DOI: 10.5604/01.3001.0015.6890

THE PROBLEM OF LEGAL REGULATION OF THE SECURITY OF A PERSON, SOCIETY, STATE IN THE FORMATION OF THE INFORMATION SOCIETY IN UKRAINE

Anatolii Marushchak

National Academy of Security Service of Ukraine
Maksymovycha street 22, Kyiv
ORCID: 0000-0003-0069-3727
amarushchak@ukr.net

Stanislav Petrov

National Academy of Security Service of Ukraine
Maksymovycha street 22, Kyiv
ORCID: 0000-0001-7786-4657
kibpetrov@gmail.com

Mykola Romanov

Department of Political Science and National Security
National University of Ostroh Academy
Seminarska street 2, Ostroh
ORCID: 0000-0002-1086-9485
mykola.romanov@oa.edu.ua, dir@oa.edu.ua

Oksana Balashova

Department of Political Science and National Security
National University of Ostroh Academy
Seminarska street 2, Ostroh
Rivne Region, 35800
ORCID: 0000-0002-9200-9808
oksana.balashova@oa.edu.ua

Abstract

In this article a scientific hypothesis is proposed, dividing the subject of legal regulation of the security of a person, society and state into three components: information security, the security of information with limited access and cybersecurity. Legal regulation that relates to the field of information security is aimed at the following: creating a legal framework to provide security for information with limited access, as well as providing access to necessary information, etc. Making regulations to provide cybersecurity involves the detection of, prevention of and counteraction against real and potential threats to parts of the critical information infrastructure. While ensuring the information security of a person, society and state, the dispositive method of legal regulation predominates. However, in this study, we discovered a need to imperatively strengthen the security of a person, society and state by creating new legislation to make, in some cases, the spread of disinformation a criminal offence. Legal regulation of the security of restricted information is carried out using the imperative method of legal regulation, and the dispositive method of legal regulation in the circulation of information with limited access is applied when collecting and disseminating necessary information publicly. Providing cybersecurity in the public domain is done by the imperative method of legal regulation, although for the regulation of public-private partnership issues, it is concluded that there is a need for an exclusively dispositive method of legal regulation.

Key words: *Information Security, Cybersecurity, the Security of Rstricted Information, Legal Regulation, Method, Information Law*

INTRODUCTION.

One of the principles of information society development in Ukraine is free access to information and knowledge, except for the restrictions established by law. Our state declares and adheres to the constitutional principles of freedom of speech and the right to have free access to information.

The subject of regulation of information law involves the circulation of information, in particular, its creation, reception, collection, storage, protection, usage, dissemination, etc. The relevant sources of information law are the Laws of Ukraine “On Information”, “On Access to Public Information”, “On Public Appeals”, “On Printed Media (Press) in Ukraine”, “On Television and Radio Broadcasting”, “On Information Agencies”, “On the National Archive Fund and Archives”, “On Libraries and Librarianship”, “On State Statistics”, “On State Secrets”, “On Access to Judicial Decisions”, “On Electronic Documents and Electronic Documents Circulation”, “On Protection of Information in Automated Systems”, “On Cinematography”, “On Scientific and Technical Information”, “On the National Informatisation Program”, “On Mandatory Copy of Documents”, “On the Procedure for Covering Activities of Bodies of State Power and Local Self-Government by Mass Media in Ukraine”, “On Advertising”, “On the System of Public Television and Radio Broadcasting of Ukraine” and “On Main Principles of Maintaining Cybersecurity of Ukraine”, etc.

Most legal studies refer to the classical methods of legal regulation: the dispositive and imperative methods. R. A. Kaliuzhnyi and A. H. Martseniuk (2008) updated the

discussion on the subject and methods of information law. A team of scientists led by M. Ya. Shvets, R. A. Kaliuzhnyi, and V. P. Melnyk (2009) attempted to systematise the information law of Ukraine on a single methodological basis. The methodological foundations of information law in Ukraine were also presented by A. Marushchak (2011).

It was I. V. Panova (2011) who laid the foundation for research that would help develop the information law system of Ukraine. In her works, L. P. Kovalenko (2014) proposes considering, as a means of creating information law, the possibility of using all the methods of influencing public relationships already fixed in the norms of this field. Their use would make it possible to create the proper environment for the realisation and protection of citizens' rights in the information sphere and normal functioning of the information society. However, these authors do not dwell on the exact means of applying such techniques in the modern information society.

METHODS

This study employed the theoretical methods of analysis, synthesis and comparison. In particular, it involved an analysis of domestic legislation, as well as an examination of the initiatives of the European Union in the information sphere, aimed at controlling relevant matters to ensure the security of a person, society and state. The comparative legal method was used when conducting a comparative study of Ukrainian and European legislation.

Analysis of the empirical foundations of the study, namely the regulative acts of Ukraine, the practice of the relevant public authorities, scientific papers, etc. provided an opportunity to formulate a research hypothesis. Regarding the problem of the protection of legal regulation of the security of a person, society, state in the formation of the information society in Ukraine, we also set up a provisional hypothesis that the normalisation of public relationships in the information sphere depends on the types of information and legal status of the entities entering into legal relationships.

The main methodological approach to the study of legal regulation of security of the individual, society, state in the formation of the information society in Ukraine has been based on the fact that current public information matters are gaining further development compared to paper resources. Among them are the new types of relationships, including information (digitalisation) of public life, activities in the field of telecommunications, state policy in the field of electronic communications and radio frequency spectrum, geospatial data, etc.

Considering the above, both theoretical and practical problems were solved at each stage of research on the basis of the theory of cognition by applying the dialectical method of studying reality in its contradictions, integrity and development. The use of the dialectical method in this study has determined the disclosure of phenomena and processes that occur in the information sphere, in their movement, development and change. This method has revealed the causal relationships, shortcomings and

inconsistencies of legal regulation. The issues of improving the legal regulation of various cooperation types arising in relation to the security of the individual, society, state in Ukraine have been revealed with the use of the legal analogies method.

With the use of these methods, we have revealed patterns and positive and negative experiences of relevant information activities. The set of these methods has given the opportunity to achieve the goal of the study, solving the problem of formulating the content and features of the basic concepts and determining the nature of the legal regulation of certain security matters. In particular, we have introduced in Ukraine the organisational and legal mechanisms aimed at forming an effective cyber security system in accordance with the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"; raised the issue of human rights and established grounds for their restriction only in accordance with law and in exceptional cases. It has been determined that such cases should include the fight against terrorism in cyberspace, such as disruptions in the operation of process control information systems in critical infrastructure. That is why the formulation of long-term legislation in order to improve the protection of the interests of the individual, society and the state in Ukraine should take into account international democratic standards in this area, in particular the requirements of the Convention on Cybercrime.

In this study, the works of specialists in the field of information law were analysed, first of all, the work of L. P. Kovalenko (2014) on this subject and the methods used for determining the information law of Ukraine. Using the method of system synthesis, the definitions given by him were compared with the provisions of the legislation of Ukraine, revealing the specific properties of legal regulation for the security of a person, society and state in Ukraine.

The work of I. Panova on the tendencies in the development of the information law system of Ukraine was also investigated in detail, taking into account the subject of this paper (Panova, 2011). To compare the domestic experience of legal regulation with European approaches, the works of D. Frau-Meigs, B. O'Neil, V. Tome, A. Soriano (2017) on digital citizenship education and C. Wardle and H. Derakhshan (2017) on information disorder were considered.

In the course of this study, national and international legal acts were developed, among which are important acts such as the Convention on Cybercrime of the Council of Europe[1], the Law of Ukraine "On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015"[2], the Law of Ukraine "On State Secrets"[3], the Law of Ukraine "On Information"[4], as well as other regulatory legal acts.

[1] Conventions of Council of Europe about Cybercrime from Nov. 21, 2011 (2011). [E-Resource]. Available at: http://zakon4.rada.gov.ua/laws/show/994_575.

[2] Main Foundations for Development of Informational Society in Ukraine for 2007-2015 (2007). Bulletin of Verkhovna Rada of Ukraine, 12. P. 102.

[3] Law of Ukraine "On State Secret" from April 19, 1994. Bulletin of Verkhovna Rada of Ukraine, 16. P. 93.

[4] Law of Ukraine "On Information" from December 01, 1992. Bulletin of Verkhovna Rada of Ukraine, 48. P. 650.

DISCUSSION

1. A METHODOLOGICAL APPROACH TO THE SUBJECT OF THE LEGAL REGULATION OF THE PROBLEM OF INFORMATION SECURITY

In the face of external aggression against Ukraine, there arises a scientific and practical problem of how to define the boundaries of the regulation of the issues regarding the security of a person, society, and state in the information sphere. Calling the subject of our research «the security of a person, society and state in the information sphere» was chosen not by chance, but with the following considerations in mind. Firstly, recent legislation of Ukraine is moving towards a distinction between «information security» and «cybersecurity». This is not simply the inherent classical approach used to provide the security of restricted information.

The definition of «information security», as expressed in the Law of Ukraine "On the Basic Principles for the Development of an Information-Oriented Society in Ukraine for 2007–2015", is all-encompassing, as it was considered a way to protect the vital interests of a person, society and state from harm which can be inflicted by:

the use of incomplete, untimely and untrue information;

the impact of negative information;

the negative effects that can be produced using information technology;

the unauthorised dissemination or use of information, as well as taking information out of context, disclosing confidential information or depriving access to information.

These things have been prevented.[5] In 2007, a definition of «information security» included the issues of information security (information resources), the security of information space and the security of the functioning of the information and telecommunication infrastructure [Marushchak, 2013].

Today, however, the concept of "information security" acquires another, narrower meaning. Having analysed, for example, item 4.11 of the National Security Strategy of Ukraine, regarding the priorities of providing information security, we understand that it concerns "*the counteraction to information operations against Ukraine, used to manipulate public consciousness and disseminate distorted information, as well as to protect national values and strengthen the unity of Ukrainian society. It also involves the development and implementation of coordinated information policies of public authorities, the identification of Ukrainian information space entities created and/or used by Russia to wage an information war against Ukraine, as well as the creation and development of institutions responsible for information and psychological security, taking into account the practices of NATO member states*", etc. (Shvets et al., 2009) Thus, information security covers the processes and communication that take place in the information space of the state. A similar approach is utilised in the Doctrine of Information Security of Ukraine, which defines Ukraine's national interests in

[5] Main Foundations for Development of Informational Society in Ukraine for 2007-2015 (2007). Bulletin of Verkhovna Rada of Ukraine, 12. P. 102.

the information field, threats to their fulfilment, and the directions and priorities of state policy in the information sphere. After all, the priorities of the state policy in the information sphere are determined in the Doctrine by ensuring the protection and development of the information space of Ukraine, as well as the constitutional right of citizens to information; the openness and transparency of the state to the citizens; and the formation of a positive international image of Ukraine.[6]

Given such «narrowing» of the concept of «information security», as well as the position of scientists on the problem of security in information flow (Kravets V. M, Petrov V. V, Laputina Yu. A., Tkachuk T. Yu.) we assume the scientific hypothesis that the security of a person, society, and state in the information sphere should be defined as a type of national security, and the relevant public relationships as a subject of legal regulation is conditionally divided into three components: information security, the security of restricted information (hereinafter referred to as RI), and cybersecurity. In determining the methods of legal regulation of the security of a person, society, and state in the information sphere, it is necessary to take into account the conceptual difference between the regulation of communication in information security (where a decisive factor is the counteraction of the influence of negative information), the circulation of RI (which requires clear regulation of the procedures for creating an appropriate organisational-determining mode and access rights) and cybersecurity (which is related to the timely detection, prevention and neutralisation of real and potential threats to critical information infrastructure).

2. METHODS OF LEGAL REGULATION OF INFORMATION SECURITY OF A PERSON, SOCIETY, STATE

Today, much of the information confrontation takes place precisely in the information space, where disinformation processes are increasingly influencing the security of a person, society and state. For example, the expediency of legal regulation of communicationwithin social networks for a long time did not even emerge as a relevant problem in the field of law, due to the existence of the democratic concept of free circulation of information and the possibility of its free dissemination by any means and in any way.

Currently, the negative effects of such dispositive regulation are detrimental to the interests of a person, society and state, for example, the spread of the New Zealand massacre video, the use of social media to overthrow the constitutional order and calls for violence, etc. The nature of the development of information flow has given rise to scientific controversy over the need for the legal regulation of communication in social networks, in particular regarding the dissemination of harmful information. There are already objective reasons for this, as well as the willingness of executives to regulate Internet interactions. In particular, at the end of March 2019, M. Zuckerberg

[6] Strategy of National Security of Ukraine (2015). Decree of President of Ukraine on May 26, 2015 #287/2015 “On Decision of Council of National Security and Defence of Ukraine from May 6, 2015 “On Strategy of National Security of Ukraine”. Official Bulletin of Ukraine, 43. P. 1353.

stated the need for state regulation of such activities to counteract the spread of harmful content, to guarantee fair elections, and to protect citizens' personal data, as well as the possibility of transferring data between services.[7]

It is also worth noting that the Ministry of Information Policy of Ukraine and Facebook representatives discussed cooperation in the field of information security on January 23, 2019. The result of the meeting was that Facebook limited political advertisements for Ukrainian users during elections (from February 1, 2019) Namely, to prevent external interference, the placing of campaign ads from abroad was forbidden [Zuckerberg, 2019].

Similar trends in the regulation of information security issues during the elections are also observed in the European Union. For example, in late February 2019, the European Network and Information Security Agency (ENISA) developed recommendations to improve cybersecurity (a term used presumably as a type of information security – author's note) of elections. In particular, EU Member States are advised to improve national legislation in order to address the problems of Internet disinformation while respecting the fundamental rights of EU citizens. In particular, it has been proposed that the following be introduced into national legal systems: possibilities for the identification and blocking of botnets, the strengthening of the regulation of digital service providers, social media, online platforms and providers of messaging at the EU level, the deployment of unusual traffic detection technologies by the above-mentioned entities, and the consolidation of legal Member States' commitment to classifying election infrastructure as critical. It was also proposed that political parties ensure a high level of cybersecurity in their systems, processes and infrastructures.[8]

In recent years, EU Member States have been paying particular attention to countering the disinformation of society, defining it as "*any form of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm*".[9] In January 2018, the European Commission set up a high-level group of experts (HLEG) to develop proposals to counter this illegal phenomenon. The HLEG recommends in its report that the European Commission should not apply restrictive measures that would affect freedom of speech and the right to information. At the same time, it indicates the need to comply with the following measures to counter disinformation spread online:

to improve the transparency of news media by implementing adequate systems of information dissemination to ensure the protection of personal data;

to entrench media and information literacy to tackle disinformation and help citizens use the digital media environment;

[7] Doctrine of Informational Security of Ukraine (2017). Decree of President of Ukraine on February 25, 2017 #47/2017 "On Decision of Council of National Security and Defence of Ukraine from December 29, 2016 "On Doctrine of Informational Security of Ukraine". Official Bulletin of Ukraine, 20. P. 554.

[8] MIP and Facebook discussed counteraction to intrusion to electoral processes (2019). [E-Resource]. Available at: https://mip.gov.ua/news/2917.html.

[9] ENISA makes recommendations on EU-wide election cybersecurity (2019). [E-Resource]. Available at: http://www.enisa.europa.eu.

to bring into use technical tools for users and journalists to identify disinformation and facilitate positive engagement with rapidly evolving information technologies;
to promote diversity and the sustainability of the European media ecosystem;
5) to continue research on the effects of disinformation in Europe to develop measures for various bodies with continuous improvement in the proper response. [10]

As is evident, in 2018, experts, including scholars, proposed "soft" dispositive legal solutions to counter the threat of disinformation to the information security of a person, society and state. In February 2019, ENISA, in its recommendations (which are mainly dispositive and aimed at information security issues during elections), suggests introducing peremptory norms to prevent negative consequences for a person, society and state.

Now, the problem of EU citizens' exposure to wide-reaching disinformation is even more of a serious challenge than it was before. Since 2018, large companies and networks, operating within the EU, have joined the Code of Practice on disinformation (Facebook, Twitter, Mozilla, Google, Microsoft, etc.). The Code of Practice is the first initiative where platforms and advertisers have voluntary agreed to self-regulatory standards to combat disinformation. The main goal is to achieve the objectives set out by the Commission's Communication presented in April 2018. To achieve the goal, all platforms that have agreed to follow the Code have to become transparent in political advertising, close fake accounts and demonetise disinformation providers. Signatories of the Code of Practice are also working on limiting COVID-19 disinformation and produce regular reports on this issue as well. The EU Commission is going to issue a guidance to intensify the efficiency of the Code of Practice in spring 2021. The European Digital Media Observatory funded by CEF is a new project and it is also aimed at combatting disinformation and fact-checking.[11] Another initiative that function within the EU is the StratCom task force. It has a distinctive platform for the monitoring and analysis of data, and for communication. The main goal is to monitor and combat misinformation, disinformation, and influence operations mainly originating from the Russian Federation. The EU is planning to extend the initiative to other regions and cover more strategically important countries [Pamment, 2020].

It should also be noted that disinformation is not currently classified as an offence in the information field. This is due to the construction of legal systems based on the principles of freedom of expression and right to information. However, given the socially negative consequences of disinformation, a bill has already been registered in Ukraine that provides for legal liability for this type of information offence in order to "*protect a person's constitutional rights to honour, dignity and business reputation by Ppreventing the dissemination of inaccurate information in the mass media."*[12] Ukraine

[10] Ibid.

[11] Tackling online disinformation. (2020) **European Commission.** [E-Resource]. Available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

[12] European Commission (2018). A multi-dimensional approach to disinformation: Report of the independent High-level Group on fake news and online disinformation. European Commission. Tackling Online Disinformation: A European Approach". COM 236. Available at: http://ec.europa.eu/newsroom/

is not the only country to implement such a bill. For example, in 2019 the Albanian parliament passed a new anti-defamation bill aimed at the criminalisation of disinformation. That bill allows the government to fine the media for publishing false information. In Bosnia and Herzegovina, the government also implemented similar rules designed to combat disinformation (mainly related to COVID-19) and fake news in 2020 [Greene et al., 2020]. In the end of 2020, Poland also implemented a new bill, which, however, was aimed at combating censorship and allows filing a complaint against social media platforms that censor posts, which do not meet with Polish law. In the UK, the parliament is going to implement a 2021 Online Safety Bill aimed at protecting users from harmful content online, naming cyber bullying and disinformation as harmful content [Calagui, 2020]. In Germany, the Network Enforcement Act was passed in 2017. It is aimed at removing posts that include mis-, dis-, and mal-information. France, likewise, implemented a bill against the manipulation of information in 2018. This law allows the removing of fake information on social media websites and even blocking those sites. The bill also forces social media platforms to produce financial transparency reports on sponsoring content published before elections. In 2020, Taiwan also implemented a similar bill, aimed at preventing foreign forces from interfering in the internal affairs of the country. The bill prohibits political campaigns carried out with the support of foreign forces. It also designed to prevent the spreading of mis- and disinformation [Nagasako, 2020].

Objectively, civil society actors are against criminal responsibility for the spread of false information in the media and the Internet. For example, the FreeNet Ukraine Coalition emphasises the inadmissibility of introducing criminal liability for the media and persons who publicly disseminate their ideas and information, as «*such legislative initiatives can be a dangerous tool for censorship and pressure on independent media*».[13] Such bills are usually highly criticised by international organisations, domestic NGOs and human rights activists. For example, the Organisation for Security and Co-operation in Europe warned Ukraine over the bill aimed at tackling disinformation, stating that it can cause various violations of human rights and could create a risk to freedom of speech [14].

Summing up what is stated in this part of the work, we note that in ensuring the information security of a person, society and state, the dispositive method of legal regulation predominates, since the processes of circulation of mainly open information are regulated and there is a requirement to observe the constitutional principles of freedom of speech and the right to information. Participants in such interactions exercise the freedom to choose forms and methods of obtaining and disseminating information. However, in this direction we propose the prospective strengthening of

dae/document.cfm?doc_id=51804.

[13] Project of Law on introduction of changes to certain leagislative acts of Ukraine about preventing distribution of false information in mass media #10139 from March 12, 2019. Available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=65657&pf35401=479177

[14] OSCE warns Ukraine over disinformation bill, from Feb. 6, 2020. **Euractiv**. [E-Resource]. Available at: https://www.euractiv.com/section/europe-s-east/news/osce-warns-ukraine-over-disinformation-bill/

the imperative settlement of issues for ensuring the security of the individual, society and the state, and also propose making the spread of disinformation a type of legal offence.

3. METHODS OF LEGAL REGULATION OF THE CIRCULATION OF RESTRICTED INFORMATION

When regulating the security of RI, it is preferable to use the imperative method of legal regulation, since it concerns mostly the protection of the right to such information. Examples of the application of the imperative method of legal regulation are most clearly traced in the formation of regimes for the protection of state secrecy, personal data, bank secrecy, and trade secrecy. For example, the regime of protection of state secrecy implies a citizen signing a written obligation to keep a state secret, which will be entrusted to him as a necessary condition for granting admission to such secrecy[15] or imposes on the citizen additional duties to keep the state secret, namely:

not to allow the disclosure of state secrets that are entrusted to him or became known in connection with the performance of official duties;

not to participate in the activities of political parties and public organisations whose activities are prohibited in the manner prescribed by law;

not to assist foreign states, foreign organisations or their representatives, as well as individual foreigners and stateless persons in carrying out activities detrimental to the interests of the national security of Ukraine;

to comply with the requirements of the secrecy order, etc.[16]

In the European Union, restricted information is one of the types of classified information. In most cases, this type of information is the least classified one and indicates the information that is contrary to the interests of the organisation and/or its members[17].

Domestic legislation contains a global democratic approach to the existence of RI in terms of the possibility of its dissemination (RI) if such information is "*socially necessary, that is, a subject of public interest and the public's right to know this information outweighs the potential harm from its spread*".[18] Moreover, the subject of public interest is considered to be the information that indicates:

a threat to the state sovereignty or the territorial integrity of Ukraine;

the implementation of constitutional rights, freedoms and duties;

a possibility of human rights violation;

deception of the public;

[15] Law of Ukraine "On State Secret" from April 19, 1994. Bulletin of Verkhovna Rada of Ukraine, 16. P. 93.

[16] Ibid.

[17] Guidance Guidelines for the classification of information in research project, from Jan. 7, 2020. European Commission. [E-Resource]. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/secur/h2020-hi-guide-classif_en.pdf

[18] Law of Ukraine "On Information" from December 01, 1992. Bulletin of Verkhovna Rada of Ukraine, 48. P. 650.

harmful negative consequences of the activity (or inactivity) of individuals or legal entities, etc.[19]

Such norms are the result of the use of the dispositive method of legal regulation in the circulation of RI, that is used by journalists and other entities to conduct journalistic investigations in the modern information society.

4. METHODS OF LEGAL REGULATION OF CYBERSECURITY

In contrast to the definition of «information security», which, as noted, is somewhat outdated and does not objectively correspond to the current activities and realities of legal regulation, a rather progressive definition of the term «cybersecurity» is utilised in Ukraine - it is the protection of vital interests of a person and citizen, society and state through the use of cyberspace, which ensures sustainable development of the information society and digital communication environment, timely detection, prevention and counteraction to real and potential threats to the national security of Ukraine in cyberspace.[20]

The Law of Ukraine of 05.10.2017 "On the Main Principles of Maintaining Cybersecurity of Ukraine" has expanded the understanding of the term "cybercrime (computer crime)", which is defined as a socially dangerous act in cyberspace which is recognised as a legal crime by Ukrainian law and/or by Ukrainian international treaties. We draw attention to the fact that, given the general "imperativeness" of the Law, there is a dispositivity in referring to cybercrimes not only as "classical", namely, as provided for in Section XVI of the Criminal Code of Ukraine "Crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks," but also when designating other public threats using cyberspace to carry out cybercrimes. With the development of information technology, the list of such crimes will increase steadily, as today there remain fewer crimes perpetrated without the use of the Internet. The list of historically known criminal offences of phishing, carding and in banking fraud (payment) systems will expand.

It should be noted that the Council of Europe Convention on Cybercrime ratified by Ukraine on November 21st, 2001 (hereinafter - the Convention) is aimed at increasing the efficiency of criminal investigations and prosecutions related to criminal offences involving computer systems and data, and at the possibility of the collection of electronic crime-related evidence.[21] Fifty-six countries have joined the Convention: EU members as well as the USA, Japan, Australia, Argentina, Chile, Senegal, Ukraine and others. In 2016, a representative of the Security Service of Ukraine was elected to the governing body of the Committee - the Bureau of the Committee of the Convention.

[19] Ibid.

[20] Analysis of Project of Law #10139 on introduction of changes to certain leagislative acts of Ukraine about preventing distribution of false information in mass media Available at: https://medium.com/@cyberlabukraine/аналіз-законопроекту-10139-щодо-запобігання-розповсюдженню-недостовірних-відомостей-у-змі-c27dcce53d06.

[21] Conventions of Council of Europe about Cybercrime from Nov. 21, 2011 (2011). [E-Resource]. Available at: http://zakon4.rada.gov.ua/laws/show/994_575.

Predominantly by utilising the imperative method of legal regulation, the Convention focuses on combatting cybercrime as the greatest threat to cybersecurity - that is, to the vital interests of a person and citizen, society and state in cyberspace.

The principles of the Convention regarding the promptness of executing requests for the preservation of electronic evidence and providing answers to requests for legal assistance by national ISPs, etc. are based on imperativeness.

The EU has three Cybersecurity strategies, with the last one recently being implemented. The first two strategies resulted in regulations, namely the Network and Information Security Directive and the Cybersecurity Act, which explains the role of the European Union Agency for Network and Information Security (ENISA). Many legal measures regarding cybersecurity are stated in directives (e.g. the NIS Directive and the Directive on Attacks against Information Systems). In practice, this means that "*Member States are free to choose the form and methods to implement requirements stemming from such directives.*"(Fuster & Jasmontaite, 2020) The EU's Cybersecurity Strategy for the Digital Decade (Joint Communication – the third strategy) was presented on 16th of December in 2020 by the European Commission. This strategy will improve the EU's resilience against cyber threats and help with solving cybercrimes. Moreover, the Commission has made proposals "*to address both cyber and physical resilience of critical entities and networks: a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'), and a new Directive on the resilience of critical entities."* These directives influence a broad spectrum of sectors and address "*online and offline risks, from cyberattacks to crime or natural disasters, in a coherent and complementary way.*" The sphere of cybersecurity became an even more urgent priority for the EU in recent years and it is also included in the EU's long-term budget 2021-2027. Moreover, during the COVID-19 pandemic the number of cybercrimes and cyberattacks has increased, hence the EU has invested further in cybersecurity under the Recovery Plan for Europe. The key pillars of the new strategy are resilience, operational capacity and advancing cyberspace.[22]

The new strategy also indicates the EU lacks collective awareness of cyber threats. That is because the governments of the EU member countries do not gather and disseminate information about cybersecurity and its current level in the EU. The EU's new Cybersecurity Strategy for the Digital Decade is a core element of many other of the EU's key documents in various areas of foreign and security policies. For example, it is directly connected to such document as the Security Union Strategy 2020-2025, Shaping Europe's Digital Future, the Commission's Recovery Plan for Europe, and the Global Strategy for the EU's Foreign and Security Policy. The strategy demonstrates the way the EU's cybersecurity network works and it also shows the aim of becoming an international leader in securing the safety of an open Internet and cyber networks. The information security area is the most important part of the strategy

[22] New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, from Dec. 16, 2020. European Commission. [E-Resource]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

and the EU has made a great step forward towards better understanding of cyber threats, their detection, prevention and towards better protection of classified information and sensitive unclassified information within the EU. The implementation of this strategy will contribute to the strengthening of the EU's cybersecurity sphere and its position worldwide. Moreover, the EU should also improve its rules and standards for "cybersecurity for essential services and critical infrastructures, as well as the development and application of new technologies." The Commission and the High Representative, in accordance with their separate competences, will review progress under this strategy and create rules for assessment. The Commission and the High Representative will also continue to classify practical measures to bridge the four cybersecurity communities in the EU, where necessary. Furthermore, the Commission and the High Representative will carry on with engaging with the multi-stakeholder community, underlining everyone's commitment to play their part in maintaining a reliable and protected cyberspace, where each person can operate safely [23].

European and world practice shows that public-private partnership is an integral part of law enforcement action in the field of cybercrime. The settlement of these relationships, both in the context of crime and in the context of cybersecurity, should be addressed with due regard to the rights and interests of stakeholders. In this context, it is advisable to create a basis for cooperation by signing a Memorandum of Understanding between ISPs and the Ukrainian law enforcement agencies. Ultimately, domestic practice confirms that imperative decisions are not properly implemented. For example, the NSDC decision of April 28, 2017 "On Application of Personal Special Economic and Other Restrictive Measures (Sanctions)", enacted by Presidential Decree No. 133 of May 15, 2017, on the provision of information security and cybersecurity, requires the development and introduction of a mechanism for blocking information resources by operators and providers through their telecommunication and data telecommunications network.

However, it is known that the Draft Law on amendments to certain legislative acts of Ukraine on countering national security threats in the information sphere, which envisaged the creation of mechanisms aimed at prompt detection, response, aversion, prevention, and counteraction of cyber threats, cyber-attacks and cybercrime and the restoration of the stability and reliability of the functioning of communication and technological systems, has not yet become law. This was largely due to a lack of proper public discussion of the relevant mechanisms (the existence of which, during hybrid aggression against Ukraine is, in most cases, justified) as well as the lack of a basis for effective public-private partnerships. It should be noted that in this respect the Situational Center for Cybersecurity of the Security Service of Ukraine is a rather progressive platform from which we can promote such partnerships in the field of cybersecurity.

[23] Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade, from Dec. 16, 2020. European Commission. [E-Resource]. Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

Thus, measures regarding ensuring cybersecurity are settled mainly by the imperative method of legal regulation (for example, when setting the technical requirements for the protection of state electronic information resources). However, a dispositive method should be used to normalise public-private partnership issues.

CONCLUSIONS

his work proposes a scientific hypothesis suggesting the dividing of the subject of legal regulation of the security of a person, society, state into three components: information security, the security of restricted information and cybersecurity.

The legal regulation of measures for information security is aimed at counteracting the impact of negative information in the information space of the state, and controlling matters regarding security. The goal of the RI is the regulation of measures on cybersecurity in relation to the prevention and counteraction of real and potential threats to critical information infrastructure facilities, as well as creating an organisational and legal regime and providing access, etc.

The paper concludes that when ensuring the information security of a person, society and state, the dispositive method of legal regulation dominates since the processes of circulation of mostly open information are regulated and there is a requirement to comply with the constitutional principles of freedom of speech and the right to information. However, in this study, we discovered a need to imperatively strengthen the security of a person, society and state by creating new legislation to make, in some cases, the spread of disinformation a criminal offence.

Legal regulation of the security of RI is carried out largely using the imperative method of legal regulation since it mainly concerns the protection of the right to such information. The emphasis is on the fact that the dispositive method of legal regulation in the circulation of RI is applied in terms of collecting and disseminating socially necessary information.

Public activities aimed at the ensurance of cybersecurity are regulated mainly by the imperative method of legal regulation, although, in order to normalise public-private partnership issues, it is concluded that it is necessary to use an exclusively dispositive method of legal regulation.

REFERENCES:

Analysis of Project of Law #10139 on introduction of changes to certain leagislative acts of Ukraine about preventing distribution of false information in mass media Available at: https://medium.com/@cyberlabukraine/аналіз-законопроекту-10139-щодо-запобігання-розповсюдженню-недостовірних-відомостей-у-змі-c27dcce53d06.

Calagui, J. M. Poland's New Bill Slaps $2.2 Million Fines For Social Media Companies Censoring Lawful Posts, from Dec. 23, 2020. [E-Resouce]. Available at: http://www.christianitydaily.com/articles/10369/20201223/poland-s-new-bill-slaps-2-2-million-fines-for-social-media-companies-censoring-lawful-posts.htm

Conventions of Council of Europe about Cybercrime from Nov. 21, 2011 (2011). [E-Resource]. Available at: http://zakon4.rada.gov.ua/laws/show/994_575.

Doctrine of Informational Security of Ukraine (2017). Decree of President of Ukraine on Febru-

ary 25, 2017 #47/2017 “On Decision of Council of National Security and Defence of Ukraine from December 29, 2016 “On Doctrine of Informational Security of Ukraine”. Official Bulletin of Ukraine, 20. P. 554.

ENISA makes recommendations on EU-wide election cybersecurity (2019). [E-Resource]. Available at: http://www.enisa.europa.eu.

European Commission (2018). A multi-dimensional approach to disinformation: Report of the independent High-level Group on fake news and online disinformation. European Commission. Tackling Online Disinformation: A European Approach”. COM 236. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804.

Frau-Meigs, D.; O’Neil B.; Tome, V.; Soriano A., (2017). Competences in Digital Citizenship Education. Strasbourg: Council of Europe.

Fuster, G.G.; Jasmontaite L., (2020) Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. [E-Resouce]. Available at: https://doi.org/10.1007/978-3-030-29053-5_5

Greene, G.; Asmolov, G.; Fagan, A.; Fridman, O.; Gjuzelov, B., (2020). Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them, from Dec., 2020. Directorate General for External Policies of the Union. [E-Resouce]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf

Guidance Guidelines for the classification of information in research project, from Jan. 7, 2020. European Commission. [E-Resouce]. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/secur/h2020-hi-guide-classif_en.pdf

Joint Communication: The EU’s Cybersecurity Strategy for the Digital Decade, from Dec. 16, 2020. European Commission. [E-Resouce]. Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

Kaliuzhnyi, R.; Martseniuk, A., (2008). Subject and Methods of Informational Law. Legal Informatics, 3(19), 5-12.

Kovalenko, L., (2014). Subject and Methods of Informational Law of Ukraine. Bulletin of V. Karazin Kharkiv National University. #1137. Series “Law”, Vol.18. 83-86.

Law of Ukraine “On Information” from December 01, 1992. Bulletin of Verkhovna Rada of Ukraine, 48. P. 650.

Law of Ukraine “On Main Foundations for Ensuring Cybersecurity of Ukraine” from October 02, 2017. Bulletin of Verkhovna Rada of Ukraine, 45. P. 403.

Law of Ukraine “On State Secret” from April 19, 1994. Bulletin of Verkhovna Rada of Ukraine, 16. P. 93.

Main Foundations for Development of Informational Society in Ukraine for 2007-2015 (2007). Bulletin of Verkhovna Rada of Ukraine, 12. P. 102.

Marushchak, A., (2011). Informational Law of Ukraine. Kyiv: Dakor.

Marushchak, A., (ed.) (2013). Foundations of Informational Security of Ukraine: Textbook. Kyiv: Scientific and Publishing Department of National Academy of Security Service of Ukraine.

MIP and Facebook discussed counteraction to intrusion to electoral processes (2019). [E-Resource]. Available at: https://mip.gov.ua/news/2917.html.

Nagasako, T., (2020). Global disinformation campaigns and legal challenges. International Cybersecurity Law Review, 1, 125–136. https://doi.org/10.1365/s43439-020-00010-7

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, from Dec. 16, 2020. European Commission. [E-Resouce]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

OSCE warns Ukraine over disinformation bill, from Feb. 6, 2020. Euractiv. [E-Resouce]. Available at: https://www.euractiv.com/section/europe-s-east/news/osce-warns-ukraine-over-disinformation-bill/

Pamment, J., (2020). The EU’s Role in Fighting Disinformation: Crafting A Disinformation Framework, from Sept. 24, 2020. Carnegie Endowment for International Peace. [E-Resouce]. Available at: https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-

disinformation-crafting-disinformation-framework-pub-82720

Panova, I., (2011). Tendencies in Development of System of Informational Law of Ukraine at Modern Stage. Forum Prava, 2, 694-699.

Project of Law on introduction of changes to certain leagislative acts of Ukraine about preventing distribution of false information in mass media #10139 from March 12, 2019. Available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=65657&pf35401=479177.

Shvets, M.; Kaliuzhnyi, R.; Melnyk, V., (eds.) (2009). Foundations of Informational Law of Ukraine: Textbook. 2nd Edition. Kyiv: Znannia.

Strategy of National Security of Ukraine (2015). Decree of President of Ukraine on May 26, 2015 #287/2015 "On Decision of Council of National Security and Defence of Ukraine from May 6, 2015 "On Strategy of National Security of Ukraine". Official Bulletin of Ukraine, 43. P. 1353.

Tackling online disinformation. (2020) European Commission. [E-Resource]. Available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Wardle, C.; Derakhshan, H., (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Report to the Council of Europe. Available at: https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.

Zuckerberg, M., (2019). Four Ideas to Regulate the Internet. [E-Resouce]. Available at: https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet.