INFORMATION SECURITY RISK ASSESSMENT MODEL BASED ON COMPUTING WITH WORDS

Oleg Tymchuk[1], Maryna Iepik[2], Artyom Sivyakov[3]

[1,2]Vasyl' Stus Donetsk National University
Department of Computer Technologies
21, 600-richya str., Vinnytsia
Ukraine
[1]o.s.timchuk@gmail.com, [2]marinayepik@gmail.com

[3]DTEK Energy
Information Security Department
57, Leo Tolstoy str., Kiev
Ukraine
[3]arteom.sivyakov@gmail.com

Abstract: *The basis for company IT infrastructure security is information security risks assessment of IT services. The increased complexity, connectivity and rapid changes occurring in IT services make it impossible to apply traditional models of quantitative/qualitative risk assessment. Existing quantitative assessment models are time-consuming, at the same time, qualitative assessment models do not take into account the subjective expert assessments and the uncertainty of risk factors. This paper presents the new information security risk assessment model for IT services based on computing with words. The model methodology is based on OWASP risk rating methodology for web applications. To evaluate risk factors, it is proposed to use dictionary consisting of 16/32 granular terms (words). Problems of uncertainty in perceptual assessments of risk factors are taken into account using methods of the theory of discrete interval type-2 fuzzy sets and systems.*

Keywords: *risk, risk assessment, risk factor, information security, IT service, discrete interval type-2 fuzzy set, computing with words.*

1 Introduction

Implementation of new IT services into company IT infrastructure increases the number of vulnerabilities, the exploit of which is a key object of cyber criminals' interest. The level of company IT infrastructure security depends on correct information security (IS) risks assessment of IT services and, as consequence, on effectiveness of the selected countermeasures [1]. As a rule, in the IS risk assessment are used models based on qualitative assessment of risk factors. Quantitative estimates are time-consuming and require additional knowledge, which are not always available to developers [2].

The main IS risk assessment models associated with IT services are: Open Web Application Security Project (OWASP) Risk Rating Methodology [3], Common Vulnerability Scoring System (CVSS) [4], OCTAVE A [5], ISO27005 [6]. Researchers in the field of IS have proposed many IS risk assessment models based on the methods of computational intelligence [7, 8]. The analysis of main models, published research results and standard based on IS risk assessment methods [9] shows that risk factors of IT services are uncertain. The main reasons of uncertainty are the following:

- there is ambiguous interpretation of risk factors among experts;
- risk factors are represented by a verbal description which is intuitive;
- time series of risk factors have a nonlinear structure.

In addition, practical methods for identifying risk factors (for example, brainstorming or an individual expert survey) have several disadvantages:

- hesitation of experts during information exchange in the presence of the heads of the company departments;
- the domination of experienced experts during discussions in groups;
- the difficulty of comparing different experts' opinions;
- the difficulty of collecting and analysing expert assessments.

Traditional methods of computational intelligence, as well as methods of the theory of type-1 fuzzy sets and systems do not let us to fully take into account the uncertainty of risk factors and resolve the shortcomings of methods of their determination. Therefore, we propose to use the methods of theory of discrete interval type-2 fuzzy sets (DIT2FSs) and systems (DIT2FLSs) [10] and the methods of theory of perceptual computing [11] to interpretation of existing IS risks assessment models of IT services.

2 Information Security Risk Assessment Model

The company does annual IS risk assessment according to IS risk assessment plan for information resources of critical business processes or when IT services have been changed. IS risk assessment consists of 3 main stages: risk identification, analysis and evaluation [9].

According to the theory of DIT2FSs and DIT2FLSs lets present a IS risk assessment model of IT service

$$\begin{aligned} &\sum_{i=1}^{I} r_i x_i \to \max, \\ &\sum_{i=1}^{I} a_i x_i \le S, \\ &a_i > 0, c_i \ge 0, \\ &x_i \in \{0,1\}, \end{aligned} \tag{1}$$

where r_i – value of i-th risk,
x_i – binary variable x_i=1 states that it was decided to reduce the i-th risk,
I – the number of identified risks,
a_i – cost of the i-th risk reducing,
S – budget allocated by the company to reduce the identified risks.

Define the value of the i-th risk as

$$\begin{aligned} &r_i = F(LI, LO, R, IN_i), \\ &LI = \langle li_n \rangle, n = \overline{1,N}, \\ &R = \langle r_m \rangle, m = \overline{1,M}, \\ &IN_i = \langle in_n^i \rangle, \end{aligned} \tag{2}$$

where F – Mamdani fuzzy inference system,
LI – set of input linguistic variables describing the risk factors of IT service,
N – the number of input linguistic variables,
LO – output linguistic variable describing the levels of IT service risk,
R – set of fuzzy rules,
M – the number of fuzzy rules,
IN_i – set of fuzzy input values.

Set of input linguistic variables contains 4 linguistic variables

$$LI = \langle li_1, li_2, li_3, li_4 \rangle, \tag{3}$$

where li_1 – linguistic variable defines the vulnerability levels; contains 3 terms: “none to very little”, “a moderate amount”, “a maximum amount”; it is defined on primary variable X_1=[0;10] (see Fig. 1a),
li_2 – linguistic variable defines the levels of threat agent; contains 5 terms: “none to very little”, “some”, “a moderate amount”, “a large amount”, “a maximum amount”; it is defined on primary variable X_2=[0;10] (see Fig. 1b),
li_3 – linguistic variable defines the levels of possible technical impact as a result of vulnerability exploitation; contains 3 terms: “negligible”, “moderate”, “critical”; it is defined on primary variable X_3=[0;10] (see Fig. 1c),
li_4 – linguistic variable defines the levels of possible business impact as a result of vulnerability exploitation; contains 5 terms: “negligible”, “minor”, “moderate”, “critical”, “catastrophic”; it is defined on primary variable X_4=[0;10] (see Fig. 1d).

Output linguistic variable LO defines the levels of IT service risk. LO is defined on primary variable X_{res}=[0;5] and contains 4 terms: “low”, “medium”, “high”, “extreme” (see Fig. 2).

Fuzzy rule base R contains 225 standard IF-THEN rules.

Let’s consider the example of fuzzy rule from the set R

$$\begin{aligned} r^m : IF\ in_1\ \ is\ \ \text{"a moderate amount"}\ \ and\ \ in_2\ \ is\ \ \text{"a large amount"}\ \ and \\ in_3\ \ is\ \ \text{"critical"}\ \ and\ \ in_4\ \ is\ \ \text{"catastrophic"} \\ THEN\ \ y\ \ is\ \text{"high"}. \end{aligned} \tag{4}$$

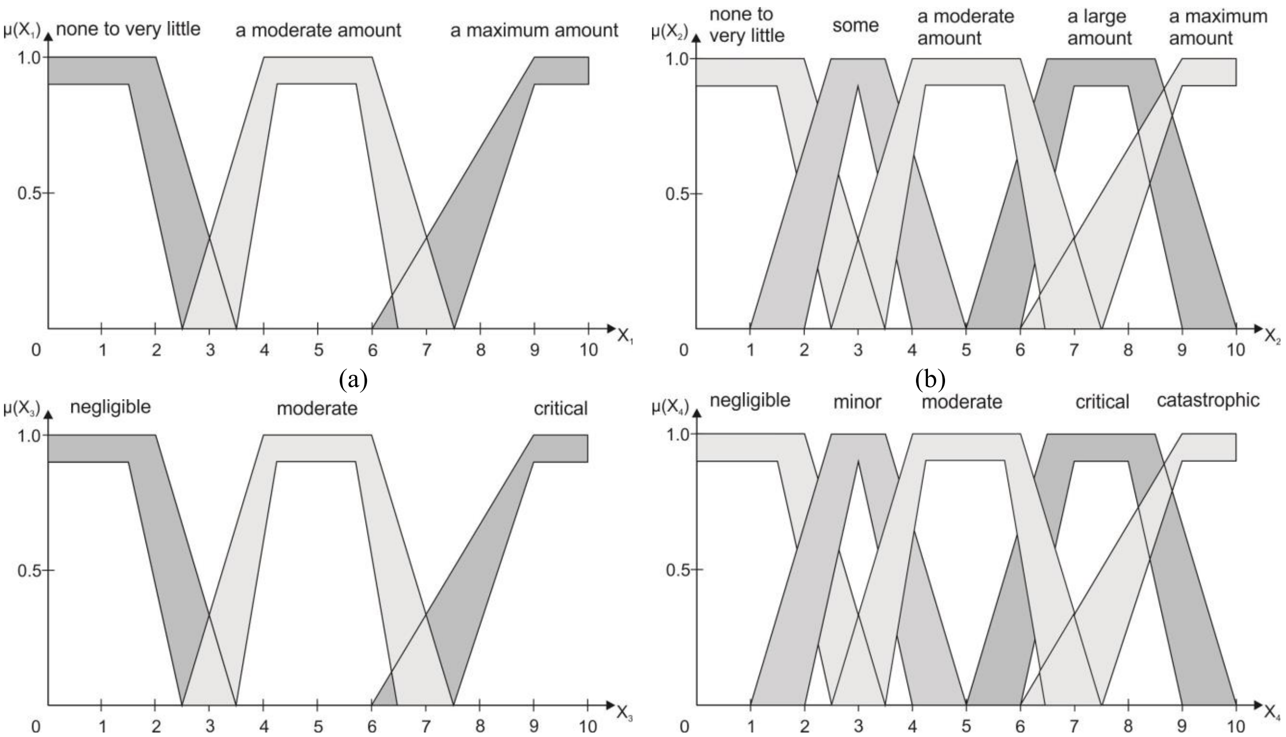
Vector IN_i activates the terms of input linguistic variables LI. IN_i contains 4 expert evaluations

$$IN_i = \langle in_1^i, in_2^i, in_3^i, in_4^i \rangle, \tag{5}$$

where in_1^i – DIT2FS describing expert evaluations of factors of the i-th vulnerability,
in_2^i – DIT2FS describing expert evaluations of threat agent factors for the i-th vulnerability,

in_3^i – DIT2FS describing expert evaluations of factors of possible technical impact as a result of the i-th vulnerability exploitation,

in_4^i – DIT2FS describing expert evaluations of factors of possible business impact as a result of the i-th vulnerability exploitation.



(a) (b)

(c) (d)

Figure 1: Input linguistic variables LI
(a) – linguistic variable li_1; (b) – linguistic variable li_2;
(c) – linguistic variable li_3; (d) – linguistic variable li_4;

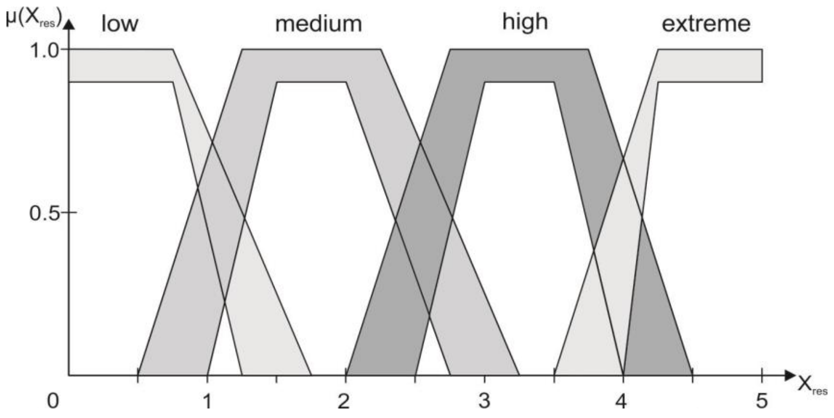


Figure 2: Output linguistic variable LO

The method of perceptual computing proposed by Wu and Mendel [11] is used to obtain expert evaluations

$$\begin{aligned} & in_n^i = F\left(V, W^i\right), in_n^i \in IN, \\ & V = \left\langle v_j \right\rangle, \ j = \overline{1, J}, \\ & v_j = \left\langle T_j, \widetilde{Y}_j \right\rangle, \\ & W^i = \left\langle w_k^i \right\rangle, w_k^i \in V, \ k = \overline{1, K}, \end{aligned} \tag{6}$$

where F – function realizes computing with words,
V – dictionary,

W^i – set of expert verbal evaluations,
v_j – granular term described by a word and a DIT2FS,
J – the total number of granular terms in the dictionary, J=16 or J=32,
T_j – word,
$\widetilde{Y}_j$ – DIT2FS describing word,
w_k^i – expert evaluation,
K – the number of experts taking part in the survey.

Risks prioritization allows to manage the most significant of them, allocating necessary resources for this purpose. Determination of the necessary protection for identified risks is carried out by the person responsible for the IS risk management in cooperation with the owners of relevant business processes. While identifying countermeasures, organizational and technical means / actions, allowing to eliminate (or significantly decrease) the potential damage are taken into consideration. To choose countermeasures and substantiate the necessity of allocating resources for their implementation, an assessment of the costs optimization for their realization is performed. The cost of the means used to guarantee IS should not exceed possible damage occurring upon threat identification.

3 Results

The test of the proposed model was performed during the analysis of IT service “Print server”, which is included in company IT infrastructure. Five expert groups (group of business owners – 4 experts, group of technical owners – 3 experts, team of developers – 4 experts, group of administrators – 3 experts and group of end users – 5 experts) participated in IS risk assessment of IT service “Print server”. During the risk identification stage, five IS risks were registered (see Table 1).

Table 1: Identified IS risks of IT service “Print server”

No	Risk	Properties
1	Confidential Information Leaks	Confidentiality
2	Destruction of critical information	Integrity
3	Substitution / misrepresentation of critical information	Integrity
4	Loss of critical data availability	Availability
5	Denial of IT service	Availability

Each expert from 5 groups evaluated factors (vulnerability, threats, technical impact and business impact) of the identified risks. Risk factors were evaluated in two modes:

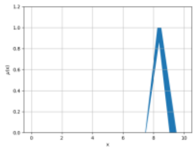
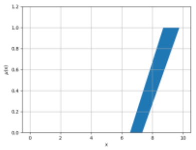
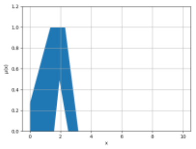
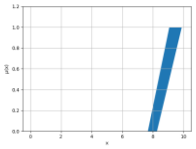
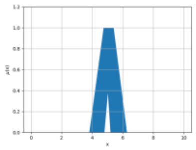
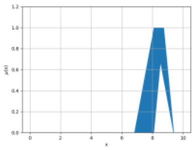
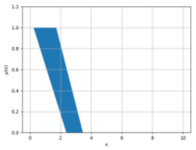
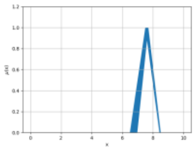
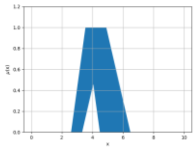
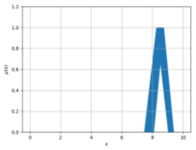
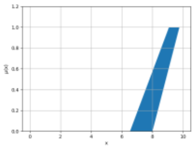
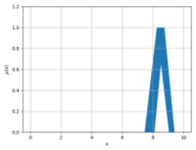
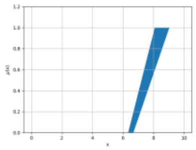
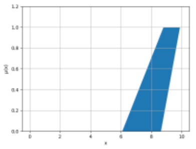
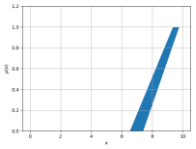
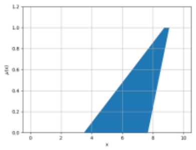
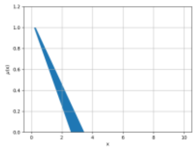
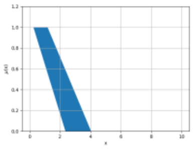
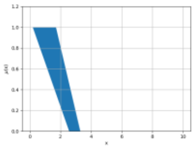
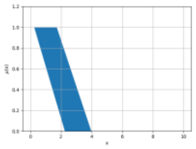
- mode 1 – traditional tabular method – each risk factor is evaluated regarding a five-point scale and the result is defined as arithmetic average of expert evaluations;
- mode 2 – method of perceptual computing – for risk factor evaluation experts used 32 granular terms / words (none to very little, teeny-weeny, a smidgen, tiny, very small, very little, a bit, little, low amount, small, somewhat small, some, some to moderate, moderate amount, fair amount, medium, modest amount, good amount, sizeable, quite a bit, considerable amount, substantial amount, a lot, high amount, very sizeable, large, very large, humongous amount, huge amount, very high amount, extreme amount, maximum amount) and the result is represented as DIT2FS.

An example of experts’ evaluations of “Denial of IT service” risk factors is presented in Tab. 2 (mode 1) and Tab. 3 (mode 2). DIT2FLS Toolbox and Package Library [12] and developed Python-module for computing with words were used to obtain the risk values in mode 2.

Table 2: Expert evaluations of “Denial of IT service” risk factors (mode 1)

Expert groups	Expert groups evaluations			
	Threat agent factors	Vulnerability factors	Technical Impact	Business Impact
Group of business owners (4)	AVG=4.00	AVG=4.25	AVG=1.50	AVG=4.75
Group of technical owners (3)	AVG=3.33	AVG=4.67	AVG=2.00	AVG=4.33
Team of developers (4)	AVG=2.25	AVG=4.00	AVG=4.50	AVG=3.50
Group of administrators (3)	AVG=3.00	AVG=5.00	AVG=5.00	AVG=4.67
Group of end users (5)	AVG=1.75	AVG=2.00	AVG=1.25	AVG=2.00

Table 3: Expert evaluations of “Denial of IT service” risk factors (mode 2)

Expert groups	**Expert groups evaluations**			
	Threat agent factors	**Vulnerability factors**	**Technical Impact**	**Business Impact**
Group of business owners (4)	Evaluations: a lot, high amount, considerable amount, maximum amount. Result: 	Evaluations: very high amount, extreme amount, a lot, sizeable. Result: 	Evaluations: small, tiny, a bit, small. Result: 	Evaluations: maximum amount, extreme amount, large, substantial amount. Result: 
Group of technical owners (3)	Evaluations: some to moderate, fair amount, medium. Result: 	Evaluations: very sizeable, very large, considerable amount. Result: 	Evaluations: very little, a bit, low amount. Result: 	Evaluations: good amount, quite a bit, considerable amount. Result: 
Team of developers (4)	Evaluations: some, some, moderate amount, fair amount. Result: 	Evaluations: very large, a lot, very sizeable, substantial amount. Result: 	Evaluations: high amount, huge amount, very high amount, very sizeable. Result: 	Evaluations: very sizeable, a lot, large, medium. Result: 
Group of administrators (3)	Evaluations: good amount, quite a bit, sizeable, very sizeable. Result: 	Evaluations: extreme amount, maximum amount, very high amount, maximum amount. Result: 	Evaluations: very large, humongous amount, huge amount, very high amount. Result: 	Evaluations: medium, maximum amount, very large, large. Result: 
a group of end users (5)	Evaluations: a smidgen, tiny, very small, none to very little, tiny. Result: 	Evaluations: very little, a bit, a bit, very small, little. Result: 	Evaluations: small, little, teeny-weeny, none to very little, small. Result: 	Evaluations: some to moderate, a bit, low amount, very little, a bit. Result: 

The result of risks evaluations of IT service “Print server” is presented in Tab. 4.

Table 4: Risks evaluations of IT service “Print server”

Risk	**Risk value**	
	mode 1	**mode 2**
Confidential Information Leaks	4.41	High (4.1)
Destruction of critical information	4.82	High (4.2)
Substitution / misrepresentation of critical information	3.9	Medium (2.4)
Loss of critical data availability	2.87	Low (0.9)
Denial of IT service	3.39	Medium (2.1)

The Table 4 shows that risk values from mode 1 and mode 2 differ significantly. Experts who participated in the experiment favoured the results from mode 2. The benefits of developed model can be summarized as follows:

1. Perceptual data pre-processing stage [11] allows to exclude from consideration insignificant user estimates.
2. Perceptual assessment of risk factors is natural for experts.
3. The use of DIT2FSs and DIT2FLSs allows to take into account the uncertainty of risk factors.

4 Conclusion

We propose the information security risk assessment model for IT services. Risk assessment methodology is based on OWASP Risk Rating Methodology, which allows to analyse the main risk factors: vulnerability factors, threat agent factors, technical and business impact factors. Evaluation of risk factors is performed by using the method of perceptual computing proposed by Wu and Mendel. Uncertainty of risk factors and perceptual evaluations is taken into account by using methods of the theory of discrete interval type-2 fuzzy sets and systems.

Experiments have shown that the risk values obtained with the help of the developed model are objective and take the views of all process participants. Moreover, the perceptual data pre-processing stage allows to determine bad data of correspondingly unconscientious/incompetent participants of risk assessment process.

The design and implementation of cross-platform risk calculator “Fuzzy Risk Calculator” based on developed model was made. “Fuzzy Risk Calculator” is presented as a set of extensible dynamic modules which can be integrated into the company information security system.

References

[1] Wangen, G.: An initial insight into Information Security Risk Assessment practices. In: 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), vol. 8, pp. 999–1008. IEEE, Gdansk, Poland (2016).

[2] Lee, M.-C.: Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology (IJCSIT), 6 (1), 29-45 (2014).

[3] OWASP Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (2017). [Online; accessed 05-May-2017]

[4] Common Vulnerability Scoring System. https://www.first.org/cvss (2017). [Online; accessed 05-May-2017]

[5] Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R.: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Tech. report CMU. Software Engineering Institute (2007).

[6] ISO/IEC 27005:2011: Information Technology, Security Techniques, Information Security Risk Management. 2nd edn. (2011).

[7] Song, Y., Shen, Y., Zhang, G. and Hu, Y.: The information security risk assessment model based on GA - BP. In: 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 119 - 122. IEEE, Beijing, China (2016).

[8] Wang, J., Fan, K., Mo, W., Xu, D.: A Method for Information Security Risk Assessment Based on the Dynamic Bayesian Network. In: 2016 International Conference on Networking and Network Applications, pp. 279-283. IEEE, Hakodate, Japan (2016)

[9] IEC 31010:2009: Risk management, Risk assessment techniques. 1st edn. (2009).

[10] Mendel, J.M, John, R.I.B.: Type-2 Fuzzy Sets Made Simple. IEEE Transactions on Fuzzy Systems, 10 (2), 117-127 (2002).

[11] Mendel, J.M., Wu, D.: Perceptual Computing: Aiding People in Making Subjective Judgments. 1st edn. Wiley-IEEE (2010).

[12] Petrenko, T., Tymchuk, O.: Package library and toolbox for discrete interval type-2 fuzzy logic systems. Proceedings of the 18th International Conference on Soft Computing (MENDEL), pp. 233-238. Brno, Czech Republic (2012).