Advances in Economics, Business and Management Research, volume 170
Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021)

Ensuring the Stability of Ukraine's Cybersecurity System in the Current Context

Liliia Veselova[1 *] [0000-0001-6665-0426], Tetiana Rekunenko[2] [0000-0001-7668-0581]

[1]*Odesa State University of Internal Affairs, Odesa, Ukraine*
[2]*Donetsk Law Institute of the Ministry of Internal Affairs of Ukraine, Kryvyi Rih, Ukraine*
[*]*cvet-Liliya@ukr.net*

ABSTRACT
The paper pays special attention to the issue ensuring the stability of Ukraine's cybersecurity system in today's conditions. A number of tested effective methods of foreign countries, which are used during illegal actions in cyberspace, are considered. It is determined that in modern conditions of cybersecurity of Ukraine, stability as a socio-cultural phenomenon, turns into a complex multidimensional concept, which as a fundamental principle determines the crucial role of the security facilities themselves, which at the same time become key actors in cybersecurity. At the same time, cybersecurity does not primarily depend on the nature or level of cyber threat, but on the ability of cybersecurity actors to resist them, the vulnerability and ability of the national cybersecurity system in the context of cyberattacks, cybercrimes, etc. It is concluded that ensuring the stability of the state should be addressed by addressing strategic and critical issues of cybersecurity, critical infrastructure, strengthening the resilience of society as a whole, as well as monitoring the vulnerability of the national cybersecurity system.

Keywords: *crisis situation, cyberattack, cyber incident, monitoring, risk assessment, vulnerability.*

1. INTRODUCTION

In the current context, the development of the information society and its legal framework guarantee the effectiveness of information rights and responsibilities of citizens, determine the development degree of the information sphere of Ukraine, the state of information law and order, the level of legal protection and protection of social values. At another point, our sphere of life is covered by information technologies, information and telecommunication systems, and victims of hackers can become not only people, but also the whole state. That is why cybersecurity is one of the main problems not only in Ukraine, but in the whole world. Thus, the issue of national security in general, in particular its information component, requires the formation of a security environment and "sustainability" of society. In addition, real administrative and legal reforms on administrative and legal support of cybersecurity in Ukraine encourage the formation of appropriate legal regulation of key modern approaches to cybersecurity and improve the system and methods to combat cyber threats.

For Ukraine, the study and use of positive foreign experience in ensuring the stability of the state and society in the field of national security is due primarily to the need to form a new quality of domestic security and defense sector, which should have the characteristics of sustainable systems: smooth operation (normal) mode, adaptation to changing conditions; ability to withstand unexpected shocks; restoration after the destructive consequences of phenomena/actions of any nature to the desired equilibrium (at the previous or new level) provided that the continuity of the management process is maintained [1]. The purpose of this study is to identify the main directions and key measures to ensure the stability of the system in the field of cybersecurity in Ukraine.

2. RESEARCH METHODOLOGY

To achieve this goal, general scientific and special methods are used, which are tools of scientific research (formal-legal method, comparative method, method of scientific abstraction, etc.). The reports of the State Service for Special Communications and Information Protection of Ukraine and the Governmental Computer Emergency Response Team of Ukraine CERT-UA on statistics on cyberattacks and detected cyber incidents were used.

3. RESEARCH RESULTS

Development issues to increase resistance of cyber threats, the emphasis should be put on identifying vulnerabilities [2] society for them and coordinated activities for estimation and forecasting referred threats [3]. Vulnerability assessment is a process of "scanning" of the information environment, aimed at identifying gaps in this chain, through which an attacker can make a cyberattack [4].

In course, a cyberattack is any illegal action in the information environment by a cyber offender.

In order to obtain (stole) confidential information or data [5], disable critical infrastructure objects, etc.

Today, there are a huge number of types of cyberattacks - attacks that aim to overflow the network bandwidth of the server, making it inaccessible; attacks that target the server's system resources, causing it to stop responding to legitimate requests; attacks in the form of software vulnerabilities' using (this type of attack targets a specific vulnerability in the server software to disable it or gain control over it), etc. Only for the last 3 months, according to the operative information of the State Special Communications Service for the protection of state information resources, more than 26 million suspicious events have been registered by the cyber protection system of state information resources and critical infrastructure at monitoring facilities (Figure 1) and more than 70,000 of attacks of various kinds (Figure 2), which the system of secure access of government agencies to the Internet blocked.

The vast majority (more than 90%) are applicationlevel network attacks [6] (SQL injections, DNS cache poisoning, cross-site scripting, HTTP session manipulation, distributed denial of service, etc.). For network attacks, the main factor is the object of attack, such as attacks on tools, control systems, networks, main equipment, etc. [7]. Thus, the Internet space (online stores, online money transfers, payment of electronic bills, online replenishment of mobile accounts, etc.) is characterized by injection attacks (the attacker inserts malicious code into the lines transmitted to the server for parsing and execution). SQL Attack (SQLIA) is the most common type of vulnerability, in which an attacker receives an arbitrary query to the database to obtain personal information about other users [8]. To protect important business information, as well as information about customers and other stakeholders in the financial sector, it is advisable to use methods of analysis and risk management in banking systems to ensure the security of banking operations on the Internet [9]. Researchers also consider it necessary to develop a methodology for recognizing applied-level cyberattacks by their artifacts for use in forensic research [10].

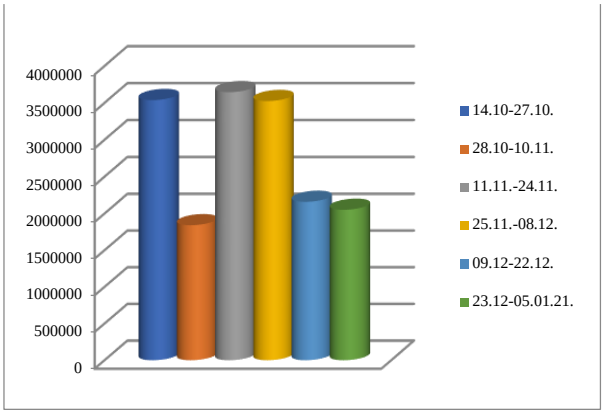

Figure 1

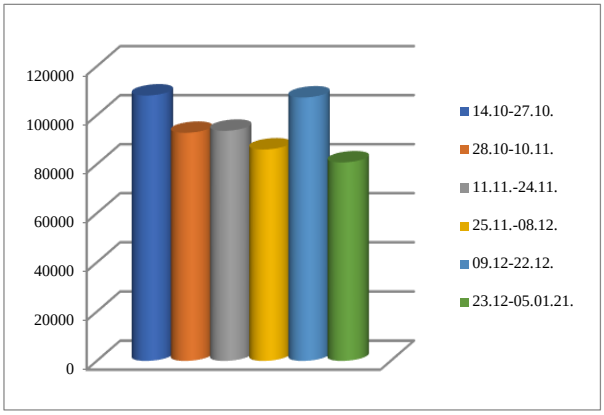

Figure 2

The second place in terms of quantity is occupied by attacks such as "Harvest Attack" [6]. One of the most effective tools for protecting corporate mail from BEC scams is the cloud service to protect the company's mail traffic SaaS security solution Panda Cloud Email Protection - a kind of e-mail firewall- to prevent all types of threats and attacks through corporate mail. The principle of operation is as follows: when a DHA attack is detected, the IP address used by the suspicious sender becomes temporarily banned and excluded from the allowed traffic, including that traffic that may seem legitimate [11].

The American multinational company Cisco offers its product to protect corporate mail. The Cisco Advanced Malware Protection (AMP) system provides in-depth monitoring, control and retrospective analysis to control the flow of data at the input and output of the enterprise environment [12].

Among the statistics on the website of the State Special Service for the Protection of State Information Resources are also some figures on DDoS attacks, the vast majority of which relate to the web resources of the Office of the President of Ukraine and the National Anti-Corruption Bureau of Ukraine [6]. Schematically, a DDOS attack (UDP flood, TCP flood, TCP SYN flood, Smurf attack, ICMP flood) looks like this: a huge number of erroneous requests from many computers from

different parts of the world crashes on the server selected as a victim. As a result, the server spends all its resources on servicing these requests and becomes virtually inaccessible to ordinary users. An effective method in the above crisis situations is to simulate data traffic during global cyberattacks. Simulation techniques include additional precautions such as increasing the size of the virtual memory paging file to the maximum level allowed by the OS. Modeling can be useful for electronic government systems, which should support the ability to work in crisis situations [13].

It is known that cyber threats lead to a significant loss of network resources and can lead to "disability" of the system as a whole. The use of countermeasures for certain threats can reduce the impact on the system. One of the main tasks to prevent or reduce the impact of cyberattacks on information systems is to monitor the state of network equipment and the ability to support network infrastructure during critical situations in working condition [14].

Since October 2020, the Government Computer Emergency Response Team of Ukraine CERT-UA has registered and processed more than 35,000 cyber incidents (Figure 3).

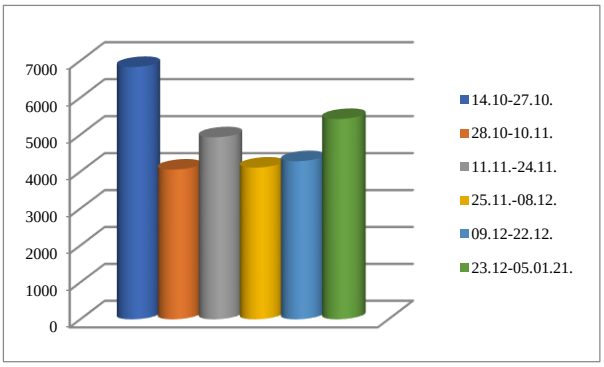

Figure 3

The majority of incidents concerns the distribution of malicious software (more than 95%) [6]. Among the methods of cyber incident monitoring, a networkcentric method of cyber incident monitoring has been developed and is used, which allows to identify the most important objects of protection and to predict the category of cyber incidents that may occur as a result of cyberattack and their criticality. Tools that have been developed based on a network-centric method can be useful for cyber incident response teams such as CERT / CSIRT to effectively handle and adequately respond to cyber incidents [15].

Information security largely depends on the reliability of the operating system, as it is an intermediary and controller of hardware and application software of information and telecommunication systems, but we must not forget about measures related to the risks of vulnerability of computer systems in general [16; 17]. To assess the reliability of the operating system, scientists have proposed an analytical approach to assessing and comparing the risk of vulnerabilities in operating systems [18]. It is worth mentioning among the effective practices of foreign countries statistical methods (used to detect cyberattacks on computer networks). Methods of statistical analysis have different interpretations based on different dynamics of network traffic characteristics; the advantage of using statistical methods is the ability to immediately record the negative impact on the object. Statistical methods do not require constant updating of databases, which greatly simplifies the maintenance of these systems. They can detect unknown attacks, etc. [19].

The latter researches show that a significant percentage of vulnerabilities are traced by mobile users. These vulnerabilities need to be reduced, firstly, by making users aware of cyber threats and implementing security policies and procedures (basic security guidelines, such as installing licensed antivirus software on devices, password management instructions, etc.) [18].

To identify key vulnerabilities, taking into account specific hybrid indicators, it is necessary to analyze the risks affecting institutions and networks, understand risk management, which is a systematic process of risk assessment and resolution to ensure the sustainability of organizations, persons in various fields [20].

The ever-increasing digitalization has an integral dimension of security, which poses particular challenges to the resilience of information network systems around the world, as cyberattacks know no borders.

Cybersecurity is critical to both prosperity and security. As everyday life and the economy become increasingly dependent on digital technology, society is becoming more vulnerable. Strong cyber resilience requires a collective and broad approach that provides for more robust and effective structures that promote cybersecurity and respond to cyberattacks in countries, institutions, agencies, missions and operations. Awareness of cybersecurity in institutions should be raised by improving the safety culture and strengthening training.

4. DISCUSSION OF RESULTS

In the current context of cybersecurity in Ukraine, resilience as a socio-cultural phenomenon is becoming a complex multidimensional concept, which as a fundamental principle defines the crucial role of security objects themselves, which also become key actors in cybersecurity. At the same time, cybersecurity primarily depends not on the nature or level of cyber threat, but on the ability of cybersecurity actors to resist them, the vulnerability and ability of the national cybersecurity system in the context of cyberattacks, cybercrimes, etc. Sustainability can practically be achieved through the formation of public-private partnerships and the necessary culture of cybersecurity actors, borrowed and the use of foreign proven methods to detect and prevent

cyberattacks. It is necessary to focus not only on forecasting situations, but also to deal with the formation of administrative and legal mechanism (precautionary mechanism). This mechanism must consist of such aspects as formation of the system's resilience to cyber threats and attack prediction, risk forecasting, risk management. Sustainability in the field of cybersecurity is formed based on the understanding of cyberspace as one that has fundamental uncertainties about the nature and forms of cyber threats, the time of their manifestation and spread, and therefore acquires the content of the target setting on the basis of regulatory implementation of effective administrative regulation and implementation of a system for assessing the risks of cyber threats and determining the vulnerability of society as a precautionary measure. Thus, the concept of "sustainability" is not just a successful text construct used in developed countries and international organizations.

5. CONCLUSION

Ensuring the resilience of the state should be addressed by addressing strategic and critical issues of cybersecurity, critical infrastructure, strengthening the resilience of society as a whole, and monitoring the vulnerability of the national cybersecurity system: capacity building through support measures, coordination and communication on modern technology and innovation. cybersecurity; raising the culture in the field of cybersecurity, creating special educational platforms and coordinating training opportunities in the field of cybersecurity; providing an interagency (inter sectoral) systemic approach to countering threats to encroachment on critical infrastructure, taking into account the interrelationships and on the basis of the implementation of measures within the work processes to prevent, ensure preparedness and response; formation of indicators' system of potential vulnerability of critical infrastructure objects to hybrid threats and measures to eliminate shortcomings and increase resilience; increasing the efficiency of development of the system of formation, reproduction and use of human resources on the basis of formation and consideration of key characteristics of competence, effective process of human resources management; development of information and analytical direction based on using of modern methodologies and tools; capacity building of analytical (situational) centers, newly created units that implement tasks based on international standards; structured cooperation in order to raise public awareness and education, including targeted campaigns on social networks, to separate misinformation from information, prevent the spread of hostile misinformation and hybrid external interference in information idleness.

It is necessary to take measures to raise awareness of key societal vulnerabilities through monitoring and risk assessment, taking into account the assessment level of specific cyber threats; developing a methodology for assessing cybersecurity risks and measures to prevent, respond to and recover by identifying and implementing effective procedures, as well as by studying the application and practical implications of interdepartmental communication capabilities in cases of large-scale and significant hybrid attacks (development of an interagency operational protocol outlining the crisis management process in the event of a cyberattack; creating a mechanism for rapid response to events caused by cyber threats to coordinate the activities of response forces and early warning systems, outlining ways to coordinate, summarize and analyze analytical materials).

REFERENCES

[1] Reznikova, O.O. (2017), "Urgency of building of state and public resilience to terrorist threat in today's environment", *Strategic priorities*, No. 3 (44), pp. 23-24.

[2] Korystin, O.Ye. and Svyrydyuk, N.P. (2020), "Methodological principles of risk assessment in law enforcement activity", *Nauka i pravooxorona*, vol. 3, pp. 191-197. DOI: https: //doi.org/10.36486/np.2020.3(49).19

[3] Koval`chuk, T.I. Korystin, O.Ye. and Svyrydyuk, N.P. (2019), "Hybrid threats in the civil security sector in Ukraine", *Nauka i pravooxorona*, vol. 3 (45), pp. 69-79. DOI: doi.org/10.36486/np.2019308

[4] I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita and Dewa Made Sri Arsa (2020), "Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City)". *International Journal of Computer Network and Information Security*, Vol. 12, No. 4, pp. 30-40. DOI: 10.5815/ijcnis.2020.04.03.

[5] Qamar Atta Ul Haq (2019), "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan", *International Journal of Computer Network and Information Security*, Vol. 11, No. 1, pp. 62-69. DOI: 10.5815/ijcnis.2019.01.06.

[6] Operational information of the State Special Communication on the protection of state information resources, Website of Prosecutor General's Office of Ukraine, available at: https://cip.gov.ua/ua/filter?tagId=8252.

[7] Tumer, H. White, J. Camelio, H. and et al. (2015), "Are modern production systems reliable?", *Open Systems*, No 3, pp. 29-33.

[8] Harish Dehariya, Piyush Kumar Shukla and Manish Ahirwar (2016), "A Survey on Detection and Prevention Techniques for SQL Injection Attacks", *International Journal of Wireless and Microwave*

Technologies, Vol. 6, No. 6, pp. 72-79. DOI: 10.5815/ijwmt.2016.06.08.

[9] Joseph A. Ojeniyi, Elizabeth O. Edward and Shafii M. Abdulhamid (2019), "Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study", *International Journal of Education and Management Engineering*, Vol. 9, No. 2, pp. 1-14. DOI: 10.5815/ijeme.2019.02.01.

[10] Snigurov, A. Balashov, V. and Serdyk, A. (2017), "Analysis of mechanisms of network attacks at the application layer for criminal investigations of cyber crimes. *Collection of scientific works of Kharkiv National University of the Air Force*, No 2 (51), pp. 64-68.

[11] Next-gen antivirus to protect your digital life, available at: https://www.pandasecurity.com

[12] Website of Cisco, available at: www.cisco.com/go/emailsecurity.

[13] Mosorov, Volodymyr Kosowski, Andrzej Kolodiy, Roman and Kharkhalis, Zenoviy (2015), "Data Traffic Modeling During Global Cyberattacks", *International Journal of Computer Network and Information Security*, Vol. 7, No. 11, pp. 20-36. DOI: 10.5815/ijcnis.2015.11.03.

[14] Tolubko, Volodymyr Vyshnivskyi, Viktor Mukhin, Vadym Haidur, Halyna Dovzhenko, Nadiia Ilin, Oleh and Vasylenko, Volodymyr (2018), "Method for Determination of Cyber Threats Based on Machine Learning for Real-Time Information System", *International Journal of Intelligent Systems and Applications*, Vol. 10, No. 8, pp. 11-18. DOI: 10.5815/ijisa.2018.08.02.

[15] Zhengbing Hu, Viktor Gnatyuk, Viktoriia Sydorenko, Roman Odarchenko and Sergiy Gnatyuk (2017), "Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure", *International Journal of Computer Network and Information Security*, Vol. 9, No. 6, pp. 30-43. DOI: 10.5815/ijcnis.2017.06.04.

[16] Alhazmi, O.H. Malaiya, Y.K. and Ray I. (2007), Measuring, analyzing and predicting security vulnerabilities in software systems, *International Journal of Computers and Security Journal*, Vol. 26, No. 3, pp. 219–228.

[17] Alhazmi, O.H. and Malaiya, Y.K. (2008), "Application of Vulnerability Discovery Models to Major Operating Systems", *IEEE Transactions on Reliability*, Vol. 57, No. 1, pp. 14-22.

[18] Noah N. Gana, Shafi'i M. Abdulhamid and Joseph A. Ojeniyi (2019), "Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria", *International Journal of Information Engineering and Electronic Business*, Vol. 11, No. 2, pp. 35-43. DOI: 10.5815/ijieeb.2019.02.05.

[19] Zhengbing Hu, Roman Odarchenko, Sergiy Gnatyuk, Maksym Zaliskyi, Anastasia Chaplits, Sergiy Bondar, Vadim Borovik (2020), "Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior", *International Journal of Computer Network and Information Security*, Vol. 12, No. 6, pp. 1-13. DOI: 10.5815/ijcnis.2020.06.01.

[20] Dugguh, S.I. and Diggi, J. (2015), "Risk Management Strategies in Financial Institutions in Nigeria: the Experience of Commercial Banks", No 2(6), pp. 66–73**.**