The System for Ensuring the Information Security of the Organization in the Context of COVID-19 Based on Public-Private Partnership

Halyna Dzyana [†], **Vasyl Pasichnyk** [††]**, Yevgen Garmash** [†††]**, Mykhaylo Naumko** [††††]**, Oleg Didych** [†††††]

sych.yul@gmail.com   nationaluniversity_11@yahoo.com   dahluniversity_halyna@yahoo.com
laskav_np@yahoo.com   lenok_leno@ukr.net

[†] *Lviv Polytechnic National University, Ukraine*
[††] Lviv Polytechnic National University, Ukraine
[†††] Vice-rector for Academic Affairs University of Customs and Finance, Dnipro, Ukraine
[††††] National Academy of Land Forces named after Hetman Petro Sagaidachny, Lviv, Ukraine
[†††††] Lviv Polytechnic National University, Ukraine

Abstract

The main purpose of the study is to analyze the current state of the organization's information security system in the context of COVID-19 on the basis of public-private partnership. The development of public-private interaction in information security is one of the priorities of the state policy of many estates. Among the priorities of public-private partnership in cybersecurity and information security, there is an expansion of interaction between government agencies and private scientific institutions, public associations and volunteer organizations, including in training, as well as increasing the digital literacy of citizens and the security culture in cyberspace. As a result of the study, the foundations of the organization's information security system in the context of COVID 19 were formed on the basis of public-private partnership.

Keywords:
public-private partnership, information security, cybersecurity, digital literacy.

1. Introduction

Recently, the direction of development of the world community is aimed at technological progress and the introduction of information technologies, which greatly facilitate the processes of searching and exchanging information, this process has become especially relevant during the times of COVID-19. The widespread use of computer and telecommunication technologies in all areas of public life, especially Internet technologies, has many advantages along with an increase in the volume of threats. The implementation of which causes damage at the state level and in the international arena. Which leads to the need to solve these problems in order to minimize, eliminate and prevent cyber threats and ensure information security in the context of COVID-19. Today, cybercrime, for which there are no state borders, threatens not only society, but also infringes on national interests. There is a high activity of cyber attacks, the activities of criminal groups, industrial and financial groups and persons working in the system in the performance of official activities (insiders). Cyber threat incidents are becoming more frequent, better organized, easier and cheaper to prepare and implement. Therefore, it is necessary to look for new ways to counteract, to improve the country's cybersecurity mechanisms, including by introducing the concept of public-private partnership.
country.

In modern conditions, when ultra-modern information technologies are being introduced into almost all spheres of life, telecommunication systems are rapidly developing, new global networks based on the use of interactive information dissemination tools are emerging, it becomes possible to satisfy one's own interests, obtain (almost instantly) the necessary information. Now everyone can find out the latest events in any corner of the world. At the same time, there is another side of progress: the authorities, citizens of any state, without the use of military tools, but only thanks to the Internet, social networks, information transmission channels, are able to weaken or even destroy a competing state, for example, disable the banking system or any a website, for example, the provision of public services, interfere with the work of the email of a single department (as was the case with the FBI mail), etc. Unfortunately, quite often we hear about hacker attacks, from which no one, as it turned out, is not

protected. Eloquent and indicative in this context, in our opinion, are the data provided in the Microsoft report on hacker attacks during 2020-2021, made on the basis of information collected by its security systems. Thus, according to Microsoft, Russia is involved in 58% of attacks. "The majority of hacker attacks were directed against the United States - 46%. Ukraine ranks second in this ranking (19%), the third is the UK with a significant margin (9%). Also, part of the attacks fell on Belgium, Japan, Germany (3%) and other countries.

The above is of particular relevance in view of the fact that, and we have cited statistics, now most states are faced with the fact that their system of ensuring information security and protecting information sovereignty turned out to be vulnerable, and this negatively affects the ability of the state to effectively protect its national interests in the information sphere. Thus, according to experts, one of the most dangerous external factors can be safely recognized as the process of globalization, accompanied by the undermining of traditional and other values imposed on countries and peoples, in particular, through new information and telecommunication systems and technologies. The volume of the world information industry in the early 90s of the last century reached 2 trillion. US dollars, and at the beginning of the 21st century increased by an order of magnitude.

There is a growing awareness of the need to adhere to certain global principles of behavior, since the alternative may be the uncontrolled growth of global risks from which no one can hide. Hence, we are witnessing an unprecedented rate of spread of new international and even global agreements to regulate certain components of human activity." In the context of the above, special attention should be paid to the fact that in the context of the globalization of information processes, the formation of the world information space, and the rapid growth of the world information market, no state, of course, can function in information isolation. This is what is alarming, because in this case, information sources and flows on the territory of any country are almost completely protected from interference, attacks, external information influence and leakage of internal information.

The term "cybersecurity" usually refers to corporate governance, management and focuses on specific forms of complex attacks and covers their technical and social aspects. Let's look at some definitions of this concept. The EU formally recognizes that cybersecurity generally refers to measures and activities aimed at protecting cyberspace in the civil and military spheres from threats that can damage or are associated with interconnected networks and information infrastructure. Cybersecurity aims to maintain the availability and integrity of networks and infrastructure, as well as the confidentiality of the information they contain.

According to most regulations in different countries of the world, the role of the state in the information security system in the context of COVID-19 consists of the following elements:
- formation of the sphere of information protection and ensures its implementation within its competence;
- determination of the requirements and the procedure for creating an integrated protection system;
- exercise control over ensuring the protection of state information resources or information with limited access, the protection requirement of which is established by law;
- takes measures to identify a threat to state information resources from unauthorized actions in information, telecommunications and information and telecommunication systems and makes recommendations to prevent such a threat.

Special subjects for ensuring information security in the public-private partnership system are state bodies that, in addition to general functions, are authorized to combat cybercrime and cyberterrorism, as well as to ensure cybernetic protection of national and private infrastructure.

2. Methodology

To achieve the goals set in the study, we applied the following methods: induction and deduction, comparison and systematization; synthesis and analysis; abstract-logical - for theoretical generalizations and conclusions of the study.

3. Research Results and Discussions

The increasing influence of destabilizing factors of the external and internal environment on the information security of enterprises, characterized by an aggravation of contradictions in the economic

sphere, reducing the efficiency of their activities, manifests itself in the theft of property, corruption, fraud, cybercrime, inaccurate financial reporting data, a decrease in investment attractiveness and the development of an appropriate enterprise protection system

In the context of the need for constant monitoring of the activities of enterprises, one of the determining directions for increasing the efficiency, sustainability and ability to manage an enterprise is to improve the system of economic security through its financial component through the formation of information and analytical support, the development of procedures for verifying and confirming information.

The introduction of quarantine caused by the COVID-19 pandemic has forced most enterprises to transfer employees to remote work. However, the massive use of digital technologies is fraught with hidden threats associated with cybercrime. In this article, we will consider the impact of information technologies and resources on the economic security of enterprises in a pandemic and methods to counter them.

The subjects of the cyber security system are in close interaction with each other, but at the same time, each of them specializes in solving specific problems in accordance with their subject competence and within the limits of authority determined by law. Despite this, information security threats are actualized through the action of such factors as an insufficient level of coordination, interaction and information exchange between the subjects of cybersecurity.

Ensuring informational nature as a state of protection of the vital interests of a person and a citizen, society and the state in cyberspace, which is achieved by the complex application of a set of legal, organizational, informational measures, should be based on the basic principles (Table 1).

Table 1: Basic principles of implementation of information security system in the context of COVID-19 based on public-private partnership

№	Basic principles
1	the rule of law and respect for the rights and freedoms of man and citizen, openness, accessibility, stability and security of cyberspace
2	public-private partnership, broad cooperation with civil society in the field of cybersecurity and cyber defense, proportionality and adequacy of cyber defense measures to real and potential risks; prioritization of measures
3	inevitability of punishment for committing cybercrimes; priority development and support of domestic scientific, scientific, technical and industrial potential
4	international cooperation in order to strengthen mutual trust in the field of cybersecurity and develop joint approaches to countering cyber threats, consolidating efforts in investigating and preventing cybercrimes, and preventing the use of cyberspace for illegal and military purposes

The implementation of cybersecurity through the use of public-private partnerships involves the involvement as a private partner of business entities using elements of critical infrastructure that depend on ICT; server equipment manufacturers, software developers, payment settlement operators. It is necessary to develop relations related to the disclosure of confidential, commercial and personal information, to achieve a balance of interests of partners, to develop control and supervisory procedures.

The term public-private partnership reflects the leading role of the state in the implementation of public-private partnership projects. The term "public-private partnership" can be considered in a broad and narrow sense. In a broad sense, public-private

partnership is a system of relations between the state and business, which is widely used as a tool for national, international, regional, urban, municipal, economic and social development. In a narrow sense, public-private partnerships are specific projects implemented together by state bodies and private companies at state and municipal property.

Today, public-private partnerships are recognized by both states and non-state actors as a key element in building a truly effective state cybersecurity system. Almost every cybersecurity strategy (national or supranational) or departmental vision document (which deals with information security) mentions the desire to develop public-private partnerships.

Along with the variety of forms of implementation in international practice, the main stages of public-private partnership are determined: assessment of opportunities for the provision of services within the framework of public-private partnership; preparation for the provision of a service or the implementation of a project within the framework of a public-private partnership; choice of partner; negotiation process and conclusion of the contract; execution and monitoring of the contract. Table 2 depicts the main objectives of the public-private partnership in the context of ensuring the system of the information security of the organization in the context of COVID-19

Table 1: Basic principles of implementation of information security system in the context of COVID-19 based on public-private partnership

№	The main tasks
1	regulate technical security and data processing;
2	provide reliable access to the Internet;
3	exchange information regarding threats and vulnerabilities;

4	to provide assistance in resolving situations related to threats or illegal content on the Internet.

The principles of public-private partnership in the field of information security are based on economic efficiency and innovation; ensuring integrity and availability; privacy and freedom; responsibility and transparency; justice.

The modern attitude of the countries of the world to the problem of cyber security has come a long way

- from understanding to a comprehensive vision of protection systems. It was largely influenced by several factors that determined the principles, priorities and modern horizons. The main ones are:

- novelty, complexity and number of challenges and threats that arose at the initial stage in the formation of the foundations of information security;

— positive perception of guidelines regarding the current and future development of the legal support of cyber security, outlined by a number of universal and regional international organizations;

focusing on legal issues related to cyber and information security, mainly on the positions of protecting universally recognized human rights;

- the gradual spread of various crimes related to the use of new digital technologies and the need to prevent crime and create criminal justice in the fight against high-tech and computer crime;

- the presence of predominantly soft law ("soft law") rules on cyber and information security, which were contained in resolutions of international bodies and organizations, in general statements, declarations, and communiqués.

The development of public-private partnerships in the field of cybersecurity is one of the main and effective tools for creating cybersecurity/cyberdefence systems. This tool is used in international practice. The modern DPP model is formed by the US Department of Homeland Security (DHS). For quick and timely exchange of threat information indicators between the public and private sectors, the Department has created an automated cyber threat program [1-15].

In order to implement the task of protecting critical infrastructure (National Strategy for the Protection of Critical Infrastructure, CIP) at the strategic and operational level, the German Federal Government has developed the KRITIS Public-Private Partnership Plan (Umsetzungsplan KRITIS). Since 2007, the public-private cooperation "UP CRITIS" has been implemented by the government in cooperation with critical infrastructure operators. The main goal of the CRITIS Plan is to improve the protection of critical infrastructure in various security sectors.

The experience of foreign countries in real life shows that the solution of the main tasks of cybersecurity is impossible without creating:

1) an interdepartmental structural body that would ensure, on an ongoing basis, the coordination of the activities of certain departments, law enforcement and law enforcement agencies on issues of ensuring cyber security;

2) central authorities in the structure of certain departments, law enforcement and law enforcement agencies with the functions of identifying and assessing the level (determining the degree) of criticality of extraneous cyber influence, developing conceptual foundations and providing recommendations on countering its manifestations, as well as actively counteracting cyber attacks of warring parties and influencing their ITS ;

3) bodies of their own information and cyber security - state institutions (departments) and commercial structures that should closely cooperate with the indicated central authorities on the development of a unified policy to protect both their own and the general national information cyberspace.

We believe that the following measures are necessary to ensure the further implementation of public-private partnership mechanisms in the field of information security:

- carrying out reforms in the country that will turn it into a modern competitive state and lead it out of the crisis;

- fight against corruption at all levels of state power and local self-government;

- elimination of shortcomings in the legal regulation of public-private partnership and cybersecurity;

- information and analytical support for cybersecurity subjects and increasing the effectiveness of monitoring in this area;

- ensuring close cooperation between the state, the private sector and society for strategic planning of cybersecurity;

- preparation of recommendations for the implementation of public-private partnership projects for all subjects of cybersecurity;

- strengthening the predictive function of the cyber security management system;

- training of qualified public administration specialists for the practical implementation of public-private partnership projects.

4. Conclusions

From the study, we can conclude that today the system of state-legal partnership in the world pays sufficient attention to improving cybersecurity processes and ensuring the functioning of the information security system, but security regulation remains ineffective. Therefore, the involvement of business and citizens in solving these issues, using the model of public-private partnership, becomes especially relevant. Business as a private participant has technical, financial, intellectual, human capital that can help the state in solving certain market problems. The public-private partnership solves the following tasks in the field of improving cybersecurity: safety and data protection, reliable access to the Internet, the exchange of data on threats and attacks, assistance in solving emerging problems in the Internet space. The cybersecurity policy is based on the following principles: innovation and efficiency, integrity and accessibility, freedom and fairness, responsibility and transparency. Today, the development of a mechanism for interaction between business and the state is completely dependent on the domestic legal framework on cybersecurity issues and the introduction of innovative approaches. Subsequent research, in our opinion, should be aimed at scientific substantiation of innovative forms of introducing the mechanism of public-private partnership in the field of information security in the context of COVID-19.

References

[1] Kryshtanovych, M., Oliinyk, N., Skliaruk, T., Voityk, O., & Doronina, I. Problems of shaping the business environment in countries with economies in transition: aspects of anti-corruption. *Management Theory and Studies for Rural Business and Infrastructure Development*, 43(2), 2021, 316–327. Retrieved from

https://ejournals.vdu.lt/index.php/mtsrbid/article/view/2332

[2] Soja, E. Information and communication technology in active and healthy ageing: Exploring risks from multi-generation perspective. Information Systems Management, 2017, 34(4), 320–332. https://doi.org/10.1080/10580530.2017.1366217

[3] Calof, J. Government sponsored competitive intelligence for regional and sectoral economic development: Canadian experiences. Journal of Intelligence Studies in Business, 2016, 6(1), 48– 58.

[4] Savytska, N., Chmil, H., Hrabylnikova, O., Pushkina, O., & Vakulich, M. Behavioral models for ensuring the security of functioning and organizational sustainability of the enterprise. Journal of Security and Sustainability, 2019, 9(1), 63-76. https://doi.org/10.9770/jssi.2019.9.1(6)

[5] Pylypenko, K. A., Babiy, I. V., Volkova, N. V., Feofanov, L. K., & Kashchena, N. B. Structuring economic security of the organization. Journal of Security and Sustainability, 2019, 9(1), 7-38. https://doi.org/10.9770/jssi.2019.9.1(3)

[6] Huang, X. & Xu, W. Method of Information Security Risk Assessment Based on Improved Fuzzy Theory of Evidence. International Journal of Online Engineering (iJOE). 2018, 14. 188. https://doi.org/10.3991/ijoe.v14i03.8422

[7] Kryshtanovych, M., Ortynskyi, V., Krasivskyy O., Maziy, N., & Pasichnyk, V. Methodical approach to countering threats of economic security in the context of ensuring the protection of national interests. Financial and Credit Activity: Problems of Theory and Practice, 4(39), 2021, 202–208. https://doi.org/10.18371/.v4i39.241309

[8] Fedotova, G. & Kovalenko, O. & Malyutina, T. & Glushchenko, A. & Sukhinin, A. (2019). Transformation of Information Security Systems of Enterprises in the Context of Digitization of the National Economy.2019. https://doi.org/10.1007/978-3-030-13397-9_84

[9] Okereafor, K. Cybersecurity in the COVID-19 Pandemic, 2021, https://doi.org/10.1201/9781003104124

[10] Merry, Mannebäck, E.; Padyab, A. Challenges of Managing Information Security during the Pandemic. Challenges 2021, 12, 30. https://doi.org/10.3390/challe12020030

[11] Kochnev He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review, J Med Internet Res, 2021, 23(4), e21747 https://doi.org/10.2196/21747

[12] Ying He & Chris Johnson (2017) Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization, Informatics for Health and Social Care, 42:4, 2016, 393-408, https://doi.org/10.1080/17538157.2016.1255629

[13] Schwab, K. (2020), "The Fourth Industrial Revolution: what it means, how to respond", World Economic Forum.

[14] Kryshtanovych, S., Gutsulyak, V., Huzii, I., Helzhynska, T., & Shepitchak, V. Modeling the process of risk management response to the negative impact of risks as the basis for ensuring economic security. Business, Management and Economics Engineering, 19(2), 2021, 289-302. https://doi.org/10.3846/bmee.2021.14798

[15] Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams–challenges in supporting the organisational security function. Computers & Security 2012;31(5):643–52. https://doi.org/10.1016/j.cose.2012.04.001