Method for Identification of Critical Information Infrastructure Objects of the State

Serhii Toliupa[a], Ivan Parkhomenko[a] and Viktoriia Antoniuk[b]

[a] *Taras Shevchenko National University of Kyiv, 24 Bogdana Gavrylishina Str, 04116, Kyiv, Ukraine*
[b] *National Aviation University, 1 Liubomyra Huzara ave., 03058, Kyiv, Ukraine*

Abstract

The progressive development of information technology in the world has caused an incredible dependence of the population on services provided by various areas of critical infrastructure. Currently, access to these services and their quality is one of the key characteristics of the country's infrastructure, and the smooth operation and protection of these services is considered a necessary and integral part of state protection of developed countries. The increase in methods and resources for protecting different infrastructures has determined the need to rank critical infrastructure. Taking this into account, the paper analyzes the regulatory framework, global approaches to the identification of critical infrastructure objects and developed a method of identifying critical information infrastructure, which will allow the identification of critical objects of a certain industry and determine the degree of their criticality, which systematizes the objects of critical infrastructure and facilitates the choice of means and ways to protect them from threats.

Keywords [1]

critical infrastructure, critical information infrastructure, identification of critical infrastructure objects, method for identification of critical information infrastructure objects, critical objects

1. Introduction

To date, natural and man-made threats, the level of terrorism, the scale and complexity of cyberattacks have increased significantly. And the number of cyberattacks aimed at impressing various areas of critical infrastructure is growing steadily. The most famous cyberattack in Ukraine was Petya, which caused considerable damage to the country's financial infrastructure.

The Situation Center of the Security Service of Ukraine records an increase in the number of cyberattacks aimed at public authorities, critical infrastructure facilities and private sector organizations in Ukraine. For the most part, hacker groups subordinated to the secret services of the Russian Federation became more active. The Security Service of Ukraine neutralized more than 300 cyberattacks and cyber incidents on critical infrastructure during the first half of 2021. Almost 20 hacker groups were involved in these cyberattacks, which were also exposed and neutralized by the secret service. Their purpose was to harm the Ukrainian state bodies and enterprises of the defense-industrial complex. Thus, in April 2021, a cyberattack on the ITS of public authorities was detected, using bait documents on the subject of COVID-19. Downloading these files from the Internet and interacting with them led to the destruction of users' computers and uploading work files to the attackers' servers. These situations have increased the urgency of the problem of critical infrastructure protection, especially information and communication technologies, which are strategically important for the existence and functioning of our state, as well as ensuring the security of the Ukrainian people. In addition, disruption of such facilities can lead to economic and social collapse of the state. In many countries, the concept of critical infrastructure is being implemented, which allows us to focus on systems, networks and

Information technology and implementation (IT&I-2021), December 1–3, 2021, Kyiv, Ukraine
EMAIL: tolupa@i.ua(S. Toliupa); parkh08@ukr.net , parkh08@gmail.com (I. Parkhomenko); vika82134@gmail.com (V. Antoniuk)
ORCID: 0000-0002-1919-9174 (S. Toliupa); 0000-0001-6889-9284 (I. Parkhomenko); 0000-0003-0806-9873 (V. Antoniuk)

individual facilities, the destruction or disruption of which will have serious negative consequences for national security. As world experience shows, the process of formation of the regulatory framework in the field of critical infrastructure protection is quite time-consuming and lengthy. The laws of different countries on the protection of critical infrastructure are often inconsistent, and there are some problems with the mechanisms for classifying facilities as critical infrastructure. Each state determines its critical infrastructure, taking into account its specifics, the criticality of individual sectors and the importance of certain services for society and security of the state. Thus, for each country the concept of "critical infrastructure" has its own meaning and specificity [1].

Therefore, research in the field of detection and protection of critical infrastructure from cyber threats is relevant and necessary. That is why there is a need to develop a critical information infrastructure identification method, which will allow the identification of critical objects of a particular industry and determine the degree of their criticality, which systematizes critical infrastructure and facilitate the choice of means and ways to protect them from threats .

2. Analysis of existing research and approaches

In Ukrainian legislation, the term critical infrastructure (CI) is understood as a set of state infrastructure facilities that are most important for the economy and industry, the functioning of society and public safety and the decommissioning or destruction of which may affect national security and defense, natural environment, lead to significant financial losses and human casualties. Objects of CI are enterprises and institutions (regardless of ownership) of such industries as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, health care, utilities, which are strategically important for the functioning of the economy and security of the state, society and population [2].

CI sectors are are presented in Fig. 1:

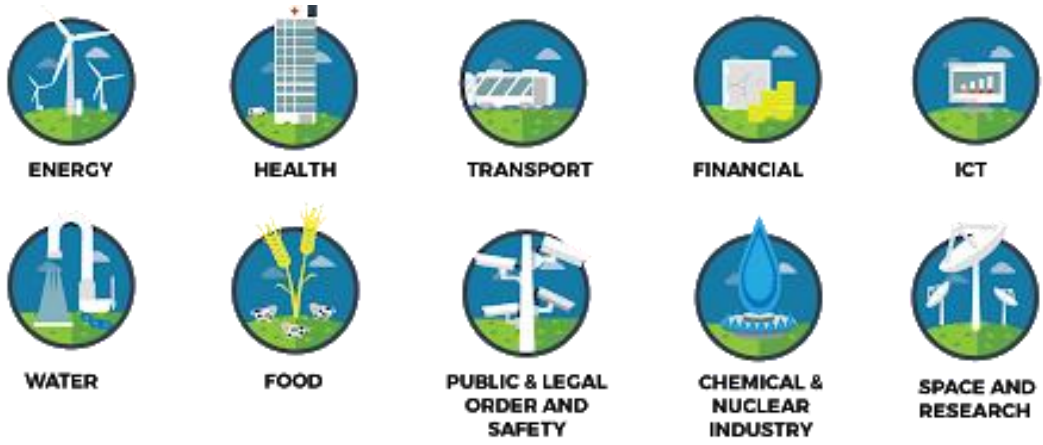

Figure 1. Critical infrastructure sectors

To ensure the protection of the most important critical information infrastructure (CII) objects, it is necessary, first of all, to identify these objects according to certain criteria or critical parameters. In [3] an analytical study of the regulatory framework of developed countries on various variations of key concepts in the field of CII protection (critical infrastructure, CII, critical infrastructure protection, CII).

The United States deserves the most attention from the world experience. An important component of critical infrastructure is its information component - critical information infrastructure, the concept of protection of which, first developed in the United States, was later developed and adapted in most of the world's leading countries. As world practice shows, the process of formation of the regulatory framework in the field of critical infrastructure protection is quite time-consuming and lengthy. Each state determines its critical infrastructure, taking into account the criticality of individual sectors and the importance of certain services for the state's economy and the security of its society. Despite all the differences, there is a common feature of the critical infrastructure of different countries, namely: its undeniable importance for the security of citizens, society and the state [1].

Since Ukraine is joining the European Union, it is impossible not to mention the recommended measures to protect CI, which should be followed by Ukraine:

• develop a national CI protection program;

• ensure a level of health, technological security, socio-economic well-being that would guarantee the "resilience" of the nation to threats;

• unify efforts aimed at protecting CIs by providing a single state body reporting on this issue to coordinate the actions of public authorities responsible for individual industries to which CI facilities belong;

• identify public authorities responsible for CI sectors and relevant private companies;

• create conditions for effective interaction and exchange of information, data and experience between EU member states, government agencies and the private sector;

• to contribute to the creation of a harmonized methodology of risk analysis [1].

Examining scientific publications and analytical materials related to international experience in the formation and implementation of critical infrastructure protection, we can conclude that the organization of activities for critical infrastructure protection in different countries is implemented differently. In some countries, the organizational model is defined and forms a certain structure, and measures - targeted and systemic, and in others it is unsystematic, when activities are carried out informally [1]. The document [4] introduces new concepts of "critical information infrastructure" (CII) and is interpreted as "a set of objects of critical information infrastructure" and "object of critical information infrastructure", which reveals more clearly the previous term, and means communication or technological system of a critical infrastructure object, a cyberattack which will directly affect the sustainable functioning of such a critical infrastructure object ". The document [5] provided a new term "identification of the object of critical information infrastructure", which means "the procedure of assigning the object of information infrastructure to the objects of critical information infrastructure".

As for the Ukrainian legislation, there is currently no complete definition of the term "critical information infrastructure", and as a result, there is no list of objects of this category. It should be noted that in Ukraine the protection of objects, which according to world practice belong to this category, is regulated by numerous regulations, which are mainly internal [1].

With regard to approaches to CII identification, given the work [6-10], today in developed countries there are some methods and models that can provide managers with relevant management opportunities to make informed and correct decisions on the protection of critical infrastructures. A special link for critical objects is the method of their detection. Known approaches include:

• Clausewitz's theory - the meaning of which is to find the "central point" or "central place" of the enemy's system, where its main forces and powers are concentrated. This theory assumes that the objects of study have several mandatory parameters - critical capabilities, critical needs, critical vulnerabilities [6].

• A. Barabashi's theory - The essence of the approach is that each unstructured network under the action of a set of known rules and laws, primarily financial and social, after some time perceives the appropriate structure, without any external influence, organized by a circle of more valuable or important knots. The centers of gravity in this theory are formed for each of the sectors under the influence of the laws of economics, evolution, social development and other rules that allow unstructured networks to become self-organizing [6].

• Graph theory - in the identification of CI objects, graph theory represents CI as an oriented graph. The vertices of this graph are critical objects, and the edges of the graph symbolize the relationships between these objects [7].

• Priority model - According to [6], the essence of this model is to calculate the risk index of the object, which depends on the rating of the object on the scale of the category of factors and the significance of this factor.

• Categorization - to identify dangerous objects, it is necessary to determine the criterion of unacceptable damage - the lower level of damage, after which the object should be classified as dangerous (critical) [8].

• CIMS system - is a simulation system that combines geospatial information and four-dimensional (space-time) effect [9].

• The Athena model is a software tool designed to analyze large complex systems of strategic scale, as well as to identify the interdependence and interrelationships of their elements. This model uses the

methods of Barlow and Warden. The Barlow method determines the horizontal correlation of elements with weights. Warden's method determines the vertical connection of interdependence [6].

• Methodology of assignment critical important objects (CIO) - In the process of identification of objects for the purpose of their assignment to the category of CIO the system of criteria of assignment of objects of the state and non-state property to CIO is used [10].

As we can see, in the modern world there are enough methods of identification of CI objects, but for their further use it is necessary to evaluate them according to the following criteria: (1) clarity of mathematical calculations, (2) independent evaluation, (3) proximity to exact values, (4) universality, (5) the lack of complexity of implementation, (6) taking into account the architecture of systems and networks and (7) the speed of calculations. Comparison of CI object identification methods are shown in table 1.

Table 1

Comparison of CI object identification methods

Methods	Assessment criteria						
	1	2	3	4	5	6	7
Clausewitz's theory	+	-	-	-	-	-	-
Barabashi's theory	+	-	+	-	+	-	-
Graph theory	+	+	+	+	-	-	-
Priority model	-	-	-	-	+	-	-
Categorization	+	-	+	+	-	-	-
CIMS system	+	+	+	+	-	-	+
The Athena model	+	+	+	+	-	-	+
Methodology of assignment to CIO	+	+	+	+	-	-	-

After analyzing the data obtained in the table, we can draw reasoned conclusions that most of the methods considered are difficult to implement and do not take into account the architecture of systems and networks. The most successful approaches are those developed on the basis of graph theory and simulation. Also, some results of A. Barabashi's theory and categorization can be used to study CII objects. With this in mind, the aim of the work is to develop a formalized method of identification of critical information infrastructure of the state, which will assess the level of criticality of the elements of the CII.

3. Description of the developed method of identification of objects of critical information infrastructure

The proposed method of identification of CII objects of the state is implemented in the following 6 stages:

• Stage 1. Selection of research objects.
• Stage 2. Assess the importance of the object on the main indicators.
• Stage 3. Early analysis of the object attribution to the CI.
• Stage 4. Assess the importance of the object on additional indicators.
• Stage 5. Final analysis of the object attribution to the CI.
• Stage 6. Assess the level of criticality.

The input data of the method are: objects of research and actual values of indicators of the first and second levels. Initial data of the method: a complex indicator of the importance of the object, by which a particular object belongs to the CI of the state. Next, we consider in detail each of the stages of the proposed method of identification of CII objects:

Stage 1. Selection of research objects.

This stage consists in identifying the objects that can be attributed to the CI, and their main and additional indicators. The determination of significance coefficients is based on expert procedures of pairwise comparisons: experts make judgments as to how much one indicator exceeds another in terms

of influencing the decision to include the object in the list of CI of the state. To determine the weight of the indicators based on the results of pairwise comparisons, a positive asymmetric matrix is formed:

$$B = \begin{vmatrix} b_{11}=1 & b_{12} & \dots & b_{1k} & \dots & b_{1n} \\ b_{21}=b_{12}^{-1} & b_{22}=1 & \dots & b_{2k} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{i1}=b_{1j}^{-1} & b_{i2}=b_{2j}^{-1} & \dots & b_{ii}=1 & \dots & b_{jn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{n1}=b_{1n}^{-1} & b_{n2}=b_{2n}^{-1} & \dots & b_{nj}=b_{jn}^{-1} & \dots & b_{nn}=1 \end{vmatrix}, \quad (1)$$

For matrix (2.1), the eigenvector (EGV) is found $w_{\mathrm{B}} = \left(b_1, b_2, \dots, b_j', b_n'\right)$, the elements of which are the values of the weights of the indicators indicated above. To quantify the consistency of the judgments of one expert on the differences in indicators, the indicator is used (2.2):

$$O_s = \frac{\lambda_{max}-k}{(k-1)\cdot S_k}, \quad (2)$$

where λ_{max} – the maximum eigenvalue of the matrix B; k – matrix order B; S_k – random index k.

The closer to 0 the value of O_s, the more harmonious are the pairwise comparisons of the expert.

As a result of the expert survey, the relevant coefficients of significance for the main and additional indicators were determined. Significance of indicators in assessing the importance of the object are shown in table 2.

Table 2

Significance of indicators in assessing the importance of the object

№	Indicators	Coefficient of significance, K_i
1	P1 – the cost of annual output of marketable products	0,0841
2	P2 – total number of production staff	0,0933
3	P3 – book value of fixed assets	0,0616
4	P4 – the share of the main products of the object in the products of the same type produced in the country	0,1339
5	P5 – violation of the control of the state or region in an emergency	0,0365
6	P6 – damaging the authority of the state, including in the international arena	0,0126
7	P7 – disclosure of state secrets of confidential scientific, technical and commercial information	0,0126
8	P8 – violation of combat readiness and combat capability of the Armed Forces	0,0342
9	P9 – violation of the stability of the financial or banking systems	0,0182
10	P10 – large-scale destruction of national resources (natural, agricultural, food, production, information)	0,1100
11	P11– territory of infection (pollution) in case of accident at the facility	0,0650
12	P12 – the number of people who may be affected in the event of an accident at the facility	0,1144
13	P13 – violation of life support systems of cities and settlements	0,0611
14	P14 – mass violations of law and order	0,0306
15	P15 – stop of continuous productions	0,0391
16	P16 – accidents and catastrophes on a regional scale as a consequence of an accident at the facility	0,0927
Total		1,000

Also, the actual values of the indicators of the research objects, which are available in the documentation of the research objects, are determined. Table 3 shows an example of filling in the actual values of indicators of research objects

Table 3

Example of filling in the actual values of indicators of research objects

№	Indicators	The actual value of the indicator		
		Object №1	Object №2	Object №3
1	P1	114,6	83,5	34,4
2	P2	3,2	1,2	0,5
3	P3	153,5	118,3	44,1
4	P4	14,1	12,0	4,3
5	P11	100	40	100
6	P12	100	20	100

The values of the coefficient of significance of the main indicators and the actual values of the main indicators of the research objects are transferred to the next stage.

Stage 2. Assess the importance of the object on the main indicators.

This stage is to calculate a comprehensive indicator of the importance of the object on the main indicators. The main indicators are those that can be easily obtained from the documentation available at the site (P1-P4; P11; P12). Let's move on to the step-by-step description of this stage:

- Step 2.1 Defining the boundaries of key indicators.

This step determines the minimum (Min) and maximum (Max) values of each of the indicators, based on the actual values on the object. That is, if there are 3 objects and 3 values, then by comparing these values is finding the smallest and largest of them. Table 4 shows an example of filling the minimum and maximum values.

Table 4

Example of filling with minimum and maximum values

№	Indicators	Minimum value, Min	Maximum value, Max
1	P1	34,4	114,6
2	P2	0,5	3,2
3	P3	44,1	153,5
4	P4	4,3	14,1
5	P11	40	100
6	P12	20	100

- Step 2.2 Determine the contribution of each indicator of the object to the assessment of its importance

In this step, the value of the contributions of each indicator is calculated:

$$Y_{i=1\ldots16} = K_i \cdot \frac{(X_i - Min)}{(Max - Min)}, \quad (3)$$

where K_i – coefficient of significance of the indicator;
X_i – actual value of indicators;
Min and Max – respectively the lowest and highest value of the indicator.

According to these calculations, for each object separately, fill in the table, for example, fill in for the object №1. Tables 5 and 6 provide an example of calculating the importance of an object №1.

- Step 2.3 Determine the assessment of the importance of the object.
  For each object, the amount of contributions is calculated:

$$Y_{gen} = \sum_{i=1}^{16} Y_i, \quad (4)$$

where Y_i – contribution to the assessment of importance.

This amount is an indicator of the importance of the object.

Table 5

Example of calculating the importance of the object №1

№	Indicators	Minimum value, Min	Maximum value, Max	Actual value, X_i	Coefficient of significance, K_i	Contribution to the assessment of importance, Y_i
1	P1	34,4	114,6	114,6	0,0841	0,0841
2	P2	0,5	3,2	3,2	0,0933	0,0933
3	P3	44,1	153,5	153,5	0,0616	0,0616
4	P4	4,3	14,1	14,1	0,1339	0,1339
5	P11	40	100	100	0,0650	0,0650
6	P12	20	100	100	0,1144	0,1144

Table 6

Example of calculating the importance of the object №1 (with an indicator of importance, Y_{gen})

№	Indicators	Minimum value, Min	Maximum value, Max	Actual value, X_i	Coefficient of significance, K_i	Contribution to the assessment of importance, Y_i
1	P1	34,4	114,6	114,6	0,0841	0,0841
2	P2	0,5	3,2	3,2	0,0933	0,0933
…	…				…	
15	P15	-	-	-	0,0391	-
16	P16	-	-	-	0,0927	-
Indicator of the importance of the object, Y_{gen}					1,0000	0,5523

The value of the object's importance indicator is passed to the next step.

Stage 3. Early analysis of object attribution to the CI.

This stage allows to assign the object to the CI ahead of schedule, if the assessment of the importance of the object on the main indicators is more than 0.25, ie the condition is met:

$$Y_{gen} > 0{,}25, \quad (5)$$

where $Y_{заг}$ – indicators of the importance of the object.

Table 7 shows an example of assessing the importance of given objects by key indicators

Table 7

An example of assessing the importance of given objects by key indicators

№	Object name	Comprehensive measure of the importance of an object, Y_{gen}
1	Object №1	0,5523
2	Object №2	0,2769
3	Object №3	0,1794

If this value is less, then the object needs calculations taking into account additional indicators.

Using the example of the table data, we will determine whether the objects are suitable for CII ahead of schedule. It is obvious that two of them belong to the CII ahead of schedule. The values of the coefficient of significance of additional indicators and the actual values of additional indicators of the research objects are transferred to the next stage.

Stage 4. Assess the importance of the object on additional indicators.

This stage consists in calculating a complex indicator of the importance of the object on additional indicators and is implemented in three steps.

- Step 4.1 Determining the actual values of indicators.

  Additional indicators include those that are determined expertly (P5-P10; P13-P16) and are equal to 0 or 1 depending on the expert assessment.

The procedure for determining additional indicators is as follows: the situation is defined as indicators (P5-P10; P13-P16;), which are divided into two groups "no" or "yes": if the emergency at the facility does not lead to the situation, the actual the value of the indicator (X_i) is equal to 0, if the emergency on the object leads to the situation, the actual value (X_i) is equal to 1.

Also, the definition of additional indicators can be represented by an expression:

$$X_i = \begin{cases} 0, if\ P_{5-10,13-16} = "no" \\ 1, if\ P_{5-10,13-16} = "yes" \end{cases}, \quad (6)$$

where X_i – actual value of indicators.

Table 8 shows an example of filling in the actual values of additional indicators of the object №3.

Table 8

Example of filling in the actual values of additional indicators of the object №3

№	Indicator (situation)	Actual value, X_i
1	P5 − violation of the control of the state or region in an emergency	0
2	P6 − damaging the authority of the state, including in the international arena	0
3	P7 − disclosure of state secrets of confidential scientific, technical and commercial information	1
4	P8 − violation of combat readiness and combat capability of the Armed Forces	0
5	P9 − violation of the stability of the financial or banking systems	0
6	P10 − large-scale destruction of national resources (natural, agricultural, food, production, information)	0
7	P13 − violation of life support systems of cities and settlements	0
8	P14 − mass violations of law and order	0
9	P15 − stop of continuous productions	1
10	P16 − accidents and catastrophes on a regional scale as a consequence of an accident at the facility	0

- Step 4.2 Determine the contribution of each indicator of the object to the assessment of its importance. This step is identical to step 2.2 in the second stage: the value of the contributions of each indicator is calculated, but for additional indicators:

$$Y_{i=1\ldots16} = K_i \cdot X_i, \quad (7)$$

where K_i – coefficient of significance of the indicator; X_i – actual value of indicators

- Step 4.3 Determine the assessment of the importance of the object.

  For each object, the sum of the contributions of all indicators, both basic and additional, is calculated, and this amount is a complex indicator of the importance of the object.

  The value of the object's importance indicator is passed to the next stage.

Stage 5. Final analysis of the object attribution to the CI.

At this stage, you can finally determine the affiliation of the object to the CI and the same criteria as in the early analysis: if the assessment of the importance of the object on the main indicators is more

than 0.25, the object belongs to the CI. If this value is less, even after additional calculations, then the object can not be attributed to the CI, which should be protected more. Using the example of the table data, we will determine whether object №3 can be attributed to CII objects after additional calculations. Table 8 shows an example of assessing the importance of specified objects for all indicators.

Table 9

An example of assessing the importance of specified objects for all indicators

№	Object name	Comprehensive measure of the importance of an object, Y_{gen}
1	Object №1	0,5523
2	Object №2	0,2769
3	Object №3	0,2311

Obviously, after additional calculations, the latter object cannot be classified as a CI, which should be strongly protected.

Stage 6. Assess the level of criticality.

At this stage, after the final analysis, it becomes possible to determine the level of criticality of the object of study, which facilitates the choice of methods of protection of the object of CI of the state. Table 10 shows the level of criticality of objects with color gradation.

Table 10

The level of criticality of objects with color gradation

The level of criticality	Criticality conditions	Color gradation
IV-level	$Y_{gen} \geq 0{,}45$	
III- level	$0{,}35 \leq Y_{gen} < 0{,}45$	
II- level	$0{,}25 \leq Y_{gen} < 0{,}35$	
I- level	$Y_{gen} < 0{,}25$	

Criticality levels:

- IV-level – critical objects - facilities of national importance, extensive connections and significant impact on other infrastructure. These facilities are included in the National list of critical infrastructure facilities, requirements are formed to ensure their protection;
- III-level – vital objects, the dysfunction of which will lead to a crisis situation of regional importance. These facilities are included in the National list of critical infrastructure facilities, requirements are formed for the delimitation of tasks and powers of public authorities and critical infrastructure operators, aimed at ensuring their protection and restoration of functioning.;
- II-level – important objects, the priority of protection of which is to ensure rapid recovery of functions through diversification and reserves. Operators are responsible for the stability of the operation of facilities in accordance with the requirements established by law for interaction with public authorities;
- I-level – objects, the direct protection of which is the responsibility of the operator, which must have a plan to respond to the crisis [11].

4. Conclusions

Thus, in the course of the work the analysis of normative-legal documents in the field of CI of different countries of the world, including the legislation of Ukraine was carried out, as a result of which it was established that Ukraine needs:

- Improving the regulatory framework in the field of CI, especially the introduction of the law on critical infrastructure and its protection;
- Creation of a single public authority in the field of CI regulation;

- Organizations of international cooperation and public-private partnership for the exchange of experience and support for the regulation of the field of CI.

Also, an analysis of some existing methods of assigning objects to the CI was conducted, as a result of which it was found that:

- The considered methods are difficult to implement and do not take into account the architecture of systems and networks;
- The sphere of CI requires the creation of a single and formalized method of classifying objects as CI of the state.

In the context of a hybrid war against Ukraine, threats to critical infrastructure have increased significantly, as evidenced by damage to facilities and cyberattacks on energy infrastructure, which have shown the vulnerability of critical infrastructure of the state to new types of threats. Creating an effective system of critical infrastructure protection in Ukraine is an urgent task to be addressed in the framework of the overall reform of the security and defense sector, taking into account the full range of threats and ensuring the interconnectedness of different systems [12].

The result of the work is a developed method of identification of critical information infrastructure of the state, which by assessing the importance of objects by basic and additional indicators, and calculating the level of criticality allows identifying critical infrastructure and determine their degree of criticality. The proposed method of identification of critical information infrastructure objects can be used to study important objects for any branches of critical information infrastructure of the state and determine the degree of their criticality, which allows forming a list of critical infrastructure objects.

5. References

[1] S. Toliupa, I. Parkhomenko and H. Shvedova, "Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level Assesment", 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Jul. 2019.

[2] Resolution of the Cabinet of Ministers of Ukraine Some issues of critical infrastructure № 1109 (2020, October 9). Vidomosti Verkhovnoyi Rady Ukrayiny.

[3] D. Biriukov and S. Kondratov, Critical Infrastructure Protection: Challenges and prospects for implementation in Ukraine. Kyiv: NISS, 2012, 96 p.

[4] Law of Ukraine on the basic principles of cybersecurity in Ukraine № 45 (2017). Vidomosti Verkhovnoyi Rady Ukrayiny.

[5] Resolution of the Cabinet of Ministers of Ukraine Some issues of critical information infrastructure № 943 (2020, October 9). Vidomosti Verkhovnoyi Rady Ukrayiny.

[6] A. Kondratiev, “Modern trends in the study of critical infrastructure in foreign countries”, Foreign Military Review, no. 1, 2012. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranakh_2012/19-1-0-2082

[7] CIS - critical information segments URL: https://habr.com/ru/post/144597/

[8] A.B. Stislavsky Construction of a methodology for ensuring transport security based on categorization: collection of scientific works. Bulletin of the National University of Water Giving and Environmental Protection. Рівне: НУВГП, Part 2. No. 3 (47), 2009. URL: https://www.dissercat.com/content/upravlenie-riskami-narusheniya-bezopasnosti-infrastruktury-transportnogo-kompleksa/read

[9] Gnatyuk S., Sydorenko V., Duksenko O. Modern approaches to critical infrastructure objects detection and identification : Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3 p. 269-275.

[10] V.P. Slomyansky, V.Yu. Glebov, R.N. Galkin On some methodological approaches to the categorization of critical objects. All-Russian Research Institute for Civil Defense and Emergencies EMERCOM of Russia. URL: https://vestnik.igps.ru/wp-content/uploads/V44/15.pdf

[11] Bill of Ukraine on critical infrastructure and its protection (2019). URL: https://ips.ligazakon.net/document/view/jh7yw00a?an=472

[12] Ivanyuta S.P. Threats to critical infrastructure and their impact on national security. Department of Energy and Technogenic Safety.