Vitalii HREBENUIK[1], Yurii DREIS[2], Alla HREBENUIK[3],
Oleksii GAVRYLENKO[4]

Scientific supervisor: Alexander KORCHENKO[5]

CRITERIA FOR ASSIGNING OBJECTS TO CRITICAL INFRASTRUCTURE OF UKRAINE

Abstract: The criteria for assigning objects to the critical infrastructure of Ukraine were analyzed. They were formed into a universal set that could be supplemented with new ones to create a methodology for assigning objects to the state's critical infrastructure, ordering their certification and categorization, and improving the procedure for establishing a list of critical information infrastructure to ensure their cyber security.

Keywords: objects critical infrastructure, multiple criteria, critical information infrastructure

KRYTERIA DOBORU OBIEKTÓW DLA INFRASTRUKTURY KRYTYCZNEJ UKRAINY

Streszczenie: Analizowane są kryteria klasyfikacji obiektów dla infrastruktury krytycznej Ukrainy. Kryteria te ujęte zostały w przepisy (zasady). Są one formowane w uniwersalny zestaw, który można uzupełnić o nowe, aby stworzyć metodologię przypisywania obiektów do infrastruktury krytycznej państwa, zarządzając ich certyfikację i kategoryzację oraz usprawniając procedurę ustanawiania listy krytycznej infrastruktury informacyjnej w celu zapewnienia ich cyberbezpieczeństwa.

Słowa kluczowe: infrastruktura krytyczna, wiele kryteriów, infrastruktura informacji krytycznej

---

[1] Dr Eng (National Security Protection of Ukraine), Head of scientific department, National Academy of Security Service of Ukraine, ratel6969@meta.ua
[2] PhD Eng (Information Security), Associate Professor of IT-Security Academic Department, National Aviation University, Senior Researcher of scientific department, National Academy of Security Service of Ukraine, y.dreis@nau.edu.ua
[3] PhD Eng (Ukrainian Language), Lecturer at the department of Eastem European National Languages, National Academy of Security Service of Ukraine, ratel6969@meta.ua
[4] PhD Eng (Mathematical modeling and computational methods), Associate Professor of IT-Security Academic Department, National Aviation University, gavrylav@gmail.com
[5] Dr Eng (Information security), Professor, Laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Hu-manistyczna, Bielsko-Biała, Poland), Leading Researcher of scientific department, National Academy of Security Service of Ukraine, icaocentre@nau.edu.ua

1. Introduction

Increasingly, objects for cyber attacks and cybercrime are becoming the resources of financial institutions, transportation, communications and energy, government agencies that provide security, defense and emergency protection. The newest technologies are used not only for committing traditional types of crimes, but also for fundamentally new ones that are inherent in a society with a high level of information. The existing regulatory objects of critical infrastructure (OCI) in the information area indicates the presence of a number of problems [1, 2] with nature of the activities in question, there is a no distinct orientation of drawing up a list of information and telecommunication systems (ITS) OCI. In addition, on the conceptual and normative levels there were not developed the classification objects of critical infrastructure state (OCIS) and were not formed for ITS as objects of critical information infrastructure (OCII) [3, 4]. Also there are no criteria for determining the assessment of negative consequences to which can be caused by cyber attack on ITS OCI, etc. [5-7]. In this regard, analyzing and compiling a list of general criteria for assigning objects to a state's OCI with the aim to define clearly the completeness and boundaries of the critical information infrastructure of the state by subjects providing its cyber security is a pressing issue. Based on the above, the purpose is drawing up a list of generalized criteria of OCI items to their cyber OCII further assuring.

2. Analysis of criteria classification of objects to critical infrastructure

After analyzing scientific papers and synthesis of existing legal documents [1-21], there were formed the generalized criteria of objects to OCIS:

1) *By activity and provision of services in the critical infrastructure sector*:

- enterprises, institutions and organizations, irrespective of the form of ownership, which carry out activities and provide services in the branches [8, 9]: energy, chemical industry, transport, information and communication technologies, electronic communications, banking and finance; in the areas of livelihoods of the population, in particular, centralized water supply, drainage, electricity and gas supply, food production, agriculture, health care; are communal, emergency and rescue services, emergency services for the population; included in the list of enterprises of strategic importance for the economy and security of the state; are objects of potentially hazardous technologies and industries; are objects subject to protection and defense in a state of emergency and special period;
- belong to the state sector critical infrastructure [2]: banking and financial sector, defense and security sector; postal and transport communications (aviation, road, rail, sea, river, city electric transport), fuel and energy sector; the environmental sector; public administration and law enforcement sector; sector of life support network and others.

2) *By category of objects, which are subject to special conditions for ensuring their protection and functioning:* «… Enterprises that are of strategic importance for the economy and security of the state; objects that are included in the State Register of Potentially Dangerous Objects; objects of increased danger (including the list of

particularly dangerous enterprises, whose termination of activity requires special measures to prevent damage to life and health of citizens, property, structures, environment); important government assets; objects subject to mandatory protection by units of the State Protection Service under contracts; facilities subject to protection and defense in emergency situations and during special periods; especially important objects of electricity; especially important objects of the oil and gas industry; national confidential communication system; payment systems; emergency system for the population at the unique number 112; emergency services; immovable cultural heritage» [10].

3) *According to the criteria for the short list of certain state property objects of particular importance, which protection is provided exclusively by state enterprises and organizations on the basis of agreements on the provision of security services, where* [11]:

- stored: drugs, psychotropic substances and precursors; historical and cultural values of national importance;
- manufactured and/or stored: weapons, missiles, ammunition, explosives, firearms, special weapons charged with tear and irritant substances, active defense; stocks of fuel and lubricants, real estate and food property;
- water supply of settlements with drinking water tanks is carried out; disposal of radioactive waste; carrying out activities related to state secrets; operations with precious metals and precious stones, precious stones of organogenic formation, semi-precious stones; assessing the quality of education, conducting and reviewing the results of external independent evaluation; sports and / or entertainment; provision of medical care and medical services;
- the state authority is located;
- there is of strategic importance for the economy and security of the state according to the "List of State Property Objects of Strategic Importance for the Economy and Security of the State";
- it belongs to the object of high risk in accordance with the law.

4) *The set of criteria that determine their importance for the implementation of vital functions and the provision of vital services, indicate the existence of risks and threats to them, the possibility of crisis situations through interference in their functioning, termination of operation, human factor or natural disasters, the duration of work to eliminate such consequences until the full restoration of the regular regime, namely* [6, 8-10]:

- the existence of challenges, risks and threats that may arise with respect to critical infrastructure;
- causing significant damage to the normal living conditions of the population;
- the vulnerability of these objects, the severity of the possible negative consequences, which will cause significant harm: the health of the population (determined by the number of victims, dead and seriously injured, as well as the number of evacuated population); social sphere (destruction of social protection systems and provision of social services, loss of the state's ability to meet the critical needs of society); economy (impact on GDP, size of economic losses, both direct and indirect); natural resources of national importance; defense capabilities; the image of the country;

- the magnitude of the negative consequences for the state, which will: affect the activities of strategically important entities in several sectors of the economy or lead to the loss of unique nationally significant assets, systems and resources, have lasting consequences for the state and affect the activities of several other sectors;

- the duration of elimination of such consequences and the impact of further negative impact on other sectors of the state;

- Impact on the operation of adjacent critical infrastructure sectors:

- causing significant damage to normal living conditions of the population.

5) *On the consequences of disruption of the stable functioning of the OCI, which can cause cyber attacks* [2, 6, 12]: the occurrence of an anthropogenic situation and / or a negative impact on the state of the state (region) (H1) environmental safety; negative impact on the state of energy security of the state (region) (H2); negative impact on the state of economic security of the state (H3); negative impact on the state of defense, national security and law enforcement in the state (H4); negative impact on the system of government (H5); negative impact on the socio-political situation in the country (H6); negative impact on the image of the state (H7); disruption of the stable functioning of the financial system of the state (H8); disruption of the sustainable functioning of the transport infrastructure of the state (region) (H9); disruption of the stable functioning of the information and / or telecommunication infrastructure of a state (region), including its interaction with the corresponding infrastructures of other states (H10).

6) *By the method of identification of potentially dangerous objects* [13]:

- by type of danger: bacteriological, biological, explosive, hydrodynamic, fire, radiation, physical, chemical, environmental;

- by classification and emergency code (emergency): man-made, natural, socio-political and military in nature;

- by the level of possible emergency: national, regional, local and object level;

7) *By Criticality Category* [9]: I Criticality Category - Critical Objects, II Criticality Category - Vital Objects, III Criticality Category - Important Objects, IV Criticality Category - Required Objects.

8) *By classes of consequences (liability) of the object complexity category* [14]:

- the class of consequences of SS-1 corresponds to I and II category of complexity;

- the class of consequences of SS-2 corresponds to the III and IV categories of complexity;

- the class effects of SS-3 corresponds to V category of complexity.

9) *In the presence of OCI* [8, 9]: communication or technological system of OCI; information and telecommunication systems and networks, automated process control systems.

10) *According to the main criteria for identifying a certain critical infrastructure element*: «…territorial reach of negative results (transnational, national, regional, local); a large number of consequences (humanitarian, material, economic, political or environmental damage and loss); the temporary effect of the consequences,

especially when negative effects occur (immediately, within 24 hours); how long the negative effects can last (up to 24 hours, up to 3 days)» [18].

11) *According to the identification of high risk objects* [15-17]:

- by category of available hazardous substances: combustible (flammable) gases; flammable liquids; flammable liquids overheated under pressure; explosives; oxidizing agents; highly toxic and toxic substances; substances that pose a risk to the environment (highly toxic to aquatic organisms);
- by types and impact of the impact factors of accidents that may occur on the basis of the properties of hazardous substances: group 1 (explosion); group 2 (fire); group 3 (harmful to humans and environment).

12) *By type of information being processed* [19-21]:

- national electronic information resources: public information; state information resources; other information designed to meet the vital public needs of the citizen, individual, society and state;
- information with restricted access: confidential information (including personal data); service information; secret information.

3. Universal set of generic criteria list

The list of generalized criteria of objects to OCIS can be represented as universal set:

$$\mathbf{C} = \{\bigcup_{i=1}^{n} \mathbf{C}_i\} = \{\mathbf{C}_1, \mathbf{C}_2, ..., \mathbf{C}_n\}, \tag{1}$$

where $C_i \subseteq \mathbf{C}$ $(i=\overline{1,n})$ - i-IDs and groups subset criteria OCI, and n - the total number of these groups. For the i-th subset $\mathbf{C}_i$ is defined as:

$$\mathbf{C}_i = \{\bigcup_{j=1}^{n_i} C_{ij}\} = \{C_{i1}, C_{i2}, ..., C_{in_i}\}, \tag{2}$$

where $C_{ij} \subseteq \mathbf{C}_i$ $(j=\overline{1,n_i})$ - identifiers of the criteria of the i-th group, and n_i - their number of these groups. For the j-th subset $\mathbf{C}_{ij}$ is define as:

$$\mathbf{C}_{ij} = \{\bigcup_{j=1}^{n_i} \{\bigcup_{s=1}^{n_{ij}} C_{ijs}\}\} = \{C_{ij1}, C_{ij2}, ..., C_{in_{ij}}\}, \tag{3}$$

where $C_{ijs} \subseteq \mathbf{C}_{ij}$ $(s=\overline{1,n_{ij}})$ - identifiers of the j-th criteria of the i-th group, and n_{ij} - the number of these criteria. In view of (2) and (3) the expression (1) can be represented as:

$$\mathbf{C} = \{\bigcup_{i=1}^{n} \mathrm{C}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{n_i} \{\bigcup_{s=1}^{n_{ij}} C_{ijs}\}\}\} = \{\{C_{11}, C_{12}, ..., C_{1n_1}\}, \{C_{21}, C_{22}, ..., C_{2n_2}\}, ...,$$

$$\{C_{n1}, C_{n2}, ..., C_{nn_{i_n}}\}, ..., \{C_{nn_i 1}, C_{nn_i 2}, ..., C_{nn_{i_{nij}}}\}\}, \ (i = \overline{1,n},\ j = \overline{1,n_i}, s = \overline{1,n_{ij}}) \tag{4}$$

.

CONCLUSIONS

This study proposes a list of generalized criteria for assigning objects to OCI, which can be supplemented by new and other criteria due to its formulaic multiple representation, which can improve and improve the procedure for the formation of classifiers and registry for OCIS, a list of their OCI to determine the completeness and boundaries of the entities providing their cyber defense.

LITERATURE

1. KORCHENKO A., DREIS Y.,ROMANENKO O.: 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, 397-402.
2. KORCHENKO A., DREIS Y., ROMANENKO O.: Ukrainian critical information infrastructure: terms, sectors and consequences. Ukrainian Information Security Research Journal, 2017, vol. 19 (4), 303-309.
3. KORCHENKO A., DREIS Y., ROMANENKO O., BYCHKOV V.: Модель класифікатора об'єктів критичної інформаційної інфраструктури держави / The model of objects classifier of critical information infrastructure of the state. Ukrainian Information Security Research Journal, 2017, vol. 20 (4), 303-309.
4. KORCHENKO A., DREIS Y., ROMANENKO O.: Формування множини ідентифікаторів для класифікації об'єктів критичної інформаційної інфраструктури / Formation of a set of identifiers for the classification of critical information objects. Conf. Topical issues in cybersecurity and information security, Ukraine 2019, 59-63.
5. KORCHENKO A., KAZMIRCHUK S., DREIS Y., ROI Y., ROMANENKO O.: An assessment of the consequences of the leakage of state secret from cyberattacks to a critical infrastructure. Projekt interdyscyplinarny projektem XXI wieku: Monografia, Tom 2, Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2018, 115-122.
6. DREIS Y.: Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави / Analysis of basic terminology and negative consequences from cyber attaks on information-telecommunication systems of objects state's critical infrastructure. Ukrainian Information Security Research Journal, 2017, vol. 19 (3), 214-222.

7. KORCHENKO A., DREIS Y., ROSHCHUK M., ROMANENKO O.: Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави / Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state. Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 29-35.
8. Verkhovna Rada of Ukraine: About the basic principles of providing cyber security of Ukraine. Law dated 08.07.2018 №2163-VIII: *https://zakon.rada.gov.ua/laws/show/2163-19.*
9. Cabinet of Ministers of Ukraine: About the approval of the General requirements for cyber defense of critical infrastructure. Decree dated 19.06.2019 №518: *https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8.*
10. National Institute for Strategic Studies of Ukraine: On the problems of improving the system of critical infrastructure protection in Ukraine. Analytical note: *http://old2.niss.gov.ua/articles/1477/.*
11. Ministry of the Interior of Ukraine: Approval of the Criteria according to which the objects are included in the list of particular especially important objects of state property, which are protected only by state enterprises and organizations on the basis of security services contracts. Order dated 01.09.2015 №1053: *https://zakon.rada.gov.ua/laws/show/z1124-15.*
12. 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. Decree dated 23.08.2016 №563: *http://zakon5.rada.gov.ua/laws/show/563-2016-n.*
13. Cabinet of Ministers of Ukraine: On approval of the Procedure for classification of emergencies by their levels. Decree dated 24.03.2004 №368 (with changes 2013): *https://zakon.rada.gov.ua/laws/show/368-2004-%D0%BF.*
14. Verkhovna Rada of Ukraine: On regulation of town-planning activity. Law dated 17.02.2011 №3038-VI : *https://zakon.rada.gov.ua/laws/show/3038-17.*
15. Verkhovna Rada of Ukraine: About high risk objects. Law dated 18.01.2001 №2245-III (with changes 2014): *https://zakon.rada.gov.ua/laws/show/2245-14.*
16. Cabinet of Ministers of Ukraine: About the identification and declaration of safety of high risk objects. Decree dated 11.07.2002 №956: *https://zakon2.rada.gov.ua/laws/show/956-2002-%D0%BF.*
17. Ministry of Emergencies and Protection of Population from the Consequences of the Chornobyl Catastrophe: On approval of the Methodology for identification of potentially dangerous objects. Order dated 23.02.2006 № 98: *https://zakon.rada.gov.ua/laws/show/z0286-06.*
18. GNATYUK S., LYADOVSKAYA V.: Criteria for determining the elements of critical infrastructure of the state. Internet portal «Nauka.zinet.info»: *http://nauka.zinet.info/23/gnatyuk.php.*
19. Verkhovna Rada of Ukraine: About access to public information. Law dated 13.01.2011 №2939-VI (with changes 2015): *https://zakon.rada.gov.ua/laws/show/2939-17.*
20. KORCHENKO A., KAZMIRCHUK S., DREIS Y.: Метод аналізу і оцінки величини можливої шкоди національної безпеці держави у сфері охорони державної таємниці / A method of analysis and estimation of size of possible

harm national safety of the state is in the field of guard of state secret. Ukrainian Information Security Research Journal, 2012, vol. 3, 5-18.

21. KORCHENKO A., LUTTSKYY M., ZAHAROVA M., DREIS Y.: Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / Synthesis methodology and software implementation system evaluation harm to national security in protection of state secrets. Ukrainian Information Security Research Journal, 2012, vol. 15(1), 5-18.