Viktoriia SYDORENKO[1], Tatiana OKHRIMENKO[2], Yuliia POLISHCHUK[3]

Opiekun naukowy: Sergiy GNATYUK[4]

METODA IDENTYFIKACJI OBIEKTÓW KRYTYCZNEJ INFRASTRUKTURY INFORMACYJNEJ W LOTNICTWIE

Streszczenie: W ostatnich czasach na całym świecie wzrosła liczba różnych sytuacji kryzysowych. Każdego dnia mass media informują o klęskach żywiołowych, katastrofach spowodowanych przez człowieka, konfliktach zbrojnych, aktach terroryzmu, przestępstwach na skalę światową, aktach piractwa popełnionych zarówno przez organizacje przestępcze jak i o pojedynczych przestępstwach. Coraz częściej w wyniku tych wydarzeń wiele osób pada ofiarą, a także stwierdza krytyczne znaczenie systemów oraz zasobów, które mogą zostać uszkodzone. W związku z tym sektor lotnictwa cywilnego wymaga szczególnej uwagi, w którym istnije potrzeba ciągłej komunikacji i wzajemnych połączeń między systemami naziemnymi i lotniczymi. W ten sposób większość światowych liderów uczestniczy w metodach i środkach identyfikacji, systematyzacji i zapewniania bezpieczeństwa krytycznych obiektów infrastruktury. Utrata lub operacyjny rozkład tych obiektów może spowodować znaczące lub nieodwracalne szkody dla bezpieczeństwa narodowego państwa. W związku z tym opracowano metodę identyfikacji obiektów krytycznej infrastruktury informacyjnej, która pozwala określić elementy infrastruktury krytycznej, ich wzajemny wpływ oraz wpływ na funkcjonalne działania krytycznego systemu informacji lotniczej. Ta metoda, a także stworzona na jej podstawie aplikacja, może być wykorzystana do identyfikacji obiektów krytycznej infrastruktury informacyjnej w różnych branżach.

Słowa kluczowe: infrastruktura krytyczna, krytyczna infrastruktura informacyjna, krytyczne systemy informacji lotniczej, identyfikacja obiektów krytycznej infrastruktury informacyjnej, lotnictwo cywilne.

METHOD OF OBJECT IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE IN AVIATION

Summary: in recent times all over the world the number of different emergency situations was increased. Every day mass media informs about natural and man-caused disasters, weapon conflicts, acts of terrorism, global crimes, acts of piracy that were committed by both crime organizations and single offenders. Increasingly frequently as a result of these events many people fall a victim and also state critical importance systems and resources can be damaged. According

[1] PhD, National Aviation University, IT-security Academaic Depatment, v.sydorenko@ukr.net
[2] PhD, National Aviation University, IT-security Academaic Depatment, taniazhm@gmail.com
[3] National Aviation University, IT-security Academaic Depatment, liya7954@gmail.com
[4] DSc, National Aviation University, IT-security Academaic Depatment, s.gnatyuk@nau.edu.ua

that, civil aviation industry requires special attention, just as there is need for continuous communication and interconnection between ground-based and aircrafts systems. By this means most of world leader states have attended to methods and means of identifying, systematization and security assurance for critical infrastructure objects. Loss or operational breakdown of these objects can cause significant or irreparably damage for national security of the state. In view of this, in this work a method of object identification of critical information infrastructure is developed, which gives ability to determine the critical infrastructure elements, their mutual influence and influence on functional operations of the critical aviation information system. This method, as well as a software application developed on its basis, can be used for identification the objects of critical information infrastructure in different industries.

Keywords: critical infrastructure, critical information infrastructure, critical aviation information systems, object identification of critical information infrastructure, civil aviation.

1. Introduction

Present-day trends in information and communication technologies (ICT) have caused phenomenal dependence the society form services which different infrastructure proposed. For now, quality and accessibility of this services are the main points of infrastructure development of the state. According to that, the ensuring their protection and stability are the most essential and mandatory part of State security in developed countries. Increased concentration of facilities and resources for protection the different types of electronic infrastructure had necessitated ranking of infrastructure objects, choosing the most important of them and creating the “critical infrastructure” (CI) definition. Typically, this category relates to energy and transmission line, oil and gas line, seaports, high-speed and government communications channels, life-saving systems of megacities, high-tech enterprises and enterprises of the military-industrial complex, and also the central government authority. The civil aviation (CA), given the need to ensure sustained communication and cooperation between ground-based and aircraft systems, are required special attention. Therefore, identifying the objects which are critical for ensuring the system information continuing operation is the first priority. Nevertheless, an unlimited number of objects and system parameters that constantly varied and unforeseen behavior of objects with lots of interlinkages are the main reason for difficulties with the identified objects of state critical infrastructure. The basic component of critical infrastructure is an informational part – so-called CII (critical information infrastructure). The main reasons for the CII importance are the widespread usage in all areas of human activity of ICT, dependence on them of citizens, society and the state, as well as increasing vulnerabilities and potential threats of different nature. Moreover, in some countries a strong focus on the CI importance for the nation (even the CII definition is critical national information infrastructure). In case of Ukraine, the legislative framework for regulating the protection of CI still in an early development stage, particularly, continuing the process of identifying the objects of state CI in different fields (with no great success, unfortunately). The problematic of CII protection (CIIP) in various fields was exploring by the Ukrainian and foreign scientists such as: H. Alcaraz, D. Biryukov, D. Bobro, D. Gritsalis, O. Dovgan, E. Yeliseyev, A. Kondratiev, M. Merabti, L. Romano, H. Sitarlis, I. Fovino, V. Kharchenko and others. However, the most of researches are not systemic: 1) mostly researches oriented on development and implement preventive and countermeasures for protection particular

CI or CII objects; 2) not enough focus making on the mechanism of formulating the list of state CII, and known approaches (according to the international standards and recommended practices), which are not formalized that make it difficult to use them on the state level, especially in CA. According to that, a development the method of identifying the objects of CII is the actual scientific task that has theoretical and practical values.

2. Existing research analysis and problem statement

Modern society totally depends on ICT, the dysfunction and breakdown of which may lead to chaos, significant financial losses and even mass deaths of people. The truth is, much of mankind inclined to take the most important services (in particular, their quality) as a matter of course until something or someone breaks their work. To determinate and consolidate the most important and vulnerable assets of the state, relatively recently, the term of the CI was introduced into international law. It is known, that establishment of the regulatory framework in the field of CIIP a long process. Most developed countries formulated their own policy (concept) and have developed practical guidelines for the protection CI objects, paying particular attention to the objects of CII (information systems and networks).

The analysis of legislative framework shows the field of CII protection in our State is in an early stage of development. The current legislation still does not define an exhaustive list of the state CII objects, and only the objects of separate fields are specified [1-2], which require protection from the state: enterprises which have important meaning for economics and State security; the most essential power industry objects; especially important objects of the oil and gas industry; important state objects, including points of management of state authorities and local self-government bodies; objects of possible terrorist attacks; objects that are subject for protection and defense in the event of emergencies and during a special period; objects that must be protect by units of the State Protection Service by contracts; objects of high danger (including the list of especially dangerous enterprises, the termination of which requires special measures to prevent damage to life and health of citizens, property, buildings, the environment), objects that are included in the State register of potentially hazardous objects, radiation hazardous objects for which the object design threat is being developed; objects classified as civil defense categories; objects owned by economic entities, the project which is carried out taking into account the requirements of engineering and technical measures of civil protection; the emergency-dispatching system of emergency assistance to the population for the only free emergency call number 112; rescue services; the national system of confidential communication; payment systems; immovable objects of cultural heritage objects.

According to [3] for now, in Ukraine are continuing the development of a proposal about forming the list of ITS objects of state CI. Unfortunately, this list has not been formed in any sector of the CI. Moreover, the lack of clearly defined terminological basis complicated integration our state to the global information space. It is established that in order to protect the most important CII objects, it is necessary to identify these objects according to certain criteria or critical parameters (Fig. 1, block 1).

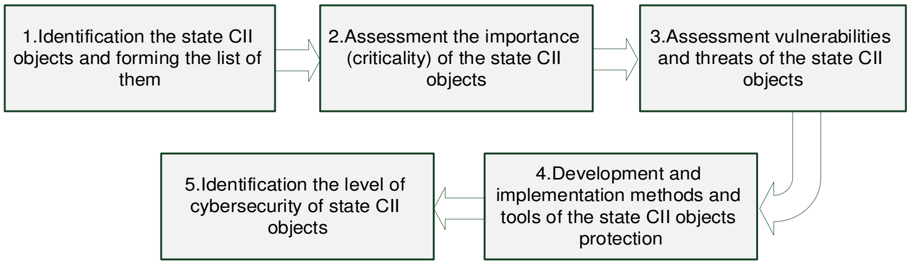

Figure 1. The general scheme of the state CIIP stages

The analysis of criteria by which it is possible to choose or identify the CII objects was conducted in [4]. It was found that one of the firsts criteria for identification of the CI was specified in the EU Directive [5]. Accordingly, each state should identify potential CI that meet the requirements of the two main groups of criteria – intersectoral and sectoral. Intersectoral criteria should include: 1) criteria of losses (estimated from the perspective of the potential number of dead or injured); 2) criteria of economic consequences (assessed in terms of the significance of economic losses and / or degradation of products and services, including potential environmental impacts); 3) criteria of impact on the public (estimated from the point of view of influence on public trust, physical suffering and the violation of everyday life, including the loss of important services). Sectoral criteria should take into account the characteristics of individual sectors of CI. They determine the features or functions of objects included in the CII objects.

In the USA, regarding to [6], adapted to divide the CI into those that related to international organizations (energy, transport, banking and financial system, ICT objects) and those that are not related to them (for example, water supply, rescue services, public administration). In accordance with [4], CI objects are classified according to the categories of impacts in different directions and sectors: economy, finance, environment, health and safety, technological environment, duration of impact. Moreover, the criticality can be described by three general characteristics [7]: critical share, critical time and critical quality.

In Ukraine just one list of criteria exists [8], which can be used for identification CII objects is the List of negative effects that a cyberattack could cause to the ITS, which includes: 1) the emerging the disaster situation of anthropogenic origin and / or negative impact on the ecological protection condition of the state; 2) negative impact on the energy protection condition of the state; 3) negative impact on the energy protection condition of the state; 4) negative impact on the defense capacity, ensuring national protection and national law order condition; 5) negative influence on the state management system condition; 6) negative influence on the socio-political situation in the state; 7) negative influence on the state image; 8) violation of the stable functioning of the state financial system; 9) violation of the sustainable functioning of the state transport infrastructure; 10) violation of the sustainable functioning of the state's ICT infrastructure, including its interaction with the relevant infrastructures of other states.

With regard to the approaches of CII identification, according to [9-10], there are in the developed countries are known a small number of methods and models that can provide managers of the relevant management units with the opportunity to make a reasonable and correct decision on the CI protection. However, the issue of feasibility and effectiveness of the application of these methods for revealing the CII objects is still not explored and open. To find and formulate the universal, clearly formalized approach that will be applied in various fields, in [11] was conducted a multicriteria analysis of approaches to the choosing and identification the CII objects. Each of the approaches to the identification of CII objects in accordance with [11-13].

1. *K. Clausewitz theory for network architectures*. The basic idea of this theory is to find the "central point" (core) of the system, where its key forces and powers are concentrated [9].

2. *The self-organizing networks A. Barabasi theory*. The essence of this theory is any unstructured (Poisson's) network under the influence of a set of well-known rules and laws, primarily of an economic and social nature, after a certain time (after some number of iterations) takes an appropriate structure without any external influence organized around the most valuable or important nodes.

3. *The graphs theory*. The essence of this theory is the CI can be represented as a weighted oriented graph whose vertices are objects, and the edges are the connections between them.

4. *Priority asset model*. The essence of this approach is to calculate the risk index of an object, which depends on the object rating using the scale of the factor category and the significance of this factor [9].

5. *Identification of the CI objects based on categorization.* The essence of this approach is to identify the dangerous infrastructure objects by comparing the value of the integral criterion with the value of "unacceptable damage" $K_{н}$: $K_{інт} = K_{л} + K_{екон} + K_{бал} + K_{екол}$, where $K_{л}$ – the financial loss, determined by the number of dead and injured people, in the case of realization the attack on the objects., $K_{екон}$ – the financial lossas a result of failure the most vulnerable elements of the object,, $K_{бал}$ – the inventory building value (or cost of reconstruction), $K_{екол}$ – the value of the expected environmental damage in the case of a terrorist attack on the object. Accordingly, "unacceptable damage" $(K_{н})$, is the lower level of damage, after which the object should be classified as hazardous [14]. The process of identification ends with creating the list of dangerous objects (for which running the condition $K_{інт} \geq K_{н}$); after that all objects should be categorized.

6. *Simulation.* The simulation that based on software reproduction of the time-wise process of functioning the system becomes a real tool for understanding and the CI full-fledged research. The purpose of simulation in accordance with [15-16] is creating a simulation model of CI objects and to carry out an imitation experiment over them.

6.1.CI modeling system. The Critical Infrastructure Interdependency Modeling System (CIMS) [16] is a discrete events simulation that modeling and imitates infrastructures and interdependences which exists between them at the level relevant to the situation.

The CIMS was developed to study the relationship between infrastructure networks, or rather the variability of system behavior, which manifests itself when one or more nodes in the system are out of order. Moreover, the system provides a highly visual and interactive environment for monitoring cascading effects and impacts on infrastructure.

6.2. "Afina" simulation model. The model – is the software tool that was developed for the big systems analysis (including politic, military, economical and information sectors) as well as for detection the interdependence and interrelated elements [9].

To assess the feasibility and effectiveness of application of analyzed approaches for identify the CII, it is need to analyzed them according to the following basic criteria (Table 1): 1) clarity of formalization (clarity and comprehensibility of mathematical calculations); 2) simplicity of implementation (absence of complicated procedures); 3) flexibility and versatility (the possibility of changing certain parameters as needed and applied in various fields of human activity); 4) accuracy (high degree of approximation of the true value of a particular parameter); 5) efficiency (the ability to correctly and quickly perform calculations); 6) information component (taking into account the features of building IS and networks, cyberspace architecture); 7) objectivity (the possibility of independent evaluation).

Table 1. Analysis of approaches to identify the CII objects

№	The known approach to identification	Core criteria						
		1	2	3	4	5	6	7
1.	K. Clausewitz theory for network architectures	+	-	-	-	-	-	-
2.	The self-organizing networks A. Barabasi theory	+	+	-	+	-	-	-
3.	The graphs theory	+	-	+	+	-	-	+
4.	Priority asset model	-	+	-	-	-	-	-
5.	Identification of the CI objects based on categorization	+	-	+	+	-	-	-
6.1	CI modeling system	+	-	+	+	+	-	+
6.2	"Afina"simulation model	+	-	+	+	+	-	+

In accordance with Table 1 and [11], the multicriteria analysis of these approaches represented that the most successful (in terms of CII application) are approaches based on the graphs theory and the simulations (CI modeling system and "Afina" simulation model), which, like many other approaches, are based on the graphs theory. In addition, the knowledge of the self-organizing networks A. Barabasi theory and the identification of the CI objects based on categorization are widely used. Furthermore, some aspects of these approaches can also be used for the CII objects.

3. Study part

3.1. The proposed method for CII identification

The method of identifying the CII objects in CA was developed, that implemented in the following stage: 1) defining of CII elements; 2) defining the possible factors of influence on the CII elements; 3) identifying the extent of damage and the weight of the factor's influence on the CII elements; 4) defining the functions of influence of CII elements; 5) the graph-analytical mapping of the functional processes of the CII system; 6) assessment of the CII system functioning quality.

Input data: 1) the structural-functional schemes of the analyzed system; 2) the information about the infrastructure elements and their functional operations of the analyzed system; 3) a detailed description of all possible factors and their parameters that may affect on the system functioning.

Output data:1) the set of identified infrastructure elements; 2) the number of influencing factors on the infrastructure element and a description of their parameters; 3) the table of extent of damage of the infrastructure elements for each factor of influence; 4) the scales table of influence of elements of infrastructure for each factor of influence; 5) the elements list of the infrastructure for which the influence ratios are established and the value of the influence function is calculated; 6) the graph of the CII system functional process; 7) the influence matrix of the infrastructure elements on their functional operations and a list of ranked by the order of importance of the CII system infrastructure elements.
Below is described in detail stages of realization the developed method. The procedure of forming the CII elements implemented at the system level (when $l = 2$ in accordance to [17-19] and refers only to elements of the information infrastructure (EII), which fully reflect the structure of the selected detailing level. The method of identifying the CII objects is implemented for a particular system, defined (1) the set $\mathbf{S} = \{\bigcup_{i=1}^{n} S_i\} = \{S_1, S_2, \ldots, S_n\}$, $S_i \subseteq \mathbf{S}$, $(i = \overline{1,n})$ are CII systems, n is the total number of systems.

Stage 1. Defining of CII elements

Step 1.1. Forming the possible CII. For forming the possible CII of the particular system S_i, each expert from $\mathbf{E}$ the set of $\mathbf{E}$ ($\mathbf{E} = \{\bigcup_{j=1}^{N} E_j\} = \{E_1, E_2, \ldots, E_N\}$, $E_j \subseteq \mathbf{E}$ $(j = \overline{1,N})$ are experts in CII field, N is total number of experts), forming all possible EII ($\mathbf{L}^j = \{\bigcup_{k=1}^{h} L_k^j\} = \{L_1^j, L_2^j, \ldots, L_h^j\}$, $L_k^j \subseteq \mathbf{L}^j$ $(k = \overline{1,h})$ are the possible EII which formed by j experts, h is the number of elements which characterize the system S_i). As a result of Step 1.1, the matrix (1) was formed, which shows all possible CII elements of the particular system S_i. The formed EII $\{L_1^j, L_2^j, \ldots, L_h^j\}$ can have the different length, so according to described approach in [20], these elements complemented by an empty element ω_0 so that all the rows of the matrix L have the same length.

$$L = \begin{pmatrix} L_1^1 & L_2^1 & \ldots & L_k^1 & \omega_0 \\ L_1^2 & L_2^2 & \ldots & L_k^2 & \omega_0 \\ & & \ldots & & \\ L_1^N & L_2^N & \ldots & L_k^N & \omega_0 \end{pmatrix} \tag{1}$$

Step 1.2. Identification of unique EII. For identification of unique EII, from obtaining the possible L_k^j, it is necessary to identify the particular set $\mathbf{F}$ ($\mathbf{F} = \{\bigcup_{ai=1}^{e} F_{ai}\} = \{F_1, F_2, \ldots, F_e\}$, $F_{ai} \subseteq \mathbf{F}$ $(ai = \overline{1,e})$ are unique EII, e is the number of unique EII).

Step 1.3. EII coherence. Forming the coherence EII from obtained unique EII F_{ai} is accomplished by establishing the matching of the F_{ai} elements in L the matrix in the form of the matrix $\mathbf{V}$ $(\mathbf{V} = \{\bigcup_{bi=1}^{d} V_{bi}\} = \{V_1, V_2, \ldots, V_d\}$, $V_{bi} \subseteq \mathbf{V}$ $(bi = \overline{1,d})$ is the matching of the F_{ai} elements in the L matrix, d is the number of matching corresponding F_{ai} in matrix L). The matching of EII elements occurs according to the expression: $V_{bi} > \frac{N}{2}$ the obtained values d and their respective EII, are proposed for approval as a coherent set of CII elements: $\mathbf{a} = \{\bigcup_{m=1}^{b} a_m\} = \{a_1, a_2, \ldots, a_b\}$, where $a_m \subseteq \mathbf{a}$ $(m = \overline{1,b})$ are CII elements, which fully reflect the structure of the CII system, b is the total number of these elements.

Step 1.4. Defining the representation graph of identifiable CII elements. The graph-analytical mapping of identifiable EII is presented by unoriented graph (2):

$$\Gamma\left(\{a_m\}, \{p_{mm'}\}\right), \qquad (2)$$

where vertices a_m $(m = \overline{1,b})$ correspond to identified CII elements, and edges $p_{m\,m'}$ are links between elements a_m, where $m = \overline{1,b},\ m' = \overline{1,b},\ m \neq m'$ (see 2).

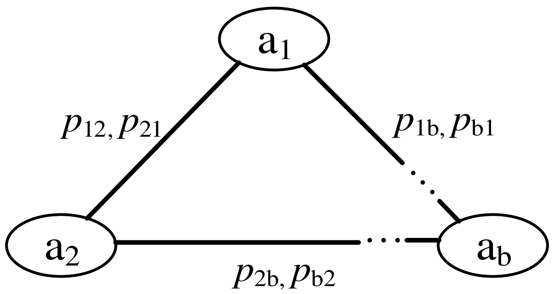

Figure 2.The graph-analytical mapping of identifiable a_m

Stage 2. Defining the possible factors of influence on the CII elements

Step 2.1. Defining the set of influence zone. On this step, forming the set of influence zone $\mathbf{Z}=\{\bigcup_{ci=1}^{v} Z_{ci}\}=\{Z_1,Z_2,\ldots,Z_v\}$, where $Z_{ci}\subseteq\mathbf{Z}$ $(ci=\overline{1,v})$ is influence zone on EII , v is the total number of influence zone, which meets the following condition: in each zone Z_{ci} gets one CII element a_m (a set of zones that are part of the CII territory system can be entered).

Step 2.2. Defining the influence factors on CII elements. For forming the possible influences factors the corresponding set should be introduced $\mathbf{\Phi}=\{\bigcup_{di=1}^{s} \Phi_{di}\}=\{\Phi_1,\Phi_2,\ldots,\Phi_s\}$, where $\Phi_{di}\subseteq\mathbf{\Phi}$ $(di=\overline{1,s})$ is influence factor on EII a_m, s is total number of the influence factors. Each factor of Φ_{di} for particular zone Z_{ci} can be introduced as the set of parameters $\mathbf{O}^{\Phi_{di}}=\{\bigcup_{ei=1}^{z} O_{ei}^{\Phi_{di}}\}=\{O_1^{\Phi_{di}},O_2^{\Phi_{di}},\ldots,O_z^{\Phi_{di}}\}$, where $O_{ei}^{\Phi_{di}}\subseteq\mathbf{O}^{\Phi_{di}}$ $(ei=\overline{1,z})$ are parameters of influence factor Φ_{di} on EII a_m, z is the total number of factors parameter Φ_{di}, that formed on the basis of expert knowledge and can be described by text message or contain the quantitative indicators. As a result of those operations, the set of possible influence factors Φ_{di}, in which each factor is a set of $\Phi_{di}\left(Z_{ci},O_{ei}^{\Phi_{di}}\right)$ is forming.

Stage 3.Identifying the extent of damage and the weight of the factor's influence on the CII elements

For each determined influence factor Φ_{di} and EII element, according to [20], the values of two quantities are fixed $d_{gi}(a_m,\Phi_{di})$ and $\varphi_{gi}(a_m,\Phi_{di})$ – the extent of element a_m damage and the weight of the factor's influence Φ_{di} on EII respectively, where $gi=\overline{1,f}$, $f=b\cdot s$. For assessment the extent of element $d_{gi}(a_m,\Phi_{di})$ damage the linguistic scale used is as follows: *Damage absent* – "0" (EII has not been influenced or influenced insignificantly); *Middle damage* – "1" (the impact on EII caused significant damage to equipment); *Complete failure* – "2" (the impact on EII led to complete destruction). The exact values of linguistic variables *Damage absent*, *Middle damage*, *Complete failure* is established for each CII system individually.

Further, each expert E_j determining $d_{gi}(a_m,\Phi_{di})$ and $\varphi_{gi}(a_m,\Phi_{di})$ for all elements a_m for all factors Φ_{di}. In addition, for any EII a_m must fulfill the condition $\sum_{di=1}^{s}\varphi_{di}(a_m)=1$.

After that, the data is processed from all the experts E_j as an agreed assessment of the extent of element damage $d_{gi}(a_m,\Phi_{di})$ and the weight of influence $\varphi_{gi}(a_m,\Phi_{di})$ on CII elements the values are taken in accordance with (3), where the values of the threshold values t_0,t_1 get the condition $0<t_0<t_1\le 2$ are set in advance and can be reviewed depending on the CII system.

$$d(a_m, \Phi_{di}) = \begin{cases} 0, \text{ if } \frac{1}{N}\sum_{gi=1}^{f} d_{gi}(a_m, \Phi_{di}) < t_0; \\ 1, \text{ if } t_0 \le \frac{1}{N}\sum_{gi=1}^{f} d_{gi}(a_m, \Phi_{di}) < t_1; \\ 2, \text{ if } t_1 \le \frac{1}{N}\sum_{gi=1}^{f} d_{gi}(a_m, \Phi_{di}); \end{cases}$$
$$\varphi(a_m, \Phi_{di}) = \frac{1}{N}\sum_{di=1}^{s} \varphi_{di}(a_m, \Phi_{di}) \quad (3)$$

Stage 4. Defining the functions of the influence of CII elements

Step 4.1. Define the relations of influence between CII elements. At this step, the existence the relations of influence between the CII elements are determined and agreed by the following rule: two CII elements a_m and $a_{m'}$ $(m = \overline{1,b},\ m' = \overline{1,b},\ m \ne m')$ related to the ratio of influence if the damage to the element a_m causes damage to the element $a_{m'}$

Thus, for each possible pair of CII elements $(a_m, a_{m'})$ each expert indicates the value of the ratio of influence r as follows $(r \in [-;+])$: if there is influence, then put "+", if there is no influence – put "-". The following is the processing of the data received from each E_j , where the value $K_{m\,m'}$ is equal to the number of "+" in the line corresponding to the pair $(a_m, a_{m'})$, and the value r_w is agreed score, takes value "+", if in the appropriate line is performed the inequality: $K_{m\,m'} > \beta N$, "-" – if is not performed. The value of the score $0 < \beta < 1$ is pre-determined and can be reviewed depending on the CII system.

Step 4.2.Define functions of mutual influence between CII element pairs.
For defining the value of influence the damage elements on the other CII elements, on the basis of the proposed approach in [20], each expert E_j fixes the value of the function of influence – $h_{m\,m'}(d_{gi})$. Definition of the latter is carried out as follows: for EII pairs $(a_m, a_{m'})$, for which is established in step 4.1 the ratio of influence r_w = "+", it is necessary to specify a value $h_{m\,m'}$ which shows the influence degree on the element $a_{m'}$, if the element is damaged a_m (definition $h_{mm'}$ conducted relative to two levels of influence degree *Middle damage* – "1", and *Complete failure* – "2"). Further, received data from all experts E_j is processed – as an agreed assessment of the function of influence $h_{m\,m'}(d)$ for pair $(a_m, a_{m'})$ values are taken according to (4), where $y = \overline{1,u}$. The limit value τ fulfills the conditions $0 < \tau \le 2$, is pre-determined and can be reviewed depending on the CII system.

$$h_{mm'}(d) = \begin{cases} 1, \text{ if } \frac{1}{N}\sum_{y=1}^{u} h^{y}_{mm'}(d) \le \tau, \\ 2, \text{ if } \tau < \frac{1}{N}\sum_{y=1}^{u} h^{y}_{mm'}(d), \ d = 1,2 \end{cases} \quad (4)$$

Stage 5. The graph-analytical mapping of the functional processes of the CII system

The mapping of the functional processes of the CII system based on the approach described in [20], can be represented by an oriented acyclic graph (5):

$$G\left(\{B_{ii}\} \cup \{A_q\} \cup \{C_{ji}\}, \{P_{qq'}\}\right), \quad (5)$$

where vertices $A_q, (q = \overline{1,x})$ are functional operations performed by one EII a_m (x is total number of functional operation), vertices B_{ii} $(ii = \overline{1,g})$ and C_{ji} $(gi = \overline{1,w})$ are input and output data the system operations resp. (regarding this system, where g is total number of input data, w is the total number of output data), and edges $P_{qq'}$ are connections between operations $A_q, A_{q'}$, where $q = \overline{1,x}, q' = \overline{1,x}, q \ne q'$.

The availability of the oriented edge $P_{qq'}$ in the graph, which comes from the vertices A_q to vertices $A_{q'}$, means that the operation A_q is performed initially and then is performed $A_{q'}$ operation. The edge that comes from B_{ii} to A_q, called input for this system and symbolizes that on the input of the operation A_q received the data that is the result of the operation B_{ii} .In turn, the edge, that comes from A_q to C_{ji}, called output for this system and symbolizes that on the input of the operation C_{ji} received the data that is the result of the operation A_q (see Fig. 3).

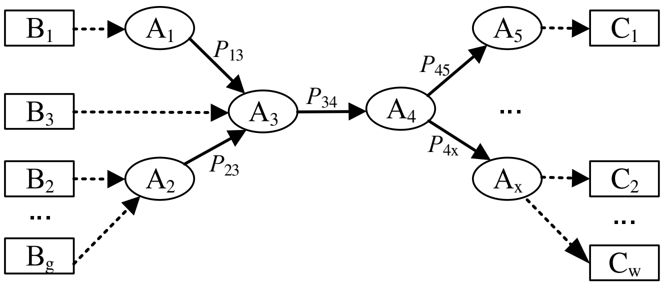

Figure 3.The graph-analytical mapping of the functional processes of the CII system

Such representation allows mapping in a convenient form the formalized description of the functional stages of operations and links between them, as well as the corresponding input and output data.

Stage 6. Assessment of the CII system functioning quality
The result of the influence on EII may be a reduction of the quality of performance the functional operations. To evaluate the quality of execution of functional operations $Q(A_q)$ is introduced in following linguistic scales: *Normal* – "0" (the operation is performed in accordance with the functional rules); *Deviation* – "1" (the operation is carried out, but there are significant deviations from the functional regulation); *Interruption* – "2" (operation is not performed). The influence matrix $Q_d^q(d(a_m))$ shows the execution of a functional operation A_q provided that EII a_m has a corresponding damage $d(a_m)$ and it is formed consistently by each expert E_j for all EII and their respective operations, where is the top index expression Q_d^q corresponds to the number of the operation and the lower index of expression corresponds to the value of the damage $d \in \{0,1,2\}$. Then, data is processed, received from each expert E_j ,as a coordinated assessment of the performance the functional operation, the value is taken in accordance with (6), where the limit value s_0, s_1 fulfills the conditions $0 < s_0 < s_1 \le 2$ (established by the head of the relevant infrastructure and experts pre-determined and can be reviewed depending on the CII system).

$$Q(A_q) = \begin{cases} 0, \text{ if } \frac{1}{N}\sum\limits_{q,d,m} Q_d^q(d(a_m)) < s_0; \\ 1, \text{ if } s_0 \le \frac{1}{N}\sum\limits_{q,d,m} Q_d^q(d(a_m)) < s_1; \\ 2, \text{ if } s_1 \le \frac{1}{N}\sum\limits_{q,d,m} Q_d^q(d(a_m)) \end{cases} \tag{6}$$

Ranging the agreed qualities of the functioning of the CII system by all E_j owing occurs by comparing the quantitative values obtained in the influence matrix. The sum of the quantitative indicators of quality $Q(A_q)$ obtained for one EII a_m, is compared with the sum of the quantitative indicators of quality $Q(A_q)$, obtained for other EII and ranging as follows; $\{VEI_1 > VEI_2 >,...,> VEI_o\}$, where the set of $\mathbf{VEI} = \{\bigcup\limits_{li=1}^{o} VEI_{li}\} = \{VEI_1, VEI_2, ..., VEI_o\}$, $VEI_{li} \subseteq \mathbf{VEI}$, $(li = \overline{1,o})$ is ranked in order of importance for EII system, o is the number in order of ranked EII relative to the sum of quality indicators (it should be noted that the number $o = b$).

3.2. The experimental study for identifying CII objects in CA
For the pilot study of the CII object identification method experiment, a specialized software tool was developed that allows identifying the CII objects in any field and determining their influence on functional operations.
The technology platform provides objects (data and metadata) and objects management mechanisms. Objects (data and metadata) are described as configurations. When automating any activity (software development), it consists of its own configuration of objects, which is a complete application. The configuration

is created in the special operation software mode called "Configurator", and then the operating mode called "1C: Enterprise" is started, in which the user gets access to the basic functions implemented in this application (configuration). The platform itself is not a software product for end users but serves as a foundation for the development and operation of application solutions.

In [24], the pilot study of the EII object identification method in CA was carried out based on the system S_{SNS} are satellite navigation systems, level of system detail $l = 2$, and the adequacy of the method response to change the input data has been proved.

This software implements the following features: entry of input parameters; defining the set of CII identifiable elements; defining the possible factors of influence on the CII element and description of their parameters; creation of tables of extent of damage and the weight of the factor's influence on the CII elements; determination the list of CII element pairs, for which the influence ratios and their calculated values of the influence function are established; allocation of functional stages of operations, connections between them, corresponding input and output data and construction a graph of functional processes; defining the influence matrix of CII elements on their functional operations and selecting the list of ranked by the importance order of the CII elements.

Stage 1. Defining of CII elements

For system S_{SNS} [22], on stage 1, at $N = 3$, the matrix of the possible EII was formed, accordingly (1):

$$L = \begin{pmatrix} L_1^1 & L_2^1 & L_3^1 & L_4^1 & L_5^1 \\ L_1^2 & L_2^2 & L_3^2 & L_4^2 & \omega_0 \\ L_1^3 & L_2^3 & L_3^3 & L_4^3 & L_5^3 \end{pmatrix},$$

where L_1^1 is artificial satellite, L_2^1 is control station, L_3^1 is additional station, L_4^1 is observation station, L_5^1 are receivers; L_1^2 is artificial satellite, L_2^2 is control and observation station, L_3^2 are additional stations, L_4^2 are receivers; L_1^3 is artificial satellite, L_2^3 is control and observation station, L_3^3 are additional stations, L_4^3 are SPS-receivers, L_5^3 are PPS- receivers.

After that a set of unique EIIs is allocated, at $e = 8$, $\mathbf{F}_{\text{SNS}} = \{\bigcup_{ai=1}^{8} F_{ai}\} = \{F_1, F_2, \ldots, F_8\}$, where F_1 is the artificial satellite, F_2 is control station, F_3 is the additional station, F_4 is observation station, F_5 are receivers; F_6 is control and observation station, F_7 are SPS-receivers, F_8 are PPS-receivers.

Then, a set of coincidences, at $N = 3$, $d = 8$, $\mathbf{V}_{\text{SNS}} = \{\bigcup_{bi=1}^{8} V_{bi}\} = \{V_1, V_2, \ldots, V_8\} = \{3,1,3,1,2,2,1,1\}$, and an agreed EII set are allocated: $\mathbf{a}_{\text{SNS}} = \{\bigcup_{m=1}^{4} a_m\} = \{a_1, a_2, ..., a_4\}$, where a_1 is the artificial satellite, a_2 is control and observation station, a_3 is the additional station, a_4 are receivers, accordingly [22-23].

Results of the implementation stage 1 are shown in Fig. 4

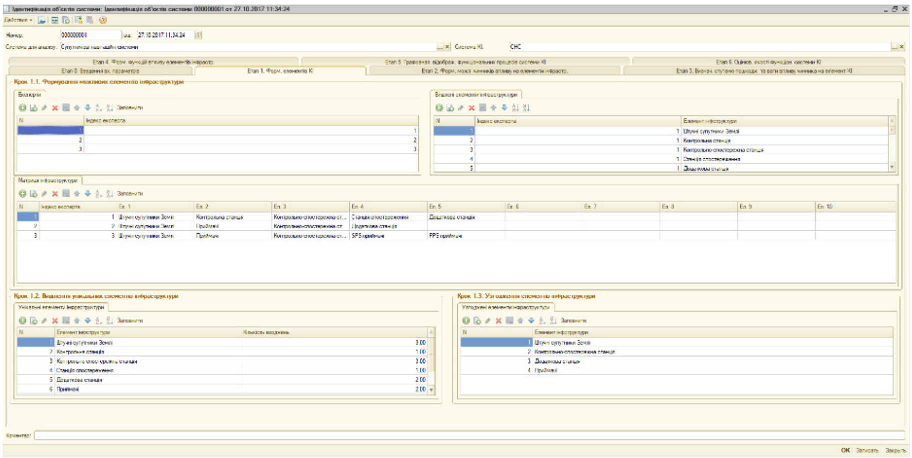

Figure 4.The stages of CII elements defining

For the system S_{SNS}, at $b=4$, accordingly (2), the graph vertices r is a_1 the artificial satellite, a_2 is control and observation station, a_3 is the additional station, a_4 are receivers, and the links between these elements are edges: $p_{12}, p_{21}, p_{13}, p_{31}, p_{14}, p_{41}, p_{23}, p_{32}, p_{24}, p_{42}, p_{34}, p_{43}$ (see Fig. 5).

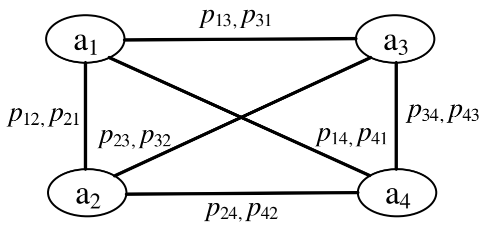

Figure 5.The graph-analytical mapping of CII elements at $b=4$ for S_{SNS}

Stage 2. Defining the possible factors of influence on the CII elements

For system S_{SNS}, at, $b=4$ and $v=2$, accordingly [22], the zone set presented as: $\mathbf{Z}_{SNS} = \{\bigcup_{ci=1}^{2} Z_i\} = \{Z_1, Z_2\}$, where Z_1 is space or orbital zone, Z_2 is ground management and control zone. For S_{SNS}, at, $b=4$ and $s=7$, accordingly [24-25] the set of factors of influences can be presented as: $\mathbf{\Phi}_{SNS} = \{\bigcup_{di=1}^{7} \Phi_{di}\} = \{\Phi_1, \Phi_2, ..., \Phi_7\}$, where Φ_1 is geometric factor (GDOP), which indicates the state of the influence of pseudo-range metrics errors (the last one characterizes the measure of remoteness of the consumer from the GPS-satellite)of hours for accuracy of coordinate calculation; Φ_2 is horizontal factor (HDOP), which shows the influences degree of the accuracy the definition of the horizontal on the calculation of coordinates error; Φ_3 is relative factor (RDOP), dimensionless index describing the effect on the accuracy of determining the coordinates of the pseudo-range error; Φ_4 is time factor (TDOP), is equal to the factor of reduction of the accuracy normalized for the period of 60 s; Φ_5 is vertical factor (VDOP), describes the degree of influence of the accuracy of the hours metrics on the accuracy of coordinates; Φ_6 are situation factors (PDOP), which shows the influence degree of the error in the vertical plane on the determination of coordinates accuracy; Φ_7 is communication factor (CDOP), which shows the value of network connection records according to the NLS-KDD database [26]. Moreover, for factor Φ_7, at $z=5$, the set of parameters of the influence factor represented as: $\mathbf{O}^{\Phi_7}=\{\bigcup_{ei=1}^{5} O_{ei}^{\Phi_7}\}=\{O_1^{\Phi_7},O_2^{\Phi_7},...,O_5^{\Phi_7}\}$, where $O_1^{\Phi_7}$ are basic parameters; $O_2^{\Phi_7}$ are content parameters; $O_3^{\Phi_7}$ are time parameters; $O_4^{\Phi_7}$ are hardware parameters; $O_5^{\Phi_7}$ is presence / absence of attack parameter. After that, the possible sets of parameters $\Phi_7\left(z_1,O_1^{\Phi_7},O_2^{\Phi_7},O_3^{\Phi_7},O_4^{\Phi_7},O_5^{\Phi_7}\right)$; $\Phi_7\left(z_2,O_1^{\Phi_7},O_2^{\Phi_7},O_3^{\Phi_7},O_4^{\Phi_7},O_5^{\Phi_7}\right)$ to form for a factor Φ_7.

Stage 3. Identifying the extent of damage and the weight of the factor's influence on the CII elements

For system S_{SNS} at $b=4$ and $s=7$, accordingly [22, 25], agreed by the experts in accordance with (3) the values of the extent of damage and the weight of the factors are indicated in the Table 3 (the value of limit score $t_0=1$ and $t_1=1{,}5$).

Table 3. An example of damage degree value and influence weight on CII elements

	Φ_1		Φ_2		Φ_3		Φ_4		Φ_5		Φ_6		Φ_7	
	d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4	d_5	φ_5	d_6	φ_6	d_7	φ_7
a_1	1	0,2	1	0,1	0	0,1	1	0,1	1	0,2	0	0	2	0,3
a_2	1	0,2	1	0,2	1	0,2	1	0,2	1	0	1	0	1	0,2
a_3	1	0,1	0	0,1	0	0,1	0	0,1	0	0,1	1	0,1	1	0,4
a_4	1	0,2	0	0,1	0	0,1	0	0,1	0	0,1	0	0,1	1	0,3

Stage 4. Defining the functions of influence of CII elements

For the specified system S_{SNS}, at $b=4$, accordingly [22], the possible EII pairs are formed and the influence between these elements is estimated (the value of score). The processed value presented in Table 4 (the value $\beta=0{,}5$), where, by gray color, are marked pairs, for which established the ratio of influence.

Table 4. The ratio of influence between CII elements

The pair $(a_m, a_{m'})$	**The result**			**The number of "+"** $(K_{m\,m'})$	**The agreed score** (r_w)
	1	**2**	**3**		
(a_1, a_2)	+	+	+	***3***	+
(a_1, a_3)	-	-	+	***1***	-
(a_1, a_4)	+	-	+	***2***	+
(a_2, a_1)	+	+	+	***3***	+
(a_2, a_3)	+	+	+	***3***	+
(a_2, a_4)	+	-	+	***2***	+
(a_3, a_1)	-	-	-	***0***	-
(a_3, a_2)	-	-	-	***0***	-
(a_3, a_4)	+	+	+	***3***	+
(a_4, a_1)	-	+	-	***1***	-
(a_4, a_2)	+	-	-	***1***	-
(a_4, a_3)	+	-	-	***1***	-

For pairs for which, according to (4), established the ratio of influence (Table 4), should be define the value of the function of influence and displayed it's in the Table 5($\tau = 1$).

Table 5. Evaluating the functions of impact

The pair $(a_m, a_{m'})$	**The result**			**The agreed score** $\left(h^y_{mm'}(d)\right)$
	1	2	3	
(a_1, a_2)	$h^1_{12}(1) = 2,$ $h^1_{12}(2) = 2$	$h^2_{12}(1) = 1,$ $h^2_{12}(2) = 2$	$h^3_{12}(1) = 2,$ $h^3_{12}(2) = 2$	$h^y_{12}(1) = 2,$ $h^y_{12}(2) = 2$
(a_1, a_4)	$h^1_{13}(1) = 1,$ $h^1_{13}(2) = 1$	$h^2_{13}(1) = 1,$ $h^2_{13}(2) = 2$	$h^3_{13}(1) = 1,$ $h^3_{13}(2) = 2$	$h^y_{13}(1) = 1,$ $h^y_{13}(2) = 2$
(a_2, a_1)	$h^1_{21}(1) = 0,$ $h^1_{21}(2) = 2$	$h^2_{21}(1) = 1,$ $h^2_{21}(2) = 1$	$h^3_{21}(1) = 0,$ $h^3_{21}(2) = 2$	$h^y_{21}(1) = 1,$ $h^y_{21}(2) = 2$
(a_2, a_3)	$h^1_{23}(1) = 1,$ $h^1_{23}(2) = 1$	$h^2_{23}(1) = 1,$ $h^2_{23}(2) = 1$	$h^3_{23}(1) = 1,$ $h^3_{23}(2) = 1$	$h^y_{23}(1) = 1,$ $h^y_{23}(2) = 1$
(a_2, a_4)	$h^1_{24}(1) = 1,$ $h^1_{24}(2) = 2$	$h^2_{24}(1) = 1,$ $h^2_{24}(2) = 2$	$h^3_{24}(1) = 1,$ $h^3_{24}(2) = 2$	$h^y_{24}(1) = 1,$ $h^y_{24}(2) = 2$
(a_3, a_4)	$h^1_{34}(1) = 1,$ $h^1_{34}(2) = 1$	$h^2_{34}(1) = 1,$ $h^2_{34}(2) = 1$	$h^3_{34}(1) = 1,$ $h^3_{34}(2) = 2$	$h^y_{34}(1) = 1,$ $h^y_{34}(2) = 2$

Stage 5.The graph-analytical mapping of the functional processes of the CII system

For the studied system, accordingly [23], at $x=4$, $g=2$, $w=2$, to display the scheme of the functional process using the graph (5), in which the vertices A_q correspond to functional operations (A_1 is satellite segment, A_2 is control and observation, segment A_3 is additional segment, A_4 is user segment), vertices B_1, B_2, C_1, C_2 are correspond to the input and output data of operations A_q, and edges $P_{12}, P_{14}, P_{21}, P_{23}, P_{24}, P_{34}$ are links between elements $A_q, A_{q'}$ (was installed in step 4.1) (Fig. 6).

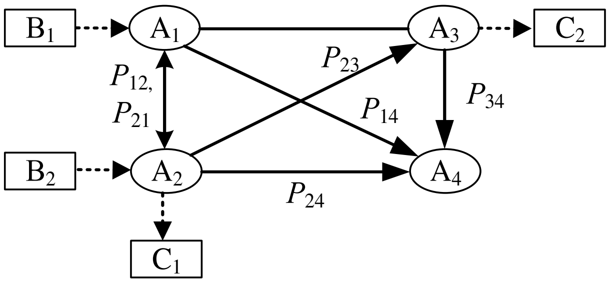

Figure 6. The stage of mapping of the functional processes of the CII system

Stage 6. Assessment of the CII system functioning quality.

For system S_{SNS} accordingly (6), we will construct the agreed influence matrix of all EII on all functional system operations ($q_0 = 0,5, q_1 = 1,5$) will be constructed. Moreover, will form, at $b=o=4$, a set of ranked by the importance order for the EII system: $\mathbf{VEI}_{\mathrm{SNS}} = \{a_1, a_2, a_3, a_4\}$, where a_1 is artificial satellite, a_2 is control-observation station, a_3 is additional station, a_4 are receivers.

Results of the implementation stage 6 are shown in the Table 6.

Table 6. The influence matrix of CII elements on functional operations

Operation (A_q)	**The chart of degrees of elements damage to elements** a_m		
	$d(a_1)=0$	$d(a_1)=1$	$d(a_1)=2$
A_1	*0*	2	2
A_2	*0*	*1*	2
A_3	*0*	*1*	2
A_4	*0*	*1*	*1*
	$d(a_2)=0$	$d(a_2)=1$	$d(a_2)=2$
A_1	*0*	*1*	2
A_2	*0*	2	2
A_3	*0*	*1*	2
A_4	*0*	*1*	*1*
	$d(a_3)=0$	$d(a_3)=1$	$d(a_3)=2$
A_1	*0*	*0*	*1*

A_2	*0*	*0*	*1*
A_3	*0*	*1*	*2*
A_4	*0*	*1*	*2*
	$d(a_4)=0$	$d(a_4)=1$	$d(a_4)=2$
A_1	*0*	*0*	*1*
A_2	*0*	*1*	*1*
A_3	*0*	*0*	*1*
A_4	*0*	*1*	*2*

For assessment the adequacy of proposed method, its response to the change in input data was checked. For the studied system S_{SNS}, the number of EIIs and CII elements of KII are changed, which respectively indicated a change in the output data. Below is a verification of the developed method. Consequently, an experimental study proved the possibility of using the developed method for identifying elements of the CII field, determining the interaction and impact on CAIS functional operations.

4. Conclusion

The analysis of modern approaches to the state CII objects identification was carried out. As a result, it was established that today in Ukraine there is no exhaustive list of CII objects and effective mechanisms for its defining. It is also determined that well-known approaches to the CI objects identification are oriented, as a rule, to economic, environmental, technogenic and other state security domains, and do not take into account the CII characteristics. The analysis allowed to formalize the tasks of scientific research – methods and models development for formalization, identification and cybersecurity ensuring of the CII objects in CA.

The method of identification was developed, which makes it possible to define elements of the CII field, their mutual influence and influence on CAIS functional operations. Also a special software application that can be used to identify the CII elements and determine their impact on functional operations, both in aviation and in other areas of state CI is developed and implemented.

REFERENCE

1. DOVGAN O. (2013). Critical infrastructure as an object of protection against cyberattacks. Information security: the challenges and threats of our time, 17-20.
2. BIRIUKOV D., KONDRATOV S. & SUKHODOLIA O. (2015). Green paper on critical infrastructure protection in Ukraine.
3. BIRIUKOV D. & KONDRATOV S. (2012). Critical infrastructure protection: problems and prospects of implementation in Ukraine: analytical report, 96 p.
4. LYADOVSKA V. (2014). Methods and criteria for the identification of objects of the state's critical infrastructure. Integrated intelligent robotic complexes, 19-20 (May), 356-358.
5. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC.

6. TSIGICHKO V., SMOLYAN G., CHERESHKIN D. (2006). Ensuring the safety of critical infrastructures in the USA, 27.
7. FEKETE A. (2011). Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science, 2(1), 15-24.
8. Resolution on approval of the procedure for the formation of the list of information and telecommunication systems of critical infrastructure objects of the state. Resolution of the Cabinet of Ministers of Ukraine of 23.08.2016, №563.
9. KONDRATIEV A. (2012). Modern trends in the study of critical infrastructure in foreign countries.Foreign Military Review, 1, 19-30.
10. MATTIOLI R., LEVY-BENCHETON C. (2014). Methodologies for the identification of critical information infrastructure assets and services. ENISA Report, 43 p.
11. GNATYUK S., SYDORENKO V., DUKSENKO O. (2015). Modern approaches to critical infrastructure objects detection and identification. Ukrainian Scientific Journal of Information Security, 21 (3), 269-275.
12. GNATYUK S., SYDORENKO V. (2015). An overview of methods for evaluating critically important objects. Problems and prospects for the development of aviation and cosmonautics, 28-29 (October), 110.
13. SYDORENKO V., ALEKSANDER M., NAGI, A. (2016). Modern approaches to the definition and identification of critical information infrastructure. Current issues of cyber security and information security, 24-27 (February), 134-137.
14. STISLAVSKY A. (2009). Building a methodology for ensuring transport security based on categorization. Bulletin of the national university of water management and nature management, v. 2, n. 3(47), 155-165.
15. BRATUSHKA S. (2009).Simulation as a tool to study complex economic systems. Scientific bulletin NLTU Ukraine, 8, 22-28.
16. DUDENHOEFFER D., PERMANN M., MANIC, M. (2006). CIMS: a framework for infrastructure interdependency modeling and analysis. Proceedings of the winter simulation conference WSC 2006, Monterey, California, USA, 478-485.
17. GNATYUK S., SYDORENKO V., SEILOVA N. (2017). Universal data model for the formation of the critical information infrastructure of the state objects list. Ukrainian Scientific Journal of Information Security, 23 (2), 80-91.
18. SYDORENKO V., ZHMURKO T., POLISHCHUK YU., GNATYUK, S. (2017). Data model for forming critical infrastructure objects and determining its connectivity. Inzynier XXI wieku, Monografia, Poland: ATH, 329-350.
19. GNATYUK S., ALEKSANDER M., SYDORENKO V. (2018). Unified data model for defining state critical information infrastructure in civil aviation. The 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT-2018), 24-27 May, 2018, Kyiv, pp. 37- 42.
20. SHERSHAKOV V., TRAHTENGERTS E., KAMAEV, D. (2015). Network-centric methods of computer support for the management of emergency response, LENAND,
21. GNATYUK S., SYDORENKO V., KINZERIAVYI V. (2017). Method of object identification of critical information infrastructure in aviation. Information technology and security, 5 (2), 27- 39.
22. SOLOVIEV,, YU. (2000). Satellite navigation systems, Eco-Trendz, 270 p.
23. GOLUB O., SHEREMET S. (2016). Satellite navigation systems in transport, Electronic text book.

24. SNOVIDOV I. (2015). Factors affecting measurement accuracy, Bulletin of the state hydrography, 1 (48).
25. MAKSIMENKO YU. (2016). Investigation of the parameters of ground and onboard receivers using the GPS system.
26. TAVALLAEE M., BAGHERI E., LU W., GHORBANI A. (2009). A detailed analysis of the KDD CUP 99 data set. Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).