Current Problems of Information Law: Analysis of Current Trends in Cybersecurity

Nataliya Davydova [1†], Iuliia Baieva[2] , Svitlana Miserzhy[3], Yevgen Pereguda [4] and Valentina Zgurska[5]

[1]Department of Private Law
Academician F.H. Burchak Scientific and Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Sciences of Ukraine, 01042, 23-a Raevsky Str., Kyiv, Ukraine
[2]Department of Political Sciences and Law Kyiv National University of Construction and Architecture
31. Povitroflotsky Avenue, Kyiv, 03037, Ukraine, 0000-0002-7734-3568
[3]Department of Philosophy, Bioetics and History of Medicine
Bogomolets National Medical University 34. Peremohy Avenue, Kyiv, 03057, Ukraine, Morphological building

[4]Department of Political Sciences and Law Kyiv National University of Construction and Architecture
31. Povitroflotsky Avenue, Kyiv, 03037, Ukraine

[5]Department of Political Sciences and Law Kyiv National University of Construction and Architecture
31. Povitroflotsky Avenue, Kyiv, 03037, Ukraine

Summary

Purpose of the article. To determine the peculiarities of the formation of information law as the basis of trends in modern cybersecurity, which is important in modern society. Informatization and post-industrialization is one of the factors in the development of modern cybersecurity.
Methodology. Methods of systematic analysis of scientific works on this problem, as well as the use of methods of analysis and synthesis and method of generalization to determine the results. Philosophical (dialectical), general theoretical, (gnoseological, structural, and functional), special (comparative and legal, inductive), and interdisciplinary methods of scientific knowledge (historical, analytical), which application is predetermined by a systematic approach, were used as a methodological basis of research.
Scientific novelty. The author proposed a study consisting in clarification of the concept of information law in the context of the development of modern cybersecurity. The article reflects the peculiarities of cybersecurity as an aspect of information law. Based onthe theoretical and methodological analysis, the essential features of information law were analyzed, the characteristic features of cybersecurity as a manifestation of information law in the context of globalization processes were analyzed. The features of informatization as one of the elements of technology were considered, and the tasks and issues of cybersecurity were defined. The features of information law as an aspect of global cybersecurity are summarized. The article reflects the main components of cybersecurity. The appropriateness of analyzing current trends in information law as a goal achievement is substantiated. **The relevance of the study** is due to the definition of intensive development of information and communication technologies in the modern period of formation of the post-industrial information society.
Conclusions. The research has become the basis for the concretization of the concept of the information society. The presented research does not exhaust the whole essence and requires further study of individual aspects.

Keywords: *information society, cyber-attacks, digitalization, information and communication technologies, hybrid wars, information law; information policy.*

1. Introduction

At the present stage of social development information and communication technologies are actively developing, determining the features of the development of different spheres of activity. Information society requires special approaches to the implementation of safe space around the world, which is important in the context of the introduction of innovative technologies, because it is necessary to form cybersecurity in the information space, and it is necessary to acquire skills and abilities to use innovative technologies in the process of determining the main trends of cybersecurity formation. Information law as a security system process requires modernization by the requirements of modern technological advances [5].

At the same time, an important role in the process of information activity is played by the personality in the implementation of legal analysis. Therefore, to achieve the true signs of determining the features of modern cybersecurity should be analyzed modern information law as one of the manifestations of information and communication technologies. The relevance of the response problem lies in the conditions of hybrid warfare. Hybrid warfare is a modern problem that intensifies in the process of the information society. Thus, cyber-attacks are active and can cause great harm. A cyber-attack is a

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.101

manifestation of information warfare, but the harm is done in the physical environment.

The Internet is one of the most important factors in the development of modern society. The Internet increases the efficiency of scientific and economic activities, as well as increases productivity in various spheres through the exchange of information, ideas, cultural innovations, which erases certain boundaries between people [6]. Accordingly, based on this conclusion, it can be argued that the Internet is the cause of the global revolution, scientific, communicative, and business. However, there are also negative manifestations of Internet technology, which is shown in cyberspace, which has many connections and connections, which leads to serious risks, because such connections can be used not only by law-abiding people but also by offenders. An attacker can find a vulnerable link in the network and carry out a cyberattack.

Researchers Bessarab A. (2021) [5], Mitchuk O. (2021) [5] studied social networks as a phenomenon of the information society. Bondar I. (2021) [6], Humenchuk A. (2021) [6] studied conceptual and innovative approaches of higher education institutions to the model of successful specialist training. So, based on the analysis of theoretical and methodological approaches the main trends in the use of information law as an aspect of cybersecurity have been identified.

The purpose of the article is to investigate the effectiveness of information law trends in the context of cybersecurity definition. The goal defined the corresponding objectives: analyze the theoretical and methodological basis for the application of information law; determine the peculiarities of cybersecurity in the context of information law; examine the effectiveness of information law.

2. Materials and Methods

The modern stage of the strategic formation of security space involves the improvement of information law and is a factor in deterring rivals. The SBU has neutralized cyber incidents and cyber-attacks on information resources. Therefore, cyber security is an important trend of protection against cyber-attacks on information resources. Also important is countering cyber threats and ensuring national cyberspace [7]. Human information culture and critical thinking is important in the process of escalation and hybrid warfare. Effective measures ensure the protection of each individual in the context of the formation of information law and cyber defense.

The research work is based on the approaches of scientists who researched the main conceptual provisions of the mentioned problem. The method of analysis and synthesis was applied to define the concept of cybersecurity in the context of information law formation [8]. Thus, the researchers analyzed the conclusions of scientists on the appropriateness of using appropriate methods in the process. The scientific method was used to determine the essence of the concept of information law in the context of activities in the information space.

In the course of the study, cybersecurity trends were analyzed [16]. Yes, computer technology was involved for them, through which they studied information law. With the help of philosophical methods, which became the ontological basis of scientific work, in particular, dialectics, investigated cybersecurity as an important component of information in the broad sense and national security of Ukraine, identified the key structural components of cybersecurity. The study analyzed the interdependence of cybersecurity and hybrid warfare. The historical method analyzed the evolution of cyber security theories and concepts. The use of the analytical method contributed to the classification and structuring of cybersecurity threats to Ukraine, determining the specifics of mechanisms to counter them, as well as analyzing the functioning of cybersecurity actors in Ukraine. The comparative legal method underpinned the study of international cybersecurity experience in the context of information law. The formal-legal method was used in the interpretation of legal information norms to clarify their essence, content, and the will of the legislator expressed in them. The structural and functional analysis allowed us to determine the compliance of normative legal acts with which the current system of legal support for cybersecurity in Ukraine is related to real social relations in this area.

3. Results

The need to define today's conceptual approaches to the formation of the system of legal regulation of information security in the conditions of great challenges in the global information society is largely related to the construction of digital economy and globalized information society, the transition of the innovative economic system, post-industrial society of a new formation, as well as the need for modernization and transformation of law in the information space, conceptual identification of interdisciplinary links and features in the field, integrated legal regulation of relationships in the field of information security.

The old approach to building a system of legal regulation in the context of information security, based on a hierarchical system of normative legal regulation, needs a new rethink [9]. It is possible to identify, first of all, international factors, conditions, and regularities that condition this process - it is a change of paradigms in the international legal regulation of the sphere of information

security, creation of international information law, and interstate alliances and formations, inducing the role of international principles of legal provision of information security, development of international threats in the sphere of cybersecurity [11]. At the international level, the transformation of the legal provision of information security is also increasingly influenced by the processes of the increasing complexity of digital technologies, primarily artificial intelligence and cyber-physical systems, neural networks, and quantum technologies [12]. A significant contribution to the processes of transformation of the legal provision of information security is also made by the rapid development of legislation in the field of information security at the national level.

Information law is shaped in the context of the development of interdependencies defined around the information space. Information is the main resource under protection and at the same time is a mechanism for creating cybersecurity [13]. Analysis of theoretical approaches to information law allows us to argue that the basis of new legal approaches is the creation of a system of virtual information legal field, which is much broader and more global covering relationships in modern information post-industrial society.

The experience of foreign states and experience shows an avalanche-like process of adopting a huge array of legal, technical, ethical, organizational norms aimed at regulating various processes in the sphere of information security. Great challenges in the conditions of information society make it necessary to find more universal, complexly organized mechanisms for building a system of legal regulation of information security, taking into account the specifics of the mechanisms of law transformation, the need for closer development of legal, technical, moral and corporate norms [14].

The experience of individual countries in the openness of the normative legal environment is instantly transformed, improved, and implemented in the context of the new challenges of our time. Patterns of benefits of legislative borrowing in the field of information security of some countries, integration associations in others are formed. Everyone can feel the danger in the conditions of hybrid or information warfare, regardless of the real place of residence [15]. Breakthrough, innovative projects are also often implemented at the level of individual states to create unique legal regimes in the sphere of certain institutions in the field of information security - this is what distinguishes one country from another, including the use of artificial intelligence and neural network technologies, information security internet of things and industrial internet, information security of information infrastructure, etc.

All these factors have a systemic impact on the development of a number of institutions in the sphere of legal regulation of information security. The importance of interdisciplinary research projects related to the processes of intensifying the transition to the digital age in all spheres of society, the development of public policy, including the formation of strategic planning in this area, information and legal issues of improving the system of public administration to ensure the development of law in the conditions of formation of the information society, digital economy, and the implementation of strategic objectives of information security is also growing. In this regard, it is important to form new approaches to the problems of harmonization and comprehensive cross-sectoral legal regulation of information security based on the development of a new generation of national strategic policy documents and a new regulatory environment to ensure a favorable legal regime of modern information technology development and information security [16]. Given these circumstances, modern legal approaches caused by the emergence of essentially new social relations, new regulators, the development of a system of experimental legal regimes, the emergence of new subjects and objects of legal relations, the need to transform the institute of responsibility, taking into account the growth of risks and threats in the field of information security.

Among the urgent problems of shaping the system of regulation of information law enforcement in the context of the great challenges in the global information society and the transformation of the law, the problem of the impact of digital technologies on information security should be highlighted. It should be recognized that today the processes of practical implementation of digital technologies, including cyber-physical systems, have intensified in various areas [17]. Yes, no one is surprised anymore by the emergence of drones not only in the field of transportation. As an example of this use, there are projects to actually replace courier services with product delivery using drones. Journalists and 1T specialists point out that in the near future, drones will become full-fledged jobs, swarm together and gain a certain degree of autonomy within neural networks. They will accumulate information, analyze it according to a predetermined algorithm, and react independently (recognize a person in a photo).

One of the promising areas of digitalization and implementation of innovative solutions are becoming transportation systems, where already today unmanned vehicle technologies are used for automatic identification with instant data transfer. Experts plan to change transportation systems under the influence of unmanned technologies, increased environmental requirements, fluctuating fuel prices, and changes in workforce management [18]. Despite the development of cyber-

physical systems, no proper legal solutions have yet been found on the issue of their legal personality, liability, and a number of problems arising from it. In a broader sense, it is obvious that all this requires systemic science-based projects in the field of information security and its component - cybersecurity. Of course, it is advisable to consider these problems in this ratio.

One of such advanced directions of digitalization today is stated as the development of a national approach in the implementation and enforcement of information law.

The dynamics of creating new technologies, products, and scientific solutions is growing very intensively, which in modern conditions confirms the hypothesis about the importance of cybersecurity and ensuring information law, and also confirms the importance of the information world in modern conditions.

The modern world demonstrates the high dependence of human beings on technology in various manifestations of social life. People often use social media, which leads to danger as personal data and other problems are disclosed. This requires the prompt and systemic response of various public institutions and defines one of the main challenges of information law and legal information security vectors [19]. To successfully cope with modern challenges and threats in legal science and especially in information law, new theoretical and practical solutions are needed, defining principles and regularities of their organization and development, which will increase the efficiency of law enforcement in the conditions of modern digital transformation and a variable world.

To determine from the perspective of information law trends in the development of the legal provision of information security in the context of the formation of the digital economy, digitalization of public administration, the globalization of the digital space requires analysis of current legal risks and threats in the field of legal provision of information security, the synergy of these processes, development, and implementation of national projects of legal problems to improve the system of strategic planning documents, as well as the role of legal forecast The above list, however, is not exhaustive, only generally reflects these problems.

Thus, we must recognize that the inertia of the development of law and legal science has not yet allowed creating the necessary legal mechanisms, tools to protect individuals, society, and the state from new challenges and threats, to overcome risks, to explore and justify the role and place of synergistic processes in this area, given their non-linearity and non-triviality All this requires modernization of legal approaches to regulating new social relations.

For the implementation of strategic, doctrinal tasks of ensuring information security, fundamental multidimensional research, the obvious role of legal provision, the transformation of the system of human rights are important [20]. Analysis of the trends of legal regulation of relations in the information sphere in foreign countries, the adoption of international acts shows different approaches.

The structure of information law corresponds to certain norms and consists of objects, subjects, and other components of the law. Also, to implement information legal relations, one must have certain responsibilities as defined by the regulation of information legal relations.

The threat to humanity is hybrid warfare, which is potentially destructive to the state. Hybrid war involves the destruction of state security because the main weapon in such a war is false information, which is spread against a person or state as a whole. Confrontation leads to negative consequences. Therefore, in hybrid warfare, it is also important to ensure cybersecurity. The main task of cybersecurity is the protection of information. In particular, protection must be at the level of the state, the world, as well as for a single individual.

Thus, as a result of the analysis of information law, in particular in the creation of cybersecurity, intellectual independence, creativity, social and information competence is formed. Today, information law has proven its importance and need at all levels. Its implementation contributes to the creation of additional opportunities for updating the content, methods of formation of information law, and dissemination of knowledge based on modern multimedia technologies. Information law allows diversifying the social process, which is also a factor in increasing interest in the discipline and motivation. Thus, the introduction of information law is a promising direction for the development of society, their use improves the quality of cybersecurity due to such advantages as efficiency, flexibility, modularity, meeting the requirements of the modern concept of the institution of protection.

4. Discussion

The issue of cybersecurity depends mainly on the institutional implementation of information law. This statement may or may not be true. We believe that information law is decisive in increasing the effectiveness of cybersecurity [5]. The success of a person's activity in the information space is directly related to knowledge in the legal field. Informational orientation is defined as an individual's readiness to learn, mastering relevant activities that play a particularly important role in future practical

competence in cybersecurity [6]. In recent decades, there has been a dissatisfaction with information security training, which leads to hybrid warfare and the negative consequences of the information flow. The main reason for the lack of practical skills in the field of informatization is considered a decrease in their information capacity [7]. We have analyzed the theoretical basis of the information law factor in the context of cybersecurity formation, which encourages a creative solution to the problem. Success can be achieved only with a creative solution to the problem because another option, i.e., a similar solution can only lead to the consequences that have already been. Therefore, there will be no progress in development.

The study of the data provided the basis for determining the factors of information law to achieve the goal that contributed to the establishment of cybersecurity features. For example, the formation of a positive motivation for the implementation of information law, the implementation of work in this area affects many factors [8]. Among the main ones: a flexible system of information process organization, a clearly delineated range of tasks and possible ways and means of their implementation, fruitful cooperation between each other, control and self-monitoring, the ability of a person to self-evaluate.

Keep in mind that an effective approach to enhancing personal protection is knowledge and skills that must be disseminated not only to professionals but also to ordinary people. Information security is a dialogical process in which interaction between people takes place in the context of information protection as a leading manifestation of cybersecurity. Unlike one-way communication in a linear cybersecurity system, multilateral communication in the context of information cooperation involves the activity of each subject of the educational process, not just the teacher, parity, absence of repressive management measures, and mentorship. This is a strategy of higher education, the purpose of which is the intellectual autonomy of the person with developed information competence [9]. Let us consider the main aspects of the creation and implementation of information law in public life, which are used in the process of creating cybersecurity.

During the analysis, we determine that knowledge provides an opportunity for influence, encouraging people to be mentally active, to be creative, to explore and search for new ideas to solve various problems of activity in the context of cybersecurity. The main goal of information security organizations is not only the delivery of information but also its active assimilation. The requirements for this form of cooperation are two-way flow of information or dialogical, innovative nature of the information delivered and preparation of information security; constant interactivization, that is, overcoming the one-sidedness of the information flow through methods and technologies [10]. The latter can include the interpretive dialogue of creating internal motivation for the upcoming collaborative work, providing psychological comfort, the installation of active search, and obtaining new knowledge in the process of cybersecurity formation.

Consequently, during the implementation of information knowledge, it is better to talk rather than talk to the audience, which contributes to the creation of a dialogic form of learning. It should be noted that an important factor for modern man is “provoking a smile” - humor contributes to the development of a comfortable environment for critical thinking in the process of forming a safe environment [11]. To increase the effectiveness of the use of information law in the final stage - the solution of creative tasks aimed at independence and creative search, where the person acts as an organizer, consultant, and adviser. It can be argued that compared to other methods, information law is focused on more interaction of professionals with each other, on the dominance of human activity in the process of cybersecurity formation [12]. It has been suggested that the dominant role of the specialist in the field gives way to the activity of ordinary people, and the task of the specialist becomes the creation of conditions for their initiative. He regulates the cybersecurity process and deals with its overall organization, defining a certain direction.

As a result, it has been proved that if appropriate methods are used in the process of implementation of information law, it is possible to achieve a significant increase in the effectiveness of the process by purposeful activation of thinking, when people are forced to be active in organizing their virtual life, to show independence, creativity in the process of organizing cybersecurity. In our opinion, the introduction of a number of approaches activates individual or group work in the process of creating cybersecurity.

So, we have proven that information law is the most effective factor in creatively addressing cybersecurity, which, in turn, is a major factor in modern life.

5. Conclusions

The research was conducted to determine the effectiveness of information law in the process of organizing cybersecurity. The basic theoretical basis for the use of innovative methods as an effective technology for organizing cybersecurity was analyzed.

Based on the findings of researchers on the importance of cybersecurity in the development of innovative technologies, it was determined that the information law

most effectively shapes creative problem solving, and therefore contributes to the level of creativity in the new challenges of the information society. Thus, the results of the study confirm that the information society is a factor in the formation of favorable conditions for the creation of information security. It is determined that informativeness contributes to creativity.

The research was conducted on the formation of cybersecurity based on information law. To determine the effectiveness of cybersecurity, indicators of creativity in organizing communication were compared. According to the results of the study, it can be argued that informational methods are significantly more effective because they have significantly higher rates.

The form of implementation of information law using information and communication technologies provide interactive interaction in the process of organizing information security, which is the essence of cybersecurity. Modern life is transformed into a digital environment, so there is a need to possess the knowledge and skills to use information and communication capabilities.

Summarizing the theoretical foundations of scientific papers on the topic, as well as methods and materials of the study, it was determined that cybersecurity is a major factor in the implementation of information law in modern life.

References

[1] Bessarab A., Mitchuk O., Baranetska A., Kodatska N., Kvasnytsia O., Mykytiv H.: *Social networks as a phenomenon of the information society*. Journal of Optimization in Industrial Engineering, vol. 14(1), pp. 35–42, (2021)

[2] Bondar I., Humenchuk A., Horban Yu., Honchar L., Koshelieva O.: *Conceptual and innovative approaches of higher education institutions to the model of preparing a successful professional during the Covid pandemic*. Journal of Management Information and Decision Sciences, vol. 24(3), pp. 1–8. (2021).

[3] Pylypchuk V. H.: *Actual problems of state policy on the protection of human rights and security in the information sphere*. In: Information law: modern challenges and directions of development: Materials of the first scientific-practical conference, October 18, 2018, Kyiv. Arranged: V. M. Furashev, S. Yu. Petriaiev. Kyiv: National Technical University of Ukraine IhorSikorskyi Kyiv Polytechnic Institute “Polytechnika” Publishing House. 2018. 196 p.

[4] Skulysh Ye. D: *Information security: the latest challenges for Ukrainian society*. Information and Law, vol. 2/5, pp. 170-175 (2012)

[5] Tarasiuk A. V.: *Conceptual and categorical synthesis of legal provision of cybersecurity of Ukraine*. Comparative and analytical law, pp. 296-298.

[6] Abulalrub , I. & Stensaker, B.: *How are universities responding to demands for improved learning environments?* Journal of Further and Higher Education. (2017). https://doi.org/10.1080/0309877X.2017.1311991.

[7] Allessie D., Sobolewski, M., Vaccari, L., and Pignatelli, F. Blockchain for Digital Governments. JRC Science for Policy Report (2019). https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government

[8] Allman B.: Socioculturalism. In R. Kimmons, The Students' Guide to Learning Design and Research. EdTech Books. (2018). Retrieved from https://edtechbooks.org/studentguide/socioculturalism

[9] Brown A., Fishenden, J., Thompson, M. and Venters, W., Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: towards a Platform Assessment Framework (PAF). Government Information Quarterly (2017). ISSN 0740-624X

[10] Burnett, C. Merchant, G.: *Is There a Space for Critical Literacy in the Context of Social Media?* English Teaching: Practice and Critique, vol.10, no. 1, pp.41-57 (May 2011)

[11] Goel, V., Raj, S. and Ravichandran, P.: *How WhatsApp Leads Mobs to Murder in India*. (2018). https://www.nytimes.com/interactive/2018/07/18

[12] Gygli, S., Haelg, F., Potrafke, N., & Sturm, J. E.: *The KOF globalisation index-revisited*. The Review of International Organizations, no.14, pp. 543–574 (2019) https://link.springer.com/content/pdf/10.1007/s11558-019-09344-2.pdf

[13] Maj Gen PK Mallick. U.S.: *National Cyber Strategy and Department of Defence (DoD) Cyber Strategy: An Analysis*. (2018) https://www.vifindia.org/sites/default/files/US-National-Cyber-Strategy-andDepartment-of-Defence-Cyber-Strategy.pdf

[14] Menthe, D. Jurisdiction In Cyberspace: A Theory of International Spaces. (n.d.) https://repository.law.umich.edu

[15] McKinsey Global Institute. Applying artificial intelligence for social good. McKinsey Global Institute. (2018). https://www.mckinsey.com/featuredinsights/artificial-intelligence/applyingartificial-intelligence-for-social-good

[16] Vuckovic, T.: *The Overall Goal of Education and General Purpose*. International Journal For Empirical Education and Research, vol. 3(20), pp. 53-66. (2019), https://journals.seagullpublications.com/ijeer/assets/paper/IJ0620191784/f_IJ0620191784.pdf

Nataliya Davydova, Doctor of Science of Law Professor Leading Researcher, Department of Private Law Academician F.H. Burchak Scientific and Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Sciences of Ukraine 01042, 23-a Raevsky Str., Kyiv, Ukraine, ndavydova11@gmail.com, 0000-0002-2362-3724
AAR-8239-2021
57224514537

Iuliia Baieva, Candidate of Political Sciences Assistant Professor Department of Political Sciences and Law Kyiv National University of Construction and Architecture 31 Povitroflotsky Avenue, Kyiv, 03037, Ukraine, 0000-0002-7734-3568

Svitlana Miserzhy, Candidate of Political Sciences Assistant Professor
Department of Philosophy, Bioetics and History of Medicine Bogomolets National Medical University
34. Peremohy Avenue, Kyiv, 03057, Ukraine, Morphological building, 0000-0002-7403-9261

Yevgen Pereguda, Doctor of Political Sciences Professor Head of the Department Department of Political Sciences and Law Kyiv National University of Construction and Architecture 31 Povitroflotsky Avenue, Kyiv, 03037, Ukraine, pereguda.iev@knuba.edu.ua, yevgennn@ukr.net
38-097-396-92-60, 0000-0001-7561-7193
O-8559-2018, 56156421900

Valentina Zgurska, Candidate of Political Sciences Assistant Professor Department of Political Sciences and Law Kyiv National University of Construction and Architecture 31 Povitroflotsky Avenue, Kyiv, 03037, Ukraine, 0000-0001-7490-1942