UDC 004.056

SECTORS OF CRITICAL INFORMATIONAL INFRASTRUCTURE

Yurii Dreis, PhD in Eng.,Associate Professor,
Head of the Department of Innovative
Technologies Professional Education,
National Aviation University
y.dreis@nau.edu.ua

Mariia Roshchuk, PhD student,
Department of constitutional and administrative law,
Research institute of law, National Aviation University
roshchkmv@gmail.com

Olga Romanenko, Student,
Insitute of Computerized Information Systems,
Academic Department of Computerized
Information Security Systems, National Aviation University
olya_olek@ukr.net

Summary. *the analysis of absence a list of critical infrastructure sectors is analyzed, taking into account experience the developed countries of the world. The main sectors of critical infrastructure are presented and in view of the fact that in most objects of critical infrastructure there is an information and telecommunication system that is vulnerable to various types of cyberattacks, a list of these sectors is proposed.*

The analysis of native scientific publications [1-3] and current legislation of Ukraine [4-5] was carried out, the problem lack of a list of critical infrastructure (CI) sectors and criteria for their attribution to these sectors was revealed.

The problem of the absence a list sectors of the CI and elements is proposed to be solved by analyzing sectors CI in the majority of countries in the world and, due to international experience [1,2], distinguishing those that exist in Ukraine.

The results of a comparative analysis (Table 1) show that the USA has the largest number of sectors CI, unlike Sweden. It has also been found that the most demanded sectors are banks and finance, energy, telecommunications, since these sectors were classified by most countries in the CI. Therefore, nowadays it is paramount to pay attention to the protection of these CI sectors.

Table 1

List sectors of the state`s CI

№	State / Sector CI	USA	Australia	Canada	Great Britain	Germany	Norway	Austria	Switzerland	Japan	Italy	Netherlands	Poland	New Zealand	Finland	France	Russia	Sweden
1.	Banks and Finance	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2.	Power engineering	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
3.	Telecommunications	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4.	Transport	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+	+	-
5.	Water supply	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	-	-
6.	Healthcare	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	-	-
7.	Fuel and energy complex	+	+	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-
8.	Bodies of executive power	+	+	+	+	+	+	-	+	+	-	+	+	+	-	-	-	+
9.	Emergency and Emergency Response	+	+	+	+	+	+	+	-	-	+	-	-	+	-	-	-	-
10.	Public Order Protection Service	-	+	+	+	-	-	+	+	-	+	-	-	+	-	+	-	-
11.	Agriculture	+	+	+	+	+	-	-	+	-	-	+	+	-	+	-	-	-

12.	The defense industrial complex	+	+		-	-	-	-	-	-	-	-	-	-	+	+	+	-
13.	Waste management	-	+	+	+	-	+	-	+	-	+	-	-	-	-	-	-	-
14.	Justice bodies	+	-	-	+	+	-	-	-	-	-	+	-	+	-	-	-	-
15.	Communal networks	-	+	-	-	+	+	+	-	-	-	-	-	-	+	-	-	-
16.	Dangerous Materials (Chemical, Biological, Radiation, Nuclear) (CBRN)	+	-	+	+	-	-	-	-	-	-	-	+	-	-	-	-	-
17.	National symbols	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18.	Postal services	+	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-
19.	Air traffic control system	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-
20.	Dams	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21.	Logistic	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-

It is obvious that in certain of CI sectors the main element of regular (normal) functioning of their objects is ITS, which in general are critical information infrastructure. It is clear that ITS is vulnerable to various types of cyberattacks which result in system halts, loss of control or failure of the system. Due to the increasing number of successful cyberattacks on ITS, most leading countries of the world are consolidating the critical objects of the most vulnerable ITS and networks into a single system, since the loss or disturbance of continued functioning of such objects may lead to significant or even irreparable negative consequences for national security and defense.

In Ukraine, in which the key element of ITS is the core element, it is necessary to include the following sectors of the CI: banking and finance, security and defense sectors, postal communication, transport, fuel and energy, environmental, public administration and law enforcement, life-support network, etc. (Fig. 1)

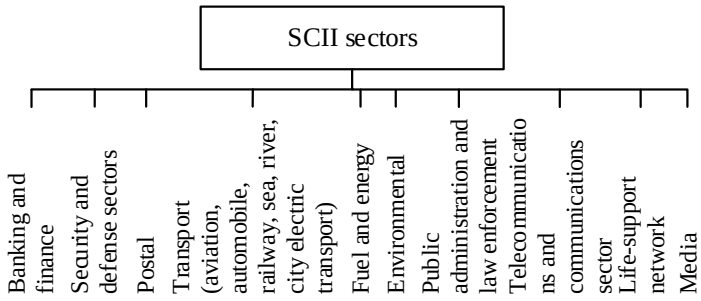

Fig1. List sectors of Ukraine CII

Thus, the problem of lack of a list of CI sectors was analyzed, resulting in the main of CI sectors being allocated and ranked from the experience of the leading countries of the world. It has been discovered that objects of CI with ITS are vulnerable to various types of cyberattacks, therefore the list of the main sectors of the critical information infrastructure of the state, which does not function without ITS, is proposed.

LITERATURE

1. A. Korchenko, Y. Dreis, O. Romanenko, “Analysis problems in the field of state’s critical infrastructure”, Projekt interdyscyplinarny projektem XXI wieku: Monografia. Tom 1. – Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2017. – pp.397 - 402.
2. Biryukov D., Kondratov S., Sukhodolya A.: Green Book on critical infrastructure protection in Ukraine. Kyiv, 2016, 176.: http://www.niss.gov.ua/public/File/2016_book/Syxodolya_ost.pdf
3. Dreis Y.: Comparative analysis of the negative effects of cyber attacks on the critical information infrastructure of different countries. Kropivnitsky,ммм 2017, 40-43.
4. Cabinet of Ministers of Ukraine: On Approval of the Procedure for the Formation of the List of Information and Telecommunication Systems of the State Critical Infrastructure Facilities. Regulation, Order from 23.08.2016 № 563.: http://zakon5.rada.gov.ua/laws/show/563-2016-п
5. Sheet from Internet Association of Ukraine №32 from 28.02.2017 President of Ukraine regarding the decision NSDCU from 29.12.2016: On threats to cybersecurity of the state and urgent measures of their neutralization: http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-29122016-pro-zagrozy