FUZZY MAJORITY MODELLING OF INFORMATION SECURITY RISKS

Sadegh Derakshandeh[1], Yadigar Imamverdiyev[2]

Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]*smdk364@yahoo.com*, [2]*yadigar@lan.ab.az*

Management of information security is grounded on the analysis and evaluation of information security risks. At present, there exist a number of standards (ISO 27001, NIST, MITRE), approaches and many instrumental means based on them (COBRA, CRAMM, MethodWare, RiskWatch, Avangard, GRIF), for evaluation of risks of information security [1-4].

But their application in practice faces a number of difficulties. One of the significant considerations in compared analysis of risk evaluation methodology is the efficiency of results achieved on these methodologies [5-6]. Complicated methodologies requiring accurate primary estimations in entry and giving ambiguous results in exit would hardly assist to establish an efficient security system.

Methodologies of information security risks evaluation may be divided into methodologies based on quantity, quality and fuzzy logic. The fundamental problem in quantity approach to the analysis of risks is the estimation of realization possibility of specific threats in the system concerned. Complicated algorithms are used for estimation of the frequency and possibility of occurrence of threats.

Quallity approach to the evaluation of risks is much easier than that of quantity evaluation. The methodology of "risks matrix" is much widely spread among the methodologies of this class. This is the sufficiently ordinary risk analysis methodology. In the process of evaluation possibility of occurrence of each risk and the scale of losses relate to it are defined by the experts. The evaluation is carried out by the scale of three degrees: "high", "medium", "low". The system as a whole is evaluated on the ground of estimations for separate risks; the risks themselves are ranged (lined up). The methodology concerned allows carrying the evaluation fast and correctly. But the interpretation of the achieved results is not always possible. One of the principle shortages of analyzed instrumental means is that, the evaluation of the state of information security system within a real period of time is impossible, because expert evaluations may not be changed.

Risks evaluation based on fuzzy logic allows substituting the approximate schedule estimation for adequate modern mathematic methodology on the problem concerned [7-9]. The approach based on fuzzy logic allows the evaluation of risks for information system resources in a real period of time taking into consideration the possible majority of influences and the dynamic of changes of their parameters in the process of exploitation.

In this article, using fuzzy logic, there suggested a model for minimizing the remaining risk. The following signs are accepted in the suggested model:

$O = \{o_k\},\ k = \overline{1,K}$ – protected majority of assets;

$T = \{t_i\},\ i = \overline{1,I}$ – majority of threats directed to assets;

$M_i = \{m_{ij}\},\ j = \overline{1,i_J}$ – majority of existing protection mechanisms against *i* threat;

$C_i = \{c_{ij}\},\ j = \overline{1,i_J}$ – majority of values of protection mechanisms against *i* threat;

$R_0 = \{r_{i0}\},\ i = \overline{1,I}$ – majority of estimations of the risk incurred by threats;

$R_i = \{r_{ij}\},\ j = \overline{1,i_J}$ – majority of estimations of the remaining risk while choosing protection mechanism for *i* threat.

For calculation of $\mu(r_{ij}) = \mu(r_i)$ relation function of the remaining risk it is suggested to use the Rothstein methodology [10].

Let's suppose that, the experts have compared protection mechanisms for i threat and got the following pair comparison matrix:

$$A_i = \begin{pmatrix} 1 & a_{12} & \dots & a_{1J_i} \\ a_{21} & 1 & \dots & a_{2J_i} \\ \dots & \dots & \dots & \dots \\ a_{J_i1} & a_{J_i1} & \dots & 1 \end{pmatrix} \quad (1)$$

We should note that, for the elements of this matrix $a_{ij} = 1/a_{ji}$ is correct. Relation function may be calculated by the following formulas:

$$\mu(r_i) = \left(\sum_{j=1}^{J} a_{ij} \right)^{-1} \quad (2)$$

or

$$\mu(r_i) = \sqrt[i_j]{\prod_{j=1}^{J_i} a_{ij}} \quad (3)$$

Example: Let's suppose that, as a result of pair comparison of antivirus means by the experts the following pair comparison matrix is got:

$$A_1 = \begin{pmatrix} 1 & 3 & 5 \\ 1/3 & 1 & 7 \\ 1/5 & 1/7 & 1 \end{pmatrix}$$

According to the formula (3) the calculations result the following estimations.

$$\mu(r_{11}) = \sqrt[3]{1 \cdot 3 \cdot 7} = 2.76;$$

$$\mu(r_{12}) = \sqrt[3]{0.33 \cdot 1 \cdot 7} = 1.32;$$

$$\mu(r_{13}) = \sqrt[3]{0.2 \cdot 0.143 \cdot 1} = 0.31.$$

After normalization $\mu(r_{11}) = 0.63$; $\mu(r_{12}) = 0.30$; $\mu(r_{13}) = 0.07$ is got.

For example, C – is the general budget which may be spent on getting protection mechanisms. It's clear that, threats may be of different significance (criticism) from the point of view of information system; first of all it is necessary to prevent the most critical ones. Therefore, let's suppose that, the weight of i threat is v_i.

Enter the variable $x_{ij} \in \{0,1\}$, $i = \overline{1,I}$, $j = \overline{1,i_J}$. If j mechanism is chosen for i threat, then $x_{ij} = 1$, otherwise $x_{ij} = 0$. It's clear that, $\sum_{j=1}^{i_J} x_{ij} = 1$. In order to take into consideration the

case when no mechanism is chosen for i threat, we must "widen" x_{ij} variable accepting $x_{ij} = 1$ for $j = 0$".

We may express the problem of minimizing of accepted remaining risks as follows:

$$\sum_{i=1}^{I}\sum_{j=0}^{i_j} v_i \mu(r_{ij}) x_{ij} \to \min \tag{4}$$

$$\sum_{i=1}^{I}\sum_{j=1}^{i_j} c_{ij} x_{ij} \le C \tag{5}$$

$$\sum_{j=1}^{i_J} x_{i\,j} = 1 \tag{6}$$

Thus, the problem (4)-(6) of minimizing of the remaining risk is brought to the fuzzy linear programming problem. We may use different methods for its settlement.

Literature

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements. www.iso.org/iso/catalogue_detail?csnumber=42103
2. С.А. Петренко, С.В. Симонов Управление информационными рисками. Экономически оправданная безопасность – М.: ДМК Пресс, 2004. – 384 с.
3. C. J. Alberts, S. G. Behrens et al. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Framework. Pittsburg, Carnegie Mellon, 1999, pp.1-69.
4. B. Barber, J. Davey. The use of the CCTA risk analysis and management methodology CRAMM. Proc. MEDINFO92, North Holland, 1992, pp.1589 –1593.
5. K.Buyens, B.De Win, W.Joosen. Empirical and statistical analysis of risk analysis-driven techniques for threat management. The Second International Conference on Availability, Reliability and Security – ARES 2007. 10-13 April 2007, pp.1034-1041.
6. A. Vorster, L. Labuschagne. A Framework for Comparing Different Information Security Risk Analysis Methodologies. ACM International Conference Proceeding Series; Vol. 150, 2005, pp.95-103.
7. R.M. Alguliyev, Y.N.İmamverdiyev. About One Method of Risk Measurement of Maintenance of Information Security of Corporative Networks Because of Fuzzy Sets. Proceedings of the 4th Int. Conf. on New Information Technologies'2000. December 5-7, Minsk, Belarus, Vol.1, 2000, pp.76-81
8. M. Hentea. Enhancing information security risk management with a fuzzy model. Proceedings of 19th International Conference on Computer Applications in Industry and Engineering, Las Vegas, Nevada, 2006, pp.132-139.
9. S.Derakshandeh, Y.N.İmamverdiyev. Mürəkkəb sistemlərdə informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi. Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları Respublika elmi konfransının materialları, 26-27 November 2007, Sumgait pp.254-256.
10. А.П. Ротштейн. Интеллектуальные технологии идентификации. Винница: Универсум-Винница, 1990, 320 с.