УДК 342.52
DOI: 10.31359/1993-0909-2019-26-3-88

Анатолій Іванович Марущак

Навчально-науковий інститут перепідготовки
та підвищення кваліфікації кадрів СБУ
Національна академія Служби безпеки України
Київ, Україна

МЕТОДИ ПРАВОВОГО РЕГУЛЮВАННЯ БЕЗПЕКИ ОСОБИ, СУСПІЛЬСТВА, ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. *Інформаційний чинник є важливим фактором суспільного розвитку, оскільки виконує організаційно-управлінську та регулятивно-контрольну функції в сучасному інформаційному суспільстві. Тому основна мета роботи полягає у аналізі методів правового регулювання безпеки особи, суспільства, держави в інформаційній сфері. У статті запропоновано наукову гіпотезу про поділ предмету правового регулювання безпеки особи, суспільства, держави на три складові: інформаційна безпека, безпека інформації з обмеженим доступом та кібербезпека. Правове регулювання відносин щодо інформаційної безпеки спрямовується на протидію негативному інформаційному впливу в інформаційному просторі держави, унормування відносин з приводу безпеки інформації з обмеженим доступом (ІзОД) на створення організаційно-правового режиму, надання доступу до інформації тощо, а регламентація відносин щодо кібербезпеки пов'язана з виявленням, запобіганням і нейтралізацією реальних і потенційних загроз об'єктам критичної інформаційної інфраструктури. При забезпеченні інформаційної безпеки особи, суспільства і держави переважає диспозитивний метод правового регулювання, хоча зроблено припущення про перспективне посилення імперативного врегулювання питань забезпечення безпеки особи, суспільства і держави у частині протидії дезінформуванню як виду інформаційного правопорушення. Правове регулювання безпеки ІзОД здійснюється з використанням імперативного методу правового регулювання, а диспозитивний метод правового регулювання при обігу ІзОД застосовується у частині збирання і поширення суспільно необхідної інформації. Суспільні відносини з приводу забезпечення кібербезпеки урегульовуються імперативним методом правового регулювання, хоча для унормування питань державно-приватного партнерства зроблено висновок про необхідність застосування виключно диспозитивного методу правового регулювання.*

Ключові слова: інформаційна безпека, кібербезпека, безпека інформації з обмеженим доступом, правове регулювання, метод, інформаційне право.

Anatoly I. Marushchak

Academic and Research Institute of Advanced Training and Retraining of Staff
National Academy of Security Service of Ukraine
Kyiv, Ukraine

METHODS OF LEGAL REGULATION OF THE SECURITY OF THE INDIVIDUAL, SOCIETY, STATE IN THE INFORMATION SPHERE

Abstract. *Information factor is an important component of social development, as it performs organizational and managerial and regulatory oversight functions in the modern information society. Therefore, the main purpose of the article is to analyse the methods of legal regulation*

of security of a person, society, state in the information sphere. The paper proposes a scientific hypothesis on the division of the subject of legal regulation of the security of a person, society, state into three aspects: information security, classified information security and cybersecurity. Legal regulation of information security relations is aimed at counteracting the negative information impact in the information space of the state, normalizing relations in terms of security of classified information to establish organizational and legal regime, to provide access to information, etc., and regulation of cybersecurity relations is connected with detection, prevention and neutralization of real and potential threats to critical information infrastructure facilities. Upon ensuring the information security of the individual, society and the state, the dispositive method of legal regulation prevails, although further reinforcement of imperative regulation of issues of ensuring the security of the person, society and the state with regard to combating misinformation as a type of information offense is presumed. Legal regulation of the security of classified information is ensured through the imperative method of legal regulation, and the dispositive method of legal regulation in the circulation of classified information is used in the part of collecting and disseminating publicly required information. Public relations regarding cybersecurity are governed by the imperative method of legal regulation, although with regard to normalization of public-private partnership matters, a conclusion is made on the necessity of application of dispositive method of legal regulation exclusively.

Key words: information security, cybersecurity, security of classified information, legal regulation, method, information law.

INTRODUCTION

In the context of a transborder information society, an important strategic objective is to develop the system of international information security as a state of global information space, which excludes the possibility of violations of the rights of the individual, society and the state. The dynamics and nature of the development of the global information society offer great opportunities for intensifying the latest challenges and threats to the individual as a vulnerable subject of information relations.

Scientific interest in the problematics of information security is manifested in various humanities – philosophy, political science, cultural studies, psychology, pedagogy, economics, sociology and others, which as a general rule is reflected in the research of the laws of development of information and security field as a backbone component of life of modern society on the whole and life of every member of this society. In the global information society, the tendency to form an understanding of the features and significance of the realization of the interests of the individual, society, state, including the need for security, requires greater attention from science, especially in the context of the analysis of methodological approaches [1–4].

Large-scale transformations in the conditions of development of information and telecommunication technologies cause aggravation of national security issues, actualize modern tendencies of realization of the triad of interests of the individual, society and the state in the context of security in the information sphere. Currently, the leading principles of building an information society in Ukraine include free access to infor-

mation and knowledge, except for the restrictions established by law [5; 6]. At the same time, our state declares and consistently upholds the constitutional principles of freedom of speech, the right to information and security of the individual, society, state, and the security dimension of the researched issue is especially revealed in the light of the legal regulation of social relations [7–10]. In particular, a number of current regulations is indicative of the urgency of ensuring information security in the territory of our country, including such Laws of Ukraine as: "On Information"[1], "On Citizens' Appeals"[2], "On Printed Mass Media (Press) in Ukraine"[3], "On Television and Radio Broadcasting"[4], "On Information Agencies"[5], "On the National Archival Fund and Archival Institutions"[6], "On Libraries and Librarianship"[7], "On State Statistics"[8], "On State Secrets"[9], "On Access to Judgments"[10], "On Electronic Documents and Electronic Document Circulation"[11], "On Protection of Information in Information and Telecommunication Systems"[12], "On Scientific and Technical Information"[13], "On the National Informatization Program"[14], "On the Procedure for Reporting on the Activity of State Bodies and Local Self-Government Bodies in Ukraine by the Mass Media"[15],

[1] Law of Ukraine "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12

[2] Law of Ukraine "On Citizens' Appeals" (2019, July). Retrieved from https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80

[3] Law of Ukraine "On Printed Mass Media (Press) in Ukraine" (2018, November). Retrieved from https://zakon.rada.gov.ua/laws/show/2782-12

[4] Law of Ukraine "On Television and Radio Broadcasting" (2018, November). Retrieved from https://zakon.rada.gov.ua/laws/show/3759-12

[5] Law of Ukraine "On Information Agencies". (2019, July). Retrieved from https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80

[6] Law of Ukraine "On the National Archival Fund and Archival Institutions". (2015, May). Retrieved from https://zakon.rada.gov.ua/laws/show/3814-12

[7] Law of Ukraine "On Libraries and Librarianship". (2017, January). Retrieved from https://zakon.rada.gov.ua/laws/show/32/95-%D0%B2%D1%80

[8] Law of Ukraine "On State Statistics". (2014, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2614-12

[9] Law of Ukraine "On State Secrets". (1994, January). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12

[10] Law of Ukraine "On Access to Judgements". (2017, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3262-15

[11] Law of Ukraine "On Electronic Documents and Electronic Document Circulation". (2018, November). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15

[12] Law of Ukraine "On Protection of Information in Information and Telecommunication Systems". (2014, April). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

[13] Law of Ukraine "On Scientific and Technical Information". (2014, April). Retrieved from https://zakon.rada.gov.ua/laws/show/3322-12

[14] Law of Ukraine "On National Informatization Program". (2016, August). Retrieved from https://zakon1.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

[15] Law of Ukraine "On the Procedure for Reporting on the Activity of State Bodies and Local Self-Government Bodies in Ukraine by the Mass Media". (2019, July). Retrieved from https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80

"On Advertising"[1], "On Basic Principles of Cyber Security of Ukraine"[2], etc. The aforementioned regulations, in their communication and interdependence, establish a system of official opinions, which defines national interests as objectively significant needs of the individual, society and the state in ensuring their protection and sustainable development. Thus, in the face of new challenges and threats of a transborder global information society, the relevance of scientific and legal issues and the development of new approaches to counteracting information and psychological, destructive influence is determined by the substantial objectives of ensuring legal information security of the individual, proceeding from doctrinal approaches and the developed methodology [11–14].

The above determines the relevance of the legal groundwork for information security of the individual, society and state, of scientific research and development of doctrinal provisions aimed at substantiating the place and role of a given legal institution in the science of information law, as well as the relevance of specifying the methods of legal regulation of the researched institution [15–17]. Proceeding from the position of representatives of the doctrine, we shall note that the subject of regulation of information law are relations regarding the circulation of information, in particular its creation, reception, collection, storage, protection, application, dissemination, etc. In turn, the methodology of legal regulation of the researched institution has a multivariate approach to its interpretation. Thus, the majority of legal research refers to classic methods of regulation – dispositive and imperative. As early as 2008, R. A. Kalyuzhny`j and A. G. Martsenyuk actualized the discussion regarding the subject and methods of information law [18]. A team of scientists led by M. Ya. Shvets, R. A. Kalyuzhny`j, and V. P. Melnyk made an attempt to systematize the information law of Ukraine on a single methodological basis [19]. The author of this paper also made an attempt to uncover the methodological foundations of information law of Ukraine in 2011 [20]. The specified direction of scientific search was also developed by I. V. Panova in the context of development of the system of information law of Ukraine [21]. In his works, L. P. Kovalenko proposed an original definition of the method of information law and substantiated the possibility of creating, with its help, proper conditions for realization and protection of citizens' rights in the information sphere, as well as normal functioning of the information society [22]. At the same time, despite the presence of sufficiently sound scientific achievements of representatives of national doctrine, the subject of the paper remains relevant in the context of modern transformational realities and new approaches to legal consciousness and methods of legal regulation.

In consideration of the foregoing, the purpose of the article is to conduct a com-

[1] Law of Ukraine "On Advertising". (July, 2018). Retrieved from https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80

[2] Law of Ukraine "On Basic Principles of Cyber Security of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

prehensive research of the methods of legal regulation of the security of the individual, society, state in the information sphere, factoring in the doctrinal approaches and modern realities of law enforcement practice. Proceeding from the stated purpose, the following research objectives are outlined: 1) to clarify the methodological approach to the subject of legal regulation of the issues of security in the information sphere; 2) to analyse methods of legal regulation of information security of a person, society, state; 3) to identify methods of legal regulation of cybersecurity and circulation of classified information.

1. MATERIALS AND METHODS

The methodological basis of the article is represented by a set of general scientific and special legal methods of cognition. Thus, the dialectical method was used upon researching the development patterns of the security dimension of the individual, society, state in the conditions of the global information space development. The Aristotelian method was used in the analysis of information legislation, determining the content of basic concepts, systematization of material to obtain generalized conclusions within the stated problematics. In addition, the basis of the methodology of scientific research includes a factorial, cause-consequence analysis, aimed at identifying the circumstances, components of methodological approaches to ensuring the security of the individual, state, society in the information space. Taking into account that factorial analysis as a technique is applied in various fields of knowledge, it is proposed to use it for a comprehensive and systematic research of the nature of the influence of certain factors in the form of challenges and threats to information security.

The comparative law method facilitated the identification of tendencies and comparison of approaches of foreign countries. In particular, the analysis of national legislation, as well as European Union initiatives in the information sphere, focused on normalizing the corresponding relations to ensure the security of the individual, society and the state. To obtain and summarize knowledge on the essence and stages of development of the method of legal regulation of the information security institution, the historical law method was applied.

The system analysis enabled the assessment of the formed approaches to the legal support of the information security of the individual, facilitated their correlation with objectively existing social relations, and the sociological method allowed to perform an assessment of the factors influencing the behaviour of the individual as a subject of information relations. The predictive method – in the form of legal modelling – was applied upon the determination of the legislation development prospects, aimed at creating a system of effective legal support for information security of the individual, society, state, factoring in the latest approaches to the methods of legal regulation and approbation of foreign successful practices.

The theoretical basis of the research is formed from the works of scientists in the field of information law, in particular, the works of L. P. Kovalenko on the subject and

methods of information law of Ukraine are researched [22]. Using the method of systemic synthesis, the definitions provided by the scientist were compared with the provisions of the legislation of Ukraine and the features of legal regulation of relations in the field of security of the individual, society and the state are revealed. For a detailed study of the research subject, the works of I. V. Panova were analysed, which cover the tendencies of development of the system of information law of Ukraine [21]. To compare the domestic practices of legal regulation with European approaches, the works of D. Frau-Meigs, B. O'Neil, V. Tome, A. Soriano on digital education of the population [23] and C. Wardle and H. Derakshan on "information clutter" were considered [24].

In the course of the research, national and international legal acts were processed, among which special attention was given to such acts as the Council of Europe Convention on Cybercrime[1], the Law of Ukraine "On the Fundamental Principles of Information Society Development 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 regulations.

2. RESULTS AND DISCUSSION

2.1 Methodological approach to the subject of legal regulation of the issues of information security

In the light of external aggression against Ukraine there is a scientific and practical issue of defining the boundaries of regulation of relations regarding the security of the individual, society, state in the information sphere. The wording "security of the individual, society, state in the information sphere" was chosen not by chance, but with the following considerations in mind. Firstly, in recent times, the legislation of Ukraine is heading towards outlining a distinction between "information security" and "cybersecurity" [25; 26]. Instead, the "classic" regulation is inherent in the relationship with the classified information security.

The definition of "information security", enshrined in the Fundamental Principles for the Development of the Information Society in Ukraine for 2007-2015, is all-encompassing, as it was considered a state of protection of vital interests of the individual, society and the state, wherein harm is prevented through:

– incompleteness, untimeliness and unreliability of the information used;
– negative information impact;
– negative consequences of the application of information technologies;

[1] Council of Europe Convention on Cybercrime. (2001, November). Retrieved from http://zakon4.rada.gov.ua/laws/show/994_575

[2] Basic Principles of Information Society Development in Ukraine for 2007-2015. (2007, January). Retrieved from https://zakon.rada.gov.ua/laws/show/537-16

[3] Law of Ukraine "On State Secrets". (1994, January). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12

[4] Law of Ukraine "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12

– unauthorized distribution, use and violation of the integrity, confidentiality and accessibility of information[1]. In 2007, such a definition of "information security" included issues of information security (information resources), security of the information space and security of functioning of the information and telecommunication infrastructure [27].

Today, however, the concept of "information security" acquires a different, "narrow" 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 refers to "counteraction to information operations against Ukraine, manipulation of public consciousness and dissemination of distorted information, protection of national values and strengthening of unity of Ukrainian society; development and implementation of coordinated information policy of public authorities; identification of Ukrainian information space subjects created and/or exploited by Russia to wage an information war against Ukraine; creation and development of institutions responsible for information and psychological security, with consideration of the practices of NATO Member States", etc.[2]. Thus, information security encompasses processes and relationships that occur in the information space of the state. A similar approach is enshrined in the Doctrine of Information Security of Ukraine, which defines Ukraine's national interests in the information sphere, threats to their implementation, directions and priorities of national policy in the information sphere. Indeed, the priorities of the national policy in the information sphere stipulated therein are determined by ensuring the protection and development of the information space of Ukraine, as well as the constitutional right of citizens to information; openness and transparency of the state to the citizens; formation of a positive international image of Ukraine[3].

Factoring in such "narrowing" of the content of the concept of "information security", as well as the position of scientists on the issue of security in information relations we shall assume the scientific hypothesis that the security of the individual, society, state in the information sphere should be defined as a type of national security, and the corresponding public relations as a subject of legal regulation shall be conveniently divided into three aspects: information security, classified information security, cybersecurity.

Upon the determination of the methods of legal regulation of the security of a person, society, state in the information sphere, it is necessary to consider the conceptual difference between the regulation of relations in information security, where de-

[1] Basic Principles of Information Society Development in Ukraine for 2007-2015. (2007, January). Retrieved from https://zakon.rada.gov.ua/laws/show/537-16

[2] National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine". (2015, May). Retrieved from https://zakon.rada.gov.ua/laws/show/287/2015

[3] Doctrine of Information Security of Ukraine "On Decisions of the National Security and Defence Council of Ukraine". (2017, February). Retrieved from https://mip.gov.ua/documents/100.html

cisive is the counteraction to negative information influence, regarding the circulation of classified information, in which the clear regulation of procedures for creating an appropriate organizational and legal regime, provision of access, as well as regarding cybersecurity connected with the timely detection, prevention and neutralization of real and potential threats to critical information infrastructure objects [28].

2.2 Methods of legal regulation of information security of a person, society, state

Today, a substantial part of the information confrontation occurs precisely in the information space, where misinformation processes are increasingly influencing the security of the individual, society and the state. For example, the scientific issue of the expediency of the legal regulation of relations in social networks for a long time did not even come up in the jurisprudence as relevant in connection with the existence of a democratic concept of free circulation of information, the possibility of its free dissemination in whatever form and by whatever medium [29]. Currently, the negative effects of such dispositive regulation are detrimental to the interests of the individual, society and the state, for instance, the dissemination of video on massacres in New Zealand, the use of social media to overthrow the constitutional order, calls for violence, etc. This nature of the development of information relations has given rise to scientific controversy regarding the necessity of legal regulation of relations in social networks, particularly in terms of dissemination of harmful information. Objective reasons for this already exist, as well as the willingness of executives to regulate Internet relations. In particular, at the end of March 2019, M. Zuckerberg stated the necessity for state regulation of such relations to counteract the spread of harmful content, hold fair elections, and protect the personal data of citizens and the ability to transfer data between services [30].

It is also noteworthy that, on January 23, 2019, the Ministry of Information Policy of Ukraine and representatives of Facebook discussed cooperation in the field of information security. The result of the meeting was that Facebook restricted political advertising for Ukrainian users from February 1, 2019 for the period of the election, including the prohibition of campaigning from abroad to prevent external interference [31].

Similar tendencies in the settlement of information security issues during the elections are also observed in the European Union. Thus, at the end of February 2019, the European Network and Information Security Agency (ENISA) developed recommendations to improve cybersecurity (a term was presumably used as a type of information security – author's note) of elections. In particular, EU Member States are advised to improve national legislation to address the issues of Internet misinformation while respecting the fundamental rights of EU citizens. In particular, it is proposed to implement into national legal systems the possibility of identifying and blocking botnets, strengthening the regulation of digital service providers, social media, online platforms and messaging providers at EU level, deploying of unusual traffic detection technolo-

gies by the aforementioned subjects, reinforcing the legal obligation for Member States to classify election infrastructure as critical, as well as the obligation for political parties to ensure a high level of cybersecurity in their systems, processes and infrastructures [32].

In recent years, EU Member States have paid particular attention to counteracting misinformation by defining it as "any form of false, inaccurate or misleading information designed, presented and disseminated intentionally to harm the public or to profit" [33]. In particular, in January 2018, the European Commission established the High-Level Expert Group ("the HLEG") to develop proposals regarding the counteraction of this illegal phenomenon. In its report, the HLEG recommends that the European Commission takes o restrictive measures that would affect freedom of expression and the right to information. At the same time, it highlights the need to adhere to the following measures of counteracting misinformation on the Internet:

1) increase the transparency of online news by introducing adequate systems of information dissemination to ensure the protection of personal data;

2) introduce media and information literacy to counteract misinformation and help citizens use the digital media environment;

3) implement technical tools for users and journalists to identify misinformation and facilitate positive engagement with rapidly evolving information technologies;

4) ensure the diversity and sustainability of the European media ecosystem;

5) continue researching the impact of misinformation in Europe to develop measures for different subjects to continually improve appropriate counteraction [33].

As is evident, in 2018, experts, including scientists, offered “soft” dispositive legal solutions to counteract such a threat to the information security of the individual, society and the state as misinformation. And in February 2019, ENISA, in its recommendations (which are predominantly dispositive), focusing on the issue of information security during elections, proposes to introduce mandatory rules to prevent negative consequences for the individual, society and the state [34].

It should also be noted that misinformation is not currently classified as an offense in the information sphere. This is conditioned by the construction of legal systems based on the principles of freedom of expression and the right to free access to information. However, in view of the socially negative consequences of misinformation, a draft law has already been registered in Ukraine that provides for legal liability for this type of information offense in order to "protect a person's constitutional rights to honour, dignity and business reputation by preventing the dissemination of misinformation in the media"[1]. Objectively, representatives of civil society are against criminal liability for the dissemination of misinformation in the media and on the Internet. For example, the FreeNet Ukraine Coalition emphasizes the inadmissibility of introducing

[1] Draft Law “On Amendments to Certain Legislative Acts of Ukraine on Prevention of Dissemination of Misinformation in Mass Media”. (2019, March). Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=65657&pf35401=479177.

criminal liability for the media and other persons that publicly disseminate their ideas and information, as "such legislative initiatives can be a dangerous tool for censorship and pressure on independent media" [35].

Summarizing the points outlined in this section, we shall note that upon ensuring the information security of the individual, society and the state, the dispositive method of legal regulation prevails, since the processes of circulation of mostly open information are regulated and there is a requirement to observe the constitutional principles of freedom of expression and the right to information. Participants in such relationships exercise the freedom to freely choose the forms and methods of obtaining and disseminating information. Although in this direction we make the assumption on promising strengthening of the imperative regulation of the issues of ensuring the security of the individual, society and the state, and even the establishment of legal liability for misinformation as a type of information offense.

2.3 Methods of legal regulation of the circulation of classified information

Upon regulating the security of classified information, the imperative method of legal regulation is predominantly applied, as it largely concerns the protection of the right to such information. Most clearly examples of application of the imperative method of legal regulation are traced in the formation of regimes of protection of state secrets, personal data, bank secrecy, trade secrets. For example, the regime of protection of state secrecy provides for to undertake a written obligation to keep a state secret that will be entrusted to them as a necessary condition for granting admission to such secrecy[1], or imposes on a citizen additional duties regarding the preservation of a state secret, namely:

– not to disclose in any way the state secret which is entrusted to them or which became known in connection with the performance of official duties;

– not to participate in the activities of political parties and public organizations whose activities are prohibited in accordance with the legally established procedure;

– not to assist foreign states, foreign organizations or their representatives, as well as individual foreigners and stateless persons in performing activities that harm the interests of national security of Ukraine;

– to comply with the requirements of secrecy, etc. [9].

Domestic legislation contains a worldwide democratic approach to the existence of classified information in terms of the possibility of its (classified information) dissemination, if such information is "publicly necessary, i.e. it is a matter of public interest, and the right of the public to know this information outweighs the potential harm from its dissemination"[2]. Moreover, the subject of public interest is information that:

[1] Law of Ukraine "On State Secrets". (1994, January). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12

[2] Law of Ukraine "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12

– indicates a threat to state sovereignty, territorial integrity of Ukraine;
– ensures the exercise of constitutional rights, freedoms and obligations;
– indicates the possibility of violation of human rights;
– indicates circumvention of the public;
– indicates harmful negative consequences of activity (inaction) of individuals or legal entities, etc.[1].

Such provisions are the result of the application of the dispositive method of legal regulation in the circulation of classified information and are used by journalists and other subjects to conduct journalistic investigations in the modern information society.

2.4 Methods of legal regulation of cybersecurity

In contrast to the definition of "information security", which, as noted, is somewhat outdated and such that does not objectively correspond to the current relations and realities of legal regulation, a rather progressive definition of the term "cybersecurity" is established in Ukraine – it is the protection of vital interests of human and citizen, society and the state upon using cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security of Ukraine in cyberspace[2].

The new Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" dated 05.10.2017 has expanded the understanding of the term "cybercrime (computer crime)", which is defined as socially dangerous act within cyberspace and/or with its use, the liability for which is stipulated by Law of Ukraine on criminal liability and/or is recognized as a crime by international treaties of Ukraine. We shall point at the fact that despite the general "imperativeness" of the said Law, there is place for dispositive features in the treatment as cybercrime of not only "classic" offenses, expressly stipulated by Section XVI of the Criminal Code of Ukraine "Crimes in the field of application of electronic computing machines (computers), systems and computer networks and telecommunication networks", but also of other socially dangerous actions involving the use of cyberspace. With the development of information technology, the list of such offenses will steadily increase, as the number of offenses committed without the use of the Internet grows smaller. The list of historically known criminal offenses of phishing, carding, fraud in banking (payment) systems will only expand.

It should be noted that the Council of Europe Convention on Cybercrime of 21.11.2001 (hereinafter referred to as "the Convention"), which is ratified by Ukraine, is aimed at increasing the efficiency of criminal investigations and prosecutions con-

[1] Law of Ukraine "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12

[2] Law of Ukraine "On Basic Principles of Cyber Security of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19

nected with criminal offenses related to computer systems and data, at the possibility of gathering evidence connected with criminal offenses in electronic form[1]. 56 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 Council of Ukraine was elected to the governing body of the Committee – the Bureau of the Convention Committee. Predominantly using the imperative method of legal regulation, the Convention addresses the issue of combating cybercrime as the greatest threat to cybersecurity – that is, to the vital interests of individuals and citizens, society and the state during using cyberspace.

The provisions of the Convention regarding the promptness of processing requests for the preservation of electronic evidence, the provision of information by national Internet service providers, replies to requests for legal aid, etc. are based on imperative grounds.

European and world practices indicate that public-private partnership form an integral part of law enforcement action in the field of cybercrime. The management of these relationships, both in the context of crime and in the context of cybersecurity, should be addressed with due regard for 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 the Internet service providers and Ukrainian law enforcement bodies. After all, domestic practices confirm that imperative decisions do not obtain proper implementation. For example, the decision of the Council for National Security and Defence of Ukraine dated April 28, 2017 "On Application of Personal Special Economic and Other Restrictive Measures (Sanctions)"[2], enacted by Presidential Decree No. 133 dated May 15, 2017, regarding the provision of information security and cyber security, requires the development and implementation of the mechanism of blocking of information resource by operators and providers through their telecommunication and information and telecommunication networks. 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, prediction, prevention, neutralization of cyber threats, cyber-attacks and cybercrime and the restoration of the stability and reliability of the functioning of communication, technological systems, was not adopted. This was largely due to the lack of proper public discussion of the relevant mechanisms (the existence of which during a hybrid aggression against Ukraine is reasonable in most cases) and the lack of a basis for effective public-private partnerships. It is noteworthy that in this respect the Situation Centre for Combating

[1] Council of Europe Convention on Cybercrime. (2001, November). Retrieved from http://zakon4.rada.gov.ua/laws/show/994_575.

[2] Law of Ukraine "On Application of Personal Special Economic and Other Restrictive Measures (Sanctions)" (2017, April). Retrieved from https://zakon.rada.gov.ua/laws/show/n0002525-19

Cyber Threats of the Security Service of Ukraine is a rather progressive platform for elaboration of such a partnership in the field of cybersecurity.

Thus, relations regarding cybersecurity are predominantly governed by the imperative method of legal regulation (for example, upon establishing technical requirements for the protection of state electronic information resources). However, only a dispositive method should be applied for normalization of the public-private partnership matters.

CONCLUSIONS

This paper proposes the scientific hypothesis on the division of the subject of legal regulation of the security of a person, society, state into three aspects: information security, classified information security and cybersecurity.

Legal regulation of information security relations is aimed at counteracting negative information influence in the information space of the state, normalization of relations concerning the classified information security is aimed at creating an organizational and legal regime, provision of access, etc., and regulation of relations regarding the cybersecurity is connected with detection, prevention and neutralization of potential threats to critical information infrastructure objects.

The paper concludes that the dispositive method of legal regulation prevails upon ensuring information security of the individual, society and the state, since the processes of circulation of mostly open information are regulated and there is a requirement to observe the constitutional principles of freedom of expression and the right to information. At the same time, a presumption is made about further reinforcement of imperative regulation of issues of ensuring the security of the person, society and the state in the part of combating misinformation as a type of information offense.

Legal regulation of classified information security is predominantly performed with the application of the imperative method of legal regulation, as it mainly concerns the protection of the right to such information. Emphasis is placed on the fact that the dispositive method of legal regulation in the circulation of classified information is applied in the part of collecting and disseminating socially necessary information.

Public relations in terms of ensuring cybersecurity are predominantly governed by an imperative method of legal regulation, although it is concluded that the exclusive application of dispositive method of legal regulation is necessary for the normalization of the public-private partnership issues.

REFERENCES

[1] Soomro, Z.A., Shah, M.H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225.

[2] Xu, D. (2017). Active security architecture of cyberspace information based on the law of universal logical partial order. *Boletin Tecnico/Technical Bulletin,* 55(17), 401–409.

[3] Volkova, V.N., & Chernyi, Y.Y. (2018). Application of systems theory laws for investigating information security problems. *Automatic Control and Computer Sciences, 52*(8), 1164–1170.
[4] Cervone, H.F. (2016). Information doesn't always want to be free: An overview of regulations affecting information security. *Digital Library Perspectives,* 32(2), 68-72.
[5] Efremova, M.A., & Agapov, P.V. (2016). Crimes against information security: International legal aspects of fighting and experience of some states. *Journal of Internet Banking and Commerce,* 21(S3), 34–37.
[6] Camaj, L. (2016). Governments' uses and misuses of freedom of information laws in emerging european democracies. *Journalism and Mass Communication Quarterly,* 93(4), 923–945.
[7] Naarttijärvi, M. (2018). Balancing data protection and privacy – the case of information security sensor systems. *Computer Law and Security Review,* 34(5), 1019–1038.
[8] Park, W., Na, O., & Chang, H. (2016). An exploratory research on advanced smart media security design for sustainable intelligence information system. *Multimedia Tools and Applications,* 75(11), 6059–6070.
[9] Anderson, C., Baskerville, R.L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems,* 34(4), 1082–1112.
[10] Wang, C. (2017). Analysis of six legal systems on cyber security law. *Journal of Nanjing University of Posts and Telecommunications (Natural Science),* 37(1), 1–13.
[11] Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. *Journal of Management and Governance,* 21(4), 793–814.
[12] Porcedda, M.G. (2018). Patching the patchwork: Appraising the EU regulatory framework on cyber security breaches. *Computer Law and Security Review,* 34(5), 1077–1098.
[13] Haeberle, K.S., & Todd Henderson, M. (2018). A new market-based approach to securities law. *University of Chicago Law Review,* 85(6), 1313–1393.
[14] Parmar, A., & Patel, K. (2016). *Critical study and analysis of cyber law awareness among the netizens. Advances in Intelligent Systems and Computing,* 409*,* 325–334.
[15] Zhao, X. (2017). Optimization mode analysis of personal information legal protection under the network environment. *Boletin Tecnico/Technical Bulletin,* 55(8), 274–281.
[16] Schulzke, K.S., & Berger-Walliser, G. (2017). Toward a unified theory of materiality in securities law. *Columbia Journal of Transnational Law,* 56(1), 6–70.
[17] Berliner, D. (2016). Transnational advocacy and domestic law: International NGOs and the design of freedom of information laws. *Review of International Organizations,* 11(1), 121–144.
[18] Kalyuzhny`j, R.A., & Martsenyuk, A.G. (2008). Subject and Methods of Information Law. *Legal Informatics*, 3(19), 5–12.
[19] Shvets, M.Ya. (2009). *Fundamentals of Information Law of Ukraine.* Kyiv: Znannia.
[20] Marushchak, A.I. (2011). *Information Law of Ukraine.* Kyiv: "Dakor".
[21] Panova, I.V. (2011). Tendencies in the Development of the Information Law System of Ukraine at the Present Stage. *Law Forum*, 2, 694–699. Retrieved from http://www.nbuv.gov.ua/e-journals/FP/2011-2/11pivnce.pdf
[22] Kovalenko, L.P. (2014). Subject and Methods of Information Law of Ukraine. *Bulletin of the V.N. Karazin Kharkiv National University No.1137. Series "Law"*, 18, 83–86.
[23] Frau-Meigs, D., O'Neil B., Tome, V., Soriano A. (2017). *Competences in Digital Citizenship Education.* Strasbourg: Council of Europe.

[24] Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Report to the Council of Europe.* Retrieved from https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.
[25] Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review,* 103(3), 985–1031.
[26] Park, D. (2016). Analysis and comparison of regulations for national cybersecurity. *International Journal of Security and its Applications, 10*(10), 207–214.
[27] Meiss, K., Krivtsova, T., Naumik-Gladka, K., & Liadova, Y. (2017). Improvement of public financial control in the context of ensuring financial security of the state. *Economic Annals-XXI*, 168(11-12), 63-68.
[28] Eichensehr, K.E. (2017). Public-private cybersecurity. *Texas Law Review,* 95(3), 467–538.
[29] Shin, Y.Y., Lee, J.K., & Kim, M. (2018). Preventing state-led cyberattacks using the bright internet and internet peace principles. *Journal of the Association for Information Systems,* 19(3), 152–181.
[30] Zuckerberg, M. *Four Ideas to Regulate the Internet.* Retrieved from https://newsroom.fb.com/news/2019/03/four-ideas-regulate-internet.
[31] Shamsi, J.A., & Khojaye, M.A. (2018). Understanding privacy violations in big data systems. *IT Professional,* 20(3), 73–81.
[32] Štitilis, D., Pakutinskas, P., & Malinauskaite, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal,* 30(4), 1151–1168.
[33] European Commission "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. (2018). Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804.
[34] Almazkyzy, K., & Esteusizov, Y.N. (2018). The essence and content of cybercrime in modern times. *Journal of Advanced Research in Law and Economics,* 9(3), 834–841.
[35] Analysis of the Draft Law "On Prevention of the Dissemination of Misinformation in the Mass Media". Retrieved from https://medium.com/@cyberlabukraine/аналіз-законопроекту-10139-щодо-запобігання-розповсюдженню-недостовірних-відомостей-у-змі-c27dcce53d06.

Anatoly I. Marushchak
Doctor of Law, Professor
Director of the Academic and Research Institute of Advanced Training and Retraining of Staff
National Academy of Security Service of Ukraine
03022, 22 M. Maksimovicha Str., Kyiv, Ukraine

Suggested Citation: Marushchak, A.I. (2019). Methods of legal regulation of the security of the individual, society, state in the information sphere. *Journal of the National Academy of Legal Sciences of Ukraine*, 26(3), 75–89.

Submitted: 13/05/2019
Revised: 16/08/2019
Accepted: 11/09/2019