DOI: 10.55643/fcaptp.3.50.2023.4075

MODELING THE CYBERSECURITY OF THE SOCIO-ECONOMIC SYSTEM UNDER MARTIAL LAW

Mykola Izha
Doctor of Political Science, Professor, Director of the Educational and Scientific Institute of Public Service and Management, Odesa National Polytechnic University, Odesa, Ukraine;
ORCID: 0000-0002-7263-6193

Tetyana Pachomova
D.Sc. in Public Administration, Professor, Head of the Department of Local Self-Government and Development of Territories of the Educational and Scientific Institute of Public Service and Management, Odesa National Polytechnic University, Odesa, Ukraine;
e-mail: standigt32@gmail.com
ORCID: 0000-0001-9940-1418
(Corresponding author)

Olena Lypach
PhD Student of the Department of Local Self-Government and Development of Territories of the Educational and Scientific Institute of Public Service and Management, Odesa National Polytechnic University, Odesa, Ukraine;
ORCID: 0009-0009-2934-0408

Oleksiy Yakubovskyi
Candidate of Historical Sciences, Professor of the Department of Local Self-Government and Development of Territories of the Educational and Scientific Institute of Public Service and Management, Odesa National Polytechnic University, Odesa, Ukraine;
ORCID: 0009-0004-6745-8550

Anatolii Akhlamov
D.Sc. in Economics, Professor of the Department of Local Self-Government and Territories Development Institute of Public Service and Administration, Odesa National Polytechnic University, Odesa, Ukraine;
ORCID: 0000-0002-9356-2103

Received: 03/04/2023
Accepted: 13/06/2023
Published: 30/06/2023

ABSTRACT

Industry 5.0 is already gradually beginning to manifest itself in various aspects of our lives. It is especially sensitive for ensuring socio-economic development. At the same time, cyber threats are increasing, which have a negative impact on ensuring economic security. That is why there is an urgent need to protect information in wartime conditions. The main goal of the article is to determine ways to ensure the cyber security of the socio-economic system under martial law. The object of the study is the cyber security system. As a result of the study, the author's model was presented for enabling the provision of cyber security in wartime conditions. For this, a modern method of modelling structural systems was applied. The practical and scientific significance of the obtained research results can be presented in the form of an information model for ensuring the cyber security of the socio-economic system under martial law. Innovative elements of the obtained results are the presented processes of cybersecurity, which allows to detail the key ideas of modelling. The research has limitations in the form of taking into account only the features of ensuring cyber security of the socio-economic system in the conditions of the military state of one country.

Keywords: martial law, security, cybersecurity, information, model, security, system, socio-economic system

JEL Classification: K24, F52, K22, H56

INTRODUCTION

One of the main consequences of informatization, which arose during the formation of the modern information age, was the emergence and rapid development of a new sphere of confrontation between states - confrontation in cyberspace. If today between the most militarily and economically developed states a strategic parity has developed to some extent in weapons of mass destruction and conventional weapons, then the question of parity in cyberspace remains open. And, as a result, for any state, security in cyberspace (cybersecurity) has become the most acute problem in ensuring national security.

Digitalization has become an objective reality in all areas of human activity. In today's digitalized world, attacks on digital infrastructure are an integral part of the war, as they have a destructive socio-economic impact, make it impossible to conduct an effective confrontation and contribute to the depletion of resources. At the same time, the generation of threats in the digital sphere, as a rule, requires relatively insignificant costs and is accompanied by minimal risks for the attacker, with a potentially significant amount of damage caused. Therefore, the prediction of risks and real threats to economic security in the digital sphere, preparation for them and timely response are updated with an increase in the level of global tension, and escalation of existing conflicts and within existing ones, including the russian invasion of Ukraine.

The continuous socio-technical development of the world economy, associated with a new technological transition to the information age and the dominance of the service market in developed countries, has made the digitalization process an integral part of globalization. The digital infrastructure has united the world even more, has given network access from one country to another, and has made the Internet global. Along with

DOI: 10.55643/fcaptp.3.50.2023.4075

the benefits, cybercrime and cyberterrorism developed. All these crimes are committed by the anonymity of Internet agents, including to increase the negative impact of transnational companies, destructive communities and the implementation of hostile actions at the geopolitical level, which constantly generates new risks and threats to the digital economy.

The task of cyber warfare is to achieve a specific goal in the economic, political, military and other sectors. At the same time, an additional task is set to carry out a targeted influence on society and power with pre-prepared information. Therefore, cyber warfare is also psychological and one of the types of information warfare in cyberspace. After all, computer technology and the Internet are used all over the world not only in the daily lives of people but also in enterprises and government agencies. Manipulation of data received from the above institutions creates a threat to the national security of the state. Therefore, cybersecurity is an integral part of protecting national security in this confrontation.

The development of international cooperation in the direction of strengthening the cyber resilience of Ukraine is a priority task in order to prevent global information threats, ensure a high level of quality in the investigation of cybercrimes, arrest and prosecute malicious agents, and overcome cybersecurity problems. At the same time, there are areas in the field of cybersecurity that negatively affect Ukraine's position in these ratings and need to be improved. In particular, the low level of contribution to global cybersecurity to date, the insufficient level of protection of digital services, and the underdeveloped direction of military cyber operations. It should be noted that since the beginning of 2022, active work has been carried out on all the noted problematic aspects: Ukraine has become an active participant in international cooperation in the field of cybersecurity; there is a process of forming a cyber-troop [14] responsible for information security, protection of critical infrastructure and intelligence.

LITERATURE REVIEW

It is not uncommon to find in the leading literature the thesis that society is transforming into a cyber society. As noted by Hadlington, (2017) [1], Mouheb, Abbas, Merabti, (2019) [2], Fakiha, (2021), Shtangret, et. al., (2021) [4], the Internet is becoming a part of everyday life, penetrating into all spheres of the economy, education, culture, science, public and private life. This is not only technology but also a way of organizing relationships between people. Communication built on the personal participation of everyone in the creation, storage and distribution of content allows you to better realize your personal potential from all points of view. On the one hand, these are new prospects for entrepreneurship and the development of civil society, and on the other hand, they are a temptation for potential criminals, terrorists and politicians who think in terms of wars and conflicts. Cyberspace provides the best opportunities for personal development, business projects and social progress. But under these conditions, competition among market participants and in the international arena is also intensifying.

As noted by Kryshtanoyvch et.al., (2023) [5], and Weru, et.al., (2017) [6] today there is a transition of the information society to its highest socio-economic phase - the so-called knowledge-oriented society, in which more than half of the world's gross product is produced with the help of intelligent information technologies. At the same time, the latest scientific and technological achievements in the information industry are becoming available to a criminal group, as evidenced by the rapid increase in cyber threats aimed at unauthorized access to information resources of government agencies, businesses and individuals. Information security is becoming an important component of the functional efficiency of the information and telecommunication system. At the same time, one should be aware that since organized cybercriminals are proficient in modern hardware and software of information and communication technologies, the main ways to neutralize their criminal activities are the development and use of new promising intelligent information analysis technologies in integrated information security systems data (Kryshtanoyvch, et.al., (2021) [7]; Sylkin, et. al., (2021) [8]).

Also, in the literature it is noted by Sylkin, et. al. (2021) [9]; Musman, Turner, (2018) [10]; Martinez, Duran, (2021) [11]; Gorbieiev, et.al. (2021) [12] that the development of information and communication technologies, determined by the growth of traffic and the need of consumers for the emergence of new services, leads to the need for constant growth and modernization of telecommunication systems and networks. In recent years, video information services such as video telephony, video conferencing, broadcasting of television programs, and video on demand have become the most in demand. A feature of video traffic is large amounts of transmitted data, sensitivity to delay time and packet loss during transmission over a communication channel. Taking into account these requirements, it is necessary to pay special attention to the quality of the services provided, which is ensured in telecommunication networks using the QoS service. However, it is used only from the standpoint of adjusting the parameters of the transport network to a given category of quality of the transmitted traffic, which can lead to errors or data transmission losses. Therefore, in order to improve the quality of the video information service, it is necessary to additionally control the conditions for matching the source bit rate with respect to the communication channel bandwidth. The most promising methods for reducing the intensity are special

mechanisms for controlling the parameters of video frame processing, which make it possible to flexibly adjust the source bit rate to the current parameters of the telecommunications network.

The simultaneous influence of these two factors creates the phenomenon of digital globalization (Chowdhur, et.al., (2022) [13]; Carlin (2016) [14]; Rodrihues, et.al., (2022) [15]). But, in addition to economic and scientific development, accelerating financial transactions and stimulating human development, it contributes to the creation of new methods and technologies for the destruction of real and digital infrastructure, technological espionage, interference in elections, the spread of destructive ideas and real "Fake news" threats to the economic security of the states in the digital sphere. Thus, digital globalization has transferred wars and conflicts to a new plane, has become a source of new tools to influence the economy and the political environment in a war, and risks and threats in the information space significantly undermine the defence capability of countries. Cyberterrorism, including interstate terrorism, is one of the most dangerous risks to the economic security of the state since it is an effective modern tool for waging wars and defending geopolitical interests (Shakhatreh, (2023) [16]; Al Azzam, (2019) [17]; Saleh, et. al., (2020) [18]; Kryshtanovych, et.al., (2021) [19]; Sylkin, et. al., (2020) [20]).

AIMS AND OBJECTIVES

The main purpose of the article is to determine ways to ensure the cybersecurity of the socio-economic system under martial law. The object of the study is the cybersecurity system. At the same time, the scientific task is to form a model for ensuring the cybersecurity of the socio-economic system under martial law.

METHODS

The essence of data flow modelling in the design of complex socio-economic systems in the framework of cybersecurity is the creation of so-called data flow diagrams. Below we will use the generally recognized abbreviation DFD, which comes from the English term Data Flow Diagram. These schemes reflect the ways in which information flows and transforms within the framework of cybersecurity.

DFD for cybersecurity is a simple but robust graphical tool that is quite adaptable to the needs of system designers and users. DFD depicts cybersecurity in terms of data movement in the system. At the same time, it is possible, within the framework of ensuring cybersecurity, to refine the display by revealing the features of the system at several levels of the hierarchy. A set of diagrams is accompanied by more detailed information, which is completed through special documentation. A hierarchical set of diagrams together with a set of documents is called a data flow model.

The model is based on processes presented in the form of blocks (Figure 1).

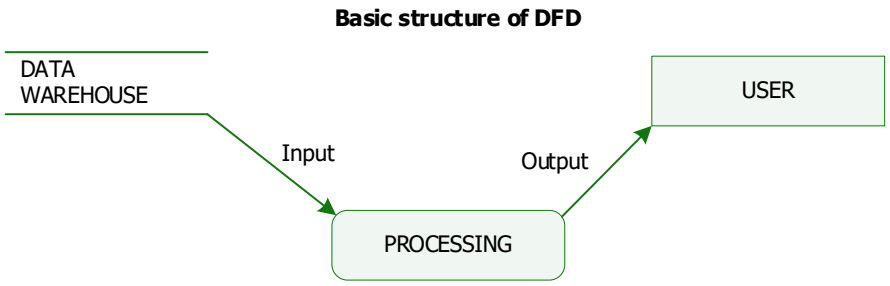

Figure 1. The essence of the block modelling system.

The data flow modelling methodology outlined below provides a fairly simple way to model the functional components of cybersecurity both at the stage of survey and analysis of system requirements and at the initial stages of developing new design solutions.

DOI: 10.55643/fcaptp.3.50.2023.4075

RESULTS

understanding of the basic and basic postulates of safe use of the network will increase the stability of the cybersecurity system of Ukraine. The main mistakes of users are the provision of personal data to a third party since they are often used to send viral advertising, and the main danger is that data about a person is used for illegal and dubious operations, namely, opening secret enterprises, money laundering, taking loans and other crimes.

Further development of the system for protecting cyberspace from cyber attacks depends on the level of interaction between the interested parties: the state, citizens, scientific and technical systems, and private households and consists in the development of the latest information and communication technologies, legislative and regulatory framework, and a system for educating the population in the safe use of cyberspace. This issue is relevant because a new concept comes into play - "cyber warfare", in its own way showing the use of the Internet, technical and information means by any aggressor country, the purpose of which is to cause harm to the economic, political, technical, military and information security and sovereignty of our state.

In 2022, the damage from cyber-attacks increased to USD 4.2-6 trillion (Figure 2). It is predicted that in 2025 the volume of financial losses from cybercrime will be USD 10.5 trillion.

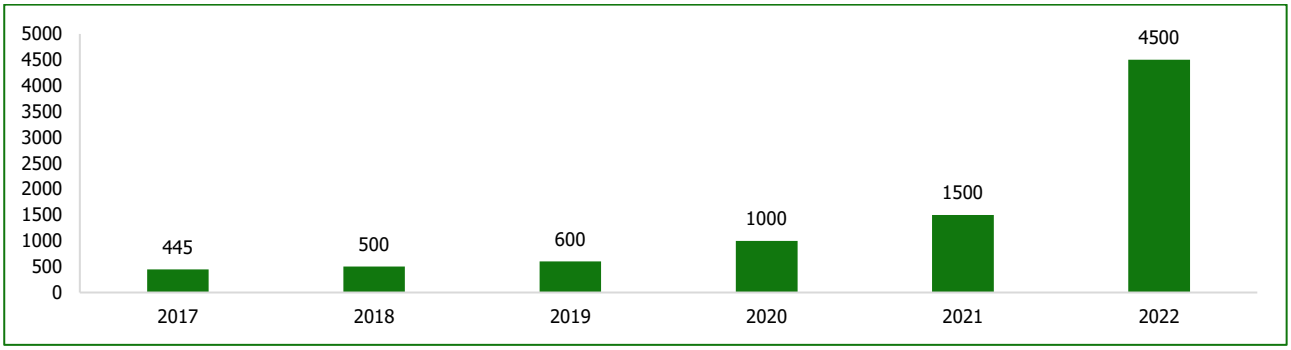

Figure 2. Global financial losses from cyber attacks in 2017–2022, USD billion.

The digitalization of the economy creates many advantages: it accelerates the turnover of financial assets, lowers thresholds and barriers to entering a business, reduces the level of all types of costs through automation and access to the global labour market, creates new jobs, etc. The prerequisites for the emergence of these benefits of digitalization can be determined by the high profitability of IT, with low costs and small investments in tangible assets, which can be interrupted in the event of external shocks. What is important is flexibility and the ability to work for the domestic market, covering the demand of the national economy for software, and infrastructure, and selling the surplus outside, without significant costs for the delivery of services or goods, which is a source of foreign exchange earnings and has a positive impact on the purchasing margin. In general, the digitalization of the economy speeds up financial transactions, asset turnover, frees up funds and resources, promotes the direction of investments in high-risk and high-return start-up projects that help curb the decline of the national economy and maintain a sufficient level of economic security of the state in a war.

It should be noted that during the year of the war, the largest cyber attacks in Ukraine were in the transport and energy sectors. This also applies to the central authorities and the economy (Figure 3).

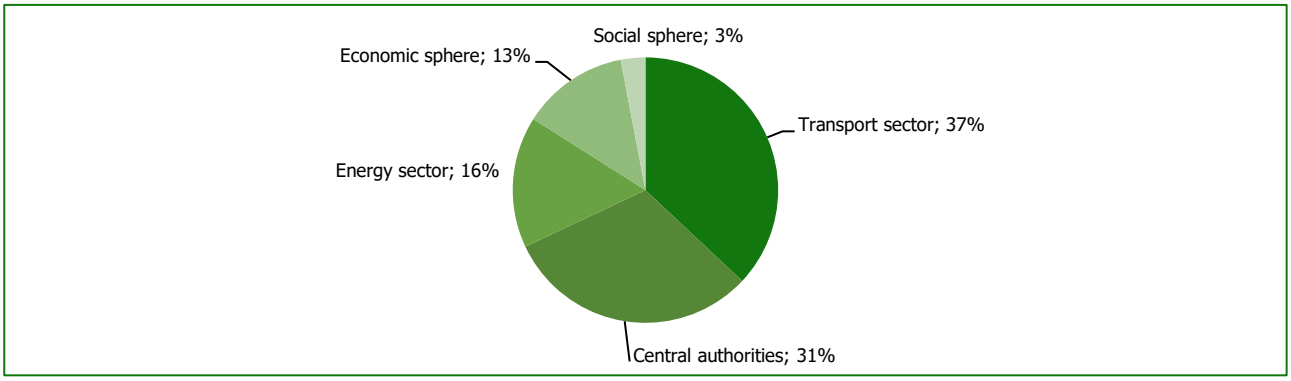

Figure 3. Spheres of cyberattacks during the full-scale war in Ukraine.

Thanks to globalization and the majority of programs available, the blocks do not require implementation at high financial costs. Everything can happen within the existing budget of the Ministry of Digital Policy. The proposed modelling method is designed to integrate new processes into the digital space. At the beginning of the modelling, we will present the main blocks for achieving the goal of the model: information support for cybersecurity under martial law (Figure 4).

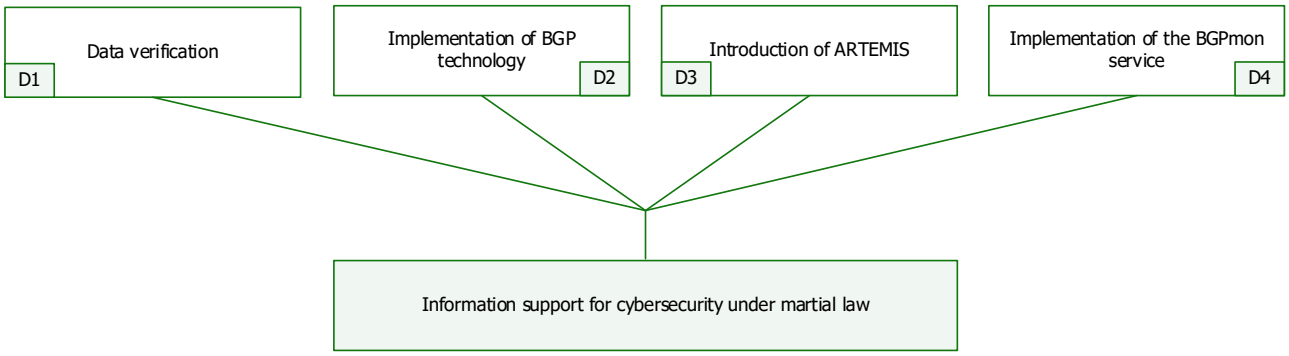

Figure 4. The main blocks for achieving the goal of the model.

Next, with the definition of key blocks, the model itself should be presented. The simulation process is unique and requires appropriate software. Skipping intermediate calculations, we note that through vector programs, each block goes through several stages of the so-called "detailing" in which all the necessary context elements are selected. Further, it combines into one integral system model. As a final result, we will present the basic model of ensuring cybersecurity within the framework of martial law (Figure 5).

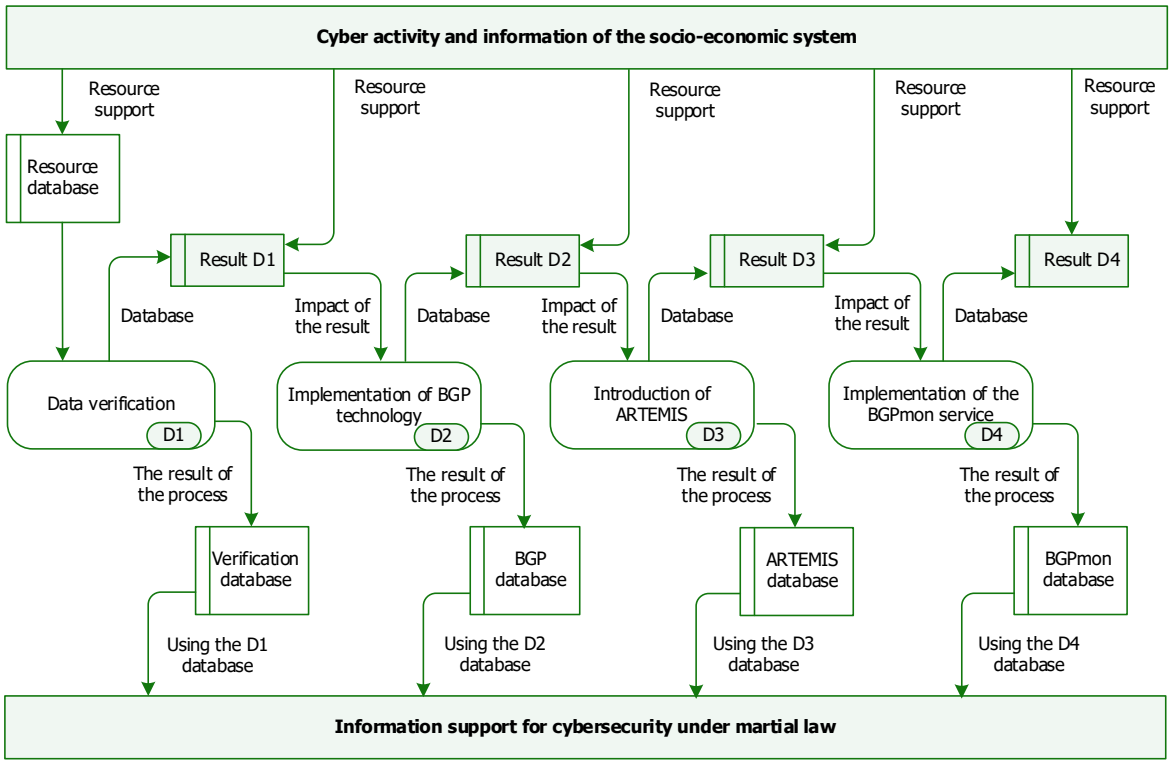

Figure 5. The basic model of ensuring cybersecurity within the framework of martial law.

The key blocks of this model are: D1 (Data verification), D2 (Implementation of BGP technology), D3 (Introduction of ARTEMIS) and D4 (Implementation of the BGPmon service).

D1. Data verification. For IP, which provides network layer connectivity to the Internet, it is important that each connected device must have a unique address, so it is important that the allocation of IP addresses is carefully recorded to avoid conflicts. The purpose of the Internet Routing Registry (IRR) is to ensure that network operators share up-to-date routing information and thus contribute to the stability and integrity of Internet routing as a whole. The IRR consists of several

DOI: 10.55643/fcaptp.3.50.2023.4075

databases where operators publish their own routing policies and announcements so that other operators can build their input and output filters based on the IRR data. With the help of IRR, the topology of the Internet has become more visible. The essence of IRR is as follows: network operators register their routing policy in the database, namely with whom and how the network interacts, and network set-top boxes that the network uses and announces on the Internet. The formal RPSL language is used to describe policies. There is also a programming toolkit, the most famous of which is IRRToolset, which allows you to automate the configuration of the provider's routing according to IRR data.

D2. Implementation of BGP technology. A technology called "peer lock" (Peer Lock) proposed the construction of BGP peering with the fixation of relations between all neighbouring ASs through the "client-provider" or "neighbour-neighbour" relations. These relationships had to be enforced through administratively defined BGP message filters to protect a particular BGP system from the situation where a "client" or "neighbours" advertise routes to large stubs that they don't really care about. Peer Lock has obvious drawbacks - it is an inflexible administrative interaction mechanism, the impossibility of verifying the declared data, the lack of influence on routes that do not pass through the "defender", and the impossibility of countering prefix capture due to illegitimate source replacement.

D3. Introduction of ARTEMIS. ARTEMIS (from Automatic and Real-Time Detection and Mitigation System) is open-source software that provides the following services to the operating network that deploys it: – monitoring of route updates Real-time BGP using streaming data from special services that collect route data from a distributed network of "sensors"; – Accurate and comprehensive detection of BGP prefix hijacking attacks within seconds of their initiation.

D4. Implementation of the BGPmon service. The BGPmon service monitors the status of routes to the specified prefix on an ongoing basis. The service has an official website at www.bgpmon.com and is currently owned by Cisco. Even before the change of ownership, the service used hundreds of route observation points around the world. The principle of operation of BGPmon is as follows. Once a network prefix is registered with BGPmon, it will be monitored from more than one hundred locations around the world, allowing for regional events to be detected that may not be detected by a single-point monitoring system. Monitoring concerns route hijacking, prefix hijacking, prefix de-aggregation, route source change, or any other violation of the routing policy. The BGPmon web interface allows the user to prioritize each type of alert and message. Information about the notification is displayed in the graphical interface on the map for the regional binding of the detected incident.

It should be noted that the difference between our study and similar ones is that the modelling process takes into account the special conditions for the introduction of cyber warfare and the fact that the proposed cyber defence measures have a powerful security system and are aimed exclusively at mass cyber-attacks.

The model is not a "universal" solution in the framework of cybersecurity, but it involves the use of modern and very strong software measures to counter mass cyber-attacks. That is why the model should be applied already now in such areas as transport, economic and state management. Even though the results of the implementation of the model are not significant, the programs that will be involved will provide some experience for further advances.

The main risks and threats to the economic security of Ukraine in the digital sphere in war conditions are the use of cyber attacks by the enemy for economic, political and military intelligence; destruction of critical infrastructure facilities using digital technologies; obstruction of the activities of state and commercial enterprises, institutions, organizations; spreading fake news to destabilize society. With the growing level of digitalization of the economy, the priority of countering cyber threats is indisputable. Therefore, the digitalization of the economy should be accompanied by a proportional increase in security measures: data protection, risk diversification, training of specialists and dissemination of media literacy. At the same time, the growing budget spending on security measures, which are of key importance in war, creates new risks and challenges for the economic security of the state in the financial sector. That is why there is a need for further research and forecasting of the impact of real threats in the digital sphere on all components of the socio-economic security of the state. The use of digital space in real armed conflicts requires the formation of a methodology for identifying and assessing a new type of digital threat, which is the fundamental basis of state cybersecurity.

Given the achievements of Ukraine in cyberspace, it is legitimate to define it as an equal participant in the international arena in the field of cybersecurity. Promising tasks should be the further improvement of information protection systems for critical infrastructure facilities based on the best world practices, as well as the coordination of actions with international organizations to counter threats associated with the development of the digital economy and the information society. Building an effective cybersecurity system in terms of a comprehensive response to cyber threats will contribute to the formation of a preventive mechanism for countering threats and their containment, a proactive response to dynamic changes taking place in cyberspace.

DISCUSSION

Separately, it should be noted the discussion that the indispensable attributes of modern globalization processes are rapid scientific and technological progress: the digitalization of social relations, the exit of mankind into cyberspace, and the penetration of the virtual world into all spheres of life. In the final version, all of the above form the endless and diverse possibilities of the modern development of the information society. However, along with the development of progressive components, technological progress stimulates the emergence of new challenges and individual threats, including the balance of safe and secure interests at the national and international levels. In recent years, threats of violating the interests of people, the state itself and humanity in general in cyberspace have moved from potential and hypothetical to quite real ones. So countering their spread has become a priority at the national level of governments and the international community.

It should be noted that since the beginning of the war in Ukraine, an unofficial public movement of cyber resistance to the enemy, the so-called "Cyber Army", has become more active. Ordinary people, along with IT professionals, deal a crushing blow by attacking the enemy in cyberspace, causing damage to him and frustrating plans.

1. Try to study and actively analyze cyber defence weaknesses in order to strengthen them daily. Hackers always do a lot of intelligence operations in Ukraine. In this way, they find the weakest points in the defence of our companies and take advantage of this to attack by hitting them. There has never been and never is a 100% secure system. It should be noted that the less the evil of any system costs fraudsters, the higher their motivation will be.
2. Those in the cyber risk zone should continuously monitor the relevant messages on various official resources of the State Service for Special Communications and CERT-UA. These bodies are the first to publish official warnings not only about possible cyber threats but also about how to minimize their risks.
3. You must always remember about the safety of the system, which depends specifically and exactly on each employee. Hackers are able to attack a company or institution and through employees of various companies and institutions, steal their data. The military, as well as all statesmen, are in particular danger. These categories of people should definitely get used to cyber hygiene and accept it as the norm of everyday life, so as not to deal with serious consequences in the event of attacks.
4. For those hackers who carry out dangerous and daily cyber attacks on enemies and are engaged in a bag hunting with a clear plan to improve and strengthen Ukrainian cybersecurity in wartime conditions, in order to avoid unresolved problems with the law enforcement service, you need to be fully prepared to prove that their activities are in line with the interests of Ukraine.

It should be noted that a mega-effective and qualified counteraction to threats to national security in the cyber sphere becomes real only under a certain condition for the integrated use of the entire arsenal of legal means to best ensure cybersecurity. This applies to clauses that apply to all structured elements of public administration and at all stages of information circulation. We can safely say that the best effect lies in the full interaction of the subjects of ensuring the cybersecurity of Ukraine. the national security of Ukraine.

At the same time, digitalization in Ukraine creates additional reserves for the financial stability of the national economy in a war. It is worth noting that even before the war, the financial security of Ukraine was in a limited state with a significant level of risks and threats, as well as some positive trends in general, so the crisis was caused by COVID-19 and the war hit a weak economy. Thus, in the overall structure of Ukraine's exports, a third is the export of IT services, which in 2021 accounted for about 36% along with the agro-industrial complex and the raw materials industry. At the same time, further development of the digital sector of the national economy of Ukraine during the war is envisaged, because it contributes to the inflow of currency into the country and an increase in economic activity in a turbulent period. In addition, the development of the digital sphere also contributed to the formation of a significant source of financial support for the economic security of Ukraine in the conditions of war through the accumulation of crypto resources, the help of crypto investors and crypto exchanges.

Discussing our research results, we should highlight their innovativeness. The innovative elements of the obtained results are the presented processes in the form of blocks for ensuring the cybersecurity of the socio-economic system in a state of martial law.

DOI: 10.55643/fcaptp.3.50.2023.4075

CONCLUSIONS

One of the main instruments of politics, international politics, in particular, is information. Distortion of information heightens tension, especially in times of war, and alters the perception of facts to suit the preferences of the actors seeking to influence. It should be noted that advances in the field of digital media, and the abolition of information borders, leave countries open and vulnerable to interference in their political and information space by other states. The information space affects economic, political and cultural processes, the development of military affairs and technology. With the accelerated transition to digital control systems, the threat of cybersecurity has increased, because Ukraine has always been among the strategic goals of russia's foreign policy among other countries, so we strive to ensure cybersecurity. Cybersecurity in a war is of particular importance since today it is almost impossible to imagine a single object of technological infrastructure that would not be equipped with various software systems, many of which have access to the Internet, which carries serious risks. Cyberattacks can be used as an auxiliary tool in the framework of information warfare, with the aim of cracking classified data and publishing it, or "throwing in" fake information, including with reference to sources that inspire confidence. All this makes us look at the problem of cybersecurity in a new way, especially when it comes to dangerous objects or life support systems. Threats in cyberspace are the most serious for the national security of Ukraine. Cybersecurity is now a key issue in economic, political, social and military aspects. However, it remains a less understood and underestimated threat. Therefore, it should be understood that cyberspace is currently the most important theatre of warfare. The struggle for cyber dominance - and therefore the ability to withstand cyber-attacks - means a new era of military relations that will significantly change the nature and structure of the military. It should also be noted that cybersecurity cannot be achieved at the state level. It needs to integrate the efforts of both the private sector and enterprises, international coordination and cooperation on an unprecedented scale.

Since the beginning of the full-scale invasion, the russian-Ukrainian war has demonstrated that the cyberattacks of the aggressor coincide with military actions, that is the capture or destruction of critical infrastructure. Note that russia has used hacking campaigns to support its full-scale attack on Ukraine, combining malware with missiles in several attacks, including on television stations and government institutions. We believe that the training of relevant specialists in our case in the military, political, and industrial spheres plays an important role in creating an effective cybersecurity system, because one of the main problems in ensuring cybersecurity in Ukraine is insufficient professionalism - even with advanced technologies, the country still lacks appropriate specialists. Given the situation in Ukraine, it is difficult to resist the cyberattacks that russia is using. Thus, thanks to the vigorous activity of pro-European forces and with the constructive support of external players, Ukraine manages to resist the russian federation.

As a result, a modern information model for ensuring the cybersecurity of the socio-economic system under martial law has been obtained. The study is limited by taking into account only the features of ensuring the cybersecurity of the socio-economic system in the conditions of the martial law of one country. Prospects for further research should be devoted to ensuring the cybersecurity of the socio-economic system in the post-war period.

REFERENCES

1. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
2. Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. In: Pan, Z., Cheok, A., Müller, W., Zhang, M., El Rhalibi, A., Kifayat, K. (eds) Transactions on Edutainment XV. Lecture Notes in Computer Science, vol 11345. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59351-6_9
3. Fakiha, B. (2021). Business organization security strategies to cybersecurity threats. International *Journal of Safety and Security Engineering, 11*(1), 101-104. https://doi.org/10.18280/ijsse.110111
4. Shtangret, A., Korogod, N., Bilous, S., Hoi, N., & Ratushniak, Y. (2021). Management of Economic Security in the High-Tech Sector in the Context of Post-Pandemic Modernization. *Postmodern Openings, 12*(2), 535-552. https://doi.org/10.18662/po/12.2/323
5. Kryshtanovych, M., Lyubomudrova, N., Bondar, H., Motornyy, V., & Kuchmenko, V. (2023). An intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. *Ingénierie des Systèmes d'Information, 28* (1), 41-47. https://doi.org/10.18280/isi.280105
6. Weru, T., Sevilla, J., Olukuru, J., Mutegi, L., & Mberi, T. (2017). Cyber-smart children, cyber-safe

teenagers: Enhancing internet safety for children. 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, pp. 1-8. https://doi.org/10.23919/ISTAFRICA.2017.8102292

7. Kryshtanovych, M., Ortynskyi, V., Krasivskyy O., Maziy, N., & Pasichnyk, V. (2021). 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), 202–208. https://doi.org/10.18371/.v4i39.241309
8. Sylkin, O., Bosak, I., Homolska, V., Okhrimenko, I., & Andrushkiv, R. (2021). Intensification of Management of Economic Security of the Enterprise in the Post-Pandemic Space. *Postmodern Openings, 12*(1Sup1), 302-312. https://doi.org/10.18662/po/12.1Sup1/286
9. Sylkin, O., Buhel, Y., Dombrovska, N., Martusenko, I., & Karaim, M. (2021). The Impact of the Crisis on the Socio-Economic System in a Post-Pandemic Society. *Postmodern Openings, 12*(1), 368-379. https://doi.org/10.18662/po/12.1/266
10. Musman, S., & Turner, A. J. (2018). A game oriented approach to minimizing cybersecurity risk. *International Journal of Safety and Security Engineering, 8*(2), 212-222. https://doi.org/10.2495/SAFE-V8-N2-212-222
11. Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering, 11*(5), 537-545. https://doi.org/10.18280/ijsse.110505
12. Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., & Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. *International Journal of Safety and Security Engineering, 11*(4), 361-367. https://doi.org/10.18280/ijsse.110409
13. Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International *Journal of Safety and Security Engineering, 12*(3), 299-310. https://doi.org/10.18280/ijsse.120304
14. Carlin, J. P. (2016). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. Harvard National Security Journal, 7, 391-577. https://www.csis.org/events/detect-disrupt-deter-whole-government-approach-national-security-cyber-threats
15. Rodrigues, A.R.D., Ferreira, F.A., Teixeira, F.J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance, 60*, 101616. https://doi.org/10.1016/j.ribaf.2022.101616
16. Shakhatreh, H. (2023). Payment of canal dues by carriers carrying out international overseas transportation – A case of legal discrimination. *Studia Iuridica Lublinensia, 32*(1). https://doi.org/10.17951/sil.2023.32.1.251-273
17. Al Azzam, F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. *JANUS.NET e-journal of International Relations, 10*(1). https://doi.org/10.26619/1647-7251.10.1.5
18. Alazzam, F.A.F., Saleh A., & Aldou Kh. (2020). Impact of pandemic COVID-19 on the legal regulation of world trade activity using the example of the medical supplies. *Wiadomości Lekarskie, 23*(7), 1521-1527. https://doi.org/10.36740/WLek202007139
19. Kryshtanovych, S., Gutsulyak, V., Huzii, I., Helzhynska, T., & Shepitchak, V. (2021). 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), 289-302. https://doi.org/10.3846/bmee.2021.14798
20. Sylkin, O., Kryshtanovych, M., Bekh, Y., & Riabeka, O. (2020). Methodology of forming model for assessing the level financial security. *Management Theory and Studies for Rural Business and Infrastructure Development, 42*(3), 391-398. https://doi.org/10.15544/mts.2020.39

Іжа М., Пахомова Т., Липач О., Якубовський О., Ахламов А.

МОДЕЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СОЦІАЛЬНО-ЕКОНОМІЧНОЇ СИСТЕМИ В УМОВАХ ВОЄННОГО СТАНУ

Індустрія 5.0 уже поступово починає проявлятися в різних аспектах нашого життя. Особливо чутливою вона є в забезпеченні соціально-економічного розвитку. Разом із цим посилюються кіберзагрози, які мають негативний

DOI: 10.55643/fcaptp.3.50.2023.4075

вплив на забезпечення економічної безпеки. Саме тому виникає нагальна потреба захисту інформації в умовах війни. Основною метою роботи є визначення шляхів забезпечення кібербезпеки соціально-економічної системи в умовах воєнного стану. Об'єктом дослідження є система забезпечення кібербезпеки. Як результат дослідження представлено авторську модель забезпечення кібербезпеки в умовах війни. Для цього застосовано сучасний метод моделювання структурних систем. Практичну й наукову значимість отриманих результатів дослідження можна представити у вигляді інформаційної моделі забезпечення кібербезпеки соціально-економічної системи в умовах воєнного стану. Інноваційними елементами отриманих результатів є представлені процеси забезпечення кібербезпеки, що дає змогу деталізувати ключові ідеї моделювання. Дослідження має обмеження у вигляді врахування лише особливостей забезпечення кібербезпеки соціально-економічної системи в умовах воєнного стану однієї країни.

Ключові слова: воєнний стан, безпека, кібербезпека, інформація, модель, забезпечення безпеки, система, соціально-економічна система

JEL Класифікація: K24, F52, K22, H56