DOI: 10.18372/2410-7840.19.12220
УДК 004.056 (045)

UKRAINIAN CRITICAL INFORMATION INFRASTRUCTURE: TERMS, SECTORS AND CONSEQUENCES

Oleksandr Korchenko, Yurii Dreis, Olga Romanenko

The article is devoted to the study of Ukraine the critical information infrastructure in order to increase the efficiency of use and protection of state information resources circulating in the information and telecommunication systems of critical infrastructure objects. The analysis of international experience and current domestic regulation of this field have revealed such basic problems as: the lack of basic terminology, the need to create a system for critical infrastructure protection and crisis management, the formation and development of a system of public-private partnership, the absence of sectors and elements in Ukraine critical infrastructure and of criteria attribution of objects to critical infrastructure, the lack of criteria for assessing the negative consequence of cyberattacks on the information telecommunicative system of the object of critical infrastructure, as well as the need for legislative changes. To resolve some of them, the authors introduce new concepts in this article, propose sectors of Ukraine the critical infrastructure with the definition of those relating to critical information infrastructure, unification of the negative consequence of cyberattacks on the information and telecommunication system of the critical infrastructure object in order to further evaluate the damage inflicted on the national security of Ukraine in the event of the leakage of state information resources.

Keywords: *critical information infrastructure, information and telecommunication system, cybersecurity, negative consequence of cyberattacks.*

Topicality. In the beginning of two-thousands most European Union countries began to increasingly focus on the need to develop mechanisms for protecting European critical infrastructure (CI), based on transatlantic economic and security relations. However, in terms of the number of unprecedented terrorist acts, positional leadership in this area is occupied by the United States of America (USA), in which protection of the CI from terrorist threats is defined as one of the main tasks of the national security system.

In Ukraine, taking into account the latest developments, the number of implemented cyberattacks has significantly increased while the assessment of vulnerability and potential consequences of the cessation or destruction of infrastructure is becoming one of the main functions of the state. Therefore, in the interests of ensuring national security, there is an arising question of the need to increase the efficiency of use and protection of state information resources, especially of restricted information, which is processed in information and telecommunication systems (ITS) of objects critical infrastructure (OCI), the loss of which can cause severe consequences. Therefore, the problem of determining the severity of the negative consequences and the magnitude of the harm done, as well as other possible costs of restricting access and protecting information with limited access from its source, which may lead to cyberattack on the ITS OCI, is a relevant scientific and practical task.

The purpose of the article is to increase the efficiency of the use and protection of state information resources circulating in the ITS OCI by expanding the concept and terminology apparatus, identifying sectors of critical information infrastructure (CII) and unifying the negative consequences of cyberattacks.

Analysis of recent research and stting objectives. The analysis of scientific works [1-21] in the field of state`s CII (SCII), especially concerning the provision of cybersecurity in the ITS, and identifying its crisis situation for national security, has highlighted a number of problems:

1. Lack of basic terminology.

The writings [2-5] emphasize the lack of clearly defined conceptual-terminological basis in the legislation of Ukraine in the field of critical information infrastructure of the state, but for the solution of this problem, the authors have not proposed any new concepts.

It should be noted, that in the adopted draft Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" [3] there are no such basic concepts as "state critical information infrastructure", "protection of state critical information infrastructure", "subject protection of state the critical information infrastructure", etc., which, in turn, is impeding the integration of our state into the world information space.

2. The need to create a critical infrastructure protection system.

Works [6-8] are devoted to the question of the formation of state policy in the field of CI and the need to create a system for its protection from the point of view of events in the east of Ukraine.

The authors propose creating a system protection CI (SPCI) and a crisis management center that should

respond to a set of threats and aim to ensure the sustainability of functioning of the life-sustaining system of society, the national economy and the state [5, 9].

3. Formation and development of public-private partnership system.

In the leading countries of the world, considerable attention is devoted to this problem. For example, the National Defense Strategy of Canada's CI [2] states that responsibility for ensuring the protection of the CI of the country should be borne by all public authorities and the private sector, as well as by all Canadians as members of the Canadian society. The latter should be prepared to confront emergencies at least during the first hours of a given event.

Regarding the "European Protection Program", the responsibility for the protection of its objects lies with their owners (operators) and the government of the respective member state of the European Union.

In analytical reports [6, 7], it is noted that the protection of Ukraine the CI, in terms of ensuring the operational functioning of the SPCI for terrorist threats, is possible only on the basis of cooperation concerning the exchange of information between the public and private sectors. However, public and private companies are not interested in establishing such a partnership, since, firstly, it is not forseen by the legislation of Ukraine, and secondly, it will lead to additional burdens and costs.

4. Lack of sectors and elements in the CI and criteria for assigning the OCI.

The paper [5] describes the flaw of there not being a list of priority sectors of the CI, the absence of criteria and methodology for assigning of Ukraine OCI, the need to modify the existing classification of threats to the CI, taking into account world experience, but the author has not provided any ways to address these shortcomings.

However, in [6, 7] a list sectors of CI is proposed, as well as a general structure of criteria for assigning OCI, but without taking into account the experience of international countries.

It is worth mentioning that none of the existing categories of objects, for which there are special conditions for ensuring their protection and functioning, have any grounds to be included in the full membership of the CI.

5. Lack of criteria for assessing the negative consequences of cyberattacks on ITS OCI.

The Order [10] suggests the formation of a list of ITS OCI, where it is necessary to determine the negative consequences of cyberattacks on ITS. However, the letter [11] from the Internet Association of Ukraine has indicated the impossibility of implementing this resolution, as paragraph 8 of the Order needs to supplement the list of criteria for determining the assessment of these negative consequences, which can lead to cyberattack on the ITS OCI.

In the works [12-14], an analysis of the negative consequences that could lead to cyberattacks on ITS has been conducted, as well as other serious consequences of restricted access information leakage, which need to be taken into further account.

6. Changes in national legislation.

For expanding the basic terminology, creating a state-owned SPCI and a crisis management center, as well as developing criteria for assigning in Ukraine the OCI, changes to national legislation are necessary. In this case, it is appropriate to adopt a separate Law of Ukraine defining the principles of state policy, subjects, objects, objectives, and structure in Ukraine of the CI.

The purpose of the paper is to research the scientific and regulatory bases of national and international experience regulation in sectors CI of developed countries for the necessity of formation a list of sectors CII of Ukraine and expanding basic terminology.

The main part resears. Extension of basic terminology. In order to solve the aforementioned problem concerning the necessity of expanding the concept-terminology apparatus in the SCII filed, authors suggest introducing definitions of such basic concepts as [16]:

State critical information infrastructure is a set of information and telecommunication systems of objects critical infrastructure that ought to, first and foresmost, be protected from cyberattacks that are included in their list determined by the legislation;

Protection of state critical information infrastructure - this activity is aimed at insuring the protection of information processed in the information and telecommunication systems of critical infrastructure objects in order to prevent cyberattacks from possible negative consequences of their implementation;

Security of state critical information infrastructure is apartment security of the information and telecommunication systems of objects critical infrastructure from cyberattacks, in which the basic security services of information processed in these systems are provided.

It should be noted that the primary concepts in the SCII field are also regulatory-defined concepts: cyberattack, critical infrastructure, critical infrastructure objects [10]; ITS, telecommunication system, information system, protection of information in the system, unauthorized actions regarding information in the system, information processing in the system,

comprehensive information security system, cryptographic protection of information, technical protection of information, etc. [17].

Significant expansion of terminology in the SCII field will be carried out owing to the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine", which has introduced the notions of [3]: cyberattack, cybersecurity, cyberdefense, cyberthreats, cybersecurity incident, cybercrime incident, cybercrime, cybercrime, cyberspace, cyberintelligence, cyberterrorism, cyberespionage, critical infrastructure, national telecommunication network, national electronic information resources, electronic informationresources, object CII, process control system, a system of electronic communications.

2 List sectors of the critical information infrastructure. 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, 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 sectors CI.

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	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2.	Power engineering	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
3.	Telecommunications	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.	Transport	X	X	X	X	-	X	X	X	X	X	X	X	X	X	X	X	-
5.	Water supply	X	X	X	X	X	X	X	X	X	X	X	X	-	X	X	-	-
6.	Healthcare	X	X	X	X	X	X	X	X	X	X	X	X	-	X	X	-	-
7.	Fuel and energy complex	X	X	X	X	X	X	-	-	X	X	X	X	X	-	-	X	-
8.	Bodies of executive power	X	X	X	X	X	X	-	X	X	-	X	X	X	-	-	-	X
9.	Emergency and Emergency Response	X	X	X	X	X	X	X	-	-	X	-	-	X	-	-	-	-
10.	Public Order Protection Service	-	X	X	X	-	-	X	X	-	X	-	-	X	-	X	-	-
11.	Agriculture	X	X	X	X	X	-	-	X	-	-	X	X	-	X	-	-	-
12.	The defense industrial complex	X	X		-	-	-	-	-	-	-	-	-	-	X	X	X	-
13.	Waste management	-	X	X	X	-	X	-	X	-	X	-	-	-	-	-	-	-
14.	Justice bodies	X	-	-	X	X	-	-	-	-	-	X	-	X	-	-	-	-
15.	Communal networks	-	X	-	-	X	X	X	-	-	-	-	-	-	X	-	-	-
16.	Dangerous Materials (Chemical, Biological, Radiation, Nuclear) (CBRN)	X	-	X	X	-	-	-	-	-	-	-	X	-	-	-	-	-
17.	National symbols	X	X	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18.	Postal services	X	-	-	-	-	-	X	-	-	-	-	-	-	-	-	-	-
19.	Air traffic control system	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-
20.	Dams	X	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
21.	Logistic	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-

Analyzing the foreign experience of the leading countries of the world in relation to the sectors CI, a general list of Ukraine sectors the CI and the main departments (state regulators) that provide the necessary functioning within the framework of statutory powers are proposed (Table 2).

It is obvious that in certain sectors of the CI the main element of regular (normal) functioning of their objects is ITS, which in general are CII. 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).

Table 2

List sectors of state`s CI

№	Sectors of CI in Ukraine	State regulator
1.	Banking and Financial Sector	National Bank and other banking institutions. Ministry of Finance
2.	Fuel and energy sector	Ministry of Energy and Coal Industry
3.	Telecommunications and Communications Sector	State Service for Special Communications and Information Protection of Ukraine (SSCIPU)
4.	Transport sector (aviation, automobile, railway, sea, river, city electric transport)	Ministry of Infrastructure of Ukraine, Ministry of Regional Development, Construction and Housing and Communal Services. Ukrposhta, Nova Poshta and others
5.	Postal connection	State Emergency Service (SES), Ministry of Regional Development, Construction and Housing and Communal Services
6.	Life support network	Ministry of Health
7.	Healthcare sector	Ministry of Internal Affairs
8.	Public administration and law enforcement	SES
9.	Emergency and Civil Protection Sector	Ministry of Agrarian Policy and Food of Ukraine
10.	Food industry and agro-industrial complex	Ministry of Defense of Ukraine, SSCIPU, Security Service of Ukraine (SSU), National Police of Ukraine, National Bank, intelligence agencies
11.	Security and Defense Sector	SES
12.	Hazardous Materials Sector (CBRN)	Ministry of International Affairs
13.	Diplomatic missions	Ministry of Culture of Ukraine
14.	National cultural heritage	Ministry of Environment and Natural Resources. Ukrainian Hydrometeorological Center
15.	Media	Ministry of Information Policy, SSU

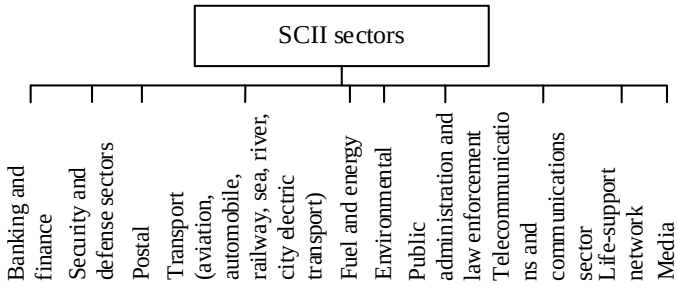

Fig. 1. List sectors of Ukraine CII

Negative consequences of cyberattacks on ITS of the state`s OCI. The Annex of the Order [10] provides suggestions for the formation of a list of OCI of the ITS, which contain information such as: serial number, ITS name, form of ownership, name of the owner (manager) of the ITS, the type of information processed in the ITS (public data, confidential information, information of state secret in accordance with the Law of Ukraine "About information"), the negative consequences that a cyberattack can cause on the ITS, personal information (security administrators) responsible for the operation of the ITS (surname, name, patronymic, telephone number, e-mail address mail, etc.). In accordance with these proposals, it is necessary to determine the negative consequences that a cyberattack can cause on ITS, namely Order [10]: emergence of an emergency situation of anthropogenic nature and/or negative impact on the apartment of the ecological security of the state (region); negative impact on the apartment of energy security of the state (region); negative impact on the

apartment of economic security of the state; negative impact on the apartment of defense, ensuring national security and law and order in the state; negative influence on the apartment control system of the state; negative impact on the so socio-political situation in the state; negative impact on the image of the state; violation of the stable functioning of the financial system of the state; violation of the sustainable functioning of the transport infrastructure of the state (region); violation the functioning of the information and/or telecommunication infrastructure of the state (region), including its interaction with the corresponding infrastructures of other states.

However, with the indication of the kind of information being processed, for example, the state secret, it is necessary to take into account other serious consequences that are determined by limiting access to this information, and to mention them in those proposals, since this cyberattack can also lead to its leakage. That is, depending on the type of classified information that is processed in the ITS and its possible leakage, other additional grave consequences are recognized, namely [19]: 1) the first category: the complete disruption of diplomatic relations, which may lead to an cyberattack on Ukraine or its allies or military operations; full control of state encrypted correspondence from another state; 2) the second category: the rupture of diplomatic relations with one or several developed countries; full or partial (30% or more) disclosure of the intelligence capabilities of the state abroad; a threat to life or liberty for persons performing intelligence or counter-intelligence tasks; 3) the third category: the rupture of diplomatic relations with other states (state); closure of the embassy (representation) of Ukraine in any country; decrease in the level of representation of Ukraine in any country; full or partial (30% or more) reduction of the effectiveness of operational and strategic plans; full or partial (30% and more) loss of combat command of troops, the need to develop new algorithms of troop control systems, the creation of new control points; partial (up to 30%) disclosure of the intelligence capabilities of the state abroad; 4) the fourth category: the failure of Ukraine to conclude an international treaty; failure or impossibility of performing an intelligence, counterintelligence or other special operation; partial (up to 30%) decrease in the effectiveness of operational and strategic plans; partial (up to 30%) loss of military command of troops, the need to develop new algorithms of the system of combat command troops; disclosure of the identity of the person who executes on an unsupervised basis an intelligence, counterintelligence or other operational task; disclosure of forces or means of tacit operational control that are used by state authorities to carry out operative-investigative activities; 5) the fifth category: disruption of negotiations on arms-disarmament problems; economic sanctions against Ukraine; the breakdown of trade and economic ties with other states; unauthorized access (penetration) to objects where special authorization and protection mode is introduced.

In addition, [21] a comparative analysis of the negative consequences of cyberattacks on SCII in different countries of the world has been conducted.

Conclusions. Given a significant number of successful cyberattacks, for every country in the world, priority is now given to providing cybersecurity. Particularly, it concerns those cyberattacks which are aimed at stopping the functioning of especially important state objects that provide vital functions of society. Therefore, there is the CI. The protection of ITS OCI from cyberattacks as a field of SCII requires considerable attention.

In order to increase the efficiency of the use and protection of the state information resources of Ukraine the CII, an analysis has been undertaken regarding international experience and current domestic regulation of the CII area. New concepts have also been introduced; the sectors of Ukraine the CI have been suggested, with the definition of those relating to CII. The negative effects of cyberattacks on ITS OCI have been unified, with the purpose of further evaluation of the damage inflicted to national security of Ukraine in case of leakage of state information resources.

REFERENCES

[1]. Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On threats to cybersecurity of the state and urgent measures for their neutralization", [Electronic resource]. Access mode: http://www.rnbo.gov.ua/documents/437.html.

[2]. "Protection in Ukraine of the critical infrastructure of implementation": an analytical report. K: NISS, 28 p, 2012. [Electronic resource]. Access mode: http://www. niss. gov.ua/content/articles/files/Sots_zahust-86178.pdf.

[3]. "On the Basic Principles of Ukraine the Cybersecurity", Verkhovna Rada of Ukraine, Draft Law dated May 13, 2017. № 2126a, [Electronic resource]. Access mode: http://w1. c1.rada. gov. ua/ pls/zweb2/webproc4_1?pf3511=55657.

[4]. Z. Hu, S. Gnatyuk, et al, "Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure", *I. J. Computer Network and Information Security*, no. 6, pp. 30-43, 2017. [Electronic resource]. Access mode: http://www.mecs-press.org/ijcnis/ijcnis-v9-n6/IJCNIS-V9-N6-4.pdf.

[5]. V. Yevseyev, "Possible ways to improve the protection of Ukraine of the critical infrastructure in the light of world experience", *Sb. sciences Works of the Narvik National Air Force University*, no. 4(49), pp. 168-172, 2016.

[6]. D. Biryukov, S. Kondratov, O. Nashvit, O. Sukhodolya, "Green Book in Ukraine on the Protection Critical Infrastructure", *K: NISS*, 2015. [Electronic resource]. Access mode: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf.

[7]. D. Biryukov, S. Kondratov, O. Sukhodolya, "Green Book in Ukraine on the Protection of Critical Infrastructure": *Sb. Matlab International. expert. meetings*. K: NISS, pp. 176, 2016. ISBN 978-966-554-258-2 [Electronic resource]. Access mode: http://www.niss. gov.ua/public/File/2016_book/Syxodolya_ost.pdf.

[8]. O. Sukhodolya, "Protection of critical infrastructure in a hybrid war: problems and priorities of the state policy of Ukraine", *Strategic Pre-Rites*, no. 3 (40), pp. 62-76, 2016.

[9]. O. Sukhodolya, "The system of protection of critical energy infrastructure of Ukraine: the state and problems of formation", *Scientific and Information Bulletin of the Academy of National Security*, no. 1-2, pp. 134-146, 2015.

[10]. "On approval of the order for the formation of the list of information and telecommunication systems of critical infrastructure objects of the state", the Cabinet of Ministers of Ukraine; Regulation, Order from 23.08.2016 № 563. [Electronic resource]. Access mode: http://zakon5.rada.gov.ua/laws/show/563-2016-п.

[11]. Letter №32 dated 28.02.2017 to the President of Ukraine regarding the decision of the National Security and Defense Council dated 29.12.2016 "On threats to the cyber security of the state and urgent measures of their neutralization", from the Internet Association of Ukraine. [Electronic resource]. Access mode: http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-9122016-pro-zagrozy.

[12]. Y. Dreis, "Comparative analysis of the negative consequences of cyberattacks on the critical information infrastructure of different countries," Information security and computer technologies: Sb. Abstracts II International science-practice Conf., Kropivnitsky: CNTU, pp. 40 – 43, 2017.

[13]. Y. Dreis, M. Movchan, "Analysis of negative consequences of cyberattacks on information resources of objects the state of critical infrastructure", *Topical problems of cybersecurity and information security: third international. science-practice conf.,* K: European University, pp. 71-74, 2017.

[14]. O. Korchenko, S. Kazmirchuk, Y. Dreis, "Method of analysis and estimation of the magnitude of possible damage to the national security of the state in the sphere of state secrets protection", *Information Protection* vol. 14, no. 3 (56), pp. 5-18, 2012.

[15]. D. Biryukov, "The concept of critical infrastructure protection as an element of pan-European security policy", Scientific notes, no. 6 (68), pp. 106-115, 2013. [Electronic resource]. Access mode: http://www.ipiend.gov.ua/uploads/nz/nz_68/birukov_kontseptsia.pdf.

[16]. Y. Dreis, O. Romanenko, "Extension of basic terminology in the field of protection of state the critical information infrastructure", *Sb. theses of the All-Ukrainian Scientific and Practical Internet Conference*, November 16-17, 2017, Kropivnitsky: CNTU, pp. 185-187, 2017.

[17]. "On the protection of information in information and telecommunication systems". Verkhovna Rada of Ukraine; The law of 05.07.1994 № 80/94. [Electronic resource]. Access mode: http://zakon2.rada.gov.ua/laws/show/80/94-вр.

[18]. D. Birukov, S. Kondratov, *Protection in Ukraine of critical infrastructure: problems and prospects of implementation*, K: NISS, 2012, 96 p.

[19]. O. Korchenko, O. Arkhipov, Y. Dreis, *Assessment of damage to the national security of Ukraine in the event of leakage of state secrets: a monograph*, K.: Sci. Center on the Security Service of Ukraine, 332 p., 2014, ISBN 978-617-7092-26-0.

[20]. M. Zakharova, Y. Dreis, "Methodology of synthesis and program realization of the system of estimation of damage to national security in the sphere of state secrets protection", *Information protection*, vol. 15 no. 1, pp. 14-20, 2013.

[21]. Y. Dreis, "Analysis of Basic Terminology and Negative Consequences of Cyberattacks on Information and Telecommunication Systems of State Critical Infrastructure Facilities", *Information Protection*, vol. 19, no. 3, pp. 214-222, 2017.

КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА УКРАЇНИ: ТЕРМІНИ, СЕКТОРИ І НАСЛІДКИ

Стаття присвячена розгляду критичної інформаційної інфраструктури України з метою підвищення ефективності використання та захисту державних інформаційних ресурсів, що циркулюють в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури. Аналіз міжнародного досвіду та чинного законодавства в цій галузі виявили такі основні проблеми, як відсутність базової термінології, необхідність створення системи захисту критичної інфраструктури та управління кризовими ситуаціями, формування та розвиток системи державно-приватних партнерство, відсутність секторів та елементів в критичній інфраструктурі України та критеріїв віднесення об'єктів до критичної інфраструктури, відсутність критеріїв оцінки негативних наслідків кібератак в інформаційній телекомунікаційній системі об'єкта критичної інфраструктури, а також

необхідність внесення змін до чинного законодавства. Для вирішення деяких проблем в статті запропоновано сектори критичну інфраструктуру України з визначенням тих, що стосуються критичної інформаційної інфраструктури, об'єднання негативних наслідків кібератак на інформаційно-телекомунікаційній системі критично важливої інфраструктури об'єкт для подальшої оцінки шкоди, завданої національній безпеці України у разі витоку державних інформаційних ресурсів.

Ключові слова: критична інформаційна інфраструктура, інформаційно-телекомунікаційна система, кібербезпека, негативні наслідки кібератак.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА УКРАИНЫ: ОПРЕДЕЛЕНИЯ, СЕКТОРЫ И ПОСЛЕДСТВИЯ

Статья посвящена рассмотрению критической информационной инфраструктуры Украины с целью повышения эффективности использования и защиты государственных информационных ресурсов, циркулирующих в информационно-телекоммуникационных системах объектов критической инфраструктуры. Анализ международного опыта и действующего законодательства в этой области обнаружили такие основные проблемы, как отсутствие базовой терминологии, необходимость создания системы защиты критической инфраструктуры и управления кризисными ситуациями, формирование и развитие системы государственно-частного партнерства, отсутствие секторов и элементов в критической инфраструктуре Украины и критериев отнесения объектов критической инфраструктуры, отсутствие критериев оценки негативных последствий кибератак в информационной телекоммуникационной системе в "Объекта критической инфраструктуры, а также необходимость внесения изменений в действующее законодательство. Для решения некоторых проблем в статье предложен сектора критическую инфраструктуру Украины с определением касающихся критической информационной инфраструктуры, объединение негативных последствий кибератак на информационно-телекоммуникационной системе критически важной инфраструктуры объект для дальнейшей оценки ущерба, нанесенного национальной безопасности Украины в случае утечки государственных информационных ресурсов.

Ключевые слова: критическая информационная инфраструктура, информационно-телекоммуникационная система, кибербезопасность, негативные последствия кибератак.

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, візит-професор Університету в Бельсько-Бялій (Гуманітарно-технічна академія в Бельсько-Бялій, м. Бельсько-Бяла, Польща), провідний науковий співробітник Національної академії СБ України.
E-mail: icaocentre@nau.edu.ua

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, визит-профессор Университета в Бельско-Бялой (Гуманитарно-техническая академия в Бельско-Бялой, г. Бельско-Бяла, Польша), ведущий научный сотрудник Национальной академии СБ Украины.

Korchenko Oleksandr, 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-Humanistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine.

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри інноваційних технологій професійної освіти Національного авіаційного університету.
E-mail: y.dreis@nau.edu.ua

Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой инновационных технологий профессионального образования Национального авиационного университета.

Yurii Dreis, PhD in Eng., Associate Professor, Head of the Department of Innovative Technologies Professional Education, National Aviation University (Kyiv, Ukraine).

Романенко Ольга Олександрівна, студент, Інститут комп'ютеризованих інформаційних систем, кафедра комп'ютеризованих систем захисту інформації, Національного авіаційного університету.
E-mail: olya_olek@ukr.net

Романенко Ольга Александровна, студент, Институт компьютеризированных информационных систем, кафедра компьютеризированных систем защиты информации, Национального авиационного университета.

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