УДК 37:004:316.722.5

Бірець Костянтин Євгенійович

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВА СКЛАДОВА СИСТЕМИ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКИХ КРАЇН

Вінницький національний технічний університет

Анотація: *Стаття присвячена дослідженню правових і організаційних засад забезпечення кібернетичної безпеки ЄС у сучасних умовах розвитку інформаційного суспільства. Автор з'ясовує концептуальні підходи щодо забезпечення безпеки в європейському кіберпросторі і визначає перспективні напрямки удосконалення існуючого механізму забезпечення кібербезпеки в ЄС.*

Ключові слова: Європейський Союз, кібербезпека, кіберзагроза, мережева і інформаційна безпека, інформаційна інфраструктура.

Abstract: *The article is devoted to the study of the legal and organizational foundations of ensuring EU cyber security in modern conditions of information society development. The author elucidates conceptual approaches to ensuring security in European cyberspace and defines perspective directions of perfection of an existing cybersecurity mechanism in the EU.*

Keywords: European Union, cyber security, cyber threat, network and information security, information infrastructure.

Considering the current state and relevance of the problems in the field of telecommunications associated with the assessment and control of risks arising from the use of computers and computer networks, most countries in the world are implementing comprehensive measures to ensure national cybersecurity. These efforts are linked, above all, to the development and improvement of legal and regulatory acts, as well as the creation of institutional and governmental structures that regulate and are responsible for ensuring security in the cyber space. The problem of ensuring cyber security is a very important and complex issue, and the negligent attitude of the state to this issue can lead to unprecedented consequences. The European Union is also active in the field of cyber security. Today The European Union unites highly developed countries that exert a significant influence on international relations, setting norms and standards of behavior of states in the political, economic, social, informational and other spheres. Guaranteeing international information security and its component - cybersecurity - remains one of the strategic tasks of the EU, since the majority of political and economic and other spheres political and military conflicts in the world take place or are mirrored precisely in the in the virtual space. Investigating the issues of normative and organizational principles of cybersecurity The EU is gaining a remarkable sense, and its scientific understanding of the aggregate of transformations that take place in the dimensional and information sphere. Under these conditions it is important to Complex research of the European approach to the issue of security especially considering the European integration aspirations of Ukraine. Analysis of the latest studies and publications. Study of the state of scientific development of the problems of security of the EU cybersecurity issues has shown that at the present stage of the current stage, no special study of these issues has been conducted. was not carried out. However, certain aspects of such The activity of the EC was discussed in the scientific works of I. M. Zabara. I.M. Zabara, O.Y. Zaporozhets, V.K. Konakh, V.A. Lipkan, A.M. Orlean, Y.B. Tikhomirova, and others. Unresolved Early Problems. In spite of the presence of a large number studies in this area, the dynamic nature of the of infrastructure development in the area and in the information information sphere, as well as the spread of Cyberlocality requires new scientific developments and directions for the development of joint approaches in combating cyberthreats and other measures in the field of security protection. In 2001. The European Commission presented The first document titled "Meregeva and Information Security: A European Policy Approach European Policy Approach" (Network and Information Security Proposal for A European Policy Approach), which outlines a European approach to the problem of information security. The document is used the term "security and information security. information security", which is interpreted as the ability of the network or information system to prevent accidental or malicious events The actions that pose a threat to accessibility, authenticity, integrity and confidentiality of data stored or transmitted, as well as services provided via these networks and systems [1]. The European Partnership emphasizes that network and information security is already becoming a key factor in the development of the information society. First of

all, networks and information systems contain confidencial data and economically valuable information, which increases incentive for attacks. Attacks on information systems can be serious on a national scale. consequences, such as malfunctions in communication systems, leakage of confidencial information, etc. On 10 February 2004, the European Agency for Europe was founded. European Agency for the Development of Communication and Information Information Security (European Union Agency for Network and Information Security - ENISA). ENISA is one of the EU agencies that has been has set a specific deadline for completing their work: 2020 p. The agency has been operational since December 1, 2005, Is located in Iraklion, Crete, (Greece). The mission of ENISA is to improve the quality of the services and information provided by the organization. and information security in the European Union. The Agency promotes the development of a culture of information and security for the benefit of people, consumers, enterprises and public organizations in the EU, contributing to Uninterrupted functioning of the EU internal EU market. ENISA assists the European Commission, EU member countries and the private sector comply with European Commission and EU member countries and the private sector to ensure global and information security, including current and future EU, European Union legislation. ENISA is a center of expertise both for the member countries and for the EU institutions to obtain advice on issues related to networks and information information security. European Agency for Affairs network and information security closely takes with the European police office (Europol) and the European Center fight against cybercrime (European Cyber Criminal Center), as well as with others EU institutions, in particular: - European Agency for Reconstruction and Development law enforcement training (European Union Law Enforcement Training Agency, CEPOL); - Body of European regulators electronic communications (Body of the European Regulators of Electronic Communications, BEREC) [2].

- European Agency operational management of large-scale IT systems in the areas of freedom, security and of Justice (European Agency for the Operational management of large-scale IT systems in the area of freedom, security and justice, eu-LISA);

- (European Aviation Safety Agency, EASA). ENISA manages the European Cyber Europe program. This is a series of exercises from cyber incidents and crisis management situations at EU level for state and private sectors of member countries. Cyber Europe Exercises is a simulation large - scale incidents involving cybersecurity, which, as they increase, may become cyber crises. Exercises offer opportunities for the analysis of advanced technical measures with cybersecurity, solving problems related to crisis situations. Cyber Europe Exercises are rich scenarios real events developed European cybersecurity experts. Each of the exercises provides learning experience for participants [3]. In its activities, the ENISA Agency based on annual work plans / programs, which contain a list of key priorities and objectives and planned activities for implementation tasks. In work programs. Agencies are defined as strategic priorities:

- increasing ability European electronic networks to resist external influences;

- development of cooperation between EU member states in the field of network and information security;

- identification of new risks in the field of information security and formation mutual trust. In order to improve cooperation between judicial and other authorized bodies authorities, including the police and other specialized law enforcement agencies of EU member states in the field protection of information systems February 24, 2005 the Framework Decision of the Council of the EU 2005/222 / JHA on attacks on information a system that has set minimum rules on the definition of criminal offenses and sanctions in the field of attacks on information systems. The document states that the violation protection of information systems are obvious, in particular as a result of threats from the outside organized crime, and increase concerns about the possibility of terrorist attacks attempts to disrupt existing information systems part of the infrastructure that needs special protection of Member States. There should be measures are envisaged for cooperation between Member States to ensure effective action against attempts violation of information systems protection. Therefore, Member States should use the existing network of existing contact points listed in the Recommendation Council Directive 2001 / C 187/02 as regards paragraphs round-the-clock support service crimes in the field of high technology from 25 June 2001, providing round-the-clock support in the fight against high-tech crimes and for the exchange of information. Frames the decision provides that the intentional is illegal access to computer systems, including the data stored in them must be punished as a criminal offense [4]. In May 2007 by the European Commission presented the document "On the way to the general policies in the field of combating cybercrime " (Towards a general policy on the fight against cyber crime), which defines the term "Cybercrime" and highlights the main ones directions of EU policy in counteraction cybercrime [5]. According to the document, cybercrime - these are criminal acts committed with use electronic communication networks and information systems or against such networks and systems. This concept includes three categories crimes:

- traditional forms of crime (fraud and counterfeiting in electronic communications networks and information systems);

- publication of illegal content in electronic media (child pornography, materials with calls for racial hatred and etc.);

- specific crimes in electronic networks (attacks on information systems, hacking, etc.). It is important to note that politics European Commission in the field of counteraction cybercrime is implemented as follows main directions:

- participation in the rule-making process (development and adoption of international law documents in the field of combating cybercrime);

- international promotion cooperation of law enforcement agencies of EU member states (organization of scientific and practical conferences, seminars, trainings on issues countering cybercrime, creation round-the-clock contact points in EU member states, development of a training platform experts in the field of combating cybercrime and etc.);

- development of cooperation between public and private sectors in the field countering cybercrime, in particular cooperation between law enforcement and private companies;

- encouraging the signing by EU member states and other countries of the Convention on cybercrime in 2001, etc [6 ; p 39].

It was published in March 2009 Communication from the European Commission "Protection Europe from large-scale cyber attacks and destruction: increased preparedness, Security and Sustainability "(Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience), in which identified the main challenges / problems that need an immediate EU response as well outlines the main measures required for strengthening European security and capabilities critical information infrastructure resist external influences [7]. According to this document, today major information security challenges EU infrastructures are:

- uncoordinated national approaches to security of information infrastructures that reduces the effectiveness of national measures;

- Absence at European level public-private partnerships sectors;

- the EU's limited capacity for early security warning and response incidents caused by uneven development incident monitoring and notification systems in member countries, underdeveloped interstate cooperation and exchange information on these issues;

- lack of international consensus on priorities in the implementation of protection policy critical information infrastructure. February 7, 2013 by the European Commission the Cyber Security Strategy was approved "Open, reliable and safe cyberspace "(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace). This document is the EU's comprehensive vision of how best prevent and eliminate cyber threats. The Strategy notes that incidents related to cybersecurity are growing more and more often, become more complex and do not know borders. These incidents can be serious damage to the security and economy of states. For prevention and disposal of cyber threats it is recommended to develop interstate cooperation in this field. The document also states that previous efforts of the European Commission and individual EU member states were too fragmented to solve problems on cybersecurity. It is the Strategy cybersecurity will help further European values of freedom and democracy, will encourage the safe growth of digital economy. Provided in the document are specific measures aimed at strengthening cyber resilience information systems, reduction of cybercrime and strengthening the EU's international policy on cybersecurity and cyber defense. The strategy formulates the EU's vision for

Cybersecurity with five priorities:

1. Achieving cyber resilience.

2. Significant reduction of cybercrime.

3. Development of cyber defense policy, related to the Common Security Policy and defense.

4. Development of production and technological resources for cybersecurity.

5. Creating a coherent international cyberspace policies for the EU and promotion core values of the EU.

The Strategy states that "International cyberspace policy in the EU promotes respect for the fundamental values of the EU,determines the norms of responsible behavior, advocates the application of existing international cyberspace documents as well assists non-EU countries develop cybersecurity capabilities, and also promote international cooperation in countering cybercrime [8]. Immediately after the publication of the Strategy cybersecurity work has begun on relevant directive. It is important to emphasize that this document was not developed separately from other areas, and as part of the Strategy Digital Single Market Strategy), on the one hand, and part of the European Security Agenda (European Agenda on Security), on the other [9]. Strategy and Agenda were published in the spring of 2015, in July 2016 The European Commission presented "Additional measures to promote the development of the industry cyber defense ", and on July 6, 2016 it was approved EU directive on security measures high overall level of network security and information systems throughout the Union (Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive) [10]. This Directive lays down uniform rules and cybersecurity requirements for all EU countries, but reserves the right to each member state take their own measures to implement the rules of this Directive into national law. To achieve the purpose of the Directive (providing a higher level of network and information security within the EU) is necessary take action in three main areas:

- increase the capacity of the system cybersecurity at the national level;

- raise the level of European cooperation;

- introduce risk management and oblige to report cyber incidents basic service operators and providers digital services. To increase capacity cybersecurity at the national level EU member states must develop a national one network and information security strategy (which should include strategic objectives, priorities and state basis, measures for preparing for and responding to cyber incidents and recovery after them, the principles of public-private partnership, educational program, training and enhancement activities awareness, research plan, risk assessment and management plan, list stakeholders responsible for implementation strategy), identify one or more public bodies that will be responsible for implementation Directives, create one or more teams responding to computer emergencies. Among the main threats to the national national strategies have been developed for cyberspace EU member states determine:

- Cyber espionage and military action, which carried out with the support or with the knowledge of the state. All technologically advanced countries and corporations are subject to cyber espionage, which aims to seize state or industrial secrets, personal data or other valuable information.

- Use of the Internet in terrorist purposes. Terrorist groups use the Internet for propaganda purposes, fundraising and recruiting supporters.

- Cybercrime: kidnapping personal data and money laundering, obtained illegally. Attackers sell information about bank numbers cards, passwords from computer servers and malware. Accordingly, national legislation countries, as a rule, regulate issues:

- protection of personal data (Netherlands, Estonia, Sweden, Finland, Spain);

- protection of e-commerce and security electronic transactions and payments instruments (Poland Estonia, Italy);

- protection of important objects infrastructure and information systems (France) [11, p.3]

September 13, 2017. European Commission presented the document "Stability, restraint and protection: creating strong cybersecurity for EU "(Resilience, Deterrence and Defense: Building strong cybersecurity for the EU), in which it is stated that cybersecurity is crucial importance for the prosperity and security of member countries. If you do not take action cybersecurity, the risk of threats will increase according to digital transformations. Risk of politically motivated attacks on civilian targets and military shortcomings cybersecurity further exacerbates the risk. Though Member States remain responsible for national security, scale and the cross-border nature of cyber threats is created incentives for Member States to develop and support for more powerful national opportunities for EU cybersecurity in general. Strong cyber resilience requires collective and large-scale approach. It needs to be more reliable and efficient structure to promote cybersecurity and responding to cyberattacks in member countries, and also in EU institutions and bodies [12]. The European Commission emphasizes that full implementation by all member countries The NIS directives allow for improved resilience use of capacity building national cybersecurity; promote the best cooperation between Member States; and demand from the private sector services effective risk management measures and report serious incidents national authorities. On raising the European level special networks are created for cooperation and the Cooperation Group that will provide planning, management, information exchange and

preparation of cybersecurity reports EU member states. legislative novelties are very important concerning the working conditions of the base operators services and digital service providers. Definition of "basic service operators" each and gives itself, but on the basis of common for all EU criteria:

- enterprise (regardless of form property) provides a service that is basic to support for critical socio-economic activity;

- provision of services use of network or information systems;

- Security breaches will be significant destructive impact on the provision of basic services. In possibly the following sectors:

- energy: electricity, oil, gas;

- transport: air, rail, water, road;

- banks, credit institutions;

- financial market infrastructure: exchanges, central counterparties;

- health care facilities;

- drinking water supply;

- digital infrastructure: exchange points Internet traffic, system providers domain names, service providers, registries top-level domain names.

Under the digital service providers that are covered by this Directive mind online trading platforms, cloud service providers, search systems. Such enterprises must take necessary (technical and organizational) measures in order to prevent risks cyber incidents, provide networking and information security (according to potential risks), as appropriate respond to cyber incidents in order minimize damage, report competent authorities on cyber incidents. Directive as well compliance with international is expected standards by these enterprises, constant monitoring, audit and testing. The plausible fact is that the accumulation large arrays of information and their operation, provision of electronic services, and initial connection in the European Union, in the coming years, more than a billion devices to Electronic networking provides not only benefits but and has a negative impact - the number increases, volume, scope and diversity of cybernetic threats. Understanding the essence of threats and taking into account current situation, the European Commission in 2017 offered her vision of a new, challenged sometimes, European cybernetic architecture security and its legal support. To achieve this goal, the European the commission proposed new tools including the establishment of the European Agency for Reconstruction and Development Cybersecurity and the European Research Center and cybersecurity competencies to help Member States to protect themselves from such cyber attacks

Conclusions. The analysis of tendencies inEU cyber policy security, given the strengthening of cybersecuritycomponents in the national security system EU member states, allowed the following

conclusions:

- At the same time, the advantages of the modern digital world and information development technologies have led to new threats for the national security of European countries. Modern information technology is transforming information systems are extremely vulnerable to implement cyber threats objects. IN under these conditions, the main task of European, and other countries are taking action that will allow to reduce in principle (and in some places - to prevent completely) the negative consequences of cyberattacks. An important role in the development of unified approaches to cybernetic security as a component of national security European countries is played by the European Union.

- The European Union is active upgrades its own security sectors in cyberspace according to the challenges modernity. This process occurs by: streamlining the regulatory framework that has ensure the integrity of public policy in in this area; development of European guidelines principles for sustainability and stability of the Internet and their promotion in the international arena; increasing the number units involved in the cybersecurity system; strengthening control over the national information space; strengthening protective mechanisms for critical information of EU infrastructure; carrying out pan - European exercises and research with problems of security incidents in the network Internet; strengthening cooperation between the state and

private sectors; creation of European a forum for the exchange of information between member countries; creation of a European system early warning of cyber threats, etc.

- Given the significant progress and the experience of the European Union in the development and improving the provisioning mechanism cybersecurity of European countries, Ukraine must become an active participant in these security processes. On the one hand, given integration aspirations of Ukraine, it will contribute improving the image of the state, and on the other - to influence the formation of organizational and legal basics of national cybersecurity Of Ukraine. In the conditions of development of Ukraine national legislation in the field cyber security can be effective taking into account the experience of the EU, promising future plans, programs and projects as well participation in joint European projects with cyber security. In terms hybrid warfare and the introduction of practices e-government cyber issues security for Ukraine should be the focus public policy.

- Strengthening the cyber component in EU state security systems stipulates the need for order as soon as possible policy of the Ukrainian state in the field cybersecurity. The key in this the process should be to define their goals and methods achievements (primarily short- and medium-term). Properly designed strategy of foreign policy of Ukraine on cooperation with The EU in the field of cyber security, of course, will lead to a mutually beneficial partnership in solving problematic issues regarding ensuring national interests in the field cybersecurity.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Network and information security: proposal for a european policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52001DC0298 (дата звернення 01.06.2018).
2. About ENISA / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa (дата звернення 01.06.2018).
3. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (дата звернення 01.06.2018).
4. Council framework decision 2005/222/JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32005F0222 (дата звернення 03.06.2018).
5. Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=LEGISSUM%3Al14560 (дата звернення 02.06.2018).
6. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин. 2009. Вип. 87, ч. II. С. 36-45.
7. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience»: adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52009DC0149 (дата звернення 04.06.2018)
8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity (дата звернення 03.06.2018).
9. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення 04.06.2018).
10. Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive: Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 / Official Journal of the European Union. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення 05.06.2018).
11. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. Київ: Інфоцентр, Європейський інформаційно-дослідницький центр, Лабораторія законодавчих ініціатив, 2016. 37 с. 12. Resilience, Deterrence

and Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=JOIN:2017:0450:FIN (дата звернення 05.06.2018).