JEE Journal of Ecological Engineering

Journal of Ecological Engineering, 2025, 26(7), 286–294
https://doi.org/10.12911/22998993/203529
ISSN 2299–8993, License CC-BY 4.0

Received: 2025.01.12
Accepted: 2025.04.30
Published: 2025.05.15

Implementation of a risk assessment methodology for emergency situations at critical infrastructure objects

Nataliia Kichata[1], Oleg Tretyakov[1], Galyna Kalda[2,3], Mykhaylo Pashechko[4*], Yevgeny Doronin[1], Pavlo Maidan[5]

[1] Department of Civil and Industrial Safety, National Aviation University, 1, Huzara Lubomyra Ave., Kyiv, 03058, Ukraine
[2] Department of Water Supply and Sewage Systems, Rzeszow University of Technology, al. Powstancow Warszawy 12, 35-959, Rzeszow, Poland
[3] Department of Construction and Civil Security, Khmelnytskyi National University, Instytuts'ka St. 11, 29000, Khmelnytskyi, Ukraine
[4] Department of Mathematics and Information Technology, Lublin University of Technology, Nadbystrzycka 38, 20-618, Lublin, Poland
[5] Department of Machines and Apparatus, Electromechanical and Energy Systems, Khmelnytskyi National University, Instytuts'ka St. 11, 29000, Khmelnytskyi, Ukraine
* Corresponding author's e-mail: mpashechko@hotmail.com

ABSTRACT

Ukraine is in a crisis regarding the development of critical infrastructure objects. The main factors contributing to this situation include military actions, systemic underfunding, insufficient maintenance, and infrastructure deterioration. This not only complicates the fulfillment of key socio-economic functions but also poses threats to national security. As a result, there is a need to develop a methodology for assessing the risks of emergencies at critical infrastructure objects. The goal of this study is to develop a methodology for assessing the risks of emergencies at critical infrastructure (CI) objects and to implement it using the example of the Donets water treatment complex. The research results include a developed algorithm for quantitative risk assessment of CI and its elements, enabling the evaluation of all threats and the analysis of potential threat realization scenarios. It has been established that, in many cases, the failure of a single system element significantly affects the ability of other elements and the object as a whole to perform their functions. A new approach has been developed and implemented for identifying and assessing risks in the critical infrastructure sector related to life-support systems, specifically water supply. This approach allows for the identification of potential vulnerabilities of the object to various threats while considering possible cascading effects. The study provides probabilistic estimates of event developments based on predefined scenarios for the Donets water treatment complex.

Keywords: critical infrastructure, risks, threat; emergency situation, water treatment complex.

INTRODUCTION

In the context of the current war and threats to Ukraine's national security, it is important to ensure the resilience of each critical infrastructure object. Timely detection and prevention of threats to these objects are key elements of state policy for their protection. Life support sector is a critical component of infrastructure, encompassing key services and systems necessary to meet the basic needs of the population, such as water supply. The resilience of water supply is determined by the ability of water intake, treatment, and distribution systems to provide a continuous supply of potable water during crises, technological or natural disasters, as well as attacks or other threats. Important factors for resilience include the reliability of equipment, backup capacity, protection against contamination, energy independence of systems, and the ability to quickly recover after incidents. A crucial task is to minimize the risks of outages or failures that could lead to cascading effects, impacting other critical

infrastructure facilities and the normal functioning of other sectors.

In this regard, it is particularly relevant to assess the risks of emergency situations at critical infrastructure objects. The study of aspects related to risk assessment for emergency situations at critical infrastructure objects is extremely important today. Risk assessment is a part of the overall risk management process, which includes risk identification, risk analysis, and risk evaluation [1]. Issues of CI protection are covered in the works of domestic scientists such as Biriukov, Kondratov, Nasvit, and Sukhodolia. These authors analyze the theoretical foundations and experiences in developing the concept of CI protection, as well as identify priorities for forming a CI protection policy and methods for its implementation [2].

In their research, Mardirossian and Ranguelov analyze the theoretical foundations and experience in developing CI protection concepts [3]. Authors [4] identify priorities in security policy formation and methods for its implementation. However, several unresolved issues remain, particularly in risk assessment, the development of comprehensive models for predicting cascading effects, and the creation of effective mechanisms for monitoring and responding to potential threats [5]. One of the reasons for this is the absence of unified standards and methodologies for risk assessment, limited funding for the implementation of modern monitoring and protection technologies, as well as insufficient awareness among personnel regarding the latest approaches to ensuring security.

Many studies examine international experience in protecting critical infrastructure, particularly vulnerability assessment methodologies and strategies for adapting to modern threats. For example, in the study [6,7], the authors analyze the European critical infrastructure risk management system based on the All-Hazards Approach methodology, which considers both natural and technological threats. At the same time, the work [8] focuses on cybersecurity strategies for critical facilities, emphasizing the implementation of early attack detection systems and the development of rapid incident response protocols.

Despite the significant contribution to understanding international approaches to critical infrastructure protection, these studies have several limitations. First, they are primarily oriented toward developed countries with high levels of technological support, making it challenging to adapt their methodologies to resource-constrained countries such as Ukraine. Second, most studies focus on cybersecurity or technological risks, while insufficient attention is given to the integrated analysis of threats, including military actions and cascading effects.

The work [1, 11] presents research results on risks for CI objects, emphasizing the necessity of assessing not only the direct consequences of threats to these objects but also the indirect harm caused to CI. Indirect consequences can include cascading effects, where damage to one CI object leads to disruptions in the functioning of other objects or systems [9, 10, 12–14]. Understanding both direct and indirect impacts helps create more comprehensive and effective strategies to protect facilities and minimize risks. This enables anticipation and preparation for potential issues arising from indirect impacts and reduces the likelihood of underestimated threats that could lead to significant damage.

Therefore, the risk assessment for emergency situations at CI objects includes a comprehensive analysis of potential threats and consequences that may lead to accidents or hazardous events. Special attention should be paid to risk factors as well as the possibility of their cascading impact on other elements of critical infrastructure.

An analysis of modern methodological approaches to infrastructure protection [2] showed that due to the inaccuracy and incompleteness of the information required for precise threat and risk assessment for critical infrastructure, as well as the need to consider numerous interconnections between objects, the universality of criticality assessment can be achieved by using statistical methods and quantitative assessments. However, in addition to assessing individual risks, it is necessary to consider their potential cascading impact on other elements of critical infrastructure.

Thus, an unresolved aspect remains the methodology for quantitative risk assessment at CI objects, which takes into account various current threats, dangers, and risks. The purpose of the study is to implement a risk assessment methodology for hazardous events at the Donets water treatment complex, which affect the safety and resilience of the object. To achieve this aim, the following tasks were defined:

1. To outline the algorithm for quantitative risk assessment for the Donets water treatment complex and its elements.
2. To implement a simulation model for cascading effects at the Donets water treatment complex.

MATERIALS AND METHODS OF THE STUDY

The object of the study is the process of emergency situation occurrence at critical infrastructure objects. The subject of the study is statistical data that allow to assess the risks and threats at the WTC Donets.

The statistical approach to defining the risk of hazardous events for critical infrastructure objects is based on the use of historical data and statistical methods to evaluate the probability of hazardous events and associated risks. This approach enables the quantitative assessment of event probabilities and the determination of risk levels for critical infrastructure objects. The statistical analysis method is employed for the quantitative analysis of cascading effects at critical infrastructure objects.

Construction of an algorithm for quantitative risk assessment for the WTC Donets and its elements

The construction of the algorithm is carried out through the following procedures:

- identification of possible dangerous events in the scenario of situational development, where the components of the scenario may influence the realization of the threat;
- determination of a set of possible event states that affect the level of threat;
- development of threat scenarios, which involves outlining the sequential actions leading to its occurrence through individual elements that form chains of events and transitions to specific states. This is reflected in a structural-logical model of the crisis situation development, which demonstrates various scenario development options at the critical infrastructure facility;
- creation of threat scenarios through a structural-logical model (orgraph) which covers all possible variants of threat realization;
- analysis of probabilities of dangerous events and their transitions between states;
- analysis of the probability of threat scenario realization.

The probability of a potential threat to the CI object and its consequences were determined using a quantitative risk assessment method. The quantitative method provides clear and measurable risk assessments, reducing subjectivity and ensuring the accuracy of the analysis, allows to identify and rank risks by their significance and potential impact, helping to focus efforts on the most critical threats. The algorithm for responding to threats is illustrated in Figure 1.

Research on the implementation of a simulation model for the cascading effects at the WTC «Donets»

The simulation model of cascading effects in critical infrastructure objects is used to study and analyze complex systems, where events or changes in one part of the system affect other parts, creating a chain of interconnected events. The WTC Donets is an important component of critical infrastructure that supplies drinking water to the city of Kharkiv. Its functions include both the delivery and purification of water. The complex consists of a water intake dam, filtration systems, and treatment processes used to process water before it is supplied to the water supply networks for consumers. These components include filtration units designed to remove impurities from raw water, chemical treatment complexes for disinfecting water from bacteria and other microorganisms, storage tanks for treated water, pumping stations that deliver the treated water into the distribution network, facilities for the analysis and control of water quality allow to control water quality according to 126 indicators [15].

The technological chain process of the water treatment complex is as follows:

- water is taken through a water intake bucket using a first-lift pumping station from the Siverskyi Donets River;
- water from the intake well is supplied to four pumps located at the first-lift pumping station;
- water is supplied to the switching chamber, from which it is routed to the treatment facilities;
- water is first chlorinated for its disinfection before entering the system;
- water enters the mixing block, where coagulants (aluminum sulfate) and flocculants (polymer acrylates and silicic acid) are added to it, which leads to the “clumping” of small colloidal or suspended particles, increasing their mass and settling speed;
- then the water is sent for clarification to horizontal sedimentation tanks, which have the shape of rectangular basins;
- after passing through horizontal sedimentation tanks, clarified water is directed to sand filters,

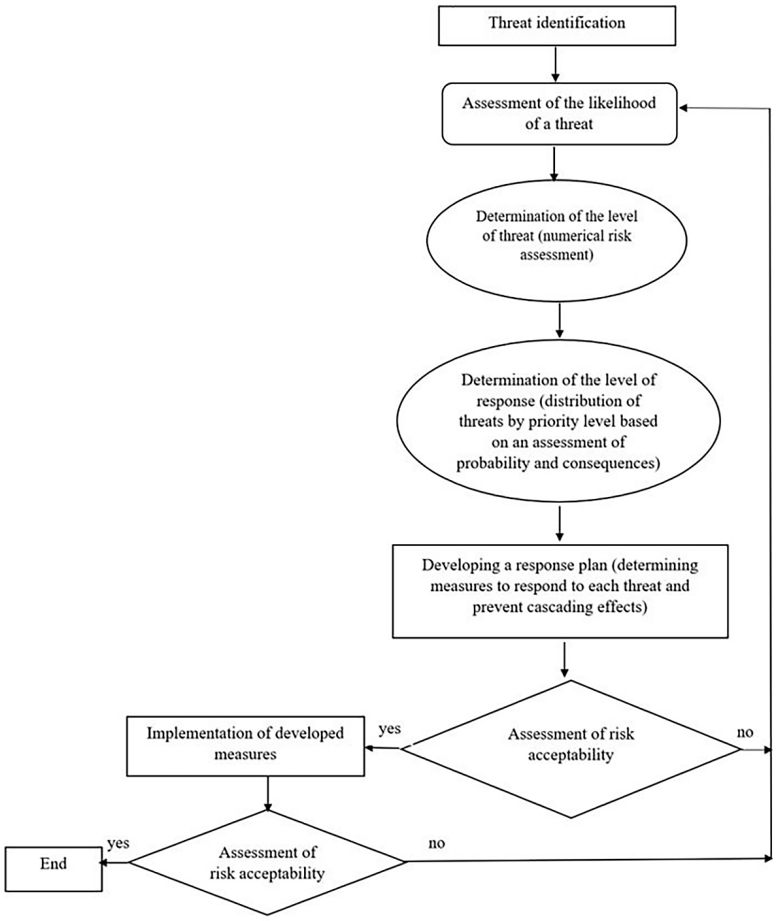

Figure 1. Algorithm for determining response in the event of threat realization

where it flows through the filtering layer from top to bottom;

- after that, the filtered water can be sent to the ozonation unit, which provides both clarification and disinfection;
- disinfection of the water occurs in the clean water reservoir using chlorine dioxide;
- from the clean water reservoir, the treated drinking water is supplied to the city's water supply network using the second-lift pumping station [16].

Thus, the water supply system is a complex network of interconnected structures that interact with each other using water. Changes in water consumption patterns lead to changes in the operation of the entire chain of water supply system structures. First of all, statistical data on all previous dangerous events that took place at the WTC Donets are collected and systematized. This includes data on natural phenomena, technological disasters, cyber incidents, and other incidents (Table 1). Analysis of events in the scenario of the situation's development involves assessing various components that may influence the realization of the threat. Let us denote the set of such elements:

$$I = \{1, 2, \ldots, n\} \quad (1)$$

Based on these events, sets of possible states of situations at the WTC Donets are defined: S_i represents the factor of a dangerous event, and $S_{j,k}$ are the indices that reflect safety or danger states for the critical infrastructure object in the context of a specific event.

The identification of risks at critical infrastructure objects is a continuous process due to the constant changes in the external and internal environment. These changes can lead to the emergence of new risks or modifications of existing ones. The main factors that determine the amount of damage caused include soil pollution, water and air pollution, shock waves from explosions, and thermal effects of a fire. These factors have a destructive impact on people and buildings, not only on the territory of the object, but also outside its boundaries. At the next stage, a structural-logical model of the development of a crisis situation is created, including possible scenarios for

Table 1. Characteristics of dangerous events at the WTC "Donets"

No. event	Description of the corresponding event
1	Natural factors (natural disasters)
1.1	Water erosion near Tetlega village, 6 km north by the Siverskyi Donets River
1.1.1	Waterlogged areas near the water intake bucket
1.1.2	Operation of pumping units becomes more difficult
1.1.3	Increased load from water contamination on the filtration system
1.2	Flood (at the Pechenizke Reservoir), 18 km from the complex, water level rise by 5 meters
1.2.1	Flooding of the water intake bucket
1.2.2	Reducing water supply to the pumping unit
1.2.3	Short circuit of automation devices (frequency converters)
1.3	Drainage of the coastal areas of the Siverskyi Donets River due to a decrease in the groundwater level
1.3.1	decrease in water supply pressure to the first-lift pumping station and reduction in pump productivity
1.3.2	Increased filter wear due to excessive contamination
1.3.3	Increased energy consumption due to extended pump operating
2	Technogenic factors
2.1	Power supply system failure
2.1.1	Pump station shutdown
2.1.2	Water supply to the system stops
2.1.3	Water purification processes disrupted
2.2	Pump failure due to wear
2.2.1	Accumulation of untreated water in the mixer
2.2.2	Stopping technological processes
2.2.3	Suspension of the WTC due to equipment malfunctions
2.3	Chemical accidents (release of harmful chemicals) in the water purification process
2.3.1	Reduction in the efficiency of cleaning processes in the reaction chamber
2.3.2	Filter damage
2.3.3	Getting coagulants, chlorine into a tank with clean water
3	Cyberattacks
3.1	Hacker attack on the complex's automation tools
3.1.1	Changing the parameters of variable frequency drives in pumps
3.1.2	Changing water purification parameters in the reaction chamber
3.1.3	Malfunction of the filters
4	Terrorist Acts
4.1	Attack on infrastructure
4.1.1	Power outage at the first lift pumping station
4.1.2	De-energizing the system's frequency converters
4.1.3	Termination of all water treatment technological processes
4.2	Explosion (proximity to the line of conflict)
4.2.1	Destruction of the pumping station, fire
4.2.2	Release of gas (chlorine) from the water storage tank
4.2.3	Contamination of water in the water supply network due to chemicals leaking from tanks
5	Drone attack (UAV attack)
5.1	Shahed 136 UAV attack
5.1.1	Damage to the pumping station and equipment, explosion, fire
5.1.2	Power outages and damage to electrical networks
5.1.3	Production stoppage due to interruption of work processes

the critical infrastructure object. The model can be represented in the form of a graph, where the nodes reflect different states of the system, and the edges represent transitions between them (Fig. 2).

Figure 2 shows $S=\{S_i\}$ – a set of general hazards for the WTC Donets, which includes various factors, where i denotes the number of factor elements (with S_1 representing natural hazards, S_2 representing technological hazards, S_3 representing cyberattacks, S_4 representing terrorist acts, and S_5 representing drone attacks); $J=\{j\_n\}$ is the set of hazards for each factor, where n is the number of factor elements (such as water erosion, flooding, draining of coastal areas, failure of the power supply system, pump failure, chemical accidents, hacker attacks, attack on infrastructure, explosion, and drone attacks); $K=\{K\_n\}$ is the set of undesirable events in various sections of the water treatment complex.

After creating the crisis situation development model, it is possible to identify all potential threat scenarios for the WTC Donets. For this purpose, a structural-logical model in the form of a orgraph is developed, illustrating the transitions between events through their sequences and interconnections (Fig. 3).

In Figure 3, events are represented as nodes connected by corresponding edges (e_1, e_2, e_n). Each edge e_n shows a possible path or transition between specific states of the system, reflecting the movement from one state to another according to the order of events. For each type of event, parameters influencing its probability are defined, such as the frequency of occurrence, the scale of

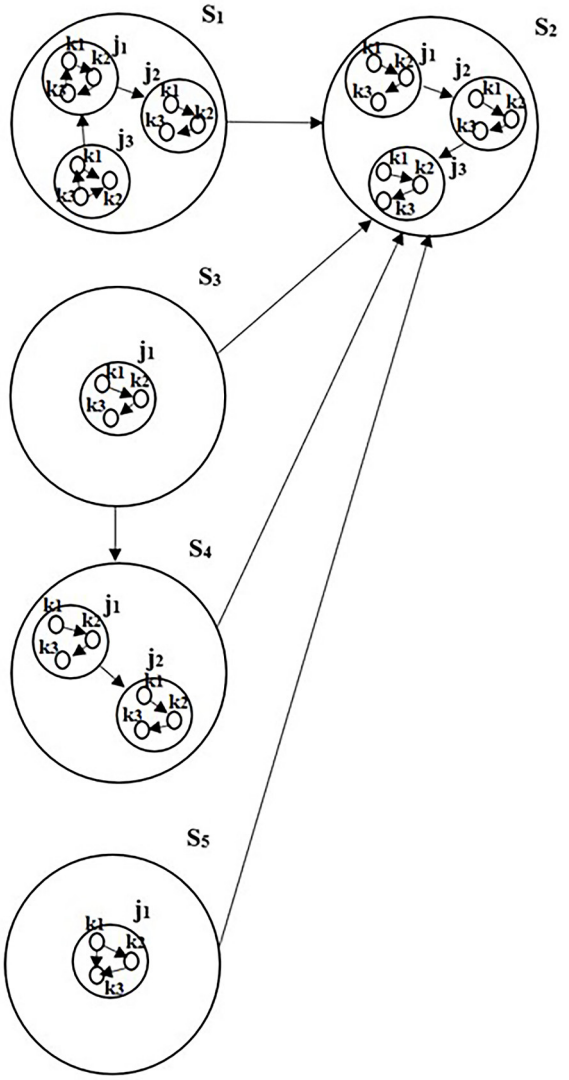

Figure 2. Directed graph (orgraph) of crisis situation development at the WTC Donets due to the impact of hazards

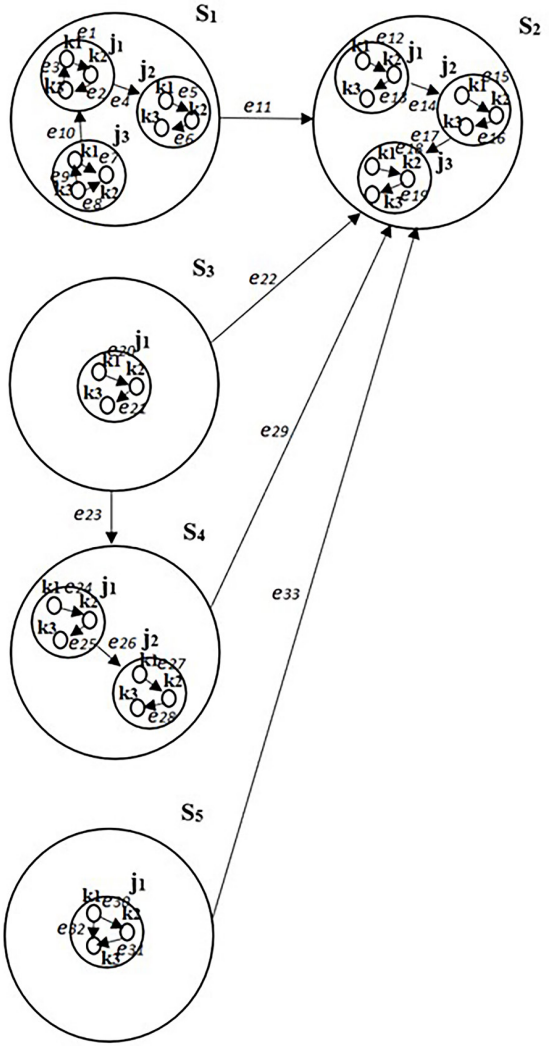

Figure 3. Orgraph of possible scenarios for the development of emergency situations at the WTC Donets with probability assessments of event transitions

consequences, the duration of the event, and the circumstances under which they occurred.

Finding the probability of risk realization for the WTC Donets was based on statistical data. An analysis of the state of the critical infrastructure was conducted over a certain period, taking into account the frequency of emergency situations, the number of recorded incidents during that time, the technical condition of the equipment, and the human factor.

If events can occur simultaneously or independently of each other, combined risks are taken into account, and different threat scenarios at the object are modeled. The scenarios outline the sequence of events and their transitions, allowing for a better understanding of potential threats. The results presented in the form of risk orgraphs, allow to visually assess the probability and consequences of each event at the critical infrastructure object.

The next step is to estimate the probabilities of event states in the threat scenario for the WTC Donets. Suppose that the event state $i \in I$ is described by a discrete random variable x_i. Let $p_i(s)$ be the probability that event i $\in I$ is in state $s \in S_i$, that is:

$$p_i(s) = P\{x_{ijk} = s\},\ s \in S_i \qquad (2)$$

Each edge of the orgraph has a corresponding value P_{jk} where $0 \leq P \leq 1$. Suppose that the values x_i for $i \in I$ are stochastically independent, and the probabilities $p_i(s) = P\{x_{ijk} = s\}$ for $s \in S_i$ are defined based on statistical data. The probabilities of transitions from one event to another are presented in the form of values given in Table 1.

Next, to combine the estimates of the probability of occurrence of dangerous events at the critical infrastructure object, we use a risk matrix that allows us to visualize general risks and determine priorities for the protection of the object (Table 2). The probability of the realization of a hazardous scenario at the critical infrastructure object depends on a number of factors related to several independent events that may occur at the object and their probabilities (P_{ijk}) [17]:

$$P_{scenario} = 1 - \prod(1 - P_{ijk}) \qquad (3)$$

where: $P_{scenario}$ – the probability of realization of the full scenario; P_{ijk} – the probability of occurrence of an individual event i, j, k, that is part of this scenario; $\prod$ – product for all possible combinations of events.

The theorem of total probability is applied when the events are independent, meaning that several mutually exclusive events affect the probability of the main event, while the probabilities of each of these events are known. If the events are sequential and dependent, we use Bayes' formula [17]:

$$P_{scenario} = \frac{P(B|A)\cdot P(A)}{P(B)} \qquad (4)$$

where: $P(B|A)$ – the probability of event B given that event A has already occurred; $P(A)$ – the probability of event A occurring; $P(B)$ – the probability of event B occurring.

Based on the data from Table 2 and using formulas, an assessment of the probability of implementation of threat scenarios for the WTC Donets was conducted, the results are presented in Table 3. Based on the obtained data regarding critical infrastructure objects, the most critical threat scenario for the WTC Donets can be identified, highlighting key events that could trigger cascading effects. The assessment of the probability of

Table 2. Matrix of characteristics of dangerous events at the WTC Donets

$Ps_1j_1k_1k_2$ (e_1)	$Ps_1j_1k_2k_3$ (e_2)	$Ps_1j_1k_3k_1$(e_3)	$Ps_1j_1j_2$ (e_4)	$Ps_1j_2k_1k_2$ (e_5)	$Ps_1j_2k_2k_3$ (e_6)	$Ps_1j_3k_1k_2$ (e_7)
0.4	0.4	0.4	0.5	0.2	0.2	0.2
$Ps_1j_3k_3k_2$ (e_8)	$Ps_1j_3k_3k_1$ (e_9)	$Ps_1j_3j_1$ (e_{10})	Ps_1s_2 (e_{11})	$Ps_2j_1k_1k_2$ (e_{12})	$Ps_2j_1k_2k_3$ (e_{13})	$Ps_2j_1j_2$ (e_{14})
0.2	0.2	0.2	0.5	0.4	0.4	0.4
$Ps_2j_2k_1k_2$ (e_{15})	$Ps_2j_2k_2k_3$ (e_{16})	$Ps_2j_2j_3$ (e_{17})	$Ps_2j_3k_1k_2$ (e_{18})	$Ps_2j_3k_2k_3$ (e_{19})		
0.1	0.1	0.1	0.1	0.2		
$Ps_3j_1k_1k_2$ (e_{20})	$Ps_3j_1k_2k_3$ (e_{21})	Ps_3s_2(e_{22})	Ps_3s_4(e_{23})	$Ps_4j_1k_1k_2$ (e_{24})	$Ps_4j_1k_2k_3$ (e_{25})	$Ps_4j_1j_2$ (e_{26})
0.1	0.1	0.1	0.5	0.9	0.9	0.5
$Ps_4j_2k_1k_2$ (e_{27})	$Ps_4j_2k_2k_3$ (e_{28})	Ps_4s_2(e_{29})				
0.5	0.5	0.7				
$Ps_5j_1k_1k_2$ (e_{30})	$Ps_5j_1k_2k_3$ (e_{31})	$Ps_5j_1k_1k_3$ (e_{32})	Ps_5s_2(e_{33})			
0.9	0.9	0.9	0.9			

Table 3. Results of calculations for evaluating scenarios at the WTC Donets

Threat scenarios	Probability of occurrence
$S_1 \rightarrow S_2$	
P_1	0.017
P_2	0.112
P_3	0.072
$S_3 \rightarrow S_2$	
P_4	0.036
$S_5 \rightarrow S_2$	
P_5	0.278
$S_3 \rightarrow S_4 \rightarrow S_2$	
P_8	0.999

threat scenarios at the WTC Donets (Table 3) indicates that the most likely scenario is $S_3 \rightarrow S_4 \rightarrow S_2$, which begins with a cyberattack and leads to terrorist acts at the water complex, ultimately resulting in explosions and fires. The cascading effect leads to an increase in problems, complicating the response to the crisis situation and increasing the scale of potential consequences.

Reducing the threat from hazards to the object requires a comprehensive approach: creating a monitoring system for early detection of potential hazards; ensuring the physical security of the objects through the implementation of security systems, video surveillance, access control and protective barriers; implementing modern cybersecurity methods, regularly updating software and conducting vulnerability testing; developing and implementing emergency response plans.

The analysis of the research results has shown that a key aspect of risk assessment for emergencies at critical infrastructure objects is identifying the interconnections between threats, integrating various types of risks, evaluating the effectiveness of response measures, and adapting the model to new potential threats.

The proposed methodology allows for the assessment of the impact of different scenarios on the safety of the object using probabilistic event development estimates. It also facilitates the identification of priority response measures and enhances the overall resilience of the object to potential emergencies. The relevance of developing a risk assessment algorithm is confirmed by its ability to identify the most vulnerable elements of infrastructure, thereby helping to prevent incidents at the object. Through the visualization of overall risks for the Donets water treatment complex, it was determined that the most significant threats are cyberattacks and terrorist acts. These threats have the highest likelihood of occurrence and a significant potential impact, making their prioritization essential in the development of risk management measures.

The strengths of the obtained results lie in their practical applicability and the potential for use in improving the security of critical infrastructure objects. The methodology, based on statistical data, ensures its adaptability to different types of objects while considering their specific characteristics. It enables the analysis of the current state of the object and the forecasting of event development under various scenarios, contributing to the prevention of emergencies.

CONCLUSIONS

This study presents a methodology for the quantitative assessment of emergency risks for CI objects based on a threat assessment algorithm. The proposed methodology enables a comprehensive analysis of potential threats to the WTC Donets, considering natural and man-made factors, cyberattacks, terrorist acts, and drone attacks. Unlike existing approaches that often focus on isolated assessments of individual threats, this methodology integrates interactions between different types of threats, allowing for a more accurate evaluation of cascading effects.

Applying this methodology has made it possible to identify the most critical threats to the WTC Donets, analyze their impact on other system elements, and calculate probable scenarios for the development of hazardous events, including forecasting the dynamics of threats while considering interrelated risk factors.

An implemented simulation model for analyzing cascading effects has enabled the assessment of the impact of local failures on the overall functionality of the object. A key advantage of this approach is its ability to model indirect consequences, which were previously overlooked in similar studies. The proposed model not only identifies the most vulnerable system elements but also aids in developing an effective response strategy, thereby reducing the likelihood of emergency situations. A risk assessment algorithm has been developed that accounts for dynamic changes in the external environment and the object's

condition. This ensures flexibility in decision-making and allows safety measures to be adapted to real-time operational conditions.

The obtained results contribute to improving risk management at critical infrastructure objects by enhancing resilience to potential threats, ensuring timely responses to hazards, and minimizing negative consequences. The proposed approach provides more effective protection for personnel and critical assets, significantly impacting national security and infrastructure stability.

REFERENCES

1. Lewis T.G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* John Wiley & Sons, Inc., 474.
2. Biriukov D.S. (2013). *On the Feasibility and Features of the Definition of Critical Infrastructure in Ukraine: Analytical Note*., URL: http://www.niss.gov.ua/articles/1026/
3. Mardirossian G., Ranguelov B., Getsov P., & Zabunov S. (2023). Two innovations for critical infrastructure protection from natural disasters. *Proceedings of the Bulgarian Academy of Sciences. 76*(10), 1554–1561.
4. Argyroudis S., Mitoulis S., Hofer L., Zanini M., Tubaldi E., & Frangopol, D.M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: case study on transport assets. *Science of The Total Environment, 714*.
5. Evans C.W. (2022). Spryyannya Kolektyvniy Oboroni NATO: Bezpeka ta stiykist' krytychnoyi infrastruktury: Posibnyk NATO COE-DAT [NATO collective defense promotion: Security and resilience of critical infrastructure: NATO COE-DAT manual], 469.
6. Yasser A., Kash B., Laura A. (2019). Resilience-driven restoration model for interdependent infrastructure networks. *Reliability Engineering & System Safety. 185*, 12–23.
7. Pawar, C.R.E.W.A., Simon, S.C. (2014). Emergency management and social intelligence. A comprehensive All-Hazards approach. *Taylor&Francis*, *248*.
8. Zhu J., Gao Y. and Mei S. (2019). Neural networks for predictive maintenance of critical infrastructure, in *IEEE Transactions on Industrial Informatics, 15*(4), 2384–2393.
9. Bobro D.H. (2015). Determination of criteria for assessment and threats to critical infrastructure. *Strategic Priorities. Economy. 4*(37), 83–93.
10. Critical Infrastructure Resilience Strategy. Australian Government. URL: http://www.tisn.gov.au.
11. Sukhodolya O.M. (2016). Energy Infrastructure: An Instrumental Dimension of New Generation Wars. O.M. Sukhodolya. Non-military Dimension of New Generation Wars. Energy Component: Materials of the *International Conference*. *Kyiv: NISS, Center for Strategy XXI*, 42–52.
12. Risk Assessment Methodologies for Critical Infrastructure Protection. Part II: A New Approach. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2015, 28.
13. Barbarin Y., Theocharidou M., Rome E. (2014). CIPRNet Deliverable D6.2: Application Scenario. CEA, JRC, Fraunhofer IAIS, Tech. Rep. URL: https://www.ciprnet.eu/
14. Chugai A.V. (2015). Assessment of the impact of gas station operation on the environment. *Bulletin of the KhNADU. 71*, 97–101.
15. Chronicle of the History of Water Supply and Sewage in the City of Kharkiv. Official website of the municipal enterprise Kharkivvodokanal. URL:https://vodokanal.kharkov.ua/content/hronikal_history_water.
16. Sashko V.O., Tereshchenko T.M. (2019). *Water Supply.* Textbook. Kyiv. 114.
17. Sachanyuk-Kavetska N.V. (2008). Elements of probability theory and mathematical statistics. *Study Guide. Vinnytsia: VNTU, part 1, 108*,