International experience of ensuring cybersecurity in the country and possibility of its application in Ukraine

Experiencia internacional en garantizar la ciberseguridad en el país y posibilidad de aplicarla en Ucrania

Experiência internacional em garantir a segurança cibernética no país e possibilidade de sua aplicação na Ucrânia

Oksana Vasilievna Pchelina[1]
Yevhenii Deoniziyovych Skulysh[2]
Iurii Buglak[3]
Roman Victorovich Myroniuk[4]

Received: February 22th, 2021
Accepted: March 25th, 2021
Published: July 6th, 2021

How to cite this article:
Oksana Vasilievna Pchelina , Yevhenii Deoniziyovych Skulysh, Iurii Buglak & Roman Victorovich Myroniuk. *International experience of ensuring cybersecurity in the country and possibility of its application in Ukraine*. DIXI, vol. 23, n°. 2, julio-diciembre 2021, 1-16.
DOI: https://doi.org/10.16925/2357-5891.2021.02.01

Research article. https://doi.org/10.16925/2357-5891.2021.02.01

[1] Doctor of Jurisprudence, Associate Professor, Assistant Professor at the Department of Criminal Procedure and Organization of Pre-trial Investigations of the Faculty № 1 of Kharkiv National University of Internal Affairs.

E-mail: pchelinaov@icloud.com

ORCID: https://orcid.org/0000-0003-0224-1767

[2] Doctor of Jurisprudence, Professor, Honored Lawyer of Ukraine, Head of the Research Center for Information and National Security of the Research Institute of Information Security of the National Academy of Sciences of Ukraine.

E-mail: Nina82mail@gmail.com

ORCID: https://orcid.org/0000-0001-9646-8473

[3] Ph.D. in Law, Academician of the Academy of Administrative and Legal Sciences, Honored Lawyer of Ukraine, Member of the Central Election Commission of Ukraine.

ORCID: https://orcid.org/0000-0002-0428-0121

[4] Doctor of Jurisprudence, Professor, Professor at the Department of Administrative Law, Process and Administrative Activity of Dnipropetrovsk State University of Internal Affairs.

E-mail: mironyk1311@gmail.com

ORCID: https://orcid.org/0000-0002-9620-5451

Abstract

The purpose of this article is to reveal the essence and characteristic features of cybersecurity as one of the most important components of stable functioning of the modern society. Examples of successful experience of developed foreign countries on cybersecurity are considered, and possible ways of its use in Ukraine are offered. In particular, the public's attention is focused on extremely important issues such as national defense in cyberspace, protection of private legitimate interests of individuals in the network and effective information policy by the state towards citizens. It is noted that the cybersphere has long been one of the most important components of the world society and the world economy. This statement is primarily based on the fact that today more and more banking, trade and other settlement or logistics operations, both within one country and in international relations, are carried out using modern computer, telecommunications and other innovative technologies and devices. It is stated that the sphere of public life, which is outlined in this article, is in dire need of its clear and unambiguous legal regulation. This is especially true in developing countries, including Ukraine. After all, their state system and legal framework are not yet stable and stable. The authors' definitions of "cybersecurity", "cyber-subjectivity" and "network sovereignty" are offered. In addition, the relationship between the level of development of the cybersphere in a particular country and the level of its economic development and general financial well-being was studied. It is determined that it is extremely important for Ukraine to adopt the successful experience of some developed foreign countries in the field of protection and processing of information in cyberspace.

Keywords: Cybersecurity, crime prevention, information technologies, interaction, international experience, national security, national legislation, network sovereignty, private interests, state system..

Resumen

El propósito de este artículo es revelar la esencia y los rasgos característicos de la ciberseguridad como uno de los componentes más importantes del funcionamiento estable de la sociedad moderna. Se examinan ejemplos de experiencias exitosas de países extranjeros desarrollados en materia de ciberseguridad y se ofrecen posibles formas de utilizarla en Ucrania. En particular, la atención del público se centra en cuestiones extremadamente importantes como la defensa nacional en el ciberespacio, la protección de los intereses legítimos privados de los individuos en la red y una política de información eficaz por parte del Estado hacia los ciudadanos. Se señala que la ciberesfera es desde hace tiempo uno de los componentes más importantes de la sociedad y la economía mundiales. Esta afirmación se basa principalmente en el hecho de que hoy en día cada vez más operaciones bancarias, comerciales y otras operaciones de liquidación o logística, tanto dentro de un país como en las relaciones internacionales, se llevan a cabo utilizando la informática moderna, las telecomunicaciones y otras tecnologías y dispositivos innovadores. Se afirma que la esfera de la vida pública, que se esboza en este artículo, necesita urgentemente una regulación jurídica clara e inequívoca. Esto es especialmente cierto en los países en desarrollo, incluida Ucrania. Al fin y al cabo, su sistema estatal y su marco jurídico aún no son estables ni están estabilizados. Los autores ofrecen definiciones de "ciberseguridad", "cibersubjetividad" y "soberanía de la red". Además, se estudia la relación entre el nivel de desarrollo de la ciberesfera en un país concreto y el nivel de su desarrollo económico y bienestar financiero general. Se determina que es sumamente importante que Ucrania adopte la experiencia exitosa de algunos países extranjeros desarrollados en el ámbito de la protección y el tratamiento de la información en el ciberespacio.

Palabras clave: ciberseguridad, prevención del delito, tecnologías de la información, interacción, experiencia internacional, seguridad nacional, legislación nacional, soberanía de la red, intereses privados, sistema estatal.

Resumo

O objetivo deste artigo é revelar a essência e as características da cibersegurança como um dos componentes mais importantes do funcionamento estável da sociedade moderna. São considerados exemplos de experiências bem-sucedidas de países estrangeiros desenvolvidos em segurança cibernética, e são oferecidas possíveis formas de seu uso na Ucrânia. Em particular, a atenção do público está voltada para questões extremamente importantes como a defesa nacional no ciberespaço, a proteção dos interesses legítimos privados dos indivíduos da rede e uma política de informação eficaz por parte do Estado para com os cidadãos. Observa-se que a ciberesfera é há muito tempo um dos componentes mais importantes da sociedade mundial e da economia mundial. Esta afirmação baseia-se principalmente no fato de que hoje em dia cada vez mais operações bancárias, comerciais e outras operações de liquidação ou logística, tanto dentro de um país como nas relações internacionais, são realizadas utilizando computadores modernos, telecomunicações e outras tecnologias e dispositivos inovadores. Afirma-se que a esfera da vida pública, que é delineada neste artigo, precisa muito de sua regulamentação legal clara e inequívoca. Isto é especialmente verdadeiro nos países em desenvolvimento, incluindo a Ucrânia. Afinal, seu sistema estatal e sua estrutura legal ainda não são estáveis e estáveis. As definições dos autores de "cibersegurança", "ciber-subjetividade" e "soberania de rede" são oferecidas. Além disso, foi estudada a relação entre o nível de desenvolvimento da ciberesfera em um determinado país e o nível de seu desenvolvimento econômico e bem-estar financeiro geral. Está determinado que é extremamente importante para a Ucrânia adotar a experiência bem-sucedida de alguns países estrangeiros desenvolvidos no campo da proteção e processamento de informações no ciberespaço.

Palavras-chave: Segurança cibernética, prevenção do crime, tecnologias da informação, interação, experiência internacional, segurança nacional, legislação nacional, soberania de redes, interesses privados, sistema estatal.

I. Introduction

Globalization's impact on society's development is reflected in the trends of the further formation and development of cyberspace as a new habitat of human activities, which are an integral part of communicative processes. As evidence of the development and growing importance of cyberspace in modern society, there are official data documenting a large increase in the volume of services in the info-communication sphere in the last decade. Contemporary conditions are contributed to by constant use of information technologies and new methods of communication, as well as by cybersphere development.[1]

Domestic and foreign experts have noted the significant impact of the cybersphere on society, economy, education and defense around the world for many years. Taken into account such an urgent importance of reliable and efficient operation of this area, it becomes clear why there have been a large number of cyberattacks,

1 Olga F. Guchinskaia & Irina I. Tolstikova. *Communications in Cyberspace: Designs Features*. First International Conference, DTGS 2016 St. Petersburg, Russia, June 22-24, 2016 Revised Selected Papers. Pg. 64.

successful and unsuccessful attempts to hack public and private accounts on the Internet, theft of information from electronic databases banks and commercial structures for at least the last two decades.

The active use of computer and information technology by more and more people in their daily activities and during personal or family leisure has led to an increase in hacker attacks by offenders. Moreover, experts found out that a large number of various crimes in cyberspace were committed both by offenders who acted alone based on feelings of revenge, jealousy or mischief and by criminal organizations that operate for a long period of time, and may have resources necessary to take actions that pose a danger to even the most secure government agencies or private companies. In this regard, it is worth supporting the statement of Chandra and Snowe that today the process of technical and technological development has transformed cybercrime into a fairly serious and widely branched business, thanks to which revenues are obtained compared to those obtained from drug trafficking. These authors define cybercrime as an act that uses computer technology to commit a crime.[2]

The formation and effective implementation of the state policy in the field of cybersecurity — in which a complex of measures on legal and institutional framework is developed — is a necessary condition for the effective development of the cyber-community in Ukraine. This complex of measures includes ensuring:

- The protection of vital interests of man and citizen, society and state,
- Ukraine's national interests in cyberspace,
- The formation and definition of the basic goals, directions and principles of this policy,
- The definition of the powers of state bodies, enterprises, institutions, organizations, entities and citizens in this sphere,
- The principles of state-private interaction and coordination of their activities on cybersecurity.[3]

This state of affairs should lead to a profound change in the attitude of our state towards the security of our own information and cyberspace, and hence to the

2 Akhilesh Chandra & Melissa J. Snowe. *A Taxonomy of Cybercrime: Theory and Design*. INTERNATIONAL JOURNAL OF ACCOUNTING INFORMATION SYSTEMS 38. 2020. Available at: https://doi/org10.1016/j.accinf.2020.100467

3 Ihor V. Diorditsa, Armenui A. Telestakova, Olga M. Koval, Olha A. Nazarenko & Andrii A. Nastiuk. *Information Interventions as a New Dimension of Ukraine's Cyber-Vulnerability*. REVISTA GENERO & DIREITO 1. 2020. Special Edition. Available at: https://www.periodicojs.com.br/index.php/gei/article/view/21

information security, its processing and the cyber-environment, in which this information circulates, the identification of targets, that is, prior to the adoption of information and cybersecurity measures.[4]

II. Methodology

In the study, scientists used methods of theoretical analysis and systematization to identify and specify the authors' position within the studied issues. When preparing conclusions and recommendations based on the results of the study, the method of generalization was used. In particular, the authors came to the conclusion that the legal regulation regarding the ensuring of cybersecurity differs depending on the peculiarities of the national legislation of each country. At the same time, there are general principles, fundamental prerequisites and goals for ensuring cybersecurity. In modern democracies, they are based on values that guarantee human rights and freedoms.

In turn, the method of analysis was used by the authors of this article to study the objective state of public relations, which are being developed in the field of ensuring cybersecurity both in Ukraine and abroad. The method of synthesis is used to generalize the positive experience of legal regulation of ensuring cybersecurity in foreign countries. Also, the forecasting method was used to identify possible ways of development of domestic law in the field of ensuring cybersecurity.

III. Analysis of the findings and discussion

Many leading scholars have paid attention to the study of domestic and international situations in the functioning of cybersecurity. However, despite the large number of papers on cybersecurity, there are virtually no studies researching the relationship between cybersecurity quality and legislation. The knowledge of the object of possible threats, as well as the kinds and types of possible damage, are important to determine the scope of jurisdiction of the concept of "cybersecurity" and the impact of quality from the standpoint of law. This knowledge is of great practical value, since

4 Zinaida Zhyvko, Taras Rudyi, Volodymyr Senyk & Liliia Kucharska. *Legal Basis of Ensuring Cyber Security of Ukraine: Problems and Ways of Eliminating*. Economics, finance and management review 2. 2020. Pg. 82-90. Available at: https://doi.org/10.36690/2674-5208-2020-2-82

it influences the content of cybersecurity strategies, the coverage of facilities that are under cybersecurity measures, the level and list of institutions and agencies, and the composition and scope of resources that should be involved. Cybersecurity is defined as a strategic problem at the state level[5] and covers various contexts. Existing activities involving cybersecurity (by coverage) do not allow us to consider it as the only science on professional perception, and it is currently almost impossible to predict the right combination with the confidence of knowledge and skills in this area.[6]

The issues under discussion have certain assumptions limited by legislative, time and other factors. Of course, cybersecurity is related to information security, complementing each other's dependence and impact. Thus, we can agree with the legislator, who defines that information security is a state of protecting vital interests of a man, society and the state, which prevents harm due to: incompleteness, lateness and unreliability of the used information; negative information impact; negative consequences of using information technology; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information. However, this definition has a significant assumption that finally does not improve the quality of cybersecurity.[7]

The law enforcement agencies' main focus aimed at combatting crimes that were committed with the use of cryptocurrency include struggling and prevention of illegal entrepreneurship, illegal banking activity, tax crime, illegal capital outflows, drug business, terrorism financing and legalization (laundering) of income. These crimes are significantly urgent in the whole world, as they provide further criminal economies and corresponding institutions' development (i.e. corruption, illegal immigration, etc.).[8]

The cybersphere includes the physical and non-physical space created by the following sources: Computers, mechanized systems and networks, software, computerized information, content, and the users themselves. The cybersphere is an

5 Oleksandr D. Dovhan & Ivan M. Doronin. ESCALATION OF CYBER THREATS TO NATIONAL INTERESTS OF UKRAINE AND LEGAL ASPECTS OF CYBERSECURITY: MONOGRAPH. NALS of Ukraine, NDIIP. ArtEk Publishing House. (2017). Pg. 27.

6 Mykola Vasilenko. *Strengthening the State of Cybersecurity of Information and Communicational Systems: Quality in the Context of Improving Information Legislation*. LAW HERALD 3. 2018. Pg. 18

7 Mykola Vasilenko. *Quality of Cybersecurity of Information and Communicational Systems (ICS) and Some Legislative Issues on Its Improvement*. LAW HERALD 4. 2018. Pg. 35.

8 Viktor V. Pushkarev, Valeriia V. Artemova, Sergey V. Ermakov, Elmir N. Alimamedov & Anton V. Popenkov. *Criminal Prosecution of Persons, who Committed Criminal Acts Using the Cryptocurrency in the Russian Federation*. REVISTA SAN GREGORIO 42. 2020. Pg. 330-335. Available at: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1566

artificial space (as opposed to sea, air, and land), and the communication between its components is carried out through bytes. This facilitates the creation of links and shared spaces among different intelligence disciplines, which in the past were compartmentalized and were only connected through people's minds. Cybersphere, as a new intelligence environment, is changing the basic assumptions about information and knowledge.[9] The cybersphere offers a novel media that is rapidly evolving global spaces for the publishing and circulation of argumentation, and it absorbs modern practices through digital conversation, platforming, distributing and circulating communications exchanges around the globe.[10]

Cyberspace is a difficult area for lawyers and lawmakers. With no physical constraining borders, the question of who is the legitimate lawmaker for cyberspace is complex.[11] At the moment, Internet law means so many different things to so many different people. In some sense, today — let alone tomorrow — whichever area of law we take up, we are dealing with Internet law. The same with methodology: It covers doctrinal, black letter dimension as much as it does socio-legal methods; it operates instruments of law and economics, and it also cannot be not politicized. The area is expanding exponentially. Digital technologies penetrate more and more areas of social life and in doing so they raise more and more legally relevant questions. The dynamism and the speed of such penetration is self-evident.[12]

In accordance with the current tendencies in most countries, the development of methods and techniques to ensure proper cybersecurity is one of the top priorities for governments. Currently, the level of protection of states from potential and actual cyberattacks is extremely different. Unfortunately, the situation with the development of computer and information technologies is unsatisfactory in Ukraine, as well as in a number of post-Soviet countries. Although it is not fatal. The level of cyber-defense and cyberattack systems is extremely impressive and powerful in regard to developed countries of the world like the United States of America, Germany, Canada, Great Britain and China.

9 David Siman-Tov & Noam Alon. *The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs*. CYBER, INTELLIGENCE, AND SECURITY 1. May 2018. Pg. 73-92, 81. Available at: https://www.inss.org.il/wp-content/uploads/2018/05/Cyber-Intelligence-and-Security-Volume-2-No.-1-May-2018.pdf

10 G. Thomas Goodnight. *Argumentation and the Cybersphere*. 2016. Available at: https://www.academia.edu/29925842/ARGUMENTATION_AND_THE_CYBERSPHERE_WSIA_v_3_von_Burg_ed_2016

11 Chris Reed. RETHINKING THE JURISPRUDENCE OF CYBERSPACE. Edward Elgar Publishing. (2018).

12 Oles Andriychuk. *Book Review: Rethinking the Jurisprudence of Cyberspace*. EUROPEAN JOURNAL OF LAW AND TECHNOLOGY 1. 2020. Available at: http://ejlt.org/index.php/ejlt/article/view/744

First of all, development in the field of combating international and national cybercrime was initiated by the Council of Europe Convention on Cybercrime (Budapest, November, 2001). At the same time, it was ratified by more than fifty countries, and the participating countries included some that were not members of the Council of Europe, such as the United States, Canada, Japan, Mexico, Australia and many others. Lets study in detail its main provisions. One should note that the provisions of the Convention do not apply for all countries because it is known that four countries have signed, but not ratified it, and there are opponents of signing — Russia and China.[13] The preamble to this international instrument states:

> The present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation.

Mindful of the need to ensure a proper balance between the interests of law enforcement and the respect for fundamental human rights, such as the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy, as well as the right to protection of personal information. The Convention provides for criminal liability at the national level for the following groups of crimes: offenses against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, device abuse); computer offenses (counterfeiting and computer fraud); content-related offenses (child pornography offenses); offenses classified as infringement of copyright and related rights.[14]

13 Viktor Boiko, Mykola Vasilenko & Serhii Kukharenko. *Cybersecurity in EU and Member States: Genesis and Problems of Its Strengthening*. Available at: http://www.academy.ssu.gov.ua/ua/page/page_1581426437.htm

14 *Convention on Cybercrime*. International Document dated from November 23, 2001. Available at: https://zakon.rada.gov.ua/laws/show/994_575#Text

Ukraine also ratified the Convention in 2005, but with some reservations, in particular: "Ukraine reserves the right not to apply paragraph 1 of the Article 6 of the Convention in respect of criminal liability for the manufacture, acquisition for use or provision for use of items specified in subparagraph 1.a.i, and the manufacture and acquisition for use of items referred to in subparagraph 1.a.ii of the Article 6 of the Convention"; "Ukraine reserves the right not to apply in full subparagraphs 1.d and 1.e of the Article 9 of the Convention", etc.

Besides, the United Nations General Assembly adopted Resolution was related to issues of ensuring cybersecurity.[15] The Resolution referred to specific measures: on the need to create the system of global culture of cybersecurity. The United Nations General Assembly suggested Member States to take corresponding approach to creating global culture of cybersecurity, in particular as part of their efforts to develop a culture of cybersecurity in their societies through the use and utilization of information technology. The Resolution also noted the importance of international cooperation to achieve cybersecurity by: Supporting national efforts to strengthen human potential; increase training and employment opportunities; improvement of public services and improvement of the quality of life through the use of advanced, reliable and secure information and communication technologies (ICTs) and networks; and promoting common access. This led to the adoption in the following year (2003) of the Geneva Declaration[16] that noted the need to accelerate the implementation of a global culture of cybersecurity in cooperation with all stakeholders and competent international agencies. Such efforts were to be based on broad international cooperation. It was considered appropriate, within the framework of a global culture of cybersecurity, to increase security and ensure data protection and privacy (paragraph 35). The practical implementation of the Resolution was the adoption of the Tunisian Program for the Information Society (paragraph 39), which emphasized the following: "We seek to increase trust and security in the use of ICTs by strengthening the basis for trust".

Nowadays, the level of development of a particular sphere of life in a particular country is usually inextricably linked with the level of its economic development. This state of affairs can be traced in most countries of the world. If the state is developed and has significant economic potential, its state authorities and private entities will be able to allocate significant funds to finance programs and research related to the

15 UN General Assembly Resolution "Creation of a Global Culture of Cybersecurity", dated from December 20, 2002, № 57/239. Available at: http://www.un.org/ru/ga/second/57/second_res.shtml.

16 Declaration of Principles "Construction of Information Society — Global Task in a New Century", dated from December 12, 2003. Available at https://zakon.rada.gov.ua/laws/show/995_c57#Text.

development of computer and information technology.[17] However, an exception is possible in this context. For example, it is a well-known fact that cybercriminals who secretly operated under the guise of the governments of Iran and North Korea were able to cause significant destructive damage to computer systems and databases in a number of government, commercial institutions and corporations in the United States, Canada, and Western Europe. It follows that a country, in order to be a powerful and influential player in the field of computer technology, does not necessarily have to belong to the list of the richest countries. However, there is indisputable fact that the level of economic well-being of a particular state has an undeniably positive impact on the state of its readiness to successfully resist to both internal and external cyberattacks. A significant amount of money also allows you to make a lot of positive creative improvements. Since most developed countries in Western Europe, as well as North America, have experienced all the dangers of cyberattacks over the past couple of decades, and have appreciated all the damage that has already been done or may be done in the future, they came to the rational conclusion that this problem should be covered and resolved at the level of adoption of relevant legal acts.[18]

Among other things, we can give an example of one of the first such steps, namely, the adoption of a relevant regulatory act (plan) by the German federal authorities, which was called the National Plan for Information Infrastructure Protection (NPSI). By using that step, German authorities of that time placed, first of all, a strong emphasis on the growing danger of cyberterrorism and computer hacking; secondly, it made a significant contribution to the consolidation of the German authorities' forces, law enforcement agencies, and research and educational institutions in their fight against cyberattacks, in particular, by providing the state plan for all of them, which was certainly a solid foundation for their joint activities.

We believe that that step of Germany's top political leadership was urgently needed at the time, as it made an effective contribution to the state's fight against cybercrime. In this context, we tend to consider that step by the German authorities to be correct and, in this regard, absolutely useful. Moreover, in our opinion, such political and legal decisions of government officials as the adoption of plans, strategies and resolutions similar to that German document create a strong unifying platform for effective action of government agencies and NGOs in their fight against crime and

17 On Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine dated from October 5, 2017, № 2163-VIII. Bulletin of Verkhovna Rada of Ukraine. 2017. № 45. Art. 403.

18 D. Dubova (Ed.). STATE AND PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY: INTERNATIONAL EXPERIENCE AND OPPORTUNITIES FOR UKRAINE: ANALYTICAL REPORT. NISD. (2018). Pp. 12-81.

offenses committed in cyberspace. Therefore, such steps should be properly adopted in the domestic plane.

It should be noted that the "State Plan for the Protection of Information Infrastructure", adopted by Germany in 2005, has become a kind of model for other developed countries in Western and Central Europe. For example, a number of states have adopted similar recommendations, strategies and legal acts that were later incorporated into their own national or regional legislation. In addition, we can highlight Sweden, whose government officials developed and adopted the Strategy to Improve Internet Security in Sweden in 2006. It should be emphasized that that Strategy has demonstrated significant effectiveness in practice, and therefore still, as of 2020, remains valid and smoothly functioning in the Swedish legislation.[19]

It is also important to note the experience of Estonia, which was one of the first Member States of the European Union to take clear, consistent and unambiguous steps to address current challenges and threats in cyberspace. The Estonian authorities have created and implemented the National Cybersecurity Strategy. Thus, the top leadership of Estonia decided to take those steps after several serious and large-scale cyberattacks were carried out against that country in 2000s.

It should be preliminary concluded that a kind of confirmation of the success of those plans and strategies adopted by governments and legislatures of European countries, as well as confirmation of their correctness, is the adoption of strategies, plans and declarations similar in structure and content by the governments of dozens of European countries, which happened later. We would like to note that the development, consideration and adoption of such an official document in Ukraine, aimed at effectively counteracting current and future dangers occurring in cyberspace, should become one of the priorities of the current government.

In addition, the states mentioned above in this article have created official documents similar in content and form, which contain steps to combat cybercrime, but those steps and the emphasis of the relevant agencies on such counteraction differ. For example, according to Estonian authorities, the key condition for the effectiveness of such strategies is their proper legal regulation. That is, without the creation of a high-quality set of legal acts regulating this strategy, together with the strategy itself, there was no significant success, according to Estonians.

The main focus and hope of state officials of the Czech Republic is on the clear and powerful operation of specific systems and devices that protect computer and

19 *Roadmap: Proposal on a European Strategy for Internet Security*. Available at: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

information systems of this country from vulnerabilities and dangers, as well as to help reduce or significantly reduce potential damage by cyberattacks. That is, government agencies and departments in the Czech Republic are focusing their efforts on the so-called "material" aspect of the fight against cybercrime. We can state that while modern technologies play a major role in the fight against cybercrime and offenses, the country must have several other important factors for full success in the fight against cybercrime in addition to its smooth functioning.

It is worth noting that information and educational factors play not the least role in solving this problem. As we can see from the Finnish experience, understanding of the basic, fundamental processes of computer and information mechanisms by the majority of the population helps them to better counteract to cybercrimes that they face even on a personal, private level. The concept of understanding cybersecurity in Finnish society, as well as the importance of ensuring it as a purely economic factor, is also positively noted. Moreover, the threats posed by the potential impact of cyber-attacks on economic damage to public and private individuals are considered by the state as challenges and threats to its own national defense.

The Republic of Lithuania has a unique experience in cybersecurity counteraction, where the main task facing the competent government agencies and institutions of the country is to ensure the simultaneous successful operation of the two phenomena. In particular, it is applied to a holistic system of confidentiality of persons and sources of their information, designed to adequately protect the rights, freedoms and legitimate interests of public relations, together with the system that guarantees the absence of censorship in the state, openness of the information to public and private persons.

Nowadays, we can confidently say that the political leadership and state agencies of the Republic of Lithuania continue to combine these two phenomena quite successfully. An important emphasis in the work of agencies and structures that counteract cyber-threats is also placed on the protection and provision of the proper functioning of information systems, telecommunication networks and critically important points of public and private infrastructure.[20] Such steps towards cybersecurity are quite consistent and appropriate, since the means of telecommunication serve in modern times as the main sources and transport routes for the timely dissemination of information. Thus, by protecting the key points of communication, databases,

20 H. Luiijf, K. Besseling, M. Spoelstra & P. de Graaf. *Ten National Cybersecurity Strategies: A Comparison*. CRITIS 2011 6th International Conference on Critical Information Infrastructures Security, September 2011. Pg. 15.

strategic power plants and similar facilities, the Lithuanian authorities are taking effective steps to minimize the negative consequences of potential cyberattacks.

Having studied the Lithuanian experience on combating cybercrime, we can say that this country, over the past two decades, has made significant progress and has repeatedly demonstrated its own success in combating it. Therefore, in our opinion, the successful experience of Lithuanian state authorities (institutions and agencies) should be adopted into the political and legal system of Ukraine as a set of effective methods and means of combating cybercrime. But it is noted that the combination of elements of this strategy should be harmonious, should not contradict the current legislation of Ukraine, and should guarantee the successful functioning of the state and authoritative mechanism of the country.

The peculiarity of normative and legal regulation of the activities of the Dutch state authorities in relation to the protection against cyberattacks is that they, in their anti-cybercrime strategy, among other things, define the concept of cybersecurity as "protection against disruption and misuse of information and telecommunication systems".[21] We mostly tend to agree with Dutch government officials and legislators in their definition of the nature and content of cybersecurity. In fact, the telecommunication and information systems they cite as targets for cyberattacks are indeed the ones that hackers and other cyber-offenders encroach on.

The experience of Great Britain deserves special attention. A characteristic feature of this state's policy in the field of combating the dangers that exist in modern global cyberspace is its focus on the development and acquisition of as many high-quality and useful innovations as possible. For example, the United Kingdom is recognized as the absolute leader among European countries in the field of financing the high-tech sector, in particular its cyber-field. Wide volumes of domestic and foreign investments aimed at ensuring state cybersecurity play a positive role in the functioning of the national cybersecurity system.[22]

Here we can state that the difference between the peculiarities of cyber-activity in both democratic and legal countries and authoritarian regimes is clearly clarified in the world. It has been pointed out that despite the possibility of some non-democratic countries to receive quite significant profits from the sale of natural resources, and then use this money to finance actions that increase the state's defense capabilities, including its cybersphere, their ability to raise funds compared to developed and

21 Mykola Vasilenko, *supra*, note 3. Pg. 17-24.

22 Lisa Schmidthuber, Simone Stütz & Dennis Hilgers. *Outcomes of Open Government: Does an Online Platform Improve Citizens' Perception of Local Government?* INTERNATIONAL JOURNAL OF PUBLIC SECTOR MANAGEMENT 5. 2019. Pg. 438-456.

democratic states is not significant. This statement is based on the fact that authoritarian regimes, in terms of their own effectiveness, are far inferior to democratic ones. Nevertheless, the main reasons for the growth of economies of democratic countries are their ability to find and attract investment from outside or inside the country, and quickly orient them to the development of those areas of life that need it most. They have such a useful opportunity because those countries have a transparent and clear state system, an independent judicial system and a low level of corruption. As a matter of fact, the creditor will be able to provide money only when they understand that the money will be returned to them guaranteed and within a certain period of time.[23]

Given the above, it is possible to make a direct conclusion that the economy, the counteraction to corruption at all levels of public administration and, one of the most important, the national system of implementing independent justice should be developed in the state along with the development of the cybersphere, which includes a set of methods and techniques to protect national information and telecommunication networks, as well as strategic communication points. The above factors undoubtedly play a useful and positive role in increasing the efficiency of cybersecurity processes in the country, since they strengthen the national economy and create additional opportunities to increase the power of cyber-systems.

IV. Conclusions

Thus, summarizing all the theses, statements and scientific views of scholars and specialists in the field of cybersecurity and jurisprudence, as well as forming the final conclusions on their basis, we can state that ensuring an appropriate level of cybersecurity is one of the most important elements of effective and the successful functioning of any modern state. It has been stated that the level of protection of any country from real and potential threats and dangers that currently exist in cyberspace has a direct economic impact on the overall level of well-being and prosperity of the state. It has been added that both government agencies and institutions and private and commercial companies and organizations should be under reliable cyber-protection.

It should be noted that the formation of a reliable system of cybersecurity of the state, which can protect the state itself and all the subjects of its legal relations without exception, requires a successful combination of several elements. For example, there

23 Maria Petrescu & Anjala S. Krishen. *Analyzing the Analytics: Data Privacy Concerns*. JOURNAL OF MARKET ANALITICS 6. 2018. Pg. 42-51. Available at: https://doi.org/10.1057/s41270-018-0034-x

should be a clear and unambiguous strategy (or plan) for achieving the success in providing a reliable cybersecurity system. Such a strategy should include a number of successful solutions that have functioned in similar strategies adopted by the developed countries of Western Europe over the past few years.

We should also create an appropriate regulatory base, the main task of which would be to ensure the effective and continuous functioning of the national cybersecurity system. It has been emphasized that the development of the relevant regulatory acts should be entrusted to prominent domestic jurists of today, with the mandatory involvement of domestic law schools. Besides, the government needs to ensure an adequate level of ongoing external and internal funding for the cyber-sector by attracting investment.

V. References

Akhilesh Chandra & Melissa J. Snowe. *A Taxonomy of Cybercrime: Theory and Design*. International Journal of Accounting Information Systems 38. 2020. Available at: https://doi/org10.1016/j.accinf.2020.100467

Chris Reed. Rethinking the Jurisprudence of Cyberspace. Edward Elgar Publishing. (2018).

David Siman-Tov & Noam Alon. *The Cybersphere Obligates and Facilitates a Revolution in Intelligence Affairs*. Cyber, Intelligence, and Security 1. May 2018. Pg. 73-92. Available at: https://www.inss.org.il/wp-content/uploads/2018/05/Cyber-Intelligence-and-Security-Volume-2-No.-1-May-2018.pdf

D. Dubova (Ed.). State and Private Partnership in the Field of Cybersecurity: International Experience and Opportunities for Ukraine: Analytical Report. NISD. (2018). Pp. 12-81.

Ihor V. Diorditsa, Armenui A. Telestakova, Olga M. Koval, Olha A. Nazarenko & Andrii A. Nastiuk. *Information Interventions as a New Dimension of Ukraine's Cyber-Vulnerability*. Revista Genero & Direito 1. 2020. Special Edition. Available at: https://www.periodicojs.com.br/index.php/gei/article/view/21

H. Luiijf, K. Besseling, M. Spoelstra & P. de Graaf. *Ten National Cybersecurity Strategies: A Comparison*. CRITIS 2011 6th International Conference on Critical Information Infrastructures Security, September 2011.

Lisa Schmidthuber, Simone Stütz & Dennis Hilgers. *Outcomes of Open Government: Does an Online Platform Improve Citizens' Perception of Local Government?* International Journal of Public Sector Management 5. 2019. Pg. 438-456.

Maria Petrescu & Anjala S. Krishen. *Analyzing the Analytics: Data Privacy Concerns*. Journal of Market Analitics 6. 2018. Pg. 42-51. Available at: https://doi.org/10.1057/s41270-018-0034-x

Mykola Vasilenko. *Quality of Cybersecurity of Information and Communicational Systems (ICS) and Some Legislative Issues on Its Improvement*. Law Herald 4. 2018.

Mykola Vasilenko. *Strengthening the State of Cybersecurity of Information and Communicational Systems: Quality in the Context of Improving Information Legislation*. Law Herald 3. 2018. Pp. 17-24.

Oles Andriychuk. *Book Review: Rethinking the Jurisprudence of Cyberspace*. European Journal of Law and Technology 1. 2020. Available at: http://ejlt.org/index.php/ejlt/article/view/744

Oleksandr D. Dovhan & Ivan M. Doronin. Escalation of Cyber Threats to National Interests of Ukraine and Legal Aspects of Cybersecurity: Monograph. NALS of Ukraine, NDIIP. ArtEk Publishing House. (2017).

Olga F. Guchinskaia & Irina I. Tolstikova. *Communications in Cyberspace: Designs Features*. First International Conference, DTGS 2016 St. Petersburg, Russia, June 22-24, 2016 Revised Selected Papers.

Viktor Boiko, Mykola Vasilenko & Serhii Kukharenko. *Cybersecurity in EU and Member States: Genesis and Problems of Its Strengthening*. Available at: http://www.academy.ssu.gov.ua/ua/page/page_1581426437.htm

Viktor V. Pushkarev, Valeriia V. Artemova, Sergey V. Ermakov, Elmir N. Alimamedov & Anton V. Popenkov. *Criminal Prosecution of Persons, who Committed Criminal Acts Using the Cryptocurrency in the Russian Federation*. Revista San Gregorio 42. 2020. Pg. 330-335. Available at: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1566

Zinaida Zhyvko, Taras Rudyi, Volodymyr Senyk & Liliia Kucharska. *Legal Basis of Ensuring Cyber Security of Ukraine: Problems and Ways of Eliminating*. Economics, Finance and Management Review 2. 2020. Pg. 82-90. Available at: https://doi.org/10.36690/2674-5208-2020-2-82