https://www.sworldjournal.com/index.php/swj/article/view/swj18-01-045
DOI: 10.30888/2663-5712.2023-18-01-045

UDC 355.58.0001:351.862.001

GENERAL APPROACHES TO THE ASSESSMENT OF THREATS TO CRITICAL INFRASTRUCTURE USING THE METHOD OF EXPERT ASSESSMENT

Valerii Popel
Head of the Department of Scientific and Technical Expertise of the State Research Institute of Cyber Security Technologies, Zaliznyaka 3, Kyiv, Ukraine
ORCID id: 0000-0001-5544-3544
Murasov Rustam Kamilovich
candidate of technical sciences, doctoral student
National University of Defense of Ukraine named after Ivan Chernyakhivskyi, 28 Povitroflotsky prospect, Kyiv, Ukraine
ORCID: 0000-0003-0800-2062
Nazar Zaika
Specialist of the Technical Information Protection Department of the State Research Institute of Cyber Security Technologies, Zaliznyaka 3, Kyiv, Ukraine
ORCID id: 0000-0002-5791-8926
Chumachenko Serhii Mykolayovych
doctor of technical sciences, professor of the department of information technologies, artificial intelligence and cyber security
National University of Food Technologies, 68 Volodymyrska Street, Kyiv, Ukraine
ORCID: 0000-0002-8894-4262
Ihor Oleksandrovych Savchenko
graduate student of the department of information technologies, artificial intelligence and cyber security
National University of Food Technologies, 68 Volodymyrska Street, Kyiv, Ukraine
ORCID: 0000-0002-5798-7104

Abstract: *in the article, the authors analyzed publications on the use of various expert methods for assessing the threats and risks of emergency situations of various nature at critical state infrastructure facilities in the conditions of the armed aggression of the Russian Federation against Ukraine.*

In order to analytically assess threats to critical infrastructure in the modern conditions of the Russian-Ukrainian war, the possibility of using the expert assessment method was considered, and appropriate recommendations and conclusions were made regarding its possibilities and feasibility of application. With the use of the computer software application developed by the authors in the Python program, practical calculations were made with scientifically based conclusions about threats. This software application developed a procedure for prioritizing critical infrastructure objects according to their level of danger, probability and consequences of damage.

Based on the results of the software application, it can be concluded that the application of the expert assessment procedure allows the analysis of threats to critical infrastructure in conditions of a priori uncertainty, the probabilistic nature of warfare and the stochasticity of missile and drone strikes.

The software application allows you to form a prioritized list of possible threats, to carry out the procedure of excluding non-priority threats from consideration in order to optimally distribute the available forces and means to minimize possible negative consequences from emergency situations of natural, man-made and military-man-made origin.

Keywords: *critical infrastructure, threats, missile-drone strikes, expert assessment, Python, assessment procedure, risk minimization, emergencies, civil protection.*

Introduction. In a war, critical infrastructure is a fundamental component of national security. Its failure or significant disruption of functioning will have large-scale destructive consequences of regional or national importance. The enemy has focused its missile and drone attacks precisely on critical infrastructure facilities (CIFs). First of all, it aims to achieve such a destructive level of its strikes in order to create an ecological, technogenic, and humanitarian catastrophe under the conditions of using conventional weapons and limiting the use of nuclear weapons.

Therefore, the problem of assessing threats to critical infrastructure in order to prevent and prevent emergency situations of military and man-made origin, and in the event of their occurrence - to minimize their consequences and to eliminate them promptly, is a relevant issue today.

Methods. To date, there are a number of mathematical approaches for expert assessment of possible threats and risks in the field of critical infrastructure. In the countries of the European Union, a systematic approach based on the assessment of threats and risks using several criteria is being actively implemented [1 - 5].

It is known that the methods of expert evaluations are based on the mobilization of professional experience and intuition of experts. Such methods of threat and risk assessment use the formal theory of decision-making under conditions of uncertainty [3]. In the event of an emergency situation (ES), the central figure and the subject of decision-making is the person making the decision (the person making the decision PMD) [5]. It can be either one person or a group of people who work out a collective solution, usually, the PMD is a manager or a governing body that formulates the problem, plays a decisive role in choosing a solution to the problem, and is responsible for the decision made. At the same time, experts and consultants are responsible for the validity of the recommendations they prepare for PMD. The final decision is always made by the PMD, in accordance with its own system of preferences, and also bears full responsibility for its choice and its consequences [6, 7].

There are several methods of assessing critical infrastructure threats:

1. Expert assessment method: In this method, several experts assess the threats and their probability based on their experience and knowledge.

2. Risk analysis methods: such as loss analysis, probability and impact analysis, Monte Carlo method, etc.

3. Mathematical modeling methods: This method creates a mathematical model that helps in threat assessment and risk analysis.

4. Machine learning techniques: such as artificial intelligence, deep learning, and data-driven machine learning.

The use of mixed methods can also be useful in critical infrastructure threat assessment.

However, in conditions of uncertainty, complexity and heterogeneity of systems (critical infrastructure), it is advisable to use the method of expert assessment. Leading scientific institutions in the field of energy security also widely use this method [1].

The expert assessment method is a threat assessment method where a group of experts uses their knowledge and experience to assess threats.

Advantages:

• Leverage expertise: Experts can more accurately assess threats by leveraging

their experience and expertise.

• Advanced threat assessment: Experts can better assess complex threats that are difficult to assess using automated methods.

• Considering the human factor: specialists take into account the influence of the human factor on threats.

Disadvantages:

• Human error: Experts can make mistakes in threat assessment that can affect the accuracy of the results.

• Lack of objectivity: experts may have a conflict of interest or limited knowledge and experience in this field.

The use of expert threat assessment is currently relevant because:

1. Information for analysis and payments is incomplete, part of it is missing;

2. A certain amount of information is of a qualitative nature;

3. The complexity of the task and limited opportunities do not allow collecting and summarizing all the necessary information;

4. Inadequacy of the mathematical apparatus for analyzing and processing information;

5. Several possible options for neutralizing the threat are not considered due to resource and technical limitations;

6. Factors of a different nature, which cannot be predicted, but which have a significant impact on the safety of critical infrastructure.

Expert assessment of threats to critical infrastructure consists in their prioritization by risk (consequences, cumulative destructive effects) with the determination of the most dangerous and the separation of those that have an insignificant and acceptable destructive effect. The main goal of such prioritization is the optimal use of available forces and means to protect critical infrastructure objects and neutralize the most significant and most likely threats.

Separate threats and cumulative destructive consequences of the implementation of which can be insignificant with a high probability, or significant, but unlikely.

Expert assessment using a qualitative method involves establishing the level of each formulated threat in a way of combining its consequences and the probabilities of their occurrence, defined in terms of significance.

For the purposes of such a study, it is often considered that all constituent parts of the control object, which can be affected by the threat h from the list of identified threats h = 1...k, are maximally vulnerable, that is, in the notation of the formula

$$\sum_{j=1}^{m} V_j L_j = 1, \quad (1)$$

V_j - vulnerability j from the list of vulnerabilities of the control object j = 1…m;

L_j - probability of implementation of the vulnerability j.

The destructive consequence of the implementation of the threat is

$$C_t = \sum_{i=1}^{n} C_i L_i. \quad (2)$$

C_i - negative consequence of the realization of the threat from the set of possible consequences i = 1…n;

L_i - the probability of the occurrence of the consequence and the realization of the threat.

Taking this into account, the prioritization of threats Rt is carried out according to a simplified version, comparing the products of the averaged expert estimates of the total probability Lt and the cumulative destructive consequences Ct of the implementation of each threat from the predetermined list $t = 1 \ldots k$.

$$R_t = L_t C_t. \quad (3)$$

It is appropriate to establish the following definitions of the scale of significance and the gradation of the measurement of significance (in points):

• for general probabilities: "low" (1), "relatively low" (2), "medium" (3), "relatively high" (4), "high" (5);

• for cumulative negative consequences: "minor" (1), "insignificant" (2), "moderate" (3), "significant" (4), "catastrophic" (5).

Similar scales are used in impact matrices (Relative Impact) for risk assessment (National Risk Assessment) in EU member states [2]. Separate attention is paid to threats for which the maximum spread of expert assessments of consequences and/or probabilities (controversial) is recorded. In such cases, the wording of the threat and/or its description needs clarification and/or additional clarification by the coordinator (moderator).

The threat is removed from the register if the average arithmetical assessment of cumulative negative consequences or total probability exceeds 2 points.

In order to increase objectivity, experts should not have access to information about the evaluations made by other evaluation participants.

An example of prioritization for assessing threats to critical infrastructure is a corresponding list formed by the Delphi method with the involvement of 10 experts.

Prioritization was performed according to the level of threats [3, 4], which was defined as the product of expert assessments of its cumulative negative consequences and the overall probability of implementation. Removal of the threat from the register was carried out if the average arithmetic expert assessment of the consequences of the probability exceeded 2 points.

The assessment of threats to critical infrastructure is given in Table 1.

The results of the assessment of threats to critical infrastructure were formed as a result of the program, which works according to a certain algorithm. First, the limits of the parameters of the examination object are described. After that, input data is generated that comprehensively describes each threat to critical infrastructure. They are entered in the register and represent a description of the threat with a set of expert assessments. The next stage is the removal from the list of the registry, which have insignificant cumulative negative consequences or are unlikely, as well as the prioritization of threats according to their consequences and probability. Based on the generated data, the system forms conclusions that provide an opportunity to adjust expert assessments, that is, dominant judgments are formed and assessments are reduced. The process of adjusting the registry, prioritization, forming conclusions, and adjusting the scores continues until consensus is reached among the threat experts or until the adjustment of the scores stops making changes to the prioritization. After the final decisions are made, the process of announcing the results takes place, which is the completion of the threat assessment by the expert assessment method.

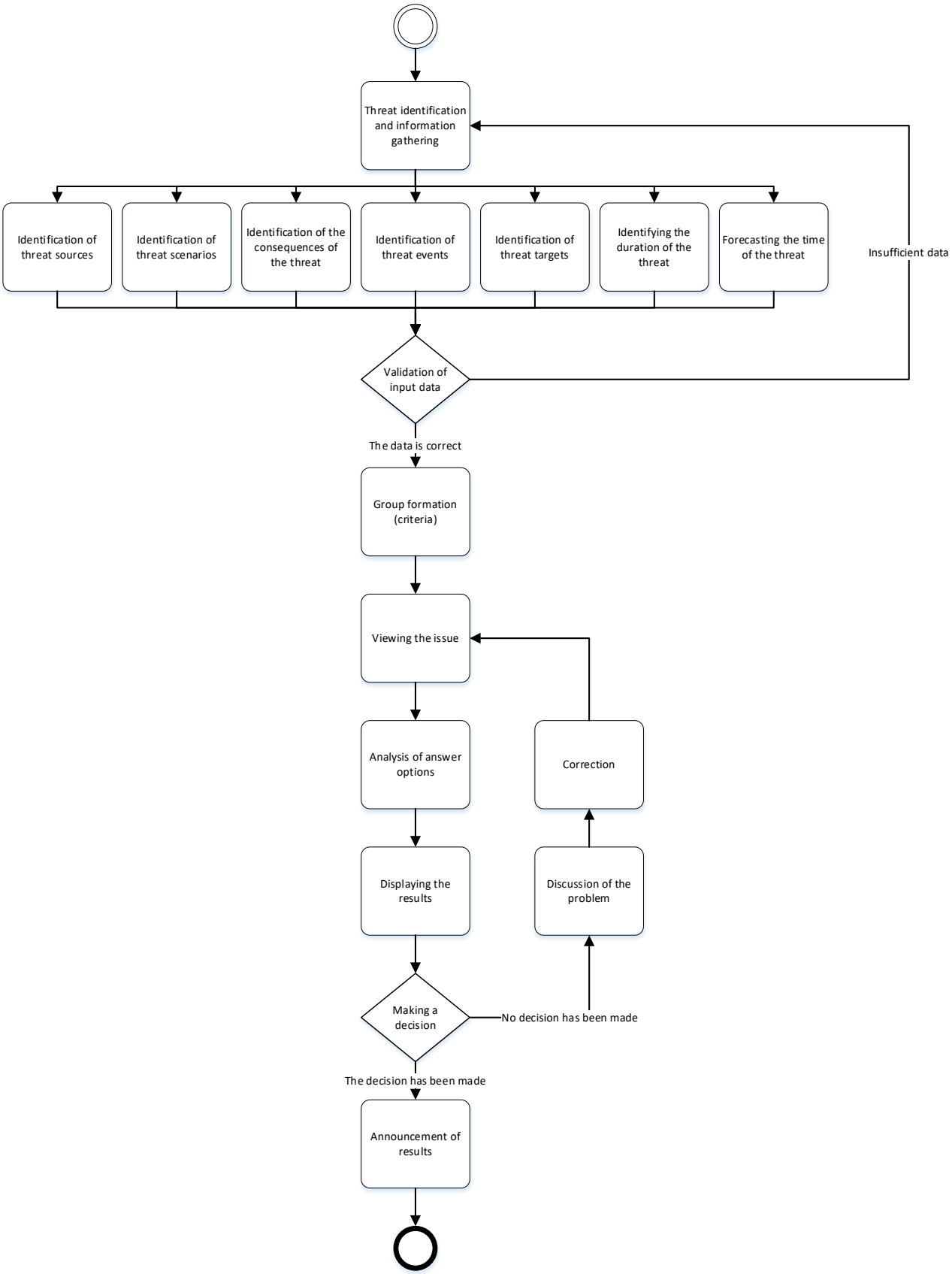

Figure 1. Block diagram of threat detection by the method of expert evaluation

Table 1. Assessment of threats to critical infrastructure

№	*Threat to critical infrastructure*	*level*	*Probability*	*Consequences*
1.	Missile and drone strikes	**20,5**	5	4,1
	Loss of controlled energy consumption	**17,6**	4,4	4
	Cyber attacks	**15**	5	3
	Technical malfunction	**14,35**	4,1	3,5
	Accidents at adjacent facilities	**13,86**	3,3	4,2
	Natural disasters	**13,2**	3	4,4
	Terrorist attacks	**12,3**	3	4,1
	Availability of reservation of critical objects	**12,3**	3	4,1
	Absence of a system of strategic planning and coordination	**12**	3	4
	Insufficient power supply	**10**	4	2,5
	Lack of fuel reserves	**10**	2	5
	Protection of potentially dangerous objects of critical infrastructure	**10**	2	5
13.	Depreciation of fixed assets, increase in accident rate	**9**	3	3
14.	Lack of energy reserves	**9**	2	4,5
	Artificial natural disasters	**8,8**	2,2	4
	Technical overload of objects	**8**	4	2
	Unclear demarcation of powers and responsibilities	**6**	2	3
	Loss of qualified technical personnel	**5**	1	5
	Inability to respond to a crisis	**5**	1	5
20.	Blocking of necessary supplies	**5**	1	5

The results. The results of the assessment of threats to critical infrastructure indicate the following.

None of the pre-formulated threats to energy security received an average arithmetical assessment of cumulative negative consequences or a total probability lower than 2. Therefore, the threats were not removed from the register.

The first five threats include: missile and drone strikes, loss of controlled energy consumption, cyber attacks, technical malfunctions, accidents at adjacent facilities. It is on these threats, according to the obtained results, that it is advisable to concentrate forces and means to prevent their implementation.

Conclusion. The results obtained should not be given undue weight or ascribed accuracy greater than the data and methods used.

Thus, using the method of expert assessments, a practical assessment of threats to critical infrastructure was carried out with prioritization of threats, which will allow to focus efforts on the most dangerous threats and prevent significant losses of critical infrastructure. It is shown that the application of the method of expert evaluations makes it possible to evaluate the threats of complex systems in conditions of uncertainty in order to find optimal solutions for the given categories. This article will be useful for civil protection experts and specialists in the prevention and localization

of emergency situations and the investigation of the causes of emergency situations in critical infrastructure.

Reference

1. Assessment of threats to energy security, analytical report https://doi.org/10.53679/NISS-analytrep.2022.11

2. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf

3. Kachynskyi A. B. Safety, threats and risk [Text] : scientific concepts and mathematical methods / A. B. Kachynskyi. - K.: 2003. - 472 p.

4. Storesund, K., Reitan, N., Schostrom, J., Rod, B., Guay, F., Almeida, R. and Theoharidou, M., New Methodologies for Critical Infrastructure Resilience Analysis, In: ESREL 2018, 17-21 June 2018, Trondheim, Norway, Safety and Security - Secure Societies in a Changing World: Proceedings of ESREL 2018, 17-21 June 2018, Trondheim, Norway, 2018, ISBN 978-0-8153 -8682-7, p. 1221-1229, JRC109960.

5. Modeling the threat of emergency situations at critical infrastructure facilities using the method of system dynamics, No. 3 (2022): Tavriysk scientific bulletin. Series: Technical Sciences, (3), 88-99. https://doi.org/10.32851/tnv-tech.2022.3.10, Murasov R.K., Nevolnichenko A.I., Chumachenko S.M., Mykhaylova A.V., Pyrikov O.V. .

6. Shapovalova O.O. Development of a software application for the implementation of the method of analysis of hierarchies / O.O. Shapovalova, R.V. Burmenskyi // Information processing systems. – 2017. – No. 3(149). - pp. 45-48. https://doi.org/10.30748/soi.2017.149.09.

7. A probabilistic method of forecasting emergency events at potentially dangerous objects of critical infrastructure, NUOU, Kyiv, scientific journal "Modern information technologies in the sphere of security and defense", No. 2(44), 2022, p.60-64-122, Murasov R.K., Kurtseitov T.L., Melnyk Y.V.