Совокупность весовых функций $w_k(n)$ позволяет уменьшить влияние краевых эффектов, возникающих за счет несовпадения амплитуды сигнала в начале обрабатываемой выборки и в конце при использовании ДПФ с естественным временным окном. В то же время система весовых функций подобрана так, что базисные функции ДПФ, взвешенные этим окном, образуют новую систему ортогональных функций – базис ДКП. Следовательно, во-первых, гарантируется отсутствие эффекта увеличения ошибок кодирования при обратном ДКП. Во-вторых, коэффициенты ДКП можно интерпретировать как спектральные отсчеты. В-третьих, можно вычислить $C_C(k)$ с помощью 2*N*-точечного алгоритма быстрого преобразования Фурье. Известно так же, что базисные векторы ДКП очень хорошо аппроксимируют собственные векторы теплицевых матриц. Это свойство позволяет рассчитывать на эффективное использование ДКП в области сжатия сигналов.

Как видно по АЧХ (см. рис. 3) коэффициенты ДКП можно интерпретировать как полосный шум с энергией, определяемой величиной соответствующего коэффициента и шириной равной частотному расстоянию этого преобразования. При этом корреляция соседних коэффициентов значительна. Однако эту проблему можно решить, если обрабатывать отдельно четные и отдельно нечетные коэффициенты преобразования.

Выводы

Сформулированы обоснованные требования, позволяющие установить наиболее перспективный класс ДОП в задачах высокоэффективной и высококачественной компрессии цифровых аудиоданных. Для целей сжатия цифровых звуковых сигналов наиболее перспективными являются ДПХ и ДКП, потенциально способные обеспечить ее максимальную эффективность.

Литература

1. Bekesy G. Ûber ein neues Audiometer // AEU. – No. 1, 1947. – P. 13.
2. Цвикер Э., Фельдкеллер Р. Ухо как приемник информации. Пер. с нем. М.: Связь, 1971. – 256 с.
3. Радиовещание и электроакустика. Под ред. Ю.А. Ковалгина. М.: Радио и связь, 2002. – 798 с.
4. Walsh J.L. A Closed Set of Orthogonal Functions // Amer. J. of Mathematics. Vol. 45, 1923. – P. 5-24.
5. Haar A. Zur Theorie der Orthogonalen Funktionensysteme // Mathematics Analytical. No. 71, 1912. – P. 38-53.
6. Поликар Р. Введение в вейвлет-преобразование. Пер. с англ. С-Пб.: АВТ-ЭКС, 2001. – 59 с.
7. Fourier J. Theorie analytique de la chaleur. Paris, 1822. – 90 s.
8. Hartley R.V.L. // Proceedings of the IRE. Vol. 30, 1942. – P. 55-62.
9. Ahmed N., Natarajan T., Rao K.R. Discrete Cosine Transform // IEEE Trans. Computers.– Vol. C-23, 1974. – P. 90-93.

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ НА ОСНОВЕ ЭКСПЕРТНЫХ СУЖДЕНИЙ

Ажмухамедов И.М.

Предложена схема построения математической модели комплексной безопасности компьютерных систем и сетей на основе экспертных суждений. Показано, что применение модифицированного метода нестрогого ранжирования позволяет определить веса Фишберна для факторов одного уровня иерархии. При этом получено обобщение данных весов на общий случай предпочтения/безразличия факторов по отношению друг к другу.

Введение

Обеспечение безопасности является одной из основных проблем функционирования компьютерных систем и сетей. Исследованию в этой области посвящено большое число работ, в которых предлагаются различные подходы.

Так, например, в [1] изложен системный подход к построению комплексной защиты информационной системы (ИС) предприятия и описана методика построения такой системы с применением отечественных технических и криптографических средств защиты. В работе [2] рассмотрены принципы и методы аудита информационной безопасности (ИБ) на основе процессорного подхода, приведены некоторые методы оценивания ИБ.

Наиболее яркое выражение системный подход к решению задач ИБ нашел в работах В.В. Домарева. Им предложена трехмерная модель информационной безопасности, включающая в себя основные этапы, направления и методы обеспечения безопасности различных систем [3]. Подчеркнуто, что специфическими особенностями задачи создания систем защиты информации (СЗИ) являются:

- неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;
- многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) СЗИ;
- наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ;
- невозможность применения классических методов оптимизации.

Нарушение безопасного режима функционирования системы может наступить в результате целого ряда взаимосвязанных между собой причин. Любые неконтролируемые внешние или внутренние процессы потенциально могут привести к возникновению угроз. Реализация этих угроз в свою очередь вызывает деструктивные процессы и оказывает негативное влияние на безопасность. Нарушается нормальное функционирование системы, что находит отражение в значениях различных критериев и показателей, используемых для оценки безопасности.

В подобных случаях критерий выбора в ситуации принятия решения (СПР) представляет собой совокупность отдельных критериев, и соответствующая задача становится многокритериальной.

При решении многокритериальных задач часто используются различные методы свертки критериев в один обобщенный (интегральный) критерий.

Наиболее простой метод построения интегрального критерия заключается в выделении одного из критериев в качестве основного, а все остальные критерии добавляются к ограничениям, в которых задается область допустимых значений вектора независимых переменных. Таким образом, задача с векторным критерием сводится к задаче принятия решения со скалярным аргументом.

Основной недостаток такого подхода заключается в том, что фактически поиск ведется лишь по одному критерию. Значения остальных критериев, если они удовлетворяют ограничениям, по существу не влияют на результаты поиска.

Кроме того, безопасность – понятие комплексное и попытка оценить ее уровень по одному какому-то параметру (например, имеющему стандартное количественное выражение) обречена на неудачу. Поэтому данный способ получения свертки при решении задач, связанных с безопасностью неприемлем.

Другими методами построения комплексного критерия являются аддитивная и мультипликативная свертка.

Аддитивный критерий, являясь наиболее простым, в тоже время из-за возможности неограниченной компенсации значений одних критериев за счет других, нечувствителен к крайним значениям отдельных критериев.

Кроме того, комплексная безопасность не может рассматриваться как простая сумма составляющих ее частей. Эти части взаимосвязаны и взаимозависимы, каждая часть критично значима. Следовательно, модели, в основе которых лежит предположение о линейном поведении системы (аддитивная свертка предполагает именно такую модель), при оценке уровня комплексной безопасности обычно не могут адекватно отражать ситуацию. Поэтому аддитивная свертка для оценки уровня безопасности, в большинстве случаев, также не подходит.

Значение же мультипликативного критерия, в отличие от аддитивного, резко уменьшается при малых значениях отдельных критериев, что позволяет исключить нежелательные варианты при принятии решения.

Таким образом, для задач, связанных с обеспечением комплексной безопасности, наиболее целесообразным представляется применение мультипликативной свертки векторного критерия:

$$K = \prod_{i=1} K_i^{\mu_i},$$

где K_i – частные критерии, μ_i – некоторым образом определенные веса, приписываемые каждому частному критерию K_i.

При построении свертки с целью унификации разнородных критериев используют переход от абсолютных значений критериев к относительным величинам.

Для этого фиксируется шкала возможных значений для критериев и возможные границы изменения для каждого из них. Например, если в качестве шкалы принять [0; 1], а границы изменения критерия K_i лежат между $K_i^{\min}$ и $K_i^{\max}$ то в качестве относительного значения критерия будет выступать величина:

$$\overline{K} = \frac{K_i - K_i^{\min}}{K_i^{\max} - K_i^{\min}} \quad .$$

Часто получение от лица, принимающего решение (ЛПР), надежной количественной информации для построения *K*, бывает затруднительным. В таких случаях стремятся получить от ЛПР, в основном, только качественную информацию. Например, о том, какой из критериев наиболее или наименее значим, какой из критериев может быть ухудшен, а для каких ухудшение крайне нежелательно и т.д.

В качестве такой процедуры получения информации может быть использован алгоритм Беленсона-Капура [4].

Многие аспекты, касающиеся безопасности системы, могут вообще не подлежать количественному измерению.

Тогда при их оценивании прибегают к искусственным приемам. Например, каждому фактору сопоставляется количественная балльная шкала [5].

При этом необходимо предложить эксперту методику, по которой он должен назначить баллы. Однако проблема заключается в том, что многие понятия, связанные с безопасностью являются сугубо качественными и, как отмечалось выше, предлагать измерять их количественно в большинстве случаев бесперспективно.

Другое дело, если сразу применять нечетко выраженные степени, например «Очень Низкая, Низкая, Средняя, Высокая, Очень Высокая».

Тогда от эксперта не требуется количественной точности, а требуется как раз субъективная оценка на естественном языке. Затем лингвистическое описание может быть сопоставлено с количественной (например, балльной) шкалой носителя с помощью методов теории нечеткого гранулирования [6].

Постановка и решение задачи

Необходимо создать методику комплексной оценки уровня безопасности компьютерной системы, основанной на качественных шкалах и отношениях предпочтения между факторами в структуре иерархии этих факторов.

Введем определение матрицы безопасности (МБ) системы *B*:

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & S_1 & T_1 \\ K_2 & F_2 & V_2 & S_2 & T_2 \\ K_3 & F_3 & V_3 & S_3 & T_3 \\ K_4 & F_4 & V_4 & S_4 & T_4 \\ - & - & - & - & - \\ K_n & F_n & V_n & S_n & T_n \end{pmatrix},$$

где K_i – показатель уровня безопасности по *i*-му критерию; F_i – тенденция изменения *i*-го критерия (возрастает, убывает, нейтрален); V_i – скорость изменения *i*-го критерия (например: очень низкая, низкая, средняя, высокая, очень высокая); S_i – степень приемлемости негативных последствий при реализации рисков, характеризуемых *i*-ым критерием; T_i – характерное для *i*-го критерия время, которое, в частности, позволяет правильно интерпретировать значения параметра V_i.

Первый и четвертый столбец МБ представляют собой вектор частных критериев безопасности и их весов и характеризуют текущее состояние комплексной безопасности, позволяя оценить сложившуюся на текущий момент времени ситуацию. Остальные столбцы матрицы отражают динамику развития процессов и позволяют строить прогноз развития на будущее.

В этом случае, мультипликативная свертка (интегральный критерий) комплексной безопасности представляет собой величину:

$$K = \prod_{i=1} K_i^{S_i}.$$

Оценки S_i могут быть получены экспертным путем. Однако для эксперта в большинстве случаев затруднительно дать непосредственные численные оценки этим коэффициентам. Поэтому предпочтительнее могут оказаться различные ранговые методы, при реализации которых требуется лишь упорядочить критерии.

Может быть использован, например, метод нестрогого ранжирования. В соответствии с этим методом экспертом производится нумерация всех критериев по убыванию степени приемлемости негативных последствий, связанных с данным критерием безопасности. Причем допускается, что эксперту не удастся различить между собой некоторые критерии. В этом случае при ранжировании он помещает их рядом в произвольном порядке. Затем проранжированные критерии последовательно нумеруются. Оценка (ранг) критерия определяется его номером.

Если на одном месте находятся несколько неразличимых между собой критериев, то, обычно, оценка каждого из них принимается равной среднему арифметическому их новых номеров [7]. Однако, представляется целесообразным несколько модифицировать такой метод оценки, приняв за ранг каждого из неразличимых критериев номер всей группы как целого объекта в упорядочении.

Таким способом могут быть оценены как степени влияния каждого параметра на частные критерии безопасности K_i, так и степени приемлемости последствий реализации угроз S_i. Например, пусть эксперт упорядочил критерии следующим образом:

$$K_5, (K_3, K_7, K_2), K_1, (K_6, K_8), K_9, K_4.$$

Критерии, не различимые между собой, объединены в круглые скобки. Тогда оценки для каждого из критериев, вычисленные в соответствии с описанной выше процедурой, равны:

$$S_5 = 1;\ S_3 = S_7 = S_2 = 2,\ S_1 = 3;\ S_6 = S_8 = 4;$$
$$S_9 = 5;\ \ S_4 = 6.$$

Применим нормирование по величине, равной сумме всех оценок:

$$R = \sum_i S_i \ .$$

В нашем случае $R = 31$. Таким образом, после линейного преобразования в шкалу [0; 1] по норме R получим:

$$S_5 = 1/31;\ S_3 = S_7 = S_2 = 2/31,\ S_1 = 3/31;$$
$$S_6 = S_8 = 4/31;\ S_9 = 5/31;\ S_4 = 6/31.$$

Найденные предложенным способом оценки представляют собой обобщение системы весов Фишберна [8] для случая смешанного распределения предпочтений, когда наряду с предпочтениями в систему входят и отношения безразличия.

Полученный результат согласуется с хорошо известным в теории принятия решений фактом [5; 7; 9]: системе убывающего предпочтения альтернатив наилучшим образом отвечает система снижающихся по правилу арифметической прогрессии весов.

Угрозы, влияющие на безопасность системы, представляют собой набор неупорядоченных факторов одного уровня иерархии.

Влияние различных факторов на уровень комплексной безопасности может быть представлено в виде ориентированного графа G, имеющего одну корневую вершину и не содержащего петель и горизонтальных ребер в пределах одного уровня иерархии:

$$\mathrm{G} = <\{F_i\};\ \{D_{ij}\} >,$$

где $\{F_i\}$ – множество факторов (вершин графа); $\{D_{ij}\}$ – множество дуг, соединяющих i-ю и j-ю вершины; $F_0 = K$ – корневая вершина, отвечающая уровню комплексной безопасности в целом (интегральному критерию безопасности). При этом дуги расположены так, что началу дуги соответствует вершина нижнего уровня иерархии (ранга), а концу дуги – вершина ранга, на единицу меньшего.

Примером такого графа, может служить четырехуровневый граф, в котором на нижнем, третьем уровне расположены обозначенные через N_i негативные факторы, влияющие на безопасность системы и Z_i – «демпфирующие» факторы, связанные с применением превентивных мер защиты и призванные ослабить влияние определенных угроз (негативных факторов). На уровень выше расположены обозначенные через U_i угрозы безопасности системы. На первом, предпоследнем уровне находятся частные критерии безопасности K_i. И, наконец, корневой вершине нулевого уровня соответствует комплексный критерий безопасности K.

Следует заметить, что данный связный граф не является деревом, поскольку не выполняется требование отсутствия простых циклов. Это обусловлено тем, что факторы, находящиеся на нижнем уровне иерархии, могут одновременно оказывать влияние на несколько факторов более высокого уровня.

Например, применение превентивных мер защиты от одной угрозы может одновременно с ослаблением негативных последствий этой угрозы усиливать или уменьшать влияние какой-либо другой угрозы. Или некоторые негативные факторы могут вызвать изменение сразу нескольких частных критериев безопасности (иногда в противоположном направлении).

Для дальнейшего построения модели комплексной безопасности системы на полученный граф необходимо наложить систему отношений предпочтения одних факторов другим по степени их влияния на заданный элемент следующего уровня иерархии:

$$\mathrm{E} = \{F_i(\mathrm{e})\ F_j \mid \mathrm{e} > (> ; \approx)\}, \qquad (1)$$

где F_i и F_j – факторы одного уровня иерархии, $>$ – отношение предпочтения, $\approx$ – отношение безразличия. Такая система может быть получена, например, изложенным выше способом нестрогого ранжирования.

Пример наложения системы отношений предпочтения типа (1) $\mathrm{E} = \{N_1 > N_2;\ N_2 > N_3 \approx N_4\ ;\ N_4 \approx N_5\}$ на фрагмент графа изображен на рис.1.

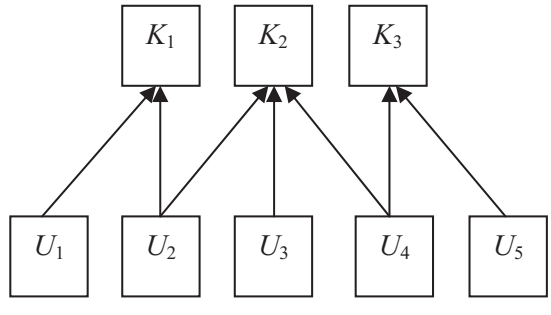

Рис. 1. Пример системы отношений предпочтения на одном из уровней иерархии

Остается ввести в рассмотрение набор качественных оценок уровней каждого фактора в иерархии:

L = {Очень низкий уровень (ОН),
Низкий уровень (Н), Средний уровень (С),
Высокий уровень (В), Очень высокий уровень (ОВ)}. (2)

Тогда, в качестве математической модели оценки комплексной безопасности системы (KBS) может быть принят кортеж:

$$KBS = <G, L, E> .$$

Выводы

Полученное описание может быть использовано для построения показателя уровня комплексной безопасности компьютерных систем и сетей на базе агрегирования значений со всех уровней иерархии факторов на основе качественных данных об уровнях факторов и их отношениях порядка на одном уровне иерархии.

Применение модифицированного метода нестрогого ранжирования позволяет определить веса Фишберна для факторов одного уровня иерархии. При этом получено обобщение данных весов на общий случай предпочтения/безразличия факторов по отношению друг к другу.

Литература

1. Садердинов А.А.,Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. М.: ИТК «Дашков К°», 2005. – 336 с.
2. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. – М.: Изд. БДЦ-пресс, 2006. – 304 с.
3. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ООО ТИД Диа Софт, 2004. – 992 с.
4. Попов Г.А. Экономическая кибернетика. Астрахань: Изд. ЦНТЭП, 2002. – 96 с.
5. Трухаев Р.И. Модели принятия решений в условиях неопределенности. М.: Наука, 1981. – 144 с.
6. Недосекин А.О. Нечеткий финансовый менеджмент. М., Аудит и финансовый анализ, 2003. – 76 с.
7. Литвак Б.Г. Экспертная информация: методы получения и анализа. М.: Радио и связь, 1982. – 92 с.
8. Фишберн П. Теория полезности для принятия решений. М.: Наука, 1978. – 155 с.
9. Рыжов А.П. Элементы теории нечетких множеств и измерения нечеткости. М.: Диалог-МГУ, 1998. – 102 с.

УДК. 621.395.4

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ КОЭФФИЦИЕНТА ПРЕВЫШЕНИЯ В СИСТЕМЕ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Маслов О.Н., Раков А.С.

В статье представлены результаты исследования характеристик коэффициента превышения в системе активной защиты (САЗ) конфиденциальной информации (КИ), выполненного методом статистического имитационного моделирования (СИМ).

Введение. Исходные определения и соотношения

При проектировании и анализе эффективности САЗ КИ [1-3] с применением компьютерного метода СИМ [3-5] и универсального лабораторного стенда для исследования случайных антенн (СА) [4] важно уяснить роль и место проводимых работ в системе мероприятий по выявлению каналов утечки КИ. Согласно [2], в данную систему входят специальные проверки технических средств (ТС); специальные обследования подлежащих защите помещений (ПЗП) и специальные исследования (СИ), включающие анализ и прогнозирование возможности формирования каналов утечки КИ за счет побочных электромагнитных излучений и наводок (ПЭМИН), наличия соединительных линий (СЛ) электропитания, заземления, управления и сигнализации; а также по акустическим, виброакустическим и др. каналам. Главным принципом при проведении СИ является анализ любой потенциально возможной утечки КИ как реально существующей угрозы, – которую следует воспроизвести и промоделировать (изучить механизм воздействия, вычислить характеристики и параметры канала утечки, оценить последствия). В этой связи оборудование стенда призвано обеспечивать проведение максимально широкого круга работ, связанных с организационным и методическим обеспечением СИ для ТС различного назначения. Однако в первую очередь нужно исследовать условия формирования каналов утечки КИ через СА за счет ПЭМИН.

Схема стенда должна удовлетворять двум противоречивым требованиям [4]. С одной стороны (по техническим и экономическим соображениям) он должен быть максимально компактным и