The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems

Sergiy Gnatyuk[a,b], Oleksiy Yudin[b], Viktoriia Sydorenko[a], Tetiana Smirnova[c] and Artem Polozhentsev[a]

[a] *National Aviation University, 1, Liubomyr Huzar Ave, Kyiv, 03058, Ukraine*
[b] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3, Maksym Zaliznyak Str, Kyiv, 03142, Ukraine*
[c] *Central Ukrainian National Technical University, 8, Universytetskyi Ave, Kropyvnytskyi, 25000, Ukraine*

Abstract

The subject of the article is methods and models for assessing the criticality of industry information and telecommunication systems (ITS). The purpose of the article is to analyze the existing methods and models for assessing the ITS criticality level and, based on the results, to propose a functional model for assessing the ITS security level. Based on the existed method of hierarchy analysis, a functional model for calculating the quantitative criteria for assessing the security level of the ITS was proposed. The model allows to obtain a quantitative score of the security level through the processing of expert evaluations. This simplifies the expert selection procedure, helps to avoid the specifics of expert data processing, and makes it possible to evaluate the ITS with limited statistical data. The conducted study revealed that the developed model for calculating the quantitative criteria for assessing the security level of the ITS, allows experts to focus on the problem by using pairwise comparisons In addition, the proposed model has a built-in criteria for assessing the quality of the expert's analysis and makes it possible to move from a qualitative assessment, in the form of an ordered series of alphanumeric combinations, to a quantitative assessment, which presented as a ratio of the basic security profile to the security profile defined by the expert.

Keywords

Information and telecommunication system, critical information infrastructure, security assessment criteria, functional security profile.

1. List of abbreviations

Confidentiality:

CT – trusting confidentiality; CA – administrative confidentiality; CO – object reuse; CC – hidden channels analysis; CE – confidentiality in the exchange.

Integrity:

IT – trust integrity; IA – administrative integrity; IR – recovery; IE – integrity in exchange.

Availability:

AR – use of resources; AF – resistance to failures; AQ – quick replacement; AD – disaster recovery.

Observability:

ON – registration; OI – identification and authentication; OC – reliable channel; OD – segregation of responsibilities; OP – integrity of the Complex of means of protection; OT – self-testing; OE – identification during exchange; OS – sender authentication; OR – recipient authentication.

IntelITSIS'2022: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2022, Khmelnytskyi, Ukraine

EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); alex@ukrdeftech.com.ua (O. Yudin); v.sydorenko@ukr.net (V. Sydorenko); t.smirnova@gmail.com (T. Smirnova); artem.polozhentsev@gmail.com (A. Polozhentsev).
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-4730-1463 (O. Yudin); 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-2897-0079 (T. Smirnova); 0000-0003-0139-0752 (A. Polozhentsev).

2. Introduction

Global trends in increasing the number and complexity of cyberattacks have led to the actualization of the need to protect the industry ITS, which are critical for the society, the socio-economic development of the state and for ensuring the information component of the national security of any state. Considering the requirements of the national security and the necessity to implement a systematic approach for handling the problem of critical infrastructure protection at the national level [1], creation of a system for the protection of the critical infrastructure is one of the priorities in the reformation of the defense and security sector of Ukraine. Given that, the main problems that should be solved are: the lack of common criteria for classifying the ITS as critical infrastructure; the lack of a common methodology for assessing threats to the ITS of critical infrastructure facilities.

It should be noted, that according to the Law of Ukraine "On the Fundamentals of Cybersecurity of Ukraine [2] there is a need to form a list of critical information infrastructure facilities and the need to develop criteria and procedures for classifying the ITS as critical infrastructure, and according to the Decree of the President of Ukraine No. 96/2016 "On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine" [3], cybersecurity of critical infrastructure should consist primarily of determining the criteria for classifying information (automated), telecommunications, and the ITS as critical information infrastructure. Therefore, legal acts of Ukraine declare the need to develop common criteria and methodology for classifying the ITS as critical infrastructure facilities. At the same time, the usage of the qualitative assessments is complicated due to their difficulty of comparison and reproduction. First of all, this is caused by the complexity of expert selection and the specifics of processing the experimental data.

The above limitations indicate that there is an important scientific challenge of determining the criteria for classifying the ITS as a critical information infrastructure. This problem has international character as well as it is important for both science and practice today.

The purpose of the study is to propose a functional model for assessing the security level of the ITS based on the results of existing methods and models analysis for assessing ITS criticality.

3. Literature Review

In order to determine the optimal method for calculation of the quantitative criteria for assessing the security of the ITS, the analysis of existing decision-making methods was conducted.

Decision-making methods are applied in case of absence of the comprehensive information about the object of the study (ITS). Decision-making methods can be classified according to the content and type of expert information that was obtained during the analysis [4-6]. Such classification is given in Table 1 [5]. The first three of the mentioned groups are related to the methods of decision-making process under conditions of certainty, and the fourth to the methods of the decision-making process under uncertainty. The most prospective [5] are the following methods: 1) Expected utility hypothesis; 2) Hierarchy analysis; 3) The theory of fuzzy sets

According to the method of expected utility hypothesis, each possible action generates consequences characterized by a particular set of properties, factors, or indicators. That particular alternative should be chosen, the consequences of which are the most preferable. Applying this method, it is necessary to obtain quantitative score of all possible outcomes, which is the result of decision-making processes. Once it done, the best result based on these scores should be chosen. In general, this method consists of five steps [6]: 1) Initial analysis. At this step, some possible options of actions that can be performed in the decision process are identified. 2) Structural analysis. Structuring the problem on a qualitative level. For this purpose, a decision tree should be built. The decision tree has two types of vertices: solutions and cases. In vertices-decisions the choice depends on the expert, and in vertices-cases the expert could foresee the choice with a certain probability. 3) Uncertainty analysis. At this step, the decision should be made to set the probability values for those branches on the decision tree that start from the node-evidence. All acquired probability values are subject to consistency validation. 4) Utility analysis. This step requires the quantitative scores of the utility consequences of the results, which are associated with the implementation of a particular path in the decision tree. 5) Optimization Procedure. The optimal strategy of action may be found by calculating the maximum level of the expected utility over the entire set of possible outcomes.

The main advantage of the method is the ability to find the best solution under the risk conditions. But, on the other hand, the methods of expected utility hypothesis have some disadvantages, namely: time consuming process, associated with the collection of information on the advantages and probability distributions related to the effects [7]; the need to involve some additional analysts; lack of mechanisms to verify experts' decision. Also, the disadvantages according to [8-9] should include that: experts do not structure the problem holistically, as it is expected in the theory; experts do not process information, especially probability, according to the principles of expected utility; expected utility theory poorly suggests human behavior when they have to make decisions in laboratory tests.

Table 1
Classification of the decision-making methods based on content and type of expert information

No.	Content of information	Type of information	Decision making method
1	Expert information is not required	-	The method of domination Method based on global criteria
2	Information on superiority on a set of criteria	Qualitative information; Quantitative assessment of the superiority of the criteria Quantitative information on substitution	Lexicographic ordering Comparison of differences in criteria Convolution methods on the hierarchy of criteria Efficiency-cost methods Methods of the thresholds Methods of the ideal point Methods of indifference curves Methods of value theory
3	Information on the benefits of alternatives	Estimation of the advantage of pairwise comparisons	Methods of mathematical programming Linear and nonlinear convolutions with an interactive way to determine its parameters
4	Information on the benefits of many criteria and the consequences of alternatives	Lack of information about the benefits Quantitative information on the consequences Qualitative information about the benefits and quantitative information about the consequences	Methods with discretization of uncertainty Stochastic dominance Methods of decision-making in conditions of risk and uncertainty based on global criteria Method of analysis of hierarchies Method of decision matrices Methods of fuzzy set theory Method of practical decision-making Methods of indifference curves for decision making in conditions of risk and uncertainty Methods of decision trees Decomposition methods of the theory of expected utility

The method of hierarchy analysis is a mathematical tool for a systematic approach for solving complex decision-making problems. It also implements a procedure for the synthesis of priorities, which are calculated on the basis of the expert's decisions. This method allows the expert to find a solution (alternative) to the problem that would be better consistent with his understanding of the issue and the requirements for its solution. In general, this method consists of five steps [10]: 1) Construction of a qualitative model of the problem, which includes the goal, alternative options for achieving the goal, and criteria for assessing the quality of the alternatives. The model is described by a means of a hierarchy; 2) Determination of the values of all hierarchy parts with the implementation of the method of pairwise

comparisons. A matrix of pairwise comparisons should be formed; 3) Synthesis of the global alternative priorities and obtaining a vector of priorities; 4) Verification of the decisions of the experts on consistency by assessing the level of consistency of the matrix of pairwise comparisons; 5) Obtaining the value of the best alternative and making a decision. The advantages of the method are [11]: the usage of pairwise comparisons, which allows the expert to focus on the problem; additionality of the original matrix; availability of the verbal and numerical scale; built-in criteria for the assessment of the quality of the expert's work, which is the consistency index, which provides information about the violation of numerical and transitive consistency of the made decisions. It should be noted, that the method is not devoid of the following drawbacks [12-14]: evaluation and comparison of more than nine [13] or ten [14] objects (criteria, alternatives). With increasing the number of objects, the complexity of constructing a homogeneous matrix of pairwise comparisons increases. Also, limitations are caused by the psychological capacity of an expert to compare and rate a large number of objects; the appearance of the reverse rank effect, which means changing the order of previously comparable alternatives by adding new or deleted existing ones; the usage of the scale of relations, which is a rank multiple of a unit scale.

The methods of fuzzy set theory consist of formalizing the input parameters by means of a vector of interval values (fuzzy interval), and getting into each interval is characterized by some level of uncertainty. The limits of the possible parameters and their most possible values are determined on the basis of the output data, experience and intuition of the expert. Thus, the basic characteristic of one or another method is the membership function with the interval parameter [15]. There are a lot of methods for determining the membership function, e.g., pairwise comparisons, expert evaluations, linguistic terms based on statistical data, parametric and interval evaluations [16]. The mentioned methods can be classified as direct or indirect [17]. In direct methods the expert directly sets the rules for determining the membership function, for example, the methods are based on a probabilistic interpretation of the membership function. On the other hand, the in indirect methods the expert select the values of the membership function in the way that satisfies the predetermined requirements, for example, the large-square method. The advantages of the fuzzy set methods are [18-21]: the ability to evaluate the alternatives sufficiently objectively by an individual criteria; the ability to include qualitative values in the analysis, to operate with the fuzzy input data and linguistic criteria; At the same time, these methods have some disadvantages, as follows [17; 22-23]: there is a subjectivity in the choice of the membership functions and the formation of fuzzy set rules, and therefore the type of function depends significantly on the available information and the nature of the problem; the information about the correlation of the criteria should be given; each method has its own limitations and specifics, and the expert must know the scope of each method; most of the fuzzy set methods show a weak stability of the results with respect to the input data. Rule-based methods have the greatest stability under such conditions. Given the above, it is recommended to apply the method of hierarchy analysis to calculate the quantitative criteria for assessing security.

4. The Model for Calculating the Quantitative Criteria for Assessing the Security Level

The model for calculating the quantitative criteria for assessing the security level of the ITS, allows to move from a qualitative assessment in the form of an ordered series of alphanumeric combinations [24], which indicate the levels of implemented services, to a quantitative assessment as a ratio of the basic security profile to the security profile determined by the expert, based on the use of the hierarchy analysis method. The input data for the model are the basic Functional Security Profile (FSP) [25] and the FSP that has been corrected by the expert. The Normative Documents in the field of Technical Protection of Information of Ukraine (ND TPI) 2.5-005-99, which defines the standard FSP of the processed information, defines the requirements for the protection of certain information from some threats and functional services and allows to counter these threats and ensure compliance with the requirements [26]. Given the limitations of the hierarchy analysis method in assessing no more than nine to ten criteria, the groups of criteria for assessing information security will be formed (Fig. 1) [27-29]. As it is shown, the largest criteria group of the second level is the observation criteria, which may include up to 9 criteria. The criteria groups of all other levels count from four to five criteria. Therefore, the method of hierarchy analysis may be used to analyze certain criteria.

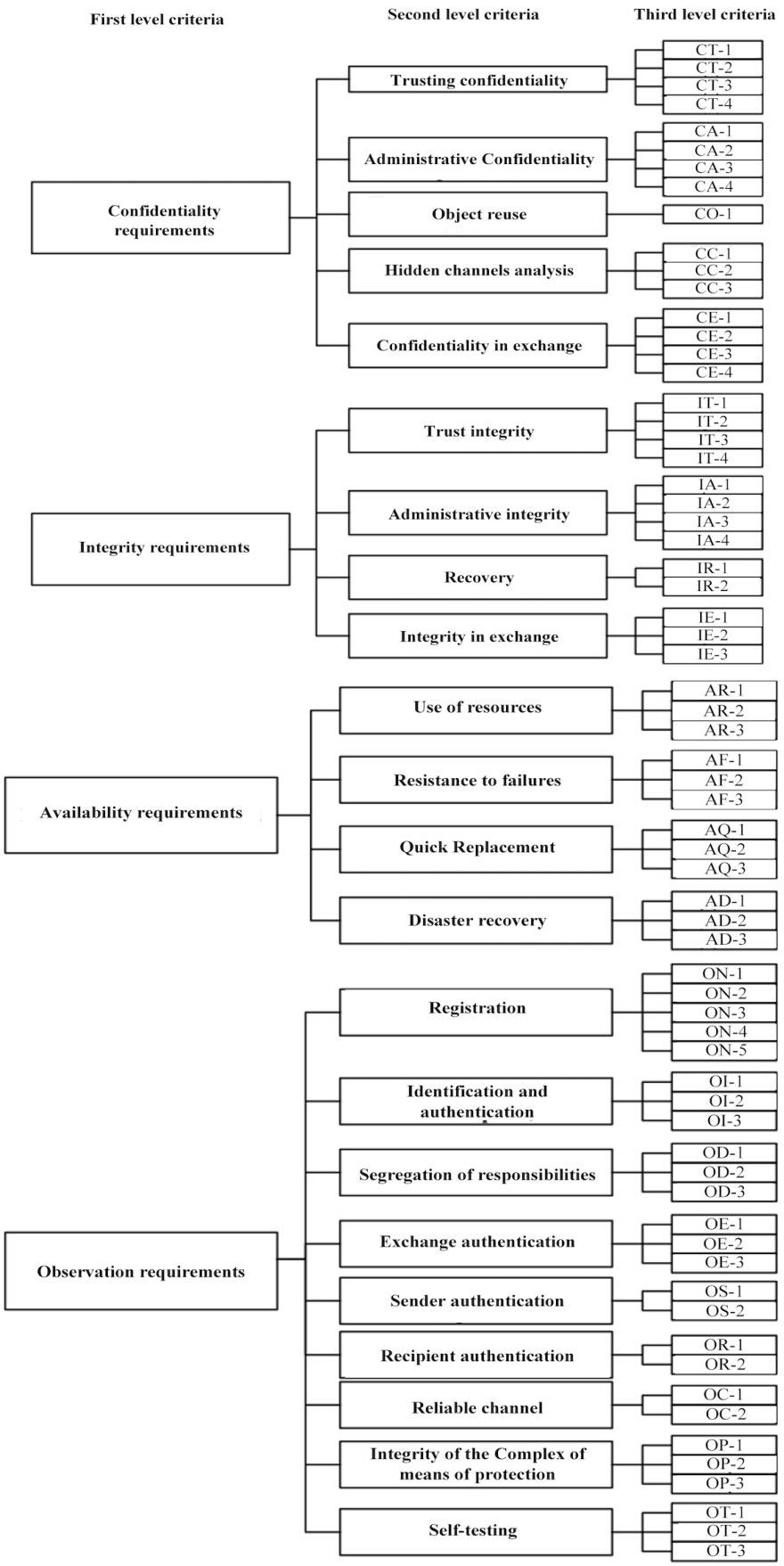

Figure 1: Groups of criteria for assessing the security of information for availability and observability

A flowchart of the model for calculating the quantitative criteria for assessing the security level of the ITS, based on the use of the hierarchy analysis method, is shown in Fig. 2.

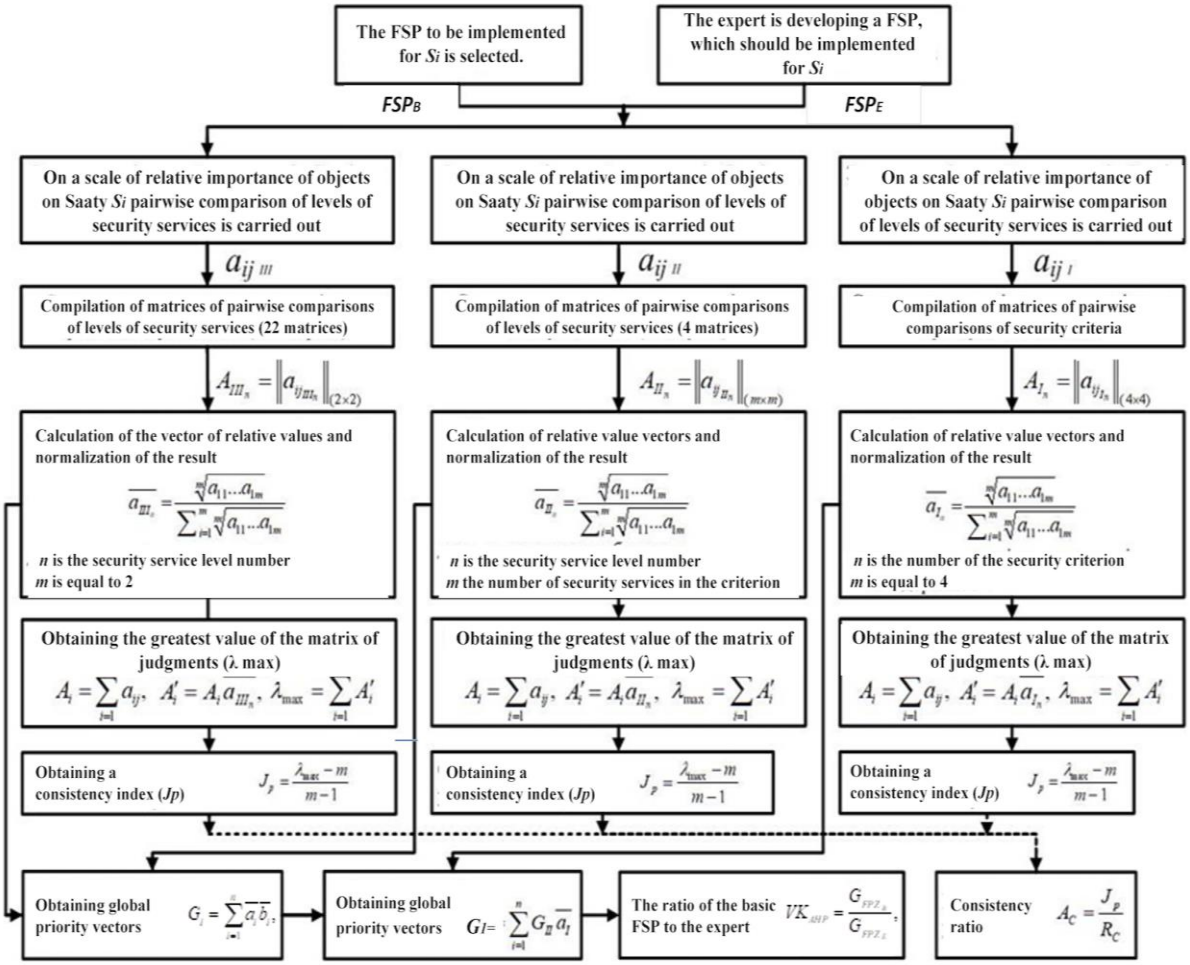

Figure 2: Flowchart of the model for calculating the quantitative criteria for assessing the security level of the ITS

The hierarchy analysis method for determining the ratio of alternatives (the basic FSP and the FSP defined by the expert) is performed in the following way:

Step 1. The matrices of pairwise comparisons should be constructed for each level of criteria (security criteria is a level 1, security service criteria is a level 2, security service level criteria is a level 3):

$$A = \|a_{ij}\|_{nxn}, \quad (1)$$

where $a_{ij} = w_i / w_j$, w_i is the value of the *i*-th criteria.

At the same time, $a_{ji} = 1/a_{ij}$, and $a_{ii} = 1.$, which means that the matrix is positive inversely symmetric.

To determine the value, the following Table 2 of relative importance will be used.

For the security service criteria, matrices of pairwise comparisons are compiled. There are up to 4 matrices in total. For security level criteria, the maximum number of matrices can be 22.

Step 2. The set of eigenvectors of the matrix should be calculated by the geometric mean for each row of the matrix:

$$a_i = \sqrt[n]{a_{i1} \cdot a_{i2} \cdot a_{i3} \cdot a_{in}} = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}, \quad (2)$$

where n is a dimension of the matrix.

Step 3. The results should be normalized, and the normalized priority vector will be obtained:

$$\overline{a_i} = \frac{a_i}{\sum_{j=1}^{n} a_j}, \tag{3}$$

Step 4. Consistency of local priorities should be checked. Calculation of the largest eigenvalue of the matrix should be performed:

$$A_i = \sum_{i=1}^{n} a_{ij}, \tag{4}$$

$$A_i' = A_i \overline{a_{ij}}, \tag{5}$$

$$\lambda_{\max} = \sum_{i=1}^{n} A_i', \tag{6}$$

Calculation of the consistency index:

$$J_p = \frac{\lambda_{\max} - m}{m-1}, \tag{7}$$

where m is the number of compared elements (matrix size).

Table 2
Scale of relative importance of criteria

Verbal assessment of the expert	The Value a_{ij}
w_i absolutely better than w_j	9
w_i significantly better than w_j	8
w_i much better than w_j	7
w_i better than w_j	6
w_i strongly predominant w_j	5
w_i predominant w_j	4
w_i slightly predominant w_j	3
w_i insignificantly predominant w_j	2
the criteria are equivalent	1
w_j insignificantly predominant w_i	1/2
w_j slightly predominant w_i	1/3
w_j predominant w_i	1/4
w_j strongly predominant w_i	1/5
w_j better then w_i	1/6
w_j much better than w_i	1/7
w_j significantly better than w_i	1/8
w_j absolutely better than w_i	1/9

For the security criteria the comparison matrix will be as shown in Table 3.

Table 3
The Matrix for security criteria

	Confidentiality	Integrity	Availability	Observability
Confidentiality	a_{11}	a_{12}	a_{13}	a_{14}
Integrity	a_{21}	a_{22}	a_{23}	a_{24}
Availability	a_{31}	a_{32}	a_{33}	a_{34}
Observability	a_{41}	a_{42}	a_{43}	a_{44}

The consistency index should be checked by calculating the A_C consistency ratio using the formula:

$$A_c = \frac{J_p}{R_c}, \tag{8}$$

where R_c is the table value (Table 4).

Step 5. Calculation of the global priority for the high-level criteria. The normalized priority vector for each lower-level criteria is multiplied by the normalized priority vector of the higher-level criteria. The products are summed at the higher level.

$$G_i = \sum_{i=1}^{n} \overline{a_i}\,\overline{b_i}, \tag{9}$$

where n is a number of the security level criteria.

Table 4

Random consistency for matrices of order 2-9

Matrix size (n)	Random consistency (RC)
2	0
3	0,58
4	0,9
5	1,12
6	1,24
7	1,32
8	1,41
9	1,45

If $A_c \geq 0{,}10$, then the data in the comparison matrix are subject to review and refinement.

Step 6. Determining the ratio of alternatives (the basic FSP and the FSP defined by the expert). For each FSP, a global priority should be calculated for the confidentiality, integrity, availability, and observability. The ratio of these global priorities, which describe the quantitative criteria, can be represented in the form of an expression:

$$VK_{AHP} = \frac{G_{FPZ_B}}{G_{FPZ_E}}, \tag{10}$$

where G_{FPZ_B} is the table value of the FSP for the industry ITS, and G_{FPZ_E} is the FSP, which was obtained by the expert, using the structural-logical model and the structural-functional method of formation of the FSP of the industry ITS.

The implementation of this model allows to move from the qualitative characteristics of security to the quantitative ones. Proposed model can be used for real ITS in critical infrastructure to calculate its security level.

Conclusion

In this paper, the analysis of existing decision-making methods for determining the optimal way for calculating the quantitative criteria for assessing the security of the ITS was conducted. The methods of expected utility theory, methods of hierarchy analysis and methods of fuzzy sets theory were investigated. Taking into account the main advantages and disadvantages of the mentioned methods, it is advisable to use the methods of hierarchy analysis to calculate the quantitative criteria for the security assessment.

The model for calculating the quantitative criteria for assessing the security level of the ITS, which is based on the use of the method of hierarchy analysis, was developed. This model works by using the pairwise comparisons, which allows the expert to focus on the problem. Also, the model has built-in criteria for assessing the quality of the expert's analysis. It is the consistency index, which provides information on the violation of numerical and transitive consistency of ratings. In addition, the developed model makes it possible to move from a qualitative assessment, in the form of an ordered series of alphanumeric combinations, which indicates the level of realized services, to a quantitative assessment in the form of the ratio of the basic security profile to the security profile determined by the

expert. In further works it is planned to carry out an experimental study of the developed model for calculating the quantitative criteria for assessing the security level of the ITS.

References

[1] M. Wright, H. Chizari and T. Viana, Analytical Framework for National Cyber-security and Corresponding Critical Infrastructure: A Pragmatistic Approach, 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 127-130, DOI: 10.1109/CSCI51800.2020.00029.

[2] Ukraine, Laws, "On the basic principles of cybersecurity in Ukraine", official text: [adopted by the Verkhovna Rada on October 5, 2017], Kyiv: Information of the Verkhovna Rada of Ukraine, 2017, No. 45, p. 403.

[3] Decree of the President of Ukraine No. 96, On the decision of the National Security and Defense Council of Ukraine of January 27, 2016, "On the Cyber Security Strategy of Ukraine", 2016.

[4] Tapan K. Sarkar; Magdalena Salazar-Palma; Ming Da Zhu; Heng Chen, Mathematical Principles Related to Modern System Analysis, in Modern Characterization of Electromagnetic Systems and its Associated Metrology, IEEE, 2021, pp. 1-20, DOI: 10.1002/9781119076230.ch1.

[5] Z. Hu, I. Tereykovskiy, L. Tereykovska, V. Pogorelov, Determination of Structural Parameters of Multilayer Perceptron Designed to Estimate Parameters of Technical Systems", International Journal of Intelligent Systems and Applications (IJISA), Vol.9, No.10, pp. 57-62, 2017. DOI: 10.5815/ijisa.2017.10.07

[6] Paul M. Anderson; Charles Henville; Rasheek Rifaat; Brian Johnson; Sakis Meliopoulos, Fault Tree Analysis of Protective Systems, in Power System Protection, IEEE, 2022, pp. 1261-1310, DOI: 10.1002/9781119513100.ch29.

[7] Z. Hu, Yu. Khokhlachova, V. Sydorenko, I. Opirskyy, Method for Optimization of Information Security Systems Behavior under Conditions of Influences, International Journal of Intelligent Systems and Applications (IJISA), Vol.9, No.12, pp.46-58, 2017. DOI: 10.5815/ijisa.2017.12.05

[8] Paul J.H. Schoemaker, The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations, Journal of Economic Literature, June 1982, No. 2, pp. 529-563.

[9] Z. Ma, S. Wang, X. Deng and W. Jiang, An improved approach for adversarial decision making under uncertainty based on simultaneous game, 2018 Chinese Control and Decision Conference (CCDC), 2018, pp. 2499-2503, DOI: 10.1109/CCDC.2018.8407545.

[10] X. Guo, M. Gao, M. Zhang, Y. Chen and S. -P. Tseng, Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method", 2020 8th International Conference on Orange Technology (ICOT), 2020, pp. 1-3, DOI: 10.1109/ICOT51877.2020.9468778.

[11] Z. -J. Wang, A Novel Triangular Fuzzy Analytic Hierarchy Process, IEEE Transactions on Fuzzy Systems, vol. 29, no. 7, pp. 2032-2046, July 2021, doi: 10.1109/TFUZZ.2020.2992103.

[12] D. Leman, Expert System Diagnose Tuberculosis Using Bayes Theorem Method and Shafer Dempster Method, 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018, pp. 1-4, DOI: 10.1109/CITSM.2018.8674380.

[13] Y. Guang, Z. Yong-di, Y. Yan-fang and Z. Rui-gang, Analysis Hierarchy Set Pair Model on Material Selection, 2009 First International Workshop on Database Technology and Applications, 2009, pp. 345-347, DOI: 10.1109/DBTA.2009.155.

[14] S. Qing and L. Fang, Research on the Intelligent Combat Decision-Making under the Simulation and Deduction System, 2021 International Conference on Big Data and Intelligent Decision Making (BDIDM), 2021, pp. 206-209, DOI: 10.1109/BDIDM53834.2021.00049.

[15] Z. Hu, Ye. Bodyanskiy, N. Kulishova, O. Tyshchenko, A Multidimensional Extended Neo-Fuzzy Neuron for Facial Expression Recognition, International Journal of Intelligent Systems and Applications (IJISA), Vol.9, No.9, pp.29-36, 2017. DOI: 10.5815/ijisa.2017.09.04

[16] O. E. Sandoval-Alfaro and R. R. Quintero-Meza, Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology, 2021 Mexican International Conference on Computer Science (ENC), 2021, pp. 1-8, DOI: 10.1109/ENC53357.2021.9534800.

[17] Tamalika Chaira, Fuzzy/Intuitionistic Fuzzy Set Theory, in Fuzzy Set and Its Extension: The Intuitionistic Fuzzy Set , Wiley, 2019, pp.1-40, DOI: 10.1002/9781119544203.ch1.
[18] J. L. Guevara Diaz, J. M. Mendel and R. Hirata Junior, "Fuzzy-System Kernel Machines: A Kernel Method Based on the Connections Between Fuzzy Inference Systems and Kernel Machines", in IEEE Transactions on Fuzzy Systems, DOI: 10.1109/TFUZZ.2022.3153141.
[19] R. Bellman, L. Zadeh, "Decision-making in vague conditions, Questions of analysis and decision-making procedures", Mir, Moscow, 1976, pp. 172-175.
[20] S. Qing and L. Fang, "Research on the Intelligent Combat Decision-Making under the Simulation and Deduction System", 2021 International Conference on Big Data and Intelligent Decision Making (BDIDM), 2021, pp. 206-209, DOI: 10.1109/BDIDM53834.2021.00049.
[21] L. Yan, Z. Pei and F. Ren, "Constructing and Managing Multi-Granular Linguistic Values Based on Linguistic Terms and Their Fuzzy Sets", in IEEE Access, vol. 7, pp. 152928-152943, 2019, doi: 10.1109/ACCESS.2019.2948847.
[22] V. Dmitrikov, V. Bakharev, Structural priorities of the expert system of environmental monitoring, Environmental safety №2 (16), 2013.
[23] P. V. S. Reddy, "Generalized Fuzzy Logic with twofold fuzzy set: Learning through Neural Net and Application to Business Intelligence" 2021 International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2021, pp. 1-5, DOI: 10.1109/iFUZZY53132.2021.9605090.
[24] ND TPI 2.5-004-99, Criteria for assessing the security of information in computer systems from unauthorized access, State Service of Special Communication and Information Protection of Ukraine, 1999.
[25] O. Yudin, Analysis of requirements for elements of information and telecommunication systems of energy infrastructure management, which provide cyber protection, Proceedings of the third all-Ukrainian scientific-practical. conf., Perspective directions of information protection, Odessa, September 02-06, 2017.
[26] Z. Hu, R. Odarchenko, S. Gnatyuk, M. Zaliskyi, A. Chaplits, S. Bondar, V. Borovik, Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior", International Journal of Computer Network and Information Security (IJCNIS), Vol.12, No.6, pp.1-13, 2020. DOI: 10.5815/ijcnis.2020.06.01
[27] S.Gnatyuk, V.Sydorenko, A.Polozhentsev, Y.Sotnichenko. Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure, Proceedings of 2020 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2020, Kyiv, Ukraine, October 6-9, 2020, pp. 757-764.
[28] A. A. Elmarady and K. Rahouma, Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment, in IEEE Access, vol. 9, pp. 143997-144016, 2021, DOI: 10.1109/ACCESS.2021.3121230.
[29] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta and R. De Nicola, Framework, Tools and Good Practices for Cybersecurity Curricula, in IEEE Access, vol. 9, pp. 94723-94747, 2021, DOI: 10.1109/ACCESS.2021.3093952.
[30] D. Tayouri, S. Hassidim, E. Bremier, A. Smirnov, P. A. Shabtai, Cybersecurity Technologies for Cloud Access, in Cybersecurity Technologies for Cloud Access, pp.1-30, 14 Feb. 2022.