Experimental Identification of the Critical Information Infrastructure Objects in Aviation

Sergiy Gnatyuk[1,2,3] [0000-0003-4992-0564], Viktoriia Sydorenko[1] [0000-0002-5910-0837], Iuliia Goncharenko[4] [0000-0002-5608-4632], Yuliia Sotnichenko[5] [0000-0002-1281-9238], Nurgul Seilova[6] [0000-0003-3827-179X] and Dinara Basshykyzy[3] [0000-0001-8601-3870]

[1] National Aviation University, Kyiv, Ukraine
[2] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
[3] Yessenov University, Aktau, Kazakhstan
[4] European University, Kyiv, Ukraine
[5] Kyiv College of Communication, Kyiv, Ukraine
[6] Satbayev University, Almaty, Kazakhstan
s.gnatyuk@nau.edu.ua, {v.sydorenko, iktkkz}@ukr.net,
dinara.bashykyzy@yu.edu.kz

Abstract. Today there are many various disasters, pandemics, weapon conflicts, acts of terrorism and global crimes. Up-to-date information and communication technologies implementation generates new vulnerabilities, threats and intrusions in cyberspace. Besides, the amount of data is increasing as well as critical data may be at risk. The world leading states have formed their state cybersecurity policy and critical information infrastructure protection principles. One of the main tasks is objects of the critical information infrastructure identification (defining) for state critical infrastructure system forming. The loss or operational breakdown of these objects can cause significant or irreparably damage for national security of the state. In previous work authors have developed a method for objects identification in critical information infrastructure; it gives a possibility to define the critical infrastructure elements, their mutual influence and influence on functional operations of the information systems. This paper presents experimental study of proposed method in aviation using developed specialized software tool. Investigation of satellite navigation system (one of the critical aviation information systems) pointed on the efficiency of developed method.

Keywords: critical information infrastructure protection; critical aviation information system; objects identification; aviation; satellite navigation system; experimental study.

1 Introduction

Modern trends in information and communication technologies (ICT) have caused phenomenal dependence of people in different states form various electronic services. The quality and security of these services are the main indicators of digital development level of the state. Digitalization in every industries and up-to-date ICT implementation generates new vulnerabilities, threats and intrusions in cyberspace. Finansial limitations and infrastructures quantity qrowing had necessitated ranking of infrastructure objects, choosing the most important of them for security ensuring and creating new concept “critical infrastructure” (CI) [1]. Typically, this category relates to energy, oil and gas lines, transportation (air- and seaports, smart cars and trains), communications channels, life-saving systems of megacities, high-technology enterprises and enterprises of the military-industrial complex, central government authority and others. Table 1 shows CII indusries of EU states [2].

Table 1. Industries of CI in accordance to ENISA

Industry / EU state	Energy	Water	Food	Health	Finance	Transport	Public admin.	ICT	Civil admin.	Space&Research
Austria	+	+	+	+	+	+	+	+	+	-
Cyprus	+	+	-	+	+	-	+	+	+	-
Czech Rep.	+	+	+	-	+	+	+	+	+	-
Estonia	+	+	+	+	+	+	+	+	+	-
Finland	+	+	+	+	+	+	+	+	-	-
France	+	+	+	+	+	+	+	+	+	+
Hungary	+	+	+	+	+	+	+	+	-	-
Lithuania	+	+	+	+	+	+	-	+	-	-
Netherlands	+	+	+	-	+	+	-	+	+	-
Poland	+	+	+	+	+	+	-	+	-	-
Slovenia	+	+	+	+	+	+	-	+	-	-
Spain	+	+	+	+	+	+	+	+	+	+
Switzerland	+	+	+	+	+	+	+	+	+	-
UK	+	+	+	+	+	+	-	+	-	-

The aviation industry [3], given the need to ensure sustained communication and strong 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 behaviors of objects with lots of interlink ages are the main reason for difficulties with the identified objects of state CI.

CI contains one value component related to informational part – so-called CII (critical information infrastructure) [4]. 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. In Ukraine, the law framework for regulating the CII protection (CIIP) still in an early development stage, particularly, continuing the process of identifying the objects of state CI in different industries [5].

2 Related Works Analysis and Problem Statement

Up-to-date society totally depends on ICT and their services. The dysfunction and breakdown of these 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. World leading states formed their own cybersecurity policy and have developed principles and practical guidelines for CIIP. The analysis of criteria by which it is possible to choose or identify the CII objects was performed in [6-7]. It was found that one of the firsts criteria for identification of the CI was specified in the EU Directive [8]. In the USA, regarding to [9-10,13], 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 and others).

According to [5] today, in Ukraine are continuing the development of a proposal about forming the list of ICT objects of state CI. Unfortunately, this list has not been formed in any sector of the CI. In Ukraine just one list of criteria exists [11], which can be used for CII objects identification is the List of negative effects that a cyber-attack could cause to the ICT. As it was already noted, the loss or operational breakdown of CII objects can cause significant or irreparably damage for national security of the state. From this viewpoint, CII objects defining and identification is the urgent and important task. In [12] multi-criteria analysis of approaches to the CII objects defining and identification was carried out. This analysis contains various industries and fields. The following methods and models were defined: K. Clausewitz theory for network architectures; A. Barabasi self-organizing networks; graphs theory; priority asset model; identification of the CI objects based on categorization; simulation (critical infrastructure interdependency modeling system; "Afina" simulation model). The analysis has shown 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 A. Barabasi self-organizing networks theory and the identification of the CI objects based on categorization are also widely used.

On this basis, authors in [7,14] have developed a method for objects identification in CII as well as specialized software tool was developed. This method gives a possibility to define the CI elements, their mutual influence and influence on functional operations of the information systems. But this method didn't verificated using real objects of CI. The main task of this work is experimental study of proposed method in aviation using developed specialized software tool.

3 The Main Part of the Study

Mentioned method for CII objects identification, which was previously developed by authors, combines six following stages: defining of CII elements (stage 1); defining the possible factors of influence on the CII elements (stage 2); identifying the extent of damage and the weight of the factor's influence on the CII elements (stage 3); defining the functions of CII elements influence (stage 4); the graph-analytical mapping of the functional processes of the CII system (stage 5); assessment of the CII system functioning quality (stage 6).

Investigation object in aviation is *satellite navigation system* (critical aviation information system [3, 14]) S_{SNS} (level of system detailing $l = 2$). S_{SNS} includes three following sub-systems: artificial satellites of Earth, control-observation stations and GPS-receivers.

Let's analyse mentioned method step-by-step performing for critical aviation information system S_{SNS} using [6-7,12-15]:

Stage 1. Defining of CII elements

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

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

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 matrix forming a set of unique EIIs is allocated, at $e = 8$:

$$\mathbf{F}_{\text{SNS}} = \{\bigcup_{ai=1}^{8} F_{ai}\} = \{F_1, F_2, \dots, F_8\}, \tag{2}$$

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 $N = 3$ and $d = 8$, $\mathbf{V}_{\text{SNS}} = \{\bigcup_{bi=1}^{8} V_{bi}\} = \{V_1, V_2, \dots, V_8\} = \{3,1,3,1,2,2,1,1\}$, and an agreed EII set are allocated:

$$a_{\text{SNS}} = \{\bigcup_{m=1}^{4} a_m\} = \{a_1, a_2, ..., a_4\}, \tag{3}$$

where a_1 is the artificial satellite, a_2 is control and observation station, a_3 is the additional station, a_4 are receivers.

For system S_{SNS}, at $b = 4$, the graph vertices Γ 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. 1).

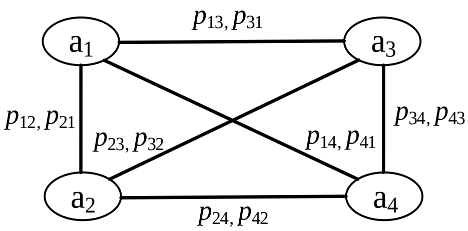


Fig. 1. The graph-analytical mapping of CII elements at $b = 4$ for S_{SNS}

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

For system S_{SNS}, at, $b = 4$ and $v = 2$, the zone set presented as following:

$$\mathbf{Z}_{\text{SNS}} = \{\bigcup_{ci=1}^{2} Z_i\} = \{Z_1, Z_2\}, \tag{4}$$

where Z_1 is space or orbital zone, Z_2 is ground management and control zone.

For S_{SNS}, at, $b = 4$ and $s = 7$, the set of factors of influences can be presented as following:

$$\mathbf{\Phi}_{\text{SNS}} = \{\bigcup_{di=1}^{7} \Phi_{di}\} = \{\Phi_1, \Phi_2, ..., \Phi_7\}, \tag{5}$$

where Φ_1 is geometric factor (GDOP); Φ_2 is horizontal factor (HDOP); Φ_3 is relative factor (RDOP); Φ_4 is time factor (TDOP); Φ_5 is vertical factor (VDOP); Φ_6 are situation factors (PDOP); Φ_7 is communication factor (CDOP), which shows the value of network connection records according to the NLS-KDD database [16].

Moreover, for factor Φ_7, at $z = 5$, the set of parameters of the influence factor represented as follows:

$$\mathbf{O}^{\Phi_7} = \{\bigcup_{ei=1}^{5} O_{ei}^{\Phi_7}\} = \{O_1^{\Phi_7}, O_2^{\Phi_7}, ..., O_5^{\Phi_7}\}, \tag{6}$$

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 .

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 $s=7$ (agreed by the experts), according to [14-15], values of the extent of damage and the weight of the factors are indicated in the Table 2 (the value of limit score $t_0=1$ and $t_1=1,5$).

Table 2. 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 CII elements influence

For the specified system S_{SNS}, at $b=4$, the possible EII pairs are formed and the influence between these elements is estimated (the value of score). The processed value presented in Table 3 (the value $\beta=0,5$), where, by gray color are marked pairs, for which established the ratio of influence.

Table 3. 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***	-

Pairs for which established the ratio of influence between elements (see Table 3), should be define the value of the function of influence and displayed this in the following Table 4 ($\tau = 1$).

Table 4. Evaluating the functions of impact

The pair $(a_m, a_{m'})$	**The result** 1	2	3	**The agreed score** $\left(h^y_{mm'}(d)\right)$
(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, at $x = 4$, $g = 2$, $w = 2$, to display the scheme of the functional process using the graph, 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 $A_q, A_{q'}$ (installed in 4.1) (Fig. 2).

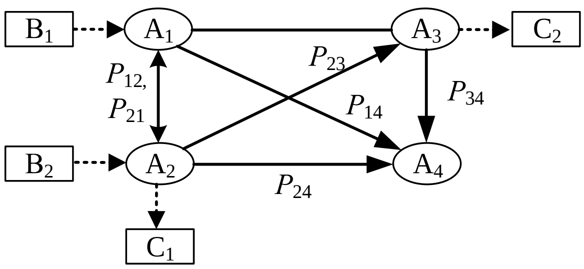


Fig. 2. The stage of mapping of the functional processes of the CII system

Stage 6. Assessment of the CII system functioning quality

For system S_{SNS} we will construct the agreed influence matrix (Table 5) of all EII on all functional system operations ($q_0 = 0,5,\ q_1 = 1,5$). Moreover, will form, at $b = o = 4$, a set of ranked by the importance order for the EII system as following:

$$\mathbf{VEI}_{\text{SNS}} = \{a_1, a_2, a_3, a_4\}\ , \tag{6}$$

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 4.

For assessment the adequacy of studied method in practice, its response to the change in input data must be verified. For the studied system S_{SNS}, the number of EIIs and CII elements of KII are changed (decreasing and increasing), which respectively indicated a change in the output data. It is optimal experimental technique in situation without objective real statistical open data in aviation. This will describe in next section of the work.

Table 5. 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*

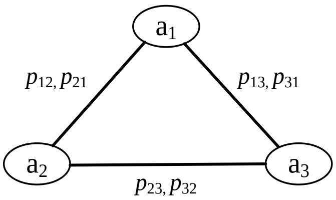
4 Results and Discussion

The verification of the studied method for system S_{SNS}, at $b=3$ and $b=6$, are shown in the Table 6 in accordance to studied method order of stages. Table 5 shows that changes of input data cause output data changing. It means that proposed method works correctly and can be used for objects identifying in aviation and other industries.

Table 6. Results of studied method verification

Result of the experiment 1 ($b=3$)

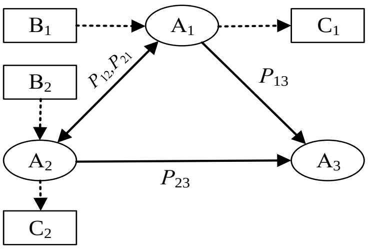
$$\mathbf{a}_{SNS} = \{\bigcup_{i=1}^{3} a_i\} = \{a_1, a_2, a_3\}$$



$$\mathbf{\Phi}_{SNS} = \{\bigcup_{di=1}^{7} \Phi_{di}\} = \{\Phi_1, \Phi_2, ..., \Phi_7\}$$

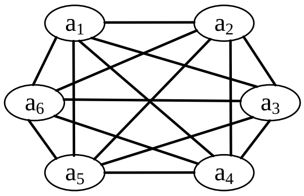
	Φ_1		Φ_2		Φ_3		Φ_4		Φ_5		Φ_6		Φ_7	
	d_1	φ_1	d_2	φ_2	d_3	φ_3	d_4	φ_4	d_5	φ_5	d_6	φ_6	d_7	φ_7
a_1	1	0,2	1	0,1	0	0,1	1	0,1	1	0,2	0	0	2	0,3
a_2	1	0,2	1	0,2	1	0,2	1	0,2	1	0	1	0	1	0,2
a_3	1	0,2	0	0,1	0	0,1	0	0,1	0	0,1	0	0,1	1	0,3

The pair	The result			The agreed score
	1	2	3	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]



Result of the experiment 2 ($b=6$)

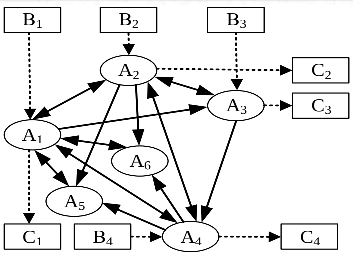
$$\mathbf{a}_{SNS} = \{\bigcup_{i=1}^{6} a_i\} = \{a_1, a_2, ..., a_6\}$$



$$\mathbf{\Phi}_{SNS} = \{\bigcup_{di=1}^{7} \Phi_{di}\} = \{\Phi_1, \Phi_2, ..., \Phi_7\}$$

	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	1	0,2	1	0,2	1	0,2	1	0	1	0	1	0,2
a_5	1	0,1	0	0,1	1	0,1	0	0,1	0	0,2	0	0,1	1	0,3
a_6	1	0,2	0	0,1	0	0,1	0	0,1	0	0,1	0	0,2	1	0,2

The pair	The result			The agreed score
	1	2	3	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]



Operation (A)	The chart of degrees of elements damage to elements a		
	$d(a)=0$	$d(a)=1$	$d(a)=2$
A	0	1	2
A	0	1	2
A	0	1	1
	$d(a)=0$	$d(a)=1$	$d(a)=2$
A	0	1	1
A	0	2	2
A	0	1	2
	$d(a)=0$	$d(a)=1$	$d(a)=2$
A	0	0	1

$$\mathbf{VEI}_{\mathrm{SNS}} = \{a_2, a_1, a_3\}$$

Operation (A)	The chart of degrees of elements damage to elements a		
	$d(a)=0$	$d(a)=1$	$d(a)=2$
A	0	1	2
A	0	1	2
A	0	1	1
A	0	1	2
A	0	1	1
A	0	1	1
	$d(a)=0$	$d(a)=1$	$d(a)=2$
A	0	1	2
A	0	2	2

$$\mathbf{VEI}_{\mathrm{SNS}} = \{a_2, a_4, a_1, a_5, a_6, a_3\}$$

Also specialized software tool was developed (see Figure 3) and this tool implements all features of method stages.

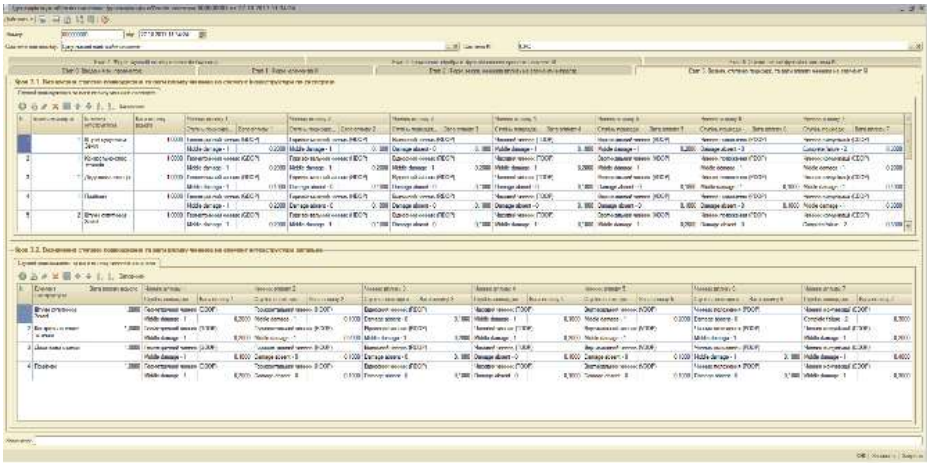


Fig. 3. Fragment of developed specialised software tool

Two additional experiments were carried out using specialised softwsre tool and simulating changeable environment. Given results verified proposed method and approvet its efficiency in aviation.

5 Conclusions and Future Work

This paper presents experimental study of authors` previously proposed method for identification CII objects in aviation using developed specialized software tool. Investigation of satellite navigation system (one of the critical aviation information systems) pointed on the efficiency of studied method for defining the CI elements, their mutual influence and influence on functional operations of the critical aviation information systems. The changing environment of CI functioning approved efficiency of proposed method and possibility of its using in aviation and other industries. Future research studies can be related to developing new flexible tools for accurate identification for various objects as well as CII objects identifying in various industries (energy, medicine, communications and others). After identifying CII objects should be evaluated and ranked by using quantitative metrics.

References

1. Wenger, V. Mauer, M. Cavelty, “International critical information infrastructure protection hand-book 2008-2009”, Center for Security Studies, ETH Zurich, 2009.
2. Critical Information Infrastructures Protection approaches in EU [Online], URL: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf
3. S. Gnatyuk, “Critical Aviation Information Systems Cybersecurity”, Meeting Security Challenges Through Data Analytics and Decision Support, NATO SPS Series, D: Information and Communication Security. – IOS Press Ebooks, vol.47, №3, pp. 308-316, 2016.
4. S. Tyurin, V. Kharchenko, “Redundant Basises for Critical Systems and Infrastructures General Approach and Variants of Implementation”, Proceedings of the 1st Intrenational Workshop on Critical Infrastructures Safety and Security, Kirovograd, Ukraine, May 11–13, 2011, vol. 2. pp. 300-307, 2011.
5. 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.
6. S. Gnatyuk, V. Sydorenko, Yu. Polishchuk and Yu. Sotnichenko, “Determining the Level of Importance for Critical Information Infrastructure Objects”, Proceedings of 2019 Intern. Scientific-Practical Conf. on the Problems of Infocommunications. Science and Technology (PIC S&T 2019), Kyiv, Ukraine, October 08-11, 2019, pp. 829-834, 2019.
7. S. Gnatyuk, V. Sydorenko, M. Aleksander, “Unified data model for defining state critical information infrastructure in civil aviation”, Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 24-27, 2018, pp. 37-42.
8. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC, 2008.
9. Tsigichko V., Smolyan G. and Chereshkin D. “Ensuring the safety of critical infrastructures in the USA”, 27 p., 2006.
10. Fekete, A.: Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science, 2(1), 15-24, 2011.
11. Biriukov D. and Kondratov S. “Critical infrastructure protection: problems and prospects of implementation in Ukraine: analytical report”, 96 p., 2012.

12. S. Gnatyuk, Z. Hu, V. Sydorenko, M. Aleksander, Yu. Polishchuk and Kh. Yubuzova. “Critical Aviation Information Systems: Identification and Protection”, Cases on Modern Computer Systems in Aviation, USA: IGI Global, pp. 423-448, 2019.
13. Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley; 3 edition, 449 p., 2019.
14. Gnatyuk S., Sydorenko V., Polozhentsev A., Fesenko A., Akatayev N., Zhilkishbayeva G., “Method of cybersecurity level determining for the critical information infrastructure of the state”, CEUR Workshop Proceedings, vol. 2616, pp. 332-341, 2020.
15. Syerov Y., Shakhovska N., Fedushko S. Method of the Data Adequacy Determination of Personal Medical Profiles. Proceedings of the International Conference of Artificial Intelligence, Medical Engineering, Education (AIMEE2018). Advances in Artificial Systems for Medicine and Education II. Volume 902, 2019. pp. 333-343. https://doi.org/10.1007/978-3-030-12082-5_31
16. Shershakov, V., Trahtengerts, E. & Kamaev, D.: Network-centric methods of computer support for the management of emergency response. LENAND, 160 p., 2015.
17. NSL-KDD dataset [Online], URL: https://www.unb.ca/cic/datasets/nsl.html