ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056

КОМПЛЕКСНАЯ ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ НА ОСНОВЕ ЭКСПЕРТНЫХ СУЖДЕНИЙ

Ажмухамедов И.М.

Предложен метод оценки комплексной безопасности компьютерных систем и сетей на основе экспертных суждений. Показатель уровня комплексной безопасности построен на базе агрегирования значений со всех уровней иерархии факторов на основе качественных данных об уровнях факторов и их отношениях порядка на одном уровне иерархии.

Введение

В [1] показано, что в качестве математической модели оценки комплексной безопасности системы (KBS), основанной на экспертных суждениях, может быть принят кортеж

$$\mathrm{KBS} = <\mathrm{G, L, E}>, \qquad (1)$$

где $G = <\{F_i\};\{D_{ij}\}>$ – ориентированный граф, отражающий влияние различных факторов на уровень комплексной безопасности, имеющий одну корневую вершину и не содержащий петель и горизонтальных ребер в пределах одного уровня иерархии; $\{F_i\}$ – 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; L – набор качественных оценок уровней каждого фактора в иерархии:

$$\mathrm{L} = \{\text{очень низкий уровень (ОН), низкий уровень (Н), средний уровень (С), высокий уровень (В), очень высокий уровень (ОВ)}\}. \qquad (2)$$

На граф G наложена система отношений предпочтения одних факторов другим по степени их влияния на заданный элемент следующего уровня иерархии:

$$\mathrm{E} = \{F_i\ (\mathrm{e})\ F_j \mid \mathrm{e} > (> ; \approx)\}, \qquad (3)$$

где F_i и F_j – факторы одного уровня иерархии, $>$ – отношение предпочтения, $\approx$ – отношение безразличия. Данная система может быть получена, например, изложенным в [1] способом нестрогого ранжирования.

Примером такой модели 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*.

Построим теперь показатель уровня комплексной безопасности на базе агрегирования значений со всех уровней иерархии факторов на основе качественных данных об уровнях факторов и их отношениях порядка на одном уровне иерархии.

Метод комплексной оценки безопасности

Чтобы произвести оценку уровня комплексной безопасности количественно и качественно, необходимо произвести агрегирование данных, собранных в рамках иерархии G. При этом агрегирование совершается по направлению дуг графа иерархии.

Агрегированию должно подлежать не отдельное значение выбранной функции принадлежности в структуре лингвистической переменной «Уровень фактора», а вся функция принадлежности целиком.

Сформируем лингвистическую переменную «Уровень фактора» с термножеством значений L вида (2). В качестве семейства функций принадлежности может выступать стандартный пятиуровневый 01-классификатор [2], где функции принадлежности – трапециевидные нечеткие числа:

$$\text{ОН: } \mu_1(x) = \begin{cases} 1;\ 0 \le x < 0{,}15; \\ 10(0{,}25 - x);\ 0{,}15 \le x < 0{,}25; \\ 0;\ 0{,}25 \le x \le 1. \end{cases} \qquad (3.1)$$

$$\text{Н: } \mu_2(x) = \begin{cases} 0;\ 0 \le x < 0{,}15; \\ 10(x - 0{,}15);\ 0{,}15 \le x < 0{,}25; \\ 1;\ 0{,}25 \le x < 0{,}35; \\ 10(0{,}45 - x);\ 0{,}35 \le x < 0{,}45; \\ 0;\ 0{,}45 \le x \le 1, \end{cases} \quad (3.2)$$

$$\text{С: } \mu_3(x) = \begin{cases} 0;\ 0 \le x < 0{,}35; \\ 10(x - 0{,}35);\ 0{,}35 \le x < 0{,}45; \\ 1;\ 0{,}45 \le x < 0{,}55; \\ 10(0{,}65 - x);\ 0{,}55 \le x < 0{,}65; \\ 0;\ 0{,}65 \le x \le 1, \end{cases} \quad (3.3)$$

$$\text{В: } \mu_4(x) = \begin{cases} 0;\ 0 \le x < 0{,}55; \\ 10(x - 0{,}55);\ 0{,}55 \le x < 0{,}65; \\ 1;\ 0{,}65 \le x < 0{,}75; \\ 10(0{,}85 - x);\ 0{,}75 \le x < 0{,}85; \\ 0;\ 0{,}85 \le x \le 1, \end{cases} \quad (3.4)$$

$$\text{ОВ: } \mu_5(x) = \begin{cases} 0;\ 0 \le x < 0{,}75; \\ 10(x - 0{,}75);\ 0{,}75 \le x < 0{,}85. \\ 1;\ 0{,}85 \le x \le 1. \end{cases} \quad (3.5);$$

В (3.1)-(3.5) x – это 01-носитель (отрезок [0,1] вещественной оси). Стандартный классификатор осуществляет проекцию нечеткого лингвистического описания на 01-носитель, при этом делает это непротиворечивым способом, симметрично располагая узлы классификации (0,1; 0,3; 0,5; 0,7; 0,9) [3]. В этих узлах значение соответствующей функции принадлежности равно единице, а всех остальных функций – нулю. Неуверенность эксперта в классификации убывает (возрастает) линейно с удалением от узла (с приближением к узлу, соответственно). При этом сумма функций принадлежности во всех точках носителя равна единице.

Построенный классификатор есть разновидность так называемой «серой» шкалы Поспелова [4], представляющей собой полярную (оппозиционную) шкалу, в которой переход от свойства A^+ к свойству A^- происходит плавно, постепенно.

Подобные шкалы удовлетворяют условиям: а) взаимной компенсации между свойствами A^+ и A^- (чем в большей степени проявляется A^+, тем в меньшей степени проявляется A^-, и наоборот); б) наличия нейтральной точки A^0, интерпретируемой как точка наибольшего противоречия, в которой оба свойства присутствуют в равной степени. В случае нашего нечеткого классификатора это абсциссы нейтральных точек: (0,2; 0,4; 0,6; 0,8).

Таким образом, мы переходим от качественного описания уровня параметра к стандартному количественному виду соответствующей функции принадлежности (нечеткое трапециевидное число).

Пусть по каждому показателю (F_{*1} ... F_{*n}) на выбранном подуровне (*) иерархии G известны лингвистические оценки L = (L_{*1} ... L_{*n}), а также определена система весов Фишберна P = (p_{*1} … p_{*n}) на основе приведенной выше системы предпочтений E. Тогда показатель подуровня F* характеризуется своей лингвистической оценкой, определяемой функцией принадлежности на 01-носителе *x*.

В подобных случаях для агрегирования обычно применяется OWA-оператор Ягера [5], причем весами в свертке выступают упомянутые выше коэффициенты Фишберна.

Однако, как было показано в [1], аддитивная свертка и осреднение для оценки уровня безопасности системы неприемлемы и необходимо использовать мультипликативную свертку для нахождения интегральных критериев

$$\mu_*(x) = \prod_{i=1}^{n} \mu_{*i}^{p_i}(x), \text{ где} \quad (4)$$

$$\mu_{*.i}(x) = \begin{cases} (3.1), \text{если } L_{*.i} - \text{очень низкий}; \\ (3.2), \text{если } L_{*.i} - \text{низкий}; \\ (3.3), \text{если } L_{*.i} - \text{средний}; \\ (3.4), \text{если } L_{*.i} - \text{высокий}; \\ (3.5), \text{если } L_{*.i} - \text{очень высокий}. \end{cases} \quad (5)$$

Полученную функцию (4) необходимо лингвистически распознать, чтобы выработать суждение о качественном уровне показателя F_*. Для этого необходимо соотнести полученную функцию $\mu_*(x)$ и функции $\mu_i(x)$ вида (3). Если

$$(\forall x \in [0,1])\ \sup \min(\mu_*(x), \mu_i(x)) = 0, \quad (6)$$

то уровень показателя F_* однозначно не распознается как уровень, которому отвечает *i*-ая «эталонная» функция принадлежности. Стопроцентное распознавание наступает, если выполняется

$$(\forall x \in [0,1])\ \min(\mu_*(x), \mu_i(x)) = \mu_i(x). \quad (7)$$

Во всех промежуточных случаях необходимо задаться мерой уровня распознавания, то есть ввести, так называемый индекс схожести (ИС) [6]. Для этого нужно определить понятие расстояния между двумя нечеткими числами *A* и *B*. В качестве такой величины может выступать линейное (хемингово)

$$\rho(A;B) = \int_0^1 \left|\mu_A(x) - \mu_B(x)\right| dx, \qquad (8)$$

или квадратичное (евклидово) расстояние

$$\rho(A;B) = \int_0^1 \sqrt{\left(\mu_A(x) - \mu_B(x)\right)^2}\ dx. \qquad (9)$$

Для определения ИС необходимо вычислить расстояние в точках, где выполняется условие

$$\mu_*(x) < \mu_i(x)) . \qquad (10)$$

С целью повышения информативности, удобно перейти к относительному расстоянию:

$$\tilde{\rho} = \rho / \mathrm{M} \qquad (11)$$

где M – «мощность» эталонного нечеткого числа, равная площади фигуры, описываемой его функцией принадлежности. В нашем случае это площадь трапеции и M = (0,3 + 0,1)*1/2 = 0,2.

Для того, чтобы избежать лингвистического несоответствия (чем выше степень близости, тем больше должен быть индекс схожести) и учитывая, что $\rho(A;B) \le 1$, в качестве ИС можно принять величину:

$$\text{ИС} = 1 - \rho(A;B) . \qquad (12)$$

Тем самым, ИС, изменяясь в диапазоне от 0 до 1, будет характеризовать близость найденной мультипликативной свертки к той или иной эталонной функции принадлежности вида (3).

Следует заметить, что при нахождении сверток значения некоторых показателей для сохранения лингвистического соответствия необходимо предварительно инвертировать. Например, при переходе от уровня негативных факторов N_i и превентивных мер защиты Z_i на уровень угроз безопасности U_i перед нахождением свертки необходимо инвертировать значения показателя Z_i, а при переходе с уровня U_i к уровню частных критериев безопасности K_i, инвертировать значения U_i согласно таблицы 1.

Таблица 1. Инверсия лингвистических переменных

№ терм-множества	Уровень показателя F	Инвертированное значение F
1	ОН	ОВ
2	Н	В
3	С	С
4	В	Н
5	ОВ	ОН

Таким образом, пройдя последовательно снизу вверх по всем уровням иерархии G и применяя соотношения (1)-(12), мы не только можем путем комплексного агрегирования данных выработать суждение о качественном уровне показателя на каждой ступени иерархии (вплоть до $F_0 = K$), но и оценить степень обоснованности данного суждения с помощью ИС.

Таблица 2. Факторы и их уровни («*» – предстоит определить)

Шифр фактора	Наименование фактора	Уровень фактора	На какие факторы влияет
K	Комплексная оценка информационной безопасности	*	–
K_1	Критерий защищенности от атак на целостность информации	*	K
K_2	Критерий защищенности от атак на доступность информации	*	K
K_3	Критерий защищенности от информационных атак	*	K
U_1	Уровень «программных» угроз информации	*	K_1 K_2, K_3
U_2	Уровень физических угроз информации	*	K_1 K_2, K_3
U_3	Уровень «внутренних» угроз информации	*	K_1 K_2, K_3
N_1	Уровень вирусной активности	Средний	U_1
N_2	Уровень техногенных угроз информационной безопасности	Низкий	U_2
N_3	Уровень угроз физического проникновения на объект	Высокий	U_2
N_4	Уровень «агрессивности» персонала организации	Средний	U_3

Таблица 2. (окончание)

Шифр фактора	Наименование фактора	Уровень фактора	На какие факторы влияет
Z_1	Уровень использования программных средств антивирусной защиты	Средний	U_1
Z_2	Уровень физической защиты объекта	Низкий	U_2
Z_3	Уровень контроля за деятельностью персонала	Средний	U_3
Z_4	Уровень настроек политик безопасности	Высокий	U_1, U_3

Если кроме качественных значений показателей имеются и количественные данные, то простейшим способом для их совместного учета при комплексной оценке является загрубление полученных количественных оценок до качественного их описания, и последующий переход к изложенной выше модели оценки.

Расчетный пример

Оценим комплексную информационную безопасность компьютерной системы по критериям защищенности от атак на целостность, конфиденциальность и доступность информации. Исходные данные для расчетов приведены в таблице 2.

При этом существует следующая система отношения предпочтений факторов:

$$\text{для } K: K_1 \succ K_2 \approx K_3 \rightarrow (2/4;\ 1/4;\ 1/4),$$
$$\text{для } K_1: U_1 \approx U_2 \succ U_3 \rightarrow (2/5;\ 2/5;\ 1/5),$$
$$\text{для } K_2: U_1 \succ U_2 \succ U_3 \rightarrow (3/6;\ 2/6;\ 1/6),$$
$$\text{для } K_3: U_1 \approx U_3 \succ U_2 \rightarrow (2/5;\ 2/5;\ 1/5),$$
$$\text{для } U_1: N_1 \approx Z_1 \succ Z_4 \rightarrow (2/5;\ 2/5;\ 1/5),$$
$$\text{для } U_2: N_3 \approx Z_2 \succ N_2 \rightarrow (2/5;\ 2/5;\ 1/5),$$
$$\text{для } U_3: N_4 \succ Z_3 \approx Z_4 \rightarrow (2/4;\ 1/4;\ 1/4).$$

В скобках указаны соответствующие системе предпочтений веса Фишберна, найденные описанным выше способом нестрогого ранжирования.

Необходимо оценить уровень комплексной информационной безопасности.

Таблица 3. Результаты расчетов

Показатель	Наименование фактора	Уровень фактора
K	Комплексная оценка информационной безопасности	низкий (0.95)
K_1	Критерий защищенности от атак на целостность информации	низкий (0,82) / средний (0,78)
K_2	Критерий защищенности от атак на доступность информации	средний (0,90) / низкий (0,80)
K_3	Критерий защищенности от информационных атак	средний (0,94) / низкий (0,79)
$U1$	Уровень «программных» угроз информации	средний (0,96)
$U2$	Уровень физических угроз информации	В.(0,65) / С.(0,55)
$U3$	Уровень «внутренних» угроз информации (инсайдинг)	средний (0,95)

Результаты расчетов приведены в таблице 3 (в скобках рядом с уровнем фактора указано значение индикатора схожести с эталонной функцией распределения).

Видно, что, несмотря на близость показателей K_2 и K_3 к уровню «средний», показатель комплексной безопасности K имеет значение «низкий». Это обусловлено тем, что показатель K_1, имеющий значение «низкий», оказывает по оценкам экспертов большее влияние на уровень комплексной безопасности компьютерной системы, чем K_2 и K_3.

Выводы

Предложенный метод на основе экспертных суждений может быть применен для оценки комплексной безопасности различных систем. При этом элементы, характеризующие систему, образуют иерархию, а факторы одного подуровня иерархии состоят в отношениях предпочтения/безразличия друг к другу. В качестве интегрированного критерия при оценке безопасности используется мультипликативная свертка.

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

Разработанный алгоритм проиллюстрирован на примере оценки уровня комплексной информационной безопасности компьютерной системы.

Литература

1. Ажмухамедов И.М. Математическая модель безопасности на основе экспертных суждений // ИКТ. Т.7, №4, 2009. – С. 103-107.
2. Рыжов А.П. Элементы теории нечетких множеств и измерения нечеткости. М.: Диалог-МГУ, 1998. – 102 с.
3. Kaufmann A., Gupta M. Introduction to Fuzzy Arithmetic: Theory and Applications. Van Nostrand Reinhold, 1991. – 161 p.
4. Поспелов Д.С. «Серые» и/или «черно-белые» [шкалы] // Прикладная эргономика. Спец. выпуск «Рефлексивные процессы». №1, 1994. – С.15-21.
5. Yager R. Families of OWA operators // Fuzzy Sets and Systems. 59, 1993. – P.53-59.
6. Проталинский О.М. Применение методов искусственного интеллекта при автоматизации технологических процессов. Астрахань: Изд. АсГТУ, 2004. – 184 с.

УДК 621.394.76

АНАЛИЗ АРХИТЕКТУР КЛАСТЕРОВ ДЛЯ СЕТЕВЫХ ЗАДАЧ

Уривский А.В., Чефранова А.О.

В статье проводится анализ архитектур построения кластеров для обработки и защиты информации, передаваемой по сетям связи. Строится теоретическая модель вычислений с учетом особенностей сетевой обработки и возможности реализации кластера из широкодоступных неспециализированных компонент. Архитектуры сравниваются по критериям производительности, отказоустойчивости и требованиям к пропускной способности сетей.

Введение

Один из способов организации высокопроизводительных вычислений состоит в параллельной обработке поступающего потока заданий на нескольких независимых элементах, образующих вычислительный кластер. Обычно элементами кластера (далее – ЭК) являются отдельные компьютеры или серверы, связанные одной или несколькими локальной коммуникационными сетями.

Регулированием состава кластера можно добиться заданной производительности. В мировом листинге суперкомпьютеров Топ-500 порядка 80% участников являются кластерами. Другой особенностью кластеров является обеспечение отказоустойчивости за счет естественного дублирования основных функций различными ЭК. Важным также является и то, что кластеры могут создаваться из уже имеющихся и широкодоступных стандартных компонент. В частности в качестве ЭК могут выступать устаревающие компоненты относительно низкой производительности. При этом характеристики кластера будут соответствовать современному уровню. Именно такого рода кластеры, создаваемые из неспециализированных компонент, являются предметом нашего исследования.

В основном кластеры используется для вычислительно трудоемких научных расчетов. Однако с интенсивным развитием инфокоммуникационных сетей высокие требования по производительности предъявляются и к сетевому оборудованию. Речь идет об исполнении разнообразных сетевых заданий: маршрутизации и транзитной обработке данных, защите информации и фильтрации трафика, почтовых службах, и т. п. Можно выделить некоторые особенности таких заданий. Во-первых, количество заданий, поступающих в единицу времени для обработки, весьма велико. Во-вторых, сложность отдельного задания относительно мала. В-третьих, обычно можно считать, что сложность задания линейно зависит от объема самого задания и/или результата исполнения. Указанные особенности существенно облегчают балансировку заданий по отдельным элементам кластера, но предъявляют специальные требования к организации их взаимодействия.

Кластер с точки зрения источника заданий и потребителя результатов представляется единым логическим сетевым элементом. При одной и той же физической организации, которая диктуется в основном используемой сетевой технологией, возможны различные логические архитектуры – способы организации взаимодействия множества ЭК. Наиболее важные архитектурные вопросы включают в себя маршрутизацию заданий и результатов обработки внутри кластера и балансировку (распределение) заданий по ЭК для обеспечения заданных характеристик. В этой статье мы рассмотрим, как влияет выбор архитектуры на