INSTITUTIONAL AND LEGAL MECHANISMS FOR IMPLEMENTATION STATE POLICY IN THE FIELD OF INFORMATION SECURITY: EXPERIENCE OF EU COUNTRIES

Svitlana Paliy[1]

[1]*Chief Specialist of the Department of Organization of the Educational Process of Distance Learning, Interregional Academy of Personnel Management, Kyiv, Ukraine, e-mail: PaliySvitlana@ukr.net, ORCID: https://orcid.org/0000-0002-9265-6407*

Abstract. *The article analyzes the features of institutional and legal mechanisms for implementation state policy in the field of information security in the EU. It is determined that the Safer Internet Program is a tool for implementation the Safer Internet Centers policy, which expands the rights and protection of children / others online by implementing awareness-raising initiatives and combating illegal (destructive) content and behavior. It is noted that a significant element of the institutional and legal mechanism for ensuring the state information policy of European countries is the involvement of civil society institutions in the process of ensuring the security of Internet use. It is noted that the fight against cybercrime in the European Union is endowed with a powerful institutional and legal mechanism. In particular, the European Commission has developed «anti-cyber measures», which were formulated in the Communication «Towards a common policy on cybercrime» (May 22, 2007). The normative act defines the main elements of this policy: the development of cooperation between law enforcement agencies, public-private partnership and international cooperation.*

It is concluded that the institutional mechanism for combating cybercrime in the European Union, along with the institutions of the European Community, includes two main specialized agencies – Europol and Eurojust.

Keywords: *institutional and legal mechanisms, state policy in the field of information security, EU, state of the public data protection sector, awareness raising mechanisms.*

JEL Classification: F52, F68.

Formulas: 0; fig.: 0; tabl.: 0; bibl.: 19.

Introduction. Ensuring state information security policy in the European Union is characterized by hierarchy. Thus, the European Commission, the Council of Europe and the European Parliament are responsible for the effectiveness of institutional regulation. In turn, the latter exercise their powers through their delegation to responsible sub-institutions.

As a result, all 27 member states of the European Community currently have Safer Internet Centers, which are responsible for ensuring the proper use of the Internet and mobile networks by children and the public [1].

These centers are divided into separate types: there are information centers (the purpose is to disseminate information materials, conduct campaigns and information interviews with children, parents, educators and teachers to raise awareness of online risks and ways to ensure safety on the Internet); helplines (personal counseling of children, parents to ensure online safety); hotlines (accept reports of illegal content on the Internet, conduct a check on them to identify their origin, based on which the law enforcement agencies of the country and Internet providers are informed to remove this content) [2, p. 21-22].

All the above highlights the need to study the best European experience in the formation of public policy in the field of information security, as well as, on this basis, the development of proposals for its effective reform in Ukraine.

Literature Review. Note that in most studies of authors such as: V.L. Buryachka, Yu.V. Bogdanovicha, P.O. Balashova, S.V. Kavuna, S.V. Kazmirchuka, O. G. Korchenka, V.O. Horoshka information security stands out as an integral element of national security, as well as an integral qualitative parameter and a characteristic indicator of the protection of the population and the state as a whole. This, in turn, highlights the importance of proper scientific substantiation of institutional and legal mechanisms for the implementation of state policy in the field of information security in the EU.

Aims – to determine the features of institutional and legal mechanisms for the implementation of state policy in the field of information security in the EU.

Methods. The methodological basis of the study is formed on the use of a number of interrelated general and special methods (systemic, historical-retrospective, comparative, structural-functional, analysis and synthesis, generalization and systematization, induction and deduction, unity of whole and part, problem and prognostic analysis).

Results. I would like to note that the information centers and helplines of the EU Safe Internet Center are merged into another supranational body – the European network of information centers "Insafe". The aim of the campaign is close cooperation between partners and other participants in order to strengthen the standards of awareness and security of the Internet, as well as to support the development of information literacy in the member states of the European Union [3].

In turn, the legal basis for the implementation of these provisions is formed in the European Community through the Recommendations on the Protection of Minors and Human Dignity 98/560/EC of 24.09.1998 and 2006/952 EC of 20.12.2006, which implemented a set of measures aimed at protecting children and individuals from destructive information in the media and the Internet. Implementation is carried out by the Member States of the European Union, the European Commission and other subjects of state control [4].

Separately, the Safer Internet Program is a tool for implementing the Safer Internet Centers policy, which expands the rights and protection of children / others online by implementing awareness-raising initiatives and combating illegal (destructive) content and behavior. The general mechanism of the program is designed to increase the uniqueness and security of the Internet in European countries.

It is important to note that the program «Safe Internet» provides for the implementation of such activities as: funding targeted projects aimed at creating a safe online environment; support for Safe Internet Day; organization of the Safe Internet Forum; stimulation and support of corporate regulation.

For example, under the Safer Internet Program Plus 2013-2020, € 55 million has been allocated to work in the following areas: public awareness of safe Internet use; creation of national contact centers (hotlines) to collect reports of citizens about

illegal and harmful information on the network; approval of self-regulation initiatives; encouraging children to participate in creating a safe Internet network; collecting data on the use of new technologies and related risks through research [5].

The European Union will regulate the procedure for implementing the Safer Internet program through targeted projects at national and European levels aimed at creating a secure online environment. As part of the institutional and legal support, there are FIVES projects (development of criminal investigations); ROBERT (study of deviant behavior online and factors of insecurity of people on the Internet) [6, p. 11].

At the same time, the Council of Europe established the International Association of Internet Hotlines (1999) to support state regulation of information security. Its members are all member states of the European Union. The Association represents the interests and coordinates the activities of the global network of Internet hotlines, creating a mechanism to combat illegal content in order to make the Internet a secure network. It is estimated that the average monthly rate of illegal Internet content detected by the Association is more than 30 thousand cases [7].

It should be noted that an indicative element of the institutional and legal mechanism for ensuring the state information policy of European countries is the involvement of civil society institutions in the process of ensuring the security of Internet use. Through a joint initiative of the European Commission and the European Parliament, the European Alliance for Child Safety Online was established in 2011, bringing together organizations to protect the rights of children (and others). The Alliance's responsibilities include developing and providing guidance to national, European and international decision-makers, including proposals for future Internet governance management [8].

Another important government action is the European Parliament's initiative to establish a Safer Internet Forum (2004). It is an annual conference on Internet security that brings together industry, law enforcement, child protection organizations and senior policymakers. The forum has an international character, because its participants, in addition to European countries, are Australia and the United States. The forum discusses such issues as: security of persons and information announced on mobile phones, the fight against illegal content and illegal behavior, mechanisms to raise awareness, etc. [9].

In addition, the European Community provides protection against the negative information impact of computer game users. The Council of the EU adopted Decision 2002 / C 65/02 on the protection of users, namely young people, by labeling a specific video game and a computer game according to age group (01.03.2002). The document draws attention to the diversity of game content, its focus on different age groups; Concern has been expressed about the possible harmful effects of content on the psyche of minors. To solve the problem, the method of age classification and appropriate labeling of computer and video games is used in order for the buyer to always have an idea of the content of the product, as well as to create mechanisms to protect children from harmful content [10].

As a control and supervisory method for monitoring the implementation of this institutional initiative, the European Commission provided information on the state of the public data protection sector (Notification dated 22.04.2008). The report notes that countries such as Cyprus, Luxembourg, Romania and Slovenia have not introduced the Pan-European Game Information age rating system (PEGI) as a voluntary system of self-regulation in this area [11].

Given the fact that the PEGI system is not accepted by the European Community (Nielsen Games survey showed that only 60% of respondents are aware of the European classification system and only 50% of parents consider the system useful when buying video games), some countries have changed the institutional and legal policy. security. For example, the German Bundesrat established the Common Agency for Youth Protection on the Internet. In addition, in Ireland, the user of the game has the right to call the 24-hour hotline (for Q&A), and Latvia arbitrarily sets strict requirements for the use and distribution of games at the government level [12].

It is also worth noting that the fight against cybercrime in the European Union is endowed with a powerful institutional and legal mechanism. In particular, the European Commission (in cooperation with the Member States and the institutions of the European Community) has developed «anti-cyber measures», which it formulated in the Communication «Towards a common policy on cybercrime» (22.05.2007). The normative act defines the main elements of this policy: the development of cooperation between law enforcement agencies, public-private partnership and international cooperation [13].

In turn, the European Commission proposes a set of measures to combat cybercrime, including the launch of operational cooperation between national law enforcement agencies, increased financial support for initiatives to train national law enforcement agencies to investigate cybercrime, support research to combat cybercrime, cybercrime, raising awareness of the dangers of cybercrime, implementing measures to prevent and counter coordinated and large-scale attacks on the information structure [14].

The European Commission has also stepped up dialogue with the private sector. From a political and practical point of view, its participation in combating cybercrime is crucial – because this sector controls most of the information infrastructure. Operational cooperation between the police and private operators was approved by two memoranda of the Council of Justice – in 2008 and 2010, respectively (are the leading and current).

In addition, the European Commission has set up a separate institutional body, the European Training Platform on Cybercrime Investments, with Europol, Sipol, Member States, civil society institutions and the private sector. In addition, the European Commission has launched the European alert platform for Internet-related offenses, together with Europol and the Member States of the European Union. This system allows you to combine information about cybercrime committed in different European countries, in order to coordinate the investigation and increase its efficiency [15].

Discussion. Continuing the analysis of theoretical and practical aspects of building of institutional and legal mechanisms of implementation state policy in the field of information security in the EU, I note that some authors, such as M.

Wittman and N. Mattord note that information security policy is a set of legal, organizational and technical measures, aimed at the formation and use of technological, infrastructural and information resources for the protection of information of national importance, as well as the rights and legitimate interests of entities involved in information relations [16, p. 38].

In my opinion, the state policy of information security is the activity of state and legal institutions to manage real and potential threats and dangers in order to meet the information needs of man and citizen, as well as the realization of national interests.

V. Nikitin notes that an effective state policy in the information sphere, including in the aspect of information security, largely depends on the correct choice of priorities in the organizational and legal solution of these problems, scientifically sound development of adequate models and approaches to their solution. .

However, I note that national security significantly depends on ensuring the information security of the country, the elements of which are the totality of information, means of its production, processing and storage, information infrastructure, entities collecting, generating, disseminating and using information, and regulatory system emerging relationships .

Conclusion. Thus, the article argues that actions against private and public IT systems in EU member states have given the problem a new dimension, demonstrating that cybercrime is a potential new economic, political and military weapon. This problem, therefore, can be considered an official confirmation of the threat of using information weapons. The European Strategy of 2003, in turn, only indirectly indicates that «in this area further work is needed to develop a comprehensive European approach, raise awareness and strengthen international cooperation» [17; 18].

References:

1. Safer Internet Centres : European Commision, Shaping Europe's Digital Future. Retrieved from: https://ec.europa.eu/digital-single-market/en/safer-internet-centres
2. European Union, Marilyn J. Raisch : American Society of International Law, 2014. – 32 p.
3. Insafe and INHOPE, BIK Portal. Retrieved from: https://www.betterinternetforkids.eu/policy/insafe-inhope
4. Protection of minors and human dignity in audiovisual and information services, 2006 : Summary of EU legislation. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24030a
5. Safer Internet Plus, European Economic Area, EFTA. Retrieved from: https://www.efta.int/eea/eu-programmes/safer-internet-plus
6. Best Practice Manual for Forensic Image and Video Enhancement, ENFSI, 2018Review. 28 p. pp. 11-12
7. International Association of Internet Hotlines: Overall Information. Retrieved from: https://www.developmentaid.org/#!/organizations/view/69681/inhope-international-association-of-internet-hotlines
8. eNACSO - The European NGO Alliance for Child Safety Online : European Economic and Social Committee, 24.10.2011. Retrieved from: https://www.eesc.europa.eu/en/documents/enacso-european-ngo-alliance-child-safety-online
9. Safer Internet Forum : Shaping Europe's Digital Future, European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/safer-internet-forum
10.Council Resolution on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group : 1.03.2002, Council of Europe, Official

Journal of the European Communities. Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:065:0002:0002:EN:PDF
11.Protection of video game users : Eurocommission, 22.04.2008. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aco0002
12.EU Law by Josephine Steiner and Lorna Woods : Oxford University Press, 753 p.
13.Communication from the Commission to the European Parliament, The Council and The Committee of Regions : Commission of the European Communities, Brussels, Belgium, 22. 05. 2007. Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF
14.Cybercrime: new survey shows Europeans feel better informed but remain concerned : European Commission, Press Release, 29.01.2020. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_143
15.European Cybercrime Training and Education Group : ECTEG, Europe, Official Web-Site. Retrieved from : https://www.ecteg.eu
16. Turchak A.V. Mehanizmi zabezpechennja informacijnoï bezpeki jak skladovoï derzhavnoï bezpeki Ukraïni. Disertacija na zdobuttja naukovogo stupenja kandidata nauk z derzhavnogo upravlinnja za special'nistju 25.00.02 – mehanizmi derzhavnogo upravlinnja. – Institut pidgotovki kadriv derzhavnoï sluzhbi zajnjatosti Ukraïni. Kiïv, 2020., 229 s.
17.Cybersecurity: current challenges and Inria`s research directions, by S. Kremer, L. Mé, D. Rémy and V. Roca. (2019). 170 p.
18.Romanenko Y.O Zhukova I.V. V Ukraïni znovu perepisali viborchij kodeks. Aktual'ni problemi rozvitku upravlins'kih sistem: dosvid, tendenciï, perspektivi: materiali shhorichn. nauk.-prakt. konf. 26 bereznja 2020 r. Kiïv. Harkivs'kij regional'nij institut derzhavnogo upravlinnja NADU pri Prezidentovi Ukraïni, 2020. Retrieved from: http://www.kbuapa.kharkov.ua/e-book/conf/2020-1/doc/1/1-1.pdf

Received: October 28, 2020
Approved: November 30, 2020