В. К. Джоган, А. П. Курило, Н. С. Шимон

ОСОБЕННОСТИ СИНТЕЗА СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Свойство иерархичности системы показателей эффективности защиты информации в компьютерных системах [1] позволяет сформировать правила структурного синтеза, в соответствии с которыми синтез системы показателей представляет собой поэтапный процесс композиции, начиная с множества элементов, отражающих исходное, несистематизированное их состояние и, через ряд промежуточных элементов, увязывающих их в связанную единой целью структуру, и заканчивая одним элементом, отражающим цель системы (рис. 1).

Иерархическая структура системы показателей эффективности защиты информации в компьютерных системах является структурой с отношениями «один ко многим». Структурные уровни иерархии характеристик формируются исходя из двух основных условий:

1) соответствие конкретному классу возможностей средств противодействия;

2) соответствие определенной степени композиции описания этих средств.

В такой структуре элементами нижнего уровня является множество характеристик средств защиты информации, получаемых в результате аудита информационной безопасности объекта информатизации, а элементы следующих уровней формируются на основе правил, устанавливающих отношения, характеризующие их влияние на классы возможностей этих средств.

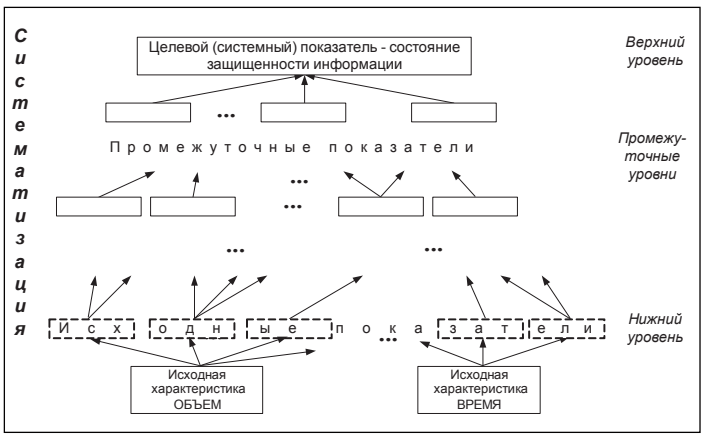

Рис. 1.

Многоуровневой структуре системы показателей эффективности защиты информации в компьютерных системах соответствует унифицированная форма их представления. Исходя из требования унифицированности методического аппарата предполагается использование для описания их свойств соответствующих математических моделей. При этом форма моделирования может видоизменяться от имитационных моделей — для оценки множества исходных характеристик, через аналитические — для оценки характеристик, являющихся производными от исходных, к логико-лингвистическим моделям — для оценки интегрального показателя. Данное положение определяет круг показателей, оценку которых целесообразно осуществлять путем логико-лингвистического моделирования. К таким показателям следует отнести показатели, которые в результате реализации процедур структурного синтеза непосредственно определяют цель защиты информации в компьютерных системах — обеспечение защищенности их информационных ресурсов.

Для синтеза системного показателя защищенности информационных ресурсов компьютерных систем как системы характеристик соответствующих механизмов защиты информации представим элементы множества B в виде:

$$b_{hi} = \langle \beta_{hi}^{(1)}, \beta_{hi}^{(2)}, \beta_{hi}^{(3)}, \beta_{hi}^{(4)} \rangle, \quad (1)$$

где $\beta_{hi}^{(1)}$ — наименование i-й, $i = 1, 2, \ldots, I_h$ характеристики h-го, $h = 1, 2, \ldots, H$ уровня иерархии их структуры;

$\beta_{hi}^{(2)}$ — класс возможностей механизмов защиты информации, определяющий данную характеристику;

$\beta_{hi}^{(3)}$ — значение характеристики;

$\beta_{hi}^{(4)} = \{\gamma_{h-1,i,j}\}$, $j = 1, 2, \ldots, I_{h-1}$ — множество характеристик $h-1$-го уровня, композиция которых формирует i-ю характеристику h-го уровня;

I_h — число характеристик h-го уровня иерархии их структуры.

С целью формализации параметра $\beta_{hi}^{(4)}$ определим на прямоугольнике $b_{hi} \times \beta_{hi}^{(4)}$ множеств b_{hi} и $\beta_{hi}^{(4)}$ композиционные отношения и опишем его соответствующей матрицей $\|\Gamma_{h-1}\|$, определяющей порядок обобщения характеристик. Элемент $\gamma_{h-1,i,j}$, $i = 1, 2, \ldots, I_h$, $j = 1, 2, \ldots, I_{h-1}$ матрицы содержит значение единица, если характеристика $b_{h-1,j}$ формирует характеристику b_{hi}, либо ноль, если связь между характеристиками $b_{h-1,j}$ и b_{hi} отсутствует.

Геометрическим изображением композиционных отношений между характеристиками является ориентированный граф:

$$G = G(B, \|\Gamma\|),$$

множества вершин и дуг которого совпадают с исходными множествами характеристик B и отношений $\|\Gamma\|$ между ними соответственно (рис. 2).

При этом собственно показатель защищенности D в терминах выражения (1) запишется в виде:

$$D = b_{Hi} = b_{H1} = \langle \delta, \delta^{(3)}, \delta^{(4)} \rangle, \quad (2)$$

где $\delta = \beta_{H1}^{(1)} = \beta_{H1}^{(2)}$;

$\delta^{(3)} = \beta_{H1}^{(3)}$;

$\delta^{(4)} = \beta_{H1}^{(4)}$.

В свою очередь, элементы множества A представляются в виде:

$$a_i = \langle \alpha_i^{(1)}, \alpha_i^{(2)}, \alpha_i^{(3)} \rangle, \quad (3)$$

где $\alpha_i^{(1)}$ — наименование i-й, $i = 1, 2, \ldots, I_1$ исходной характеристики иерархии их структуры;

$\alpha_i^{(2)}$ — класс возможностей механизмов защиты информации, определяющий данную характеристику;

$\alpha_i^{(3)}$ — значение характеристики.

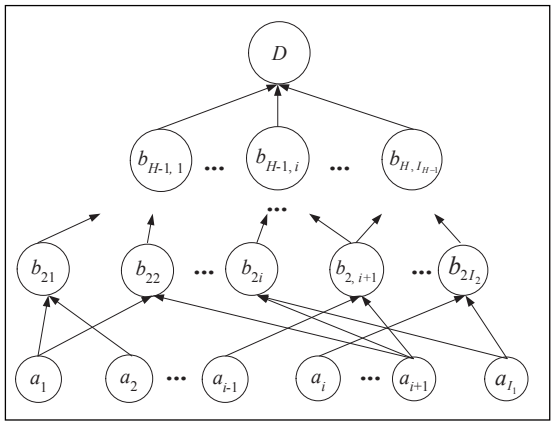

Рис. 2.

С учетом изложенных выше положений произведем структуризацию соответствующих свойств. При этом будем следовать ряду правил [3].

Правило 1. Для произвольных i-й, $i = 1, 2, \ldots, I_h$ и k-й, $k = 1, 2, \ldots, I_h$ характеристики h-го, $h = 1, 2, \ldots, H$ уровня структуры характеристик системного показателя D защищенности информационных ресурсов компьютерных систем справедливо утверждение:

$\beta_{hi}^{(2)} = \beta_{hk}^{(2)}$.

Правило 2. Для двух произвольных непересекающихся подмножеств $\{b_{hi}\}$ и $\{b_{nm}\}$ множества B характеристик справедливо условие:

$n < h$, $n = 1, 2, \ldots, H$, $h = 1, 2, \ldots, H$,

если класс возможностей $\beta_{hi}^{(2)}$ является более обобщенным, чем класс возможностей $\beta_{nm}^{(2)}$, т. е. будет характеризовать степень достижения целей реализации механизмов защиты информации в компьютерных системах в более обобщенном виде. Аналогичные рассуждения относятся и к граничным условиям: исходному множеству A характеристик и системному показателю D, характеризующему цель обеспечения защищенности информационных ресурсов компьютерных систем в самом обобщенном виде.

Правило 3. Для двух произвольных непересекающихся подмножеств $\{b_{hi}\}$ и $\{b_{nm}\}$ множества B характеристик, уровни иерархии которых связаны условием:

$n < h$, $n = 1, 2, \ldots, H$, $h = 1, 2, \ldots, H$,

будет справедливо соотношение:

$|\{b_{hi}\}| \le |\{b_{nm}\}|$, $h \ne n$.

С учетом рассмотренных методических положений дадим унифицированное формальное описание системы характеристик механизмов защиты информации в компьютерных системах в интересах синтеза показателя защищенности информационных ресурсов этих систем. При этом воспользуемся сложившейся к настоящему времени в теории информационной безопасности классификацией возможностей по обеспечению защиты информации, предполагающей их деление на четыре класса [2], применительно к:

1 — отдельным функциям защиты информации;

2 — реализации механизмов защиты информации и механизмов нарушения состояний ее защищенности;

3 — нарушениям состояния информации;

4 — целевому назначению механизмов защиты информации.

Приведенная классификация отражает степень влияния возможностей средств защиты информации на обеспечение защищенности информационных ресурсов компьютерных систем (от косвенного — класс 1, до непосредственного — класс 4).

Первый класс характеризует возможности выполнения отдельных функций защиты информации в компьютерных системах, связанные с особенностями их реализации в этих системах.

Второй класс характеризует возможности, связанные с реализацией механизмов предупреждения условий появления угроз, поиска, обнаружения и обезвреживания как самих угроз, так и их источников, а также механизмов восстановления информационных процессов после воздействия угроз.

Принимая во внимание требование иерархии показателей эффективности защиты информации, эти возможности следует рассматривать как вторичные характеристики механизмов защиты.

Третий класс характеризует возможности, связанные с предотвращением нарушения основных состояний защищенности информации — конфиденциальности, доступности и целостности. Показатели данного уровня обобщают возможности механизмов защиты информации в компьютерных системах, связанные с предупреждением условий проявления угроз, поиском,

обнаружением и обезвреживанием как самих угроз, так и их источников, а также с восстановлением информации после воздействия угроз.

Четвертый класс описывает свойство механизмов защиты информации в компьютерных системах, характеризующее степень достижения целей защиты информации в компьютерной системе — обеспечение защищенности ее информационных ресурсов. Оно выступает в качестве свойства, обобщающего возможности по обеспечению основных состояний защищенности информации.

Принимая во внимание принцип поуровневой унификации показателей эффективности защиты информации в компьютерных системах, в качестве основы для конструирования первого уровня системы этих показателей условимся использовать возможности механизмов защиты, связанные с особенностями реализации отдельных функций защиты информации в этих структурах.

При этом (3) представляется в виде:

$a_i = \langle \alpha_i^{(1)}$, «*Возможности по выполнению отдельных функций защиты информации*», $\alpha_i^{(3)} \rangle$.

Второй уровень характеризует возможности по защите информации в компьютерных системах, связанные с реализацией процедур защиты информации в этих системах, а также процедур нарушения состояний защищенности информации.

Выражение (1) для этого случая представляется в виде:

$b_{2i} = \langle \beta_{2i}^{(1)}$, «*Возможности по реализации механизмов защиты информации*», $\beta_{2i}^{(3)}$, $\beta_{2i}^{(4)} \rangle$,

$b_{2j} = \langle \beta_{2j}^{(1)}$, «*Возможности по реализации механизмов нарушения состояний защищенности информации*», $\beta_{2j}^{(3)}$, $\beta_{2j}^{(4)} \rangle$,

$i \neq j$.

Третий уровень характеризует возможности по адекватному реагированию на угрозы нарушения состояний защищенности информации: ее конфиденциальности, целостности и доступности.

Меры реагирования на угрозы нарушения состояний защищенности информации в отношении информационных ресурсов компьютерных систем считаются реализованными адекватно, если значение параметра возможностей по реализации процедур защиты информации или возможностей по реализации процедур нарушения состояний ее защищенности не превышает (либо не ниже) требуемого.

Вероятности соблюдения этих условий достаточно полно характеризуют возможности по защите информационных ресурсов компьютерных систем, связанные с адекватностью реагирования на угрозы нарушения состояний защищенности информации: ее конфиденциальности, целостности и доступности. Это позволяет использовать указанные вероятности в качестве промежуточных показателей третьего уровня синтезируемой структуры показателей эффективности защиты информации в компьютерных системах. Применительно к данному случаю выражение (1) представляется в виде:

$b_{3i} = \langle \beta_{3i}^{(1)}$, «*Возможности по адекватному реагирования на угрозы нарушения состояний защищенности информации*», $\beta_{3i}^{(3)}$, $\beta_{3i}^{(4)} \rangle$,

где $i = 1, 2, 3$;

$\beta_{31}^{(1)}$ = «*Конфиденциальность информации*»;

$\beta_{32}^{(1)}$ = «*Целостность информации*»;

$\beta_{33}^{(1)}$ = «*Доступность информации*».

Особенностью данного уровня иерархии показателей эффективности защиты информации является то, что он последний из уровней, реализующих количественную оценку значений показателей, последующий уровень обобщения предполагают оценку показателей при помощи лингвистической (качественной) шкалы [3].

Определив терм-множество значений лингвистических переменных $\{q_{ik}\}$, $k = 1, 2, \ldots, K$, являющихся значениями показателей состояний защищенности информации, а также функции принадлежности $\mu_k(\beta_{3i}^{(3)})$ количественных значений $\beta_{3i}^{(3)}$ качественным состояниям защищенности информации, переход от значений $\beta_{3i}^{(3)}$ к соответствующим значениям q_{ik} можно осуществить путем определения доминирующих термов по формуле:

$L = indexmax(\mu_k(\beta_{3i}^{(3)}))$,

$k = 1, 2, \ldots, K$.

Четвертый уровень описывает свойство, характеризующее степень достижения целей защиты информации в компьютерной системе, — обеспечение защищенности ее информационных ресурсов. Соответствующие лингвистические значения $\langle Q_k \rangle$, характеризующие показатель защищенности информационных ресурсов компьютерной системы, могут быть получены при помощи таблиц решений, в которых в качестве исходных данных используются оценки показателей третьего уровня синтезируемой системы показателей (таблица 1).

Таблица 1. Характеристическая таблица для оценки защищенности информационных ресурсов компьютерной системы

Показатели	**Комбинации оценок**			
$\beta_{31}^{(1)}$ = «*Конфиденциальность информации*»	$\langle q_{11} \rangle$	$\langle q_{12} \rangle$	…	$\langle q_{1K} \rangle$
$\beta_{32}^{(1)}$ = «*Целостность информации*»	$\langle q_{21} \rangle$	$\langle q_{22} \rangle$	…	$\langle q_{2K} \rangle$
$\beta_{33}^{(1)}$ = «*Доступность информации*»	$\langle q_{31} \rangle$	$\langle q_{32} \rangle$	…	$\langle q_{3K} \rangle$
δ = «*Защищенность информационных ресурсов*»	$\langle Q_1 \rangle$	$\langle Q_2 \rangle$	…	$\langle Q_K \rangle$

С учетом изложенного выражение (2) представляется в виде:

$D = \langle$«*Защищенность информационных ресурсов*», $\delta^{(3)}$, $\{1, 1, 1\}\rangle$.

Результаты проведенной систематизации показателей эффективности защиты информации в компьютерных системах с учетом изложенных правил наглядно представлены на рис. 3.

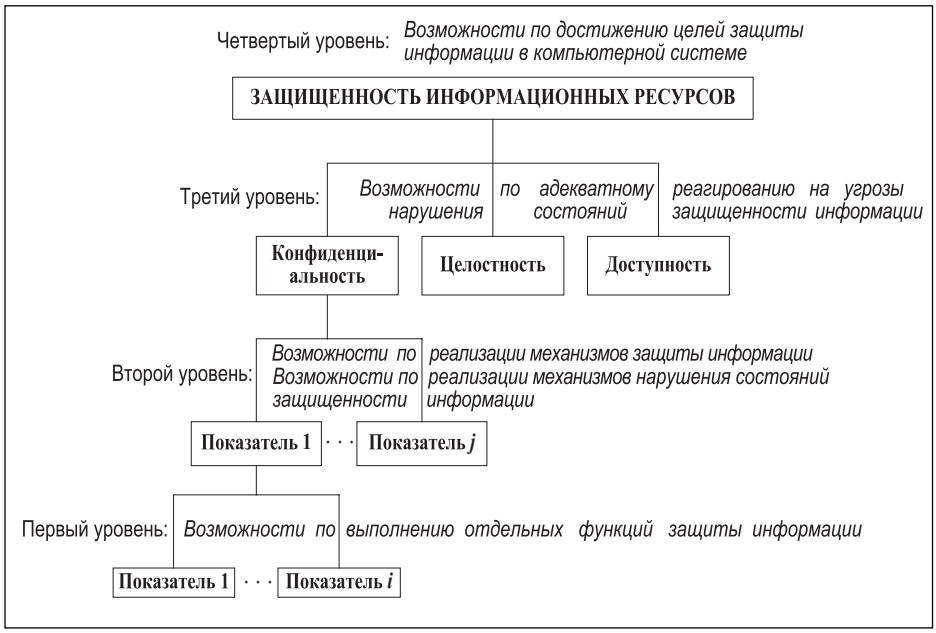

Рис. 3.

СПИСОК ЛИТЕРАТУРЫ:

1. *Курило А. П., Дураковский А. П. [и др.]*. Построения структуры показателей эффективности противодействия угрозам информационной безопасности в интересах оценки защищенности информационных процессов в компьютерных системах // Безопасность информационных технологий. 2010. № 2. С. 16–18.
2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов. М.: Горячая линия–Телеком, 2004. – 280 с.
3. *Джоган В. К.* Математическое представление структуры показателей эффективности мероприятий по комплексной защите информационных ресурсов инфотелекоммуникационных систем органов правосудия // Информация и безопасность. Воронеж: Воронежский государственный технический университет, 2010. Вып. 3. С. 455–458.