, $O'=O$. $M'[s,o]=M[s,o] \cup \{g\}$ $M'[s',o]=M[s',o']$, если $(s',o') \neq (s,o)$.
S,O,M $s \in S$, $o \in O$	Удаление права g из $M[s,o]$	$S'=S$, $O'=O$. $M'[s,o]=M[s,o] \setminus \{g\}$. $M'[s',o]=M[s',o']$, если $(s',o') \neq (s,o)$.

Здесь S — множество субъектов; O — множество объектов, причем $S \subseteq O$; $M[s,o]$ —- матрица доступа.Элементами матрицы M являются права доступа $g \in G$. Изменившиеся множества помечены штрихом.

Динамику изменения множеств S и O, а также матрицы M, представленной в таблице, поясним на примере создания субъекта s'. При создании субъекта s' этот субъект вводится в состав элементов множеств S и O. В матрице доступа появляется новая строка, соответствующая новому субъекту: $M'[s,o]=M[s,o]$. Так как субъект создан, но его права по отношению к существующим субъектам и объектам не определены, то $M'[s',o]=\varnothing; M'[s',s]=\varnothing$. Матрицы доступа в той или иной степени используются во многих защищенных системах.

22 Многоуровневые политики. Метка безопасности. Разрешенные информационные потоки. Политика MLS

Многоуровневая политика безопасности (политика MLS) принята всеми развитыми государствами мира. В повседневном секретном делопроизводстве госсектор России также придерживается этой политики.

Решетка ценностей SC, введенная в параграфе 1.3 является основой политики MLS. Другой основой этой политики является понятие информационного потока (см. 1.4). Для произвольных объектов X и Y пусть имеется информационный поток $X->_{\alpha}Y$, где X -источник, Y — получатель информации. Отображениес: O->SC считается заданным. Если c(Y)>c(X), то Y -более ценный объект, чем X.

Политика MLS считает информационный поток X->Y разрешенным тогда и только тогда, когда c(Y)>c(X) в решетке SC.

Таким образом, политика MLS имеет дело с множеством информационных потоков в системе и делит их на разрешенные и неразрешенные очень простым условием. Однако эта простота касается информационных потоков, которых в системе огромное количество. Поэтому приведенное выше определение неконструктивно. Хотелось бы иметь конструктивноеопределение на языке доступов. Рассмотрим класс систем с двумя видами доступов r и w (хотя могут быть и другие доступы, но они либо не определяют информационных потоков, либо выражаются через w и r). Пусть процесс S в ходе решения своей задачипоследовательно обращается к объектам $O_1,O_2,...,O_n$ (некоторые из них могут возникнуть в ходе решения задачи). Пусть

$$S \xrightarrow{r} O_{i1}, S \xrightarrow{r} O_{i2}, S \xrightarrow{r} O_{ik}, S \xrightarrow{w} O_{i1}, S \xrightarrow{w} O_{jn-k} \qquad (1)$$

Тогда из параграфа 1.3 следует, что при выполнении условий $c(S)>c(Oi_t)$, t=l,....k, соответствующие потоки информации будут идти в разрешенном политикой MLS направлении, а при $c(S)<c(Oj_t)$, t=l,.., п-k, потоки,определяемые доступом w, будут идти в разрешенном направлении. Таким образом, в результате выполнения задачи процессом S, информационные потоки, с ним связанные, удовлетворяют политике MLS. Такого качественного анализа оказывается достаточно, чтобы классифицировать почти все процессы и принять решение о соблюдении или нет политики MLS. Если где-то политика MLS нарушается, то соответствующий доступ

не разрешается. Причем разрешенность цепочки (1) вовсе не означает, что субъект S не можетсоздать объект O такой, что c(S)>c(0). Однако он не может писать туда информацию. При передаче управления поток информации от процесса S или к нему прерывается (хотя в него другие процессы могут записывать или считывать информацию как в объект). При этом, если правила направления потока при r и w выполняются, то MLS соблюдается, если нет, то соответствующий процесс не получает доступ. Таким образом, мы приходим к управлению потоками через контроль доступов. В результате для определенного класса систем получим конструктивное описание политики MLS.

В системе с двумя доступами r и w политика MLS определяется следующими правилами доступа

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y),$$
$$X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y).$$

Структура решетки очень помогает организации поддержки политики MLS. В самом деле, пусть имеется последовательная цепочка информационных потоков

$$O_1 \xrightarrow[\alpha]{} O_2 \xrightarrow[\beta]{} O_3 \xrightarrow[\gamma]{} \ldots \xrightarrow[\delta]{} O_k$$

Если каждый из потоков разрешен, то свойства решетки позволяют утверждать, что разрешен сквозной поток $O_1 \xrightarrow[\alpha]{} \ldots \xrightarrow[\delta]{} O_k$. Действительно, если информационный поток на каждом шаге разрешен, то $c(O_{i+1}) \geq c(O_i)$, тогда по свойству транзитивности решетки $c(O_1) \leq c(O_k)$, то есть сквозной поток разрешен.

MLS политика в современных системах защиты реализуется через мандатный контроль (или, также говорят, через мандатную политику). Мандатный контроль реализуется подсистемой защиты на самом низком аппаратно-программном уровне, что позволяет эффективно строить защищенную среду для механизма мандатного контроля. Устройство мандатного контроля, удовлетворяющее некоторым дополнительным, кроме перечисленных, требованиям, называется монитором обращений. Мандатный контроль еще называют обязательным, так как его проходит каждое обращение субъекта к объекту, если субъект и объект находятся под защитой системы безопасности. Организуется мандатный контроль следующим образом. Каждый объект O имеет метку с информацией о классе c(O). Каждый субъект также имеет метку, содержащую информацию о том, какой класс доступа

c(S) он имеет. Мандатный контроль сравнивает метки и удовлетворяет запрос субъекта S к объекту O на чтение, если c(S)>c(0) и удовлетворяет запрос на запись, если c(S)<c(0). Тогда согласно изложенному выше мандатный контроль реализует политику MLS.

Политика MLS устойчива к атакам "Троянским конем". На чем строится защита от таких атак поясним на примере, являющимся продолжением примера1 из параграфа 3.2.

Пример 1. Пусть пользователи U_1 и U_2 находятся на разных уровнях, то есть $c(U_1)>c(U_2)$. Тогда, если U_1 может поместить в объект O_1 ценную информацию, то он может писать туда и $c(U_2)<c(U_1)<c(0_1)$, то есть $c(U_2)<c(0_1)$. Тогда любой "Троянский конь" T, содержащийся в объекте O_2, который может считать информацию в O_1, должен отражать соотношение

$$c(O_2) \geq c(O_1).$$

Тогда $c(O_2)>c(U_2)$ и пользователь U_2 не имеет право прочитать в O_2, что делает съем в O_1 и запись в O_2 бессмысленным.

Несколько слов о реализации политики безопасности MLS в рамках других структур, внесенных в информацию. Опять обратимся к примеру реляционной базы данных. Пусть структура РМ и структура решетки ценностей MLS согласованы, как это было сделано в параграфе 1.6. Пусть в системе реализован мандатный контроль, который при обращении пользователя U к базе данных на чтение позволяет извлекать и формировать "обзор" только такой информации, класс которой <c(U). Процедура генерации такого "обзора" была описана в параграфе 1.6. Аналогично, мандатный контроль и правила декомпозиции позволяют поддерживать в нужном направлении информационные потоки в процессе функционирования базы данных. В результате получаем, что при наличии мандатного контроля построенная в 1.6 реляционная многоуровневая база данных поддерживает политику MLS.

Политика MLS создана, в основном, для сохранения секретности информации. Вопросы целостности при помощи этой политики не решаются или решаются как побочный результат защиты секретности. Вместе с тем, пример 2 параграфа 3.1 показывает, что они могут быть противоречивы.

24 Модель Диона

Субъекты в модели Диона

Мы будем пользоваться понятиями меток безопасности и отношения доминирования меток. В модели Диона с каждым субъектом (то есть процессом, действующим от имени определенного пользователя) ассоциируются три метки конфиденциальности и три метки целостности информации:

•*абсолютная метка конфиденциальности* (ACL(s)) — присваивается субъекту во время создания и остается постоянной во все время его существования. Обычно в качестве ACL(s) используется метка пользователя-инициатора процесса;

•*метка конфиденциальности чтения* (RCL(s)) — максимальный (в смысле отношения доминирования меток) уровень конфиденциальности, с которого субъекту разрешено читать информацию из объекта с меткой ACL(o), так что должно быть RCL(s) >= ACL(o_i) для возможности чтения из объекта o_i;

•*метка конфиденциальности записи* (WCL(s)) — минимальный уровень конфиденциальности, на который субъекту разрешено записывать информацию в объект с меткой ACL(o_i), так что должно быть WCL(s) <= ACL(o_i) для возможности записи в объект o_i, причем право записи в модели Диона понимается только как право модификации объекта без предварительного чтения;

•*абсолютная метка целостности* (AIL(s)) — присваивается субъекту во время создания и остается постоянной во все время его существования. Обычно в качестве AIL(s) используется метка пользователя-инициатора процесса;

•*метка целостности чтения* (RIL(s)) — минимальный уровень целостности, с которого субъекту разрешено читать информацию из объекта с меткой AIL(o), так что должно быть RIL(s) <= AIL(o_i) для возможности чтения из объекта o_i;

•*метка целостности записи* (WIL(s)) — максимальный уровень целостности, на который субъекту разрешено записывать информацию в объект с меткой AIL(o_i), так что должно быть WIL(s) >= AIL(o_i) для возможности записи в объект o_i.

Для каждого субъекта s должны выполняться следующие соотношения:

WCL(s) <= ACL(s) <= RCL(s)

RIL(s) <= AIL(s) <= WIL(s)

(запись LI <= L2 обозначает доминирование метки L2 над L1).

Будем говорить, что метка безопасности L2 строго доминирует над меткой L1 (обозначается L1 < L2), если уровень безопасности L2 строго больше, чем у L1, а набор категорий L1 является подмножеством набора категорий L2.

Субъект, для которого хотя бы одно из записанных выше четырех неравенств является строгим, называется надежным (в противном случае — ненадежным).

Объекты в модели Диона

Под объектом в модели Диона понимается любой элемент, способный хранить данные. С каждым объектом ассоциируются по три метки конфиденциальности и целостности:

•*абсолютная метка конфиденциальности* (ACL(o)) — присваивается объекту во время создания и остается постоянной на все время его существования. Характеризует конфиденциальность данных, хранящихся в объекте;

•*метка конфиденциальности чтения из объекта* (RCL(o)) — максимальный уровень конфиденциальности, на который могут мигрировать данные, хранящиеся в объекте (могут читаться субъектом s_i с уровнем конфиденциальности $ACL(s_j)$): $RCL(o) >= ACL(s_j)$;

•*метка конфиденциальности записи в объект* (WCL(o)) — минимальный| уровень конфиденциальности, с которого данные могут записываться в объект субъектом s_j с уровнем конфиденциальности $ACL(s_j)$: $WCL(o) <= ACL(s_j)$;

•*абсолютная метка целостности* (AIL(o)) — присваивается объекту во время создания и остается постоянной на все время его существования. Характеризует степень целостности данных, хранящихся в объекте;

•*метка целостности чтения из объекта* (RIL(o)) — минимальный уровень целостности, на который могут мигрировать данные, хранящиеся в объекте (могут читаться субъектом s_i с уровнем целостности $AIL(s_j)$): $RIL(o) <= AIL(s_j)$;

•*метка целостности записи в объект* (WIL(o)) — максимальный уровень целостности (субъекта s_i с уровнем $AIL(s_j)$), с которого данные могут записываться в объект: $WIL(o) >= AIL(s_i)$.

Для каждого объекта o должны выполняться следующие соотношения:

$WCL(o) <= ACL(o) <= RCL(o)$

RIL(o) <=AIL(o) <= WIL(o)

Условия образования информационных каналов

Модель Диона предусматривает возможность передачи информации путем организации однонаправленных каналов между объектами. Подытожим все вышесказанное: субъект s может организовать канал передачи информации из объекта o_1 в объект o_2, если выполняются следующие соотношения:

RCL(s) >= ACL(o_1)

RIL(s) <= AIL(o_1)

WCL(s) <= ACL(o_2)

WIL(s) >= AIL(o_2)

(субъект должен иметь право на чтение из объекта o_1 и на запись в объект o_2),

RCL (o_1) >= RCL (o_2)

WCL (o_1) >= WCL (o_2)

RIL (o_1) <= RIL (o_2)

WIL (o_1) <= WIL (o_2)

(эти соотношения гарантируют, что ограничения на метки чтения/записи не могут быть нарушены при посредничестве "третьих" объектов: метки конфиденциальности чтения/записи информации при перезаписи из объекта в объект не могут повышаться, целостности — понижаться),

RCL(o_1) >= ACL(s);

RIL(o_1) <= AIL(s);

WCL(o_2) <= ACL(s);

WIL(o_2) >= AIL(s).

(субъекты не должны нарушать ограничения на метки чтения/записи объектов).

Модель Диона обобщает более известные модели безопасности (Белла–ЛаПадула и Биба). В частности, из приведенных аксиом следует, что ненадежные субъекты (WCL(s) = ACL(s) = RCL(s) и WIL(s) = AIL(s) = RIL(s)) не могут переместить информацию в объект с меньшим уровнем конфиденциальности и/или более высоким уровнем целостности.

На рисунке 1 в виде графа приведены соотношения доминирования меток безопасности объектов и субъекта для возможности образования информационного канала из o_1 в o_2, (отношения доминирования обозначены стрелками).

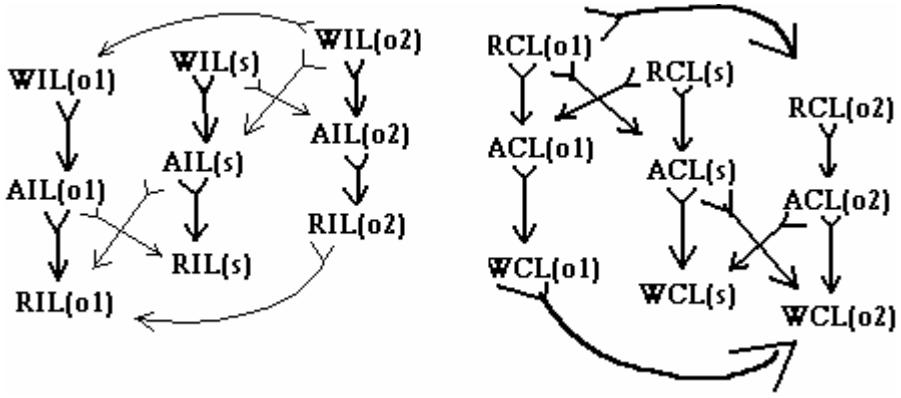


Рисунок 1 — Условия образования информационных каналов

Литература

1. Castano S., Fugini M., Martella G., Samarati P. Database Security. — Addison-Wesley, 1995.

25 Политика целостности Biba

Предположим, что опасности для нарушения секретности не существует, а единственная цель политики безопасности — защита от нарушений целостности информации. Пусть, по-прежнему, в информацию внесена решетка ценностей SC. В этой связи любой информационный поток X -> Y может воздействовать на целостность объекта Y и совершенно не воздействовать на целостность источника X. Если в Y более ценная информация, чем в X, то такой поток при нарушении целостности Y принесет более ощутимый ущерб, чем поток в обратном направлении от более ценного объекта Y к менее ценному X. Biba предложил в качестве политики безопасности для защиты целостности следующее.

В политике Biba информационныйпоток X -->$_{\alpha}$Y разрешен тогда и только тогда, когда

$$c(Y) \le c(X)$$

Можно показать, что в широком классе систем эта политика эквивалентна следующей.

Для систем с доступами w и r политика Biba разрешает доступ в следующих случаях:

$$S \xrightarrow{r} O \Leftrightarrow c(S) \le c(O),$$
$$S \xrightarrow{w} O \Leftrightarrow c(S) \ge c(O).$$

Очевидно, что для реализации этой политики также подходит мандатный контроль.

26-28 Модели контроля доступа, основанного на ролях

Рави С. Сандху*1*, Эдвард Дж. Койн, Гал Л. Файнстайн и Чарльз Е. Юман*2*.

Переработана 26 октября 1995 г.

Ключевые слова: безопасность, контроль доступа, роли, модели

Данная статья представляет семейство соответствующих моделей для контроля доступа, основанного на ролях (КДОР), в которых разрешения связаны с ролями, а пользователи являются членами соответствующих ролей. Это намного упрощает управление разрешениями. Роли тесно связаны с понятием пользовательских групп в контроле доступа. Однако, роль объединяет множество пользователей с одной стороны и множество разрешений с другой, в то время как пользовательские группы обычно определяются лишь как множество пользователей.

Основные понятия КДОР получили свое развитие с появлением многопользовательских компьютерных систем. Возрождение интереса к КДОР обусловлено потребностью в настраиваемой аппаратуре общего назначения для КДОР и необходимостью управления самим КДОР. Как следствие, состав КДОР колеблется от простого до сложного. Данная статья описывает модели для системного описания разнообразных компонентов КДОР и их взаимодействия.

1. Вступление

Понятие контроля доступа, основанного на ролях (КДОР) возникло с появлением многопользовательских и многозадачных он-лайн систем в 70-х. Центральным понятием КДОР является то, что разрешения ассоциированы с ролями, а пользователи связаны с соответствующими ролями. Это значительно упрощает управление разрешениями. Роли создаются для различных рабочих функций в организации, и пользователи закреплены за ролями в соответствии со своими обязанностями и квалификацией. Пользователи могут быть легко переведены с одной роли на другую. Ролям могут присваиваться новые разрешения при внедрении новых программ и систем, а при необходимости роли могут лишаться разрешений.

---

1 Корпорация СЕТА и Университет Джорджа Мейсона.

2 Корпорация СЕТА

Роль должна рассматриваться как семантический структурный компонент, вокруг которого формулируется политика контроля доступа. Отдельная группа пользователей и разрешений, объединенная одной ролью, является кратковременным явлением. Сама роль является более стабильным элементом, так как деятельность или функции организации меняются не столь часто.

Ниже анализируется ряд особых причин для создания роли. Роль может представлять компетенцию выполнения определенных заданий, например, доктора или фармацевта. Роль может включать власть и ответственность, например, руководитель проекта. Власть и ответственность отличны от компетенции. Джейн До может быть компетентной возглавлять несколько управлений, однако назначена возглавлять лишь одно управление. Роли могут отражать особые должностные обязанности, передаваемые между несколькими пользователями, например, дежурный врач или сменный управляющий. Модели КДОР и их внедрение должны удобно приспособиться под все эти проявления концепции роли.

Недавний анализ, проведенный NIST [1], показывает, что КДОР отвечает на многие потребности в деловых и правительственных кругах. В исследовании, проведенном в 28 организациях, выяснилось, что требования к контролю доступа обусловлены различными причинами, включая уверенность клиентов, акционеров, страховщиков, личный характер персональной информации, предотвращение незаконного использования финансов, предотвращение незаконного использования междугородней телефонной связи, следование профессиональным стандартам. В ходе исследования выяснилось, что большое количество организаций основывают свои решения по контролю доступа на ролях, которые отдельные пользователи играют в организации. Много организаций предпочитали централизованно контролировать и эксплуатировать права доступа, не столько по личному усмотрению системного администратора, сколько в соответствии с правилами защиты организации. Анализ также показал, что организации обычно рассматривали свои потребности в контроле доступа как уникальные и были убеждены, что имеющиеся программные продукты недостаточно гибки.

Другое свидетельство повышенного интереса к КДОР находится в области стандартов. Считается, что роли являются частью нового стандарта SQL3,

используемого в системах управления базами данных, основывающих свое выполнение на Оракл 7. Роли также были встроены в профиль коммерческой безопасности проекта Общих критериев [2]. КДОР также хорошо подошел основным течениям в технологии и бизнесе. Ряд продуктов поддерживают непосредственно одну их форм КДОР, другие поддерживают чрезвычайно схожие понятия как, например, группы пользователей, которые можно использовать для осуществления ролей.

Несмотря на общепризнанную полезность концепции КДОР, существует много расхождений по поводу значения КДОР. В результате этого, КДОР является сегодня аморфным понятием, интерпретируемым по-разному различными исследователями и системными разработчиками, от простого варианта до сложного. В данной работе описывается новая структура, состоящая из четырех моделей, разработанная авторами для обеспечения системного подхода к пониманию КДОР и категоризирования его применения в различных системах. Наша структура также разделяет управление КДОР и его использования для контроля доступа к данным и другим ресурсам.

2 Причины возникновения

Основным предназначением КДОР является упрощение управления и надзора за безопасностью. Большое количество коммерчески успешных систем контроля доступа для центральных процессоров применяют роли для управления безопасностью. Например, роль оператора может иметь доступ ко всем ресурсам, но не может изменять разрешения на доступ, а роль аудитора может иметь доступ к контрольному журналу сделок. Это административное использование ролей можно также обнаружить в современных сетевых операционных системах, например, в Novell Netware и Microsoft Windows NT.

Нынешний всплеск интереса к КДОР сфокусировался на общей поддержке КДОР на уровне программ. В прошлом, как и сегодня, уже разработаны особые программы с встроенным в них КДОР. Существующие операционные системы и окружение дают немного возможностей для поддержки использования КДОР на уровне программ. Такая поддержка только начинает появляться в программных

продуктах. Основной трудностью является разработка таких устройств, которые бы не зависели от программного обеспечения и были бы достаточно гибкими и одновременно простыми в использовании, для поддержки большого количества программ с минимальной необходимостью в настройке.

Усложненные версии КДОР имеют возможность устанавливать отношения между ролями, а также между разрешениями и ролями и между пользователями и ролями. Например, две роли могут быть определены как взаимоисключающие, поэтому один и тот же пользователь не будет допущен к обеим ролям одновременно. Роли также могут принимать отношения наследования, по которым одна роль наследует разрешения, приписанные другой роли. Эти отношения между ролями могут быть использованы для применения такой политики безопасности, в которую включено разделение обязанностей и передача полномочий. Прежде, подобные отношения должны были быть закодированными в программное обеспечение; при использовании КДОР они могут быть определены всего один раз для домена безопасности. С помощью КДОР возможно предопределить отношения роли и разрешения, что упрощает назначения пользователям предопределенных ролей. Исследование NIST [1] показывает, что разрешения, назначенные ролям, имеют тенденцию меняться относительно редко по сравнению с изменениями в распределении пользователей по ролям. Анализ также рекомендует разрешать администраторам назначать и аннулировать членство пользователей в имеющихся ролях без наделения данных администраторов полномочиями создавать новые роли или изменять назначения ролей по разрешению.

Назначение ролей пользователям обычно предусматривает наличие более низкого уровня технических навыков, чем наделение ролей разрешениями. Без КДОР, тем не менее, определить, какие разрешения даны каким пользователям, может быть затруднительно.

Стратегия контроля доступа встроена в различные компоненты КДОР, как, например, в отношения между ролью и разрешением, пользователем и ролью, ролью и ролью. Данные компоненты коллективно определяют, может ли определенный пользователь быть допущенным к определенному разделу данных в системе. Компоненты КДОР могут быть сконфигурированы непосредственно владельцем

системы или косвенно соответствующими ролями, как это определено владельцем системы. Стратегия, используемая в определенной системе является общим результатом точной конфигурации различных компонентов КДОР по указанию владельца системы. Более того, стратегия контроля доступа может проходить внутреннее развитие в течение жизненного цикла системы, а в больших системах так скорее всего и происходит. Важным преимуществом КДОР является возможность модифицирования стратегии для удовлетворения изменяющихся потребностей организации.

Несмотря на то, что стратегия КДОР является нейтральной по своей сути, она непосредственно поддерживает три широко известных принципа безопасности: минимальные привилегии, разделение обязанностей и абстрагирование данных. Минимальные привилегии поддерживаются с помощью того, что КДОР можно настроить так, чтобы только те разрешения, которые требуются для функций, выполняемых членами данной роли, допускались к ней. Разделение обязанностей достигается с помощью контроля за тем, чтобы в работе, требующей особой безопасности, участвовали взаимоисключающие роли, например, требуя участия рядового бухгалтера и главного бухгалтера в процедуре выписывания чека. Абстрагирование данных поддерживается с помощью абстрактных разрешений, например, кредит и дебит для бухгалтерского объекта вместо разрешений на чтение, запись и выполнение, обычно предоставляемых операционной системой. Тем не менее, КДОР не может принудительно обеспечить выполнение этих принципов. Работник службы безопасности может настроить КДОР так, что он будет нарушать данные принципы. Кроме того, уровень поддержки абстрагирования данных определяется деталями применения.

КДОР не является панацеей от всех проблем контроля доступа. Необходимо использование более сложных форм контроля доступа в ситуациях, когда возникает необходимость контроля последовательности операций. Например, предписание покупки требует ряда шагов, необходимых до выписки заказа на поставку. КДОР не ставит перед собой целью непосредственно контролировать разрешения для подобной последовательности событий. Другие формы контроля доступа могут быть надстроены над КДОР для этой цели. Мохаммед и Дилтс [3], а также Томас и

Сандху [4] уже рассматривали некоторые из этих проблем. Мы рассматриваем контроль последовательности операций лежащим за пределами КДОР, хотя КДОР может служить основанием для создания подобного контроля.

3. Роли и соответствующие понятия

Очень часто можно услышать вопрос: «В чем различие между ролями и группами?». Группы пользователей как единица контроля доступа обычно предусмотрены в большинстве систем контроля доступа. Основное отличие между большинством разработок групп и концепцией ролей является то, что группы обычно рассматриваются как совокупность пользователей с одной стороны и совокупность разрешений с другой. Роль служит как посредник между этими совокупностями.

Рассмотрим операционную систему Юникс. Групповое членство в Юниксе определяется в двух файлах, «пароль» и «группа». Следовательно, легко определить группу, к которой принадлежит конкретный пользователь или всех членов определенной группы. Разрешения даются группам на основании битов разрешений, связанных с отдельными файлами и директориями. Для определения того, какие разрешения имеет определенная группа, обычно требуется прохождение по всему дереву файловой системы. Следовательно, намного легче определить членство группы, чем определить разрешения группы. Более того, наделение групп разрешениями чрезвычайно децентрализовано. В сущности, владелец любого поддерева в файловой системе Юникса может наделить любую группу разрешением доступа к данному поддереву. (Точная вероятность того, насколько это реально, зависит от конкретного варианта Юникса.) Однако, группы Юникса могут быть использованы для осуществления ролей в определенных ситуациях, хотя эти группы не совпадают с нашим понятием ролей. Для иллюстрации качественной природы группы в отличие от различия ролей, давайте рассмотрим гипотетическую систему, в которой определение членства в группе занимает в два раза больше времени, чем определение разрешений групп. Предположим, что разрешения групп и членства могут быть изменены только системным администратором. В таком случае, механизм работы группы будет очень близок к нашему понятию роли.

Предыдущие дискуссии предлагают две отличительные черты роли: определение членства в ролях и разрешения ролей должно быть практически одинаково легким, и контроль членства в ролях и разрешения ролей должен быть относительно сосредоточенным в руках нескольких пользователей. Большинство механизмов, которые претендуют на название основанных на ролях, не соответствуют одному либо обоим этим требованиям.

Часто возникает вопрос относительно отношений ролей и ячеек. Ячейки являются частью структуры меток безопасности, используемой в секретных правительственных и оборонных секторах [5]. Ячейки основываются на понятии потребности знания, что имеет семантическую коннотацию информации, доступной под меткой ячейки, подобную семантической коннотации роли. Однако, использование ячеек характерно для специфических стратегий одностороннего потока информации в структуре меток. Роли не предусматривают особую стратегию подобного свойства.

Имеется историческое отличие между разграничительным и обязательным контролем доступа, соответственно именуемым как РКД и ОКД. Данное отличие связано с исследованиями по безопасности, проводимыми в оборонном секторе. ОКД инициализирует контроль доступа на основании меток безопасности, закрепленных за пользователями (или, более точно, субъектами) и объектами [5]. РКД инициализирует контроль доступа к объекту на основании разрешений или отказов или и того и другого, как настроено пользователем, обычно являющимся владельцем объекта. КДОР может рассматриваться как независимый компонент контроля доступа, сосуществующий при необходимости с РКД и ОКД. В таких случаях доступ разрешен, только если это разрешено КДОР, РКД и ОКД. Мы также предполагаем, что КДОР во многих случаях может существовать отдельно. В качестве близкого вопроса может рассматриваться следующий: является КДОР сам по себе разграничительным или обязательным механизмом? Ответ зависит от точности определения разграничительного и обязательного, а также от точной природы и конфигурации разрешений, ролей и пользователей в системе КДОР. По нашему мнению, «обязательный» означает то, что отдельные пользователи не имеют выбора в том, какие разрешения или пользователи относятся к той или иной

роли, в то время, как «разграничительный» указывает на то, что отдельные пользователи могут принимать такие решения. Как было сказано выше, КДОР сам по себе стратегически нейтрален. Отдельные конфигурации КДОР могут иметь более сильный оттенок обязательности, другие — разграничительности.

4. Семейство базовых моделей

Для понимания различных аспектов КДОР мы даем определения семейству четырех концептуальных моделей. Отношения между этими четырьмя моделями показаны на иллюстрации 1 (a), а их основные характеристики приведены в иллюстрации 1 (b). КДОР 0, базовая модель, находится у основания, указывая на то, что это является минимальным требованием для любой системы, создатели которой заявляют, что их система поддерживает КДОР. КДОР 1 и КДОР 2 оба включают в себя КДОР 0, однако добавляют к нему дополнительные черты. Они называются усовершенствованными моделями. КДОР 1 имеет в качестве дополнения концепцию иерархии ролей (ситуаций, когда роли могут наследовать разрешения от других ролей). КДОР 2 добавляет ограничивающие условия (устанавливающие ограничения на допустимые конфигурации различных компонентов КДОР). КДОР 1 и КДОР2 не являются абсолютно идентичными друг другу. Сводная модель КДОР 3 включает КДОР 1 и КДОР 2 и, по свойству транзитивности, КДОР 0.

Данные модели предназначаются для того, чтобы быть точкой отсчета и моделями для сравнения с системами и моделями, используемыми другими исследователями и разработчиками. Они также могут служить в качестве путеводителя по разработке продуктов и их оценке перспективными клиентами. На данный момент, мы предполагаем, что существует один сотрудник службы безопасности, который имеет право конфигурации различных наборов и соотношений данных моделей. Позднее мы представим усложненную модель управления.

4.1 Базовая модель

Базовая модель КДОР 0 состоит из той части иллюстрации 1(b), которая не относится ни к одной из трех усовершенствованных моделей. Существует три

множества объектов, называемых пользователи (U), роли (R) и разрешения (P). Диаграмма также показывает множество сеансов (S). Пользователь в данной модели является человеком. Концепт пользователя может быть обобщен до включения в него таких разумных автономных агентов как роботов, неподвижных компьютеров, или даже компьютерных сетей. Для простоты мы сконцентрируем особое внимание на пользователе в лице человека. Роль — это рабочая функция или наименование работы внутри организации с определенной связанной с ней семантикой в аспекте власти и ответственности, переданной члену данной роли.

Разрешение — это одобрение определенного типа доступа к одному или более объектам в системе. Термины авторизация, право доступа и привилегия также используются в литературе для обозначения разрешения. Разрешения всегда имеют положительный характер и подтверждают возможность владельца разрешения произвести указанное действие или действия в системе. Объектами являются данные, а также ресурсы, представленные информацией внутри компьютерной системы. Наша концептуальная модель разрешает целый ряд интерпретаций разрешения, от очень крупных частиц, например когда разрешается доступ ко всей подсети, до очень мелких частиц, когда единицей доступа является определенная область отдельной записи. В некоторых источниках по контролю доступа говорится об «отрицательных разрешениях», которые запрещают, а не разрешают доступ. В нашей структуре отрицание доступа смоделировано как ограничение, а не отрицательное разрешение.

Природа разрешения сильно зависит от внедрения деталей системы и самого типа системы. Общей моделью контроля доступа разрешения должны восприниматься как неинтерпретированные символы, в какой-то мере. Каждая система охраняет абстрактные объекты, которые она выполняет. Поэтому операционная система защищает такие вещи, как файлы, директории, устройства и порты с помощью операций чтения, записи и выполнения. Реляционная система управления базами данных защищает отношения, кортежи, атрибуты, представления операциями ВЫБРАТЬ, ОБНОВИТЬ, УДАЛИТЬ и ВСТАВИТЬ. Бухгалтерская программа защищает счета и гроссбухи с помощью таких операций, как дебет, кредит, трансферт, создать счет, и удалить счет. Так, представляется возможным

определить роль для кредитной операции без аналогичного определения той же роли для дебитной операции.

Разрешения могут быть использованы для отдельных объектов или группы объектов. Например, разрешение может быть таким узким, как доступ чтения к определенному файлу или таким общим, как доступ чтения ко всем файлам, принадлежащим отдельному управлению. То, как отдельные разрешения соединяются для образования общего разрешения для использования в качестве одной единицы, очень сильно зависит от настроек.

Иллюстрация 1 (b) показывает отношение назначения пользователя (UA) и назначения разрешения (PA). Оба отношения принадлежат к типу многие-ко-многим. Пользователь может являться членом многих ролей, а у роли может быть много пользователей. Таким же образом, у роли может быть много разрешений, и одно и то же разрешение может быть дано многим ролям. Ключ к пониманию КДОР лежит в этих двух отношениях. В конечном итоге, именно пользователь осуществляет доступ через разрешения. Метод размещения роли в качестве посредника для передачи пользователю права осуществлять решение позволяет достичь большего контроля над конфигурацией и наблюдением за доступом, чем метод прямого соотношения пользователей и разрешений.

Каждый сеанс является соотнесением одного пользователя с возможным количеством ролей, то есть пользователь начинает сеанс, в течение которого он активирует определенное подмножество ролей, чьих членом он(а) является. Двусторонняя стрелка от сеанса к R на иллюстрации 1 (b) показывает, что одновременно могут активироваться много ролей. Разрешения, имеющиеся у пользователя, являются объединением разрешений от всех ролей, активированных в данном сеансе. Каждый сеанс ассоциирован с одним пользователем, как указано односторонней стрелкой от сеанса к U на иллюстрации 1 (b). Данная ассоциация остается постоянной на все время сеанса. Пользователь может одновременно создавать множественные сеансы, например, каждый в отдельном окне на экране рабочей станции. Каждый сеанс может иметь различную комбинацию активных ролей. Данное качество КДОР 0 поддерживает принцип минимальной привилегии. Пользователь, являющийся членом нескольких ролей, может задействовать любое

их подмножество, необходимое для решения задач, поставленных в данном сеансе. Следовательно, пользователь, являющийся членом сильной роли может постоянно держать свою роль деактивированной и активировать ее только при необходимости. Мы откладываем рассмотрение всех видов ограничительных условий, включая ограничения на активацию ролей, до описания КДОР 2. поэтому в КДОР 0 именно пользователь решает, какие роли ему следует активировать в том или ином сеансе. КДОР 0 также позволяет динамическую активацию и дезактивацию ролей во время сеанса. Понятие сеанса совпадает с традиционным понятием субъекта в литературе по контролю доступа. Субъект (или сеанс) является единицей контроля доступа, и пользователь может активировать несколько субъектов (или сеансов) с разными разрешениями одновременно. Следующее определение формулирует все вышесказанное.

Определение 1.

Модель КДОР 0 имеет следующие компоненты:

U, R, P и S (соответственно, пользователи, роли, разрешения и сеансы),

PA⊆P×R, отношение между разрешением множество-множество и наделением ролями,

UA⊆U×R, отношение между пользователями множество-множество и наделением ролями,

user : S→U, функция, соотносящая каждый сеанс S_i с одним пользователем user (S_i) (неизменным на протяжении сеанса)

roles :S→2^r , функция, соотносящая каждый сеанс S_i с множеством ролей roles(S_i)⊆

{r | (user(S_i), r) ∈UA} (может меняться со временем) и сеанс S_i имеет разрешения $U_{r\in Roles(S_i)}\{p|(p,r)\in RA\}$.

Мы ожидаем, что каждая роль может быть придана как минимум одному разрешению и каждый пользователь — как минимум одной роли. Данная модель, тем не менее, этого не требует.

Как было отмечено выше, КДОР 0 принимает разрешения в качестве неинтерпретированных символов, так как точная природа разрешения является

зависимой от выполнения и системы. Тем не менее, мы требуем, чтобы разрешения относились к данным и ресурсам, а не к компонентам самого КДОР. Разрешения на изменение множеств U, R, P, и отношений PA и UA называются административными разрешениями. Они будут рассмотрены позже в модели управления КДОР. На данном этапе следует считать, что один сотрудник службы безопасности может изменять эти компоненты.

Сеансы контролируются отдельными пользователями. Что касается самой модели, пользователь может создавать сеанс и выбирать активацию некоего подмножества пользовательских ролей. Роли, являющиеся активными в данном сеансе, могут быть изменены по усмотрению пользователя. Сеанс заканчивается по инициативе пользователя. (Некоторые системы завершают сеанс, остающийся неактивным слишком долгое время. Строго говоря, это является ограничительным условием и должно принадлежать КДОР 2.)

Некоторые авторы [6] включают обязанности, в дополнение к разрешениям, в качестве атрибута ролей. Обязанность — это обязательство пользователя производить ту или иную функцию, что в общем необходимо для четкой работы организации. По нашему мнению, обязанности являются усовершенствованным концептом, не принадлежащим КДОР0. Мы также решили не встраивать обязанности в наши усовершенствованные модели. Мы считаем, что встраивание таких понятий, как обязанности в модели контроля доступа требует дополнительных предварительных исследований. Один из подходов может быть рассмотрение их как подобных разрешениям. Другие подходы могут основываться на новых парадигмах контроля доступа, как, например, авторизация по основанию задания [4].

4.2 Иерархии ролей

КДОР 1 включает иерархии ролей (ИР), как это обозначено на иллюстрации 1. Иерархии ролей практически обязательно упоминаются при обсуждении ролей в литературе [7,8,9,10]. Они также часто используются в системах, предоставляющих роли.

Иерархии ролей являются естественным методом отражения организационных структур ролей для отображения линии власти и ответственности в организации. Примеры иерархии ролей показаны на иллюстрации 2. В целях упрощения более значительные (или главные) роли показаны в верхней части этих диаграмм, а менее значительные (или второстепенные) роли — в нижней части. На иллюстрации 2 (a) наименьшая роль — это медсестра. Роль физиотерапевта более высокая по сравнению с медсестрой и соответственно наследует все разрешения от медсестры. Роль физиотерапевта может иметь дополнительные разрешения, которые не унаследованы от роли медсестры. Наследование ролей транзитивно, поэтому, например на иллюстрации 2 (a), роль физиотерапевта первой категории наследует разрешения от ролей физиотерапевта и медсестры. Физиотерапевт первой категории и специализированный физиотерапевт оба наследуют разрешения от роли физиотерапевта, однако они оба обладают различными разрешениями, переданными им непосредственно. Иллюстрация 2 (b) показывает множественное наследование разрешений, при котором роль руководителя проекта наследует разрешения ролей как тестирующего инженера, так и программиста.

Говоря математически, данные иерархии являются частичными порядками. Частичный порядок это рефлексивное, транзитивное и антисимметричное отношение. Наследование является рефлексивным из-за того, что роль наследует свои разрешения, транзитивность является естественным условием в данном контексте, а правила антисимметрии указывают на то, какие роли наследуют друг от друга и могут поэтому стать лишними.

Следующее определение формулирует КДОР 1.

Определение 2.

Модель КДОР 1 имеет следующие компоненты:

U, R, P, S, PA, UA, а также пользователь остались неизменными от КДОР 0,

RH$\subseteq$R$\subseteq$R является частичным порядком R, называемым иерархией ролей или отношением доминирования ролей, записываемым как $\geq$, и

roles : S$\rightarrow 2^R$ усовершенствовано по сравнению с КДОР 0 и требует, чтобы roles(S_i)$\subseteq$

$\{r \mid (\exists\ r' \geq r)[(\text{user}(S_i), r') \in \text{UA}]$ (может меняться со временем) и сеанс S_i имеет разрешения $U_{R \in Roles(S_i)} \{p \mid (\exists r'' \leq r)[(p, r'')] \in PA\}$.

Следует отметить, что пользователю разрешается начинать сеанс с любой комбинацией ролей, второстепенных по сравнению с той, членом которой пользователь является. Также, разрешения в сеансе или непосредственно связаны с определенными ролями, или же связаны с ролями, второстепенными по отношению к данным ролям.

Иногда представляется целесообразным ограничивать путь наследования в иерархиях. Рассмотрим иерархию на иллюстрации 2 (b), где роль руководителя проекта является главенствующей по отношению как к тестирующему инженеру, так и программисту. Теперь представим, что тестирующие инженеры решили держать ряд ролей в качестве принадлежащих только их роли и не допустить их наследования руководителями проекта в иерархии. Данная ситуация может существовать абсолютно правомочно, например, когда доступ к незавершенной работе может быть нежелателен для главенствующей роли, и КДОР данном случае может быть полезным для предоставления права доступа только тестирующим инженерам. Данная ситуация может быть решена путем определения новой роли «тестирующий инженер 0» и отнесения ее к тестирующему инженеру, как показано на иллюстрации 2 (c). Разрешения, принадлежащие только тестирующим инженерам, могут быть даны роли тестирующего инженера 0. Тестирующие инженеры активируют роль тестирующего инженера 0 и наследуют разрешения от роли тестирующего инженера, которые передаются вверх по иерархии до роли руководителя проекта. Разрешения тестирующего инженера 0, однако, не наследуются ролью руководителя проекта. Мы называем такие роли, как роль тестирующего инженера 0 частными ролями. Иллюстрация 2 (c) также показывает частную роль программиста 0. В некоторых системах эффект частных ролей достигается блокированием наследования вверх определенных разрешений. В данном случае иерархия неаккуратно отражает распределение разрешений. Поэтому рекомендуется вводить частные роли и тем самым предотвращать нарушение иерархических отношений.

Иллюстрация 3 показывает в общих чертах, как может быть построена частная подыерархия ролей. Иерархия на иллюстрации 3 (a) имеет 4 задачи, T1, T2, T3 и T4, все из них наследуют разрешения от роли P, являющейся общей для всего проекта. Роль S на вершине иерархии предназначается для руководителей проекта. Задачи T3 и T4 являются субпроектом, с общей субпроектной ролью P3 и руководящей субпроектной ролью S3. Роль $T1'$ субпроект, представленный на иллюстрации 3 (a) и состоящий из ролей S3, T3, T4, P3, требует наличия частной подыерархии, внутри которой частные разрешения проекта могут передаваться без наследования S. Полная подыерархия показана на иллюстрации 3 (c). Разрешения, наследуемые S, могут соответственно передаваться S3,T3,T4,P3, , в то время, как частные разрешения передаются $S3', T3', T4', P3'$ и могут наследоваться ими лишь в рамках субпроекта. Как и раньше, члены субпроекта непосредственно соотносятся с $S3', T3', T4', P3'$. Рисунок 3 (c) разъясняет, какие частные роли существуют в системе и помогает в мониторинге доступа при определении природы частного разрешения.

4.3. Ограничения

Модель КДОР 2 внедряет понятие ограничивающих условий, как это показано на рисунке 1 (b). Несмотря на то, что мы назвали свои модели КДОР 1 и КДОР 2, в этом не заложено какой-либо обязательной прогрессии. Можно первоначально внедрить как ограничивающие условия, так и иерархии ролей. Это показывается неотождествляемым отношением между КДОР 1 и КДОР 2 на рисунке 1 (a).

Ограничивающие условия являются важным аспектом КДОР и очень часто считается, что они являются основной функцией КДОР. Часто приводят пример разъединенных ролей, например, менеджера по закупкам и менеджера по счетам кредиторов. В большинстве организаций (исключая самые малые) одному человеку не разрешается занимать обе роли, так как это может дать повод к мошенничеству. Это — широко известный и зарекомендовавший себя принцип, называемый разделение обязанностей.

Ограничения являются мощным механизмом определения организационной стратегии на высоком уровне. При объявлении каких-либо ролей взаимоисключающими отпадает необходимость заботиться о назначении отдельных

пользователей на эти роли. Эти функции могут быть впоследствии переданы и децентрализованы без боязни подвергнуть опасности цели общей стратегии безопасности организации. Если управление КДОР сосредоточено полностью в руках одного работника службы безопасности, ограничительные условия являются чрезвычайно полезными; однако, тот же эффект может быть достигнут благоразумными действиями офицера безопасности. Однако, если управление КДОР децентрализовано (как это будет описано ниже), ограничения становятся механизмом, с помощью которого старшие офицеры безопасности могут ограничивать возможности пользователей, имеющих административные привилегии. Это позволяет главному офицеру безопасности определить широкий спектр того, что является допустимым, и сделать этот список обязательным для других офицеров безопасности и пользователей, участвующих в управлении КДОР.

По отношению к КДОР 0 ограничительные условия могут применяться в отношениях UA и PA и функциях пользователя и роли в различных сеансах. Ограничения являются предикатами, которые при применении в данных отношениях и функциях, возвращают значение «возможно» / «невозможно». Ограничения можно также рассматривать как предложения в каком-то определенном формальном языке. По интуиции, ограничительные условия лучше рассмтаривать согласно их типу и природе. Мы обсуждаем ограничения неформально, а не в их формальном понимании. Поэтому мы приходим к следующему определению.

Определение 3

КДОР 2 не отличается от КДОР 0, кроме как в требовании о наличии совокупности ограничений, определяющих возможность использования тех или иных значений и различных компонентов КДОР 0. Разрешены для использования только приемлемые значения. Требования функционирования обычно предусматривают наличие упрощенных ограничительных условий, которые можно эффективно проверить и использовать. В КДОР упрощенные ограничения можно использовать. Перейдем к обсуждению некоторых ограничительных условий, которые, на наш взгляд, стоит внедрить. Большинство, если не все, ограничения, используемые в отношении разделения пользователей, имеют аналоги,

используемые в отношении распределения разрешений. В связи с этим, мы рассматриваем ограничения параллельно по этим двум компонентам.

Наиболее часто упоминающееся ограничительное условия в контексте КДОР — это взаимоисключающие роли. Один и тот же пользователь может быть закреплен только за одной ролью в множестве взаимоисключающих ролей. Это поддерживает разделение обязанностей. Требования данного ограничения практически не нужно обосновывать. Двойное ограничение на распределение разрешений практически не встречается в источниках. На самом деле, ограничение взаимоисключения на распределение разрешений может усилить разделение обязанностей. Данное двойное ограничение требует, чтобы одно разрешение могло быть закреплено не более, чем за одной ролью в множестве взаимоисключающих ролей.

Рассмотрим пример двух взаимоисключающих ролей — бухгалтера и менеджера по закупкам. Взаимоисключение по принципам UA означает, что один человек не может быть членом обеих ролей. Взаимоисключение по принципам PA уточняет, что одно и то же разрешение не может быть закреплено за обеими ролями. Например, разрешение выписывать чеки не должно распространяться на обе роли. Обычно подобное разрешение выдается роли бухгалтера. Ограничение взаимоисключения PA предотвращает злоумышленное закрепление данной роли за ролью менеджера по закупкам. То есть, ограничения исключения по PA являются полезным инструментом ограничения распределения важных разрешений. Например, не важно, кто получит право подписи для определенного счета — роль A или B, более важно требование того, чтобы обе роли не получили данное разрешение.

Если обобщить, то членство пользователей в различных комбинациях ролей может быть как приемлемым, так и неприемлемым. Поэтому, может быть приемлемым для одного пользователя быть членом ролей программиста и испытателя в разных проектах, но неприемлемым в одном проекте. То же самое можно сказать и о распределении разрешений. Другим примером ограничения на закрепление пользователей может быть ограничение максимального количества членов определенной роли. Например, в роли руководителя управления может

находиться только один человек. Точно так же можно ограничить число ролей для одного пользователя. Мы называем подобные ограничительные условия кардинальными. Соответственно, количество ролей, за которыми закрепляется разрешение, может иметь кардинальные ограничения для контроля распределения важных разрешений. Следует отметить, что минимальные кардинальные ограничения может быть трудно исполнить. Например, если существует минимальное количество исполнителей роли, что будет делать система, если один из них исчезнет? Как система узнает об этом?

Понятие предварительных ролей основано на компетентности и соответствии, то есть пользователь может исполнять роль A только, если он уже является членом роли B. Например, только те пользователи, которые уже являются членами роли проектирования, могут быть допущены к роли испытателя внутри данного проекта. В данном примере предварительная роль является второстепенной по отношению к новой принимаемой роли. Предварительные условия между несравнимыми ролями практически не встречаются. Двойное ограничение на распределение разрешений обычно используется по отношению ко второй половине цепочки ролей в отношении PA. Представляется целесообразным требовать закрепления разрешения p за ролью только в том случае, если роль уже имеет разрешение q. Например, во многих системах разрешение на чтение файла требует наличия разрешения на чтение директории, в которой расположен этот файл. Закрепления первого разрешения без второго недостаточно.

Ограничения на закрепление пользователей эффективны, только если поддерживается должная внешняя дисциплина в закреплении идентификаторов пользователей за людьми. Если за одним и тем же человеком закреплены два или более идентификатора, происходит поломка контроля разделения и кардинальности. Между идентификаторами пользователей и людьми должны быть установлены отношения один-к-одному. Подобный аргумент работает и при ограничении разрешений. Если одна и та же операция санкционируется двумя различными разрешениями, система КДОР не может эффективно использовать ограничения кардинальности и разделения.

Ограничительные условия могут применяться по отношению к сеансам, а также к функциям пользователя и роли, связанным с сеансом. Вполне возможно, что пользователь является членом двух ролей, главное — то, что он не может активировать обе роли одновременно. Другие ограничения сеансов могут ограничивать количество сеансов, которые пользователь может активировать одновременно. Соответственно, можно ограничить и количество сеансов, за которыми закреплено разрешение.

Иерархия ролей может также рассматриваться как ограничительное условие. Ограничение заключается в том, что разрешение, выданное второстепенной роли, должно быть выдано всем главенствующим ролям. Или наоборот, ограничение может заключаться в том, что пользователь, закрепленный за главенствующей ролью, должен также быть закреплен за всеми второстепенными ролями. В некотором смысле, КДОР 1 является ненужным и поглощенным КДОР 2. Тем не менее, мы считаем целесообразным признать существование иерархии ролей как таковой. Она может быть понижена до ограничительных условий только путем ввода ненужности распределения разрешений или распределения пользователей. Предпочтительным является поддерживать иерархии напрямую, а не косвенно, путем ненужного распределения.

4.4 сводная модель

КДОР 3 объединяет КДОР 1 и КДОР 2 для обеспечения наличия как иерархий ролей, так и ограничительных условий. Существует ряд проблем, возникающих при одновременном использовании обоих понятий. Ограничения могут применяться к самой иерархии ролей, как показано пунктирной стрелкой по направлению к RH на иллюстрации 1 (b). Иерархия ролей должна быть частичного порядка.

Данное ограничение является сущностным для данной модели. Дополнительные ограничения могут ограничить количество главенствующих (или второстепенных) ролей для определенной роли. Две или более роли могут также быть ограничены и не иметь общей главенствующей (или второстепенной) роли. Подобные типы ограничений полезны в ситуациях, когда полномочия изменения

иерархии ролей децентрализованы, однако при этом старший офицер безопасности хочет усложнить саму процедуру проведения подобных изменений.

Между ограничениями и иерархиями существует ряд незаметных взаимоотношений. Предположим, что роли тестирующего инженера и программиста объявлены взаимоисключающими в контексте рисунка 2 (b). Роль руководителя проекта нарушает данное взаимное исключение. В некоторых случаях подобное нарушение взаимного исключения главенствующей ролью может быть допущено, хотя в других случаях подобное будет невозможным. Мы считаем, что данная модель не должна исключать ни одну из этих возможностей. Подобная ситуация возникает и при рассмотрении кардинальных ограничений. Предположим, что пользователь закреплен не более чем за одной ролью. Нарушает ли подобное ограничение назначение роли тестирующего инженера на рисунке 2 (b)? Другими словами, относятся кардинальные ограничения только к непосредственному членству или же они также передаются и унаследованному членству?

Иерархия на рисунке 2 (c) показывает, как ограничительные условия могут быть полезны при наличии частных ролей. В данном случае роли тестирующего инженера 0, программиста 0 и руководителя проекта могут быть объявлены взаимоисключающими. Так как у них не имеется общей главенствующей роли, то конфликт отсутствует. В общем, частные роли не будут иметь общих главенствующих ролей с другими ролями, так как они являются максимальными элементами иерархии. Поэтому взаимное исключение частных ролей может всегда быть уточнено без конфликта. Общий аналог частных ролей может быть объявлен как имеющий максимальное кардинальное ограничение нулевых членов. В таком случае тестирующие инженеры должны быть закреплены за ролью тестирующего инженера 0. Роль тестирующего инженера служит в качестве инструмента совладения разрешениями вместе с ролью руководителя проекта.

5. Модели управления

До настоящего времени мы предполагали что все компоненты КДОР находятся под непосредственным контролем со стороны одного офицера службы безопасности. В крупных системах количество ролей может достигать сотен и

тысяч. Управление этими ролями и их взаимоотношениями — трудная задача, которой обычно занимается небольшая команда администраторов безопасности.

Принимая во внимание, что основным преимуществом КДОР является упрощение процесса управления разрешениями, естественно возникает вопрос, как КДОР может быть использован для управления самим КДОР? Мы считаем, что использование КДОР для управления самим КДОР будет важным фактором в успехе КДОР. Ниже мы остановимся лишь на основных положениях данного вопроса.

Мы упомянули некоторые подходы к управлению контролем доступа, обсуждаемые в литературе. ISO разработало ряд стандартов и документов, связанных с управлением безопасностью. С ними можно ознакомиться через документацию Обзора Системного Управления [11]. Модель ISO является ориентированной на объект и включает иерархию, основанную на содержании (директория содержит файлы, а файл содержит записи). В подход ISO можно встроить и роли.

Существуют традиционные модели передачи прав доступа, в которых право передавать права контролируется с помощью специальных прав контроля. Одной из наиболее новых и разработанных является матричная модель символического доступа, разработанная Сандху [12]. И хотя очень часто представляется трудным анализировать последствия даже простейших правил передачи прав, данные модели показывают, что простые решения можно объединять для получения очень гибких и быстрых систем.

Одним из примеров работы по управлению КДОР является труд Мофле и Сломана [13], которые определяют хорошо разработанную модель, основанную на доменах ролей, владельцах, управляющих и администраторах безопасности. В их работе полномочия не контролируются или осуществляются из одной центральной точки, а согласовываются между независимыми управляющими, не испытывающими большого доверия друг к другу.

Наша модель управления КДОР показана на иллюстрации 4. Верхняя половина этой иллюстрации очень похожа на иллюстрацию 1 (b). Ограничения в иллюстрации 4 относятся ко всем компонентам. Нижняя часть иллюстрации 4

является зеркальным отражением верхней части для административных ролей и административных разрешений. Представляется целесообразным отделить административные роли AR и административные разрешения AP от соответственно обычных ролей R и разрешений P. Данная модель показывает, что разрешения могут быть даны только ролям, а административные разрешения — только административным ролям. Это — встроенное ограничительное условие.

Верхняя половина иллюстрации 4 может изменяться в сложности по мере перехода от КДОР 0, КДОР 1, КДОР 2 к КДОР 3. Нижняя часть также изменяется в сложности от АКДОР 0, АКДОР 1, АКДОР 2 до АКДОР 3, где А означает административный. В общем, мы ожидаем, что административная модель будет проще, чем сама модель КДОР. Поэтому можно будет использовать АКДОР 0 для управления КДОР 3, однако не целесообразно использовать АКДОР 3 для управления КДОР 0.

Также важно признать, что ограничения могут переходить из верхней части иллюстрации 4 в нижнюю, и обратно. Мы уже пришли к выводу о существовании встроенного ограничительного условия, согласно которому разрешения могут быть даны только ролям, а административные разрешения — только административным ролям. Если административные роли являются взаимоисключающими по отношению к обыкновенным ролям, что у нас появляется ситуация, когда администраторы безопасности могут управлять КДОР, но при этом сами не пользоваться привилегиями.

Что касается управления административной иерархией, то в принципе можно построить административную иерархию второго уровня для управления первым уровнем и так далее. По нашему мнению, даже второй уровень административной иерархии не нужен. Поэтому управление административной иерархией может быть возложено на одного старшего офицера безопасности. Этот вывод разумен для одной организации или одной административной единицы внутри организации. Вопрос того, как эти единицы взаимодействуют друг с другом, в нашей модели не рассматривается.

Административные полномочия в КДОР могут рассматриваться как возможность изменения распределения пользователей, распределения разрешений и

отношений в иерархии ролей. В модели управления следует четко определить разрешения на подобные административные операции. Четкая природа данных разрешений является специфической и зависит от применения, однако их общая природа во многом едина.

Одной из основных проблем в модели управления является круг административных полномочий, переданных административным ролям. В качестве примера рассмотрим иерархии, показанные на рисунке 3 (a). Административная иерархия рисунка 3 (b) показывает роль одного старшего офицера безопасности (CSO), которая является главенствующей по отношению к трем ролям офицеров безопасности SO1, SO2, SO3. Вопрос в том, какие роли рисунка 3 (a) будут управляться теми или иными ролями рисунка 3 (b). Допустим роль CSO может управлять всеми ролями рисунка 3 (a). Допустим SO1 работает по задаче T1. В общем, мы не хотим, чтобы SO1 автоматически наследовал способность также управлять второстепенной ролью P. Поэтому круг полномочий SO1 может быть полностью ограничен T1. Таким же образом, круг SO2 ограничен T2. Допустим, SO3 может управлять целым подпроектом, состоящим из S3, T3, T4, P3. Круг SO3, тогда, ограничен сверху S3, снизу — P3.

В общем, каждая административная роль может быть соотнесена с определенным подмножеством в иерархии ролей, за управление которым она отвечает. Необходимо также очертить ряд других аспектов управления. Например, SO1 может только добавлять пользователей в роль T1, однако для их удаления требуется вмешательство CSO. То есть, нам необходимо очертить не только роли, управляемые административными ролями, но и также разрешения и пользователей, управляемых ролью. Также важно контролировать изменения в самой иерархии ролей. Например, из-за того, что SO3 управляет подыерархией между S3 и P3, SO3 может быть уполномочен добавлять задания в данный субпроект.

6. Заключение

Мы представили семейство моделей КДОР, системно развивающихся от простого к сложному. Данные модели предоставляют общую структуру для дальнейшего исследования в данной области. Мы также представили модель

управления, с помощью которой КДОР может контролировать себя. Это подтверждает нашу позицию о том, что КДОР является стратегически нейтральной моделью.

Многое необходимо сделать для полной реализации потенциала КДОР. Одной из величайших проблем исследования в данной области является разработка системого подхода к созданию и анализу конфигураций КДОР. Последние исследования по созданию и анализу иерархии ролей уже объявлены [8,9,14]. Как было упомянуто выше, в литературе практически не обсуждаются ограничительные условия в контексте КДОР. Была бы полезной категоризация и таксономия ограничений. Следует разработать формальную нотацию для формулировки и введения ограничений, а также измерения трудности введения. Важным открытым полем исследования является возможность анализа ограничений и чистого эффекта конфигурации КДОР в условиях поставленных целей высокоуровневой стратегии. Также необходимо доработать аспекты управления КДОР. Трудностью в исследовании является развитие обобщенной систематизированной методики создания и анализа иерархий ролей, ограничений и управления КДОР. Большинство из этих открытых проблем и вопросов взаимосвязаны и требуют комплексного подхода к их решению.

Литература

[1] Дэвид Феррайоло, Деннис М. Гилберт, Никилин Линч. Анализ стратегических нужд федерального и коммерческого контроля доступа. Материалы национальной конференции NIST-NCSC по компьютерной безопасности, стр. 107-116, Балтимор, Мэриленд, 20-23 сентября 1993.

[2] Редакционная коллегия по общим критериям. Общие критерии оценки технологии информационной безопасности, декабрь 1994. Версия 0.9, проект

[3] Имтияз Мохаммед и Дэвид М. Дилтс. Разработка системы динамической безопасности, основанной на пользовательских ролях. Компьютеры и безопасность, 13 (8): 661-671, 1994.

[4] Рошан Томас и Рави С. Сандху. Концептуальные основания для мождели авторизации, основанной на заданиях. Семинар фондов компьютерной безопасности 7, стр. 66-79, Франкония, Нью-Хэмпшир, июнь 1994.

[5] Рави С. Сандху. Модели контроля доступа, основанные на структуре. IEEE Компьютер, 26(11):9-19, ноябрь 1993.

[6] Дирк Йоншер. Расширение контроля доступа с помощью реализации обязанностей активными механизмами. В журнале Безопасность баз данных VI: Состояние и перспективы, по ред. Б. Турайзингема и С.Е. Ландвера, стр. 91-111. Северная Голландия, 1993.

[7] Дэвид Феррайоло и Ричард Кунн. Контроль доступа, основанных на ролях. Материалы 15ой Национальной конференции NIST-NCSC по компьютерной безопасности, стр. 554-563, Балтимор, Мэриленд, 13-16 октября 1992.

[8] М.Ю. Ху, С.А. Демурьян, and Т.Ц. Тинг. Основанная на пользовательских ролях безопасность в объектно-ориентированном окружении дизайна и анализа ADAM. В Безопасность баз данных VIII: Состояние и перспективы, под ред. Дж. Бискапа, М. Моргенштерна, С. Ландвера. Северная Голландия, 1995.

[9] Матунда Ньянчама и Сильвия Осборн. Управление правами доступа в системе безопасности, основанной на ролях. В Безопасность баз данных VIII: Состояние и перспективы, под ред. Дж. Бискапа, М. Моргенштерна, С. Ландвера. Северная Голландия, 1995.

[10] С.Х. фон Солмс и Исаак ван дер Мерве. Управление профилей компьютерной безопасности с использованием подхода ориентированного на роли. Компьютеры и безопасность, 13 (8): 673-680, 1994.

[11] ISO/IEC 10040. Информационные технологии — Взаимосвязь открытых систем — Обзор управления системами.

[12] Рави С. Сандху. Матричная модель символичного доступа. В материалах Симпозиума компьютерного общества IEEE по безопасности и секретности информации, стр. 122-136, Оклэнд, Калифорния, май 1992.

[13] Джонатан Д. Мофлетт и Моррси С. Сломан. Передача полномочий. В журнале Управление интегрированными сетями II, под ред. И. Кришман и В.

Циммер, стр. 595-606. Научное издательство Elsevier Science Publishers B.V. (Северная Голландия), 1991.

[14] Эдуардо Б. Фернандез, Джи Ву, Минье Х. Фернандез. Структуры пользовательских групп в авторизации объектно-ориентированных баз данных. В Безопасность баз данных VIII: Состояние и перспективы, под ред. Дж. Бискапа, М. Моргенштерна, С. Ландвера. Северная Голландия, 1995.

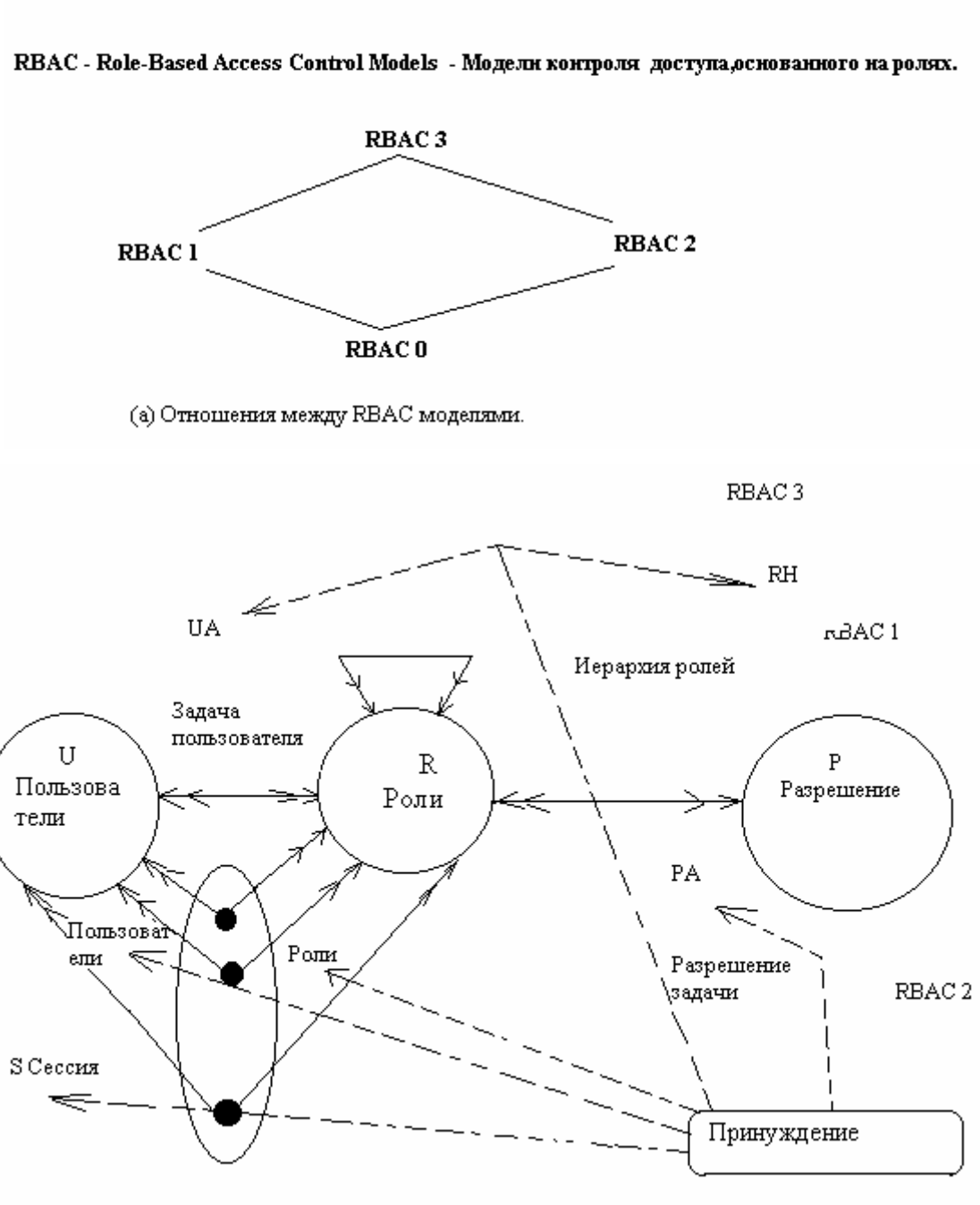


Рисунок 1 — Семейство моделей КДОР

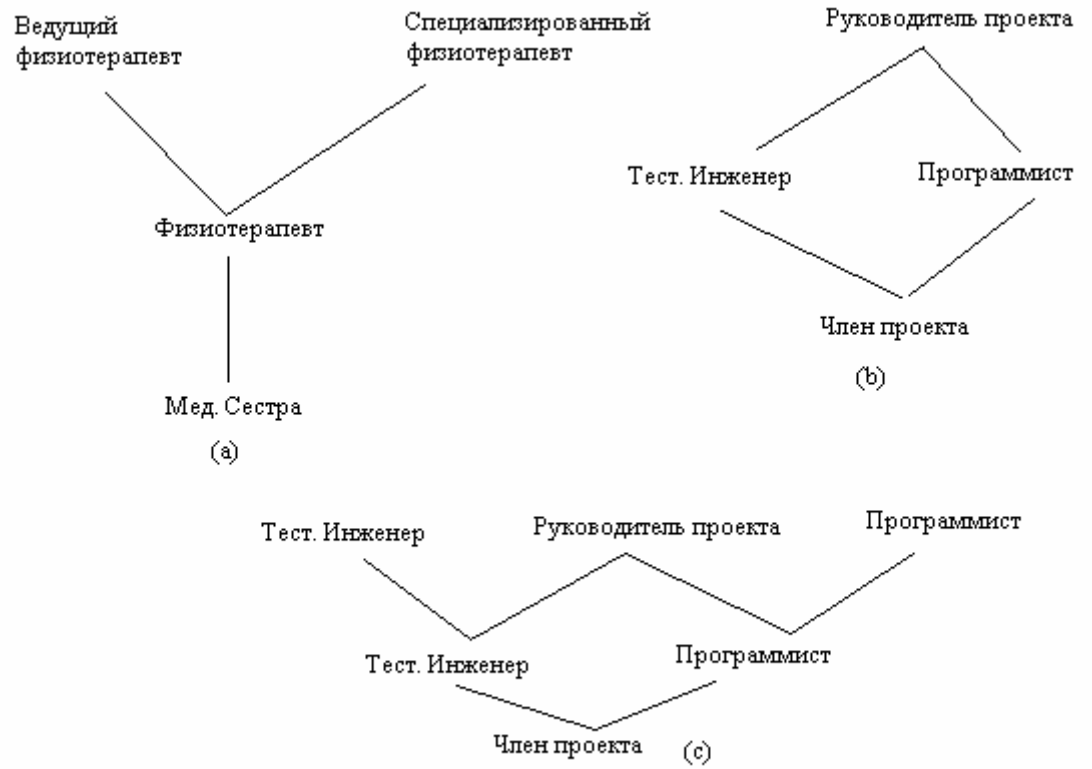


Рисунок 2. Пример иерархий ролей

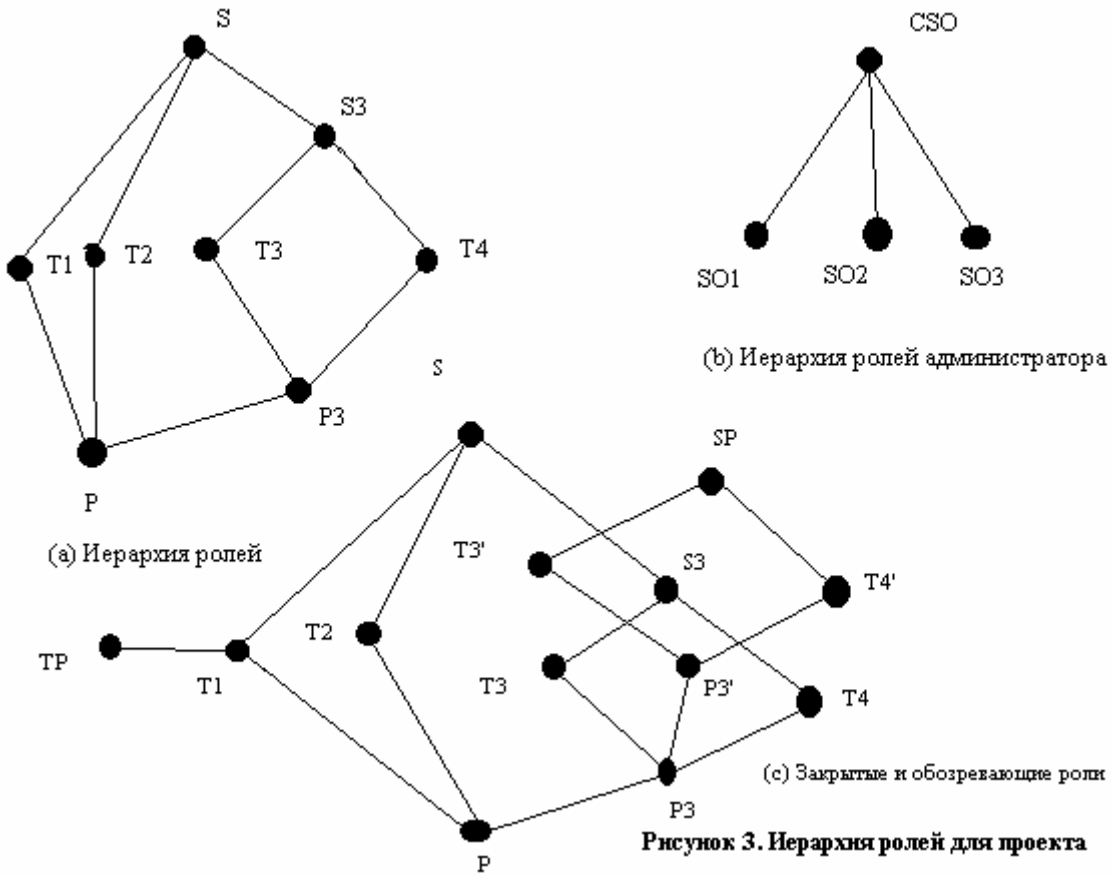


Рисунок 3. Иерархия ролей для проекта

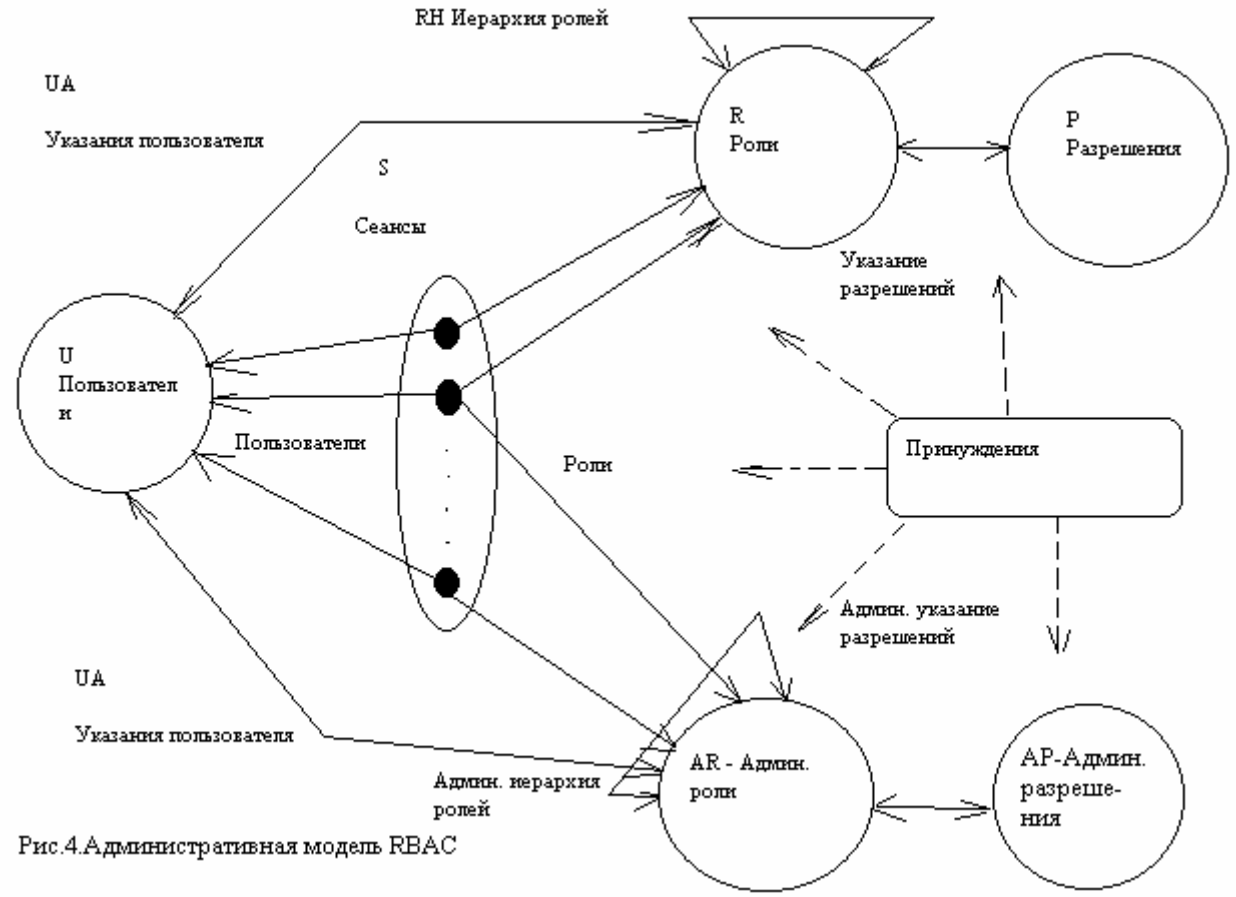


Рис.4.Административная модель RBAC

29 Анализ и управление риском

Понятие риска. Принципы управления риском

[Д. Стенг, С. Мун; 1995]:

“Если люди готовы так напряженно работать, чтобы создавать информацию, то не следует ли приложить хотя бы часть усилий для ее защиты? Когда речь о компьютерной безопасности, следует подавлять естественное желание “не говорить о плохом, не слышать плохого, не думать о плохом и не вспоминать о плохом”. Все предпочитают улыбаться и надеяться, что весь мир делает то же самое”.

Решение проблем безопасности так или иначе связано с определенным риском, который заключается в том, что в обеспечение ЗИ вкладываются слишком малые (или слишком большие) затраты, а возможные последствия (потери) для пользователя (или организации) в результате реализации той или иной угрозы могут оказаться очень большими.

Под риском или степенью риска (risk) понимается величина потерь, которые могут иметь место в случае действия конкретной угрозы или совокупности возможных угроз.

Возможный показатель риска — ожидаемые годовые потери (ALE — Annual Loss Expectancy) — это предполагаемые экономические потери, которые ожидаются от возможных происшествий и включают в себя потери от всех ценностей как материальных, так и нематериальных.

Анализ опасностей (risk analysis), или оценка риска (risk assesment) — определение вероятностей угроз и потенциальных потерь, которые могут произойти вследствие изъянов системы.

[Дэвид Стенг, президент и исполнительный директор; Сильвия Мун, специалист по информационным технологиям, Norman Data Defense Systems, Inc.: ”Секреты безопасности сетей”, с. 35]:

“Безопасность информации — это наука. В общем случае проблема решается не путем применения того или иного продукта, безопасность обеспечивается людьми, которые соблюдают планы, правила, процедуры”.

“Теория обеспечения безопасности — это царство теории вероятностей и математической статистики”.

3 фундаментальных вопроса:

- ЧТО ЗАЩИЩАТЬ?
- ОТ ЧЕГО ЗАЩИЩАТЬ?
- КАК ЗАЩИЩАТЬ?

[Хоффман Л. Дж. Современные методы ЗИ. — М.:Мир, 1980]:

“Анализ риска не обеспечивает абсолютную безопасность системы. Анализ риска представляет собой просто систематический подход к разбиению на категории угроз безопасности данных и мер противодействия этим угрозам и к принятию решения относительно плана действий, в соответствии с которым большая часть ресурсов (технических и нетехнических) будет затрачиваться на уменьшение наиболее вероятных или приносящих наибольший ущерб угроз (рисков).

Анализ риска — обеспечивает такую степень безопасности, системы, которая соизмерима с характеристиками защищаемой информации и с величиной ресурсов, которые могут быть затрачены”.

Определение системных ценностей (assets)

Это центральная часть процесса анализа опасностей, которая позволяет выявить все, что нуждается в защите, и определить его ценность.

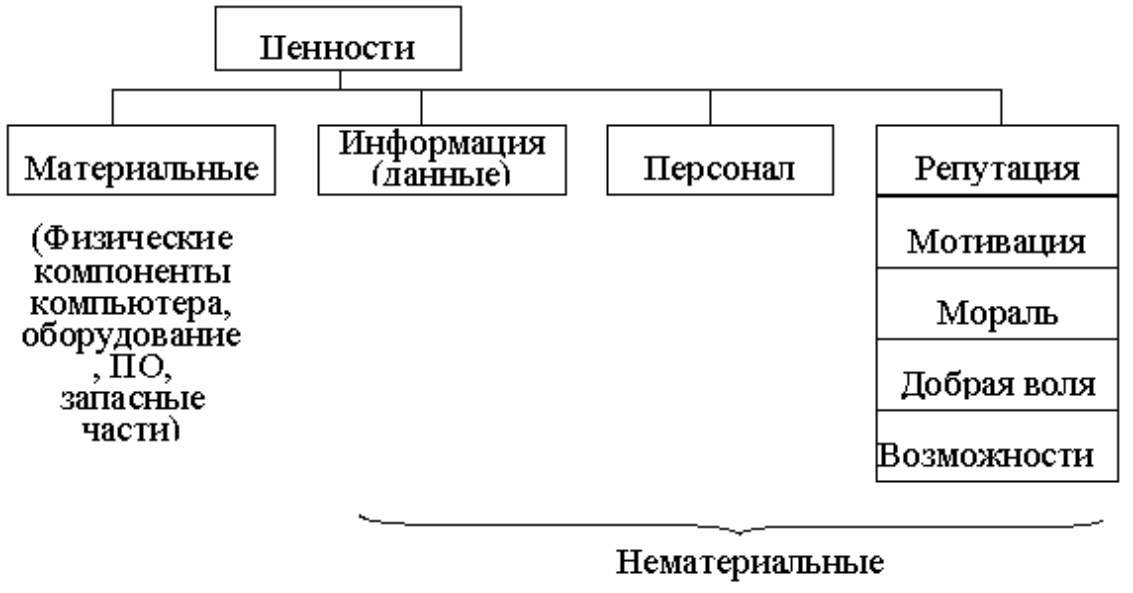


Рисунок — Классификация ценностей

Ожидаемые годовые потери (Annual Loss Expectancy)

Это предполагаемые экономические потери, которые вы ожидаете от происшествий с компьютерными системами или сетями в течение года. Следовательно, они должны включать потери от всех ценностей — как материальных, так и нематериальных.

Выбор мер обеспечения безопасности зависит от видов ценностей и их функций. В частных предприятиях и гражданских правительственных учреждениях основное внимание необходимо уделять доступности целостности информации, тогда как в военных учреждениях на первом месте должно стоять обеспечение конфиденциальности.

При выборе мер обеспечения безопасности руководители должны обратить внимание на области с наибольшими потенциальными потерями. Эффективность с точки зрения стоимости означает, что расходы на внедрение и поддержку мер безопасности не должно превышать стоимость потенциальных потерь, от которых эти меры предохраняют.

Управление риском (risk management)

Это весь спектр мероприятий (а также физический, технический, административный контроль и процедуры), которые приводят к эффективным решениям в области безопасности.

Целью управления риском является поиск наиболее эффективных мер предосторожности от случайных, преднамеренных атак против компьютерной системы.

В программу управления риском входят 4 обязательных элемента:

Рисунок — Программа управления риском

Выбор мер обеспечения безопасности (safeguard selection)

Это важная функция управления риском. Руководители должны проводить мероприятия направленные на устранение конкретной угрозы. Как правило, снижение вероятности угрозы до нуля не выгодно с точки зрения стоимости, т.к. при приближении вероятности к нулю расходы повышаются. Руководителям необходимо определить приемлемый уровень риска и установить эффективные (с точки зрения стоимости) меры безопасности для уменьшения потерь до заданного уровня. Меры могут быть предприняты в таких направлениях:

- уменьшение вероятности возникновения угрозы;
- уменьшение разрушительного воздействия при возникновении угрозы;
- облегчение восстановления после возникновения угрозы.

Конечной целью анализа опасностей является помощь в выборе наиболее эффективных (прежде всего, по стоимости) мер безопасности, обеспечивающих снижение риска до приемлемого уровня.

Вычисление показателя степени риска

1. Министерством обороны США используется следующий подход к вычислению показателя степени риска, который может использоваться в любой организации. Следовательно, учитываются два ключевых фактора: доверие к

пользователям системы и критичность данных в этой системе. Используются следующие предельные значения этих факторов: наименее безопасный пользователь, с одной стороны, и наиболее критичная информация, с другой.

Вводятся следующие категории и их значения:

- Непрозрачная: 0
- Непрозрачная, но разрешен доступ к важной негрифованной информации: 1
- Конфиденциальная: 2
- Секретная: 3
- Совершенно секретная / текущее закрытое исследование: 4
- Совершенно секретная / текущее специальное закрытое исследование: 5
- Единичная категория: 6
- Множественная категория: 7

Простая для применения система классификации использует следующие категории информации:

- Открытая — не требует защиты (ежегодные отчеты, информационные письма, материалы по исследованию рынка).
- Для служебного пользования — не требует защиты, обеспечивая сохранность информации, хранящейся внутри компании (процедуры, стратегии, стандарты, памятки, книги внутренних телефонов организации).
- Ограниченная — включает любую информацию, раскрытие которой не в интересах организации (данные о клиентах, компьютерное ПО, документация, данные о персонале и бюджетная информация).
- Конфиденциальная — включает все, что может серьезно повредить компании при разглашении (документы стратегического планирования, рыночные стратегии, собственное ПО).

Таблица — Максимальная оценка критичности данных

Классификация	Ранжирование без категорий	Ранжирование с категориями
Открытая	0	Не применяется
Для служебного	1	С одной и более категориями: 2

пользования		
Конфиденциальная	2	С одной и более категориями: 3
Секретная	3	С одной и более категориями, содержащими секретные данные: 4
		С одной и более категориями, содержащими секретные данные: 5
Совершенно секретная	5	С одной и более категориями или категориями 0 и 1, содержащими секретные или совершенно секретные данные: 6
		С двумя и более категориями, содержащими секретные или совершенно секретные данные: 7

Согласно подхода Министерства обороны США, если рейтинг доверия к пользователю меньше рейтинга критичности, показатель степени риска представляет собой абсолютную разность этих значений. Таким образом, система, создающая совершенно секретную информацию в двух и более категориях и имеющая небезопасного пользователя, будет иметь индекс риска 7-0 = 7. Индекс риска равен 1, если система имеет категории, к которым некоторые пользователи не имеют доступа, но минимальная безопасность пользователя меньше, чем максимальная критичность данных. В противном случае, индекс риска равен 0.

Анализ опасностей

Конечной целью анализа опасностей является помощь в выборе наиболее эффективных (прежде всего, по стоимости) мер безопасности, обеспечивающих снижение риска до приемлемого уровня.

Элементы анализа степени риска:

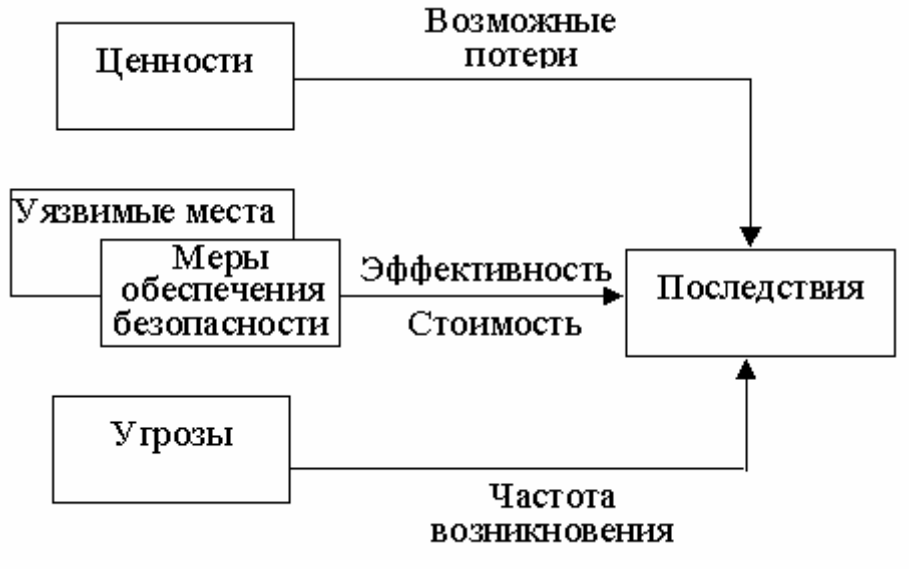


Рисунок — Элементы анализа степени риска

Анализ степени риска включает в себя следующие этапы:

а) этап идентификации ценностей (какие ценности являются существенными, их значимость для организации);

б) идентификация угроз, представляющих потенциальную опасность для ценностей;

в) оценка уязвимости (т.е. выявление уязвимых мест, которые могут привести к ущербу при возникновении опасности):

$\Rightarrow$ 2 вида уязвимых мест:

1. слабость принятия защитных мер, которые допускают нанесение ущерба конфиденциальности, целостности или ценности;
2. отсутствие средств защиты или процедур контроля, которые должны предотвратить нарушение безопасности;

г) оценка эффективности **защитных мероприятий**, в т.ч. следующих средств защиты:

1. безопасность управления;
2. физическая безопасность;
3. безопасность ПО;
4. безопасность аппаратных средств;
5. безопасность персонала;

6. безопасность окружающей среды;
7. безопасность коммуникаций;

д) определение потенциальных потерь.

[Д. Стенг, С. Мун, стр.49]:

“Не доверяйте собственным эмоциям в оценке уязвимости вашей сети (системы). Вы можете её измерить. Хотя решение этой проблемы всегда связано с субъективизмом, не стоит полагаться на собственную интуицию и прибегать к догадкам. Если обеспечение безопасности перестает быть искусством и обретает строго научную основу, то переход от интуитивных оценок к точному измерению просто необходим.

К сожалению, не всегда удается точно измерить степень безопасности сети. Источником осложнения могут быть:

- отсутствие большого опыта такого роды измерений;
- недостаточная осведомленность о методах измерения безопасности;
- наличие ряда конкурирующих методов, каждый из которых достоинства и недостатки;
- сложность вычислительных систем вообще”

Стр. 36: “Сплошь и рядом ресурсы тратятся на защиту от опасностей, не представляющих особой угрозы, в то время как настоящим опасностям не уделяется никакого (или почти никакого) внимания. До тех пор, пока руководители не осознают значимость проблемы и не увидят те области, которые в наибольшей степени подвержены опасности, защита главных компьютерных ресурсов будет бестолковым, нерациональным и расточительным занятием”.

Методика измерения потерь — применяет оценку величин методом последовательных приближений, нечеткую логику рассуждений, деревья событий и ошибок.

Управление риском: Риск. Устойчивое развитие

[Синергетика/ В.А. Владимиров, Ю.Л. Воробьев, С.С. Салов и др. — М.: Наука, 2000–-431 с.]

Введение

Цель книги — обратить внимание на проблемы стратегии управления рисками, поскольку стратегии ошибок являются самыми дорогими.

- В период Карибского кризиса, в тяжелый момент американской истории Джоном Кеннеди были сказаны крылатые слова: «У меня есть тысячи специалистов, которые могут построить пирамиду, но нет ни одного который сказал бы стоит ли ее строить»

- На основании накопленного в России и в мире опыта строится новая наука — математическая теория безопасности и риска. В качестве методической основы для такой теории могут быть использованы нелинейная динамика, системный анализ и компьютерное моделирование.

Для разработки новых парадигм, концептуальных подходов в области анализа сложных необратимо развивающихся систем (таких как техносфера и биосфера, система международных отношений и экономика), в США создан институт сложности (в Санта–Фе). Его сотрудниками являются лауреаты Нобелевской премии в области физики Гел–Ман и в области экономики Брайен Артур. Следовательно, на повестку дня поставлено построение парадигмы сложности, позволяющей строить теории сложных нелинейных систем, в которых возможны редкие катастрофические события

№5 (стр. 40) ⇒ «Риск» — «Мера опасности»

Риск сочетает в себе вероятность неблагоприятного события и объем этого события (потери, ущерб, убытки)

№ Ситуации	Вероятность возможного события	Ущерб субъекту	Риск
1	P = большая	0	R =0
2	P = 0	Ущерб = велик	R = 0
3	P = 0	0	Абсолютная безопасность

Некоторые принципы управления риском.

(разработаны фирмой Countermeasures Incarparated)

- Все системы можно пострадать от одной и той же популяции угроз. Популяция угроз бесконечна по их числу и разнообразию. В любой системе и в любом месте можно встретить проявление любой угрозы, изменяется лишь вероятность её возникновения.

- На частоту возникновения угрозы нельзя ничем повлиять. Определённые изменения частоты угроз на самом деле являются следствием принимаемых контрмер.

- Уязвимость уменьшается с увеличением количества контрмер. Уровень уязвимости снижается при их применении.

- Каждая контрмера имеет свои уязвимые места, поэтому невозможно достичь нулевого уровня уязвимости.

- С помощью контрмер можно добиться приемлемого уровня уязвимости. Существует набор контрмер, с помощью которого можно достичь любого уровня уязвимости.

Дополнительные принципы.

[Д. Стейн, С. Мун; с.39].

- Все контрмеры потребуют затрат со стороны организации. Расходы на внедрение контрмер, необходимых для достижения приемлемого уровня уязвимости, могут, в свою очередь, оказаться неприемлемыми.

- Чем меньше диапазон допустимых отклонений от необходимого уровня безопасности, тем больше расходы на внедрение и проведение контрмер. С другой стороны, чем больше расходы на контрмеры, тем больше необходима мотивация этих расходов.

- Точно измерить можно только затраты. Частоту возникновения угроз, их серьёзность и возможность предотвращения чаще всего измерить не удаётся. Выбор контрмер всегда требует потратить осязаемое (реальные расходы в связи с применением контрмер) на неосязаемое (потенциальные потери).

30 Общие принципы проектирования систем защиты информации.

1 Системный подход

а) Главная цель — обеспечения качества информации (а не ЗИ как самоцель):

– конфиденциальность;

– целостность;

– достоверность, адекватность, точность;

б) Учёт всех факторов в их взаимосвязи;

Построение системы ЗИ (т.е. комплексное использование имеющихся в распоряжении средств).

2 Типовая концепция ЗИ в АСОД

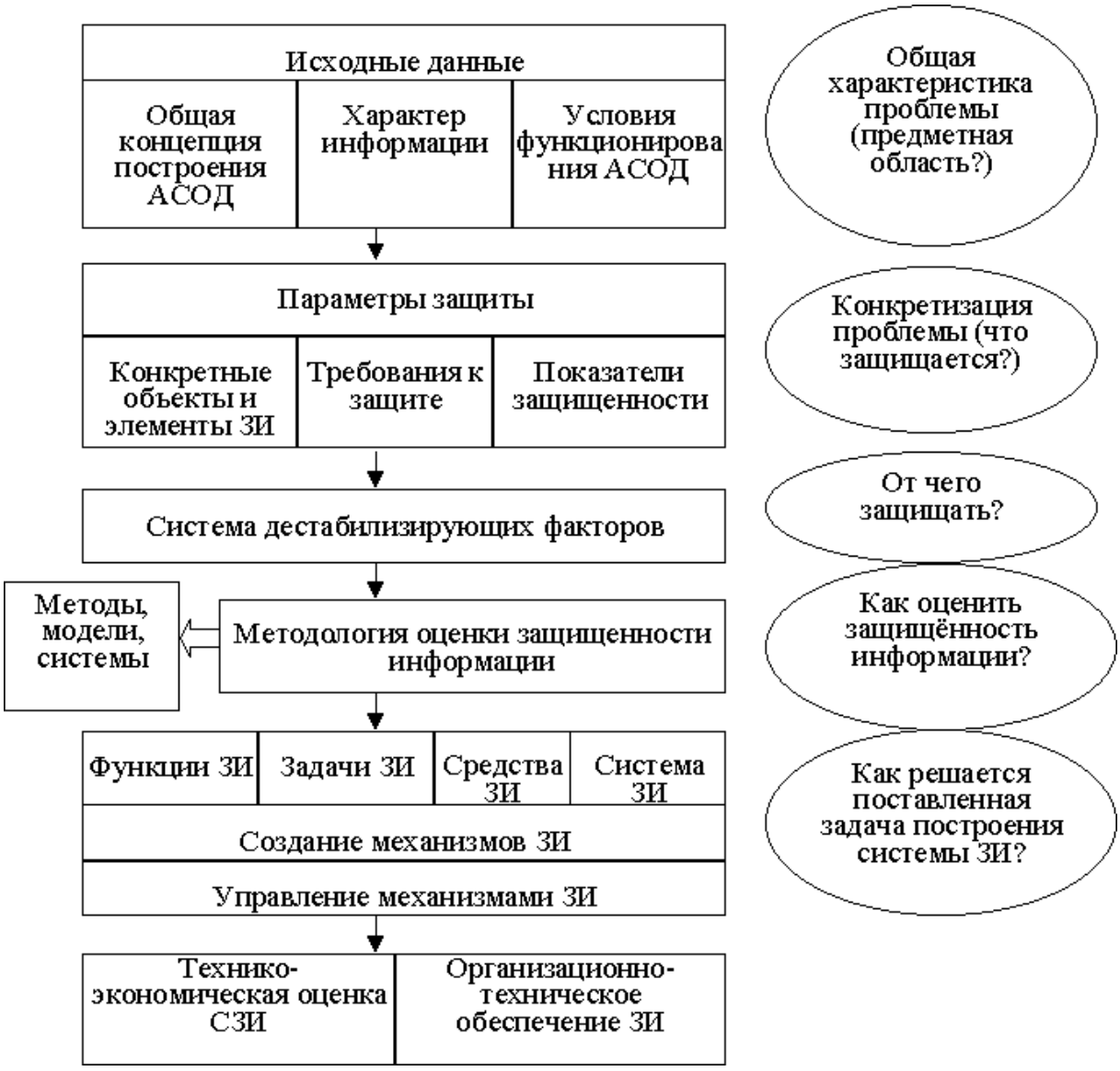


Рисунок — Типовая концепция ЗИ в АСОД

Функции ЗИ — конкретные мероприятия по ЗИ.

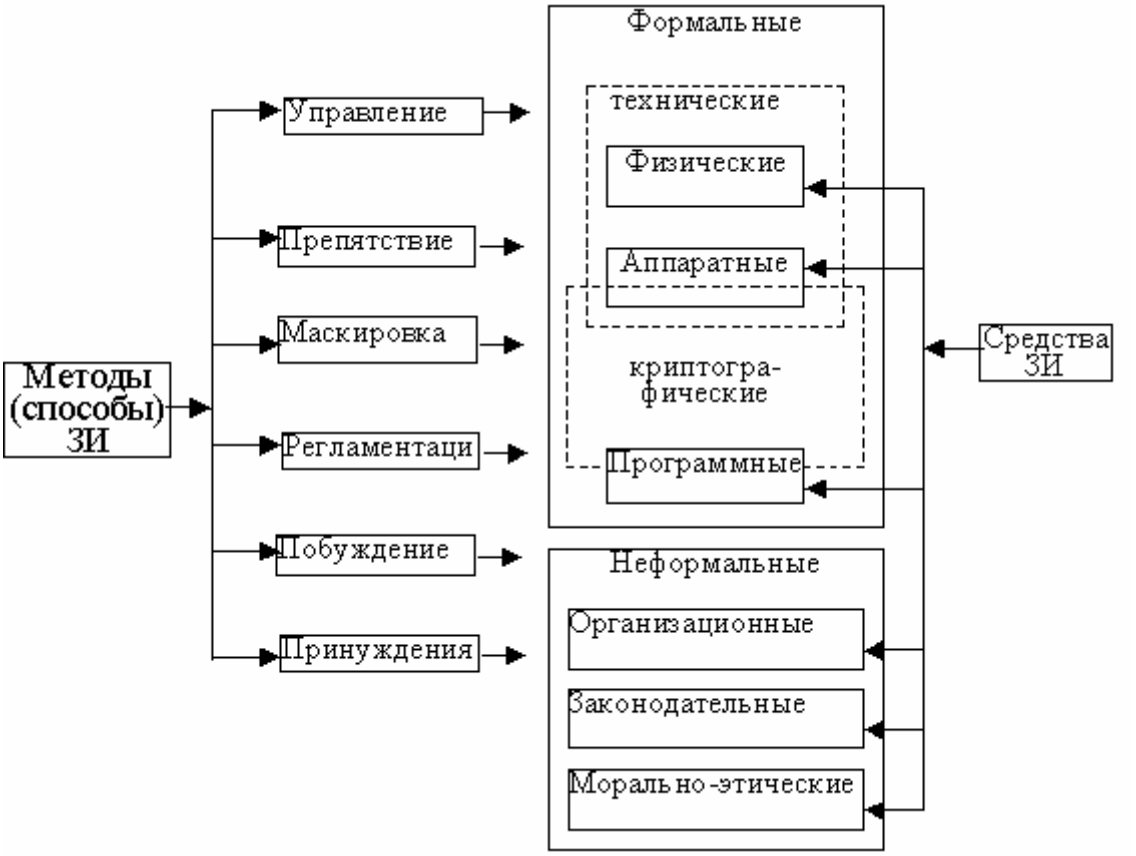
Задачи ЗИ — возможности средств методов и мероприятий, определение перечня каналов НСД(утечки) информации.

Средства ЗИ — устройства, программы, мероприятия.

Система ЗИ — совокупность всех мероприятий по ЗИ.

31 Выбор мер обеспечения безопасности. Методы и средства ЗИ

1)Классификация методов и средств ЗИ:



Управление — регулирование использования всех ресурсов системы в рамках установленного технологического цикла обработки и передачи информации, где в качестве ресурсов рассматриваются технические средства, ОС, программы, БД, элементы данных и т.п. Осуществляется путём целенаправленного воздействия подсистемы управления системы обеспечения безопасности информации (СОБИ) на средства и механизмы ЗИ и компоненты ИВС с целью обеспечения безопасности информации.

Препятствия — физически преграждают нарушителю путь к защищаемой информации.

Маскировка — метод ЗИ путём их криптографического закрытия.

Регламентация — разработка и реализация в процессе функционирования ИВС комплексов мероприятий, создающих такие условия технологического цикла обработки информации, при которых минимизируется риск.

Регламентация охватывает как структурное построение ИВС, так и технологию обработки данных, организацию работы пользователей и персонала сети.

Побуждение — создание такой обстановки и условий, при которых правила обращения с защищенной информацией регулируется моральными и нравственными нормами.

Принуждение — угроза материальной, административной и уголовной ответственности за нарушение правил обращения с защищенной информацией.

На основе перечисленных методов создаются средства ЗИ, которые можно разделить на:

Формальные— выполняют свои функции по заранее установленным процедурам без вмешательства человека;

Неформальные — реализуется в результате деятельности людей, либо регламентируют эту деятельность.

Литература:

1. Большаков А.А. и др. Основы обеспечения безопасности данных в компьютерных системах и сетях, С.-П., 1996, гл.2 (с.27-46).
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных, ч.1, гл.7 (с.234-259).

Формальные средства защиты

Физические средства защиты — создают препятствия для нарушителей на путях к защищаемой информации и выполняют следующие функции:

- Охрана территории и зданий;
- Охрана внутренних помещений;
- Охрана оборудования и наблюдение за ним;
- Контроль доступа в защищаемые зоны;
- Нейтрализация излучений и наводок;
- Создание препятствий визуальному наблюдению и подслушиванию;
- Противопожарная защита;

- Блокировка действий нарушителя и т. п.

Аппаратные средства защиты — специальные средства, непосредственно входящие в состав технического обеспечения ИВС и выполняющие функции ЗИ как самостоятельно, так и в комплексе с другими средствами. Аппаратные средства защиты можно условно разбить на группы согласно типам аппаратуры, в которых они устанавливаются:

- Средства защиты процессора;
- Средства защиты памяти;
- Средства защиты терминалов;
- Средства защиты устройств ввода-вывода;
- Средства защиты каналов связи.

Программные средства защиты — функционируют в составе ПО средств и механизмов ЗИ (они выполняют функции ЗИ самостоятельно или в комплексе с другими средствами защиты). В зависимости от функционального назначения различают следующие группы программных средств ЗИ:

- Средства внешней защиты (защита территорий, помещений, отдельных каналов связи и устройств ИВС);
- Средства внутренней защиты (контроль и использование данных и устройств и ресурсов ИВС);
- Средства управления защитой;
- Средства обеспечения функционирования СОБИ.

Неформальные средства защиты

Организационные средства защиты — организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ИВС для обеспечения безопасности информации.

Законодательные меры защиты — законодательные акты, которыми регламентируются правила использования данных ограничения доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические нормы — всевозможные нормы, которые традиционно сложились или складываются по мере развития информатизации общества. Эти

нормы не являются обязательными, однако их несоблюдение ведет, как правило, к потере авторитета, престижа человека, группы лиц или целой организации.

[Большаков А. А. и др. с. 42-44]:

Закон «О государственной тайне» (вступил в действие 21 сентября 1993 года) устанавливает органы защиты государственной тайны, к которым относятся:

- Межведомственная комиссия по защите государственной власти;
- Органы федеральной исполнительной власти (министерства безопасности и обороны, ФАПСИ, служба внешней разведки);
- Государственная техническая комиссия (ГТК) и их органы на местах (ГТК создана указом Президента РФ от 5 января 1992 года);
- Органы государственной власти, предприятия, учреждения и организации и структурные подразделения по защите государственной тайны.

ГТК РФ — является органом государственного управления РФ, который в пределах своей компетенции осуществляет руководство органами ЗИ, составляющей государственную и служебную тайну в политической, экономической, научно-технической, военной и других сферах.

На ГТК РФ возложено проведение единой технической политики и координации работ по ЗИ от утечки по техническим каналам от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее разрушения, искажения и уничтожения.

32 Оптимальные задачи ЗИ. Постановка задачи. Классификация методов принятия решения в ЗИ

Аналитические методы — решение в явном виде.

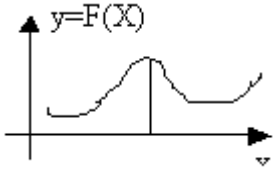
Численные методы (поиск) — решение с помощью некоторого алгоритма.

Регулярный поиск — строго определённый порядок действий.

Случайный поиск — порядок поиска может меняться.

Аналитические методы :

Дифференциальное исчисление: 1)



2) (i = 1, 2, …,n)

3) Унимодальность.

Метод неопределённых множителей Лагранжа:

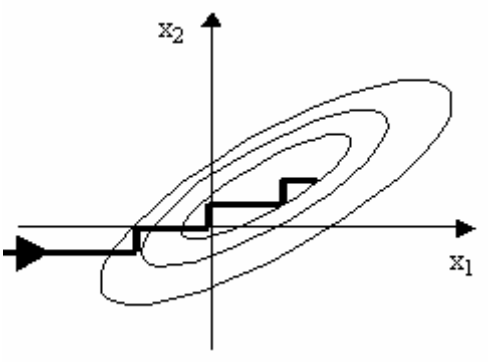
F(X) → max при $\varphi_I(X)=0$;

Функция Лагранжа: $F_0=F+\sum_j \lambda_j \varphi_j$ → max; $\frac{\partial F}{\partial x_j}=0$, $\frac{\partial F}{\partial \lambda_j}=0$

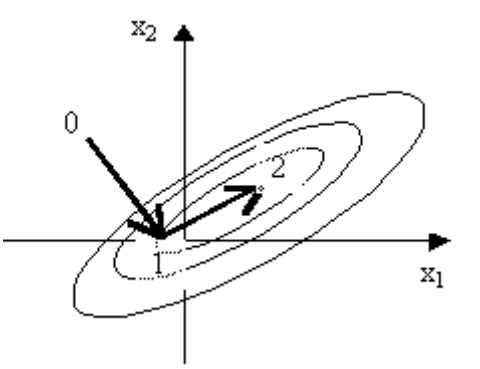
Регулярный поиск:

Одномерный поиск: Для унимодальных функций.

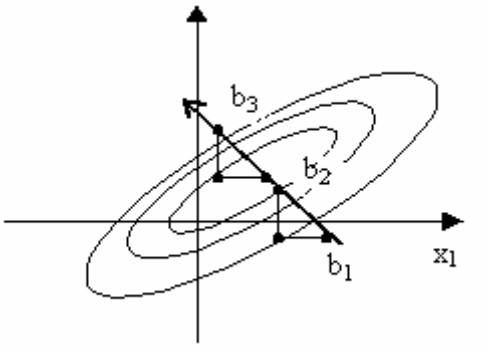
Метод Гаусса-Зейделя: метод покоординатного спуска.



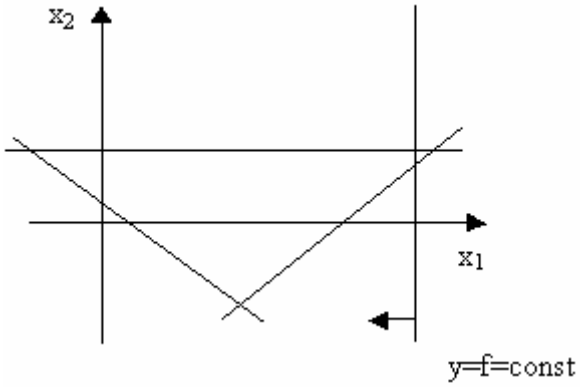
Метод наискорейшего спуска: F → max, $\text{gradF}=(\frac{\partial \text{F}}{\partial \text{x}_1},\ldots,\frac{\partial \text{F}}{\partial \text{x}_n})$, x= $x^{\circ}+h\cdot\text{gradF}(x^{\circ})$.



Метод конфигураций: может использоваться для движения по гребню.

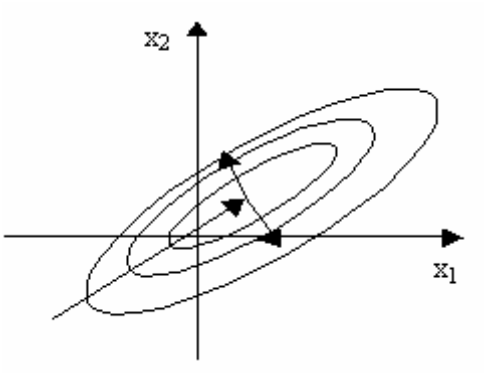


Линейное программирование:



Случайный поиск: $x_j=x_i^{\circ}+\xi_i$, где $\xi_i \in (-1; 1)$.

Лёгкий случайный поиск с возвратом.



Особенности практического применения методов оптимизации.

Сложности задач оптимизации:

Высокая размерность (≥10÷20)

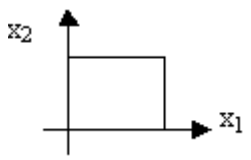
Оценка значимости параметров

Нормализация:

$\bar{x}_i = \dfrac{x_i - x_i^{\min}}{x_i^{\max} - x_i^{\min}}$, здесь $(0 \le \bar{x}_i \le 1)$.

Наличие ограничений.

– Область $X \in G$ — может быть и пустой (∅), т.е. ограничение — «жёстко».

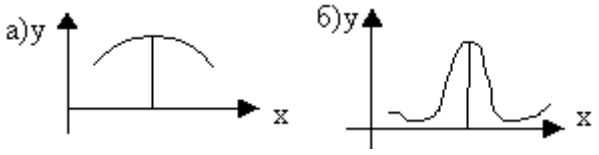


– Метод штрафных функций: $y=F(x)+\theta(x)$, функция штрафа для ограничения $\varphi(x)\le 0$; $\theta(x)=[\max\{0, \varphi(x)\}]^2 \cdot r$;

Многоэкстремальность, наличие глобального экстремума.

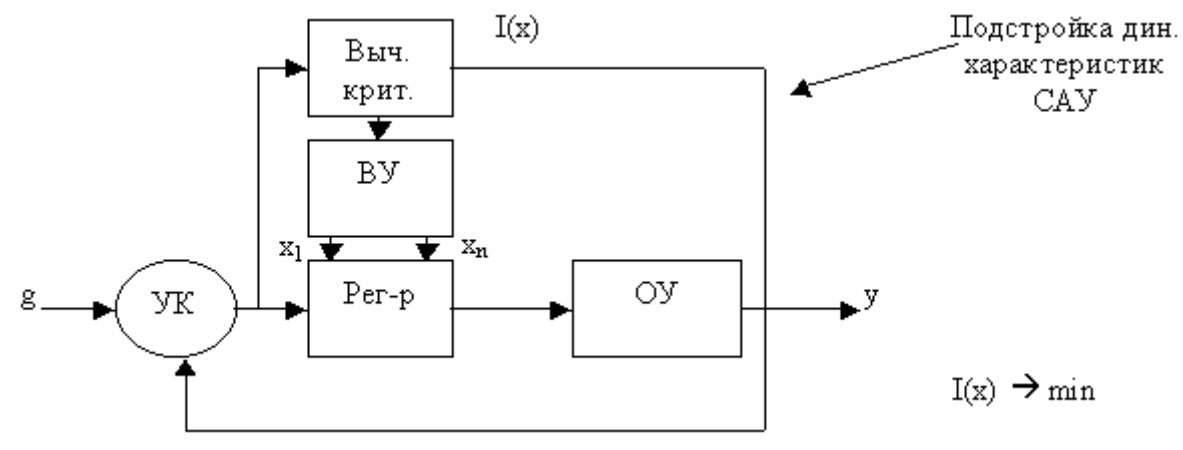
Метод сканирования; многоэтапные процедуры.

Овраги (гребни) функции цели.

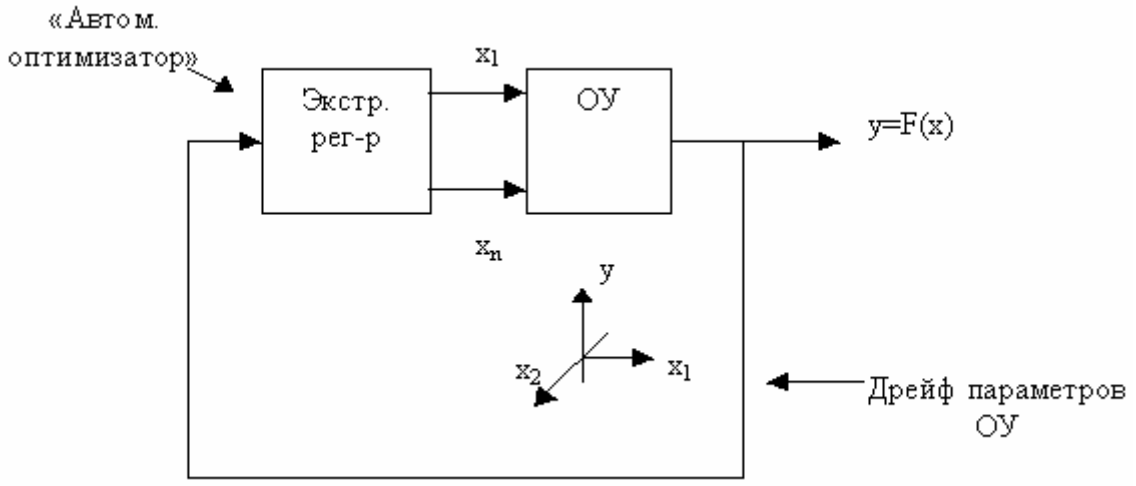


Применение алгоритмов оптимизации в экстрем. и самонастр-ся САУ:

а) Блок-схема СНС:



б) Блок-схема экстр. САУ:



Доп. литература:

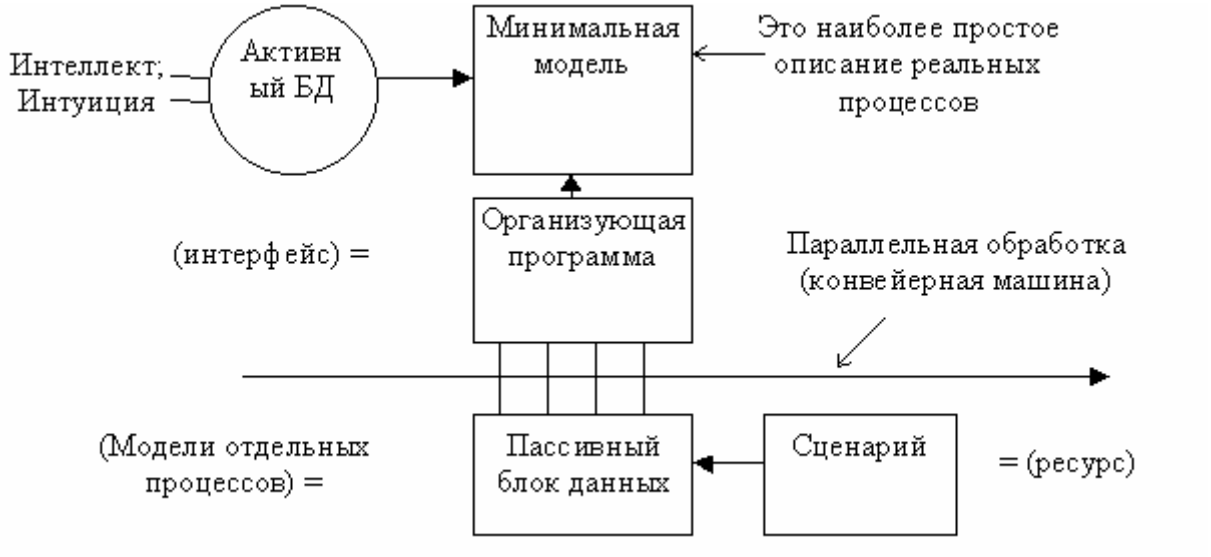
Дуглас Дж. Уайлд «Методы поиска экстремума», -М.: Наука, 1967, 268 с.

Первозванский А.А. «Поиск», -М.: Наука, 1970, 264 с.

Пример задач имитационного моделирования.

Изучение экологических проблем (Никита Николаевич Моисеев, дир-р ВЦ АН СССР, г Алма-Ата, 1986 г.).(«экология» — «изучение собственного дома»)

Работы по изучению биосферы были включены в план ВЦ АН СССР в 1971 г.



Первая версия модели биосферы ≈12-15 лет на её разработку.

Подробнее см. [Человек и биосфера, Александров, Моисеев], 1984 г.

Тестирование моделей — только на ЭВМ =(«звериное лицо объективной истины»).

Машинные эксперименты:

Влияние содержания углекислоты на состояние окружающей среды;

Анализ влияния пожаров (облака сажи) на земной климат.

Сценарий: Взаимный обмен ядерными ударами ∑мощ. ≈5000 мГтонн.

→СССР — проверяли ≈ на 360 дней (упрощ. модель).

→США — проверяли ≈ на 30 дней (полная модель с учётом океана).

Результаты совпали.

Взрыв мощностью 1 мГт → 300÷400 тыс.т пыли

10000 мГт → 3÷4 млрд.т пыли.

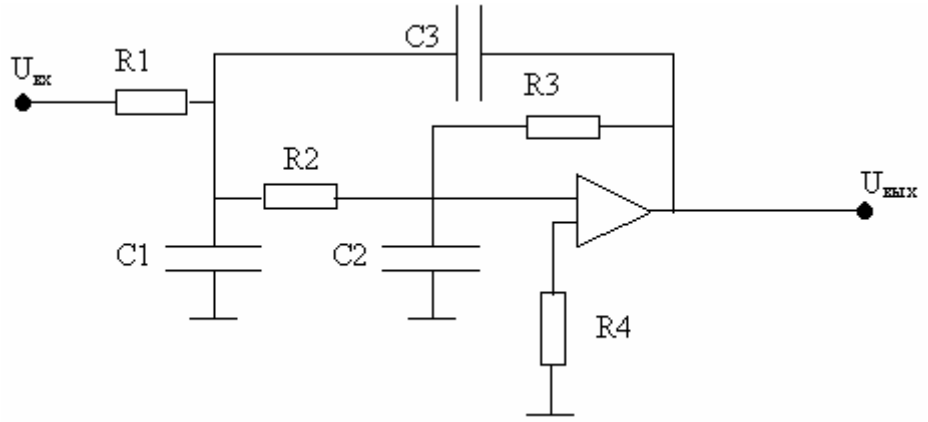
13% ядерного потенциала → превращается в костёр 1 млн.кв.км леса →

→ около 4 млрд.т. сажи.

Облака сажи над городами ≈ в 100 раз плотнее облаков, обр-ся в рез-те лесных пожаров. ⇒ «Ядерная ночь» + «Ядерная зима» (в Сев.Европе температура падает ≈ на 30° С, на восточном побережье США ≈ на 40°-50° С).

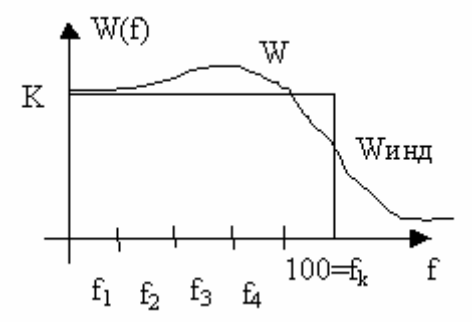
100 мГтонн = общая взрывная мощь зарядов одной-двух подв. лодок типа «Трайдент –2».

Зондирование пространства параметров [Соболь И.М., Статников Р.Б. Наилучшие решения — где их искать. –М: Знание, 1982, 64 с.]



Задача: требуется найти значения параметров R1, R2, R3, R4, C1, C2, C3, при которых АЧХ фильтра максимально близка к заданной (идеальной) характеристике:

Критерий качества:



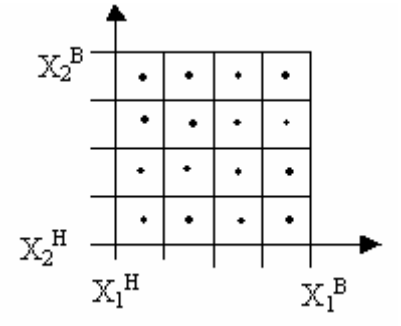
Параметры ФНЧ при этом будут удовлетворять следующим ограничениям:

$Ri^{H} \le R_i \le R_i^{B}$

$C_i^{H} \le C_i \le C_i^{B}$

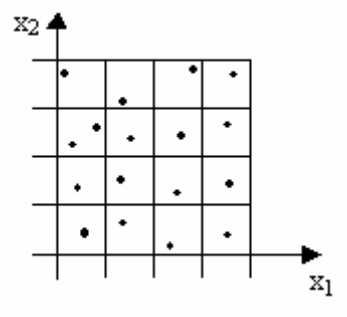
Зондирование — численное исследование пространства параметров $X=(x_1, x_2, \ldots, x_n)$ с целью определить наилучшие сочетания этих параметров.

Пример зондирования: интервал изменения каждой переменной x_i делится на m частей, итого получается m^n точек в узлах сетки. Всего $4^2=16$ точек, но если $F(x_1,x_2)$ зависит только от x_1, то 12 точек являются «лишними», неинформативными.



Более рациональная схема маш. эксп-та — Проекции точек на любую грань прямоугольника (в общем случае параллелепипеда) также образуют хорошие сетки.

Желательно чтобы соответствующие точки имели закон распределения, близкий к равномерному; т.е. закон распределения точек должен быть случайным.



Этапы решения поставленной задачи:

Выбор пробных точек A_i (I=1, 2, …, N);

Составление таблиц испытаний:

Здесь $A_i \in \{x_1, x_2, \ldots, x_n\}$ — пробные точки в заданной части пространства.

F_j / A_i	F_1	F_2
A_1	$F_1(A_1)$	$F_2(A_1)$
A_2	$F_1(A_2)$	$F_2(A_2)$
A_3	$F_1(A_3)$	$F_2(A_3)$
A_n	$F_1(A_n)$	$F_2(A_n)$

$(A_1, A_2, \ldots, A_n)$ — равномерно распределённые точки.

Определяются границы изменения критериев: $\min F_1 \le F_1 \le \max F_1$;

$\text{Min } F_2 \le F_2 \le \max F_2$.

Выбор критериальных ограничений: на этой стадии — ЛПР — может назначать дополнительные критериальные ограничения: $F_1 \le F_1^*$ и $F_2 \le F_2^*$, тем самым исключая из таблицы испытаний некоторые строки, т.е. некоторые испытательные точки A_i.

Исключение неэффективных точек:

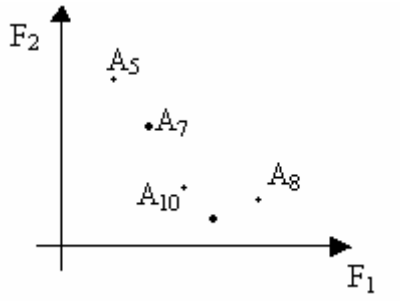
Выберем какую либо из имеющихся допустимых точек, например A_1. Просматривая все другие точки A_i, кроме отмеченной, исключим те из них, для которых выполняются условия:

$$\begin{cases} F_1(A_i) \geq F(A_1); \\ F_2(A_i) > F(A_1); \end{cases} \quad \begin{cases} F_1(A_i) > F(A_1); \\ F_2(A_i) \geq F(A_1); \end{cases}$$

– При этом из рассмотрения исключаются все безусловно худшие точки, чем A_1. Затем среди оставшихся точек выберем какую-либо другую, отметим её и повторим процесс исключения.

– В итоге получим множество приближенно эффективных точек (при $N \to \infty$ получаем в пределе множество эффективных точек).

5) а) Можно построить приближенную границу Парето-области.



б) Можно найти корреляционную зависимость критериев F_1 и F_2 :

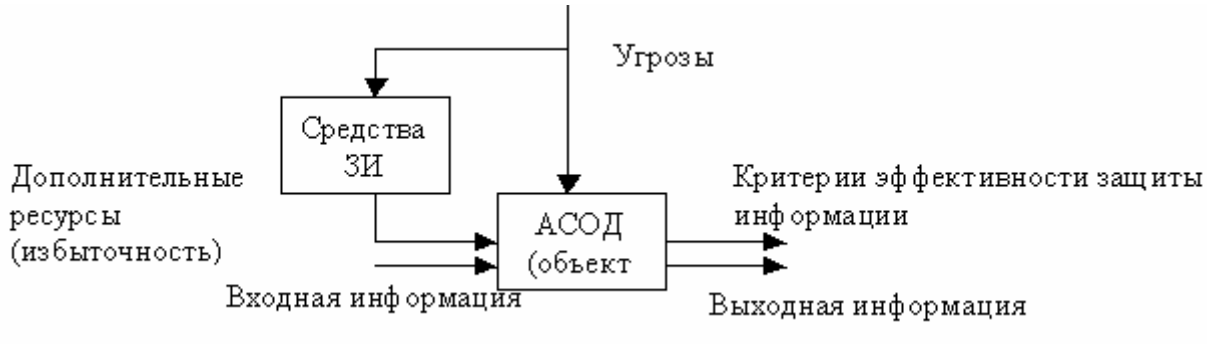
$$r_{kl} = \frac{I_{kl} - I_k \cdot I_l}{\sqrt{(I_{kl} - I_k^2) \cdot (I_{kl} - I_l^2)}}, \text{ где } I_k = \frac{1}{N} \cdot \sum_{i=1}^{N} F_k(A_i), \; I_{kl} = \frac{1}{N} \cdot \sum_{i=1}^{N} F_k(A_i) \cdot F_l(A_i)$$

r_{kl} — коэффициент корреляции.

Если $r_{kl} \approx 1$, то F_k и F_l — лин. зависимость.

Оптимальные задачи защиты информации

Общая модель системы ЗИ:



Угрозы:

- Отказы;
- Сбои;
- Ошибки;
- Злоумышленные действия;
- Стихийные бедствия.

Средства ЗИ:

- Резервирование аппаратуры;
- Контроль возникновения сбоев (ошибок) и устранение их последствий
- Контроль возможных дестабилизирующих факторов (ДФ), связанных с НСД к информации и устранение последствий
- Защита от пожаров, наводнений и т. п.

Идея ЗИ выделяются дополнительные ресурсы (материальные, временные, финансовые, людские, информационные) с целью уменьшить или полностью ликвидировать действие ДФ

1: Модель ДФ

Критерий эффективности ЗИ:

Защищенность информации;

Вероятность сохранения целостности информации ($Р_{ци}$);

Вероятность отсутствия НСД к информации ($Р_{онд}$);

Потери (ущерб) в результате действия ДФ ($С_{пот}$);

Относительные потери в результате действия ДФ ($С_{пот}/С_{\Sigma}$);

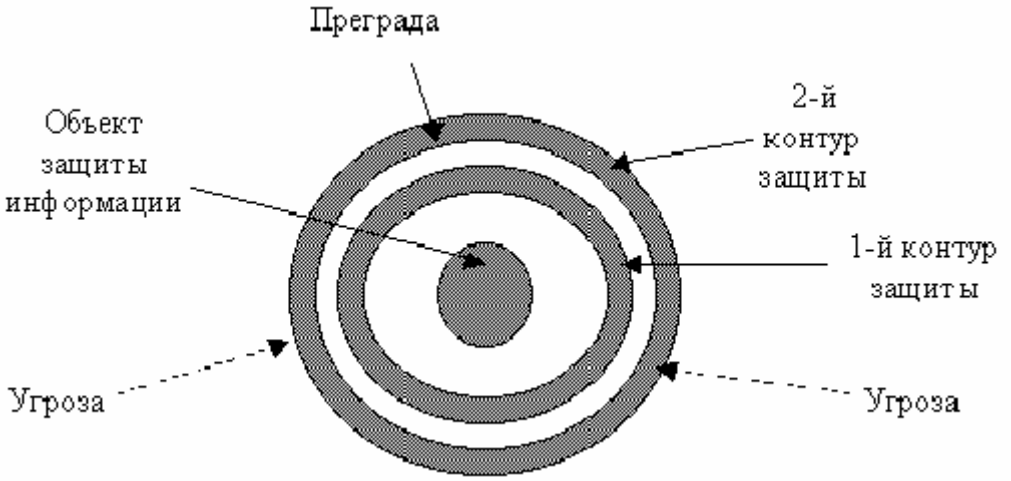
Следовательбно,можно дифференцировать:

Относительно действия конкретных угроз (ДФ) или группы ДФ:

Или по отдельным уровням (рубежам, зонам) ЗИ;

Классам защищаемой информации (по ее важности);

И т. д.)

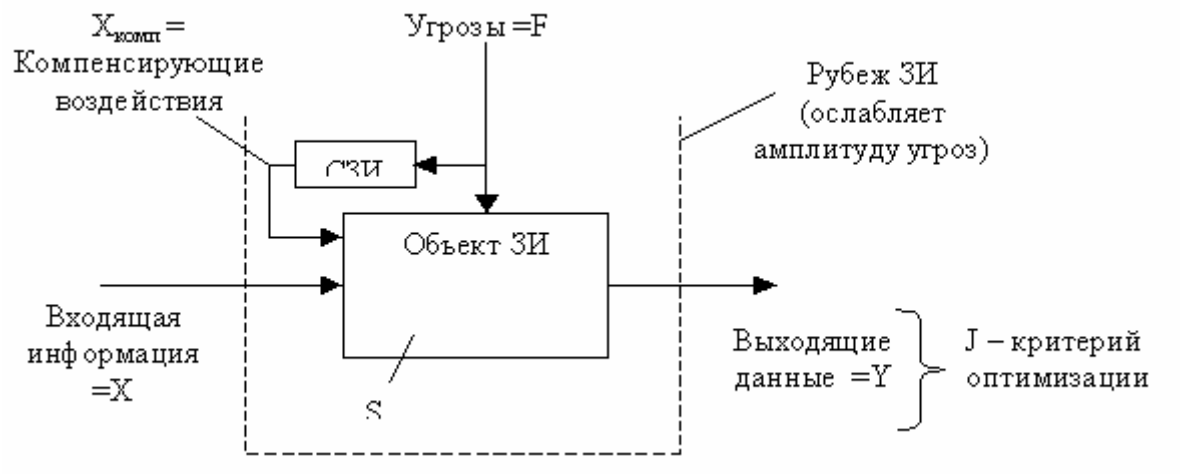


Преграда — однородная защитная оболочка.

Основное свойство объекта защиты — способность привлекать его владельца и потенциального нарушителя.

Свойство преграды — способность противостоять попыткам преодоления её нарушителем.

Академик Б.Н. Петров: « В теории известен принцип двухканальности: для предотвращения действия возмущения на выход объекта (или снижения эффекта от такого воздействия) необходимо обеспечить дополнительный канал передачи возмущения на выход, обеспечивающий измерение (обнаружение) возмущения и компенсацию его влияния путём использования дополнительных управляющих воздействий, прилагаемых ко входам объекта.»



Объект ЗИ: < X; Y; S; F; $X_{КОМП}$; J>

X — Вход

Y — Выход

S — Состояние

F — Возмущение

$X_{КОМП}$ — Компенсирующие воздействия

J — Качество инф-ии

Примеры угроз:

– помехи;

– сбои;

– вирусная атака;

– НСД; и т. д.

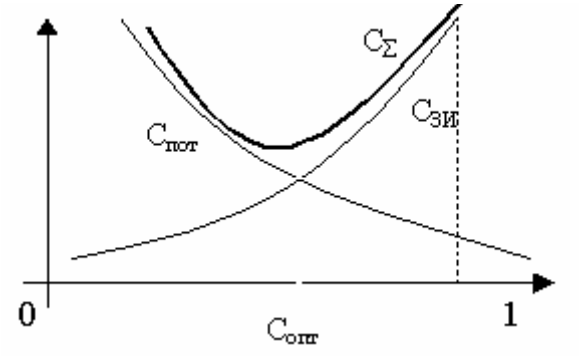
4Многокритериальная оптимизация систем ЗИ.

Оптимальная постановка задачи (различные варианты).

А) Повысить уровень защищённости информации ($P_{защ}$ → max).

Б) Снизить потери, связанные с воздействием возможных угроз на защищаемую информацию ($C_{пот}$ → min).

В) Снизить суммарные затраты, связанные с действием ДФ:



C_Σ — ожидаемая полная стоимость;

$C_{пот}$ — потери (ущерб);

$C_{ЗИ}$ — затраты на ЗИ;

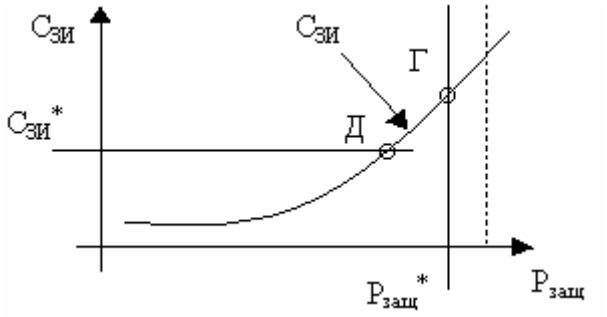
C_Σ — суммарные дополнительные затраты на эксплуатацию системы в условиях действия ДФ, включающие в себя начальные затраты на создание СЗИ, а также потери от действия ДФ.

Но: трудно дать оценку потерь (например, в случае гос., военной тайны).

Г) Получить максимальный уровень защищённости информации при ограниченных затратах (ресурсах) на ЗИ: $P_{защ} \rightarrow max$ при $C_{ЗИ} \le C_{ЗИ}^*$ (обратная задача).

Д) Обеспечить минимальные затраты на ЗИ при достижении заданного уровня защищённости информации: $C_{ЗИ} \rightarrow min$ при $P_{защ} \le P_{защ}^*$ (прямая задача).

Графическая интерпретация случаев (Г) и (Д):



Но: трудно назначить гарничные знчения $P_{защ}^*$ и $C_{ЗИ}^*$

Е) Парето — оптимизация = подход к решению задачи векторной оптимизации, предложенный в 1904 итальянским экономистом Вильфредо Парето

Идея : Допустим, что имеются 2 варианта решения задачи — А и В, которые оцениваются с помощью двух критериев ($F_1 \rightarrow min$,$F_2 \rightarrow min$) .

Тогда решение А считается «лучше », чем решение В, если:

$F_1(A)<=F_2(B)$ и $F_1(A)<=F_2(B)$,

причем хотя бы для одного критерия j: $F_j(A) < F_j(B)$

$\Rightarrow$При этом решение B считается «хуже», чем решение A

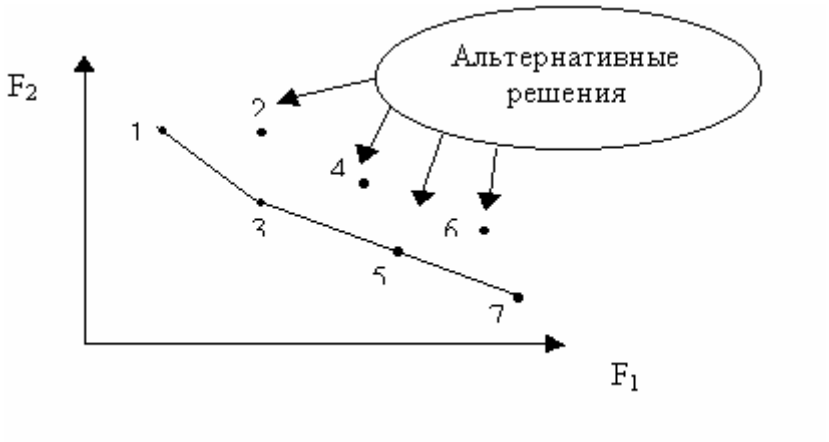
Л. Эйлер : «В природе нет ничего такого, в чем не был бы виден смысл какого-нибудь максимума или минимума»

Некорректная формулировка: «добиться максимального эффекта при минимальных затратах»

[АиФ], №17, 1997:

Защита информации обходиться, как правило, в (30-40)% от стоимости самой защищаемой информации.

Таким образом, сравнивая попарно различные решения задачи, можно получить множество «неулучшаемых» решений:



F_2 = затраты на защиту = $C_{зи}$

F_1 = показатель уязвимости информации = 1- $P_{защ}$

Решения P{1;3;5;7} образуют Парето-множество или область компромиссов или множество эффективных решений.

$\oplus$: Сужается множество альтернатив.

Но: оптимальные по Парето решения не являются единственными.

$\Rightarrow$ Окончательный выбор = за лицом, принимающем решения (ЛПР)

Особенности практического применения методов оптимизации:

- Высокая размерность
- Наличие ограничений
- Многоэкстремальность
- Наличие глобального оптимума

Обратные (гребни) функции цели

$$P_{\text{защ}} = F(C_i^{(\text{фф})}),\ i = 1,\ldots,n\ \ P_i^{(\text{фф})} = f(C_i^{(\text{фф})})$$

Ресурсы, выделенные на обеспечение *i*-й функции ЗИ

Для многорубежной системы ЗИ: $P_i^{(\text{фф})} = \prod_{k=1}^{5} P_{ik}^{(\text{фф})}$

где $i = 1,2,\ldots,5$ –номер рубежа (зоны) ЗИ,

P_{ik} –вероятность правильного выполнения *i*-й функции ЗИ в *k*-й зоне,

Кроме того : $C_i^{(\text{фф})} = \sum_{k=1}^{5} C_{ik}^{(\text{фф})}$, где C_{ik} — ресурсы, выделенные в *k*-й зоне ЗИ на выполнение *i*-й функции ЗИ

33 Формальные методы принятия решений. Многокритериальная оптимизация.

Многокритериальные задачи оптимизации.

Выше рассматривались однокритериальные задачи оптимизации.

Критерии качества электронной аппаратуры — точность; надёжность; помехоустойчивость; быстродействие; стоимость и др. — во многом являются противоречивыми.

Задача многокритериальной(векторной) оптимизации:

$$\left.\begin{array}{l} F_1(X) \to \max(\min) \\ \vdots \\ F_k(X) \to \max(\min) \end{array}\right\} \text{— Является математически некорректной}$$

при $X \in G$

Часто применяемая формулировка: «Добиться максимального эффекта при минимальных затратах» — не имеет смысла.

Основные методы решения многокритериальных задач:

Выбор приемлемого варианта (Принцип приемлемости);

Конструирование «обобщённого показателя» эффективности;

Оптимизация на основе безусловного критерия предпочтения (Принцип Парето);

Использование условных критериев предпочтения.

Рассмотрим подробнее основные методы векторной оптимизации.

Пусть требуется минимизировать значения критериев ($F_i \to \min$). Тогда задачу можно сформулировать следующим образом: САР АД:

– погрешность регистрации температуры ≤ 0,2 %;

– вероятность отказа в течении 100 часов ≤ 0,001;

– масса эл. агрегата ≤ 2 л;

– время отработки переходных процессов ≤ 2 с.

Но эта задача сводится к отсеканию приемлемого решения X, удовлетворяющего ограничениям: $X \in G$ и $F_i(X) \le F_i^*$, $i = 1, 2, \ldots, k$.

Но:

– выбор F_i^* часто бывает необоснованным;

– решение X не является оптимальным.

Задача сводится к однокритериальной, путём построения «обобщённого показателя эффективности»:

Обычно: $Э = \frac{"за \quad здравие"}{"за \quad упокой"}$.

А) Пример — мощность МП:

$W = Д \cdot \frac{П}{Б}$, где Д — длина слова; П — число адресуемых слов в памяти; Б — время выполнения шага.

Б) Информационная емкость канала связи:

$V_k = T_k \cdot F_k \cdot \log_2(1 + \frac{P_c}{P_{шум}})$, где $T_к$ — время; F_k — частотный диапазон.

В) Л.Н. Толстой:

«Критерий для оценки человека» = (Действительные достоинства человека)/(Его мнение о себе).

Но:

– построение такого критерия не всегда возможно;

– недостаток в одном показателе качества часто нельзя компенсировать за счёт других показателей.

Безусловный критерий предпочтения (БЧП) —

был сформулирован в 1904 году итальянским экономистом Вильфредо Парето.

Пусть $X'=(X_1', X_2', \ldots, X_n')$ — 2 возможных решения

и $X''=(X_1'', X_2'', \ldots, X_n'')$ задачи

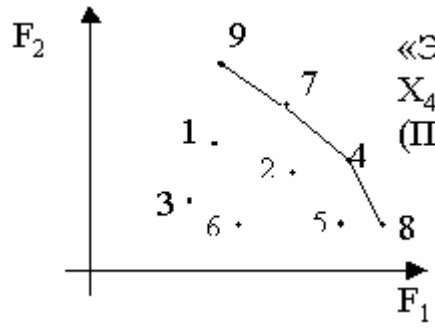
Тогда X' «лучше», чем X'', если: $F_j(X') >= F_j(X'')$ для всех j=1, 2, …k;

Причем хотя бы для одного j: $F_j(X') > F_j(X'')$.

Но тогда X''«хуже», чем X'.

Оптимальные по Парето решения — это множество «неулучшаемых» решений.

Пример: F_2



«Эффективным» является решение:
X_4, X_7, X_8, X_9 = множество Парето
(Парето-область)

Но:

– Оптимальное по Парето решение не является единственным (случается множество альтернатив).

– Окончательный выбор за ЛПР.

Условный критерий предпочтения (УКП)

А) Построение обобщённого (интегрального) критерия:

$F = f(F_1, F_2, \ldots, F_k) \rightarrow \max$, или $F = f(F_1, F_2, \ldots, F_k) \rightarrow \min$.

Функция полезности — Функция потерь (затрат)

Пример — линейная свёртка критериев:

$F = \sum_{j=1}^{k} \lambda_j F_j$ — где λ — весовые коэффициенты; например, $\lambda_j = \frac{c_j}{(F_j)\max}$;

$\sum_{j=1}^{k} c_j = 1$

Но проблема весовых коэффициентов (субъективизм).

Б) Максимальный критерий.

В) Выделение главного показателя (критерия):

Пусть: $F_1(X)$ — главный критерий качества.

Тогда: $F_1(X) \rightarrow \max$ при ограничениях $F_2(X) \geq F_2$; …

$F_k(X) \geq F_k^*$.

Но:

– трудно задать

– трудно выбрать главный критерий

Г) Метод последовательных уступок:

Пусть: критерии $F_1, F_2, \ldots, F_k$ расположены в порядке убывания важности.

Тогда: $F_1(X) \rightarrow \max \Rightarrow (F_1)\max = F_1^*$.

Затем: $F_2(X) \rightarrow \max$ при $\underbrace{F_1(X)} \geq F_1^* - \Delta F_1$.

ΔF_1 – Уступка по критерию F_1 и т. д.

Но:

- решение зависит от ранжирования критериев

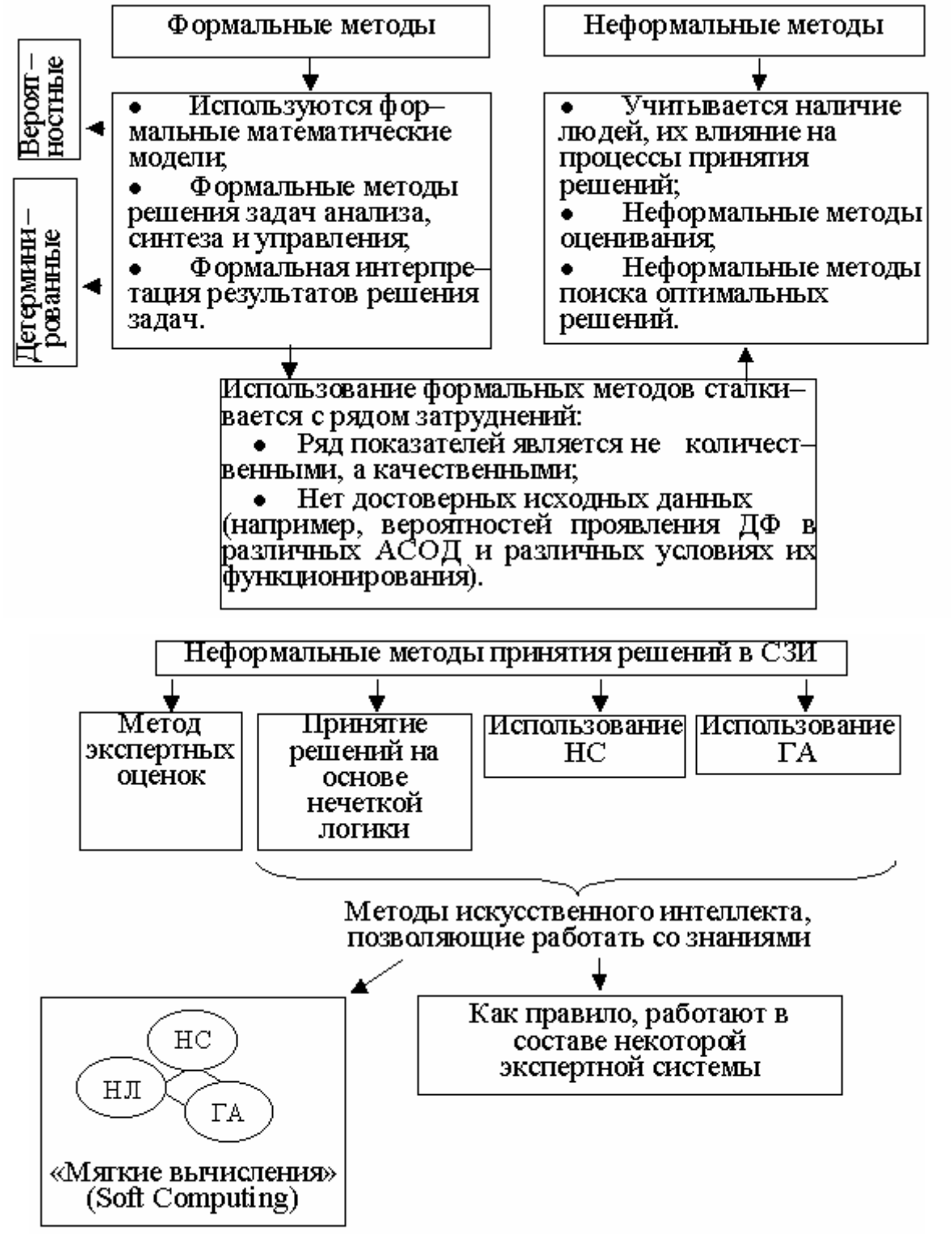
– как выбирать уступки?

– окончательный выбор за ЛПР.

Одна из важных проблем метода экспериментальных оценок — ранжирование критериев

34 Неформальные методы принятия решений в СЗИ. Метод экспертных оценок. Нечеткая логика

Формальные и неформальные методы анализа СЗИ



Метод экспертных оценок — метод поиска решений сложных задач, которые основаны на суждениях (оценках, высказываниях) специально выбираемых (назначаемых) экспертов, то есть специалистов, компетентных в той области, к которой относится решаемая задача.

Последовательность решения задачи с помощью метода экспертных оценок

Подбор экспертов — осуществляется с учетом следующих требований к ним:

- Компетентность;
- Креативность (способность решать творческие задачи);
- Антиконформизм (неподверженность влиянию авторитетов);
- Конструктивность мышления (эксперт должен давать решения, обладающие свойством практичности);
- Коллективизм;
- Самокритичность.

Различные подходы к подбору экспертов:

– самооценка;

– оценка группой каждого специалиста;

– оценка на основе результатов прошлой деятельности;

– определение компетентности кандидатов в эксперты.

[Чепурных Н. В., Новоселов А. Л. «Экономика и экология: развитие и катастрофы». — М.: Наука, 1996. — 271 с.]:

Коэффициент компетентности — определяется как среднее арифметическое коэффициентов $К_а$ и $К_з$: $К_{комп} = К_а + К_з / 2$; где: $К_а$ — коэффициент, учитывающий источники аргументации, которые послужили эксперту основанием для произведенной им оценки:

Таблица 1

Источники аргументации	Степень влияния источников		
	Высокая	Средняя	Низкая
Произведенный теоретический анализ	0,3	0,2	0,1

Производственный опыт	0,5	0,4	0,2
Обобщение работ отечественных авторов	0,05	0,05	0,05
Обобщение работ зарубежных авторов	0,05	0,05	0,05
Личное знакомство с состоянием дел за рубежом	0,05	0,05	0,05
Интуиция	0,05	0,05	0,05

Коэффициент $К_а$ находится путем суммирования численных значений таблицы 1.

Степень знакомства эксперта с обсуждаемой проблемой ($К_з$) оценивается непосредственно экспертом в пределах от 0,1 до 1.

Существуют различные разновидности метода экспертных оценок:

1. Метод простого ранжирования (ранговая шкала) — заключается в том, что каждый эксперт располагает признаки в порядке предпочтения (1 — наиболее важный признак; 2 — следующий по важности; и т.д.).

Признаки	Эксперты				
	1	2	3	.	n
x_1	a_{11}	a_{12}	a_{13}	.	a_{1n}
x_2	a_{21}	a_{22}	a_{23}	.	a_{2n}
.	.	.	.	.	.
.	.	.	.	.	.
x_m	a_{m1}	a_{m2}	a_{m3}	.	a_{mn}

После того как данные от экспертов собраны, проводится обработка полученных оценок. Определяется средний ранг j-го признака:

$$S_i = \frac{1}{n}\sum_{j=1}^{n} a_{ij}$$

(j — номер эксперта, i — номер признака).

Чем меньше величина S_i, тем больше важность этого признака.

Для того, чтобы узнать, случайно ли распределение или есть согласованность во мнениях экспертов, вычисляется коэффициент конкордации:

$$K = \frac{12\sum_{i=1}^{m} d_i^{\,2}}{n^2\left(m^3 - m\right) - n\sum_{j=1}^{n}\left[\sum_{q=1}^{Q}\left(t_q^{\,3} - t_q\right)\right]}$$

где: $d_i = \bar{S} - S_i$ — отклонение среднего ранга I — го признака от среднего ранга совокупности;

$\bar{S} = \frac{1}{m}\sum_{i=1}^{m} S_i$ — средний ранг совокупности признаков;

t_q — число одинаковых рангов, назначенных экспертами i — му признаку;

Q — количество групп одинаковых рангов.

При полной согласованности экспертов: К=1.

При полном разногласии: К=0.

2. Метод задания весовых коэффициентов (линейная шкала) — заключается в присвоении всем признакам весовых коэффициентов (коэффициентов важности). Обобщенное мнение экспертов рассчитывается как среднее арифметическое. Следовательно, чем выше величина коэффициента, тем больше важность признака.

3. Метод парных сравнений — каждый эксперт проводит попарную оценку приоритетности признаков, и эксперт заполняет матрицу $E_i=(e_ik_j)$, где

$$e_ik_j = \begin{cases} 1, \text{ если } x_k > x_j, \text{ или } x_k \sim x_j; \\ 0, \text{ если } x_k < x_j. \end{cases}$$

Далее находится сумма матриц всех экспертов: $Z_{kj} = \sum_{i=1}^{n} e_{ik}$. Определяется результирующая матрица R:

$$p_{kj} = \begin{cases} 1, z_{kj} ? n/2 \\ 0, z_{kj} < n/2 \end{cases}$$

Находится сумма баллов, которую набрал каждый признак: $в_к = \sum_{i=1}^{m} p_{kj}$

4. Метод Дельфи — метод многоуровневой экспертизы. Был разработан в начале 60-х гг. сотрудниками фирмы “РЭНД корпорейшн” О. Хелмером и Т. Гордоном.

Характеризуется тремя основными чертами:

3. анонимность;
4. регулируемая обратная связь;
5. групповой ответ.

Метод парных сравнений.

Допустим, что предлагается три альтернативных варианта построения системы ЗИ. Для выбора предпочтительного варианта создана группа из четырёх экспертов. На основе парных сравнений каждого эксперта получены матрицы парных сравнений:

Эксп

Вар	M_1	M_2	
M_1	1	1	1
M_2	0	1	1
M_3	0	0	1

Эксп

Вар	M_1	M_2	
M_1	1	0	1
M_2	1	1	1
M_3	0	0	1

$M_2>$

Эксп

Вар	M_1	M_2	
M_1	1	0	0
M_2	1	1	1
M_3	1	$M_2>$	1

Эксп

Вар	M_1	M_2	
M_1	1	0	0
M_2	1	1	0
M_3	1	1	1

M_3>

Суммарная матрица мнений всех экспертов Z:

Вар	M_1 M_2		
M_1	4	1	2
M_2	3	4	3
M_3	2	1	4

Результирующая матрица $R(p_{kj})$:

Вар	M_1 M_2		
M_1	1	0	1
M_2	1	1	1
M_3	1	0	1

Сумма баллов, которые набрал каждый вариант: $в_к = \sum_{j=1}^{n} p_{kj}$

Нечеткая логика

1.Понятие нечеткой логики (Л.Заде)

1964–1965 — Основополагающая статья по нечетким множествам (Л.Заде)

1973 — Принцип несовместимости (Л.Заде)

1974 — Применение нечеткой логики к задачам управления (Э.Мамдани)

1980–е гг. — “нечеткий бум” в Японии

2.Нечеткие множества, их основные свойства. (Fuzzy sets)

(Fuzzy sets), следовательно, определение нечетких множеств.

Основные свойства:

1. Носитель (A)
2. Высота нечеткого множества
3. α–срез нечеткого множества
4. Одноточное нечеткое множество (singleton)

5. Конечное нечеткое множество $A=\sum \mu_i / x_i$
6. Виды задания функций принадлежности

3.Понятие лингвистической переменной.

- Возраст
- Скорость
- Угроза

4.Операции с нечеткими множествами.

1. Объединение нечеткого множества
2. Пересечение нечеткого множества
3. Дополнение
4. Концентрация
5. Растяжение

5.Нечеткие отношения

$R: x \to y$; $R=\{(x,y),\mu(x,y),x \in X, y \in Y\}$

$R_1(x,y)$="x больше y"

Y / X	1	2	5	10
4	1	0.9	0.1	0
8	1	1	0.6	0.1
15	1	1	1	0.6

$R_2(x,y)$="$x \approx y$"

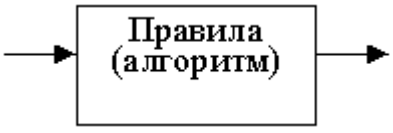
Y / X	1	2	5	10
4	0.1	0.4	0.9	0.1
8	0	0	0.5	0.8
15	0	0	0.1	0.6

Операции объединения и пересечения нечетких множеств:

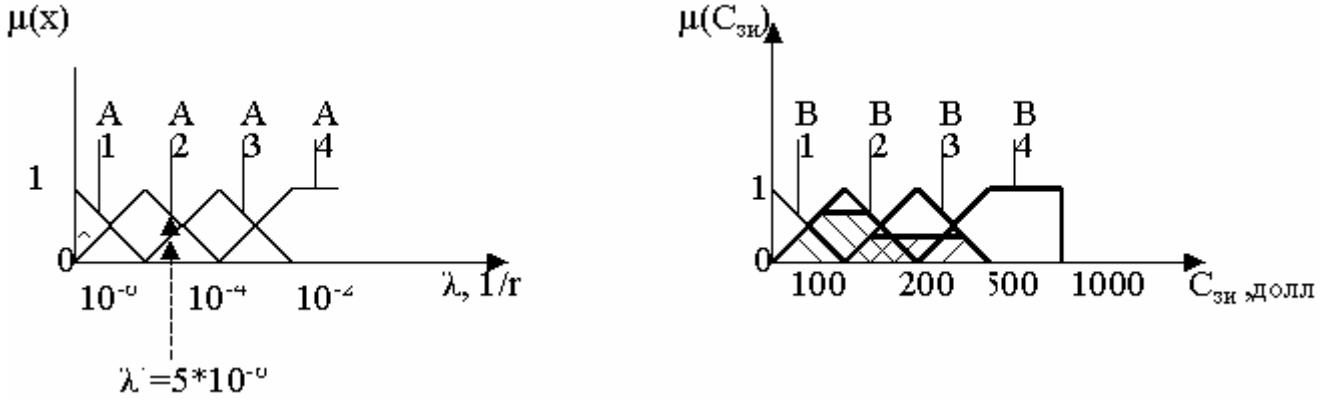
$R_1 \cup R_2$, $R_1 \cap R_2$

6.Нечеткие алгоритмы

$A \to B$



Угроза	Ресурсы на ЗИ
{Незначительная (A_1)}	{Низкие(B_1)}
{Ощутимая (A_2)}	{Средние(B_2)}
{Существенная (A_3)}	{Значительные(B_3)}
{Высокая (A_4)}	{Очень большие(B_4)}



Правило 1. Если угроза незначительная, то ресурсы низкие.

Правило 2. Если угроза ощутимая, то ресурсы средние.

Правило 3. Если угроза существенная, то ресурсы значительные.

Правило 4. Если угроза высокая, то ресурсы очень большие.

Л.Заде — профессор факультета электротехники и информатики Калифорнийского университета (г. Беркли, США) — принцип несовместимости (1973).

“Чем сложнее система, тем менее мы способны дать точные и в тоже время имеющие практическое значение суждения о её поведении. Для систем, сложность которых превосходит некоторый пороговый уровень точность и практический смысл становятся почти исключающими друг друга характеристиками. Именно в этом смысле точный количественный анализ поведения гуманистических систем (т.е. систем в которых участвует человек), не имеет, по–видимому, большого практического значения в реальных социальных, экономических и других задачах, связанных с участием одного человека или группы людей.”

“В большинстве случаев лица, принимающие решения, не могут формально представить этот процесс. И дело здесь не в том, что они плохо понимают то, что делают, а в том, что неопределенность (нечеткость) лежит в самой природе принятия решений.”

“Наш мир состоит не из одних нулей и единиц — нам нужна более гибкая логика для того, чтобы представлять реальные взаимосвязи.”

“Нужны подходы, для которых точность, строгость и математический формулизм не является чем–то абсолютно необходимым и в которых используется методологическая схема, допускающая нечеткости и частичные истины.”

- Принцип “молотка” (Л.Заде);
- Нариньяни → (“кошелёк ищут под фонарём”).

Другие примеры нечетких множеств:

Нечеткие алгоритмы принятия решений в системах ЗИ

1.Классические алгоритмы принятия решений основаны на правилах “ЕСЛИ–ТО”

Например:

ЕСЛИ (условие 1) ТО (действие 1),

ЕСЛИ (условие 2) ТО (действие 2), и т.д.

Данные правила принято называть “продукциями”.

Недостатки:

- чрезмерная “жесткость”, детерминированность;
- трудности однозначного задания правил (т.е. формализации, структурирование задачи).

2 1964–1965 гг. Латфи Заде (L.Zadeh) профессор Калифорнийского университета (США) предложил новый подход к анализу сложных систем и процессов принятия решений. Он сформулировал т.н. “принцип несовместимости”,согласно которому “неточность, нечеткость является

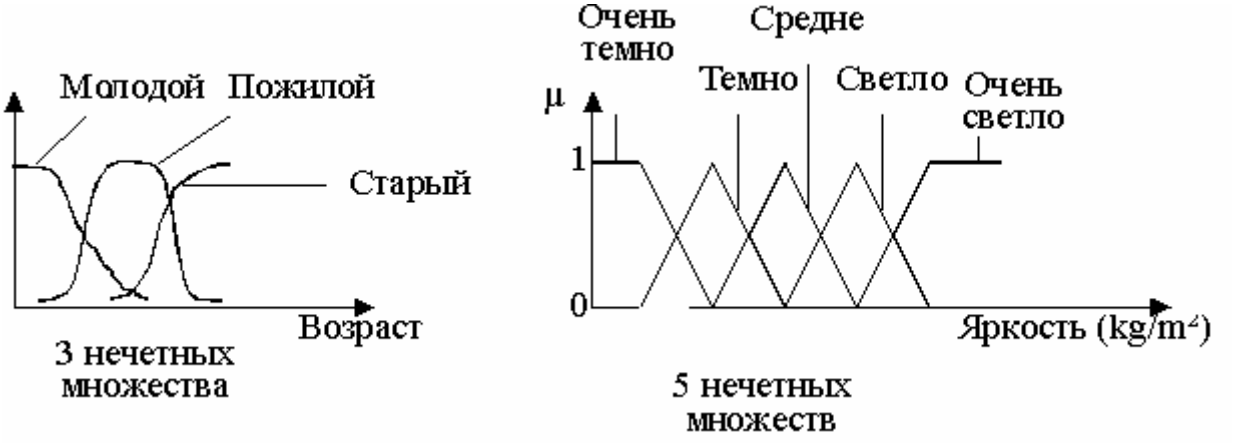
естественнымипри описании реальных сложных объектов. Они присущи самой природе этих объектов”.

Он ввел термины: Fuzzy Logic, Fuzzy Sets, Fuzzy Algorithms. Много сторонников и противников Fuzzy — бум в Японии.

3.Нечеткое множество

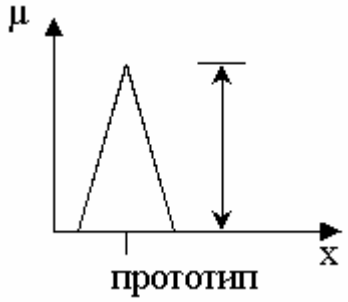
Это множество вида $A=\{(x,\mu(x)),x\in X\}$, где принадлежность каждого элемента $x\in X$ множеству A задаётся функцией принадлежности $\mu(x)\in[0,1]$.

Примеры:

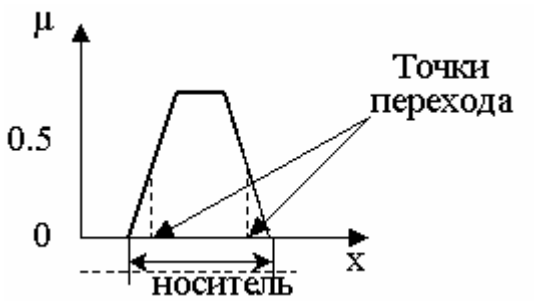


Разные способы задания функций принадлежности:

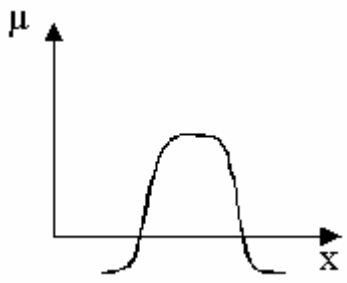
А) Треугольная



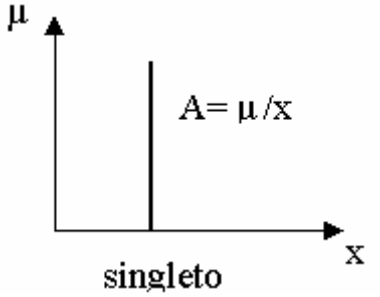
Б) Трапецеидальная



В)Колоколообразная



Г)Одноточечное нечетное



4 Лингвистическая переменная

Это переменная, значениями которой являются термы (слова, выражения).

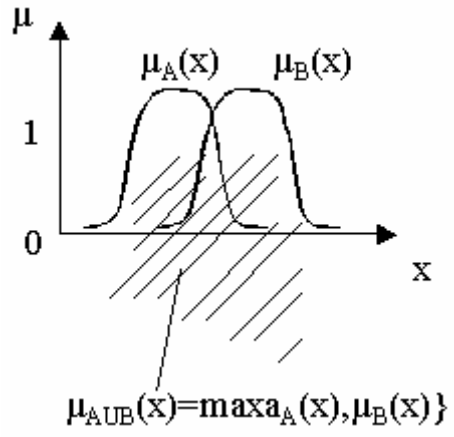
Например:

ВОЗРАСТ={МОЛОДОЙ, ПОЖИЛОЙ, СТАРЫЙ}

ЯРКОСТЬ={ОЧЕНЬ ТЕМНО, ТЕМНО, СРЕДНЕ, СВЕТЛО, ОЧЕНЬ СВЕТЛО}

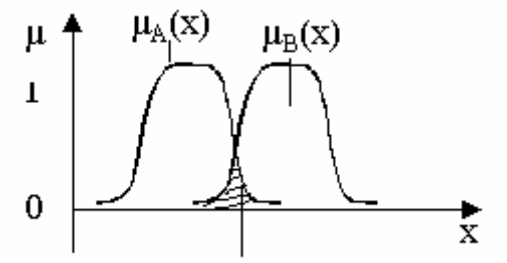
5 Операции с нечеткими множествами

6. Объединение (AUB) — соответствует логическому ИЛИ.

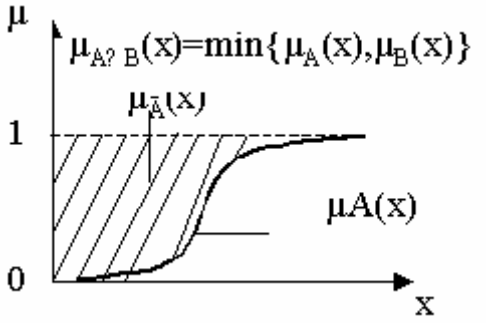


$\mu_{AUB}(x)=\max\{\mu_A(x),\mu_B(x)\}$

2 Пересечение (A∩B) — соответствует логическому И.



3 Дополнение ($\bar{A}$) — соответствует логическому НЕ.

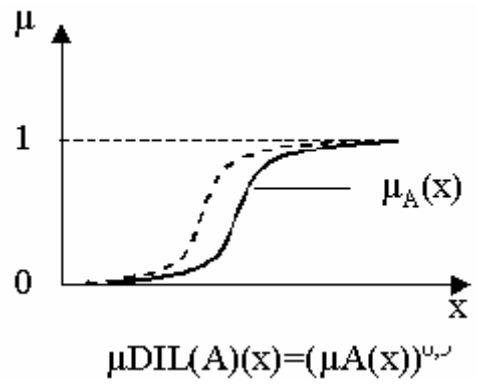


$\mu_{\bar{A}}(x)=1-\mu_A(x)$

4 Концентрация (CON(A)) — соответствует применению усиливающего термина “очень”.

$\mu_{CON(A)}(x) = \mu^2{}_A(x)$

5 Растяжение (DIL(A)) — соответствует применению термина “довольно”, выполняющего функцию ослабления.

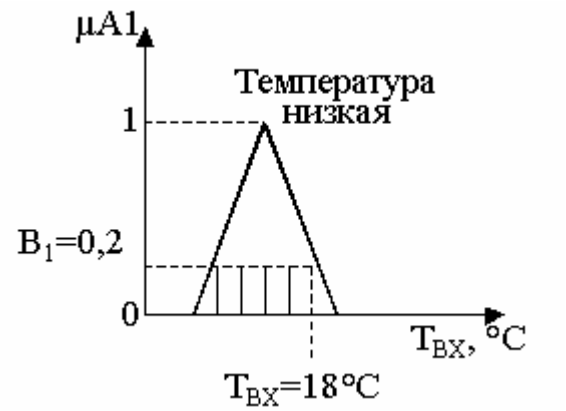


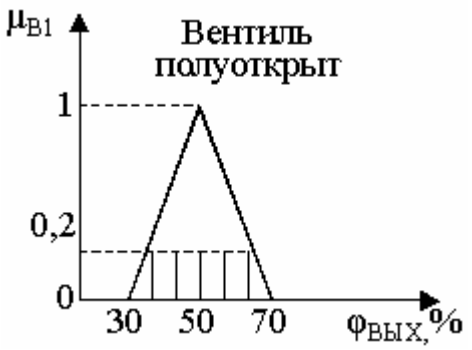
6 Нечеткий алгоритм

Это упорядоченное множество нечетких инструкций (правил), в формулировке которых создаются нечеткие высказывания.

Пример: необходимо регулировать открытие охлаждающего вентиля $\varphi_{ВЫХ}$ в зависимости от умеренного значения температуры $T_{ВХ}$

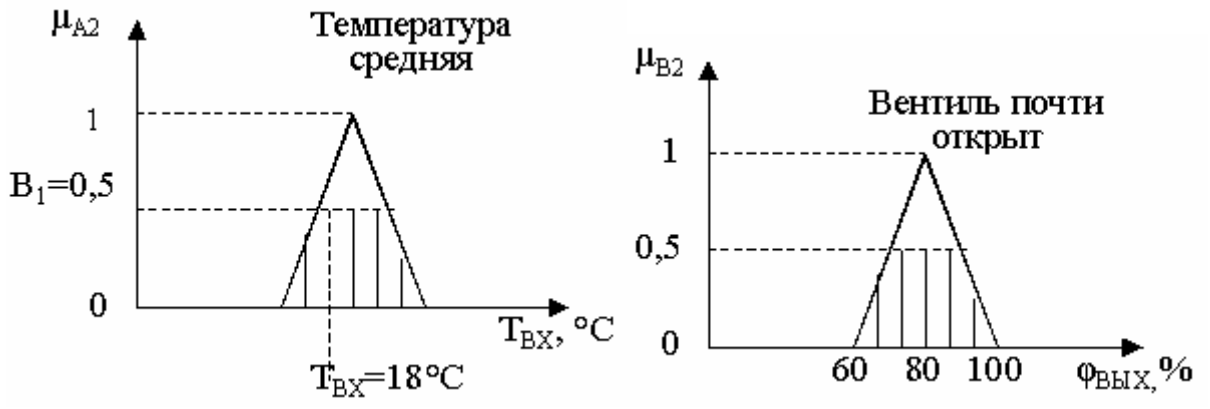
Правило 1: Если температура(A_1) низкая, то охлаждающий вентиль (B_1) полуоткрыт.





Правило (механизм) логического вывода: $\mu_{B1}(\varphi_{ВЫХ})|_{Tвх=18°c}=\min\{0,2;\mu_{B1}(\varphi_{ВЫХ})\}$.

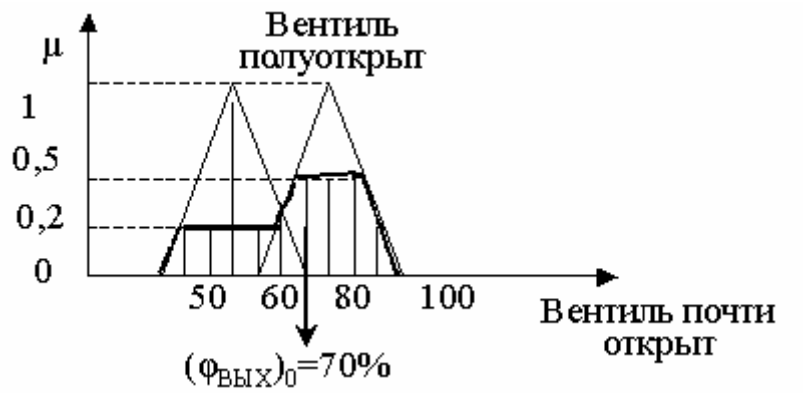
Правило 2: Если температура средняя (A_2), то охлаждающий вентиль (B_2) почти открыт.



Правило (механизм) логического вывода:

$\mu_{B2}(\varphi_{ВЫХ})|_{Твх=18°с}=\min\{0,5;\mu_{B2}(\varphi_{ВЫХ})\}$.

Результирующая функция принадлежности:



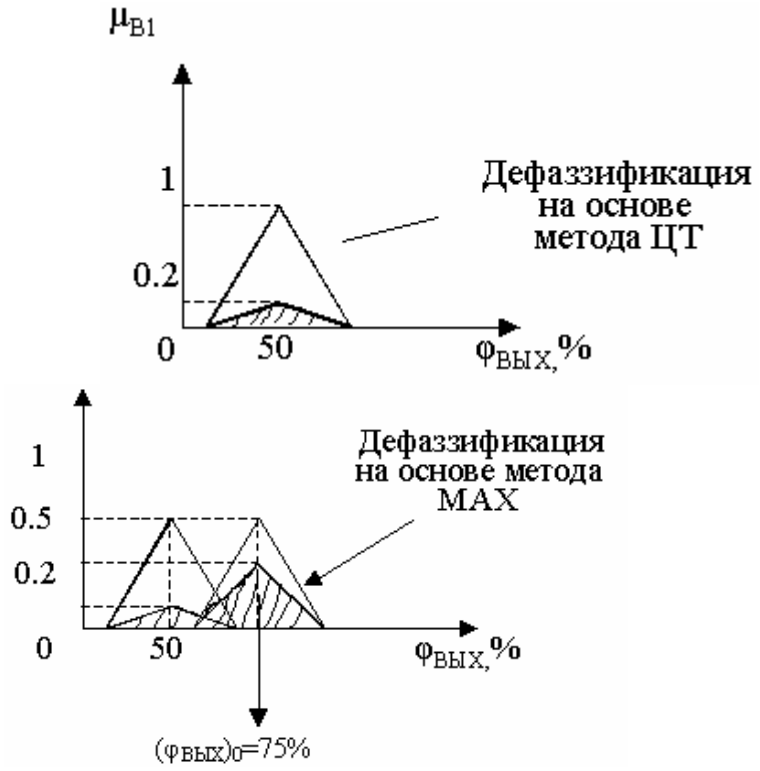
$(\varphi_{ВЫХ})_0=70\%$

Правило 1 Или Правило 2:

$\mu_{ВЫХ}=\max\{\mu_{B1}(\varphi_{ВЫХ})|_{Твх=18°с};\ \mu_{B2}(\varphi_{ВЫХ})|_{Твх=18°с}\}$ — Метод MAX–MIN.

Метод Максимума–Произведения. Методы дефаззификации.

Другой метод построения функции принадлежности выходного нечеткого множества:



$\mu_{B1}(\varphi_{ВЫХ})|_{Твх=18°с}=0{,}2*\mu_{B1}(\varphi_{ВЫХ})$

Данный метод логического вывода называется методом Максимума–Произведения.

Переход от полученного нечеткого множества к единственному (четкому) значению $(\varphi_{ВЫХ})_0$, которая и признаётся затем в качестве решения поставленной задачи называется дефаззификацией.

Методы дефаззификации:

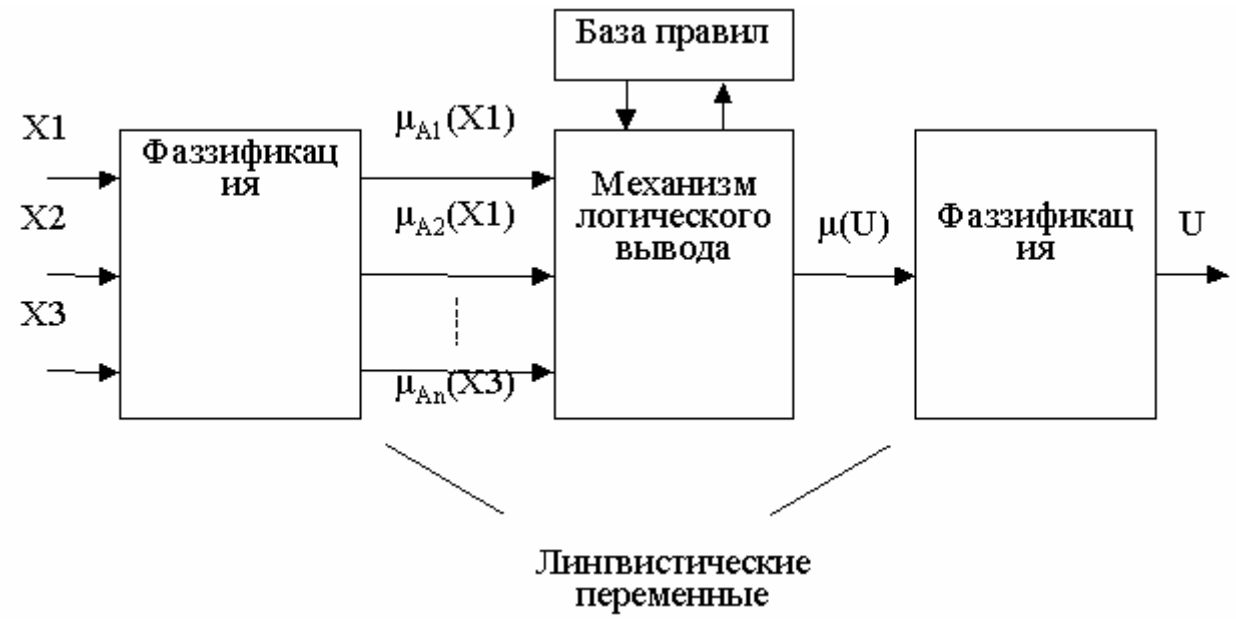
1. Метод центра тяжести (C–O–A — Center of Area) — в качестве вых. значения выбирается абсцисса центра тяжести площади под функцией принадлежности $\mu_B(y)$, т.е. $y_0=[\int_y y-\mu_B(y)dy]/[\int_y \mu_B(y)dy]$.
2. Метод максимума — выбирается то значение, которое соответствует максимуму функции принадлежности выходному множеству.
3. Метод левого (правого или средних из максимумов) — если функция принадлежности $\mu_B(y)$ имеет плато (плоскую вершину); и т.д.

Литература:

Герасименко В. А. “ЗИ в АСОД”, ч. 1, стр. 94–98.

1. Васильев В. И., Ильясов Б. Г. “Интеллектуальные системы управления с использованием нечеткой логики”, Уфа, УГАТУ, 1995.

9 Система принятия решений на основе нечеткой логики:



Intelligent (fuzzy): Control + Decision making.

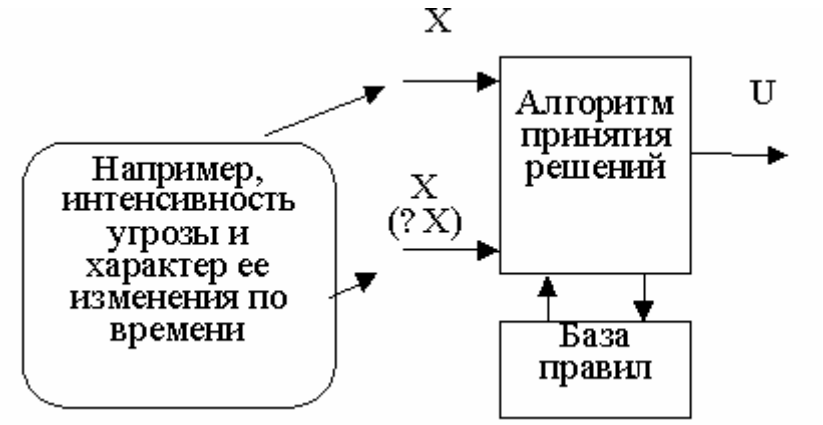
Общая процедура проектирования систем ЗИ (принятия решений по ЗИ) на основе нечеткой логики.

10 Теория нечетких множеств должна применяться в тех случаях, когда:

- Строгое описание систем и процессов их функционирования невозможно или нецелесообразно в силу самого характера решаемой задачи;
- Реализация строгого алгоритма является трудоемкой, а время на его реализацию крайне ограничено;
- Поступающая информация такого качества, что результаты реализации строгого алгоритма является сомнительными.

8 Правила принятия решений в динамических ситуациях.

В динамической модели принятия решений учитывается не только значение входной переменной, но и динамика (т. е. темп) ее изменения.



В этом случае база правил может быть представлена в виде таблицы решений (Decision table):

Z	Z	Z	Z	S	M
S	Z	Z	S	M	L
M	S	S	M	L	VL
L	M	M	L	VL	VL
VL	L	L	VL	VL	VL
X / X (ΔX)	LN	SN	Z	SP	LP

Значения выходной величины(например, затраты на ЗИ или частоты

7 Механизм логического вывода. Метод MAX — MIN.

Поскольку системы ЗИ относятся к системам с высоким уровнем неопределенности (нарушение статуса защищаемой информации, как правило, обуславливается целями и действиями людей), то методология так называемой нестрогой математики (или математики здравого смысла) должна использоваться при построении средств защиты.

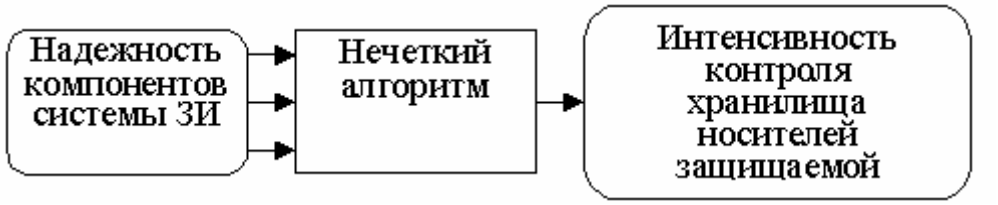
Примеры:

А) Лингвистическая переменная: вероятность доступа нарушителя к защищаемой информации может быть крайне незначительной, существенной, достаточно высокой, весьма высокой и т. п.

Б) Нечеткое высказывание: Если в системе охранной сигнализации вероятность отказа датчиков значительная, то для предупреждения проникновения

на контролируемую территорию постороннему интенсивность контроля за этой территорией должна быть повышенной.

В) Нечеткий алгоритм (сложное отношение между лингвистическими переменными):

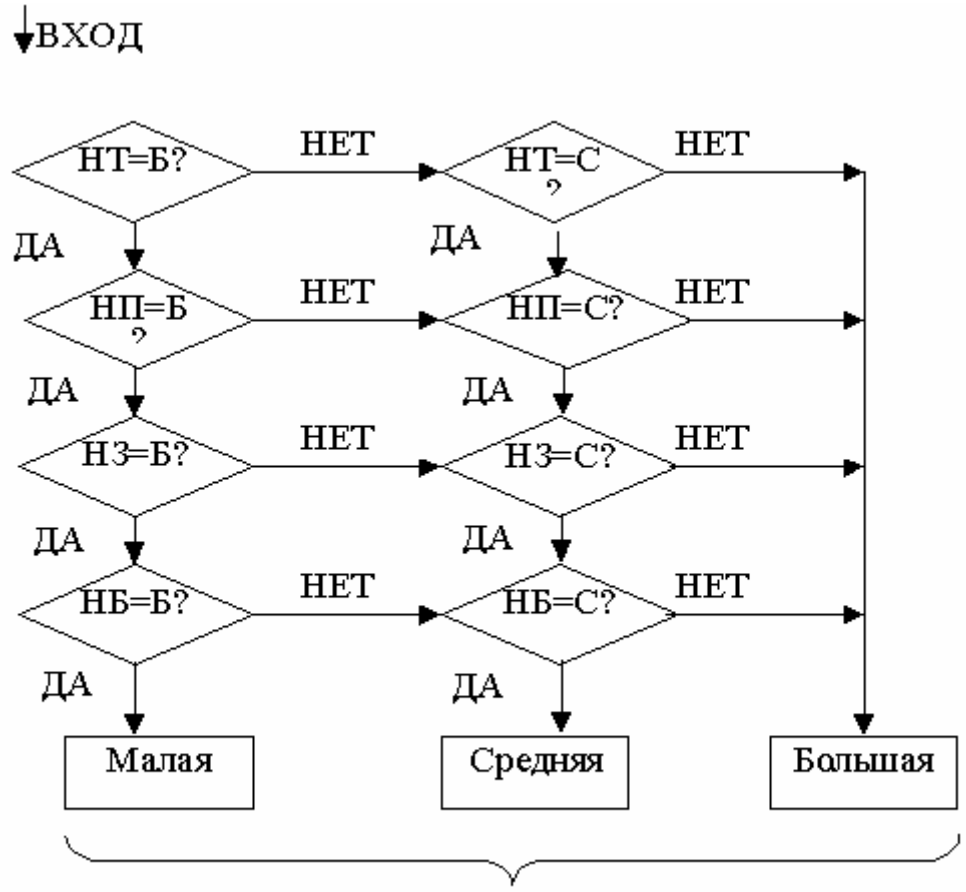


Очевидно, что интенсивность контроля должна быть тем больше, чем выше степень угрозы хищения носителей, находящихся в хранилище. Степень угрозы хищения, в свою очередь, зависит от надежности:

- Защиты территории, на которой расположены хранилища;
- Защиты помещений, в которых находятся хранилища;
- Замков на дверях хранилищ;
- Библиотекарей Хранилищ.

При этом интенсивность контроля хранилищ носителей и каждого из четырех параметров, влияющих на эту интенсивность, может принимать три возможных значения (малая, средняя, большая). Тогда нечеткий алгоритм решения данной задачи принимает вид:

Блок — схема нечеткого алгоритма принятия решений:



Интенсивность контроля хранилищ носителей

На рисунке:

НТ — надежность защиты территории, на которой расположены хранилища;

НП — надежность защиты помещений, в которых находятся хранилища;

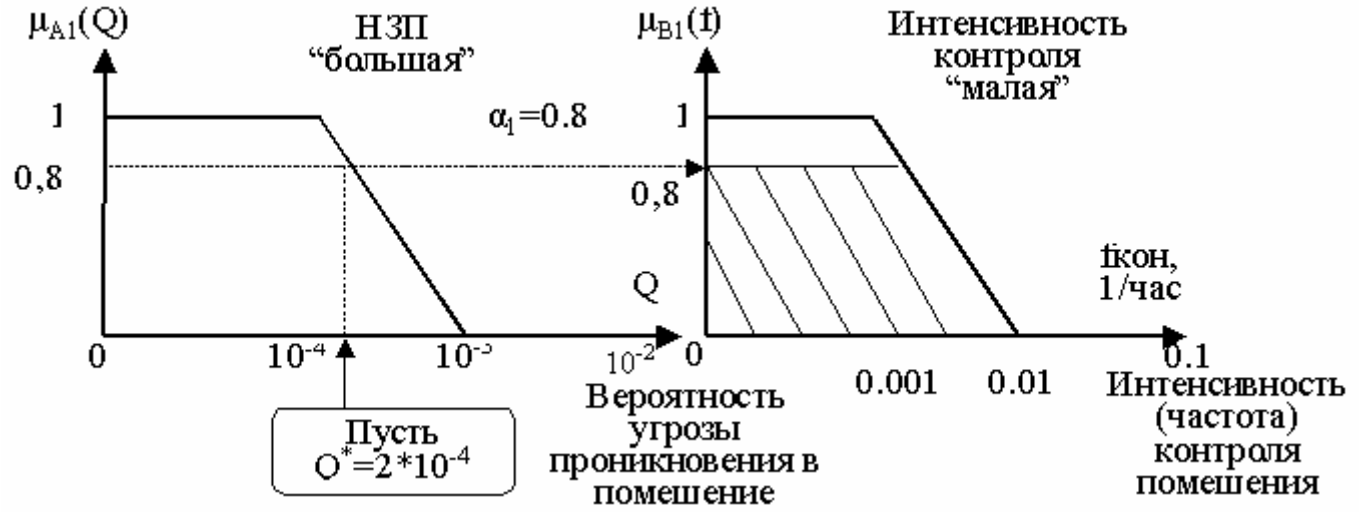
НЗ — надежность замков;

НБ — надежность библиотекарей хранилищ.

Данный алгоритм можно представить в виде системы правил (продукций). Например, правило1: ЕСЛИ надежность защиты территории “большая” И надежность защиты помещений “большая” И надежность замков “большая” И надежность библиотекарей “большая” ТО интенсивность контроля хранилищ “малая”.

Пример:

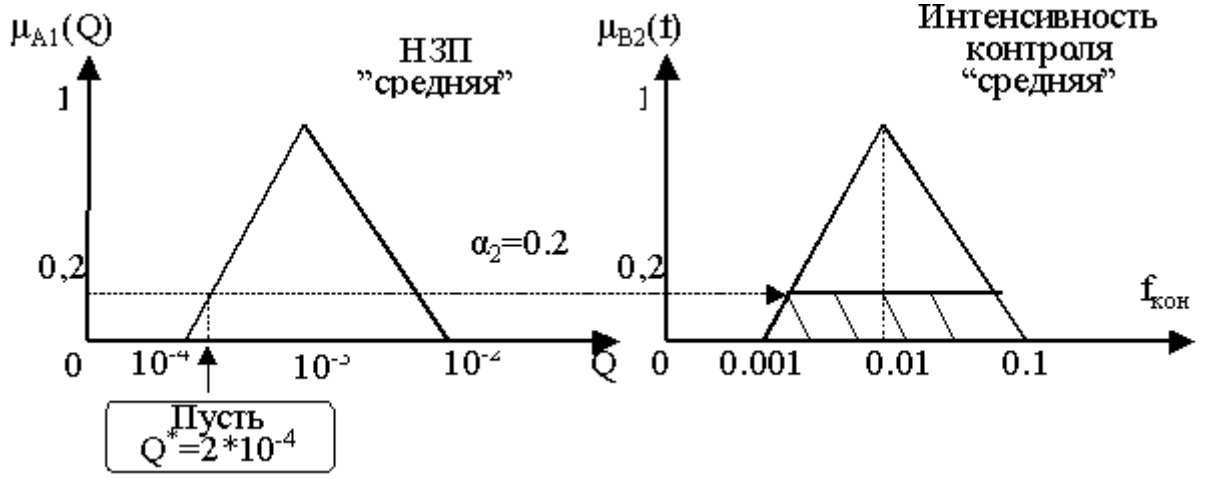
Правило 1: ЕСЛИ надежность защиты помещения “большая”, ТО интенсивность контроля “малая”.



Механизм (правило) логического вывода:

$\mu_{B1}(f_{кон})|_{Q=2*10^{-4}}=\min\{0.8; \mu_{B1}(f_{кон})\}$.

Правило 2: ЕСЛИ надежность защиты помещения “средняя”, ТО интенсивность контроля “средняя”.

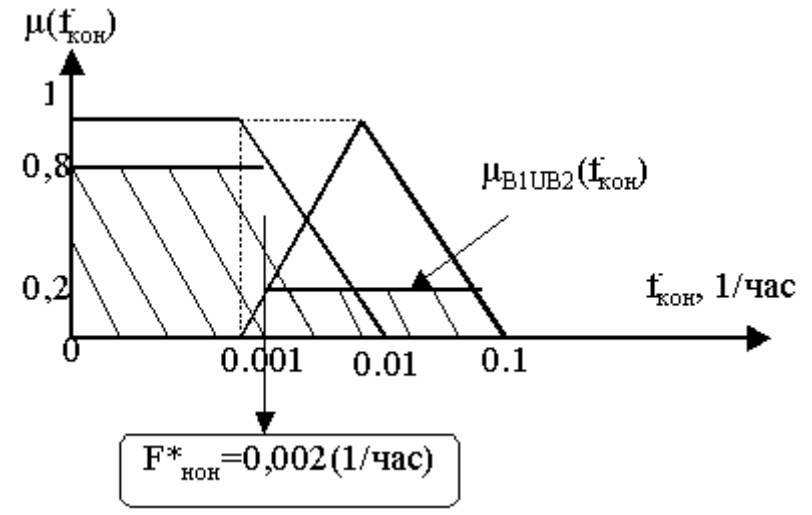


Механизм логического вывода:

$\mu_{B2}(f_{кон})|_{Q=2*10^{-4}}=\min\{0.2; \mu_{B2}(f_{кон})\}$.

Правило 1 ИЛИ правило 2:

$\mu_{B1UB2}(f_{кон})|_{Q=2*10^{-4}}=\max\ \{\mu_{B1}(f_{кон})\ |_{Q=2*10^{-4}};\ \mu_{B2}(f_{кон})\ |_{Q=2*10^{-4}}\}$ — метод MAX — MIN.



Центр тяжести:

$$F_{цт} = \frac{\int \mu(f) \cdot f \cdot df}{\int \mu(f) df} = \frac{\sum \mu(f_i) \cdot f_i \cdot \Delta f_i}{\sum \mu(f_i) \cdot \Delta f_i};$$

Процедура принятия решений на основе нелинейной логики:

- Фаззификация;
- Механизм логического вывода (метод MAX — MIN);
- Дефаззификация.

Принятие решений с использованием искусственных нейронных сетей

Термины: “Икусственные нейронные сети” (Artificial Neural Network); “Нейроматематика”; “Нейроинформатика”; “Нейрокомпьютер”; “Нейрочип”.

История вопроса:

40–е годы — термин “Нейронные сети”;

1943 — модель Мак–Каллока–Питтса;

1958 — персептрон (Ф. Розенблатт);

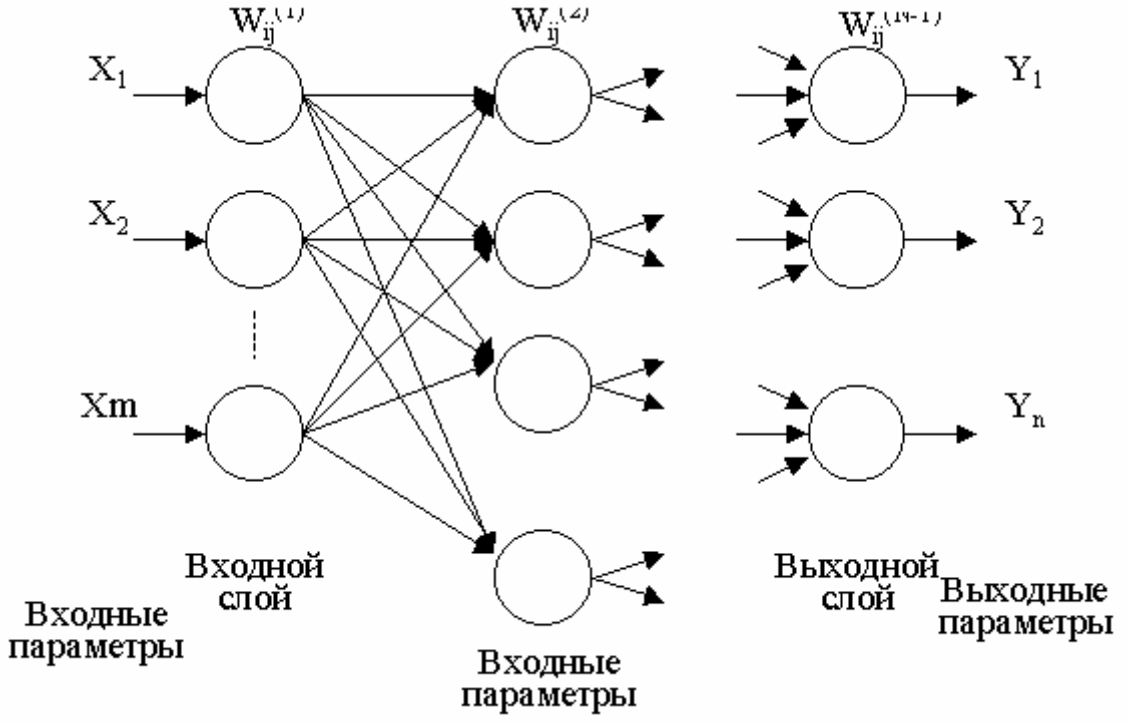
1969 — М. Мински, Пайпер (критика персептрона);

с 1988 — Нейробум (Япония).

Применение нейронных сетей в задачах ЗИ:

- Распознавание образов (лица, голоса, отпечатков пальцев, почерка, манеры работы с клавиатурой, количества атак на компьютер и т. д.).
- прогнозирование временных процессов;
- построение нелинейных моделей исследовательских сложных объектов (процессов) (например в задачах контроля датчиков).

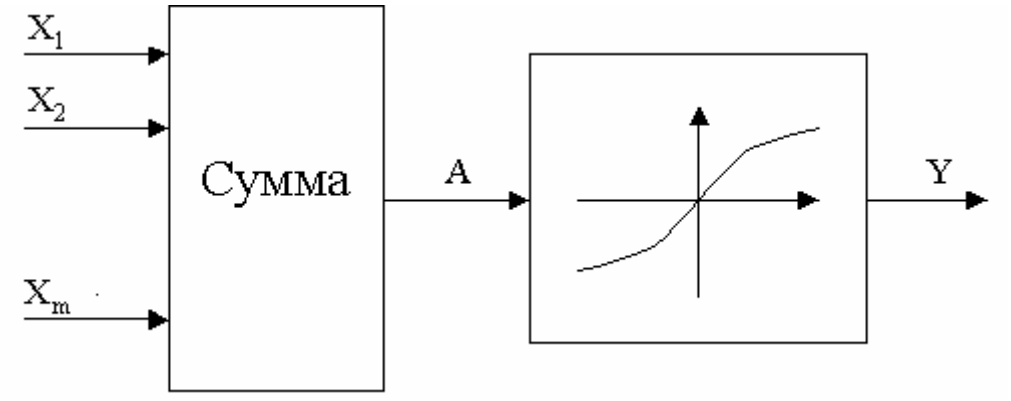
4 Структура (топология) простейшей нейронной сети — персептрона.



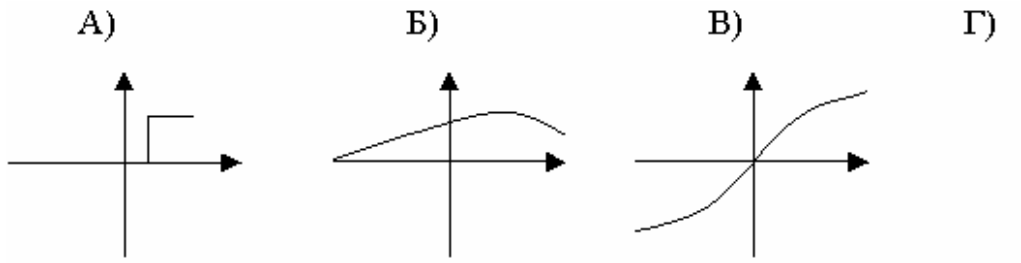
Основные свойства (признаки) персептрона:

- Нейтроны каждого слоя не связаны между собой;
- Нейтроны входного слоя не осуществляют преобразование информации;
- Выходной сигнал каждого нейтрона поступает на входы всех нейтронов следующего слоя.

Обобщенная модель нейтрона:



Примеры активации функции:



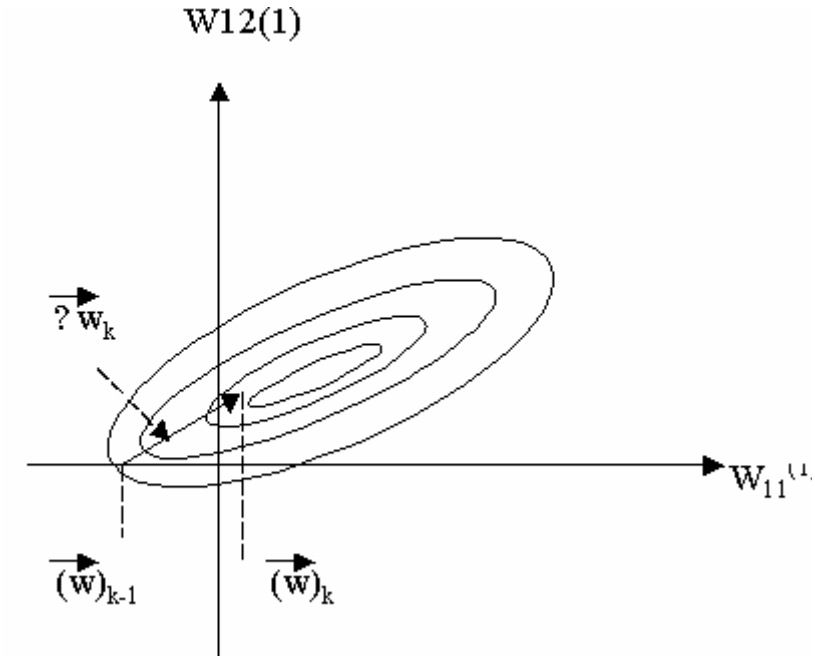
$$Y = \frac{Y_0}{C + |Y_0|}$$

$$Y = \frac{1}{1 + e^{-a \cdot Y_0}} \qquad Y = thY_0$$

Главной особенностью нейронных сетей является способность обучения весов ее синаптических связей (на примерах):

$$(w_{ij})_k = (w_{ij})_{k-1} = -c\left(\frac{\partial E}{\partial w_{ij}}\right)_{k-1}$$

5 Алгоритм обучения сети (общая процедура):



$\Delta w_k = -c \times gradE$, где $E = \sum_{i=1}^{n} \varepsilon^2 = \sum_{i=1}^{n} (d_i - y_i)^2$ — суммарная квадратическая ошибка обучения нейронной сети.

Алгоритм обучения нейронной сети:

1. Задаются начальные значения весов сети $w_{ij}^{(k)}$ (малые случайные величины);
2. На вход сети подаются вектор входных величин $X = (x_1, x_2, \dots, x_m)$;
3. Вычисляется выходная реакция нейронной сети $Y = (y_1, y_2, \dots, y_n)$;

4. Вычисляются разности $\varepsilon_i = d_i - y$, где d_i — желаемая выходная реакция по i–му выходу;
5. Вычисляются новые значения весов нейронной сети

$$(w_{ij})_k = (w_{ij})_{k-1} = -c\left(\frac{\partial E}{\partial w_{ij}}\right)_{k-1}$$

(Алгоритм обратного распространения — вначале вычисляются веса $W_{ij}^{(N-1)}$, затем $W_{ij}^{(N-2)}$, и так далее, вплоть до $W_{ij}^{(1)}$).

6) На вход сети подаются вектор $X = (x_1, x_2, \dots, x_m)$;

Обучение продолжается до тех пор, пока ошибка E не достигнет заранее заданной величины, или по достижению заданного количества циклов обучения.

Нейрокомпьютер — устройство, реализующее механизмы обучения и функционирования нейронной сети.

Способы реализации нейрокомпьютеров:

1. Программная эмуляция (нейропакеты, нейроимитаторы);
2. нейрочипы

Особенности:

- Высокое быстродействие;
- отказоустойчивость;
- помехозащищенность;
- обучение;

3. другие способы (оптические нейрокомпьютеры и др.).

Информационное оружие. Информационные войны

[PC Week, 10 июня 1997, # 22, с. 46-47]:

“Американское Министерство обороны сформулировало долгосрочную глобальную концепцию развития своей армии в XXI в.

По мнению МО США, для достижения победы в вооруженных конфликтах нового столетия необходимо в первую очередь оперативно получать, обрабатывать и передавать информацию.

Для гарантированной победы необходимо получить так называемое информационное превосходство (ИП) над противником. Оно позволит опередить врага в понимании быстро меняющейся ситуации на поле боя, принять решения, учреждающие его действия и правильно спроектировать ход сражения. Описание текущей ситуации должно быть масштабным, охватывающим все аспекты сражения, достаточно обобщенным и в то же время понятным людям, принимающим решения. Для этого требуется нетривиальные алгоритмы анализа, фильтрации и сортировки динамической информации.

ИП подразумевает также охрану собственной информации и технологии, ее обрабатывающих, ведение информационной войны, информационного шпионажа и прочих действий (в том числе и политический), которые направлены на максимальное подавление способностей вероятных противников к развитию собственных оригинальных военных технологий и приобретению информации.

Концепция ИП базируется на понятии боевого пространства (БП, battlespace), который позволяет оценить военный конфликт во всей полноте. БП включает в себя не только описание конкретной местности, где ведутся бои, но и информацию о системе материально-технического снабжения, о работе командующих всех уровней, о политических аспектах и др. Кто полнее, быстрее и точнее сможет получить описание БП, тот и будет иметь информационное превосходство. Благодаря этому командующие смогут применять силу в нужное время и в нужном месте, что позволяет решить исход сражения и даже одержать победу без кровопролития.

Концепция ИП основывается на 3-х китах:

- надо правильно понимать ситуацию в боевом пространстве;
- эффективно использовать каждую боевую единицу в сражении;
- оперативно принимать/передавать информацию в лоне БП с помощью интегрирования сети.

Что же реально дает информационное превосходство?

Американские военные выдают 4 направления использования ИП:

1. Командующие, получая оперативную информацию о местонахождении и состоянии каждого подразделения в зоне БП и о наиболее важных объектах противника, способны осуществить синхронный упреждающий маневр с нанесением ударов по ключевым целям, что сразу приведет к победе.
2. Определение наиболее значимых объектов для уничтожения и захвата.
3. ИП позволяет организовать многоплановую оборону, позволяя не опасаться неожиданной атаки противника.
4. Организация целевого материально-технического снабжения, основанного на непрерывно поступающей информации из зоны БП.

Достижение существенного преимущества в этих направлениях должно сделать, по замыслу информационных идеологов, американскую армию непобедимой.

Достижение ИП будет основываться на уникальном комплексе технологий — многофункциональной боевой информационной системе МБИС (ABIS, Advanced Battlespace Information System).

МБИС представляет собой интегрированный в глобальную информационную сеть (Internet станет лишь небольшой частью этой сети) набор распределенных программ и данных, которые предназначаются для информационного обслуживания военных конфликтов любого масштаба.

Функциональная модель МБИС не зависит от структуры управления, так как обмен информацией с подразделениями будет происходить напрямую, в интерактивном режиме.

Планируется существенный, пересмотр принципов управления армией. Придается бóльшая самостоятельность подразделениям нижнего уровня с

сохранением прямого управления или из вышестоящего центра. Любая из структур, действующих в БП, будет обладать полным доступом к информации о ходе сражения и сможет самостоятельно синхронизировать свои действия с действиями других частей.

Акцент в новом проекте делается на постоянном увеличении информационного отрыва от потенциальных противников.

Эру противостояния стратегических вооружений сменяет эра информационных войн.

[2]: 2. "Информационная война" — что это: новомодное словечко или понятие, которое действительно пополнит лексикон информационной безопасности?

Мартин Либики (Университет национальной обороны):

"Попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет ее деревом; тот, кто ощупывает его хвост, называет его канатом и т.д. Возможно, слона-то и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом..."

[2]: Определение, вышедшее из стен кабинета Директора информационных войск Министерства обороны США:

"Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой нашей собственной информации и информационных систем. Информационная война представляет собой всеобъемлющую целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах. Объектом внимания

становятся информационные системы (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений".

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести "бесконтактную" войну, в которой количество жертв (в прямом значении слова) сведено до минимума.

Высшая форма победы теперь состоит в том, чтобы выигрывать без крови.

[2]: По коридорам Пентагона гуляет шутка: "Информационная война — что это такое?" — "О, это компьютерная безопасность плюс деньги".

[2]: В отличие от компьютерного преступления, которое представляет собой факт нарушения того или иного закон и может быть случайным или специально спланированным, обособленным или частью некоторого плана атаки, ведение информационной войны подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий — будь то на реальном поле брани, либо в экономической, политической или социальной сферах.

"Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий", — сказал один из руководителей Пентагона — "Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума".

[1]: Создающееся сегодня единое мировое информационное пространство требует унификации информационных и телекоммуникационных технологий всех стран — субъектов информационного сообщества. Это дает возможность мощным индустриальным державам, таким как США и Япония, усиливать свое политическое, экономическое и военное превосходство за счет лидерства в информатизации и в принципе осуществлять глобальный информационный контроль над мировым сообществом и фактически навязывать свои правила жизни.

[1]: В докладе Объединенной комиссии по безопасности, созданной по распоряжению министра обороны и директора ЦРУ в США в июне 1993 года и завершившей свою работу в феврале 1994 года, говорится:

"…Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с "электронными скоростями" при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела.

Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны…"

[2]: В США вышло специальное «Пособие Института компьютерной безопасности по компьютерной преступности и информационной войне: существующие и потенциальные угрозы».

Комитет по правительственным делам Сената США проводит серию слушаний по компьютерной безопасности.

Администрация Клинтона намерена сформировать специальную группу в Министерстве юстиций под названием "Группа обеспечения кибербезопасности» (Cyber Security Assurance Group), призванную оказать содействие в защите компьютеров от нападений в информационном пространстве, реагировать на чрезвычайные ситуации и расследовать любые диверсии кибертеррористов.

Должна быть разработана специальная программа контроля безопасности киберпространства.

Литература:

1. Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны// Защита информации. «Конфидент», июль-август 1996, №4(10).- С. 9-12.

2. Завадский И. И. Информационная война — что это такое?// Защита информации. «Конфидент», июль-август 1996, №4(10).- С. 13-20.
3. Кузнецов П. А. Информационная война и бизнес// Защита информации. «Конфидент», июль-август 1996, №4(10).- С. 21-24.
4. Черняк Л. Информационное оружие// Мир связи и информации. Connect», сентябрь-октябрь1996.- с. 30-34.

[PC Week/RE, 15 июля 1997, # 27, с. 8]:

“Сегодня в США треть бюджета Министерства обороны расходуется на решение задач, связанных с «информационными войнами”.

“На одном из заседаний в 1996 году Совета Федерации, посвященном обсуждению стратегии развития Министерства обороны РФ, отмечалось, что на 2-ом месте после угрозы термоядерной войны (по степени нанесения потенциального ущерба для нашей страны) стоит угроза “информационной войны”.

[4]: 3. Информационное оружие — это набор средств, использующих информацию для ведения войны, начиная от дезинформации и пропаганды до средств радиоэлектронной борьбы.

Более точно, информационным оружием можно назвать средства уничтожения, искажения или хищения информационных массивов; средства преодоления систем защиты; средства ограничения допуска законных пользователей; средства дезорганизации работы технических средств, компьютерных систем.

С чисто военной точки зрения, информационное оружие можно разделить на наступательное и оборонительное.

Наступательное информационное оружие — это:

- **Компьютерные вирусы**, способные размножаться, внедрятся в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и тому подобное;
- **Логические бомбы** — программные закладные устройства, которые заранее внедряются в информационно-управляющие центры военной или

гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

- **Средства подавления** информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;
- **Средства нейтрализации** тестовых программ;
- Различного рода **ошибки**, сознательно вводимые лазутчиками в ПО объекта.

Оборонительное информационное оружие должно обеспечить доступность, целостность и конфиденциальность информации и поддерживающей ее инфрастуктуры, несмотря на агрессивные действия противника.

Иногда в шутку говорят, что подобное оружие — это информационная безопасность, на реализацию которой наконец-то нашлись деньги.

Театр информационных боевых действий — ведется на различных фронтах:

– Электронное поле боя (электронные вооружения, предназначенные для боевых действий в области командования и управления войсками или «штабной войны»);

– Атаки инфраструктуры (удары по телекоммуникационным или транспортным системам);

– Промышленный шпионаж и другие виды разведки;

– НСД к конфиденциальной информации.

[Компьютерра, 2 июня 1997 года, # 22, с. 8-9]:

Согласно данным Пентагона, первые большие испытания мощи компьютеризованных подразделений армии США показали, что при использовании компьютеров нанесение ударов по самим себе случается в 3 раза чаще, чем без их применения.

В ходе испытания боеспособности экспериментальных боевых сил (Army’s Experimental Force) было истрачено 750 млн. долларов для оснащения танков, бронетехники и воинских подразделений ПК разного рода. Теперь министр обороны

США У. Кохен и председатель совета начальников штабов Дж. Шаликашвили запрашивают еще 1 миллиард долларов.

Анализ результатов боевых учений, в которых участвовали 6 тысяч солдат и 900 единиц “компьютеризованной” боевой техники, проводившихся и марте 1997г. на полигоне Форт Ирвин (Калифорния), показал следующее. Поведение компьютеров было столь несоответствующим, что несколько десятков специалистов по их ремонту были вынуждены находится на полигоне все время, пока продолжались учения. Согласно этим результатам, не было зафиксировано никаких улучшений в таких показателях, как уровень поражения войск противника, выживаемость солдат армии США или скорость проведения операции, которые можно было бы отнести на счет применения компьютеров.

Мнение официальных лиц:

– Пока еще слишком рано делать заключение о боевых характеристиках войск, оснащенных компьютерной техникой.

Модели общей оценки угроз информации

[Герасименко В.А., ч.1, гл.4–5]

Данные модели характеризуют меру угроз информации от всей совокупности или от отдельно взятых дестабилизирующих факторов (ДФ), в соотнесении с теми потерями, которые могут иметь место при реализации угроз.

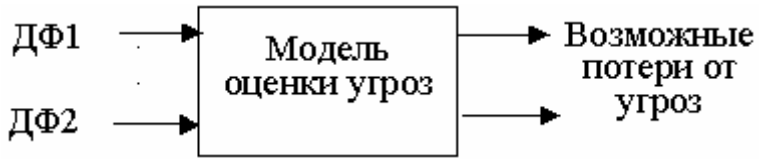


Рисунок — Соотнесение ДФ с потерями при реализации угроз

Исходная предпосылка при разработке моделей:

- с одной стороны, при нарушении защищенности информации наносится некоторый ущерб;
- обеспечение ЗИ сопряжено с расходованием средств.

Полная ожидаемая стоимость ЗИ равна сумме расходов на защиту и потерь от ее нарушения.

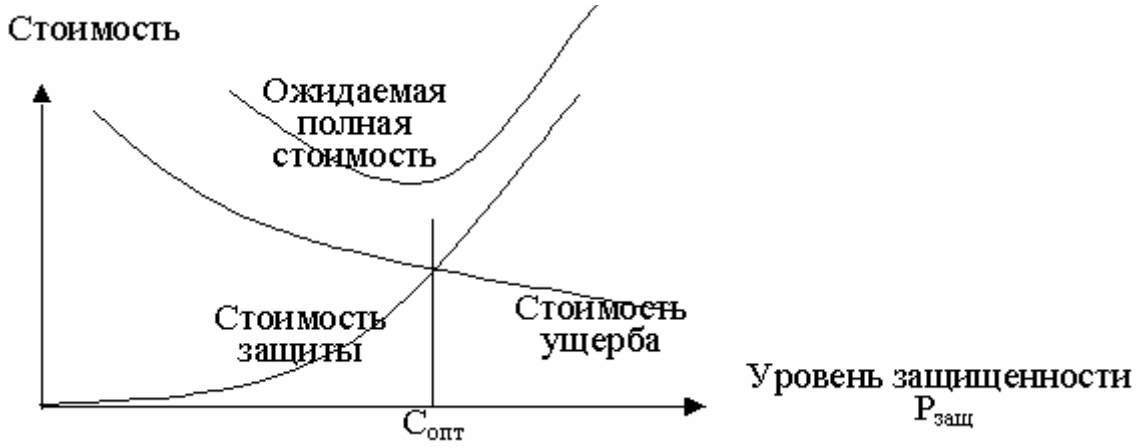


Рисунок — Соотношение между уровнем защищенности истоимостью защиты

Следовательно, Оптимальное решение соответствует минимуму общей стоимости ЗИ

Но: трудно дать оценку потерь при нарушении статуса защищенности информации, содержащей государственную, военную или другую подобную тайну

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо знать:

- полный перечень угроз информации;

- потенциальную опасность для информации каждой из угроз;
- размеры затрат, необходимые для нейтрализации каждой из угроз.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту обычно состоит в том, что этот уровень должен быть равным уровню ожидаемых потерь при нарушении защищенности ($C_{защ}=C_{ущерба}$) , то достаточно определить только уровень ожидаемых потерь ($R=C_{ущерба}$).

Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь R_i от i–й угрозы информации:

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

где: Si — коэффициент, характеризующий возможную частоту возникновения i–й угрозы;

V_i — коэффициент, характеризующий значение возможного ущерба при ее возникновении.

(Значения коэффициентов S_i и V_i смотри ниже)

Суммарная стоимость потерь:

$$R = \sum_i R_i$$

Но: данный подход является весьма приближенным и условным.

[Герасименко В.А., ч.1, с.136]

Значения коэффициента S_i:

Ожидаемая (возможная) частота появления угрозы	Предлагаемое значение S_i
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 100 лет	3
1 раз в год	4
1 раз в месяц (≈10 раз в год)	5
2 раза в неделю (100 раз в год)	6
3 раза в день (1000 раз в год)	7

Возможные значения коэффициента V_i:

Значение возможного ущерба при проявлении угрозы (долл.)	Предлагаемое значение V_i
1	0
10	1
100	2
1000	3
10000	4
100000	5
1000000	6
10000000	7