VOL 1, No 61 (61) (2021)

The scientific heritage
(Budapest, Hungary)
The journal is registered and published in Hungary.
The journal publishes scientific studies, reports and reports about achievements in different scientific fields.
Journal is published in English, Hungarian, Polish, Russian, Ukrainian, German and French.
Articles are accepted each month.
Frequency: 24 issues per year.
Format - A4
ISSN 9215 — 0365

All articles are reviewed
Free access to the electronic version of journal
Edition of journal does not carry responsibility for the materials published in a journal.
Sending the article to the editorial the author confirms it's uniqueness and takes full responsibility for possible consequences for breaking copyright laws

«The scientific heritage»
Editorial board address: Budapest, Kossuth Lajos utca 84,1204
E-mail: public@tsh-journal.com
Web: www.tsh-journal.com

CONTENT

BIOLOGICAL SCIENCES

ECONOMIC SCIENCES

TECHNICAL SCIENCES

Таким чином, розраховані показники демонструють низьку ефективність використання виробничих запасів, незадовільний середній термін перебування запасів на складі та їх використання та стабільну ефективність використання власного капіталу підприємства.

Щодо показників ліквідності підприємства, то всі вони відображають стабільність та змогу підприємства погасити свою кредиторську заборгованість за рахунок власних коштів. Підприємства має абсолютну ліквідність (коефіцієнт миттєвого покриття вище нормативного значення). Але перевищення значення коефіцієнтами верхньої межі свідчить про незадовільне управління активами підприємства за рахунок нераціонального накопичення запасів, нарощення дебіторської заборгованості, тобто про неефективність використання власних коштів.

На основі загальноприйнятої методики [3] нами розраховано тип фінансового стану державного підприємства «Очаківське лісомисливське господарство», зокрема він визначений як безризиковий стан, що має риси дестабілізаційного аспекту [3]. Тобто, загалом фінансовий стан демонструє позитивні параметри в аспектах прибутковості, ліквідності та фінансової незалежності підприємства, що засвідчує відсутність будь-яких ознак загрози банкрутства найближчим часом. Підставою для діагностування ознак дестабілізаційного аспекту суб'єкта господарювання стали відхилення від нормативних значень у сфері ділової активності. Відмічено нераціональність використання кредиторських можливостей підприємства, а тому рекомендується підвищити рівень ділової активності, залучивши додаткові кошти, в тому числі і бюджетного фінансування, на збільшення обсягів реалізації продукції.

Висновки. Таким чином, здійснена оцінка ефективності системи управління на прикладі окремого лісогосподарського підприємства свідчить про його повну залежність від бюджетного фінансування. В той же час позитивними на кінець періоду дослідження слід вважати такі управлінські заходи, що обумовили результати діяльності підприємства: відбулося скорочення чисельності персоналу; спостерігається поява чистого прибутку; спостерігається збільшення показника фондовіддачі; ефективне використання власного капіталу підприємства (спостерігається ріст його рентабельності); підприємство має абсолютну ліквідність; спостерігається тенденція збереження фінансової незалежності підприємства.

До негативних можна віднести такі управлінські заходи, що обумовили результати діяльності підприємства: спостерігається зменшення показника зарплатовіддачі та відповідне збільшення показника зарплатомісткості; перевищення темпів росту фонду оплати праці (406,4%) над темпами росту чистого доходу підприємства (72,2%); спостерігається стрімкий ріст показника продуктивності праці з 2016 по 2018 роки, але на кінець 2019 року цей показник значно зменшився; показник фондоозброєності не відповідає нормативним значенням; низька ефективність використання виробничих запасів (незадовільний середній термін перебування запасів на складі); значне перевищення величини дебіторської заборгованості над кредиторською (в 3,5 рази).

Список літератури

1. Мних Є.В., Барабаш Н.С. Фінансовий аналіз: підручник /Є.В. Мних, Н.С. Барабаш// –К. : Київ. нац. торг-екон. ун-т, 2014. – 536 с.

2. Кірейцев Г. Г. Фінансовий менеджмент: навчальний посібник / за ред. Г. Г. Кірейцева// –3-є вид., перероб. і доп. –К.: ЦНЛ, 2004. –531 с.

3. Зуєв Є.С. Щодо питання інтегрального оцінювання фінансового стану підприємств лісового господарства. Лісівництво і агролісомеліорація: Зб. наук. пр. - Харків: УкрНДІЛГА, 2009. - Вип. 116. - С. 276-281.

METHODS AND MEANS OF ENSURING CYBER SECURITY AS A COMPONENT OF THE INFORMATION SECURITY OF THE STATE

Kiporenko S.
assistant of the department of computer science and economic cybernetics
Vinnytsia National Agrarian University,
Vinnytsia, Ukraine
DOI: 10.24412/9215-0365-2021-61-1-21-27

Abstract

The article is devoted to the analysis of the peculiarities of cybersecurity as an important component of information security in Ukraine, legislative and regulatory support of this area. Some approaches to defining the essence of cybersecurity have been investigated, taking into account the latest changes in legislation. Certain contradictions in the current legislation on these issues are revealed, the author's definition of cybersecurity is proposed, and an approach to understanding the relationship between cybersecurity and other components of information security is generalized. The main disadvantages and prospects of ensuring the protection of cyberspace are indicated. It was noted that in Ukraine, issues related to ensuring cybersecurity are defined in the Cybersecurity Strategy of Ukraine, approved by the decision of the National Security and Defense Council of Ukraine. The concept and nature of the emergence of cybercrimes as the main factor in the violation of cybersecurity in the country has been substantiated.

Keywords: cyberspace, cybersecurity, information security, cybercrime, cyberterrorism.

Problem statement. Recently, the development of information and communication technologies (ICT), cybernetics and the Internet has caused significant changes in society. The spread of the Internet has brought great social benefits to the world for many forms of activity. These profits have become significant for people, business, the state and society as a whole. Today, information and communication technology systems are integrated into all aspects of society and are critical to its functioning. And cyberspace and technology have become the basis for interaction between different sectors, both public and private, and can be considered a fundamental social infrastructure. But with the salient advantages, you must know some of the disadvantages as well. This phenomenon has led to a significant number of dangers that affect society both nationally and internationally. Thus, there is a need for mechanisms to protect cyberspace, which are described in the national strategies of world powers, which in turn are dedicated to ensuring its protection. Therefore, a very important topic at the present stage is the study of cybersecurity, as well as the justification of methods and means of its provision as a component of information security of the state. It will also be useful to gain experience in the formation and implementation of mechanisms for cyber security in Ukraine.

Goals setting. The purpose of the article is to analyze and study the concept, methods and means of cybersecurity as a component of information security in Ukraine.

Analysis of recent research and publications. Directly, the theoretical aspects, components of cybersecurity, its functions and tasks are considered in the scientific works of many Ukrainian researchers, namely: Bilenchuk P.D., Buryachok V.L., Butuzov V.M., Holina V.V., Holovkin B.M., Dovhan′ O.D., Dubov D.V., Markiv S. I., Myalkovs′kyy D.V., Obikhod T.V., Pysarenko V.P., Stets′ V., Tarasyuk A.V., Tolubko V.B., Tolyupa S.V., Khoroshko V.O. and others. Along with the significant and fruitful results of scientific research in the field of cybersecurity, there are a number of theoretical issues that need to be deepened, clarified and concretized, the disclosure of which will qualitatively increase the level of protection of national cyberspace. One of such topical issues is the development and justification of the principles and theoretical positions of building a theoretical model of cybersecurity. But the solution to this problem, first of all, requires clarification of the theoretical foundations of its separation as a component of the information security system of the state.

Presentation of the main material of the research. The growing number, scale, intensity, complexity of cyber incidents and cyber threats in global cyberspace, which cannot be effectively countered by any of the states, is one of the main factors that necessitates their international cooperation in cybersecurity and cyber defense, joining forces and means to reduce the level of cyber threats to citizens, society and the state [1, p. 216].

According to V.P. Pysarenko, today computer crimes are one of the most dynamic groups of socially dangerous encroachments. The number of these crimes is constantly increasing, their social danger is growing. This is due to the accelerated development of science and technology in the field of computerization, as well as the constant and rapid expansion of the field of computer technology [2, p. 89].

Today, there are many different scientific approaches and official definitions for defining the concept of "cybersecurity", which reflect the essence of cybersecurity from different angles.

It is considered that the concept of "cybersecurity" is most fully defined in the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", approved on 05.10.2017. According to this law, cybersecurity is the protection of vital interests of man and citizen, society and the state during use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security of Ukraine in cyberspace [3].

The National Security Strategy of Ukraine provides a distinction between the concepts of cybersecurity and information security, by identifying threats to information security and threats to cybersecurity and security of information resources. Thus, threats to information security include waging an information war against Ukraine; lack of a holistic communication policy of the state, insufficient level of media culture of society. Threats to cybersecurity and security of information resources are identified in the vulnerability of critical infrastructure, government information resources to cyberattacks, as well as in the physical and moral obsolescence of the system of protection of state secrets and other types of information with limited access [4].

In the "Cyber Security Strategy of Ukraine" cybersecurity is defined as a state of protection of vital interests of man and citizen, society and the state in cyberspace, which is achieved by comprehensive application of a set of legal, organizational, informational measures [5].

In NATO, cybersecurity is understood as maintaining a state of readiness to repel potential threats of "high intensity" and taking appropriate countermeasures. Experts from the NATO Center for Cyber Defense consider the militarization of the Internet as one of the main and most dangerous trends in the development of global cyberspace: "Modern military structures are ready to use the information space as a" parallel battlefield "in the conflicts of the future." At the same time, it is believed that a cyberattack "in its purest form" is unlikely [6].

Buryachok V.L., Tolubko V.B., Khoroshko V.O., Tolyupa S.V. define cybersecurity as a state of protection of cyberspace of the state as a whole or individual objects of its infrastructure from the risk of third-party cyberspace, which ensures their sustainable development, as well as timely detection, prevention and neutralization of real and potential challenges, cyber interventions and threats to personal, corporate or national interests [7, p. 15].

Dubov D.V. perceives cybersecurity as a state of protection of the interests of man and citizen, society and the state in cyberspace [8, p. 191].

Dovgan O.D. considers the concept of cybersecurity as a generalization and includes issues of security of systems, communications and objects that are part of cyberspace (information security, security of network structures, Internet security, protection of critical information infrastructure, etc.) [9, p. 86].

V. Stets notes that the concept of "cybersecurity" is broader than security, and security is the main factor in the formation of cybersecurity. If we turn to the most common understanding of security in general, it is a state where there are no threats and no danger. Threats can be classified according to various criteria, such as the degree of vulnerability of the object. It is clear that to protect against more vulnerable threats, it is necessary to provide greater security and vice versa (in order to save resources), that is increase and decrease the level of protection should be carried out according to the level of threats [10, p. 25].

Given all the above definitions, we will give our own definition of this concept. Thus, cybersecurity is the practical protection of systems, networks, programs and information data from digital attacks, which are aimed at accessing, modifying or destroying confidential information, interrupting business processes for their own benefit. We can also say that information security is a broader concept that includes cyber security.

V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa at their works identifies 3 components of cyber security: ITS intelligence and cryptosystems of opposing parties; cybernetic influences; protection of own information system (fig. 1) [7, p. 15].

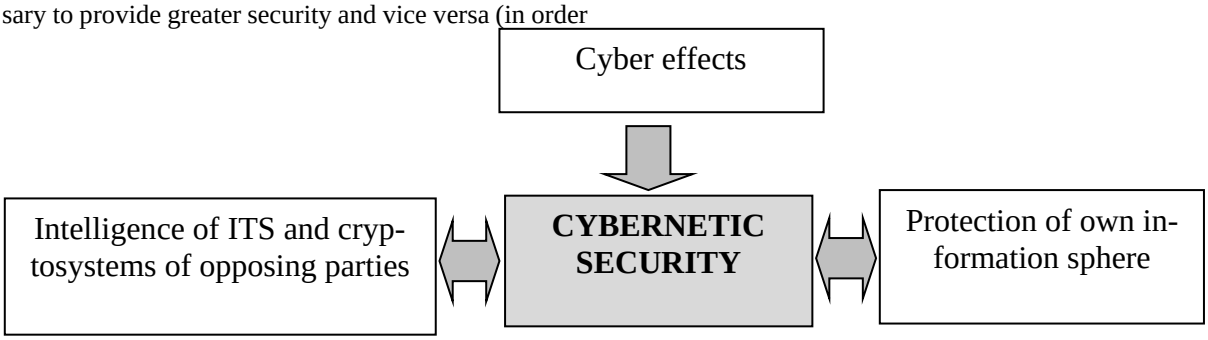

Fig. 1. Components of cyber security

Source: [7, p. 15]

The main problems of cyber security arise for the following reasons:

1) lack of clear awareness of the role and importance of the cybersecurity component in the system of national security;

2) definition, terminological and regulatory irregularities in the field of cybersecurity;

3) dependence of the state on software and technical products of foreign production;

4) the lack of proper coordination of the relevant agencies, and hence the inconsistency of actions to create certain elements of the cybersecurity system;

5) deficit in terms of methodological support and staffing of the relevant structural units [7, p. 16].

Analyzing the approaches to the interpretation of the concept of cybersecurity, it should be noted that the reason for the need to introduce this concept was the spread and increasing commission of crimes using information and communication technologies - cybercrime.

Cybercrime should be understood as a set of crimes committed in cyberspace through computer systems or through the use of computer networks and other means of access to cyberspace, within computer networks, as well as against computer systems, computers. computer networks and computer data.

The term "cybercrime" is often used in conjunction with the terms "computer crime", "crime in the field of high (information) technology", "high-tech crime". The Criminal Code of Ukraine uses the term "crimes in the use of electronic computers (computers), systems and computer networks and telecommunications networks" [11].

Cybercrimes are divided into types depending on the object, the object of encroachment, depending on the methods of commission, and so on. The most common classification of cybercrime is currently based on the structure of the Council of Europe Convention on Cybercrime. This classification is a "standard", because the available international and regional documents, as well as scientific practice, use this division:

1) offenses against the confidentiality, integrity and availability of computer data and systems: illegal access - intentional access to the entire computer system or part thereof without the right to do so for the purpose of obtaining computer data or for other unfair purposes; data interference, intentional damage, destruction, deterioration, alteration or concealment of computer information without the right to do so; interference with the system - intentionally seriously interferes with the functioning of a computer system by entering, transmitting, damaging, destroying, deteriorating, replacing or concealing computer data without the right to do so; misuse of devices, namely their manufacture, sale, purchase for use, distribution or provision for use in another way;

2) computer-related offenses;

3) offenses related to the content;

4) offenses related to infringement of copyright and related rights;

5) acts of racism and xenophobia committed with the help of computer networks [12; thirteen].

Today, the classification of cybercrime according to the nature of actions on: aggressive - cyberterrorism, threat of physical violence (for example, transmitted via e-mail), cyberbullying, cyberstalking (illegal sexual harassment and harassment of another person via the Internet), child pornography with the image of children, distribution of these materials, access to them), cyberbullying; non-aggressive - cyber theft, cyber vandalism, cyber fraud, cyber espionage, spam and virus programs [14, p. 156].

Interesting and thorough is the opinion of information specialist V. Butuzov, who provided his own comprehensive list of signs of cybercrime:

A sign of classifying certain crimes in the field of high information technology as computer is the instrument of committing a crime - computer technology. Moreover, the object of encroachment is public relations in the field of automated information processing;

A sign of classifying crimes in the field of high information technology as cybercrime is a specific environment for committing crimes - cyberspace (the environment of computer systems and networks). Moreover, the object of criminal encroachment can be the relationship of any branch of human activity, which has its manifestation in cyberspace [15, p. 119].

It is worth noting that the object of cybercrime is personal data, bank accounts, passwords and other personal information of both individuals and businesses and the public sector. Cybercrime is a threat not only nationally but also globally. The most common types of cybercrime are also: carding, phishing, vishing, online fraud, embezzlement, card sharing, social engineering, software, illegal content, refilling and others [16].

All types of cyber threats arose and spread with the development of the Internet, due to which the very fact of cyber aggravation is a consequence of the strategic trend of using cyberspace to penetrate the social, political and economic life of any social system.

Ukraine, like the vast majority of countries in the world, is taking significant steps to actively develop the information society and ensure both information and cyber security. Of course, the fight against cybercrime is no exception. Our state guarantees cybersecurity at all possible levels, including legislation.

For Ukraine in the field of cybersecurity there are only two main problems: internal and external:

1) The internal problem is that commercial entities and individuals are not aware of cyber problems. First of all, we need to work on the interaction between law enforcement agencies and those commercial organizations that can provide this service to overcome problems with attacks, hacks, etc. In addition, there should be reforms in the field of education for sufficient informational professional literacy of university graduates. Obviously, cybersecurity experts will be able to explain the need for cybersecurity, and will develop cybersecurity services accordingly. We believe that the presence of such specialists is important from the standpoint of protection of state facilities, state secrets, due to the low level of implementation of innovative technologies in the field of protection of information of state importance;

2) if we talk about foreign policy in this regard, the protection of state facilities and state secrets should also be supported by informational basic provisions. Of course, there is a very good scientific school of the Security Service of Ukraine, etc. But we must pay attention to the fact that there is technical imperfection in enterprises, and technology is known to be constantly evolving. In this area, too, constant updates are needed [17, p. 238].

As noted earlier, in Ukraine, issues related to cyber security are defined in the Cyber Security Strategy of Ukraine, approved by the decision of the National Security and Defense Council of Ukraine of January 27, 2016 and approved by the relevant Presidential Decree.

This Strategy determines that cybersecurity threats are actualized due to the action of such factors, in particular, as:

- inconsistency of the electronic communications infrastructure of the state, the level of its development and protection with modern requirements;
- insufficient level of protection of critical infrastructure, state electronic information resources and information, the requirement for protection of which is established by law, from cyber threats;
- unsystematic measures of cyber protection of critical infrastructure;
- insufficient development of organizational and technical infrastructure for cyber security and cyber protection of critical infrastructure and state electronic information resources;
- insufficient effectiveness of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature;
- insufficient level of coordination, interaction and information exchange between the subjects of cybersecurity [4].

According to the press service of the National Security and Defense Council of Ukraine, since the beginning of 2020, the country has recorded about a million cases related to cyber threats, including attempts at WEB-attacks, DDoS-attacks, the spread of malicious software. These include application-level network attacks, network scan attempts, WEB-attack attempts, phishing, DDoS-attacks, malware distribution, etc. [18].

In general, the main threats to Ukraine's cyber security are:

1) the use of cyberspace for military purposes, the creation of other states of cyber troops, cyber units in traditional types of troops;

2) development by foreign states of new types of cyber weapons;

3) the existence in other countries of plans for offensive and reconnaissance military operations in cyberspace;

4) mastering by foreign special services of methods of reconnaissance and subversive activity in cyberspace, methods of manipulation of public consciousness by means of cyberspace;

5) the possibility of involving Ukraine in armed conflicts or confrontation with other states through the use of the national segment of cyberspace;

6) attempts to interfere in the internal affairs of the state (information intervention) with the use of social networks, the spread of the cult of violence, cruelty, etc. in the national segment of cyberspace, etc.;

7) intensification of manifestations of cyberterrorism;

8) the spread of cybercrime;

9) critical dependence of the national information infrastructure on foreign manufacturers of high-tech products, the spread of the facts of inclusion in the software and hardware of hidden malicious functions;

10) increasing risks of man-made emergencies due to a decrease in the level of protection of critical information infrastructure of the state [3; 4].

Also worth noting is a well-defined system of cybersecurity measures. In Ukraine, such measures are quite broadly outlined in paragraph 4 "Priorities and directions of cyber security of Ukraine" of the Cyber Security Strategy of Ukraine [5]. Thus, in accordance with this Strategy, the fight against cybercrime will provide for the implementation in the prescribed manner, inter alia, the following measures:

1. Creation of an effective and convenient contact center for reporting cases of cybercrime and fraud in cyberspace, increasing the efficiency of responding to cybercrime by law enforcement agencies, in particular their regional units.

2. Improving procedural mechanisms for collecting evidence in electronic form relating to crime, improving the classification, methods, tools and technologies for the identification and recording of cybercrime, conducting expert research.

3. Introduction of blocking by operators and telecommunication providers of a certain (identified) information resource (information service) by a court decision.

4. Normalization of the procedure for making mandatory instructions for telecommunications operators and providers on urgent recording and further storage of computer data, storage of traffic data.

5. Settlement of the issue of the possibility of urgent procedural actions in real time with the use of electronic documents and electronic digital signature.

6. Implementation of the scheme (protocol) of coordination of law enforcement agencies in the fight against cybercrime.

7. Training of judges (investigative judges), investigators and prosecutors to work with evidence related to the crime obtained in electronic form, taking into account the specifics of cybercrime.

8. Introduction of a special procedure for removing information from telecommunications channels in the case of cybercrime investigations.

9. Advanced training of law enforcement officers [5].

Various indicators of implemented measures in the field of protection of computer and telecommunication networks from cyber-attacks and creating conditions for safe operation of cyberspace are evaluated and used to monitor and compare the state of cybersecurity in different countries in annual international rankings, the most authoritative of which is the Global Cybersecurity Index. Global Cybersecurity Index, GCI) and the National Cyber Security Index (NCSI). These cybersecurity indices are a kind of risk indicator for corporate, industrial and government information infrastructure due to the range of cyber threats.

According to the GCI-2018 rating, Ukraine took 54th place among 193 countries, rising over the last year by 5 positions [19, p. 121]. At the same time, experts noted: progressive steps in building a legal framework to guarantee the cybersecurity of the state; sustainability of government initiatives to increase cybersecurity in the field of ICT; a significant improvement in the cyber resilience of organizations over the past year, despite more than doubling targeted cyberattacks. However, if we compare Ukraine's performance in this ranking with, for example, post-Soviet countries, it becomes clear that many of them did a much better job of building cyber resilience, as they are significantly ahead of us in this ranking. Thus, Lithuania took 4th place in the overall ranking, Estonia - 5, Georgia - 18, the Russian Federation - 26, Kazakhstan - 40, Latvia - 44, Moldova - 53 and bypassed us in the GCI-2018 ranking [19, p. 121].

On June 7, 2016, the Decree of the President of Ukraine established the National Coordination Center for Cyber Security - a working body of the National Security and Defense Council. The Center consists of the head, secretary and other members of the Center. The head of the Center is the Secretary of the National Security and Defense Council. The Secretary of the Center is ex officio the head of the structural subdivision of the National Security and Defense Council, which is in charge of cybersecurity issues. Members of the Center are the First Deputy or Deputy Minister of Defense of Ukraine, Chief of the General Staff of the Armed Forces, Chairman of the Security Service of Ukraine, Head of the Foreign Intelligence Service of Ukraine, Head of the National Police of Ukraine, Head of the National Bank of Ukraine (by agreement). Intelligence Department of the Administration of the State Border Guard Service of Ukraine, Head of the State Service for Special Communications and Information Protection of Ukraine.

The Center should ensure coordination of the activities of national security and defense entities of Ukraine during the implementation of the Cyber Security Strategy of Ukraine, increase the efficiency of the public administration system in the formation and implementation of state policy in the field of cyber security. Therefore, analyzing its main tasks, I note that they can also be defined as areas of state cybersecurity policy. Such areas are:

1) generalization (implementation) of international experience in the field of cybersecurity, as our state, like all others, does not exist in isolation, but in close cooperation in various fields;

2) forecasting and identifying potential and real threats in the field of cybersecurity, which will help prevent them and facilitate the elimination of negative consequences;

3) setting priorities for attracting international technical assistance in the field of cybersecurity;

4) study of international experience in the creation and operation of national cybersecurity systems, its dissemination among organizations, institutions and establishments in accordance with its competence, monitoring of its implementation in Ukraine;

5) participation in ensuring the development and implementation by the subjects of guaranteeing cybersecurity of mechanisms for exchanging information necessary for the organization of response to cyber-attacks and cyber incidents, elimination of their factors and negative consequences [20].

On January 25, 2018, the Situational Center for Cyber Security was opened on the basis of the Department of Counterintelligence Protection of the State's Interests in the Sphere of Information Security of the Security Service of Ukraine. The key capabilities of the Center are a system for detecting and responding to cyber incidents and a laboratory for computer forensics. They will prevent cyberattacks, establish their origin, analyze to improve counteraction.

In Ukraine, the state of cybersecurity remains quite complex. Due to the fact that cybersecurity has not been addressed for a long time, we currently have high rates of Internet piracy, weak regulatory framework, outdated liability for cybercrime in the Criminal Code, weak data protection system of state importance, a large number of cyber-attacks and more. Recently, however, due to changes in the country and the entry into a new level of European development, cybersecurity has become perhaps the most pressing issue on which all government officials have focused. The development of cybersecurity in Ukraine has become a priority in public policy. At present, it is necessary to expand the regulatory framework, clearly structure it, avoiding conflicts in legislation. The Criminal Code of Ukraine in Chapter XVI needs changes and additions, it is necessary to include the concept of cybercrime and its types. Given that the cyber police is a fairly new structural unit of the Ministry of Internal Affairs of Ukraine, it is necessary to draw on the international experience of the relevant authorities of developed countries so that the work of cyber police was effective and coordinated. Ukraine is at the stage of establishing the highest European values, and the development of cybersecurity in its territory is one of the most pressing issues today.

Conclusions. The problem of defining and substantiating the theoretical foundations of the separation of cybersecurity as a subsystem of information security of Ukraine, according to the requirements of structural and functional analysis, requires the study and classification of information and cyber threats, elucidation of multi functionality and multidimensionality of the subject field of information and cyber security. and identifying objects in need of protection in relation to national, national, regional and global information and cyberspace.

An analysis of existing approaches to the definition of "cybersecurity" in scientific papers and current legislation shows that most definitions relate to the security of computer systems, telecommunications networks and information in them. In addition, the expediency of using the phrase "security status" instead of just security in the definition of cybersecurity has been proven. Taking into account the shortcomings of the definition of "cybersecurity" in the Law of Ukraine "On the basic principles of cybersecurity of Ukraine" proposed an author's version of the definition, free from redundant features and characteristics of cybersecurity.

Cybersecurity is a practical activity to protect systems, networks, programs, hardware and information data from digital attacks, which are aimed at accessing, modifying or destroying confidential information, interrupting business processes for personal gain.

Cybersecurity is the introduction of mechanisms to protect computer systems, networks, software and hardware, as well as information data from unauthorized access or damage to their hardware, software or electronic data.

Ukraine, like its international counterparts, is taking gradual steps to create a secure information society and ensure security at all levels of the cyber environment. Our state, in accordance with relevant laws and regulations, guarantees cybersecurity at all possible levels. The Government has developed special documents regulating activities in the field of cybersecurity - the Cyber Security Strategy of Ukraine, the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine".

One of the main state bodies operating in the field of cybersecurity in Ukraine is the National Security and Defense Council of Ukraine (NSDC). In accordance with the Constitution of Ukraine and in the manner prescribed by law, in general, the National Security and Defense Council coordinates and controls the activities of security and defense sector entities, including cybersecurity.

The monitoring of the level of cybersecurity of Ukraine in the world rankings and analysis of measures in the field of cyberspace protection showed that the problem of effective cybersecurity requires a comprehensive solution and requires coordinated action at national, regional and international levels to prevent, prepare, respond and repair incidents. private sector and civil society.

References

1. Mialkovskyi, D.V. (2019). Orhanizatsiino-pravovi mekhanizmy derzhavnoho upravlinnia mizhnarodnym spivrobitnytstvom Ukrainy u sferi kiberbezpeky [Organizational and legal mechanisms of state management of Ukraine's international cooperation in the field of cybersecurity]. Teoriia ta praktyka derzhavnoho upravlinnia – Theory and practice of public administration, 3, 216-226 [in Ukrainian].

2. Pysarenko V.P. (2019). Problemy kiberbezpeky v Ukraini [Problems of cybersecurity in Ukraine]. Ekonomika ta derzhava. Seriia: Derzhavne upravlinnia – Economy and state. Series: Public Administration, 4, 88-91 [in Ukrainian].

3. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. #2163-VIII [On the basic principles of cybersecurity of Ukraine: Law of Ukraine of 05.10.2017 №2163-VIII]. Retrieved from: http://zakon.rada.gov.ua/laws/show/2163-19 [in

Ukrainian].

4. Pro Stratehiiu natsionalnoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 06.05.2015 # 287/2015 [On the National Security Strategy of Ukraine: Decree of the President of Ukraine dated 06.05.2015 № 287/2015]. Retrieved from: http://zakon1.rada.gov.ua [in Ukrainian].

5. Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27.01.2016 r. «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 15.03.2016 r. # 96/2016 [Decision of the National Security and Defense Council of Ukraine dated 27.01.2016 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine dated 15.03.2016 № 96/2016]. Retrieved from: https://zakon.rada.gov.ua/laws/show/96/2016#Text [in Ukrainian].

6. NATO CCD CoE General Trends. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from: http://www.ccdcoe.org/8.html [in English].

7. Buriachok, V.L., Tolubko, V.B., Khoroshko, V.O., & Toliupa, S.V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt – Information and cybersecurity: socio-technical aspect. Kyiv: DUT, 288 s [in Ukrainian].

8. Dubov, D.V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva – Cyberspace as a new dimension of geopolitical rivalry. Kyiv: NISD, 328 s [in Ukrainian].

9. Dovhan, O.D., & Tarasiuk, A.V. (2020). Protydiia zahrozam kiberbezpetsi derzhavy na hlobalnomu rivni [Countering state cybersecurity threats at the global level]. Informatsiia i pravo – Information and law, 2, 85-98 [in Ukrainian].

10. Stets, V. (2019). Teoretyko-pravovi problemy vyznachennia sutnosti kiberbezpeky yak skladovoi informatsiinoi bezpeky [Theoretical and legal problems of defining the essence of cybersecurity as a component of information security]. Aktualni problemy derzhavnoho upravlinnia – Actual problems of public administration, 4, 24-28 [in Ukrainian].

11. Poniattia ta kryminolohichna kharakterystyka kibernetychnoi zlochynnosti [The concept and criminological characteristics of cybercrime]. Retrieved from: http://lib-net.com/content/9684_Ponyattya_ta_kriminologichna_harakteristika _kiberzlochinnosti.html [in Ukrainian].

12. Konventsiia pro kiberzlochynnist vid 23.11.2001 r. [Convention on Cybercrime of 23.11.2001]. Retrieved from: http://zakon0.rada.gov.ua/laws/show/994_575 [in Ukrainian].

13. Dodatkovyi protokol do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy vid 28.01.2003 r. [Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems of 28 January 2003]. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_687#Text [in Ukrainian].

14. Holina, V.V., & Holovkin, B.M. (2014). Kryminolohiia. Zahalna ta Osoblyva chastyny [Criminology. General and Special parts]. Kharkiv : Pravo, 513 s [in Ukrainian].

15. Butuzov, V.M. (2010). Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyi analiz) [Combating cybercrime in Ukraine (system-structural analysis)]. Kyiv : KYT, 408 s [in Ukrainian].

16. Markiv, S.I. Kiberzlochynnist. Nova kryminalna zahroza [Cybercrime. A new criminal threat]. Retrieved from: http://gurt.org.ua/articles/34602/ [in Ukrainian].

17. Bilenchuk, P.D., & Obikhod ,T.V. (2018). Kiberbezpeka i zasoby zapobihannia ta protydii kiberzlochynnosti y kiberteroryzmu [Cybersecurity and means to prevent and combat cybercrime and cyberterrorism]. Chasopys Kyivskoho universytetu prava – Journal of Kyiv University of Law, 3, 235-239 [in Ukrainian].

18. Ofitsiinyi sait Rady natsionalnoi bezpeky i oborony Ukrainy [Official site of the National Security and Defense Council of Ukraine]. Retrieved from: https://www.rnbo.gov.ua/ua/Diialnist/4658.html [in Ukrainian].

19. Trofymenko, O.H., Prokop, Yu.V., Lohinova, N.I., & Zaderaiko, O.V. (2019). Monitorynh rivnia kiberbezpeky Ukrainy u svitovykh reitynhakh [Monitoring the level of cybersecurity of Ukraine in world rankings]. Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information security of man, society, state, 3, 119-126 [in Ukrainian].

20. Polozhennia pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky vid 7 chervnia 2016 r. [Regulations on the National Coordination Center for Cyber Security of June 7, 2016]. Retrieved from: http://zakon2.rada.gov.ua/laws/show/242/2016.

VOL 1, No 61 (61) (2021)

The scientific heritage
(Budapest, Hungary)
The journal is registered and published in Hungary.
The journal publishes scientific studies, reports and reports about achievements in different scientific fields.
Journal is published in English, Hungarian, Polish, Russian, Ukrainian, German and French.
Articles are accepted each month.
Frequency: 24 issues per year.
Format - A4
ISSN 9215 — 0365

All articles are reviewed
Free access to the electronic version of journal
Edition of journal does not carry responsibility for the materials published in a journal.
Sending the article to the editorial the author confirms it's uniqueness and takes full responsibility for possible consequences for breaking copyright laws

«The scientific heritage»
Editorial board address: Budapest, Kossuth Lajos utca 84,1204
E-mail: public@tsh-journal.com
Web: www.tsh-journal.com