Comprehensive Approach to Information Security Risk Management

Tatyana I. Buldakova, Dmitrii A. Mikov
Information Security Department
Bauman Moscow State Technical University
Moscow, Russian Federation
buldakova@bmstu.ru; mikovda@yandex.ru

***Abstract*—Information security risk management as important process of data protection in automated systems has been presented. Such criteria as estimates consistency and adequacy, adaptability to qualitative data, assessment subjectivity and uncertainty, risk sensitivity, which influence risk management effectiveness, have been identified. A task of integrated methodology development has been formalized in accordance with presented criteria. A structural model of comprehensive methodology, which displays its components and relationships between them, has been designed as a flowchart. A method for drawing up the risk factors list, including information security threats, potentially possible damage, automated system vulnerabilities, based on IDEF0 modeling, has been proposed. An original expert survey method, which provides compliance with the requirements of consistency and adequacy maximization for risk factors assessment, has been suggested. A neuro-fuzzy network based on Takagi-Sugeno-Kang model for information security risk calculation from risk factors assessment has been developed in MATLAB. A countermeasures choice method based on game theory criteria has been illustrated.**

Keywords—information security risk management; estimates consistency; estimates adequacy; adaptability to qualitative data; risk assessment subjectivity; risk assessment uncertainty; risk sensitivity; model IDEF0; expert survey; neuro-fuzzy network; game theory criteria

I. INTRODUCTION

Reliability of functioning of automated systems mostly depends on ensuring their information security. Therefore, based on the specifics of automated systems, companies develop and implement a corresponding set of activities to manage information security. An important component of this process is information security risk management (e.g. [1-3]).

Information security risk management consists of:

- drawing up the risk factors list (information security threats, potentially possible damage, automated system vulnerabilities);
- expert survey for risk factors assessment;
- risk level calculation, based on risk factors estimates;
- choice of the countermeasures for reducing the risk to acceptable level.

Each stage of information security risk management must be realized by different methods and tools, which are the most effective for this particular stage. So, the main research direction in the field of information security risk management should be focused on the selection of such methods, which maximally satisfy the needs of different stages of the process [4].

Investigation of qualitative, quantitative and semi-qualitative information security risk management methods, such as hazard and operability study (HAZOP) [5], layer of protection analysis (LOPA), preliminary hazard analysis (PHA), allows to find main disadvantages and formulate a set of effectiveness criteria for a comprehensive approach:

- $a(y_k) = [0; 1]$ – consistency of risk factors estimates by method y_k;
- $b(y_k) = [0; 1]$ – adequacy of risk factors estimates by method y_k;
- $c(y_k) = [0; 1]$ – adaptability of method y_k to qualitative data;
- $d(y_k) = [0; 1]$ – subjectivity of risk assessment by method y_k;
- $e(y_k) = [0; 1]$ – uncertainty of risk assessment by method y_k (lack of accurate knowledge about the status of all risk factors in the system and fuzzy risk classification in the conditions of the particular system functioning);
- f – risk sensitivity (uneven influence of various risk factors on the level of risk in certain conditions);

The set of requirements to effectiveness criteria for a comprehensive information security risk management methodology is as in (1) and (2)

$$a(y_k) \times b(y_k) \times c(y_k) \rightarrow \max \quad (1)$$

$$d(y_k) \times e(y_k) \rightarrow \min \quad (2)$$

Practical investigation allows to develop a comprehensive information security risk management methodology based on presented set of effectiveness criteria (Fig. 1).

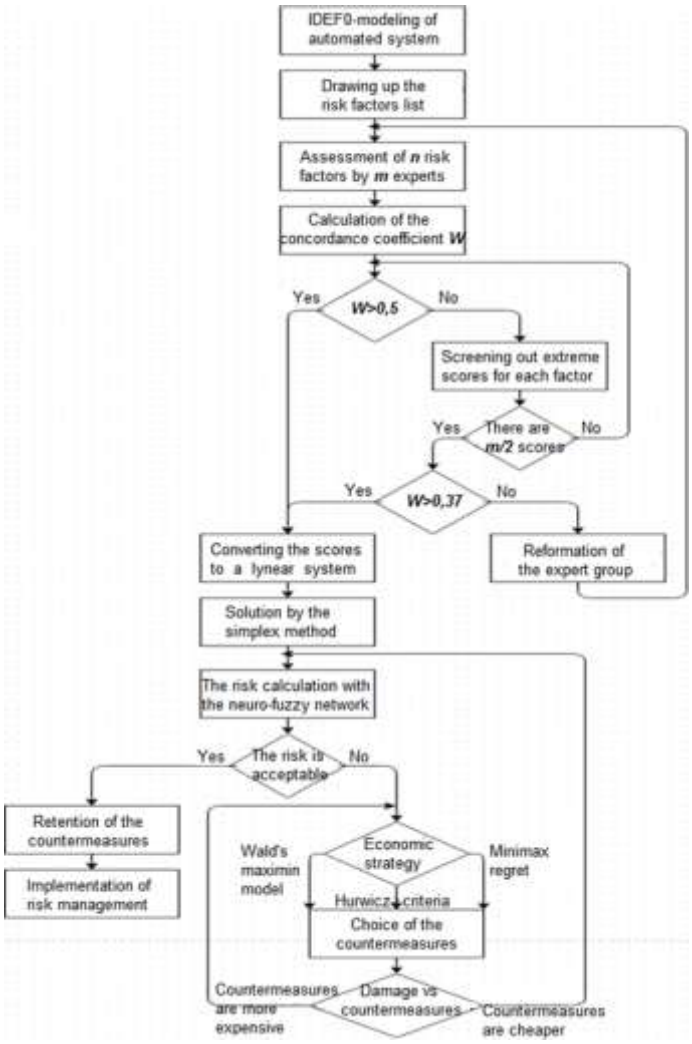

Fig. 1. Comprehensive methodology for information security risk management

II. DRAWING UP THE RISK FACTORS LIST USING IDEF0

The initial stage of information security risk management is the identification of risk factors (threats, possible damage, vulnerabilities) [4, 6, 7]. The solution of this problem is connected with the automated system modeling and the investigation of the circulating information flows [8, 9]. Comparative analysis of the ARIS, IDEF0, IDEF3, UML methodologies showed that IDEF0 takes into account and displays all necessary elements:

- input documents and data;
- output documents and data;
- persons, who implements processes;
- used tools;
- control actions over the processes implementation;
- feedbacks.

Based on the characteristics of information security risk management, it is necessary to have risk factors in the IDEF0-model according to a set of principles (Fig. 2).

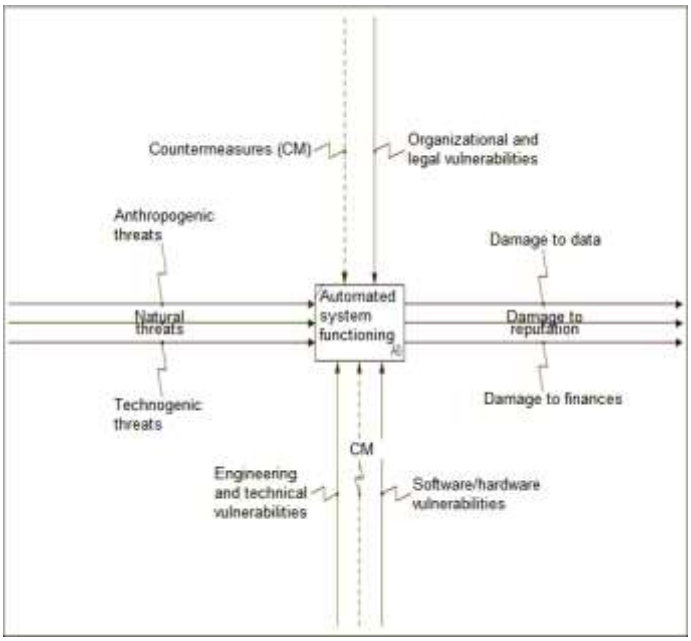

Fig. 2. The principle of risk factors location in the IDEF0 model

When countermeasures are choosing and adding to the IDEF0 model, it is necessary understand that their list is preliminary, as the identified risk factors have not been evaluated yet by the expert group. Therefore, it is impossible to make an unambiguous conclusion about the degree of their impact on found threats and vulnerabilities. After risk factors assessment and subsequently calculating the level of risk, when all quantities acquire numerical values, the list of countermeasures can be adjusted [10]. Therefore, corresponding changes in the IDEF0-model are inevitable after the implementation of further stages of management [11].

III. EXPERT SURVEY FOR RISK FACTORS ASSESSMENT

To ensure the consistency and adequacy of expert opinions in assessment of risk factors from the list compiled with the IDEF0 model, a special method of expert interview has been developed. Assessment of threats, potentially possible damage and vulnerabilities must be performed by the expert group in accordance with (3), (4) and (5):

$$x_{ij1} = k_{ij1} \times p_{ij1} \times f_{ij1} \quad (3)$$

$$x_{ij2} = k_{ij2} \times p_{ij2} \times f_{ij2} \quad (4)$$

$$x_{ij3} = k_{ij3} \times p_{ij3} \times f_{ij3} \quad (5)$$

where:

x_{ij1} – threat estimate;

$k_{ij1} \in [0; 10]$ – threat power;

$p_{ij1} \in [0; 1]$ – probability of threat realization;

$f_{ij1} \in [0; 1]$ – risk sensitivity to threat assessment;

x_{ij2} – potentially possible damage estimate;

$k_{ij2} \in [0; 10]$ – asset value;

$p_{ij2} \in [0; 1]$ – probability of the highest damage;

$f_{ij2} \in [0; 1]$ – risk sensitivity to damage assessment;

x_{ij3} – vulnerability estimate;

$k_{ij3} \in [0; 10]$ – vulnerability degree;

$p_{ij3} \in [0; 1]$ – probability of vulnerability exploit;

$f_{ij3} \in [0; 1]$ – risk sensitivity to vulnerability assessment;

$i = \{1, 2, ..., m\}$ – experts;

$j = \{1, 2, ..., n\}$ – risk factors from the list.

The consistency ($a(y_k)$) of estimates is provided by calculating the concordance coefficient W using (6), (7), (8), (9):

$$x_j = \sum x_{ij} \tag{6}$$

$$x = 1/n \times \sum x_{ij} \tag{7}$$

$$S = \sum (x_j - x)^2 \tag{8}$$

$$W = 12S/(m^2(n^3 - n)) \tag{9}$$

Then it is necessary to screen out extreme scores using an algorithm based on the verbal-numeric Margolin and Harrington scales (Fig. 1). The adequacy ($b(y_k)$) of overall threat (x_1), potentially possible damage (x_2) and vulnerability (x_3) estimates is provided by maximization of the objective function (10):

$$F(x) = x_1 + x_2 + x_3 \rightarrow \max \tag{10}$$

It is necessary to construct a linear constraint system of inequalities (11) containing the number of remaining estimates of threats (a_{i1}), potentially possible damage (a_{i2}) and vulnerabilities (a_{i3}) for each expert, and the sum of each expert estimates (b_i):

$$a_{i1} \times x_1 + a_{i2} \times x_2 + a_{i3} \times x_3 \leq b_i \tag{11}$$

The linear constraint system of inequalities reduces to the optimization problem of linear programming and can be solved using the simplex method [12].

IV. NEURO-FUZZY NETWORK FOR RISK LEVEL ASSESSMENT

It is necessary to use a method that is adaptive to qualitative data ($c(y_k)$), minimizes subjectivity ($d(y_k)$) and uncertainty ($e(y_k)$) of estimates and takes into account risk sensitivity to various factors (f).

A comparative analysis of the approaches, based on machine learning [13-15], soft calculations [16-18] and hybrid models [19, 20], showed the following results (Table I).

TABLE I. COMPARATIVE ANALYSIS OF RISK ASSESSMENT APPROACHES

Methods	**Effectiveness criteria values**			
	$c(y_k)$ (max)	$d(y_k)$ (min)	$e(y_k)$ (min)	f (max)
Bayesian networks	0,7	0,4	0,3	0,75
Genetic algorithms	0,3	0,5	0,85	0,35
Artificial neural networks	0,5	0,3	0,2	0,8
Cognitive maps	0,4	0,5	0,25	0,45
Support vector machine	0,2	0,3	0,65	0,45
Analytic hierarchy process	0,8	0,5	0,2	0,55
Fuzzy systems	0,7	0,5	0,2	0,8
Rough sets	0,35	0,5	0,55	0,3
Grey sets	0,35	0,5	0,55	0,3
Fuzzy measure theory	0,4	0,5	0,55	0,6
Neuro-fuzzy networks	***0,7***	***0,3***	***0,2***	***0,8***
Neural networks based on genetic algorithms	0,5	0,3	0,2	0,8
Fuzzy Bayesian networks	0,7	0,4	0,2	0,8
Fuzzy hierarchy models	0,8	0,5	0,2	0,8

The results of the comparative analysis show that neuro-fuzzy networks have the best effectiveness criteria values.

Therefore, a neuro-fuzzy network is chosen as a risk assessment tool, which calculates risk level using three input risk factors values received in the previous stage.

The realized neuro-fuzzy network is transformed from Takagi-Sugeno-Kang fuzzy model and contains five layers: fuzzification, aggregation, activation, accumulation, defuzzification (Fig. 3).

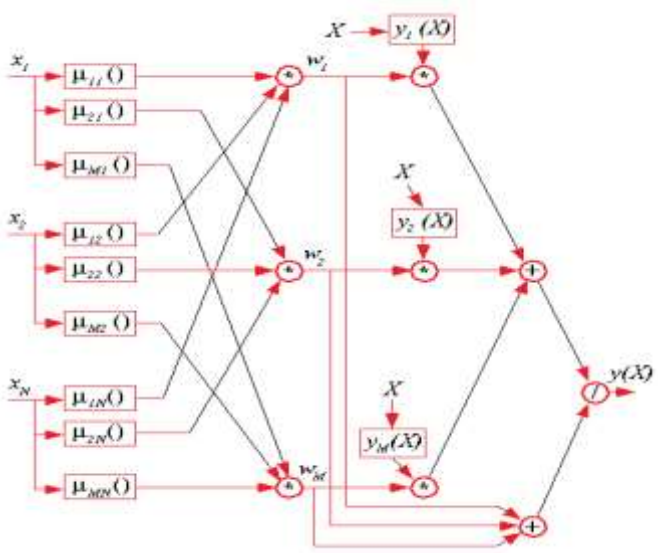

Fig. 3. Neuro-fuzzy network structure

Characteristics of the neuro-fuzzy network:

- structure – five-layered neuro-fuzzy network:
- fuzzy model type – Takagi-Sugeno-Kang;
- three input variables – threat, damage, vulnerability;
- five fuzzy sets for input variables – very low, low, medium, high, very high;
- trapezoidal membership function for input variables (Fig. 4);
- one output variable – information security risk level;
- nine values for output variable – negligibly low (0), very low (0,125), low (0,25), below average (0,375); average (0,5), above average (0,625), high (0,75), very high (0,875), critical (1);
- conjunction – algebraic product method;
- disjunction – algebraic sum method;
- defuzzification – weighted average method.

A verbal-numerical risk assessment scale, based on nine initially specified values of the output variable, has been developed. The scale allows to interpret the risk level obtained at the output in the form of a numerical index (Table II).

If the neuro-fuzzy network shows that the risk level is unacceptable, it is necessary to select the appropriate countermeasures to reduce it.

TABLE II. RISK ASSESSMENT SCALE

Risk level	Description
Negligibly low (0)	Risk can be neglected
Very low (0,125)	If the information is regarded as a very low risk, it is necessary to determine whether there is a need for corrective actions, or there is a possibility to take this risk
Low (0,25)	The risk level allows to work, but there are prerequisites for a malfunction
Below average (0,375)	It is necessary to develop and apply a corrective action plan within an acceptable period of time
Average (0,5)	The risk level does not allow to work stably, there is an urgent need for corrective actions that change the mode of work towards reducing the risk
Above average (0,625)	The system can continue to work, but the corrective action plan must be applied as quickly as possible
High (0,75)	The risk level is such that business processes are in an unstable state
Very high (0,875)	It is necessary to take measures to reduce the risk immediately
Critical (1)	The risk level is very high and unacceptable for the organization, which requires discontinuing the system operation and taking radical measures to reduce the risk

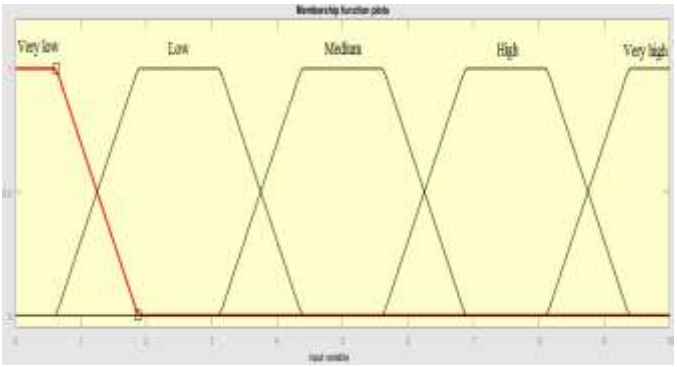

Fig. 4. Input membership function in MATLAB

V. CHOICE OF THE COUNTERMEASURES

The developed method of the countermeasures choice is based on the above expert survey method, but uses the game theory criteria for searching the optimal economic strategy. There are three possible criteria – Wald's maximin model, Hurwicz criteria and Minimax regret [21].

Wald's maximin model is aimed at minimizing the loss or guaranteed minimal result. The minimal impact of each countermeasure on any risk factor is determined, after that the countermeasure with the maximal smallest influence is chosen. It is the lower price of the game.

Hurwicz criteria is based on the choice of the pessimism indicator in the range from 0 to 1. If the pessimism indicator is maximal (equal to 1), Hurwicz criteria corresponds to Wald's maximin model, realizing a pessimistic strategy. The minimal pessimism indicator (equal to 0) should not be chosen, because the optimistic strategy is focused on maximizing the project's result, so the risk associated with unfavorable development of the external environment is not taken into account. Hurwicz criteria is the most flexible of all methods of the game theory, because it allows to compare several optimistic and pessimistic scenarios. The disadvantage is the subjectivity of the pessimism indicator choice by the researcher or the person making the decision.

Minimax regret is based on a matrix of regrets, made up of a matrix of strategies. Regrets are a lost result with a suboptimal strategy for each current state of the automated system. At first the maximal impact on each risk factor among all countermeasures is determined. Further, lost results of all countermeasures are calculated, then the regression matrix is compiled, where the maximal ineffective result of each countermeasure is determined. The countermeasure with the smallest maximal lost result is selected.

Each expert should complete two copies of the matrix of strategies (Table III) – for active countermeasures impact (c_{ija}) that reduces threats and damage, and for passive countermeasures impact (c_{ijp}) that reduces vulnerabilities and damage.

TABLE III. THE MATRIX OF STRATEGIES

Cost of countermeasures	b_1	b_2	...	b_n
$a_1 = v_1$	c_{11}	c_{12}	...	c_{1n}
$a_2 = v_2$	c_{21}	c_{22}	...	c_{2n}
...	...	...	...	...
$a_m = v_m$	c_{m1}	c_{m2}	...	c_{mn}

There are:

a_i – countermeasures;

b_j – risk factors;

c_{ij} – impact of countermeasure on risk factor;

v_i – cost of countermeasure;

After choosing a countermeasure in accordance with any of three criteria, depending on the economic strategy, the corresponding line is removed from the strategy matrix, after that it is necessary to conduct a new cycle. Countermeasures among the remaining are selected until their total value does not exceed the amount of potential damage (12):

$$\sum v \le v_d \tag{12}$$

where: $\sum v$ – total cost of selected countermeasures;

v_d – cost of potentially possible damage (budget for the countermeasures implementation).

Each expert needs to subtract his estimates of the countermeasures impact (c_{ija}, c_{ijp}) on risk factors from his earlier estimates (x_{ij1}, x_{ij2}, x_{ij3}) as (13), (14) and (15):

$$x^*_{ij1} = x_{ij1} - c_{ija} \tag{13}$$

$$x^*_{ij2} = x_{ij2} - c_{ija} - c_{ijp} \tag{14}$$

$$x^*_{ij3} = x_{ij3} - c_{ijp} \tag{15}$$

Finally, the neuro-fuzzy network calculates the residual risk level after the countermeasures implementation.

VI. CONCLUSION

The developed comprehensive information security risk management methodology meets the required effectiveness criteria, has a complex and branched structure and represents a set of methods and models used to implement various stages of management. The methodology is based on the joint use and interaction of IDEF0 model, expert survey, neuro-fuzzy network, methods of game theory and allows the most effective implementation of drawing up risk factors list, risk factors assessment, risk level calculation and countermeasures choice.

REFERENCES

[1] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. Mathematical models and applicable technologies to forecast, analyze, and optimize quality and risks for complex systems. In Proceedings of the First International Conference on Transportation Information and Safety (ICTIS), ASCE, 2011, pp. 845 – 854. DOI: 10.1061/9780784411773.

[2] Brooks D.J. Mapping the consensual knowledge of security risk management experts. In Proceedings of the 7th Australian Information Warfare and Security Conference (Edith Cowan University, Perth, Western Australia, 4-5 December 2006), 2006, 10 p. DOI: 10.4225/75/57a823cbaa0d8.

[3] Ruighaver T., Warren M., Ahmad A. Ascent of Asymmetric Risk in Information Security: An Initial Evaluation. In Proceedings of the 10th Australian Information Warfare and Security Conference (Edith Cowan University, Perth, Western Australia, 1-3 December 2009), 2009, 8 p. DOI: 10.4225/75/57a7f620aa0c6.

[4] Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, Journal of Theoretical and Applied Information Technology, 2016, vol. 88, No 1, pp. 77-88.

[5] Marques P.H., Jacinto C. Human-HAZOP studies in the risk management of major accidents. In Proceedings of the International Symposium on Occupational Safety and Hygiene (SHO'2015, Guimarães, Portugal, 12-13 February 2015), 2016, pp. 146-148. DOI: 10.13140/RG.2.1.4446.1684.

[6] Jakub B., Schindler F. Assets Dependencies Model in Information Security Risk Management. In Proceedings of the Second IFIP International Conference (ICT EurAsia, Bali, Indonesia), 2014, pp. 1-10. DOI: 10.13140/RG.2.1.3376.6480.

[7] Alan A.R., Arshad Y., Ibrahim J., et al. IT Risk, Information Security & Governance Practices in Malaysia IHLs. In Proceedings of the International Research Invention, Innovation, and Exhibition 2014 (IRIIE 2014, IIUM, Kuala Lumpur, Malaysia), 2014, pp. 459-459. DOI: 10.13140/2.1.2868.5440.

[8] Pandey P, Shekkens E.A. An Assessment of Market Methods for Information Security Risk Management. In Proceedings of the 16th IEEE International Conference on High Performance and Communications 2014 (WiP Track, Paris, France), 2014, 8 p. DOI: 10.13140/2.1.4348.5445.

[9] Yilmaz R., Yalman Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. TEM Journal. 2016. V. 5. N 2. P. 180–191. DOI: 10.18421/TEM52-10.

[10] Moore T.W., Probst C.W., Ranneberg K., van Eeten M. Assessing ICT Security Risks in Socio-Technical Systems. Dagstuhl Reports. 2017. V. 6. N 11. P. 63–89. DOI: 10.4230/DagRep.6.11.63.

[11] Aleksandrov A.A., Neusipin K.A., Proletarsky A.V., Fang K. Innovation development trends of modern management systems of educational organizations. In: 2012 International Conference on Information Management, Innovation Management and Industrial Engineering. IEEE, Sanya, China, 2012, pp. 187 - 189. DOI: 10.1109/ICIII.2012.6339951.

[12] Buldakova T.I., Mikov D.A. Ensuring the Concordance and the Adequacy of Information Security Risk Factors Assessment. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2017. N 3 (21), pp. 8-15. DOI: 10.21581/2311-3456-2017-2-8-15.

[13] McNaught K., Sutovsky P. Representing Variable Source Credibility in Intelligence Analysis with Bayesian Networks. In Proceedings of the 5th Australian Security and Intelligence Conference (Novotel Langley Hotel, Perth, Western Australia, 3-5 December 2012), 2013, pp. 44-51. DOI: 10.4225/75/57a03050ac5cb.

[14] Grigoras R., Mustata A.-M., Teodorescu C. Predicting the state of security using neural networks. In Proceedings of the 9th International Scientific Conference on eLearning and Software for Education (Bucharest, Romania, 25-26 April 2013), 2013, pp. 362-367. DOI: 10.12753/2066-026X-17-167.

[15] Starodubtsev Yu.I., Grechishnikov E.V., Komolov D.V. Use of neural networks to ensure stability of communication networks in conditions of external impacts. Telecommunications and Radio Engineering. 2011. V. 70. N 14. P. 1263-1275.

[16] Beheshti H., Alborzi M. Using Fuzzy Logic to Increase the Accuracy of E-Commerce Risk Assessment Based on an Expert System. Engineering, Technology & Applied Science Research. 2017. V. 7. N 6. P 2205-2209. DOI: 10.5281/zenodo.1118299.

[17] Sasidevi J., Sugumar R., Priya P.S. A Cost-Effective Privacy Preserving Using Anonymization Based Hybrid Bat Algorithm With Simulated Annealing Approach For Intermediate Data Sets Over Cloud Computing. International Journal of Computational Research and Development. 2017. V. 2. N 2. P. 173-181. DOI: 10.5281/zenodo.1069736.

[18] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 369 - 371. DOI: 10.1109/SCM.2017.7970587.

[19] Singh R., Prasad T.V. Exploration of Hybrid Neuro Fuzzy Systems. In Proceedings of the National Conference on Advances in Knowledge Management (NCAKM 2010, At Lingaya's University, Faridabad, Haryana, India), 2010, 6 p. DOI: 10.13140/RG.2.1.3570.0327.

[20] Derugo P. Application of competitive and transition Petri layers in adaptive neuro-fuzzy controller. Power Electronics and Drives Berlin. 2016. V. 1(36). N 1. P. 103-115. DOI: 10.5277/PED160108.

[21] Schauer S., Stamer M., Bosse C., et al. An adaptive supply chain cyber risk management methodology. In Proceedings of the Hamburg International Conference of Logistics (HICL, Hamburg, Germany), 2017, pp. 405-425. DOI: 10.15480/882.149.