Experimental study of the model for calculating the quantitative criteria for assessing the security level of information and communication systems of the state critical infrastructure

Sergiy Gnatyuk[1,*,†], Viktoria Sydorenko[1,†], Oleksii Yudin[2,†], Andrii Paziuk[1,†] and Artem Polozhentsev[1,†]

[1] National Aviation University, 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 03142 Kyiv, Ukraine

Abstract

In the context of rapid technological development and the introduction of Information Technology systems in all areas of life, including critical infrastructure management, today's potential cyber-attacks can lead to very serious consequences. Therefore, the protection of such ICS has become critical in ensuring national security. Consequently, given the current requirements of national security and the need for a systemic approach to critical infrastructure protection, new approaches to ensuring the security of such infrastructure must be developed, which is now one of the most important challenges in the Ukrainian Defense sector. Therefore, there is an important and actual need to develop methods and models for the classification of the ICS as critical infrastructure to ensure the national security of the country. The paper develops a model for calculating the quantitative criterion for assessing the level of ICS security, which is based on the method of hierarchy analysis. The quantitative index of the security level is calculated by processing expert evaluations. It makes the procedure of expert selection easier, avoids the specifics of expert data processing, as well as to evaluates the ICS according to a limited number of statistical data. The model developed in the paper makes it possible to move from a qualitative assessment to a quantitative one, specifically, to move from an ordered series of alphanumeric combinations to a correlation of functional security profiles. Also, to verify the results and conduct experimental research, new software was developed, which is based on the model under study. Verification of the developed model was carried out based on the National Confidential Communication System. As part of future research, the authors will improve the developed model to apply it to other areas of critical infrastructure.

Keywords

information and communication system, critical infrastructure, critical infrastructure object, cybersecurity, security assessment criterion, functional security profile

1. Introduction

In the context of rapid technological development and the introduction of Information Technology systems in all areas of life, including critical infrastructure (Fig. 1) management, today's potential cyber-attacks can lead to very serious consequences [1].

Therefore, the protection of such ICS has become critical in ensuring national security. Consequently, given the current requirements of national security and the need for a systemic approach to critical infrastructure protection, new approaches to ensuring the security of such infrastructure must be developed, which is now one of the most important challenges in the Ukrainian Defense sector [2].

The main open challenges to be met to achieve the above goal are the lack of unitary criteria and a specific procedure for attributing the ICS facilities to critical infrastructure; the lack of unitary methods for assessing the level of protection of critical infrastructure facilities of the ICS, etc. (Fig. 2). It is important to note that according to the Law of Ukraine "On the Fundamentals of Cybersecurity of Ukraine" [3], it is necessary to create a list of critical information infrastructure facilities, for which it is necessary to develop criteria and methods of attributing such facilities to critical infrastructure. This is confirmed by the Decree of the President of Ukraine [4], which provides that to ensure the cyber security of critical infrastructure, it is necessary, especially, to determine the criteria for attributing information, communications, and the ICS to critical

CSDP-2024: Cyber Security and Data Protection, June 30, 2024, Lviv, Ukraine
*Corresponding author.
†These authors contributed equally.
s.gnatyuk@nau.edu.ua (S. Gnatyuk); v.sydorenko@ukr.net (V. Sydorenko); alex@ukrdeftech.com.ua (O. Yudin); inet.media.law@gmail.com (A. Paziuk); artem.polozhencev@gmail.com (A. Polozhentsev)

0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-5910-0837 (V. Sydorenko); 0000-0002-5910-0837 (O. Yudin); 0000-0002-1622-1671 (A. Paziuk); 0000-0003-0139-0752 (A. Polozhentsev)

information infrastructure. In addition, at the end of 2021, a basic law in this area was adopted [5] (entered into force on June 15, 2022), providing the necessary legal and organizational principles for the development and implementation of the national system of critical infrastructure protection.

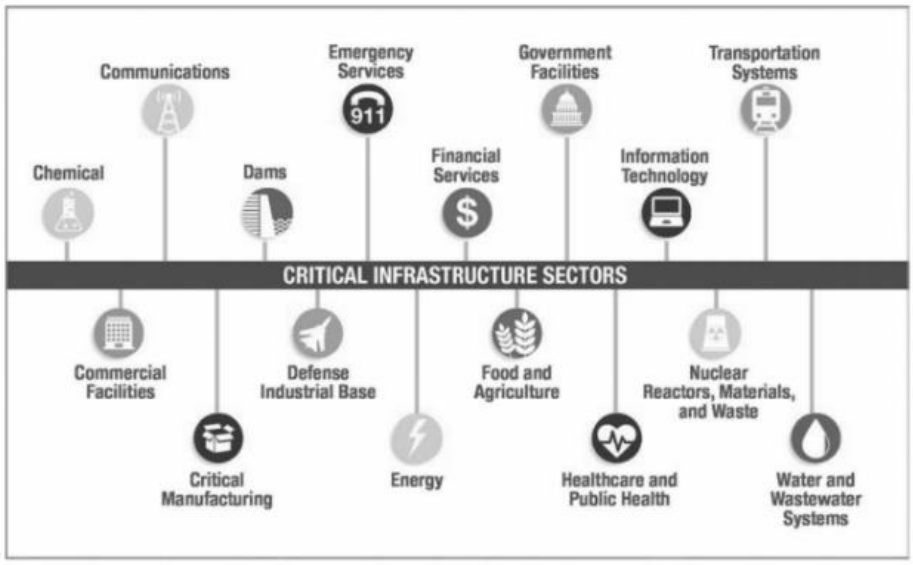

Figure 1: Critical infrastructure sectors by Guide for the Critical Infrastructure Community

Figure 2: Up-to-date ICS interconnection

The mentioned regulations of Ukraine state the need to develop unified criteria and procedures for attributing the ICS infrastructure to the state's critical infrastructure. It is important to mention that the use of qualitative (rather than quantitative) assessments is associated with the difficulty of comparing them. Above all, such limitations are due to the difficulty of selecting experts and the specifics of processing expert data. As a consequence, there is an important scientific problem in determining the criteria for attributing the ICS to critical information infrastructure.

2. Literature review

To determine the possible criteria for classifying an object as critical infrastructure, the analysis of the regulatory documents of the European Union countries was performed. During the analysis of normative documents of Austria, Spain, Sweden, the Netherlands, and Slovenia the following was found.

Austria. The Strategic Plan of the Austrian Critical Infrastructure Protection Program [6] defines the following global criteria: the number of citizens involved (health and social consequences); economic effect; environmental impact; psychological effect; political consequences; territorial extent; duration; lack of substitution options; interdependence of critical infrastructure sectors (destruction of one result in the destruction of others).

Spain. The Law of the Kingdom of Spain on the establishment of measures to protect critical infrastructure [7] defines the following criteria for classifying an object as critical infrastructure: the number of citizens involved (deaths, injuries with serious injuries, and other serious health consequences); economic impact (economic losses and deterioration of products and services); environmental impact; political impact (confidence in the public administration) and social impact (physical suffering, disruption of daily life).

Sweden. The Action Plan for the Protection of Critical Public Functions and Critical Infrastructure of the Kingdom of Sweden [8] defines critical facilities as those whose disruption results in the following: the number of citizens involved (about 30 people killed or injured with severe injuries); the occurrence of economic effects or environmental impact (direct costs of about 10 million euros); political consequences or social impact (citizens were killed, inability to influence the incident.

The Netherlands. The Dutch Ministry of Security and Justice Resilience Directive [9] divided infrastructure criticality into two categories.

Category A—Infrastructure disruptions would have the following consequences: state financial loss of more than €50 billion or a decline in revenue of about 5% in real terms; more than 10,000 people would be killed, injured, or chronically ill; more than 1 million people would be on the brink of survival or seriously mentally ill; at least two other critical infrastructure sectors would begin to deteriorate.

Category B—Infrastructure disruptions would have the following consequences: state financial losses of more than €5 billion or a decline in revenues of about 1% in real terms; more than 1,000 people would be killed, maimed, or chronically ill; more than 100,000 people would be at the brink of survival or severely mentally injured.

The Republic of Slovenia. General and sectoral criteria for defining the critical infrastructure of the national importance of the Republic of Slovenia [10] state that the main criteria for defining critical infrastructure are: deaths of more than 50 people; health effects resulting in the hospitalization of more than 100 people for a week; complications in the implementation of internal security of the state; losses of more than 10 million euros per day; inability to supply drinking water or food for a week for 100,000 people.

Summarizing the above and by [11] it can be concluded that the most common criteria for referring to critical infrastructure are the following: the number of citizens involved (health and social consequences); economic effect (financial losses); environmental impact (pollution, destruction); political consequences or social impact (citizens were killed, inability to influence the incident, reduced confidence in public administration, civil unrest, etc.

It is advised to evaluate the above criteria by qualitative and quantitative indicators.

The analysis of existing decision-making methods was carried out in [2] to find the most adequate method for calculating the quantitative criteria for assessing the level of ICS security. It was defined that decision-making methods can be classified by the content and type of expert information that can be obtained [12–14]. In addition, the methods under study are decision-making methods under conditions of certainty as well as methods under conditions of uncertainty (fuzzy). According to [2], the following methods are the most prospective in the opinion of the authors:

1. The method of the expected utility hypothesis determines that any possible action creates consequences described by a set of properties, indicators, or factors. It is necessary to choose that alternative, the result of which is the most preferred. By using the method, it is required to get a quantitative assessment of all possible outcomes, resulting from decision-making processes [2, 14].
2. The method of hierarchy analysis is a systematic approach to complex decision-making problems. Also implemented is a procedure to synthesize priorities, that is calculated based on the expert's decisions. The method makes it possible for the expert to determine a possible solution (alternative) for a problem, which would better meet his comprehension of the problem and the solution requirements.
3. The method of the theory of fuzzy sets represents the formalization of the incoming values using a vector of interval values (fuzzy interval), and each interval is characterized by some level of uncertainty. The boundaries of potential values of parameters and their maximum values are specified based on the input data, the expert's experience, and intuition.

Thus, the main parameter of any given method is the membership function of an interval parameter [15]. There are many advanced methods for the definition of the membership functions, for example, methods of pairwise comparisons, expert evaluations, linguistic terms based on statistical data, parametric, interval evaluations, and others [16].

The analysis carried out in this paper shows that the most effective methods are rule-based ones. Given the advantages and disadvantages of the above methods, to calculate the quantitative criterion for security assessment it was agreed to apply the method of hierarchy analysis. Also, in [2] the authors have proposed a calculation model for the quantitative criteria for assessment of the ICS security in the state's critical infrastructure. In this context, Fig. 3 [21] demonstrates modern ICS security threats in different domains.

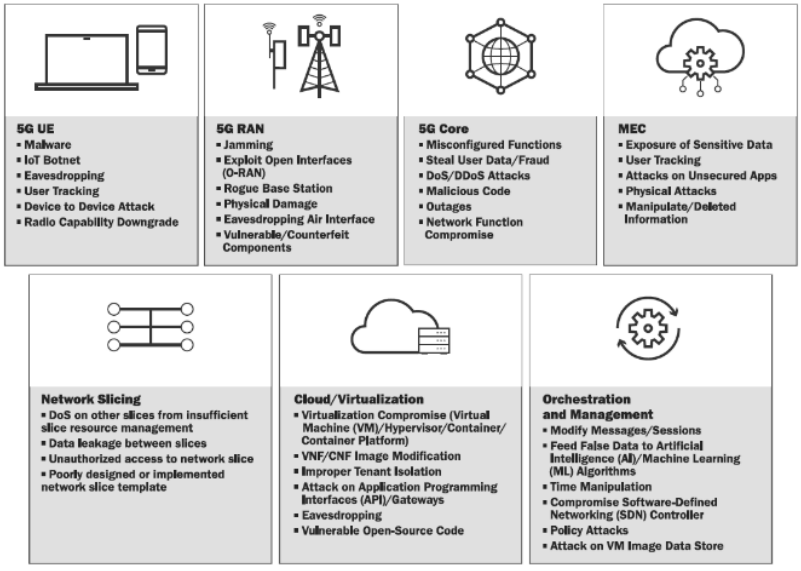

Figure 3: 5G security threats

However, this work provides only a theoretical justification of the specified model without experimental research in a particular area of critical infrastructure. With this in mind, the purpose of this work is to experimentally investigate the model for calculating quantitative criteria for assessing the level of ICS security.

3. Proposed model description

The model developed in the paper makes it possible to move from a qualitative assessment to a quantitative one, specifically, to move from an ordered series of alphanumeric combinations to a correlation of Functional Security Profiles (FSP). The model inputs are the Basic FSP [18] (FSPB) and the Expert-approved FSP (FSPE). ND TPI 2.5-005-99, which determines the FSP standard of the information being processed, contains the requirements for the protection level of specific information against certain threats and known functional protection services to counteract these threats and ensure compliance with the requirements. A block diagram of the above model for calculating the quantitative criteria for assessing the level of the ICS security based on the method of hierarchy analysis is presented in Fig. 4 [2].

The method of hierarchy analysis to determine the correlation of alternatives (FSPB and FSPE) is carried out as follows:

The pairwise comparison matrices must be calculated for each criterion level (security criterion—level 1, security service criterion—level 2, security service level criterion—level 3):

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

where $a_{ij} = w_i/w_j$, w_j 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 and inversely symmetric. The following Table 1 of the relative importance will be used to determine the value.

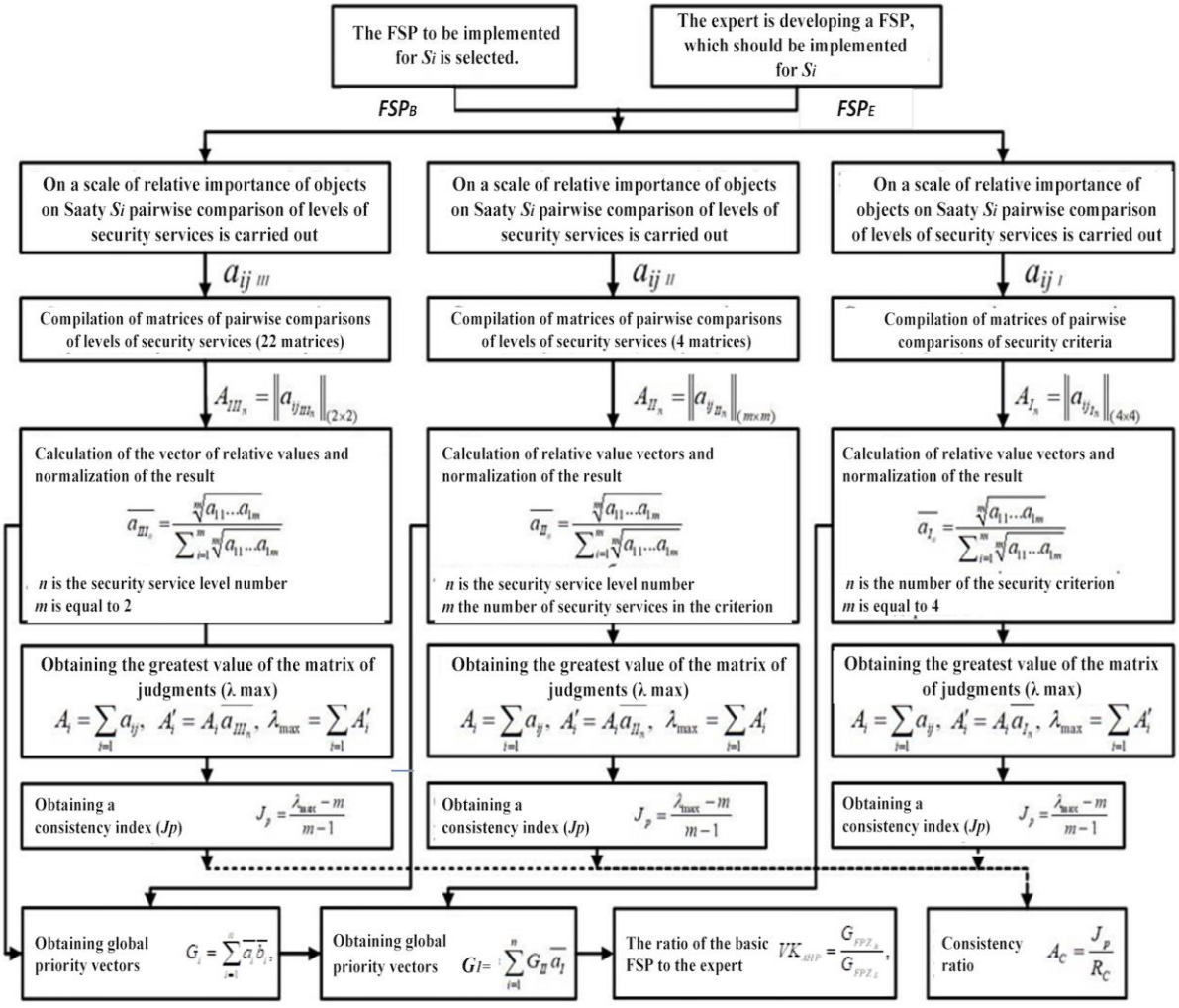

Figure 4: Block scheme of the model

Table 1
Relative importance scale of the criteria

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

The comparison matrix for the security criteria is shown in Table 2.

Table 2
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}

Matrices of pairwise comparisons are calculated for the security criteria. Up to 4 matrices in total can be used. There are 22 matrices at most for the security level criteria.

To calculate the set of eigenvectors of the matrix, the geometric mean for each row of the matrix should be calculated:

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

where n is a dimension of the matrix.

To get the results normalized, the normalized priority vector should be obtained:

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

It is necessary to check the consistency of local priorities. The largest eigenvalue of the matrix must be calculated:

$$A_i = \sum_{i=1}^{n} a_{ij}, \quad (4)$$

$$A_i' = A_i \overline{a_{ij}}, \quad (5)$$

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

Calculation of the consistency index:

$$J_p = \frac{\lambda_{\max} - m}{m-1}, \quad (7)$$

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

The index of consistency should be checked by calculating the coefficient of AC consistency according to the formula:

$$A_c = \frac{J_p}{R_c}, \quad (8)$$

where R_c is the table value (Table 3).

Table 3
Random consistency for matrices of order 2–9

Matrix size (n)	2	3	4	5	6	7	8	9
Random consistency (RC)	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

However, a comparison matrix must be revised and clarified if the AC ≥ 0,10.

The global priority calculation by high-level criteria.

For each criterion of the lower level, the normalized priority vector is multiplied by the normalized priority vector of the higher-level criteria. The results are summarized at the higher level.

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

where n is a number of the security level criteria.

Determination of the correlation of the alternatives (FSPB and FSPE).

A global priority of confidentiality, integrity, availability, and observability must be calculated for each FSP. The correlation of these global priorities, describing quantitative criteria, can be represented as an expression:

$$VK_{AHP} = \frac{G_{FPZ_B}}{G_{FPZ_E}}, \quad (10)$$

where G_{FPZ_B} is the table value of the FSP for the industry ICS, 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 ICS.

4. Experiments and discussion

In many countries of the world, the Information and Communications industry takes one of the first places on criticality after energy and transport [17, 19]. Given this, the experimental verification of the developed model was carried out on the example of the ICS of the National System of Confidential Communication (NSCC). To verify the model for calculating quantitative criteria, matrices of pairwise comparisons for each level of criteria were constructed. For the security criteria (according to [18]) the comparison matrix is as follows in Table 4.

Table 4
The matrix of comparisons for security criteria

	Confidentiality	Integrity	Availability	Observability
Confidentiality	1	a_{12}	a_{13}	a_{14}
Integrity	a_{21}	1	a_{23}	a_{24}
Availability	a_{31}	a_{32}	1	a_{34}
Observability	a_{41}	a_{42}	a_{43}	1

For the security service criteria (according to [19]) the comparison matrix will have the form presented in Tables 4–7. The matrix of confidentiality criteria is presented in Table 4, where: CT is trusting confidentiality, CA is administrative confidentiality, CO is object reuse, CC is hidden channels analysis, and CE is confidentiality in the exchange.

Table 5
The matrix of confidentiality criteria

	CT	CA	CO	CC	CE
CT	1	a_{12}	a_{13}	a_{14}	a_{15}
CA	a_{21}	1	a_{23}	a_{24}	a_{25}
CO	a_{31}	a_{32}	1	a_{34}	a_{35}
CC	a_{41}	a_{42}	a_{43}	1	a_{45}
CE	a_{51}	a_{52}	a_{53}	a_{54}	1

The matrix of integrity criteria is presented in Table 5, where: IT is trust integrity, IA is administrative integrity, IR is recovery, IE is integrity in exchange.

The matrix of availability criteria is presented in Table 6, where: AR is use of resources, AF is resistance to failures, AQ is quick replacement, AD is disaster recovery.

Table 6
The matrix of integrity criteria

	IT	IA	IR	IE
IT	1	a_{12}	a_{13}	a_{14}
IA	a_{21}	1	a_{23}	a_{24}
IR	a_{31}	a_{32}	1	a_{34}
IE	a_{41}	a_{42}	a_{43}	1

Table 7
The matrix of availability criteria

	AR	AF	AQ	AD
AR	1	a_{12}	a_{13}	a_{14}
AF	a_{21}	1	a_{23}	a_{24}
AQ	a_{31}	a_{32}	1	a_{34}
AD	a_{41}	a_{42}	a_{43}	1

The matrix of observability criteria is presented in Table 7, where: ON is registration, OI is identification and authentication, OC is reliable channel, OD is segregation of responsibilities, OP is the integrity of the Complex means of protection, OT is self-testing, OE is identification during the exchange, OS is sender authentication, OR is recipient authentication.

Table 8
The matrix of observability criteria

	ON	OI	OC	OD	OP	OT	OE	OS	OR
ON	1	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
OI	a_{21}	1	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}
OC	a_{31}	a_{32}	1	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}
OD	a_{41}	a_{42}	a_{43}	1	a_{45}	a_{46}	a_{47}	a_{48}	a_{49}
OP	a_{51}	a_{52}	a_{53}	a_{54}	1	a_{56}	a_{57}	a_{58}	a_{59}
OT	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	1	a_{67}	a_{68}	a_{69}
OE	a_{71}	a_{72}	a_{73}	a_{74}	a_{75}	a_{76}	1	a_{78}	a_{79}
OS	a_{81}	a_{82}	a_{83}	a_{84}	a_{85}	a_{86}	a_{87}	1	a_{89}
OR	a_{91}	a_{92}	a_{93}	a_{94}	a_{95}	a_{96}	a_{97}	a_{98}	1

For the matrices of security level criteria, as in our case, it is necessary to make all of the possible 22 matrices for criterion comparisons, according to Table 8, where ON-1 is external analysis; ON-2 is protected log; ON-3 is danger alarm; ON-4 is detailed registration; ON-5 is real-time analysis.

Table 9
The matrix of security level criteria

	ON -1	ON -2	ON -3	ON -4	ON -5
ON -1	1	a_{12}	a_{13}	a_{14}	a_{15}
ON -2	a_{21}	1	a_{23}	a_{24}	a_{25}
ON -3	a_{31}	a_{32}	1	a_{34}	a_{35}
ON -4	a_{41}	a_{42}	a_{43}	1	a_{45}
ON -5	a_{51}	a_{52}	a_{53}	a_{54}	1

The scale given in Table 1 is used to fill in the matrices. The set of eigenvectors of a matrix is calculated using (2) and is calculated as the geometric mean for each matrix. The calculation is made using the specialized software developed by the authors [20]. As a result, a normalized vector of priorities, calculated using (3) and the developed software [14] was obtained. The consistency check of local priorities was carried out by (4–7) also with the help of [14]. At the same time, an error was made in the selection of priorities for accessibility services (Fig. 5).

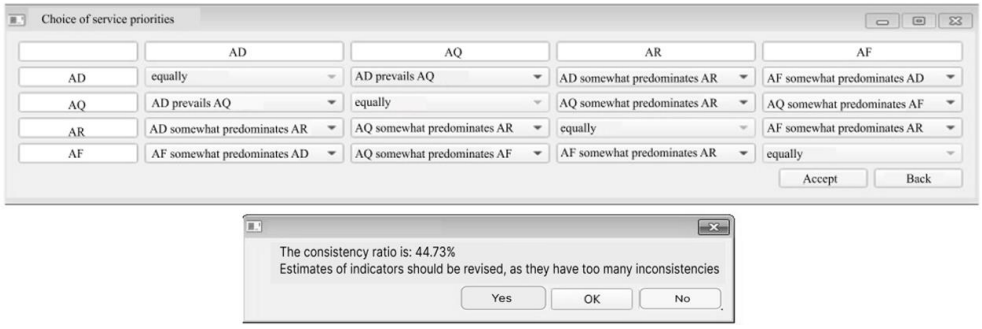

Figure 5: Possible error message

Based on the results of the error analysis, the priorities of accessibility services were revised by the experts (Fig. 6).

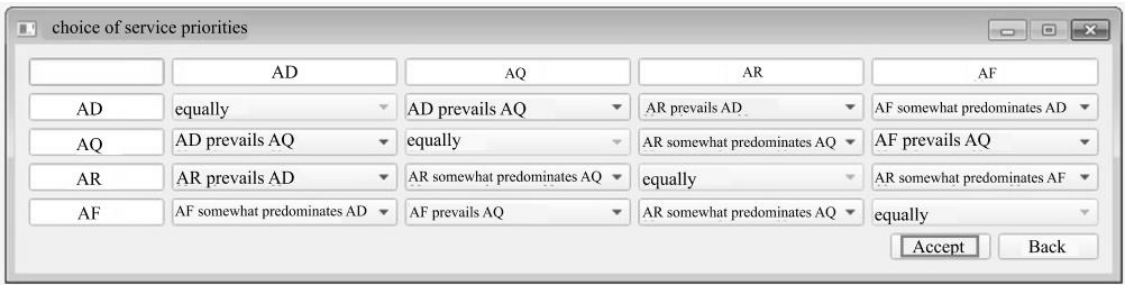

Figure 6: Matrix of availability criteria

The calculation of the global priority for the criteria of confidentiality, integrity, availability, and observability is performed using (9). The result of the calculated ratio of alternatives (FSP_B and FSP_E) is shown in Fig. 7.

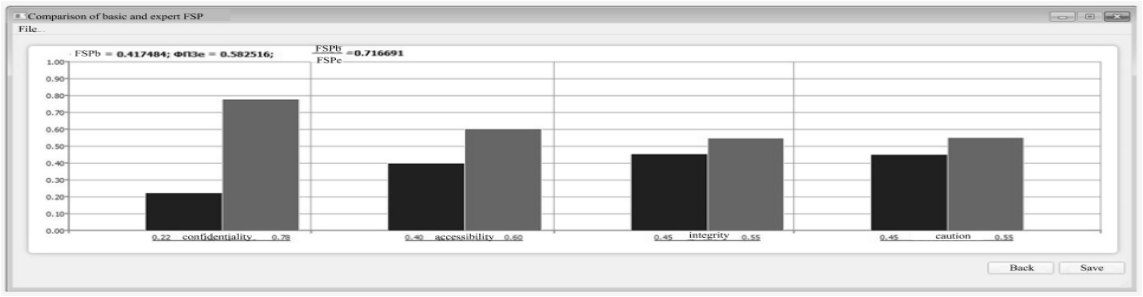

Figure 7: Result of the ratio of alternatives

According to Fig. 7, the importance index of the confidentiality criteria, implemented in the NSCC, is significantly lower than the index, which is reasonable to achieve. The ratio of global priorities, which characterize the quantitative security level, is calculated using (10). The value of these criteria is:

$$VK_{AHP} = \frac{0,417484}{0,582516} = 0,716691 \qquad (11)$$

Thus, the security level values of the main subsystems of NSCC were obtained, using the developed model for calculating the quantitative criteria for assessing the security level of the ICS [22].

5. Conclusions

Therefore, a model for calculating quantitative criteria for assessing the level of ICS security by processing expert evaluations using the method of hierarchy analysis was developed in the study. This made it possible to simplify the expert selection procedure, avoid the difficulties of expert data processing, and carry out the ICS evaluation with a limited amount of data. The developed model allows us to move from a qualitative assessment in the form of an ordered series of alphanumeric combinations, denoting the levels of realized services, to a quantitative assessment in the form of the correlation of the FSPB to the FSPE. Also, the list of the NSCC components was obtained, using the proposed model. There were identified 4 systems, 10 subsystems with Level 1, 34 subsystems with Level 2, and 1036 constituent elements. In addition, the value of the quantitative criteria of the security level was obtained, which is equal to.

In addition, special software that implements the studied model and allows to obtaining of a quantitative value that describes the ratio of the FSPB to the FSPE, using qualitative indicators (security services) was developed. In follow-up studies, it is planned to use a model to calculate quantitative criteria for assessing ICS security in other critical infrastructure industries (energy, transport, etc.) [22].

References

[1] On the Main Principles of Ensuring Cyber Security of Ukraine: officer. text, Kyiv: Bulletin of the Verkhovna Rada of Ukraine, No. 45, Art. 403 (2017).

[2] S. Gnatyuk, et al., The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems, in: Intelligent Information Technologies and Systems of Information Security, vol. 3156 (2022) 390–399.

[3] S. Gnatyuk, et al., Critical Aviation Information Systems: Identification and Protection, Cases on Modern Computer Systems in Aviation (2019) 423–448.

[4] Decree of the President of Ukraine No. 96/2016 "On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine".

[5] About Critical Infrastructure: officer. text, Kyiv: Bulletin of the Verkhovna Rada of Ukraine (2021).

[6] Masterplan Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP - Austrian Program for Critical Infrastructure Protection). URL: https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html

[7] Ley 8/2011, de 28 de Abril, Por La Que Se Establecen Medidas Para La Protección de Las infraestructuras Críticas, Boletín Oficial Del Estado 102 (2011).

[8] Action Plan for the Protection of Vital Societal Functions & Critical Infrastruc- ture/Swedish Civil Contingencies Agency (MSB). Risk & Vulnerability

Reduction Department. Natural Hazards & Critical Infrastructure Section (2014).
[9] Ministerie van Veiligheid en Justitie. Directie Weerbaarheidsverhoging (2015) URL: https://www.nctv.nl/actueel/nieuws/kabinet-versterkt-crisisbehe ersing.aspx?cp=126&cs=59950
[10] Osnovni in Sektorski Kriteriji Kritičnosti za Določanje Kritične Infrastrukture Državnega Pomena v Republiki Sloveniji (2012). URL: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/SklepVlade-potrditev_osnovnih_in_sektorskih_kriterijev_kriticnosti2012.pdf
[11] Law of Ukraine on Critical Infrastructure, 1882-IX, Kyiv: Bulletin of the Verkhovna Rada of Ukraine (2021)
[12] T. Sarkar, et al., Mathematical Principles Related to Modern System Analysis, in Modern Characterization of Electromagnetic Systems and its Associated Metrology, IEEE (2021) 1–20. doi: 10.1002/9781119076230.ch1.
[13] X. Guo, et al., Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method, 8th International Conference on Orange Technology (2020) 1–3. doi: 10.1109/ICOT51877.2020.9468778.
[14] O. Sandoval-Alfaro, R. Quintero-Meza, Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology, Mexican International Conference on Computer Science (2021) 1–8. doi: 10.1109/ENC53357.2021.9534800.
[15] Z. Hu, et al., A Multidimensional Extended Neo-Fuzzy Neuron for Facial Expression Recognition, Int. J. Intell. Syst. Appl. 9(9) (2017) 29–36.
[16] Z. Ma, et al., An Improved Approach for Adversarial Decision Making Under Uncertainty Based on Simultaneous Game, Chinese Control and Decision Conference (CCDC) (2018) 2499–2503, doi: 10.1109/CCDC.2018.8407545.
[17] S. Gnatyuk, V. Sydorenko, M. Aleksander, Unified Data Model for Defining State Critical Information Infrastructure in Civil Aviation, IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (2018) 37–42.
[18] Normative Document of Technical Information Protection 2.5-004-99, Criteria for Assessing the Security of Information in Computer Systems Against Unauthorized Access, State Service of Special Communications and Information Protection of Ukraine (1999).
[19] S. Gnatyuk, et al., Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure, IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology (2020) 757–764.
[20] Software for calculating the criticality factor of information and telecommunication systems, State Intellectual Property Service of Ukraine, Certificate of copyright registration for the work No. 9 (2018).
[21] 5G Security Evaluation Process Investigation, Version 1 (2022). URL: https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf
[22] V. Sydorenko, et al., Experimental FMECA-based Assessing of the Critical Information Infrastructure Importance in Aviation, in: CEUR Workshop Proceedings, vol. 2732 (2020) 136–156.