УДК 004.056

ЭКСПЕРТНАЯ ОЦЕНКА УРОВНЯ ИНТЕГРАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА

© 2022 К. А. Плющик

Воронежский институт ФСИН России (Воронеж, Россия)

На базе теории нечетких множеств решается задача экспертной оценки уровня информационной безопасности объекта в условиях внешних деструктивных воздействий. Предлагается метод, позволяющий решить эту задачу при наличии нечисловых параметров, определяющих информационную безопасность объекта, и в условиях их взаимозависимости. Метод может найти применение при разработке компьютерных систем поддержки принятия решений в системах обеспечения безопасности социально-экономических объектов.

Ключевые слова: информационная безопасность, нечеткое множество, функция принадлежности.

Формулировка задачи. Задача оценки уровня интегральной информационной безопасности заключается в том, чтобы, зная множество частных показателей, характеризующих отдельные аспекты информационной безопасности некоторого объекта, получить обобщенную оценку уровня его информационной безопасности в целом. Например, по ряду криптографических, технических, организационных и других показателей некоторой инфокоммуникационной сети необходимо дать обобщенную оценку степени ее информационной защищенности. Для решения таких задач, как правило, используются методы математической свертки, общим недостатком которых является предположение о независимости частных показателей информационной безопасности и возможности их количественного измерения, что не всегда представляется возможным. В статье предлагается экспертный метод, основанный на положениях теории нечетких множеств [1, 2, 3], реализация которого позволяет решить данную задачу при отказе от указанных допущений.

Сущность подхода заключается в имитации нестрогой логики мышления эксперта при оценке им информационной безопасности объекта, в замене количественных переменных на качественные, а также в использовании нечетких (эвристических) правил для установления функциональных зависимостей между частными показателями и интегральной оценкой. Метод реализуется при следующих предположениях:

– эксперт имеет представление о критических параметрах, характеризующих информационную безопасность объекта, воспринимает взаимосвязи этих параметров и умеет оперировать правилами, связывающими параметры с их оценками;

– эксперт предпочитает использовать лингвистические оценки показателей безопасности, не гарантирующие математической оптимальности, но позволяющие принимать достаточно эффективные решения в сложных управленческих ситуациях;

– любая лингвистическая переменная исчерпывающим образом описывается функцией принадлежности, а логический критерий выбора состоит в том, чтобы в качестве решения выбирать такое значение переменной, при котором функция принадлежности принимает максимальное значение.

Формализация. Пусть имеется объект Q и известны $X = \{x_1, x_2,\ldots, x_N\}$ – его входные параметры (управления), $Y = \{y_1, y_2,\ldots, y_K\}$ – выходные параметры, $Z = \{z_1, z_2,\ldots, z_M\}$ – внешние деструктивные воздействия. Будем считать, что X, Y и Z определяют состояния объекта $s \in S$, отражают его информационную безопасность в некоторый фиксированный момент времени t. Кроме того, для каждого

Плющик Кирилл Александрович – Воронежский институт ФСИН России, адъюнкт, e-mail: victor_novo@mail.ru.

параметра из множеств X, Y, Z известны его норма и допустимое отклонение от этой нормы δx*, δy*, δz*, а так же δx, δy, δz – текущие отклонения параметров от нормы.

Моделью объекта M_Q назовем кортеж $<\eta_x(X), \eta_y(Y), \eta_z(Z), \eta_s^{tec}(X,Y,Z)>$, где $\eta_x(X)$, $\eta_y(Y)$, $\eta_z(Z)$ – оценочные функции входных, выходных и внешних параметров; $\eta_s^{tec}(X,Y,Z) = \eta_s(\eta_x(X), \eta_y(Y), \eta_z(Z))$ – оценочная функция текущего состояния объекта в части его информационной безопасности. При выборе функций η_x, η_y, η_z и η_s будем исходить из того, что сами функции и взаимные зависимости их аргументов нельзя задать количественно, но можно выразить качественно, используя нечеткое η-пространство со шкалами ⟨T, P, η⟩, где T – лингвистическая шкала «часто-редко», определенная на интервале от «никогда» до «всегда», с числовым представлением [0, 1]; P – лингвистическая шкала «больше-меньше» с числовым представлением [0, 1]; η – лингвистическая шкала, элементы которой принимают значения на интервале от «хуже не бывает» до «лучше не может быть», с числовым представлением [–1, +1].

Введем предположение, что среди множества состояний s ∈ S существует нормальное состояние s*∈ S, соответствующее требуемому уровню информационной безопасности, и характеризующееся нулевыми отклонениями текущих параметров от их нормальных значений. Оценочную функцию такого состояния обозначим символом η_s*.Тогда интегральная оценочная функция информационной безопасности объекта Ω_{tec} есть кортеж $<\eta_s^{tec}(X,Y,Z), \eta_s^*, \rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))>$, где $\rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))$ – функция, выражающая степень близости текущего состояния к нормальному состоянию, а задача сводится к определению M_Q через оценочные функции $\eta_x(X)$, $\eta_y(Y)$, $\eta_z(Z)$, $\eta_s^{tec}(X,Y,Z)$ и к нахождению правил вычисления η_s^* и $\rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))$.

Определим M_Q через ее компоненты $\eta_x(X)$, $\eta_y(Y)$, $\eta_z(Z)$, $\eta_s^{tec}(X,Y,Z)$ как:

$$\eta_X(X) = \Phi\,(\eta^*_x(X), \mu(x)),$$

где

$$\eta^*_x(X) = \begin{cases} \xi(1-e^{-\upsilon(t-c_1)}); c_1 < t \le 1; \\ (-1+e^{\upsilon(t-c_1)}); 0 < t \le c_1; \\ (1-e^{-(t-c_2)}); c_2 < t \le 1; \\ \xi(-1+e^{\upsilon(t-c_2)}); 0 < t \le c_2 \end{cases} –$$

максимальная и минимальная по значениям оценочной функции огибающая по шкале η ∈ [–1,+1], построенная при условии, что δx = 0; ξ ∈ [0,+1] – экспертный коэффициент разброса оценочной функции $\eta_X(X)$, задаваемый экспертом; υ ∈ [0, 1] – параметр энтропии, характеризующий степень неопределенности знаний эксперта об информационной безопасности объекта; t – аргумент модели, совпадающий по значениям и смыслу со шкалой T; c_1 и c_2 – значения шкалы T для огибающих зависимостей по максимальным (c_1) и минимальным (c_2) значениям оценочных функций;

$$\mu(x) = 2(e^{-\lambda\frac{\delta x}{\delta x^*}} - 0{,}5)\ ,\ \mu(x) \in [-1,+1]$$

– функция принадлежности δx/δx* к области значений лингвистической переменной «норма по параметру»; λ ∈ [0,+1] – экспертный коэффициент, характеризующий жесткость требований к допустимому отклонению параметра от его нормативного значения.

Связь между $\eta^*_x(X)$ и μ(x) выразим функцией [4]:

$$\phi(f_1(x), f_2(x)) = \begin{cases} f_1(x) + f_2(x), \\ \text{signf}_1(x) \ne \text{signf}_2(x); \\ min((f_1(x), f_2(x)) + \\ +F(max(f_1(x), f_2(x))), \\ \text{signf}_1(x) = \text{signf}_2(x); \end{cases}$$

где $f_1(x) \in [-1,+1]$, $f_2(x) \in [-1,+1]$;

$$F(\alpha) = \begin{cases} -(\alpha+1)^2; -1 \le \alpha < -0{,}5; \\ -\alpha^2; -0{,}5 \le \alpha < 0; \\ \alpha^2; 0 \le \alpha < 0{,}5; \\ (\alpha-1)^2; 0{,}5 \le \alpha \le 1. \end{cases}$$

Аналогично определим оценочные функции выходных параметров $\eta_y(Y)$ и внешних возбуждений $\eta_z(Z)$. Оценочную функцию состояния объекта определим так

$$\eta_s^{tec}(X,Y,Z) = \Phi\,(\varphi(\eta_x(X), \eta_y(Y), \eta_z(Z))),$$

где $\eta_s^* = = \begin{cases} 1 - e^{-12(t-1,5)}; & 1,5 \le t \le 2; \\ -1 + e^{12(t-1,5)}; & 0 \le t < 1,5, \end{cases}$

а для определения $\rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))$ введем меру близости $s_i, s_j \in [-1, +1]$

$$\rho(s_i, s_j) = \frac{min(max\,\eta_{s_i}, max\,\eta_{s_j}) - max(min\,\eta_{s_i}, min\,\eta_{s_j})}{max(max\,\eta_{s_i}, max\,\eta_{s_j}) - min(min\,\eta_{s_i}, min\,\eta_{s_j})}.$$

Для нахождения $\eta_x(X)$, $\eta_y(Y)$, $\eta_z(Z)$, введем трехмерное ρ-пространство в шкалах ⟨T, P, ρ⟩, где ρ – шкала значений лингвистической переменной «мера близости состояний», определенная на интервале [+1, –1] от «строгое совпадение» до «полное несовпадение». Во введенном ρ-пространстве интегральная оценка нечеткой близости состояний определяется как [5]

$$\Omega_{tec}(\rho(s_i, s_j)) = \int_{t=0}^{t=2} \rho(s_i, s_j) tdt.$$

Тогда для получения интегральной оценочной функции необходимо вместо s_i подставить η_s^*, а вместо s_j – $\eta_s^{tec}(X,Y,Z)$. Окончательно имеем

$$\Omega_{tec}(\rho(\eta_s^*, \eta^{tec}(X,Y,Z))) = \frac{1}{4}[2 + \int_{t=0}^{t=2} \rho(\eta_s^*, \eta^{tec}(X,Y,Z)) tdt].$$

Заключение. В статье предложен экспертный метод оценки уровня интегральной информационной безопасности объекта в условиях внешних деструктивных воздействий, основанный на использовании положений теории нечетких множеств. Преимущества этого метода заключается в том, что он позволяет решить поставленную задачу при наличии нечисловых параметров, определяющих информационную безопасность объекта, и в условиях их взаимозависимости.

СПИСОК ИСТОЧНИКОВ

1. Заде Л.А. Понятия лингвистической переменной и его применение к принятию приближенных решений / Л. А. Заде. – М.: Мир, 1976. – 165 с.

2. Борисов А. Н. Принятие решений на основе нечетких моделей: Примеры использования / А. Н. Борисов, О. А. Крумберг, И. П. Федоров. – Рига: Зинатне, 1990. – 184 с.

3. Вересков А. А. Определение степеней принадлежности на основе совокупности матриц Саати для нечетких множеств / А. А. Вересков, В. Б. Кузькин, В. В. Федоров // Сб. тр. ВНИИСИ. – М., 1982. – № 10. – С. 117-124.

4. Жаке-Лагрез Э. Применение размытых отношений при оценке предпочтительности распределенных величин / Э. Жаке-Лагрез // Статистические модели и многокритериальные задачи принятия решений. – М.: Статистика, 1979. – С. 168-183.

5. Левиатов А. Ю. Непрямые методы диагностики / А. Ю. Левиатов, В. Н. Захаров // Международный симпозиум по искусственному интеллекту. – Л.: ISAI, 1983. – С. 67-72.

EXPERT ASSESSMENT OF THE LEVEL OF INTEGRATED INFORMATION SECURITY OF THE OBJECT

© 2022 K. A. Plushik

Voronezh Institute of the Federal Penitentiary Service of Russia (Voronezh, Russia)

On the basis of the theory of fuzzy sets, the problem of expert assessment of the level of information security of an object in the conditions of external destructive influences is solved. A method is proposed to solve this problem in the presence of non-numeric parameters that determine the information security of the object, and in the conditions of their interdependence. The method can be used in the development of computer decision support systems in the security systems of socio-economic objects.

Keywords: information security, fuzzy set, membership function.